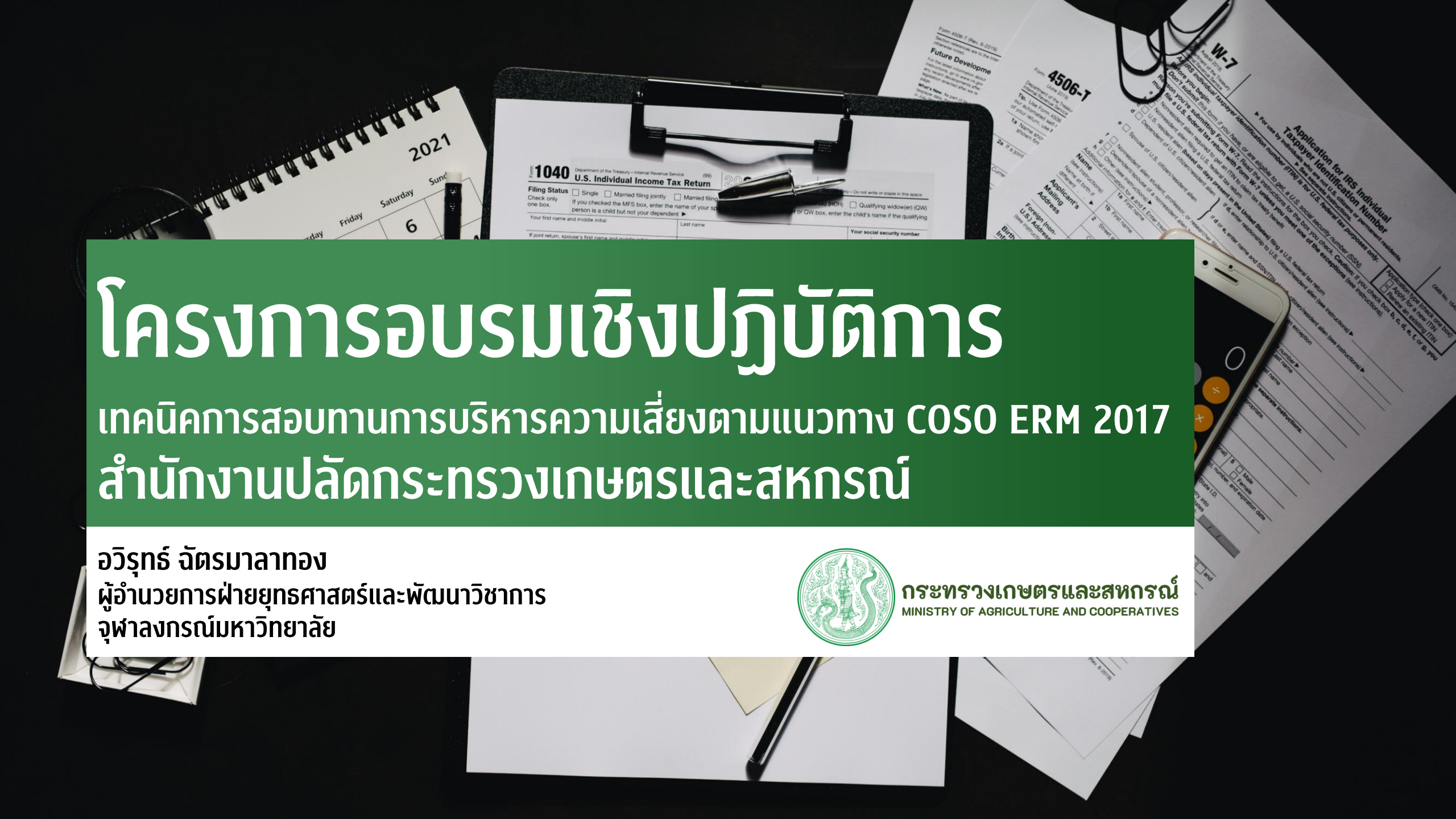


โครงการอบรมเชิงปฏิบัติการ

เทคนิคการสอบทานการบริหารความเสี่ยงตามแนวทาง COSO ERM 2017

สำนักงานปลัดกระทรวงเกษตรและสหกรณ์

อวิรุทธ์ ฉัตรมาลาทอง
ผู้อำนวยการฝ่ายยุทธศาสตร์และพัฒนาวิชาการ
จุฬาลงกรณ์มหาวิทยาลัย

กระทรวงเกษตรและสหกรณ์
MINISTRY OF AGRICULTURE AND COOPERATIVES

Profile

อวิรุทธ์ ฉัตรมาลาทอง

Education:

Ph.D. (Higher Education), Chulalongkorn University
M.Ed. (Nonformal Education), Chulalongkorn University
B.Econ (Business Economics), RMUTTO
Certificate Risk Management, IOD, Chulalongkorn University
Certificate Fraud Risk Prevention & Control, Omega Worldclass

Experience:

- ผู้อำนวยการฝ่ายยุทธศาสตร์และพัฒนาวิชาการ จุฬาลงกรณ์มหาวิทยาลัย
- ผู้อำนวยการศูนย์บริหารความเสี่ยง จุฬาลงกรณ์มหาวิทยาลัย
- หัวหน้าโครงการที่ปรึกษาด้านการบริหารความเสี่ยงและควบคุมภายใน การท่าเรือ CU Enterprise
- นักวิจัยโครงการ พัฒนาแรงจูงใจในการสร้างนวัตกรรมการปฏิรูปประเทศ สำนักงาน ป.ย.ป.
- นักวิจัยโครงการ Improvement and Development of Thailand IDEs Measures สอวช.
- นักวิจัยโครงการ Thailand Innovation Investment Ecosystem สอวช.
- นักวิจัยโครงการ Thailand : Scaleup Nation 2030 บริษัท Ananda Development
- รองหัวหน้าโครงการวิจัยพัฒนามหาวิทยาลัยแห่งการประกอบการ สอวช.
- นักวิจัยโครงการประเมินความเป็นผู้ประกอบการของมหาวิทยาลัย สวทน.
- รองประธานโครงการจัดตั้งสถาบันนวัตกรรมบูรณาการแห่งจุฬาลงกรณ์มหาวิทยาลัย
- กรรมการและผช.เลขานุการคณะกรรมการกำกับการบริหารความเสี่ยง จุฬาลงกรณ์มหาวิทยาลัย
- กรรมการบริหารความเสี่ยงและวางระบบควบคุมภายใน จุฬาลงกรณ์มหาวิทยาลัย
- วิทยากร Risk Management : โรงพยาบาลศิริราช,สถาบันคลังสมองของชาติ, ม.มหิดล, จุฬาฯ

Expertise:

- การบริหารความเสี่ยงและควบคุมภายใน (Risk Management & Internal Control)
- การวางแผนเชิงกลยุทธ์และงบประมาณ (Strategic Planning & Budgeting)
- การบริหารมหาวิทยาลัยแห่งการประกอบการ (Entrepreneurial University Management)
- การพัฒนาคุณภาพการศึกษา (Educational Quality Development)
- การออกแบบโมเดลพันธกิจหน่วยงานภาครัฐ/มหาวิทยาลัย (Mission Model Design)

AGENDA

กระทรวงเกษตรและสหกรณ์
MINISTRY OF AGRICULTURE AND COOPERATIVES

1 การเปลี่ยนแปลง ความเสี่ยง และโอกาสขององค์กรในยุค BANI ปี 2023
Change, Risks & Opportunities in the 2023 BANI era

2 หลักการและแนวคิดสำคัญในการบริหารความเสี่ยงระดับองค์กร
Foundation & Concept of Organizational Risk Management

3 แนวป้องกันสามด่าน 3-Lines of Defense & CSA
Strengthening the Organizational Governance & Risk Management

4 เทคนิคการสอบทานการบริหารความเสี่ยงตามแนวทาง COSO ERM 2017
Organizational Risk Management Identification

AGENDA

กระทรวงเกษตรและสหกรณ์
MINISTRY OF AGRICULTURE AND COOPERATIVES

1 การเปลี่ยนแปลง ความเสี่ยง และโอกาสขององค์กรในยุค BANI ปี 2023
Change, Risks & Opportunities in the 2023 BANI era

2 หลักการและแนวคิดสำคัญในการบริหารความเสี่ยงระดับองค์กร
Foundation & Concept of Organizational Risk Management

3 แนวป้องกันสามด่าน 3-Lines of Defense & CSA
Strengthening the Organizational Governance & Risk Management

4 เทคนิคการสอบทานการบริหารความเสี่ยงตามแนวทาง COSO ERM 2017
Organizational Risk Management Identification


BANI
WORLD

THE VUCA WORLD HAS EVOLVED INTO BANI WORLD.

VUCA has ...

- lost its descriptive meaningfulness
- become not suitable for today's relevance

BANI facilitates ...

- new perspectives
- an accurate description of the current situation, emotional states, and causal connections

VUCA vs. BANI

From the **1980s** shaped by the Cold War

From **2020** shaped by climate and global systemic change

serves to describe the situation of **ambiguity** and **complexity** ← THE ACRONYM → serves to describe the situation of the **Next Generation of Business**

- **V**olatile
- **U**ncertain
- **C**omplex
- **A**mbiguous

- **B**rittle
- **A**nxious
- **N**on-linear
- **I**ncomprehensible

„WORN-OUT" „UP TO DATE"

Brittle
โลกใหม่ที่เปราะบาง

Anxiety
โลกใหม่ที่เต็มไปด้วย ความวิตกกังวล

Nonlinear
โลกใหม่ที่ความสัมพันธ์ ของสิ่งต่างๆ ไม่เป็นเส้นตรง

Incomprehensible
โลกใหม่ที่เข้าใจได้ ยากกว่าเดิม

Brittleness requires	Anxiety asks for	Nonlinearity calls for	Incomprehensi-bility demands
capacity & resilience	empathy & mindfulness	context & adaptivity	transparency & intuition


CRYPTO
FOCUS
กรุงเทพธุรกิจ
SELL
FTX
ตลาดคริปโทฯ โคม่า
หวั่นวิกฤติ FTX จ่อซ้ำรอย LUNA ?


THE STANDARD
KEY MESSAGES
ค่าครองชีพทิ้งห่าง
ค่าจ้างขั้นต่ำ


Uber
ปรากฏการณ์ Tech Company เลิกจ้าง-ชะลอการจ้างงาน
สัญญาณเตือนเศรษฐกิจถดถอยทั่วโลก ?
MARKETINGOOPS.COM


DROIDSANS
มีหลายคนไม่สมควรอยู่ที่นี่ต่อ
Meta เตรียมปลดพนักงานชุดใหญ่
พร้อมปรับลดการจ้างวิศกรลง 40%

631
6,327
7,462
5,825
22,707
29,299
21,668
21,332
10,662
22,758
35,903
JAN 2022
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV

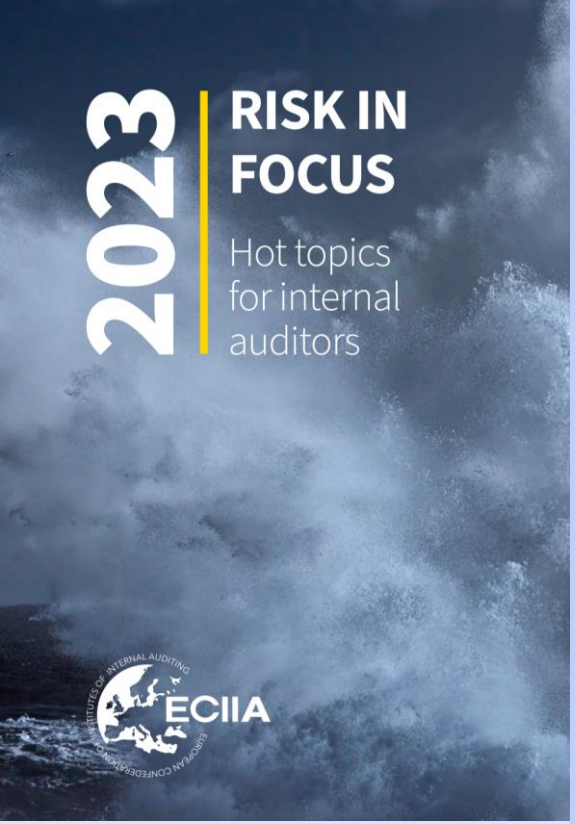

The MATTER
19 ส.ค. 2565
‘Quiet Quitting’ เทรนด์ใหม่มาแรง
เมื่อการทำงานหนักๆ ไม่ใช่คำตอบ
จะทุ่มเทเท่าที่จำเป็นก็ไม่ใช่เรื่องแย่


The MATTER
20 ต.ค. 2565
วัยรุ่นจีนนำเทรนด์ ‘ปล่อยให้เน่าไป’
เมื่อสังคมโหดร้าย ก็ปล่อยวางเรื่อง
ความสำเร็จ และทิ้งความทะเยอทะยานซะ

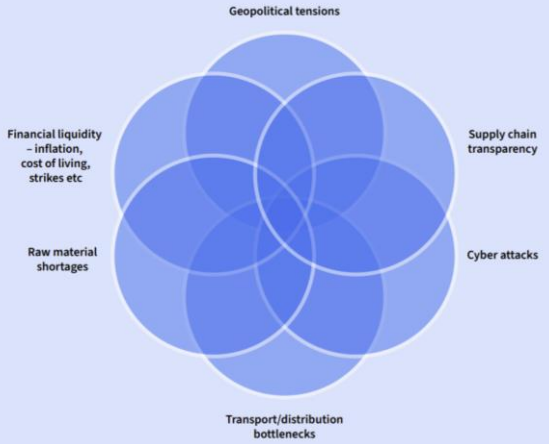

TNN
ONLINE
โควิดปี66ระบาดระลอกเล็ก
หากไม่มีการกลายพันธุ์ของเชื้อรุนแรง

แม้เปิด 2FA ก็ถูกแฮกได้ !!

ด้วยการขโมย "คุกกี้" บนเบราว์เซอร์

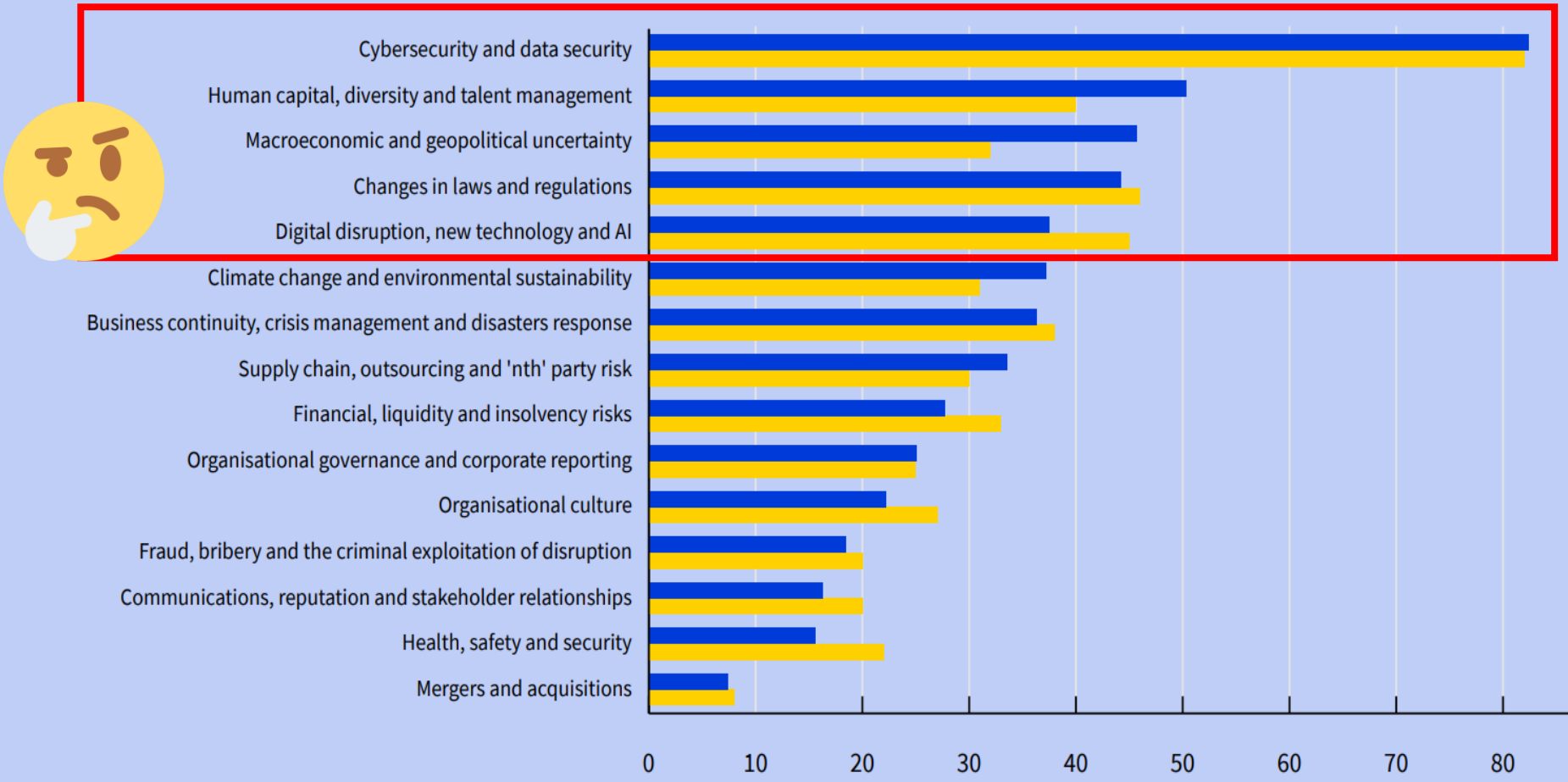


Venn Diagram Illustrating the Perfect Storm of High-Impact Interlocking Risks



What are the top five risks your organisation currently faces?

Human capital risk moves into second place this year followed by macroeconomic and geopolitical uncertainty.



KPMG

Internal Audit Key risk areas 2023

01 Economical and geopolitical uncertainty

02 Climate change

03 Talent acquisition and retention

04 ESG (Environmental, Social and Governance) reporting

05 Cyber security and data privacy

06 Organizational culture and behavior

07 Third-Party relationships and supply chain

08 Digital disruption and new technologies

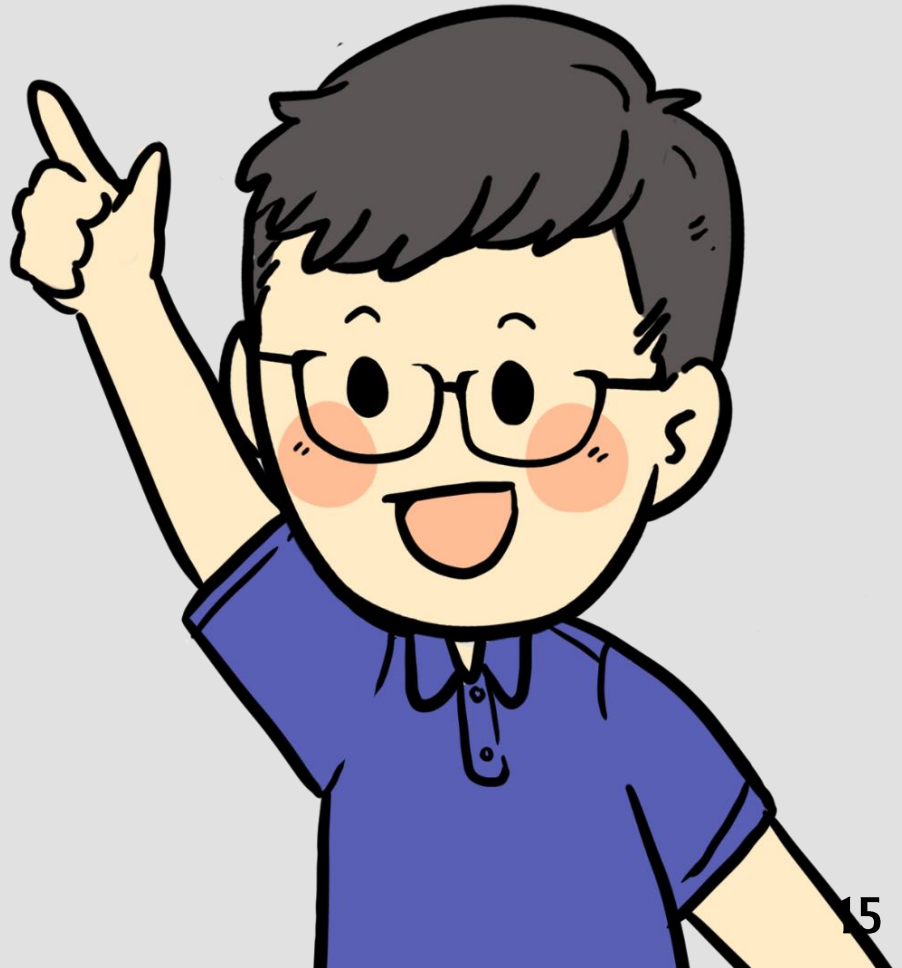
09 Business continuity and crisis response

10 Mergers and acquisitions

Organization's Risks Sharing

ท่านคิดว่าขณะนี้องค์กร

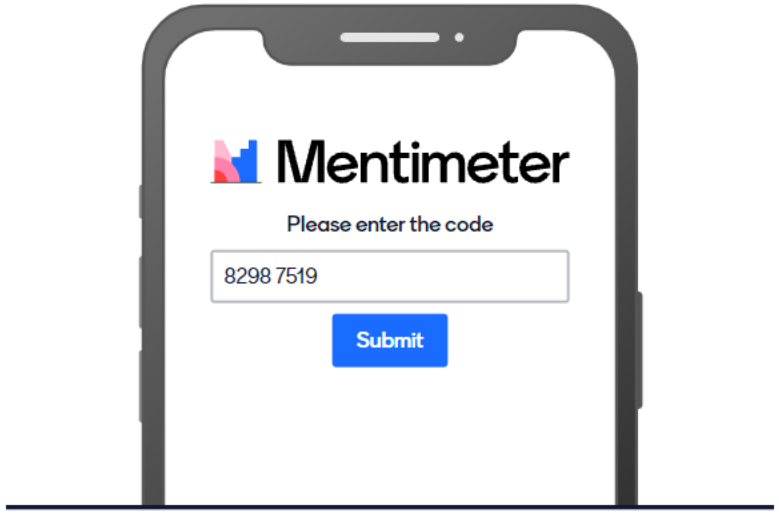
กำลังเผชิญ “ความเสี่ยง” อะไรอยู่บ้าง?



Workshop : 10 นาที

Go to

www.menti.com



Enter the code

8298 7519

Or use QR code

AGENDA

กระทรวงเกษตรและสหกรณ์
MINISTRY OF AGRICULTURE AND COOPERATIVES

1 การเปลี่ยนแปลง ความเสี่ยง และโอกาสขององค์กรในยุค BANI ปี 2023
Change, Risks & Opportunities in the 2023 BANI era

2 หลักการและแนวคิดสำคัญในการบริหารความเสี่ยงระดับองค์กร
Foundation & Concept of Organizational Risk Management

3 แนวป้องกันสามด่าน 3-Lines of Defense & CSA
Strengthening the Organizational Governance & Risk Management

4 เทคนิคการสอบทานการบริหารความเสี่ยงตามแนวทาง COSO ERM 2017
Organizational Risk Management Identification


RISK!
RISK!
PLEASE DRIVE SAFELY
RISK!

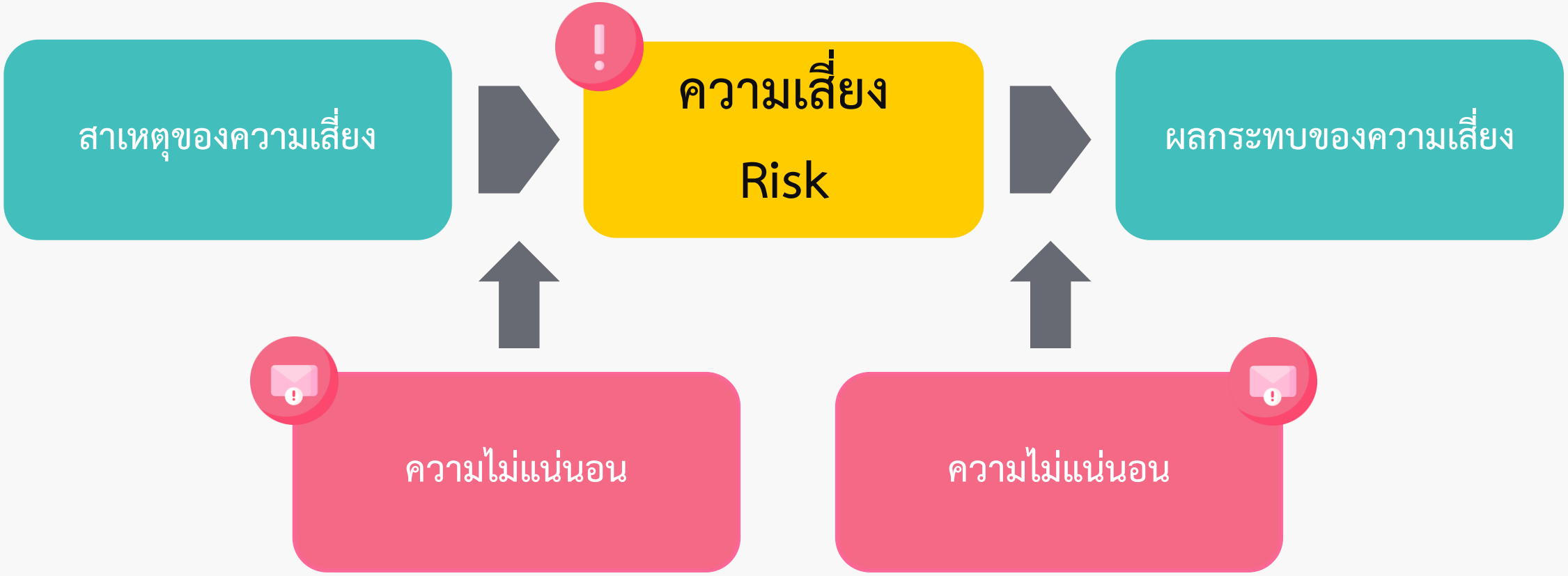
ความเสี่ยง (Risk)

ความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้นและส่งผลต่อการบรรลุกลยุทธ์และวัตถุประสงค์ขององค์กร

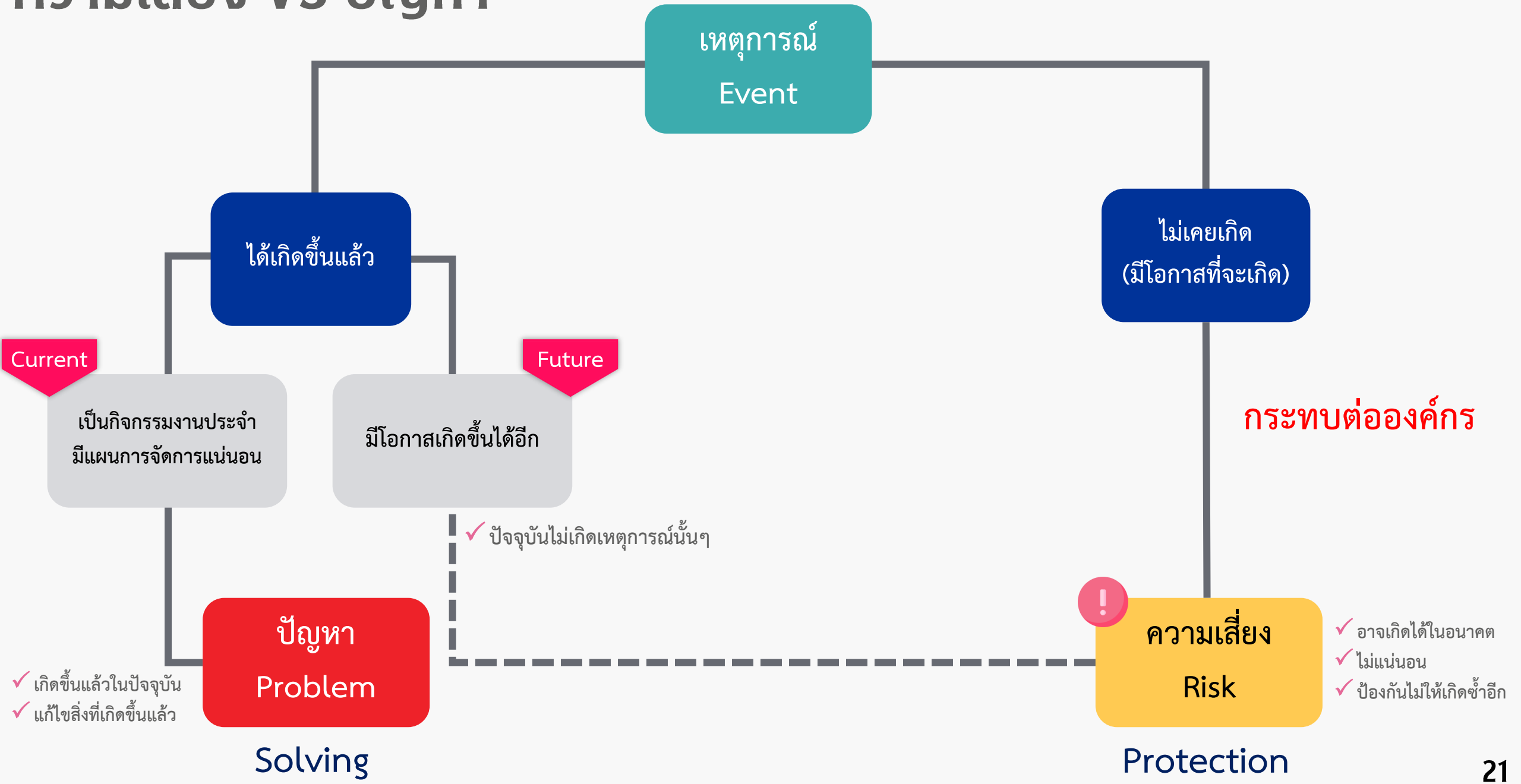
เหตุการณ์ที่อาจเกิดขึ้น อาจส่งผลกระทบต่อกลยุทธ์และวัตถุประสงค์ทางธุรกิจของกิจการ การขาดความสามารถในการคาดการณ์ถึงเหตุการณ์ที่จะเกิดขึ้นรวมถึงผลกระทบที่ตามมาได้อย่างครบถ้วน ก่อให้เกิดความไม่แน่นอนสำหรับองค์กร

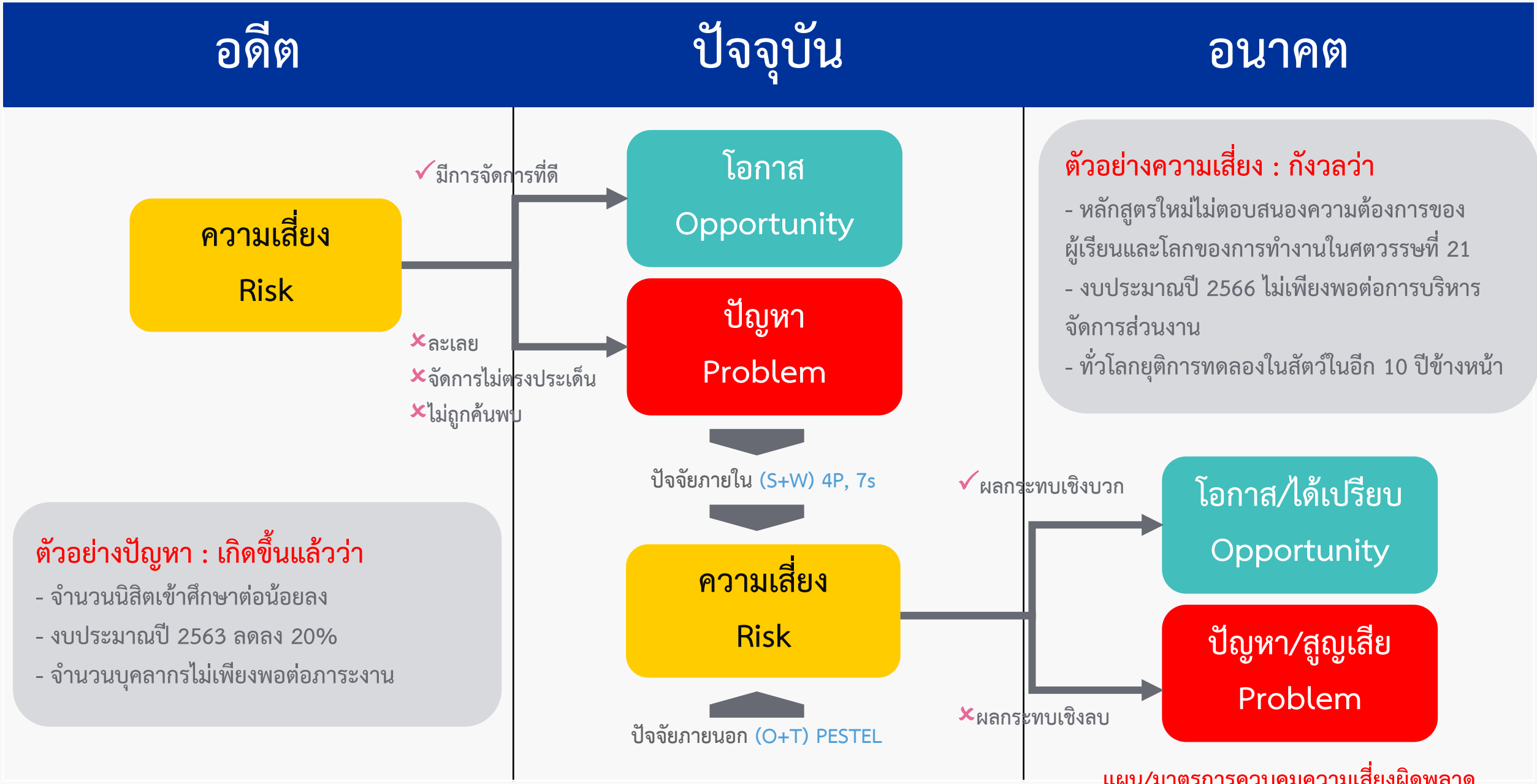
Where risks come from? I ความเสี่ยงมาจากไหน

ความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้นและส่งผลต่อการบรรลุกลยุทธ์และวัตถุประสงค์ของตนเอง/องค์กร



ความเสี่ยง VS ปัญหา





Credit: ประเสริฐ อัครปฐมพงศ์, 2563 (เอกสารการบรรยายบริหารความเสี่ยงองค์กร ศูนย์บริการวิชาการแห่งจุฬาลงกรณ์มหาวิทยาลัย)

Misunderstanding in Risk

Risk is always bad

เป็นเรื่องไม่ดีเสมอ

Risk must be eliminated at all costs

ต้องกำจัดความเสี่ยงให้หมดสิ้น

Playing it safe is the safest thing to do

ไม่เสี่ยงย่อมปลอดภัยที่สุด

Credit: ประเสริฐ อัครปฐมพงศ์, 2563 (เอกสารการบรรยายบริหารความเสี่ยงองค์กร ศูนย์บริการวิชาการแห่งจุฬาลงกรณ์มหาวิทยาลัย)

บริหารความเสี่ยง (Risk Management)

กระบวนการที่ถูกออกแบบขึ้นเพื่อใช้จัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

โดยมีการระบุ ประเมิน จัดลำดับ และกำหนดกลยุทธ์และดำเนินงานสำหรับจัดการความเสี่ยงอย่างเหมาะสม เพื่อให้ได้รับความมั่นใจอย่างสมเหตุสมผล ในการบรรลุวัตถุประสงค์ที่องค์กรกำหนดไว้

5 ความคาดหวังจากการบริหารความเสี่ยง

1 ใช้ความเสี่ยงเพื่อสร้างคุณค่าให้แก่องค์กร ไม่ใช่เพียงปกป้องคุณค่า

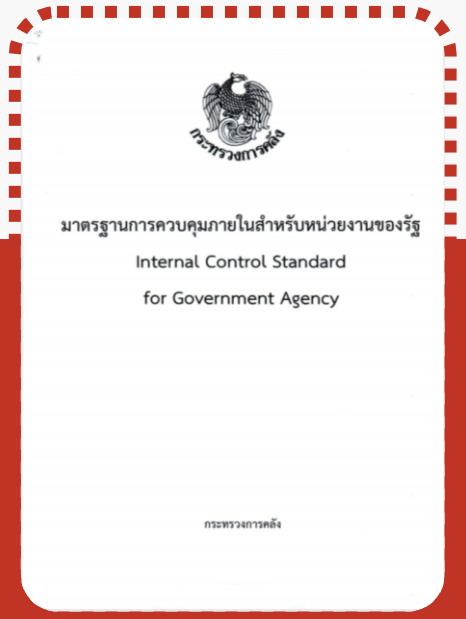
2 ลดความไม่แน่นอนของผลการปฏิบัติงานและตอบสนองต่อโอกาสได้ไวมากยิ่งขึ้น

3. ขับเคลื่อนการปรับปรุงบทบาทหน้าที่ของธุรกิจมากกว่าหลบเลี่ยงความเสี่ยง

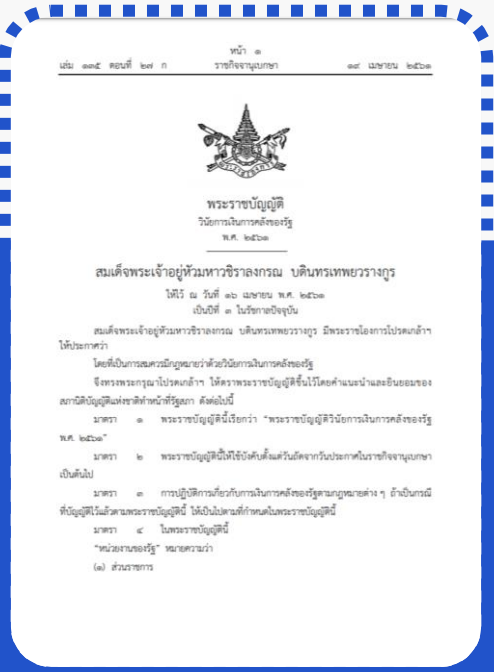
4 เข้าใจกระบวนการบริหารความเสี่ยงที่สามารถสร้างโอกาสและประเมินทางเลือกยุทธศาสตร์

5 สร้างความได้เปรียบจากการบริหารความเสี่ยงองค์กร

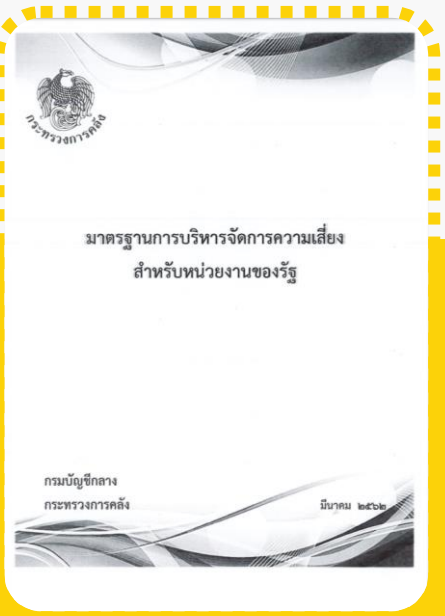
มาตรฐานปฏิบัติที่เกี่ยวข้องกับการบริหารความเสี่ยงและการควบคุมภายใน



หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ.2561



พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561



หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562

กรมบัญชีกลาง ออกแนวทาง

เรื่อง "หลักการบริหารจัดการความเสี่ยงระดับองค์กร"

เพื่อให้หน่วยงานของรัฐนำไปปรับใช้ได้อย่างเหมาะสม

ดาวน์โหลดได้ที่ www.cgd.go.th

หัวข้อ เรื่องที่น่าสนใจ >> หัวข้อ ตรวจสอบภายใน >>
เลือก ระเบียบ มาตรฐาน คู่มือ แนวปฏิบัติ >>
หัวข้อ แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ
>> เรื่อง หลักการบริหารจัดการความเสี่ยงระดับองค์กร

กรอบการบริหารจัดการความเสี่ยง

ประกอบด้วย 8 หลักการ ดังนี้

1) การบริหารจัดการความเสี่ยงต้องดำเนินการแบบบูรณาการทั่วทั้งองค์กร
2) ความมุ่งมั่นของผู้กำกับดูแล หัวหน้าหน่วยงานของรัฐ และผู้บริหารระดับสูง
3) การสร้างและรักษาบุคลากรและวัฒนธรรมที่ดีขององค์กร
4) การมอบหมายหน้าที่ความรับผิดชอบด้านการบริหารจัดการความเสี่ยง
5) การตระหนักถึงผู้มีส่วนได้เสีย
6) การกำหนดยุทธศาสตร์/กลยุทธ์ วัตถุประสงค์ และการตัดสินใจ
7) การใช้ข้อมูลสารสนเทศ
8) การพัฒนาอย่างต่อเนื่อง

กระบวนการบริหารจัดการความเสี่ยง

ประกอบด้วย 7 กระบวนการ ดังนี้

1) การวิเคราะห์องค์กร
2) การกำหนดนโยบายการบริหารจัดการความเสี่ยง
3) การระบุความเสี่ยง
4) การประเมินความเสี่ยง
5) การตอบสนองความเสี่ยง
6) การติดตามและทบทวน
7) การสื่อสารและการรายงาน

หลักการบริหารจัดการความเสี่ยง

1 กรอบการบริหารจัดการความเสี่ยง

เป็นพื้นฐานของการบริหารจัดการความเสี่ยงที่ดี เพื่อให้การบริหารจัดการความเสี่ยงเป็นเครื่องมือช่วยหน่วยงานในการกำหนดแผนระดับองค์กร (Strategic plans) และการกำหนดวัตถุประสงค์เป็นไปอย่างมีประสิทธิผล รวมถึงการตัดสินใจของผู้บริหารอยู่บนพื้นบนฐานข้อมูลสารสนเทศที่สมบูรณ์

หลักการบริหารจัดการความเสี่ยงระดับองค์กร

กระบวนการบริหารจัดการความเสี่ยง 2

เป็นกระบวนการที่เกิดขึ้นอย่างต่อเนื่อง (Routine Processes) ของการบริหารจัดการความเสี่ยง ซึ่งตั้งอยู่บนพื้นฐานของกรอบบริหารจัดการความเสี่ยงของหน่วยงาน

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

Principle of COSO-ERM 2017

1 การกำกับดูแลและวัฒนธรรม

1. ควบคุมดูแลความเสี่ยงโดยคณะกรรมการ
2. จัดตั้งโครงสร้างดำเนินงาน
3. กำหนดวัฒนธรรมที่พึงประสงค์
4. แสดงให้เห็นถึงการยึดมั่นต่อคุณค่าหลัก
5. ดึงดูด พัฒนาและรักษาบุคคลที่มีความสามารถ

3 ผลการปฏิบัติ

10. ระบุความเสี่ยง
11. ประเมินความรุนแรงของความเสี่ยง
12. จัดลำดับความสำคัญของความเสี่ยง
13. นำวิธีการตอบสนองความเสี่ยงไปปฏิบัติ
14. พัฒนาภาพรวมความเสี่ยง

5 สารสนเทศ การสื่อสาร การรายงาน

18. ใช้ประโยชน์จากสารสนเทศและเทคโนโลยี
19. สื่อสารสารสนเทศด้านความเสี่ยง
20. รายงานความเสี่ยง วัฒนธรรม และผลการปฏิบัติงาน

2 กลยุทธ์และการกำหนดวัตถุประสงค์

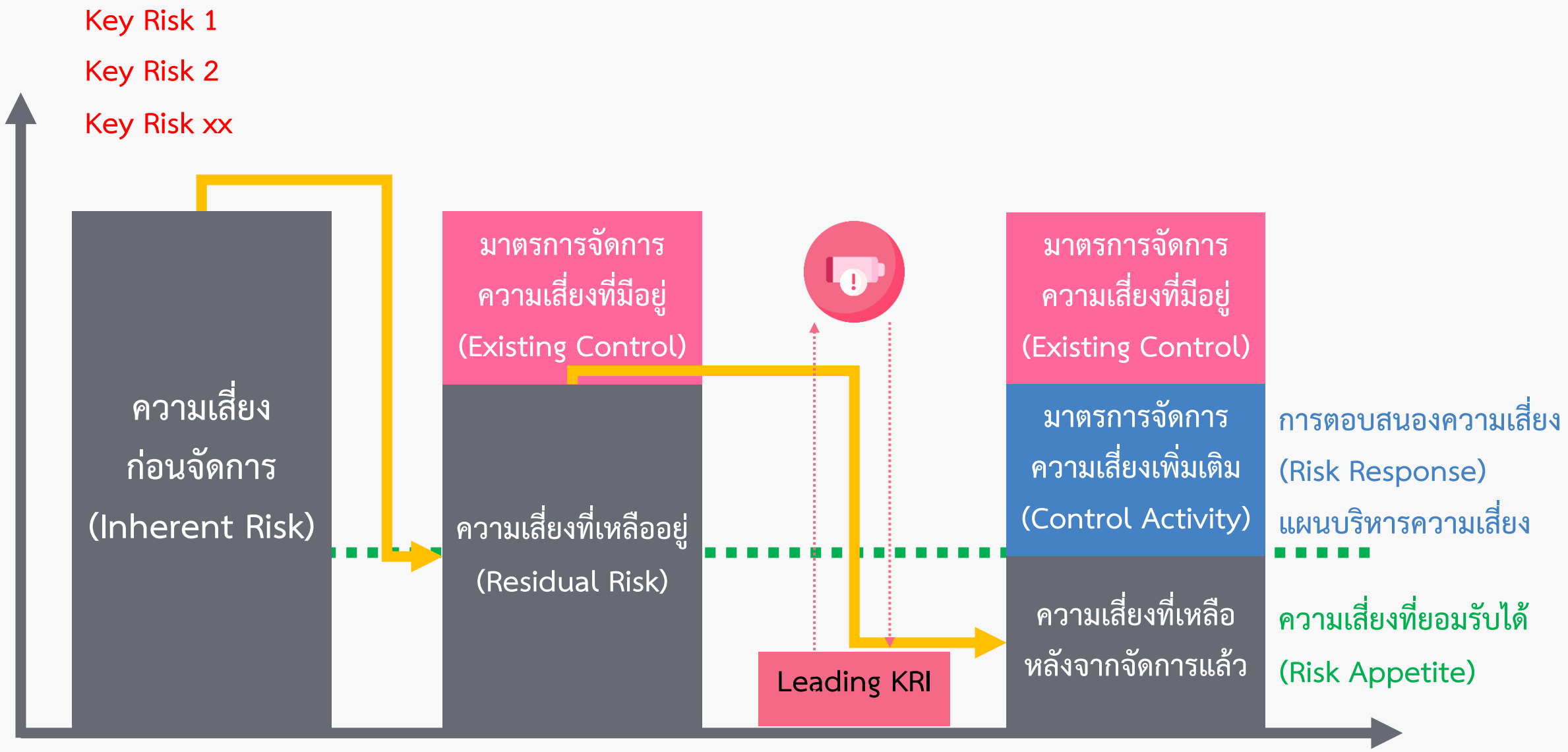
6. วิเคราะห์บริบททางธุรกิจ
7. กำหนดระดับความเสี่ยงที่ยอมรับได้
8. ประเมินกลยุทธ์ทางเลือก
9. กำหนดวัตถุประสงค์ทางธุรกิจ

4 การสอบทานและการแก้ไขปรับปรุง

15. ประเมินการเปลี่ยนแปลงที่สำคัญ
16. สอบทานความเสี่ยงและผลการปฏิบัติงาน
17. พยายามปรับปรุงการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง

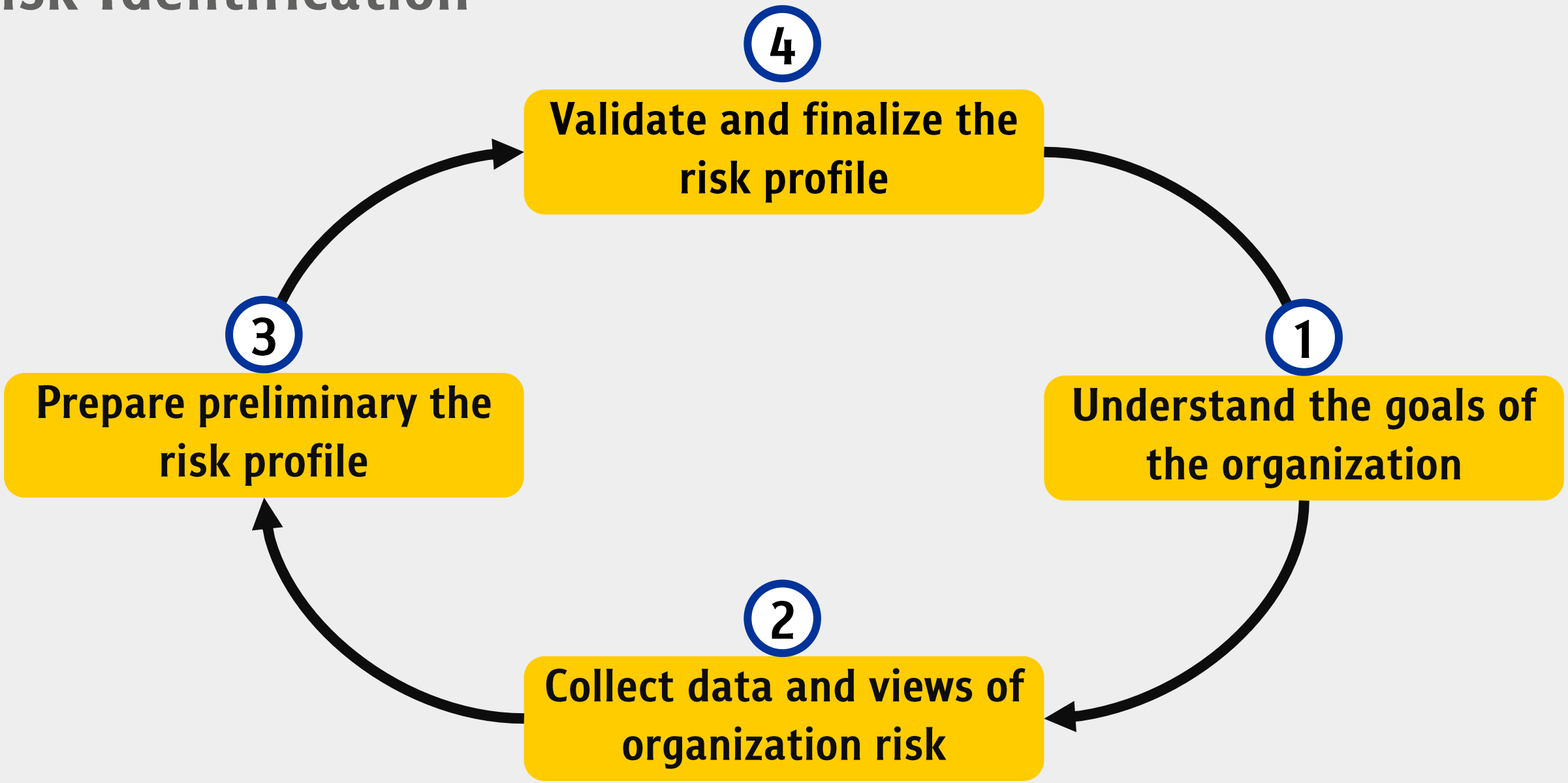
Integrated ERM Framework

กระบวนการบริหารความเสี่ยงและ Performance



Credit: ประเสริฐ อัครปฐมพงศ์, 2563 (เอกสารการบรรยายบริหารความเสี่ยงองค์กร ศูนย์บริการวิชาการแห่งจุฬาลงกรณ์มหาวิทยาลัย)

Risk Identification

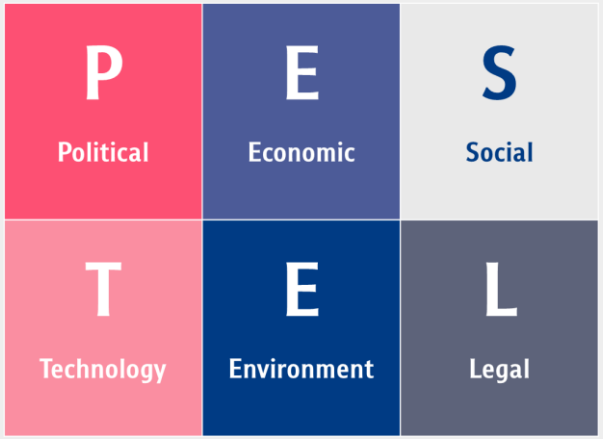


How to Identify Risk

ระบุปัจจัยที่มีผลกระทบเชิงลบต่อเป้าหมายองค์กร (ทั้งงานยุทธศาสตร์และงานประจำ)

Environmental Scanning

- Internal Factor (SWOT Analysis)
- External Factor (PESTEL Analysis)
- What-If (เหตุการณ์ร้ายต่างๆที่อาจเกิดขึ้น) Change & Uncertainty



Types of Risk

- Strategic Risk ความเสี่ยงด้านกลยุทธ์
- Operational Risk ความเสี่ยงด้านปฏิบัติการ
- Financial Risk ความเสี่ยงด้านการเงิน
- Compliance Risk ความเสี่ยงด้านกฎระเบียบ

Strategic Risk
ความเสี่ยงด้านกลยุทธ์

ความเสี่ยงที่เกิดขึ้นจากการกำหนดกลยุทธ์ หรือนโยบายการบริหารงาน ทำให้องค์กรไม่สามารถบรรลุกลยุทธ์และเพิ่มมูลค่าให้องค์กรได้ เช่น นโยบายไม่สอดคล้องกับตลาด โครงสร้างองค์กรที่เปลี่ยนไป ผลิตบัณฑิตแล้วไม่ตอบภาคอุตสาหกรรม ผลงานวิจัยไม่สามารถนำไปใช้ประโยชน์ได้

Operational Risk
ความเสี่ยงด้านปฏิบัติการ

ความเสี่ยงที่เกิดจากการปฏิบัติงานในขั้นตอนต่างๆ โดยเกี่ยวข้องกับกระบวนการทำงาน อุปกรณ์ เทคโนโลยี บุคลากร ซึ่งทำให้ประสิทธิภาพและประสิทธิผลต่อการดำเนินพันธกิจขององค์กร เช่น ความล่าช้า ขาดอุปกรณ์ที่มีประสิทธิภาพ บริหารสัญญาขาดประสิทธิภาพ ระบบ IT ขัดข้อง

Financial Risk
ความเสี่ยงด้านการเงิน

ความเสี่ยงที่เกิดขึ้นจากการขาดข้อมูล การวิเคราะห์ การวางแผน การควบคุม และจัดทำรายงานเพื่อนำมาใช้ในการบริหารการเงินอย่างถูกต้อง ส่งผลต่อสถานภาพหรือเสถียรภาพทางการเงินขององค์กร เช่น แผนการลงทุนขาดความชัดเจน การลดลงของงบประมาณประจำปี การไม่สามารถจัดเก็บรายได้ให้เป็นไปตามเป้าหมาย

Compliance Risk
ความเสี่ยงด้านกฎระเบียบ

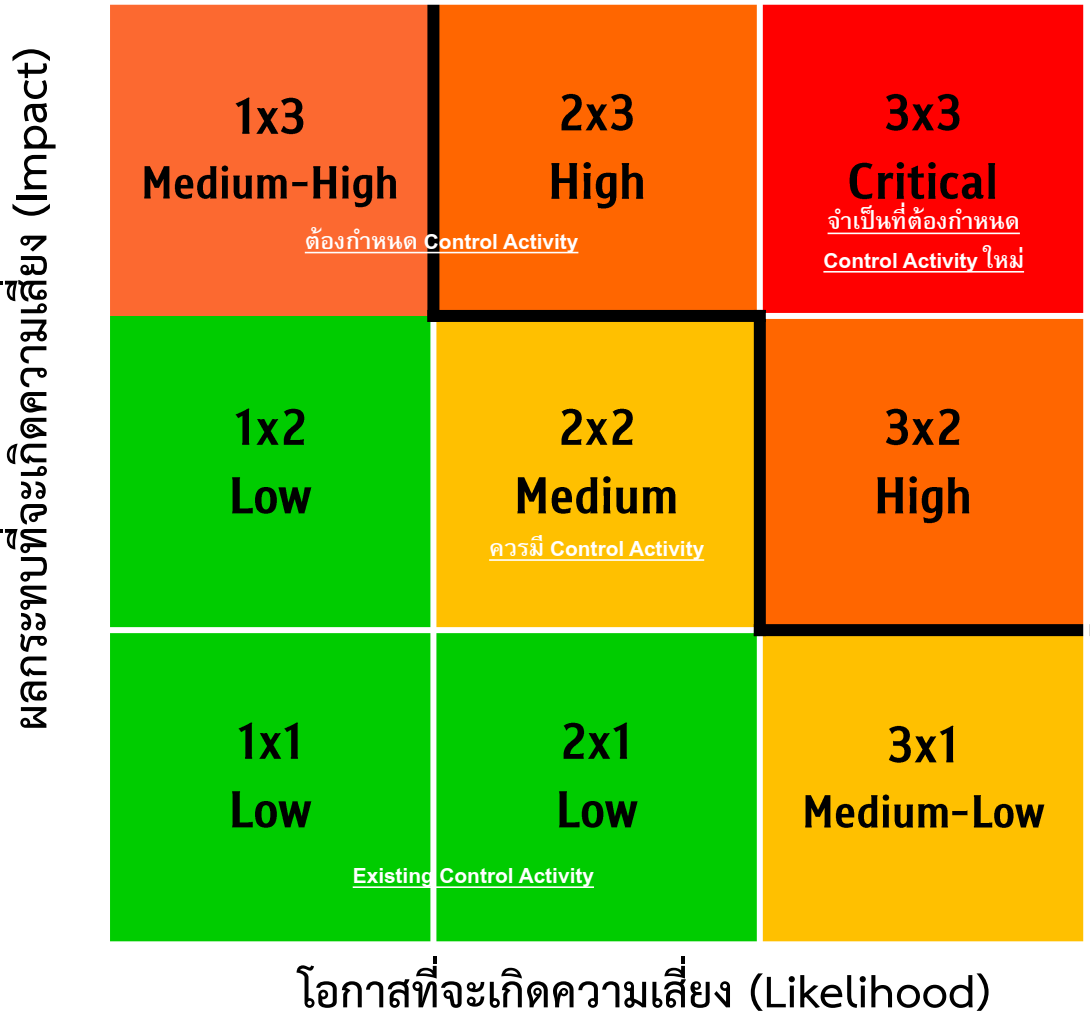
ความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรฐานที่เกี่ยวข้องกับการดำเนินงานได้ กฎหมายที่มีอยู่เป็นอุปสรรคต่อการปฏิบัติงาน นโยบายและวิธีปฏิบัติงานที่กำหนดขึ้นไม่สามารถปฏิบัติได้ เช่น ไม่สามารถดำเนินงานตามกฎหมายใหม่ได้อย่างครบถ้วน ความสับสนในการเลือกกฎ/ระเบียบที่จะบังคับใช้

Key Risk Profile: ตัวอย่างความเสี่ยงที่สำคัญ

Risk Profile	Type	Description
รัฐบาล/มหาวิทยาลัยเปลี่ยนแปลงทิศทางในการสนับสนุนการดำเนินภารกิจของส่วนงาน	S	ความเสี่ยงด้านยุทธศาสตร์ : เกิดจากการไม่สามารถดำเนินภารกิจตามแผนงาน หรือเกิดจากปัจจัยและสภาพแวดล้อมเกิดการเปลี่ยนแปลงจนกระทบต่อโมเดลธุรกิจ
รูปแบบพันธกิจของมหาวิทยาลัยไม่สอดคล้องกับโลกในอนาคต	S	
ระบบ Internet ภายในคณะขัดข้องส่งผลต่อกิจกรรมต่างๆของส่วนงาน	O	ความเสี่ยงด้านปฏิบัติการ : เกิดจากความผิดพลาด หรือความไม่เพียงพอในกระบวนการควบคุมภายในบุคลากร ระบบต่างๆ เทคโนโลยีสารสนเทศ เป็นต้น
เกิดการทุจริตในระบบจัดซื้อจัดจ้างของหน่วยงาน (Fraud Risk)	O	
งบประมาณของส่วนงานมีแนวโน้มลดลงและไม่เพียงพอต่อการบริหารจัดการ	F	ความเสี่ยงด้านการเงิน : ความเสี่ยงที่มีผลกระทบทางการเงินและงบประมาณขององค์กร
ต้นทุนในการดูแลรักษาระบบเทคโนโลยีในห้องทดลองสูงขึ้นร้อยละ 10 ต่อปี	F	
ปรับกระบวนการในหน่วยงานได้ไม่ทันกับ พ.ร.บ. xxxx ฉบับใหม่	C	ความเสี่ยงด้านการปฏิบัติตามกฎเกณฑ์ : เกิดจากการไม่สามารถทำตามกฎหมาย ระเบียบ ที่เกี่ยวข้องกับส่วนงานได้ รวมถึงการฝ่าฝืน ละเมิด ประมาทจนอาจถูกภาคทัณฑ์
หลักสูตรไม่ได้รับการรับรองมาตรฐานจากสภาวิชาชีพ/กระทรวงฯ	C	

ตารางวิเคราะห์ความเสี่ยง (Risk Matrix) 3x3

Step 2



(โอกาส x ผลกระทบ) = ระดับความเสี่ยง

ระดับความเสี่ยง	ระดับคะแนน	ความหมาย
สูงมาก (Critical)	3x3	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที
สูง (High – Medium High)	1x3 2x3 3x2	ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับยอมรับได้
ปานกลาง (Medium)	2x2 3x1	ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงไปยังระดับที่ยอมรับไม่ได้
ต่ำ (Low)	1x1 1x2 2x1	ระดับที่ยอมรับได้ โดยใช้วิธีควบคุมปกติตามขั้นตอนการปฏิบัติงานที่กำหนดอย่างสม่ำเสมอ

การตอบสนองความเสี่ยง (Risk Response) “4Ts”

Take

Take (ยอมรับ)

ความเสี่ยงหลังการควบคุมอยู่ในระดับที่ยอมรับได้ โดยไม่ต้องดำเนินการใดๆเพิ่มเติมที่มีผลต่อโอกาสเกิด หรือผลกระทบของความเสี่ยง [ตั้งใจดำเนินตามแผนต่อไป ยอมรับทั้งหมด จัดหาเงินทุนสำรองเพื่อรองรับผลที่อาจจะเกิด จัดเตรียมแผนรับมือ]

Treat

Treat (ลด)

การดำเนินการเพิ่มเติมเพื่อลดโอกาสเกิดหรือผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ [ปรับกลยุทธ์ ระบบงาน กระบวนการให้มีประสิทธิภาพ พัฒนาบุคลากรให้ชำนาญ ปรับโครงสร้างองค์กร จัดทำแผนฉุกเฉิน พัฒนาแผนฟื้นฟู]

Transfer

Transfer (กระจ่าย / ถ่ายโอน)

การโอนย้าย หรือการแบ่งความเสี่ยงบางส่วนไปยังบุคคลอื่น/องค์กรอื่น [การประกันภัย การร่วมทุน การสร้างพันธมิตรธุรกิจ การจ้าง Outsourcing]

Terminate

Terminate (หลีกเลี่ยง)

การยกเลิกหรือหลีกเลี่ยงกิจกรรมที่ก่อให้เกิดความเสี่ยง แต่จำเป็นต้องพิจารณาให้ถี่ถ้วนว่าจะทำให้งานบรรลุได้หรือไม่ [หยุดกิจกรรม ลดขนาดการลงทุน ปรับเป้าหมาย ออกจากตลาดเพื่อรักษาส่วนแบ่งไว้]

การติดตามผลการบริหารความเสี่ยง (Risk Monitoring)

Board Reporting

เน้นรายงานเฉพาะข้อมูลที่สำคัญ

Risk	Current Risk			Consequence	Controls	Residual Risk		
	Impact	Likelihood	Degree			Impact	Likelihood	Degree

Regular Updating

- การเปลี่ยนแปลงที่เกิดขึ้นกับความเสี่ยง
- ความเสี่ยงใหม่ที่เกิดขึ้น (Emerging Risk)
- Key Risk Indicators (KRI)
- การเปลี่ยนแปลงวิธี/มาตรการควบคุม
- ข้อมูลที่สำคัญเพื่อให้ Board/กรรมการตัดสินใจ

Reference: IOD. Risk Issues for Board

การติดตามผลการบริหารความเสี่ยง (Risk Monitoring)

Considering Risk Report

Risk Identification

- ความเสี่ยงที่ถูกระบุไว้ใช่ความเสี่ยงที่สำคัญจริงหรือไม่
- ได้วิเคราะห์สภาพแวดล้อมภายในและนอกองค์กรก่อนที่จะระบุความเสี่ยงหรือไม่

Risk Methodology

- กระบวนการบริหารความเสี่ยงมีการอัพเดทให้เป็นปัจจุบันหรือไม่
- ความเสี่ยงถูกประเมินระดับและจัดเรียงลำดับได้อย่างเหมาะสมหรือไม่
- ฝ่ายบริหาร/ Risk Owner ได้ใช้มาตรการตอบสนองความเสี่ยงได้เหมาะสมแล้วหรือยัง

Reference: IOD. Risk Issues for Board

Integrated ERM Framework

Information Communication & Report : Listed Companies

Risk Assessment	Identify High-Risk Process	Set Up Risk Control Measures	Randomized Assessment of Control Measures by Auditors	Review Internal Process and Control of Risks Quarterly
• Conducted by risk champions • Assessed risks include legal compliance, data security, cyber threat, human rights,corruption, randomized assessment by governmental agencies and consumers' complaints	• In 2020, 25 processes have been identified as high-risk processes from 254 processed conducted across marketing, production, procurement, and distribution	• In 2020, there are 10 control measures in total for 25 high-risk process • There has been communication on risk control measures to relevant parties, along with risk champions	• Auditors comprise of risk management function, corporate process simplification function, and audit function	• Review by risk champions along with the process' function owners

Impacts and Benefits

There are **1,849** risks submitted by employees.

5 risks recognized for awards comprises

- Personal data breaches
- Capacity in handing a new wave of pandemic
- Environmental issues
- Products and services
- Human right and safety

Information Communication & Report : Chulalongkorn University

PROTECHT.ERM | System | Core Libraries | Risk Assessment | KRIs | Compliance | Applications | Actions | Checklist Audits | Analytics

2ND LINE LAUNCHPAD

All | My Items

Residual Risk Assessment

Risk Details

Risk Name	Risk Assessment: Inherent	Residual	Prior	Risk Owner
Staff bullying or misconduct	Moderate	Low		protecht.consulting
Inadequate insurance coverage	High	Low		protecht.consulting
Poor recruitment and selection process	Moderate	Low		protecht.consulting
Breach of employment legislation / regulations	High	Low		protecht.consulting
Unauthorized access to sensitive and employee data	High	Moderate		protecht.consulting
Continuous disclosure	Moderate	Low		protecht.consulting
Erroneous financial position reporting	High	Low		protecht.consulting
Unauthorized access to sensitive and employee data	High	Moderate		protecht.consulting

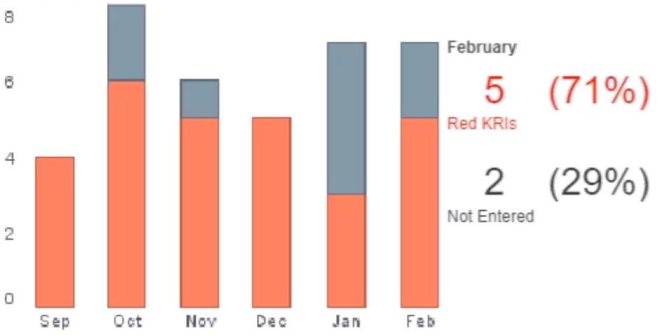
Risk

Risk Assessment Register →
Risk Dashboard →
Risk Report →
Risk in Motion →
Risk Event & Control Linkages Dashboard →

Business Unit

XYZ Limited

Key Risk Indicators



Key Risk Indicators

ID	Key Risk Indicator	Responsible
101242	Number of reporting errors noted per month	Finance
101159	The number of times an insurance review due date has been missed	Finance
100843	Number of reporting errors noted per month	Finance
101217	Number of external cyber attacks and penetration attempts	Information Technology
100915	Number of open actions (incl. Audit) relating to IT systems including failed DRP/BCP tests	Information Technology
101172	Number of open actions (incl. Audit) relating to IT systems including failed DRP/BCP tests	Information Technology
100852	Number of open actions (incl. Audit) relating to IT systems including failed DRP/BCP tests	Information Technology
101023	Number of open actions (incl. Audit) relating to IT systems including failed DRP/BCP tests	Information Technology
100862	% of all models and spreadsheets (as per Model Policy) independently reviewed in the last 12 mor	Operations

Key Risk Indicators

KRI Entry →
KRI Dashboard →
KRI Report →
KRI Monthly Trend →
KRI Above Tolerance →
RAS Metric Report →

Compliance

Compliance

Compliance

AGENDA

กระทรวงเกษตรและสหกรณ์
MINISTRY OF AGRICULTURE AND COOPERATIVES

1 การเปลี่ยนแปลง ความเสี่ยง และโอกาสขององค์กรในยุค BANI ปี 2023
Change, Risks & Opportunities in the 2023 BANI era

2 หลักการและแนวคิดสำคัญในการบริหารความเสี่ยงระดับองค์กร
Foundation & Concept of Organizational Risk Management

3 แนวป้องกันสามด่าน 3-Lines of Defense & CSA
Strengthening the Organizational Governance & Risk Management

4 เทคนิคการสอบทานการบริหารความเสี่ยงตามแนวทาง COSO ERM 2017
Organizational Risk Management Identification

Three Lines of Defense (Model)

The Institute of Internal Auditors

Board of Directors (Governing Body)

Audit Committee

Executive/ Management Committee

1st Line of Defense

All Units

- Own & Manage risk
- Implement corrective action to address process & control deficiency

Monitoring

2nd Line of Defense

Policy & Monitoring Units

- Set and implement policy and procedure
- Provide functional oversight by monitoring, supervising, and ensuring proper execution/ compliance

Assurance

3rd Line of Defense

Internal Audit Units

- Provide independence assurance on the effectiveness of GRC

Assurance

External Audit

Regulator

Three Lines of Defense: Principle

Three Lines of Defense

1. การกำกับดูแล การกำกับดูแลกิจการที่ดีจะต้องประกอบด้วยโครงสร้าง และกระบวนการปฏิบัติงานที่เหมาะสม เพื่อส่งเสริมเรื่องต่อไปนี้
    1. Accountability ผู้กำกับดูแล ดูแลให้เกิด integrity, leadership, transparency
    2. Actions บริหารจัดการทรัพยากร รวมการบริหารความเสี่ยง
    3. Assurance and Advice โดยหน่วยตรวจสอบภายใน ส่งเสริมการปรับปรุงพัฒนาต่อเนื่อง
2. บทบาทองค์คณะผู้กำกับดูแลที่เหมาะสม
3. บทบาทผู้บริหาร ด่านที่ 1 ผู้ส่งมอบสินค้าบริการ ด่านที่ 2 ผู้สนับสนุนให้คำปรึกษา ที่เหมาะสม
4. บทบาทด่านที่ 3 ตรวจสอบภายในให้ความเชื่อมั่นและให้คำปรึกษา
5. ความเป็นอิสระของด่านที่ 3
6. การสร้างและปกป้องคุณค่า โดยทุกหน่วยทำงานร่วมกันในองค์กร

Three Lines of Defense: Roles of Responsibility

Governing Body

(องค์คณะผู้มีหน้าที่กำกับดูแล)

รับผิดชอบต่อผู้มีส่วนได้ส่วนเสียในการดูแลองค์กร	ร่วมกับผู้มีส่วนได้ส่วนเสียเฝ้าระวังผลประโยชน์ของผู้มีส่วนได้ส่วนเสีย และสื่อสารอย่างโปร่งใส	ดูแลเอาใจใส่วัฒนธรรมและความรับผิดชอบที่มีจริยธรรม	กำหนดโครงสร้างและกระบวนการสำหรับการกำกับดูแล ซึ่งรวมถึงการจัดตั้งคณะอนุกรรมการ
มอบหมายภาระหน้าที่ จัดทรัพยากรให้แก่ฝ่ายบริหาร	กำหนดระดับการยอมรับความเสี่ยง (Risk Appetite) และกำกับดูแลการบริหารความเสี่ยงและควบคุมภายใน	คอยดูแลให้มีการปฏิบัติตามกฎหมาย ข้อบังคับทางการ และความคาดหวังที่ดีงามมีจริยธรรม	จัดให้มีและดูแลหน้าที่งานตรวจสอบภายในที่เป็นอิสระและเที่ยงธรรม

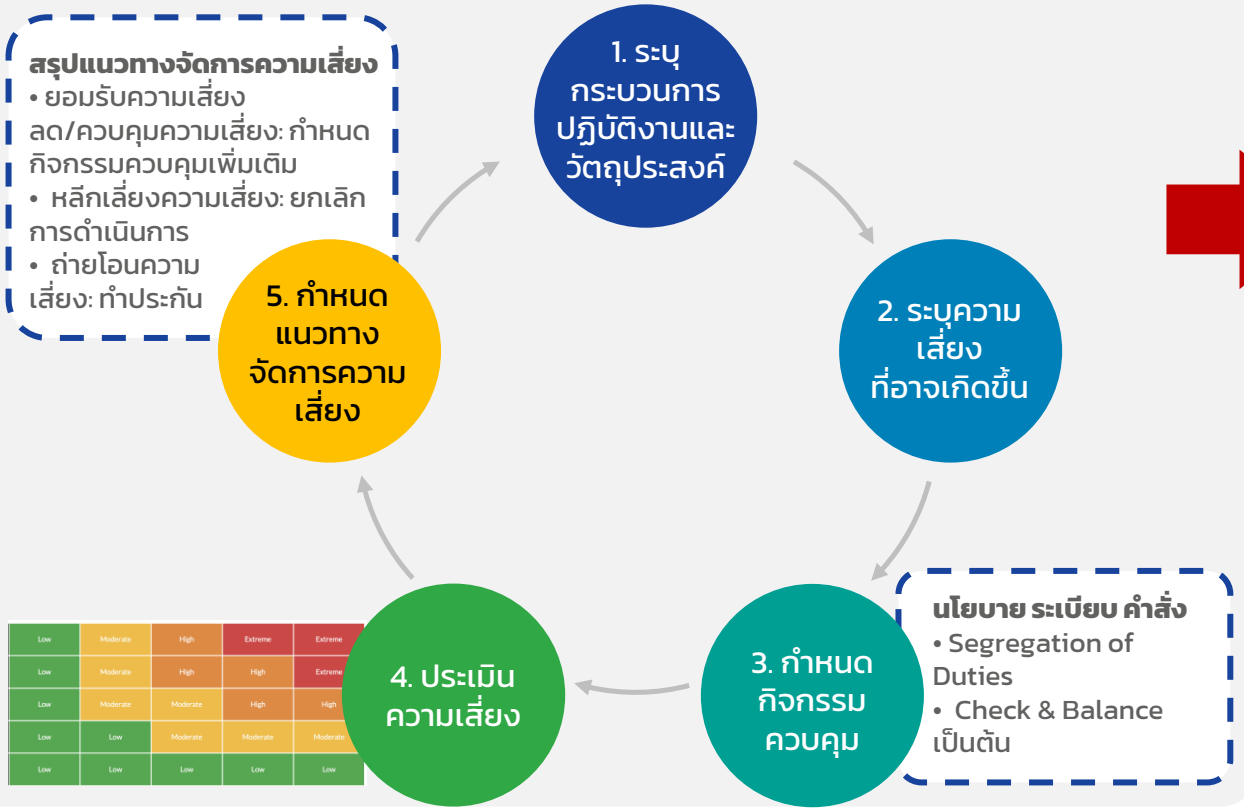
Three Lines of Defense: Roles of Responsibility

1	2	3
First Line of Defense (ผู้รับผิดชอบระดับแรก)	**Second Line of Defense (ผู้รับผิดชอบระดับที่ 2)**	**Third Line of Defense (ผู้รับผิดชอบระดับที่ 3)**
หน่วยงานต่าง ๆ ในองค์กร (Business Lines) มีหน้าที่ดูแลงานในความรับผิดชอบและระบบการควบคุมภายในให้เป็นไปตามแนวทางหรือกรอบที่กำหนดไว้	หน่วยงานที่ดูแลให้มีการปฏิบัติตามกฎเกณฑ์ (Compliance) การตรวจสอบและควบคุมคุณภาพ (Inspection and Quality Assurance) การบริหารความเสี่ยง (Risk Management)	หน่วยงานตรวจสอบภายใน (Internal Audit) มีหน้าที่ประเมินความเพียงพอของระบบการควบคุมภายในขององค์กร ให้ข้อเสนอแนะ การปรับปรุงและพัฒนา โดยรายงานต่อฝ่ายจัดการ
	ทั้ง 1st Line และ 2nd Line มีหน้าที่รายงานต่อคณะผู้บริหารหรือฝ่ายจัดการขององค์กร	คณะกรรมการ หน่วยงานตรวจสอบภายใน ควรมีความเป็นอิสระอย่างเพียงพอ (Independence) เพื่อให้ความเห็นนั้นสะท้อนประเด็นการตรวจสอบอย่างแท้จริง

Relationship between RM & IC and Three Lines of Defense

การประเมินความเสี่ยงและควบคุมภายใน

ดำเนินการร่วมกันระหว่างฝ่ายงานเจ้าของความเสี่ยง
กลุ่มงานบริหารความเสี่ยง และฝ่ายตรวจสอบภายใน
(1st / 2nd / 3rd Line of Defense)



Three Lines of Defense

1st Line

Risk Owner

มีการควบคุมภายในอยู่ในกระบวนการทำงานและมีการปฏิบัติตามการควบคุมที่มีอยู่อย่างเคร่งครัด

2nd Line

Risk Management

จัดให้มีการประเมินความเสี่ยงและการควบคุมภายในซึ่งครอบคลุมความเสี่ยงและการควบคุมด้านการทุจริตเป็นประจำทุกปี

3rd Line

Internal Audit

สอบทานประสิทธิภาพของการบริหารความเสี่ยงและการควบคุมภายในเพื่อให้มั่นใจได้ว่าการดำเนินงานของสำนักงาน รวมถึงการควบคุมภายในเป็นไปอย่างถูกต้อง และเหมาะสม

Relationship between RM & IC and Three Lines of Defense

ฝ่ายบริหารความเสี่ยงองค์กร (2nd Line of defense)

- แม่บทการบริหารความเสี่ยง.
- คู่มือบริหารความเสี่ยงด้านปฏิบัติการ
- การระบุและประเมินความเสี่ยง
- ร่วมประเมินความเสี่ยงกับฝ่ายงานต่าง ๆ (Risk Owner)
- ติดตามและรายงานผลดำเนินการตามแผนปรับปรุงการควบคุมภายใน

จัดทำรายงานผลการประเมินความเสี่ยงและแผนปรับปรุง เสนอตามลำดับ

รายงานการประเมินองค์ประกอบของการควบคุมภายใน (แบบ ปค. ๔) และรายงานการประเมินผลการควบคุมภายใน (แบบ ปค. ๕)

รายงานหนังสือรับรองการประเมินผล การควบคุมภายใน (แบบ ปค. ๑)

ฝ่ายงานเจ้าของความเสี่ยง (1st Line of defense)

เหตุการณ์ความเสี่ยงประเภทต่างๆ รวมถึงความเสี่ยงทุจริต

การควบคุมภายในที่มีอยู่

ความเสี่ยงที่เหลืออยู่หลังการควบคุมภายใน

แผนปรับปรุงการควบคุมภายใน

ผู้บริหารสูงสุด

คณะกรรมการบริหารความเสี่ยง คณะกรรมการตรวจสอบ

คณะกรรมการ (Board)

กระทรวงการคลัง

ฝ่ายตรวจสอบภายใน (3rd Line of defense)

- สอบทานผลการประเมินความเสี่ยงและการควบคุมภายในให้ครอบคลุมทุกด้าน
- ประเมินความเพียงพอของการควบคุมภายใน และแผนปรับปรุง

จัดทำรายงานผลการสอบทาน การควบคุมภายในและแผนปรับปรุงการควบคุมภายใน เสนอตามลำดับ

รายงานการสอบทานการประเมินผลการควบคุมภายใน (แบบ ปค. ๖)

AGENDA

กระทรวงเกษตรและสหกรณ์
MINISTRY OF AGRICULTURE AND COOPERATIVES

1 การเปลี่ยนแปลง ความเสี่ยง และโอกาสขององค์กรในยุค BANI ปี 2023
Change, Risks & Opportunities in the 2023 BANI era

2 หลักการและแนวคิดสำคัญในการบริหารความเสี่ยงระดับองค์กร
Foundation & Concept of Organizational Risk Management

3 แนวป้องกันสามด่าน 3-Lines of Defense & CSA
Strengthening the Organizational Governance & Risk Management

4 เทคนิคการสอบทานการบริหารความเสี่ยงตามแนวทาง COSO ERM 2017
Organizational Risk Management Identification

Principle of 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

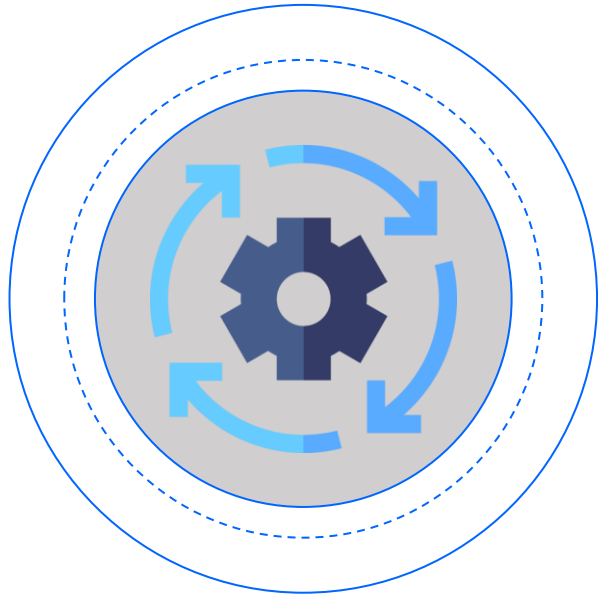
15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

INFORMATION, COMMUNICATION & REPORTING

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

Principle of COSO-ERM: 2017

องค์ประกอบที่ 4 การสอบทานและการแก้ไข



15 ประเมินการเปลี่ยนแปลงที่สำคัญ	16 สอบทานความเสี่ยงและผลการปฏิบัติงาน	17 ปรับปรุงการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง
องค์กรระบุและประเมินการเปลี่ยนแปลงที่อาจส่งผลกระทบอย่างมากต่อกลยุทธ์และวัตถุประสงค์ขององค์กร	องค์กรสอบทานผลการปฏิบัติงานขององค์กรและพิจารณาความเสี่ยง	องค์กรปรับปรุงการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง

องค์ประกอบที่ 4 การสอบทานและการแก้ไข

หลักการที่ 15 ประเมินการเปลี่ยนแปลงที่สำคัญ (Substantial Change)

สภาพแวดล้อมภายใน (Internal Environment)	• การเติบโตอย่างรวดเร็ว • นวัตกรรม • การเปลี่ยนแปลงที่สำคัญเกี่ยวกับผู้นำและบุคลากร	• ภาระงานเพิ่มขึ้น องค์กรรับมือได้หรือไม่ • การบริการผ่านช่องทางออนไลน์ ความเสี่ยงใหม่เกิดขึ้น • ผู้บริหารทีมใหม่ไม่สนใจความเสี่ยงเดิมขององค์กร
สภาพแวดล้อมภายนอก (External Environment)	• นโยบาย กฎหมาย กฎระเบียบ ข้อบังคับ • สภาพแวดล้อมทางเศรษฐกิจ > เงินเฟ้อ ดอกเบี้ย • สภาพแวดล้อมทางการแข่งขันในธุรกิจ	• องค์กรจัดการเรื่อง PDPA ได้มีประสิทธิผลหรือไม่ • ต้นทุนสินค้าสูงค้า เสี่ยงต่อการขาดทุนหรือตั้งราคาเพิ่ม • ESG องค์กรต้องดำเนินภารกิจโดยคำนึงความยั่งยืน • คู่แข่งพัฒนาโมเดลธุรกิจใหม่ที่ Disrupt วงการ

องค์ประกอบที่ 4 การสอบทานและการแก้ไข

หลักการที่ 16 สอบทานความเสี่ยงและผลการปฏิบัติงาน

บูรณาการการสอบทานเข้ากับแนวปฏิบัติขององค์กร

องค์กรทำการสอบทานผลการบริหารความเสี่ยงเพื่อตอบคำถามต่อไปนี้

- องค์กรได้ดำเนินงานตามที่คาดหวังและบรรลุเป้าหมายที่ตั้งไว้หรือไม่
- ความเสี่ยงใดกำลังเกิดขึ้นและอาจส่งผลกระทบต่อผลการปฏิบัติงาน
- องค์กรรับความเสี่ยงมากพอที่จะบรรลุเป้าหมายหรือไม่
- การประเมินค่าความเสี่ยงถูกต้องหรือไม่

องค์ประกอบที่ 4 การสอบทานและการแก้ไข

หลักการที่ 16 สอบทานความเสี่ยงและผลการปฏิบัติงาน

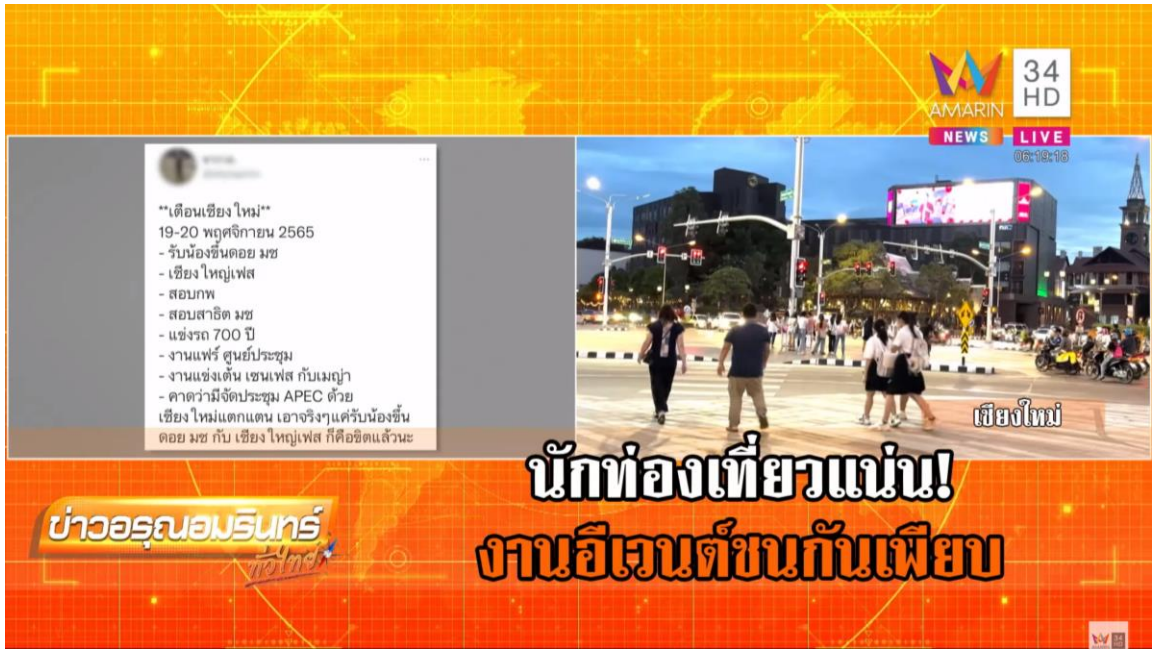
หากผลการบริหารความเสี่ยงไม่เป็นไปตามเป้าหมายที่คาดไว้...องค์กรควร!

สอบทานวัตถุประสงค์ขององค์กร	สอบทานกลยุทธ์	สอบทานวัฒนธรรมองค์กร	ปรับเปลี่ยนเป้าหมายผลการปฏิบัติงาน
ประเมินทบทวนความรุนแรงของผลกระทบของความเสี่ยง	สอบทานการจัดลำดับความสำคัญของความเสี่ยง	สอบทานการตอบสนองต่อความเสี่ยง	ปรับเปลี่ยนระดับความเสี่ยงที่ยอมรับได้

องค์ประกอบที่ 4 การสอบทานและการแก้ไข

หลักการที่ 16 สอบทานความเสี่ยงและผลการปฏิบัติงาน

การพิจารณาความสามารถขององค์กร



Risk? > จังหวัดจัดการไหวหรือไม่

Risk? > เกษตรกรจะผลิตได้ทันไหม

องค์ประกอบที่ 4 การสอบทานและการแก้ไข

หลักการที่ 17 ปรับปรุงการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง

8 ประโยชน์ที่องค์กรจะได้รับจากการสอบทานความเสี่ยง

เทคโนโลยีใหม่ๆ	ข้อบกพร่องในอดีต	การปรับเปลี่ยนกระบวนการในองค์กร	ระดับความเสี่ยงที่ยอมรับได้
ประเภทความเสี่ยง	การสื่อสาร	การเปรียบเทียบกับองค์กรอื่นๆ	อัตราการเปลี่ยนแปลง

COSO Internal Control Components

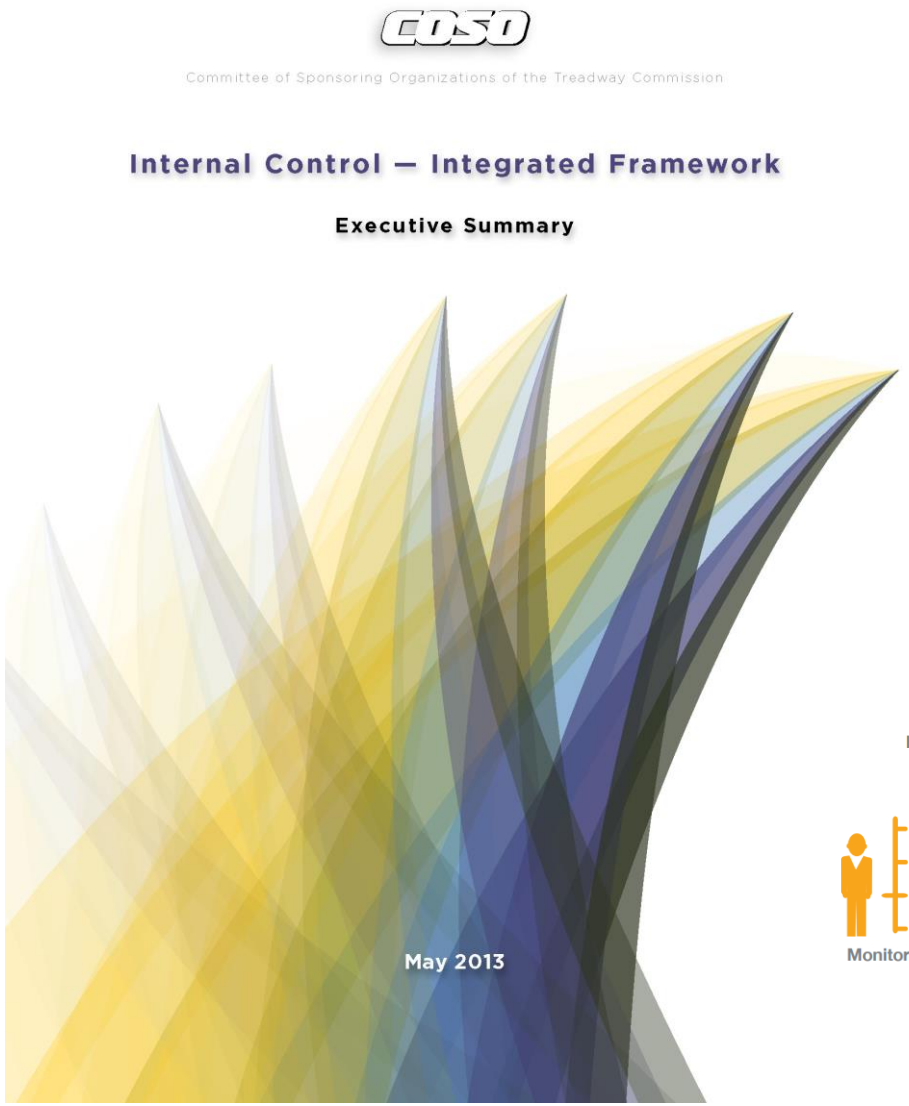


Exhibit 1. **The COSO Cube**

Principle of COSO Internal Control: 2013

5 องค์ประกอบ	17 หลักการ
สภาพแวดล้อมการควบคุม (CE) **Control environment**	1. องค์กรยึดหลักความซื่อตรงและจริยธรรม 2. คณะกรรมการแสดงออกถึงความรับผิดชอบต่อการกำกับดูแล 3. คณะกรรมการและฝ่ายบริหาร มีอำนาจการสั่งการชัดเจน 4. องค์กร จูงใจ รักษาไว้ และจูงใจพนักงาน 5. องค์กรผลักดันให้ทุกตำแหน่งรับผิดชอบต่อการควบคุมภายใน
การประเมินความเสี่ยง (RA) **Risk assessment**	6. กำหนดเป้าหมายชัดเจน 7. ระบุและวิเคราะห์ความเสี่ยงอย่างครอบคลุม 8. พิจารณาโอกาสที่จะเกิดการทุจริต 9. ระบุและประเมินความเปลี่ยนแปลงที่จะกระทบต่อการควบคุมภายใน
กิจกรรมการควบคุม (CA) **Control activities**	10. ควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ 11. พัฒนาระบบเทคโนโลยีที่ใช้ในการควบคุม 12. ควบคุมให้นโยบายสามารถปฏิบัติได้
สารสนเทศและการสื่อสาร (IC) **Information and communication**	13. องค์กรมีข้อมูลที่เกี่ยวข้องและมีคุณภาพ 14. มีการสื่อสารข้อมูลภายในองค์กร ให้การควบคุมภายในดำเนินต่อไปได้ 15. มีการสื่อสารกับหน่วยงานภายนอก ในประเด็นที่อาจกระทบต่อการควบคุมภายใน
การติดตามและประเมินผล (MA) **Monitoring activities**	16. ติดตามและประเมินผลการควบคุมภายใน 17. ประเมินและสื่อสารข้อบกพร่องของการควบคุมภายในทันเวลา และเหมาะสม

Principle of COSO Internal Control: 2013

สภาพแวดล้อมการควบคุม Control environment

หลักการ 1 องค์กรยึดหลักความซื่อตรงและจริยธรรม	1. แสดงให้เห็นโดยผ่านคำสั่ง การกระทำ พฤติกรรม 2. จัดทำมาตรฐานของจรรยาบรรณ 3. ประเมินการยึดมั่นในมาตรฐานของจรรยาบรรณ 4. รายงานการเบี่ยงเบนในเวลาที่เหมาะสม
หลักการ 2 คณะกรรมการแสดงออกถึงความรับผิดชอบต่อการกำกับดูแล	1. กำหนดความรับผิดชอบในการกำกับดูแล 2. กรรมการบริษัทมีความรู้ความชำนาญที่เกี่ยวข้องกับธุรกิ 3. ดำเนินการอย่างเป็นอิสระ จากฝ่ายบริหาร 4. กำกับดูแลในเรื่องสภาพแวดล้อมของการควบคุม การประเมินความเสี่ยง กิจกรรมการควบคุม ข้อมูลสารสนเทศและการสื่อสาร และการติดตามประเมินผล
หลักการ 3คณะกรรมการและฝ่ายบริหาร มีอำนาจการสั่งการชัดเจน	1.พิจารณาโครงสร้างทั้งหมดของกิจการ 2. กำหนดสายการรายงาน 3. กำหนด มอบหมาย และจำกัดขอบเขตของอำนาจหน้าที่และความรับผิดชอบ
หลักการ 4 องค์กร จูงใจ รักษาไว้ และจูงใจพนักงาน	1. วางนโยบายและวิธีปฏิบัติเกี่ยวกับการบริหารบุคลากร 2. ประเมินความสามารถรายบุคคลและระบุส่วนที่ยังขาดอยู่เพื่อปรับปรุงแก้ไข 3. จูงใจ พัฒนาและรักษาบุคคลากร 4. วางแผนและเตรียมสรรหาผู้สืบทอดตำแหน่ง (Succession
หลักการ 5 องค์กรผลักดันให้ทุกตำแหน่งรับผิดชอบต่อการควบคุมภายใน	1. บังคับให้มีความรับผิดชอบต่อการควบคุมภายในผ่านโครงสร้างองค์กร อำนาจหน้าที่ และความรับผิดชอบ 2. กำหนดตัวชี้วัดผลการปฏิบัติงาน การสร้างแรงจูงใจและการให้รางวัล 3. ประเมินตัวชี้วัดผลการปฏิบัติงาน สิ่งจูงใจ และรางวัลอย่างต่อเนื่อง 4. พิจารณาความกดดันในการท างานที่มากเกินไป 5. ประเมินผลการปฏิบัติงาน การให้รางวัล และการลงโทษพนักงานเป็นรายบุคคล

Principle of COSO Internal Control: 2013

การประเมินความเสี่ยง Risk assessment

หลักการ 6 กำหนดเป้าหมายชัดเจน	1. องค์กรปฏิบัติตามมาตรฐานบัญชีที่รับรองโดยทั่วไป 2. องค์กรกำหนดสาระสำคัญของรายงานทางการเงิน 3. รายงานทางการเงินสะท้อนถึงกิจกรรมขององค์กร 4. คณะกรรมการอนุมัติและสื่อสารนโยบายบริหารความเสี่ยงให้ผู้บริหารและพนักงานรับทราบ และเป็นส่วนหนึ่งของวัฒนธรรมองค์กร
หลักการ 7 ระบุและวิเคราะห์ความเสี่ยงอย่างครอบคลุม	1. ระบุความเสี่ยงทุกประเภท ทั้งระดับ องค์กร ฝ่ายงาน 2. ให้ผู้บริหารทุกระดับมีส่วนร่วม 3. ประเมินนัยสำคัญของความเสี่ยงที่ระบุ 4. กำหนดว่าจะตอบสนองความเสี่ยงอย่างไร
หลักการ 8 พิจารณาโอกาสที่จะเกิดการทุจริต	1. กำหนดว่าจะตอบสนองความเสี่ยงอย่างไร 2. ทบทวนเป้าหมาย แรงจูงใจและแรงกดดัน 3. คณะกรรมการตรวจสอบได้พิจารณาและสอบถามผู้บริหารเกี่ยวกับโอกาสเกิดทุจริต และมาตรการป้องกัน
หลักการ 9 ระบุและประเมินความเปลี่ยนแปลงที่จะกระทบต่อการควบคุมภายใน	1. ประเมินการเปลี่ยนแปลงสภาพแวดล้อมภายนอก 2. ประเมินการเปลี่ยนแปลงรูปแบบการทำธุรกิจ 3. ประเมินการเปลี่ยนแปลงผู้นำองค์กร

Principle of COSO Internal Control: 2013

กิจกรรมการควบคุม Control activities

หลักการ 10 ควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้	1. การควบคุมเหมาะสมกับความเสี่ยง และลักษณะเฉพาะขององค์กร สภาพแวดล้อม ลักษณะของงาน 2. มีมาตรการการควบคุมภายในที่กำหนดเป็นลายลักษณ์อักษร เช่น นโยบาย คู่มือ ระเบียบ 3. กำหนดกิจกรรมควบคุมให้มีความหลากหลายอย่างเหมาะสมการผสมผสานของ กิจกรรมการควบคุมหลายๆ ประเภท 4. กำหนดให้มีการควบคุมทุกระดับขององค์กร 5. มีการแบ่งแยกหน้าที่ ผู้อนุมัติ ผู้บันทึก ผู้ดูแลเก็บรักษา
หลักการ 11 พัฒนาระบบเทคโนโลยีที่ใช้ในการควบคุม	1. กำหนดความเกี่ยวข้องกันของการใช้ IT ในกระบวนการธุรกิจกับการควบคุมทั่วไป ทางด้าน IT ให้เหมาะสม 2. กำหนดกิจกรรมการควบคุมด้านโครงสร้างพื้นฐานให้เหมาะสม 3. กำหนดกิจกรรมการควบคุมด้านความปลอดภัยให้เหมาะสม 4. กำหนดกิจกรรมการควบคุมด้านการจัดหา การพัฒนา และดูแลรักษาระบบ
หลักการ 12 ควบคุมให้นโยบายสามารถปฏิบัติได้	1. มีนโยบายที่รัดกุมเพื่อติดตามการทำธุรกรรมของผู้ถือหุ้นรายใหญ่ กรรมการ ผู้บริหาร 2.มีนโยบายเพื่อให้การอนุมัติการท าธุรกรรมกระทำโดยผู้ที่ไม่มีส่วนได้เสีย 3. มีนโยบายเพื่อให้การอนุมัติธุรกรรมคำนึงถึงประโยชน์สูงสุดของบริษัท 4. มีกระบวนการติดตามดูแลการด าเนินงานของบริษัทย่อย บริษัทร่วม 5. กำหนดหน้าที่และความรับผิดชอบในการนำนโยบายไปปฏิบัติ 6. นโยบายและกระบวนการปฏิบัติได้รับการน าไปใช้ในเวลาที่เหมาะสม 7. ทบทวนนโยบายและกระบวนการท างานให้เหมาะสมอยู่เสมอ

Principle of COSO Internal Control: 2013

สารสนเทศและการสื่อสาร Information and communication

หลักการ 13 องค์กรมีข้อมูลที่เกี่ยวข้องและมีคุณภาพ	1. ระบุสารสนเทศที่ต้องการใช้ในการดำเนินงาน 2. พิจารณา ต้นทุน ประโยชน์ รวมทั้งปริมาณและความถูกต้องของข้อมูล 3. ดำเนินการเพื่อให้กรรมการมีข้อมูลที่เพียงพอในการตัดสินใจ 4. ดำเนินการเพื่อให้กรรมการได้รับหนังสือเชิญประชุมและเอกสารล่วงหน้าก่อนการประชุมตามที่กฎหมายกำหนด 5. ดำเนินการเพื่อให้รายงานการประชุมมีรายละเอียดสามารถสอบย้อนได้ 6. องค์กรมีการด าเนินการดังนี้ เก็บเอกสารเป็นระบบ แก้ไขข้อบกพร่องการควบคุม ตามความเห็นผู้สอบ
หลักการ 14 มีการสื่อสารข้อมูลภายในองค์กร ให้การควบคุมภายในดำเนินต่อไปได	1. มีกระบวนการสื่อสารข้อมูลอย่างมีประสิทธิภาพ มีช่องทางที่เหมาะสม 2. มีการรายงานข้อมูลที่สำคัญถึงกรรมการอย่างสม่ำเสมอ 3. จัดให้มีช่องทางสื่อสารลับเพื่อแจ้งเบาะแสเกี่ยวกับการทุจริต
หลักการ 15 มีการสื่อสารกับหน่วยงานภายนอก ในประเด็นที่อาจกระทบต่อการควบคุมภายใน	1. สื่อสารกับผู้มีส่วนได้เสียภายนอกอย่างมีประสิทธิภาพ มีช่องทางที่เหมาะสม 2. มีช่องทางสื่อสารลับ ส าหรับผู้มีส่วนได้เสียภายนอก แจ้งเบาะแสการทุจริต

Principle of COSO Internal Control: 2013

การติดตามและประเมินผล Monitoring activities	
หลักการ 16 ติดตามและประเมินผลการควบคุมภายใน	1. จัดให้มีการติดตามการปฏิบัติตามจริยธรรมธุรกิจและข้อก าหนด ในลักษณะที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์ 2. จัดให้มีการตรวจสอบการปฏิบัติตามระบบการควบคุมภายในที่วางไว้ โดยการประเมินตนเอง และ/หรือการประเมินโดยผู้ตรวจสอบภายใน 3. ความถี่การติดตามและประเมินผล มีความเหมาะสมกับการเปลี่ยนแปลงขององค์การ 4. ติดตามและประเมินผลการควบคุมภายใน โดยผู้มีความรู้ความสามารถ 5. กำหนดแนวทางการรายงานผลการตรวจสอบภายใน ขึ้นตรงต่อคณะกรรมการตรวจสอบ 6. ส่งเสริมให้ผู้ตรวจสอบภายในปฏิบัติหน้าที่ตามมาตรฐานสากล การปฏิบัติงานวิชาชีพการตรวจสอบภายใน
หลักการ 17 ประเมินและสื่อสารข้อบกพร่องของการควบคุมภายในทันเวลา และเหมาะสม	1. ประเมินผลและสื่อสารข้อบกพร่องของการควบคุมภายใน และด าเนินการแก้ไขอย่างทันท่วงที 2. รายงานต่อคณะกรรมการบริษัททันทีที่เกิดเหตุการณ์ทุจริตร้ายแรง การฝ่าฝืนกฎหมาย หรือการกระทำที่ผิดปกติ ซึ่งกระทบชื่อเสียงและฐานะการเงินบริษัทอย่างมีนัยสำคัญ 3. รายงานข้อบกพร่องที่เป็นสาระสำคัญ พร้อมแนวทางแก้ไข ต่อคณะกรรมการบริษัท/คณะกรรมการตรวจสอบในเวลาอันควร

Principle of COSO Internal Control: 2013

การสอบทานการบริหารความเสี่ยงขององค์กร

5 องค์ประกอบ	คำถามสำหรับสอบทาน
สภาพแวดล้อมการควบคุม (CE) **Control environment**	1. กระบวนการจัดทำแผนบริหารความเสี่ยงและวางระบบการควบคุมภายในของส่วนงาน 2. การมีส่วนร่วมในการบริหารจัดการความเสี่ยง 3. การสื่อสาร ติดตามกระบวนการบริหารความเสี่ยง 4. ความรู้ความเข้าใจในการบริหารความเสี่ยง
การประเมินความเสี่ยง (RA) **Risk assessment**	5.เครื่องมือที่ใช้ในการประเมิน/วิเคราะห์ความเสี่ยง 6. วิธีการประเมินความเสี่ยง 7. การประเมินความเสี่ยงของส่วนงานและการเชื่อมโยงกับกรอบการบริหารความเสี่ยงฯ ของมหาวิทยาลัย
กิจกรรมการควบคุม (CA) **Control activities**	8. การมอบหมายผู้ปฏิบัติงานจัดการความเสี่ยง 9. การดำเนินกิจกรรมควบคุมความเสี่ยงตามแผนงาน 10. ปัญหาและอุปสรรค
สารสนเทศและการสื่อสาร (IC) **Information and communication**	11. การสื่อสารข้อมูลไปยังบุคลากรของส่วนงาน 12. บุคลากรหรือผู้ที่เกี่ยวข้องกับมีความเข้าใจในเรื่องความเสี่ยงและระบบการควบคุมภายในและวิธีการปฏิบัติงานได้
การติดตามและประเมินผล (MA) **Monitoring activities**	13. ติดตามและประเมินผลการควบคุมภายใน 14.การนำเสนอผลการติดตาม

Principle of COSO Internal Control: 2013

การสอบทานการบริหารความเสี่ยงขององค์กร

Step 1 วางแผนการสอบทาน	Step 2 ปฏิบัติการสอบทาน	Step 3 สรุปผลการสอบทาน	Step 4 จัดทำรายงานผลการสอบทาน
วางแผนการสอบทานการบริหารความเสี่ยงขององค์กร/หน่วยงานภายใต้องค์กร พร้อมกำหนดขอบเขตการตรวจสอบ เช่น ตรวจสอบตามกรอบ COSO IC 2013 หรือ ตรวจสอบด้วยแบบ ป.ค. 6	นำแผนบริหารความเสี่ยงและรายงานผลการบริหารความเสี่ยงของหน่วยรับการสอบทานมาทวนสอบ วิเคราะห์และประเมินผล ตามองค์ประกอบต่างๆที่กำหนดไว้ ประกอบด้วย ประเด็นเสี่ยง ปัจจัยเสี่ยง การประเมินความเสี่ยง มาตรการจัดการความเสี่ยง ผลการบริหารความเสี่ยง	นำผลการปฏิบัติการสอบทานมาสรุปผลการสอบทานการบริหารความเสี่ยง ระบุหลักฐาน พร้อมให้ข้อเสนอแนะเพื่อการปรับปรุงและพัฒนาแผนบริหารความเสี่ยง	นำผลการสอบทานมาจัดทำรายงานเพื่อเสนอกลับไปยังหน่วยรับการสอบทาน ฝ่ายบริหารองค์กร และคณะกรรมการที่เกี่ยวข้อง

เอกสารประกอบ

การสอบทานตามมาตรฐานการควบคุมภายในสำหรับหน่วยงานของรัฐ ตาม COSO 2013 ประกอบด้วย 5 องค์ประกอบ 17 หลักการ ดังนี้

เรื่อง	มี/ไม่มี	ผลการสอบทาน
องค์ประกอบที่ 1: สภาพแวดล้อมการควบคุม (Control Environment)		
หลักการที่ 1 – หน่วยงานของรัฐแสดงให้เห็นถึงการยึดมั่นในคุณค่าของความซื่อตรงและจริยธรรม		
หลักการที่ 2 – ผู้กำกับดูแลของหน่วยงานของรัฐ แสดงให้เห็นถึงความเป็นอิสระจากฝ่ายบริหารและมีหน้าที่กำกับดูแลให้มีการพัฒนาหรือปรับปรุงการควบคุมภายใน รวมถึงการดำเนินการเกี่ยวกับการควบคุมภายใน		
หลักการที่ 3 - หัวหน้าส่วนงานของรัฐจัดให้มีโครงสร้างองค์กร สายการบังคับบัญชา อำนาจหน้าที่และความรับผิดชอบที่เหมาะสมในการบรรลุวัตถุประสงค์ของหน่วยงานของรัฐภายใต้การกำกับดูแลของผู้กำกับดูแล		
หลักการที่ 4 – หน่วยงานของรัฐแสดงให้เห็นถึงความมุ่งมั่นในการสร้างแรงจูงใจ พัฒนาและรักษาบุคลากรที่มี		

ผลการสอบทาน

1. สอบทานตามมาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ ข้อ 2 มาตรฐาน

มาตรฐาน	มี/ไม่มี	ผลการสอบทาน
1. หน่วยงานของรัฐต้องจัดให้มีการบริหารจัดการความเสี่ยง เพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผลแก่ผู้มีส่วนได้เสียของหน่วยงานว่าหน่วยงานได้ดำเนินการบริหารจัดการความเสี่ยงอย่างเหมาะสม		
2. ฝ่ายบริหารของหน่วยงานของรัฐต้องจัดให้มีสภาพแวดล้อมที่เหมาะสมต่อการบริหารจัดการความเสี่ยงภายในองค์กร		
3. หน่วยงานของรัฐต้องมีการกำหนดวัตถุประสงค์เพื่อใช้ในการบริหารจัดการความเสี่ยงที่เหมาะสม รวมถึงมีการสื่อสารการบริหารจัดการความเสี่ยงของวัตถุประสงค์ด้านต่าง ๆ ต่อบุคลากรที่เกี่ยวข้อง		

Risk Quotes

Risk Comes From Not Knowing What You’re Doing.

#WarrenBuffett

ขอบคุณครับ

ดร.อวิรุทธ์ ฉัตรมาลาทอง

ผู้อำนวยการฝ่ายยุทธศาสตร์และพัฒนาวิชาการ
สำนักบริหารวิชาการ จุฬาลงกรณ์มหาวิทยาลัย

Contact Us:

Location: อาคารจามจุรี 5 ชั้น 6 จุฬาลงกรณ์มหาวิทยาลัย
Email: awirut.c@chula.ac.th
Website: http://www.knackbox.me
Phone: 086-416-1566

Follow Me

KNACK BOX

Enterprise Risk Management Solutions

Knack Box: กล่องขนมสมองของนักเรียนรู้

4K likes • 4.4K followers