เทคนิคการจัดทำแผนการบริหารความเสี่ยง (RISK MANAGEMENT PLAN) ตามหลัก COSO

ณ ห้อง NAKA BALLROOM โรงแรม ดุสิต ปริ๊นเซส

อ.เมือง จ.พัทลุง

ระหว่างวันที่ 3 - 4กุมภาพันธ์ 2568

จัดโดย : มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

ผู้บรรยาย : สุรพงษ์ ชูรังสฤษฎ์, CIA 30836

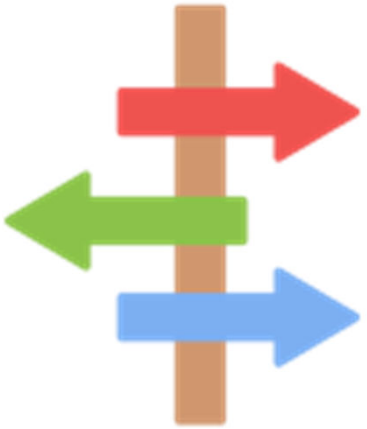
เนื้อหา

- ทบทวนความรู้ การบริหารความเสี่ยง และกระบวนการ เครื่องมือ ในการบริหารความเสี่ยง
- การประเมินระดับความเสี่ยง (Degree of Risk) ตามแนวทาง COSO
- ความเชื่อมโยงของทิศทางการดำเนินงานองค์กรกับการตั้งเป้าหมายในการบริหารความเสี่ยง
- Key Risk Indicator (KRI)
- work shop : การจัดทำ Risk Appetite , Risk Tolerance , Trigger point ในการติดตามความเสี่ยงและปัจจัยเสี่ยง
- work shop : การจัดทำแผนที่เชื่อมโยงความเสี่ยง Risk Correlation Map และรากของปัญหาที่นำไปสู่การกำหนดมาตรการตอบสนองความเสี่ยง และกลยุทธ์การตอบสนองความเสี่ยง
- นำเสนอแผนการบริหารความเสี่ยง ระดับหน่วยงานและระดับมหาวิทยาลัย และวิเคราะห์แลกเปลี่ยนเรียนรู้ร่วมกับวิทยากร เป็นรายหน่วยงาน

Governance

พรบ. วินัยการเงิน การคลังของรัฐ พ.ศ. 2561 – โดยมาตรา 79

หลักเกณฑ์กระทรวงการคลัง



การบริหารความเสี่ยง

(COSO –ERM)

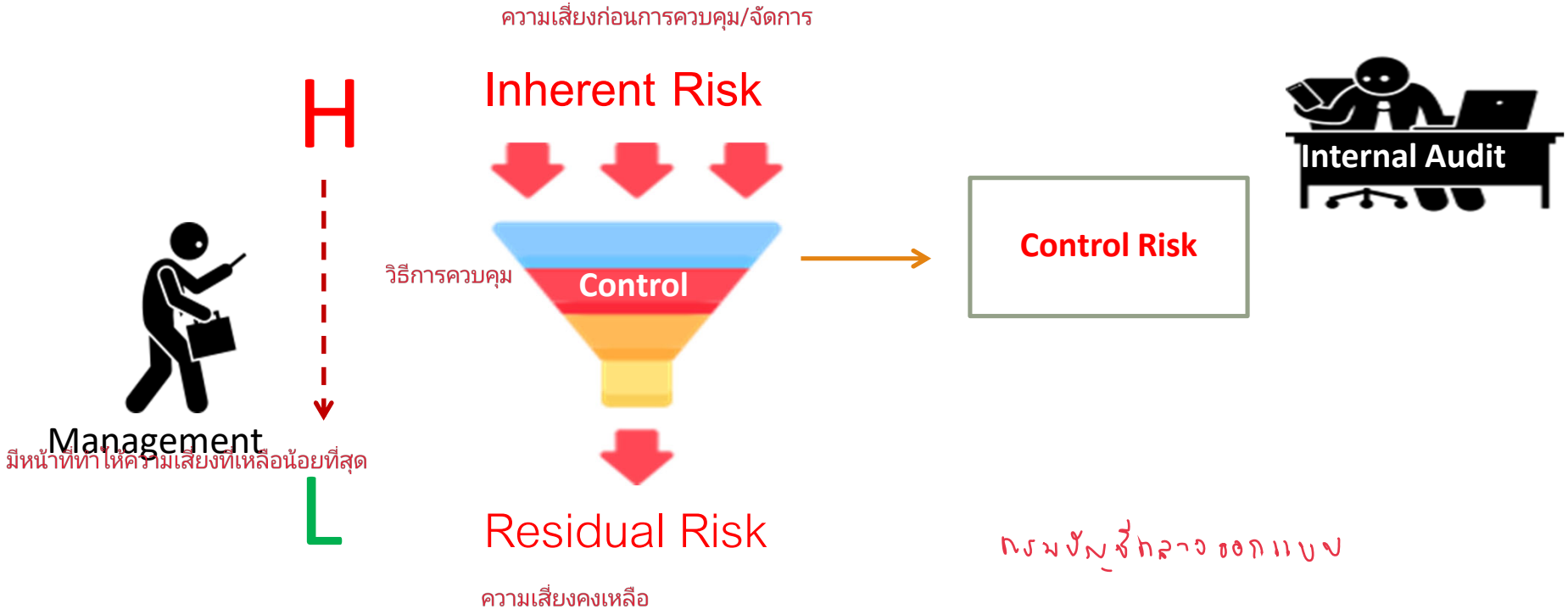
การตรวจสอบภายใน

(IIA Standard)

การควบคุมภายใน

(COSO Internal Control

Risk –Control –Internal Audit
ทำไมต้องกำหนดให้มี?



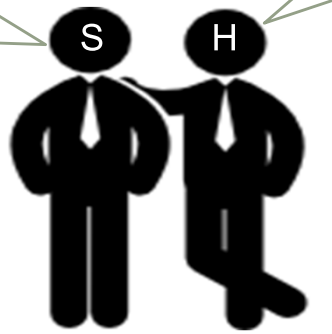
ปัญหา ในการใช้(Implement)

ควรจะเริ่มจากเข้าใจก่อน

เข้าใจก่อน
แล้วค่อยทำ

ทำตามนี้ก่อนแล้ว
จะ เข้าใจเอง

ทำมาตั้งนานแล้ว
ยังไม่เข้าใจ



Soft Side ⇌ Hard Side

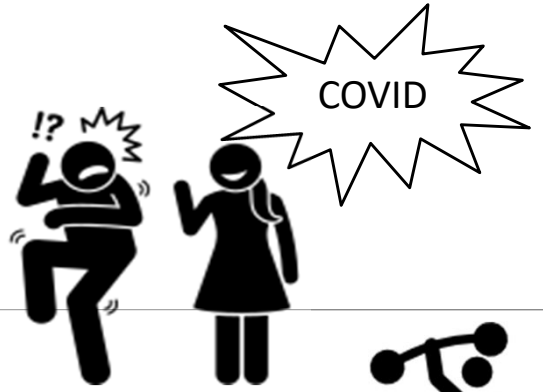
นโยบาย หลักเกณฑ์ และแนวปฏิบัติ

ออก → สักวันหนึ่งจะเข้าใจเอง

- ความเข้าใจตรงกัน และรับรู้ถึงความรับผิดชอบ
- สร้างวัฒนะธรรมองค์กร

ทบทวนแนวคิด - ความเสี่ยง

ใครมีความเสี่ยงใน กรณีCovid ไม่



A

ติดเชื้อ Covid รักษาตัวอยู่ รพ.

ไม่มีความเสี่ยง

แต่เป็นปัญหา เพราะเป็นโควิดแล้ว

B

- อยู่ คอนโด
- ออกจากบ้านทุกวัน ใช้รถสาธารณ
- ทานอาหารที่ร้าน
- ฉีด วัคซีน 1 เข็ม

C

- อยู่ บ้านเดียว
- ออกจากบ้านทุกวัน ใช้รถส่วนตัว
- นำอาหาร ทานที่ทำงาน
- ฉีด วัคซีน 1 เข็ม

D

- อยู่บ้านเดี่ยว คนเดียว
- ออกกำลังกายประจำ
- ออกจากบ้านเท่าที่จำเป็น
- สั่งอาหารมาทานที่บ้าน/ทำเอง
- ฉีด วัคซีน 2 เข็ม

ทบทวนแนวคิด-ความเสี่ยง

ใช้คิดถึงปัญหาในอดีต ว่ายังจะเกิดขึ้นมั้ย
แก้ไขซ่อมบางแล้ว แต่ก็ยังมีความเสี่ยงในการอาจจะเกิดอีก

วันนี้

Problem

แล้วมันจะเกิดความเสี่ยงขึ้นเมื่อไหร่
- ถนนเป็นหลุมเป็นบ่อ ✗
- รอยที่ซ่อมชำรุด ✗
- เจอตำรวจ ✗ → ปัญหา
- ตกใจที่มีมอเตอร์ไซค์ออกจากบ้าน ✓

8.30 น.

วันพรุ่งนี้และต่อ ๆไป

มีความเสี่ยง? / เกิดความเสี่ยง

8.30 น.

ธรรมชาติของ ความเสี่ยง

- “ความไม่แน่นอน” เป็น “สิ่งที่แน่นอน”
- ความไม่แน่นอน เป็นที่มาของความเสี่ยง
- “ ความเสี่ยง” เป็นสิ่งที่ไม่อาจห้าม ไม่ให้เกิดขึ้นได้

ข้อคิดสำคัญ ก่อนเริ่มต้น

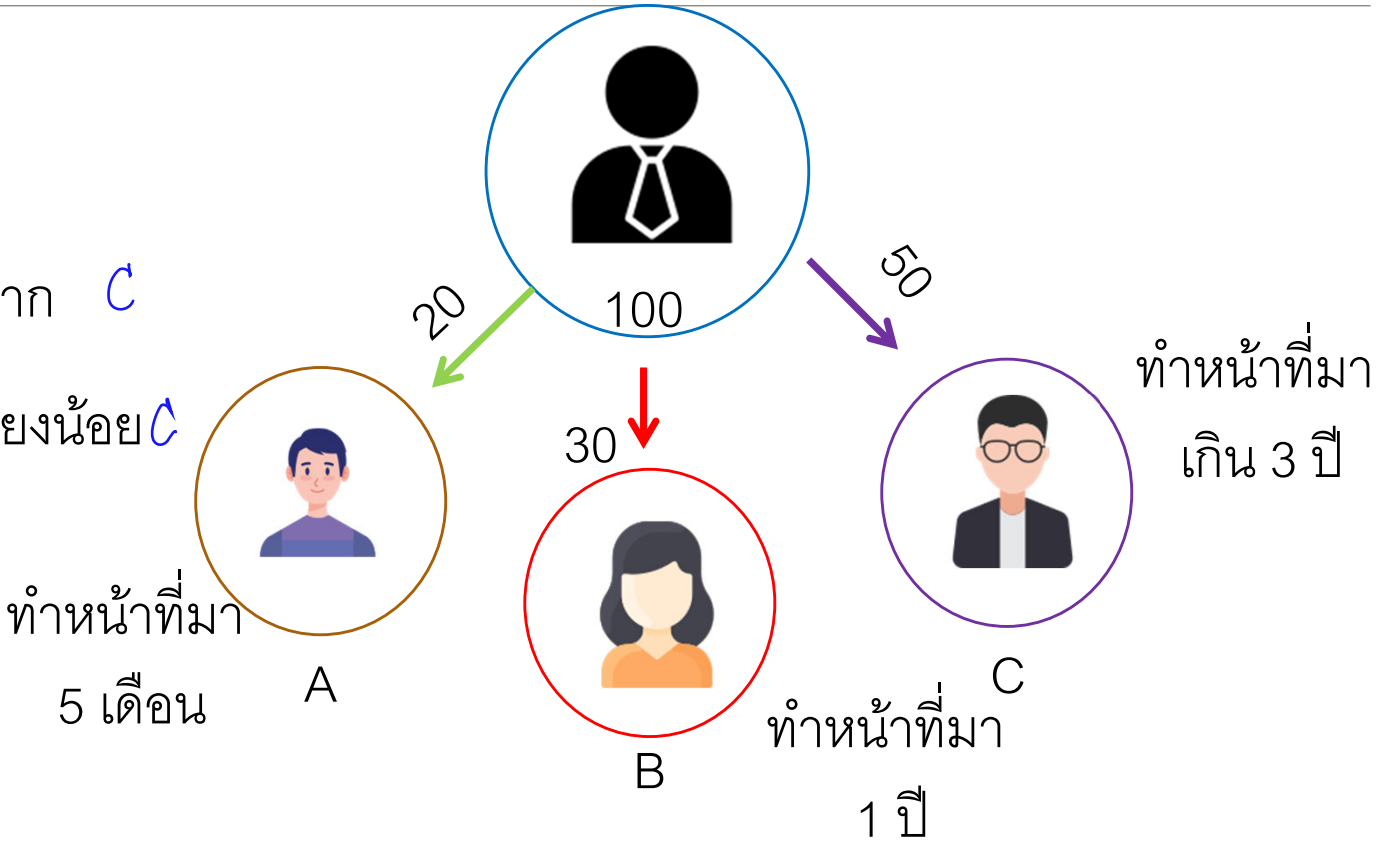
งานที่เราทำอยู่?

งานที่มหาวิทยาลัยให้เรา

มุมมอง ของความเสี่ยง

1. ใครรับความเสี่ยงมาก C

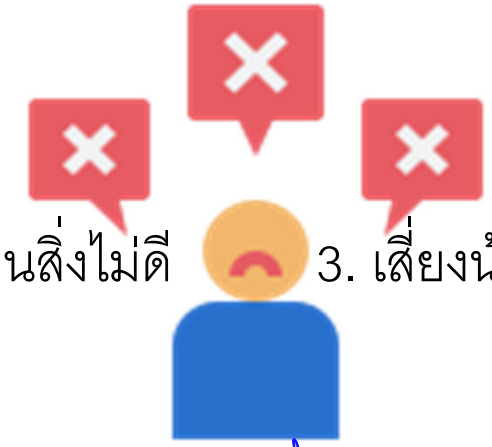
2.ใช้ใครความเสี่ยงน้อย C



ความเชื่อ และ ปัญหาในการนำ การบริหารความเสี่ยง สู่การปฏิบัติ

3 ความเชื่อผิดๆ

2. ความเสี่ยงต้องทำให้หมดไป จนเหลือความเสี่ยง



1. ความเสี่ยงเป็นสิ่งไม่ดี

3. เสี่ยงน้อยที่สุด ดีที่สุด

✓ ผลของการมาจากความเสี่ยง

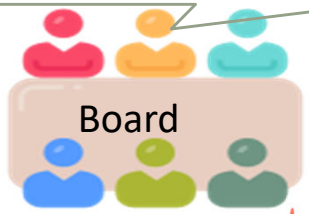
- x คนในองค์กรเข้าใจเรื่อง “ความเสี่ยง” ไม่ตรงกัน
- x คนในองค์มีทัศนคติในทางลบ/ต่อต้าน
- x วัฒนะธรรมองค์กร ← ทัศนคติ พฤติกรรม
- x ผู้บริหารไม่สนับสนุน
- x ไม่ได้รับความร่วมมือจากคนส่วนใหญ่
- x ไม่รู้บทบาท และความรับผิดอบที่ชัดเจน
- x ไม่รู้แนวทาง เป้าหมายและวิธีปฏิบัติที่ชัดเจน

Core value → สร้างวัฒนธรรมองค์กร

จุดเริ่มต้นที่ดี

2. Develop an effective organizational control structure ควบคุม ความเสี่ยง

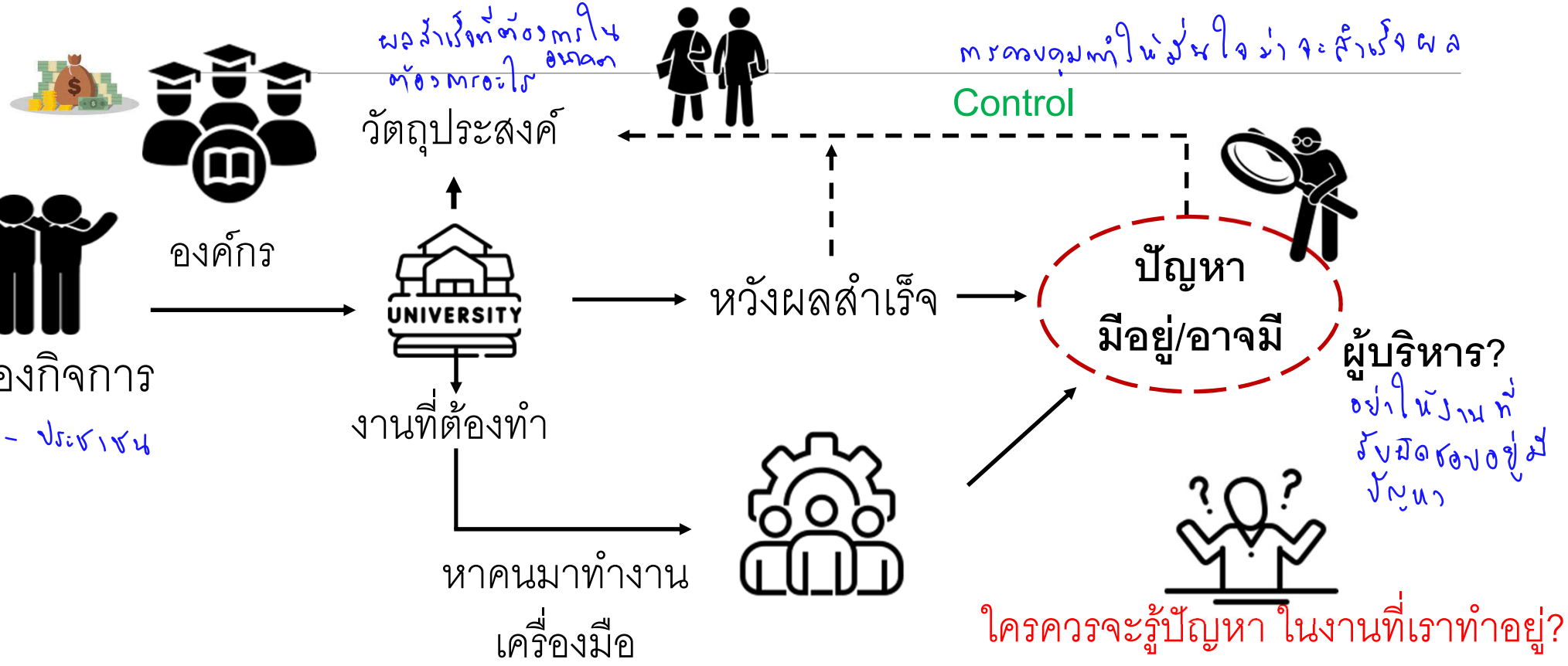
1. Develop a common risk language -- “speak the same language”



3. Create a process view – embedded within all key process

สร้างกระบวนการหลัก

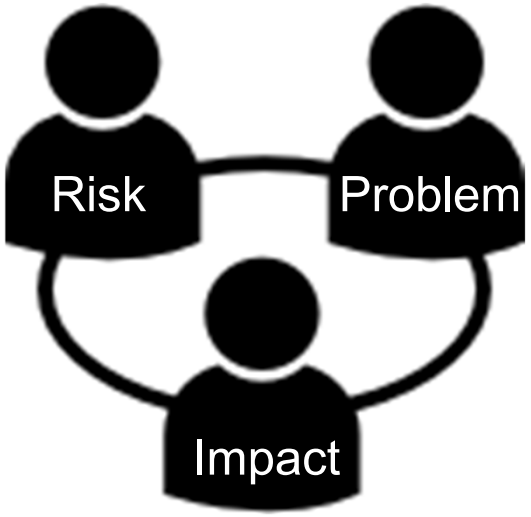
ความเสี่ยง – องค์กร – ผู้บริหาร - บุคลากรขององค์กร



ความเสี่ยง – ปัญหา – ความเสียหาย – ผู้เสียหาย
- ใครทำให้เกิดความเสียหาย

ความเสี่ยง

ข้อสอบอาจรั่ว



ปัญหา

ข้อสอบรั่ว

ตกเป็นข่าวเสียชื่อ

เส้นปัจจุบัน หมายถึง ความเสี่ยง ถึง ปัญหา

1. ใครเสียชื่อ ?
2. ใครทำให้เกิดความเสียหาย?
3. สาเหตุ ?

Risk & Problem

Problem

- เงินทดรองจ่ายค้างเกินกำหนด
- เอกสารสัญญา เสียหาย/สูญหาย
- ผู้ลงนามในสัญญา ไม่ใช่ผู้มีอำนาจ
- ผู้รับเหมา ทิ้งงาน

Risk

- เงินทดรองจ่ายอาจค้างเกินกำหนด
- เอกสารสัญญา อาจเสียหาย/สูญหาย
- ผู้ลงนามในสัญญา อาจไม่ใช่ผู้มีอำนาจ
- ผู้รับเหมา อาจทิ้งงาน

1. อะไรเกิดขึ้นก่อน ?
2. ควรรู้อะไร เพื่อไม่ให้เกิดอะไร?

การบริหารความเสี่ยง

ปัจจัย ที่มีผลต่อ โอกาส หรือ ผลกระทบ ความเสี่ยง

(KRI)

ค้นหา ระบุ วัดความเสี่ยง

กำหนด วิธีการควบคุม

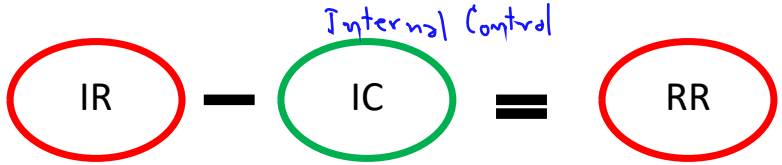
ปัจจัย - คน กระบวนการ ที่ไม่มีปัญหา
- เครื่องมือที่ใช้
- ข้อมูล (ไม่มีข้อมูล) information

Key Risk Indicator : เป็นตัวเตือนภัยไม่ใช่ตัวจัดความเสี่ยง

ความหมายของคำต่างๆ ที่ควรทราบ

- *Risk – เหตุการณ์ที่อาจเกิดขึ้น ส่งผลต่อความเสียหายหรือทำให้ไม่บรรลุวัตถุประสงค์*
- *Risk Management – การรับรู้ จัดการ และเฝ้าระวัง ความเสี่ยง*
- *Inherent Risk – ความเสี่ยงที่มีอยู่ตามสภาพ (ก่อนการควบคุม)*
- *Residual Risk – ความเสี่ยงคงเหลือ จากการควบคุม*

- *Risk Appetite* - " degree/level of uncertainty an enterprise is willing to accept to reach its goals." "**ระดับที่ยอมเสี่ยง**"
- Risk Tolerance หมายถึงระดับความเบี่ยงเบน**ที่ยอมรับได้**ที่สัมพันธ์กับการบรรลุวัตถุประสงค์ใด วัตถุประสงค์หนึ่ง

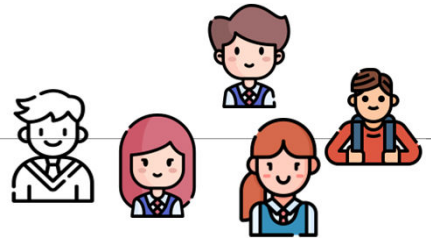


Inherent Risk– Residual Risk ,Risk Appetite – Risk Tolerance-KPI?

รับความเสี่ยงได้ขนาดนี้

Inherent Risk

นักศึกษา อาจเรียนไม่จบหลักสูตร ตามเวลา

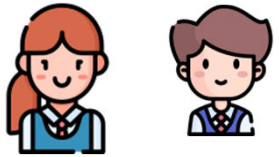


H

Risk Appetite

- เฉพาะที่จบสายวิทยาศาสตร์
- เกรดที่จบไม่ต่ำกว่า 2.5
- จำนวนนักศึกษาสูงสุด ไม่เกิน 150 คน

กำหนดรายปี



ควบคุมให้อยู่ใน Risk Appetite

- กำหนด%เข้าเรียน
- อาจารย์ที่ปรึกษา
- ทดสอบระหว่างภาค

ควบคุมให้มั่นใจว่า
จะจบได้ตามเวลาที่กำหนด

Control

Residual Risk = L

เป้าหมาย นักศึกษาที่จบตามเวลาที่กำหนด
ระดับที่ยอมรับได้

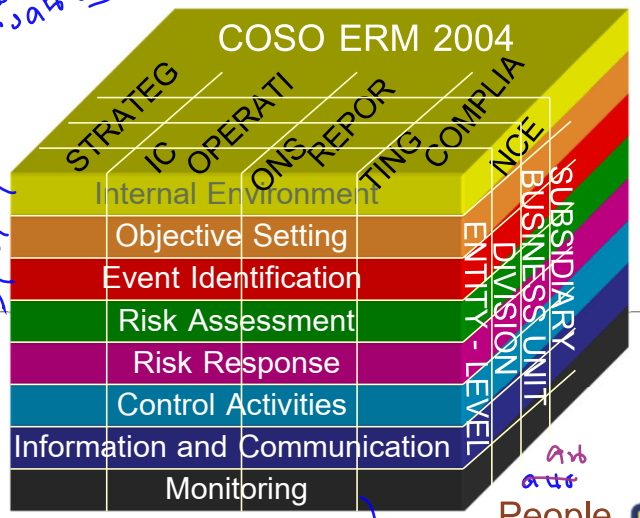
97%
↓
100%

Risk Tolerance ผลสำเร็จที่ยอมรับได้

COSO 1992 → การควบคุมภายในมีปัญหา

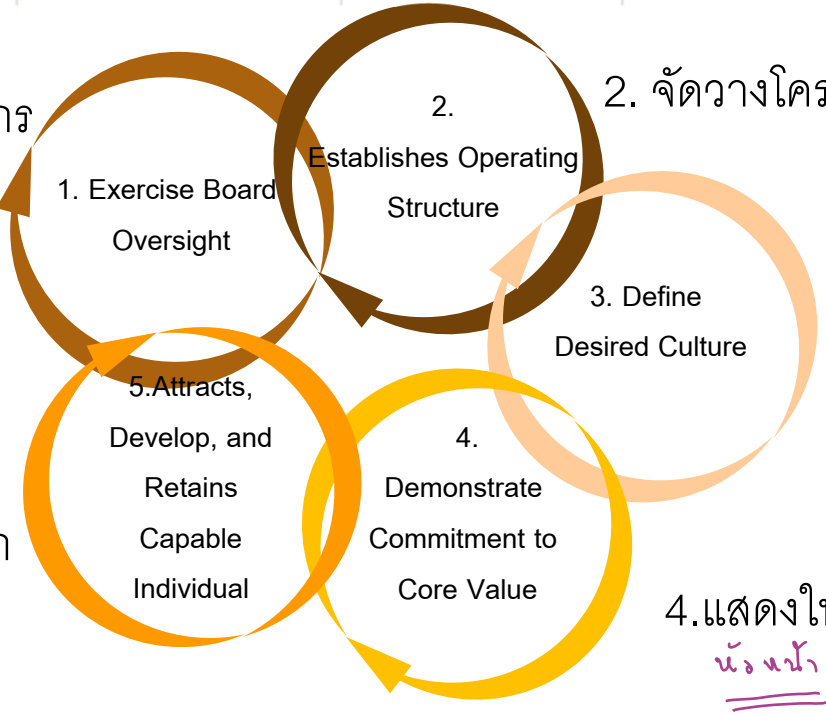
COSO ERM

ERM คือกระบวนการ ที่จะเกิดผลได้จากการร่วมมือกันระหว่างกรรมการ คณะผู้บริหารและบุคคลอื่นๆขององค์กร นำมาประยุกต์ใช้ในการกำหนดกลยุทธ์ และใช้ทั่วทั้งองค์กร เพื่อบ่งชี้เหตุการณ์ที่อาจเป็นไปได้ ซึ่งอาจมีผลกระทบต่อองค์กร และจัดการกับความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ เพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผล เกี่ยวกับการบรรลุวัตถุประสงค์ขององค์กร



ปรับปรุง COSO ERM 2017

1.คณะกรรมการองค์กร
กำกับดูแลความเสี่ยง
ผู้ทรงจากบุคคลภายนอก

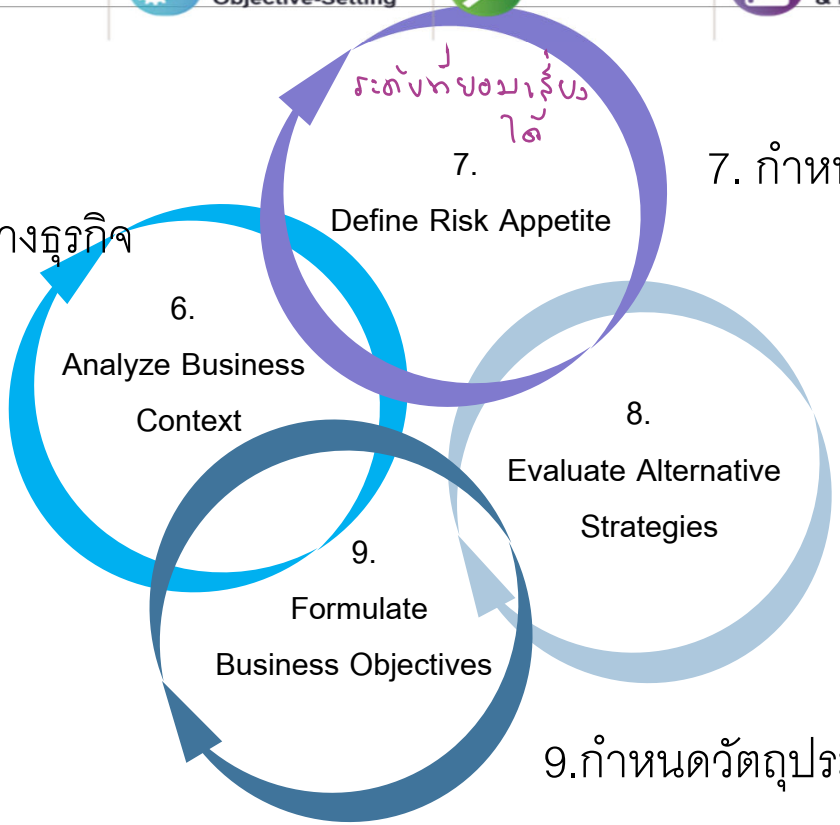


2. จัดวางโครงสร้างการดำเนินงาน

3.กำหนดวัฒนะธรรมองค์กร
ที่ควรจะเป็น

5. จูงใจ พัฒนา และรักษาไว้
ซึ่งบุคคลากรที่มีความสามารถ

4.แสดงให้เห็นถึงค่านิยมองค์กร
หัวหน้าต้องเป็นตัวอย่างให้เห็นถึงค่านิยมองค์กร



6.วิเคราะห์โครงสร้างทางธุรกิจ

7. กำหนดระดับที่องค์กรยอมเสี่ยงได้

8. ประเมินทางเลือก ด้านกลยุทธ์

ใช้รูปแบบการบรรลุวัตถุประสงค์

9.กำหนดวัตถุประสงค์ในการดำเนินธุรกิจ

10. ระบุความเสี่ยง

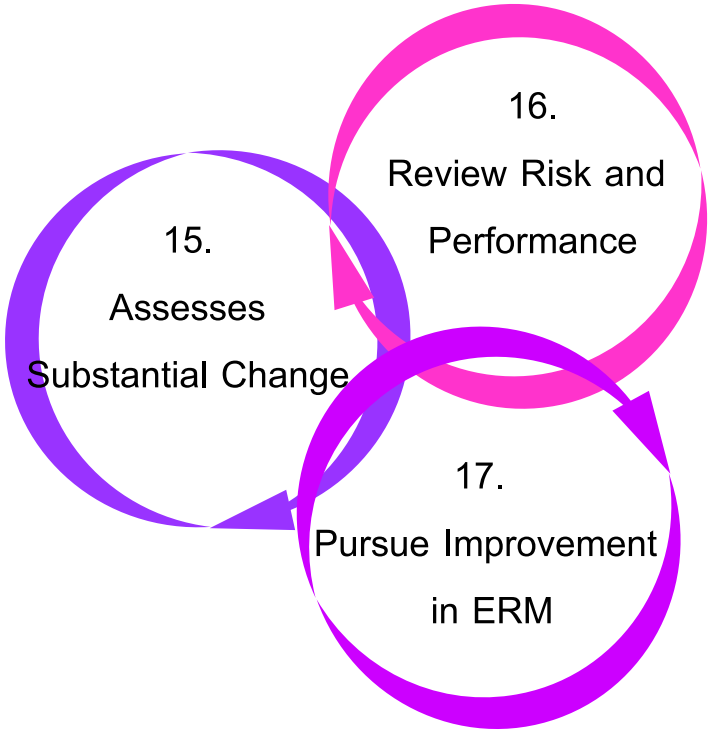
11. ประเมินความรุนแรงของความเสี่ยง

12. . จัดลำดับความเสี่ยง

13. ดำเนินการตอบสนองต่อความเสี่ยง

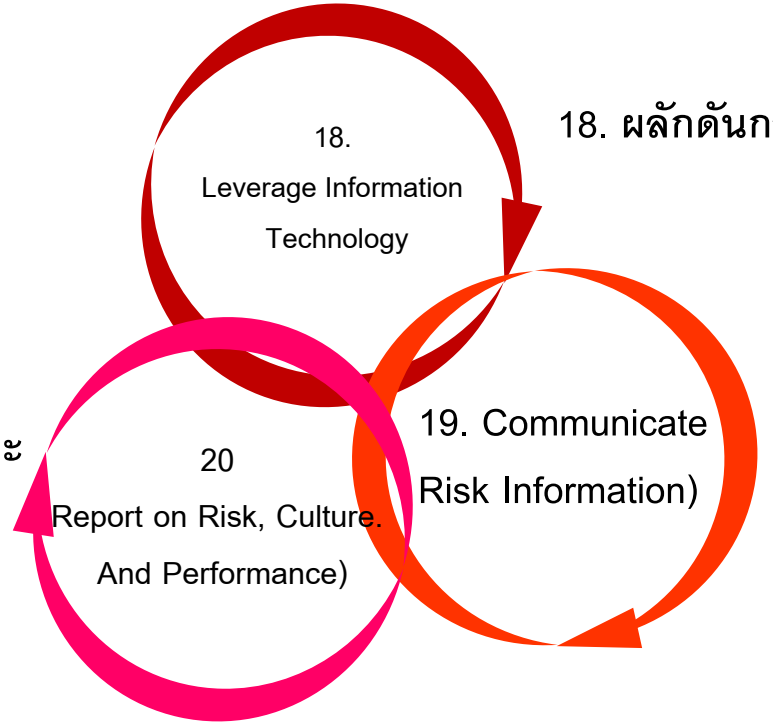
14. จัดทำภาพรวมความเสี่ยงองค์กร

15. ประเมินการเปลี่ยนแปลงที่มี



16 ทบทวนความเสี่ยงและผลการดำเนินงาน

17. หาแนวทางในการปรับปรุง
การบริหารความเสี่ยงขององค์กร



18. ผลักดันการใช้เทคโนโลยีสารสนเทศ

19. สื่อสารข้อมูลความเสี่ยง

20. รายงานความเสี่ยง วัฒนธรรม และผลการดำเนินงาน

การควบคุม เกี่ยวข้องกับวัตถุประสงค์และความเสี่ยง

ผลสำเร็จที่ต้องการ ความหวัง

"The things an organization wants to accomplish"

สิ่งที่ช่วยให้เกิดผลสำเร็จด้วยการจัดการความเสี่ยง

"things that help Meet an objective by managing the risk."

การควบคุม

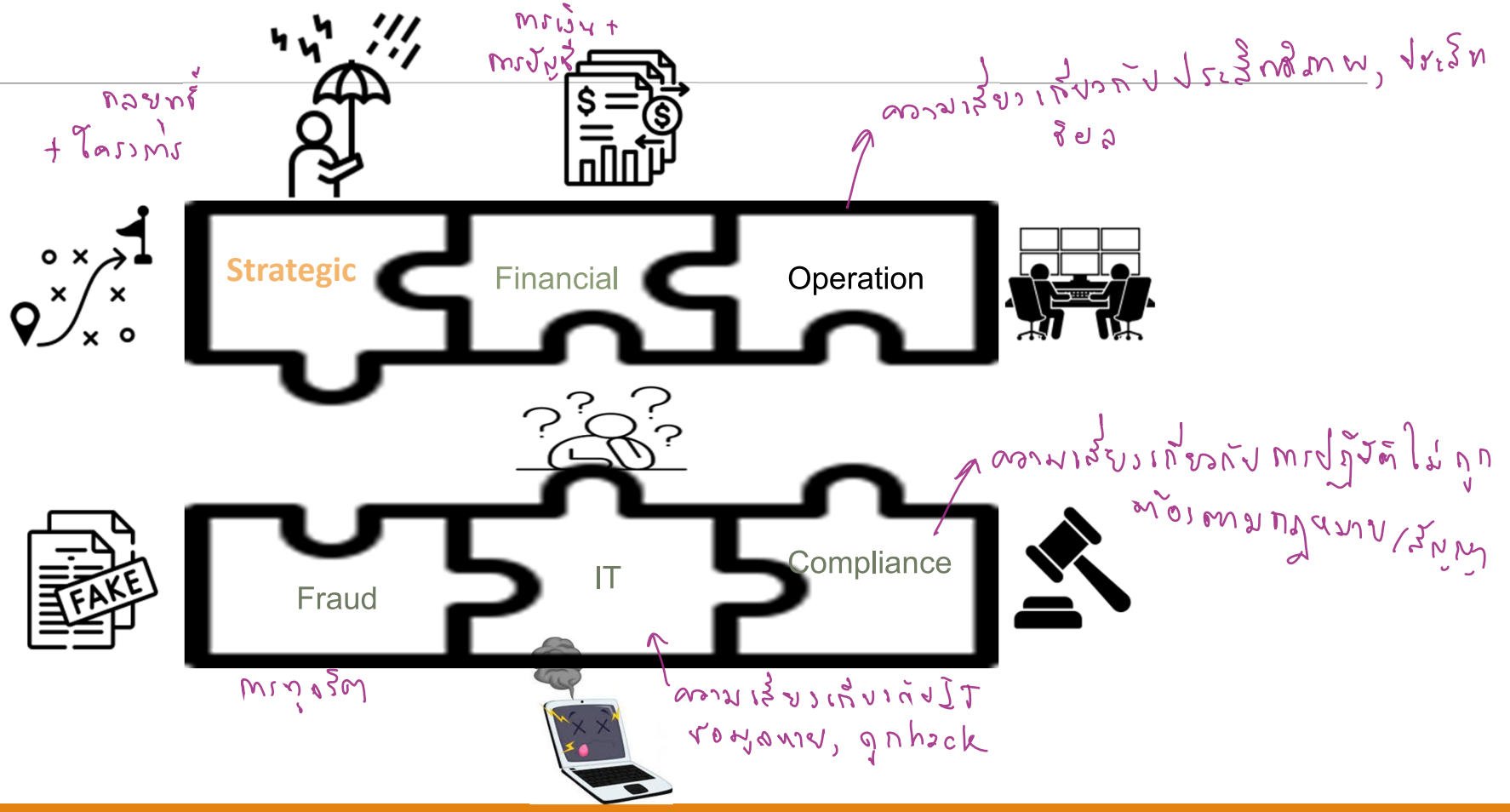
สิ่งที่เป็นอุปสรรคต่อผลสำเร็จ

"Things that might prevent accomplishment an objective"

สิ่งที่ทำให้ไม่สำเร็จ

Governance : ความรับผิดชอบในหน้าที่

ประเภทความเสี่ยง



Compliance Risk

เหตุฝ่าฝืนข้อกำหนดของทางการ กฎหมาย หรือ สัญญา เช่น ไม่รายงานธุรกรรมที่น่าสงสัย ให้เปิดบัญชีโดยไม่มีหลักฐานแสดงตน ผิดเงื่อนไขสัญญาที่องค์กร ทำไว้กับบุคคลภายนอก เป็นต้น

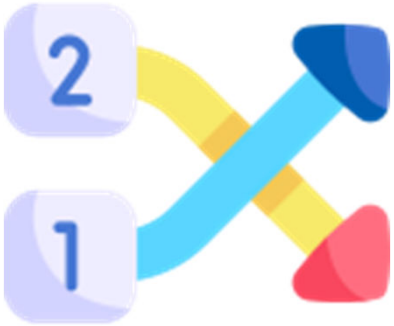
ระเบียบการจัดซื้อจัดจ้างที่ออกโดยกระทรวงการคลัง เป็นการควบคุมภายในมั้ย?

นิยามการควบคุมภายใน หน่วยงานของรัฐ : กระบวนการปฏิบัติงานที่ผู้กำกับดูแล หัวหน้าหน่วยงานของรัฐ ฝ่ายบริหาร และ บุคลากรของหน่วยงานของรัฐ จัดให้มีขึ้น เพื่อสร้างความมั่นใจอย่างสมเหตุสมผล ว่า การดำเนินงานของหน่วยงานของรัฐจะบรรลุวัตถุประสงค์ด้านการดำเนินงาน ด้านการรายงาน และการปฏิบัติตามกฎหมาย ระเบียบและข้อบังคับ

Top-down Approach VS. Bottom-up Approach

Top-down

Bottom-up



1 Unit /Department

2 Risk

3 Control

Silo View

Top 10 /20 Risks 1 → 2 Key Process

Owner 3 → 4 Control

Process View

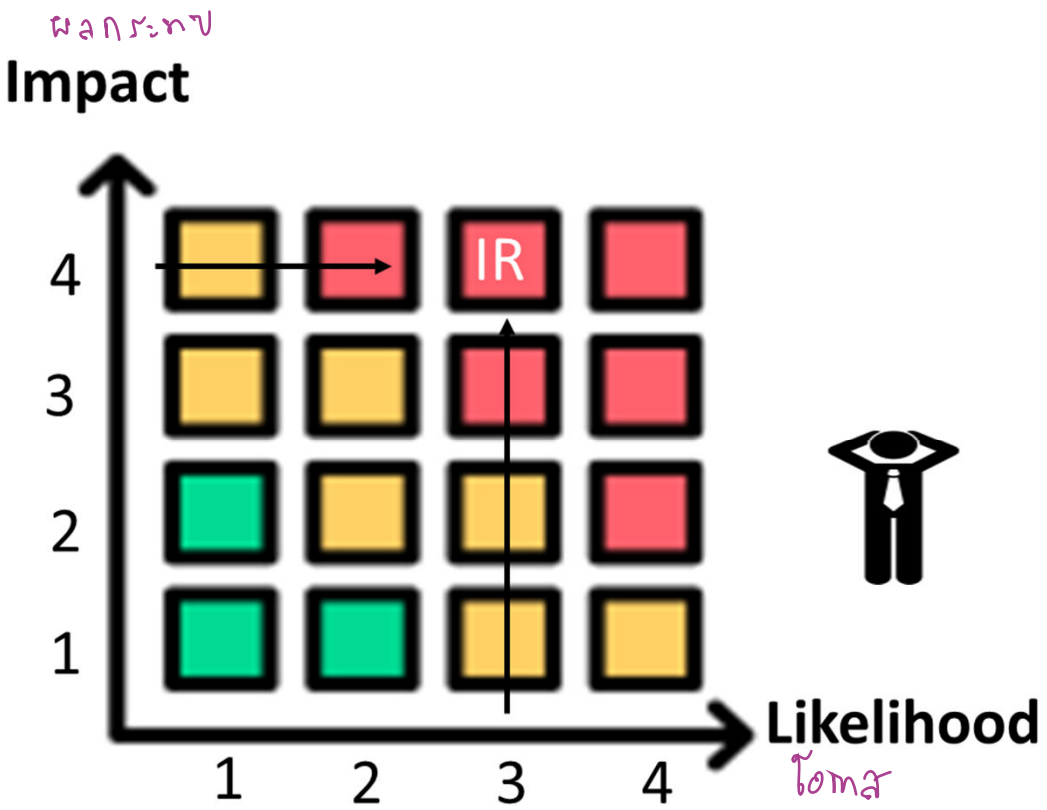
1. Risk Identification - งานที่รับผิดชอบ

ประเภทความเสี่ยง	ปัญหาที่เคยเกิดขึ้น/อาจจะเกิดขึ้น
กลยุทธ์	โครงการสนับสนุนกลยุทธ์ มีปัญหาอะไรเกิดขึ้นได้บ้าง ?
Financial	ด้านบัญชี การเงิน สภาพคล่อง
Operation	ความผิดพลาด ล่าช้า อุบัติภัยต่างๆ
Compliance	ฝ่าฝืน ไม่ปฏิบัติตาม กฎหมาย ระเบียบทางการ มาตรฐาน สัญญา
IT	การประมวลผล ความปลอดภัยข้อมูล การหยุดชะงัก ระบบการสื่อสาร
Fraud	วิธีการทุจริตที่อาจเกิดขึ้น

2. Risk Assessment & Evaluation

เป็นการประเมินในระดับ Inherent Risk

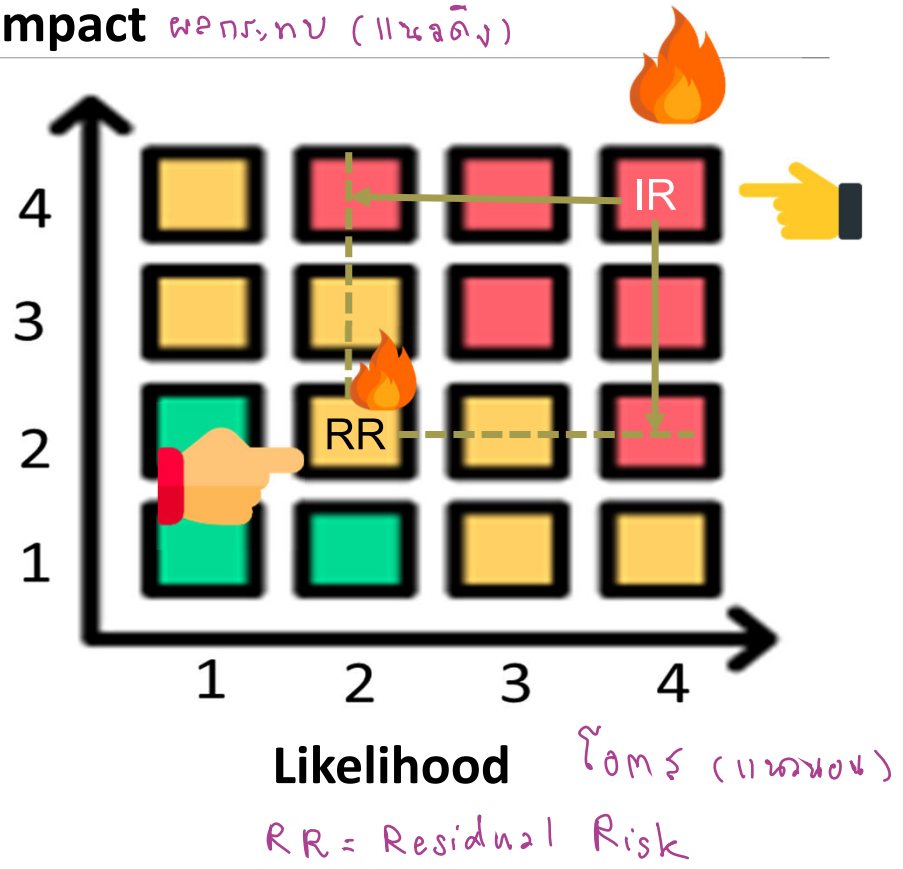
ใช้ปัจจัย โอกาส และผลกระทบ หากจัดการความเสี่ยงไม่ได้ เป็นปัจจัยประเมิน



2. การวัดความเสี่ยง Inherent & Residual Risk (Net Risk)

เกิดอัคคีภัย :

1. ทำประกันภัย
2. สัญญาณเตือนภัย
3. Smoke Detection
4. อุปกรณ์ ดับเพลิง
5. Springer
6. แผนฉุกเฉิน
7. เครื่องตัดไฟ



การรับมือกับความเสี่ยง (Risk Response)

- Identifying Risk Response
  - Avoid (e.g. exit business, sell unit) หลีกเลี่ยงไม่เกิน Risk Apitite
  - Reduce (business decisions to reduce risk impact, likelihood, or both)
  - Share (e.g. insurance, pooling, outsourcing) แชร์ไม่ outsourcing
  - Accept (no action taken)
  - Other? แผนทดแทน, แผนรองรับ เช่น การเกิดอุทกภัย

การเฝ้าระวัง : KRI – ประโยชน์ และการกำหนดค่า

ปริมาณน้ำมัน เป็นตัวเตือนภัย

Key Risk Indicator

ความเสี่ยง น้ำมันอาจจะหมด

- เป็นการกำหนด “สิ่งเตือนภัย” และ “ระดับเตือนภัย” เพื่อใช้ในการเฝ้าระวังความเสี่ยง
- ระดับเตือน ต้องกำหนดเป็น “จำนวนนับ” เป็นระดับเพื่อ “เตือน” ให้รู้ว่าอยู่เฉยไม่ได้
- พร้อมทั้งกำหนด “วิธีปฏิบัติ” เมื่อถึงระดับเตือนภัย
- สิ่งเตือนภัย เป็นได้ทั้ง Lead และ Lag (ตัวนำ และตัวตาม)

ปริมาณน้ำมันเป็นสิ่งเตือนภัย
ระดับสีแดงเป็น ระดับเตือนภัย

ความเสี่ยง : ลิฟท์ค้าง
ควบคุม : บำรุงรักษา

KRI : จำนวนครั้งที่เกิดเหตุขัดข้องของลิฟท์ เช่น 3 ครั้ง/เดือน
Risk Ap : น้ำมัน, จำนวนคน

ตัวอย่าง

ความเสี่ยง	สิ่งเตือนภัย	ระดับเตือนภัย	ข้อปฏิบัติ
เกิดอัคคีภัย	จำนวนครั้งที่เกิดไฟฟ้าลัดวงจร	2 ครั้ง ต่อเดือน	ตรวจสอบระบบไฟฟ้า
หนี้สูญ	ร้อยละของลูกหนี้ ไม่ชำระตามกำหนดเพิ่มขึ้น	2%	• ออกหนังสือเตือน • ออกเยี่ยมลูกหนี้รายใหญ่
ระบบขัดข้อง ไม่สามารถให้บริการได้	ร้อยละ ที่เพิ่มขึ้นของปริมาณรายการ	5%	ทดสอบความพร้อมของสายสำรอง

Monitoring – Risk Factors

- กำหนดปัจจัย ทีมีผลต่อความเสี่ยงสำคัญขององค์กร นโยบายภครัฐเปลี่ยน, ผู้บริหารเปลี่ยน
- ติดตามการเปลี่ยนแปลงของปัจจัย
- ประเมินผลกระทบ
- รายงานคณะกรรม

เหตุผลและความสำคัญ ที่ต้องมีการควบคุม

- เหตุการณ์ / สิ่งที่เกิดขึ้น แล้ว ทำให้ เกิด
- ความยุ่งยาก
- เสียหาย ต่อองค์กร
- ไม่ได้ผลตามที่คาดหวัง / วัตถุประสงค์

- ไม่ให้เกิด
- รู้ได้เร็ว เมื่อเกิด เพื่อ ลดความเสียหาย

ใคร ไม่อยากให้เกิดปัญหา ?

จึงต้องรู้ว่า “อาจจะมีปัญหาอะไรเกิดขึ้นได้บ้าง”
คือ ความเสี่ยง (Risk) นั่นเอง

- list งาน ที่หน่วยงานต้องรับผิดชอบ

Risk-Control-governance

- ความเสี่ยงและการควบคุมเป็นสิ่งที่แยกกันไม่ออก เสมือน “เหรียญสองด้าน” สิ่งแรกที่ต้องทำคือการค้นหาและประเมินความเสี่ยง จากนั้นจึงต้องจัดการและลดความเสี่ยงโดยอาศัยระบบการควบคุม **แต่ระบบการควบคุมจะไม่ทำงาน**ถ้าอยู่ในมือของบุคคลที่ไม่เหมาะสม ดังนั้นการกำกับดูแลกิจการที่ดี จึงเป็นพื้นฐานสำคัญ ของระบบการควบคุมภายใน
- การกำกับดูแลเป็นวิธีการที่ทำให้มีขึ้น การสื่อสาร และการบังคับ ในเรื่องของหน้าที่และความรับผิดชอบในหน้าที่ 4ผู้มีบทบาทที่สำคัญคือ คณะกรรมการ ผู้บริหารระดับสูง ผู้สอบบัญชี และ ผู้ตรวจสอบภายใน ซึ่งต้องมีภาระร่วมกันด้วยการสร้างความสัมพันธ์อย่างใกล้ชิด ความซื่อสัตย์และจริยธรรมเป็นสิ่งสำคัญที่ทำให้เกิด Governance
- Accountability ความรับผิดชอบในหน้าที่

Lessons Learned

- Executive, audit committee and board support critical to success
- Ensure there is a clear vision of success
- Speak the same language ให้มีความเข้าใจตรงกัน
- Ownership of risks must be clearly defined
- Need for more clarity around roles
- Ensure that ERM is perceived as a process and not just an event in time
- Focus on action and not just reporting

work shop

ข้อมูลจาก รายงานผล การดำเนินงานตามแผนบริหารความเสี่ยง ประจำปีงบประมาณ 2567

- การจัดทำ Risk Appetite ,
- Risk Tolerance ,
- Trigger point ในการติดตามความเสี่ยงและปัจจัยเสี่ยง

work shop

- ข้อมูลจาก รายงานผล การดำเนินงานตามแผนบริหารความเสี่ยงประจำปีงบประมาณ 2567
- ความเสี่ยงอุบัติใหม่ (ปัจจัยเสี่ยงเปลี่ยนแปลงอย่างมีนัยสำคัญ)
- จัดทำแผนบริหารความเสี่ยงปี 2568