สรุปความรู้เรื่อง การบริหารความเสี่ยงองค์กร
(Organizational Risk Management)

1. แนวคิดและหลักการบริหารความเสี่ยง

Risk (ความเสี่ยง): เหตุการณ์ที่อาจเกิดขึ้นและส่งผลต่อการบรรลุวัตถุประสงค์ขององค์กร

Risk Management: กระบวนการจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ (ไม่จำเป็นต้องกำจัดหมด)

กระบวนการบริหารความเสี่ยง 4 ขั้นตอน:

- การระบุ (Identification)
- การประเมิน (Assessment)
- การจัดลำดับ (Prioritization)
- การวางมาตรการ (Mitigation & Control)

5 ความคาดหวังจากการบริหารความเสี่ยง:

1. สร้างคุณค่า
2. ลดความไม่แน่นอนและตอบสนองโอกาสได้รวดเร็ว
3. สนับสนุนการปรับปรุงบทบาทของธุรกิจ
4. เข้าใจกระบวนการบริหารความเสี่ยง
5. สร้างความได้เปรียบจากการบริหารองค์กร

2. กรอบบริหารความเสี่ยงสากล (International Framework)

2.1 Principle of COSO – ERM (2017)

1. การกำกับดูแลวัฒนธรรม (Governance and Culture)
    1. ควบคุมดูแลความเสี่ยงโดยคณะกรรมการ
    2. จัดตั้งโครงสร้างดำเนินงาน
    3. กำหนดวัฒนธรรมที่พึงประสงค์
    4. แสดงให้เห็นถึงการยึดมั่นต่อค่านิยมหลัก
    5. ดึงดูด พัฒนา และรักษาบุคคลที่มีความสามารถ
2. กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy and Objective-Setting)
    6. วิเคราะห์บริบททางธุรกิจ
    7. กำหนดระดับความเสี่ยงที่ยอมรับได้
    8. ประเมินทางเลือกทางเลือก
    9. กำหนดวัตถุประสงค์ที่สอดคล้องกับกลยุทธ์
3. ผลการปฏิบัติ (Performance)
    10. ระบุความเสี่ยง
    11. ประเมินความรุนแรงของความเสี่ยง
    12. จัดลำดับความสำคัญของความเสี่ยง

13. นำวิธีการตอบสนองความเสี่ยงไปปฏิบัติ
14. พัฒนาภาพรวมความเสี่ยง

4. การสอบทานและการแก้ไข (Review and Revision)
15. ประเมินการเปลี่ยนแปลงที่สำคัญ
16. ประเมินความเสี่ยงและผลการปฏิบัติงาน
17. ปรับปรุงกระบวนการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง

5. สารสนเทศ การสื่อสาร และการรายงาน (Information, Communication and Reporting)
18. ใช้ประโยชน์จากสารสนเทศและเทคโนโลยี
19. สื่อสารสารสนเทศด้านความเสี่ยง
20. รายงานความเสี่ยง วัฒนธรรม และผลการปฏิบัติงาน

2.2 ISO 31000 (International Standard for Risk Management)

จุดประสงค์หลัก:

- เพื่อช่วยให้องค์กรสามารถบรรลุวัตถุประสงค์
- ปรับปรุงการระบุ วิเคราะห์ ประเมิน ตอบสนอง และสื่อสารความเสี่ยง
- พัฒนาองค์กรให้สามารถตัดสินใจโดยอิงข้อมูลความเสี่ยงอย่างมีประสิทธิภาพ

โครงสร้างของ ISO 31000 แบ่งออกเป็น 3 ส่วนสำคัญ:

1. Principles (หลักการ) – 8 ข้อ

ISO 31000 กำหนดหลักการพื้นฐานที่การบริหารความเสี่ยงที่ดีควรมี เช่น:

1. สร้างคุณค่า
2. บูรณาการกับกิจกรรมขององค์กร
3. เป็นส่วนหนึ่งของกระบวนการตัดสินใจ
4. แสดงความโปร่งใสและชัดเจน
5. มีการปรับปรุงอย่างต่อเนื่อง
6. ต้องปรับให้เหมาะสมกับบริบทขององค์กร
7. ใช้ข้อมูลที่ถูกต้อง เชื่อถือได้
8. ต้องมีการปรับเปลี่ยนให้ทันต่อการเปลี่ยนแปลง

2. Framework (กรอบแนวทาง)

เป็นโครงสร้างที่ช่วยให้องค์กรฝังการบริหารความเสี่ยงไว้ในวัฒนธรรมและกิจกรรมต่าง ๆ ประกอบด้วย:

- การบูรณาการบริหารความเสี่ยงกับบริบทขององค์กร
- การกำหนดบทบาทหน้าที่ผู้เกี่ยวข้อง
- การจัดสรรทรัพยากร
- การสื่อสารภายใน
- การปรับปรุงframeworkอย่างต่อเนื่อง

3. Process (กระบวนการบริหารความเสี่ยง)

ขั้นตอนพื้นฐานของการบริหารความเสี่ยง:

1. การสื่อสารและการปรึกษาหารือ (Communication & Consultation)
2. การกำหนดบริบท (Establishing the Context)
3. การประเมินความเสี่ยง (Risk Assessment)
    - การระบุความเสี่ยง (Identification)
    - การวิเคราะห์ความเสี่ยง (Analysis)
    - การประเมินระดับความเสี่ยง (Evaluation)
4. การจัดการ/ตอบสนองความเสี่ยง (Risk Treatment)
5. การติดตามและทบทวน (Monitoring and Review)
6. การบันทึกและรายงาน (Recording and Reporting)

2.3 Integrated ERM Framework

คือ กรอบแนวคิดการบริหารความเสี่ยงเชิงบูรณาการ (Enterprise Risk Management - ERM) มีเป้าหมายเพื่อ ผสานการบริหารความเสี่ยงเข้ากับทุกกระบวนการ ขององค์กร ทั้งระดับกลยุทธ์และการปฏิบัติงาน

จุดเด่นของ Integrated ERM Framework:

1. เน้นการบูรณาการ (Integration):
    - ไม่แยกบริหารความเสี่ยงเป็นหน่วยงานเดี่ยว แต่ให้ทุกฝ่ายในองค์กรมีบทบาทร่วมกัน
    - ความเสี่ยงกลายเป็น “ส่วนหนึ่ง” ของการตัดสินใจทุกระดับ
2. สนับสนุนการบรรลุเป้าหมายขององค์กร:
    - ทำให้องค์กรมีความสามารถในการรับมือกับเหตุการณ์ที่ไม่แน่นอน
    - เปิดโอกาสให้มองเห็นโอกาสเชิงกลยุทธ์
3. ใช้ข้อมูลความเสี่ยงสนับสนุนการตัดสินใจ (Risk-Informed Decision):
    - ไม่ใช่แค่ลดความเสี่ยง แต่ใช้เป็น “ข้อมูลเชิงกลยุทธ์” เพื่อสร้างความได้เปรียบ
4. มีลักษณะหมุนเวียนและต่อเนื่อง (Cycle):
    - Risk Identification ⟶ Assessment ⟶ Treatment ⟶ Monitoring ⟶ Communication
    - ทุกขั้นตอนต้องมีการประเมินผล และปรับปรุงอย่างต่อเนื่อง

3. การระบุประเด็นความเสี่ยง (Risk Identification)

3.1 การระบุปัจจัยเสี่ยง

- วิเคราะห์สภาพแวดล้อมขององค์กรเพื่อตรวจจับความเสี่ยงที่อาจเกิดขึ้น
- ครอบคลุมทั้งปัจจัยภายในและภายนอก

3.2 เครื่องมือที่ใช้

- Internal Factor: ใช้ SWOT Analysis
- External Factor: ใช้ PESTEL Analysis
- What-if Analysis: วิเคราะห์สถานการณ์ที่ “ถ้าเกิดขึ้น” แล้วจะมีผลกระทบใดบ้าง
- พิจารณาความไม่แน่นอน (Uncertainty) และการเปลี่ยนแปลง (Change)

3.3 ประเภทของความเสี่ยง

1. Strategic Risk – ด้านกลยุทธ์/เป้าหมายองค์กร
2. Operational Risk – ด้านกระบวนการ/บุคลากร/เทคโนโลยี
3. Financial Risk – ด้านรายรับรายจ่าย
4. Compliance Risk – ด้านกฎหมาย/ข้อกำหนด
5. Severity – ระดับความรุนแรงของผลกระทบ

4. การประเมินระดับความเสี่ยง (Risk Assessment)

ใช้เครื่องมือ: Risk Register (ทะเบียนความเสี่ยง)

4.1 ทะเบียนความเสี่ยง (Risk Register)

- คือ “ฐานข้อมูล” ที่บันทึกรายการความเสี่ยงขององค์กร
- สำหรับแต่ละรายการความเสี่ยง จะมีข้อมูลดังนี้:
    - ชื่อความเสี่ยง (Risk Name)
    - ลักษณะความเสี่ยง (Description)
    - แหล่งที่มา (Source)
    - เจ้าของความเสี่ยง (Risk Owner)
    - การประเมินระดับความเสี่ยง (Risk Level)
    - มาตรการควบคุมที่มีอยู่ (Existing Control)
    - มาตรการตอบสนองที่เสนอ (Risk Response Plan)

4.2 วิธีการประเมินความเสี่ยง (Risk Level Evaluation)

ประเมิน 2 ปัจจัยหลัก:

1. โอกาสที่จะเกิด (Likelihood):
   เช่น: แทบไม่เกิดเลย / นาน ๆ ครั้ง / บ่อย / เกิดแน่นอน
   *กำหนดคะแนน 1–5
2. ระดับผลกระทบ (Impact or Severity):
   เช่น: กระทบเล็กน้อย / ปานกลาง / สูง / สูงมาก
   * กำหนดคะแนน 1–5
   *Risk Level = Likelihood × Impact

การประเมินความเสี่ยง

1.ประเมินโอกาสเกิด (Likelihood) และระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้น (Impact)

โอกาสเกิด (Likelihood : L)				
โอกาสเกิดน้อยมากหรือไม่น่าจะเกิดขึ้น	โอกาสเกิดน้อยหรืออาจจะเกิดขึ้นได้	โอกาสเกิดขึ้นปานกลางหรือเป็นไปได้ที่จะเกิดขึ้น	โอกาสเกิดขึ้นสูงหรือเป็นไปได้ที่จะเกิดขึ้นสูง	โอกาสเกิดสูงมากมากหรือมีความแน่นอนที่จะเกิดขึ้น
1 = น้อยมาก	**2 = น้อย**	**3 = ปานกลาง**	**4 = สูง**	**5 = สูงมาก**
ผลกระทบรุนแรงน้อยมากหรือมีความสำคัญน้อยมาก	ผลกระทบรุนแรงน้อยหรือมีความสำคัญน้อย	ผลกระทบรุนแรงปานกลางหรือมีความสำคัญปานกลาง	ผลกระทบรุนแรงสูงหรือมีความสำคัญมาก	ผลกระทบรุนแรงสูงมากหรือมีความสำคัญมากที่สุด
ผลกระทบ (Impact : I)				

2.ประเมินค่าระดับความเสี่ยง

ตารางค่าคะแนนระดับของความเสี่ยง

ผลกระทบ (Impact : I)					
5	M 1x5=5	H 2x5=10	E 3x5=15	E 4x5=20	E 5x5=25
4	M 1x4=4	H 2x4=8	H 3x4=12	E 4x4=16	E 5x4=20
3	L 1x3=3	M 2x3=6	H 3x3=9	H 4x3=12	E 5x3=15
2	L 1x2=2	M 2x2=4	M 3x2=6	H 4x2=8	H 5x2=10
1	L 1x1=1	L 2x1=2	L 3x1=3	M 4x1=4	M 5x1=5
	1	2	3	4	5
		โอกาสเกิด (Likelihood : L)			

ตารางเกณฑ์ระดับความเสี่ยงและแนวทางการดำเนินการตามระดับความเสี่ยง

ระดับความเสี่ยง	ค่าช่วงคะแนน	สัญลักษณ์ระดับความเสี่ยง	มาตรการจัดการ
ระดับความเสี่ยงต่ำ (Low : L)	1-3	L	ระดับความเสี่ยงที่ยอมรับได้โดยไม่ต้องมาการควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม
ระดับความเสี่ยงปานกลาง (Medium : M)	4-7	M	ระดับความเสี่ยงที่พอยอมรับได้ แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
ระดับความเสี่ยงสูง (High : H)	8-14	H	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้โดยต้องมีการควบคุมและติดตามอย่างใกล้ชิด เพื่อให้ความเสี่ยงลดลงและป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับสูงมาก
ระดับความเสี่ยงสูงมาก (Extreme : E)	15-25	E	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ระดับที่ยอมรับได้ทันที (ต้องทำแผนการบริหารความเสี่ยง)

โดยพิจารณาประเมินความเสี่ยงจากตารางเกณฑ์ระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) และระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้น (Impact) ดังนี้

4.3 การใช้เครื่องมือช่วยประเมิน

- Risk Matrix (ตารางประเมินความเสี่ยง):
  ตาราง 5×5 หรือ 4×4 ที่แสดงความรุนแรงของความเสี่ยงด้วยสี:
  - เขียว = ต่ำ
  - เหลือง = ปานกลาง
  - แดง = สูง
- Heat Map:
  แสดงความเสี่ยงทั้งหมดเป็นจุด ๆ บนแผนที่สีเพื่อให้เห็นภาพรวมในองค์กร

5. การออกแบบมาตรการป้องกันและควบคุมความเสี่ยง (Risk Mitigation and Control)

คือการออกแบบแผนจัดการความเสี่ยงให้อยู่ในระดับที่องค์กร “ยอมรับได้” ทั้งในมุมของการ ลดโอกาสการเกิด และ ลดผลกระทบของความเสี่ยง

มาตรการตอบสนองความเสี่ยง 4Ts **ประกอบด้วย:**

1. Take (ยอมรับ)
   - ยอมรับความเสี่ยงในระดับที่องค์กรรับได้
   - ไม่ต้องดำเนินการใด ๆ เพิ่มเติม
   - เหมาะกับกรณีที่ความเสี่ยงมีน้อย หรือยอมรับได้เทียบกับโอกาส
2. Treat (ลด)
   - ดำเนินมาตรการเพื่อ ลดโอกาสเกิด หรือ ลดผลกระทบ ของความเสี่ยง
   - เช่น ปรับกระบวนการ, ฝึกอบรม, ใช้ระบบควบคุมภายใน
3. Transfer (โอนย้าย)
   - โอนความเสี่ยงบางส่วนให้ผู้อื่นรับผิดชอบ
   - เช่น การทำประกันภัย, การจ้างผู้รับเหมา หรือพันธมิตรธุรกิจ
4. Terminate (หลีกเลี่ยง)
   - ยุติหรืองดกิจกรรมที่มีความเสี่ยง
   - ใช้เฉพาะในกรณีที่ ไม่สามารถยอมรับหรือควบคุมได้เลย
   - ต้องพิจารณาว่าจะกระทบต่อการบรรลุวัตถุประสงค์หรือไม่

6. การสื่อสารและการรายงานความเสี่ยง(Risk Communication and Reporting)

6.1 Integrated ERM Framework

- ความเสี่ยงต้องไม่ใช่เรื่องของหน่วยใดหน่วยหนึ่ง แต่เป็นหน้าที่ของทุกคนในองค์กร
- ต้องมีระบบที่บูรณาการการสื่อสารและการรายงานผลอย่างต่อเนื่อง

6.2 สารสนเทศเพื่อการบริหารความเสี่ยง

- ข้อมูลความเสี่ยงต้อง ทันเวลา, ถูกต้อง, ครบถ้วน และสื่อสารได้เข้าใจง่าย
- ตัวอย่าง:
  - Heat Map
  - Dashboard
  - แผนภูมิแสดงสถานะความเสี่ยง

6.3 เทคโนโลยีสนับสนุนการบริหารความเสี่ยง

- เช่น ระบบ **URM Beyond** (จุฬาฯ) ใช้ในการบันทึก วิเคราะห์ และสื่อสารข้อมูลความเสี่ยงแบบออนไลน์

6.4 การรายงานผล

- รายงานผลควรครอบคลุม:
  - ระดับความเสี่ยง
  - แผนรับมือ
  - ความคืบหน้า
  - ปัญหาและข้อเสนอแนะ
- ควรรายงานต่อผู้บริหาร/คณะกรรมการความเสี่ยงเป็นประจำ

7. การบริหารความเสี่ยงเชิงองค์กร และการปรับปรุงอย่างต่อเนื่อง (*Organizational Risk Management Implementation & Continuous Improvement*)

หลักการควบคุมความเสี่ยงแบบ 3 ด่าน (Three Lines of Defense) อ้างอิงจาก The Institute of Internal Auditors (IIA)

ด่านที่ 1 ผู้รับผิดชอบระดับที่ 1 (15t Line of Defense) คือ หน่วยงานต่าง ๆ ในองค์กร (Business Lines) มีหน้าที่ดูแลงานในความรับผิดชอบและระบบการควบคุมภายในให้เป็นไปตามแนวทางหรือกรอบที่กำหนดไว้

ด่านที่ 2 ผู้รับผิดชอบระดับที่ 2 (2nd Line of Defense) คือ หน่วยงานที่ดูแลให้มีการปฏิบัติตามกฎเกณฑ์ (Compliance) การตรวจสอบและควบคุมคุณภาพ (Inspection and Quality Assurance) การบริหารความเสี่ยง (Risk Management)

ด่านที่ 3 ผู้รับผิดชอบระดับที่ 3 (3rd Line of Defense) คือ หน่วยงานตรวจสอบภายใน (Internal Audit) มีหน้าที่ประเมินความเพียงพอของระบบการควบคุมภายในขององค์กร ให้ข้อเสนอแนะ การปรับปรุงและพัฒนาโดยรายงานต่อฝ่ายจัดการ

การควบคุมความเสี่ยงทั้ง 3 ด่าน ช่วยให้องค์กรมีระบบป้องกันที่รัดกุม ลดความเสียหาย และรับมือกับเหตุไม่คาดคิดได้ดี ในยุคที่โลกเปลี่ยนแปลงเร็ว องค์กรควรมองความเสี่ยงเป็นโอกาส ไม่ใช่อุปสรรค กล้ารับความเสี่ยงอย่างรอบคอบ เช่น การนำนวัตกรรมมาใช้ เพื่อขับเคลื่อนองค์กรให้เติบโตอย่างมั่นคงและยั่งยืน

****

ผู้บันทึกบทเรียน นางสาวพลอยชมพู ณ ปานแก้ว หน่วยยุทธศาสตร์และพัฒนาองค์กร
ผู้ตรวจทานบทเรียน นางสาวกนกวรรณ สุวรรณรัตน์ หน่วยยุทธศาสตร์และพัฒนาองค์กร