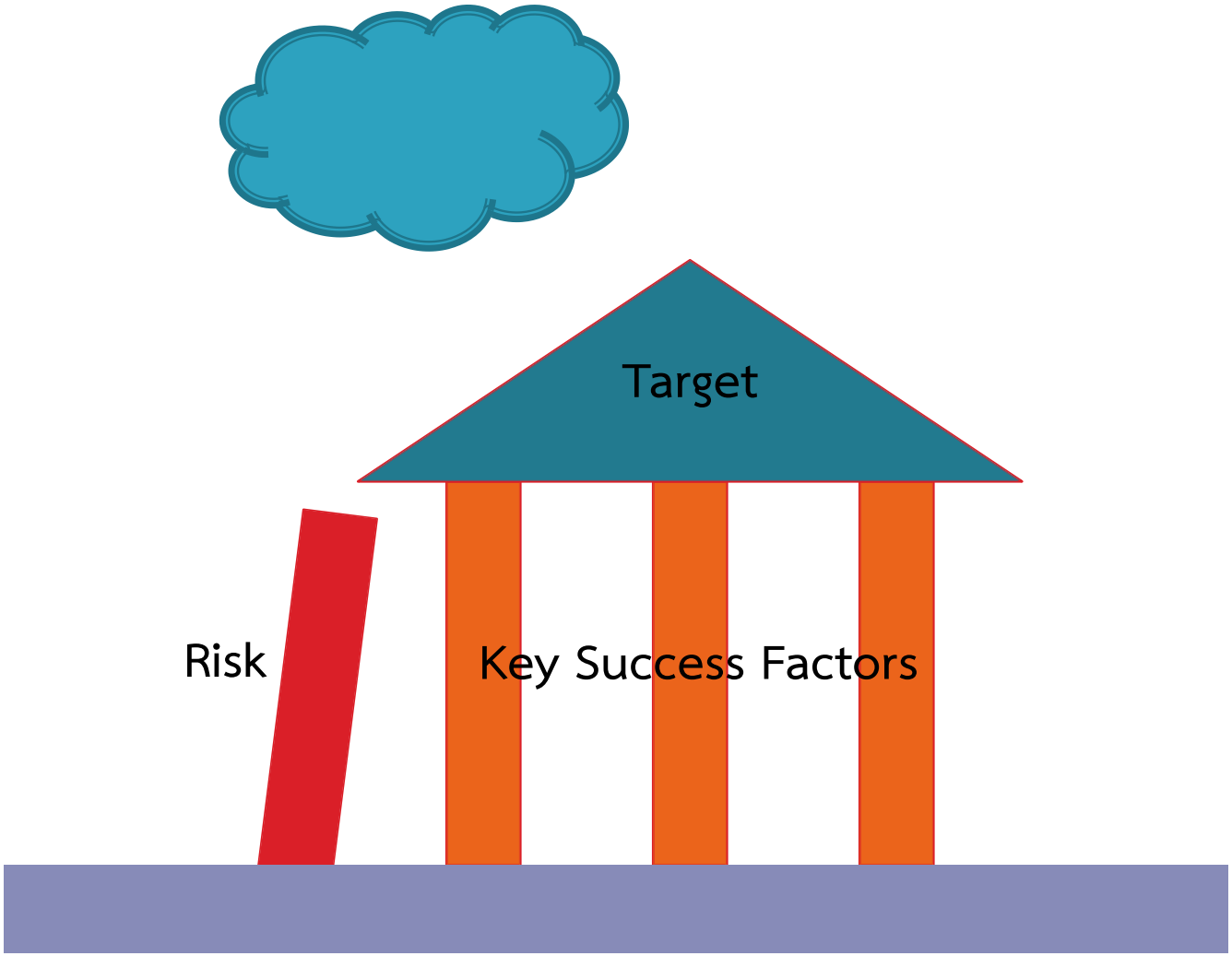
IT Risk Management (Workshop)

ดร. ธนัญชัย ตรีภาค

ความเสี่ยงคืออะไร ?

“ความเสี่ยง” ในมุมมองของเรา มันคืออะไร


Target
Risk
Key Success Factors

ความเสี่ยง กับ ปัญหา แตกต่างกันอย่างไร ?

เรามีความเสี่ยงอะไรกันบ้าง ?

เรารับมือกับความเสี่ยงกันอย่างไร ?

Our IT System

- ให้นักศึกษากำหนดรายละเอียดของระบบสารสนเทศที่ตนเองเป็นผู้ดูแลระบบ
  - ระบบสารสนเทศ มีขอบเขตการทำงานอย่างไร
  - ผู้ใช้งานระบบ
  - ฟังก์ชั่นต่างๆ
  - ผลลัพธ์ที่ต้องการของระบบ
- เขียน Network Diagram
- ระบุเป้าหมาย / Service Level Agreement ของการให้บริการระบบสารสนเทศ
- ระบุปัญหาที่เคยเกิดขึ้นในอดีตของระบบ พร้อมผลกระทบ

ความเสี่ยงของระบบสารสนเทศมีอะไรบ้าง ?

ความเสี่ยงระบบสารสนเทศ
กับ
ภัยคุกคามสารสนเทศ
แตกต่างกันอย่างไร

กระบวนการบริหารความเสี่ยง ตามมาตรฐาน COSO

(Committee of Sponsoring Organization of the Tread way Commission)

- 1. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
- 2. การระบุความเสี่ยงต่างๆ (Event Identification)
- 3. การประเมินความเสี่ยง (Risk Assessment)
- 4. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
- 5. กิจกรรมการบริหารความเสี่ยง (Control Activities)
- 6. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
- 7. การติดตามผลและเฝ้าระวังความเสี่ยงต่างๆ (Monitoring)

1. เรามีเป้าหมายในการบริหารความเสี่ยงคืออะไร

2. การระบุความเสี่ยงควรมีรายละเอียดอะไรบ้าง

รายละเอียดความเสี่ยง (ตาราง)

- ชื่อความเสี่ยง
- ประเภทความเสี่ยง
  - ความเสี่ยงทางเทคนิค
  - ความเสี่ยงจากผู้ปฏิบัติงาน
  - ความเสี่ยงจากภัยพิบัติหรือเหตุฉุกเฉิน
  - ความเสี่ยงจากการบริหารจัดการ
  - ฯลฯ

- รายละเอียดความเสี่ยง
- ปัจจัยเสี่ยง/สิ่งคุกคาม
- ผลกระทบ/ผู้รับผลกระทบ

ให้นักศึกษาเขียน
(1) ตารางรายละเอียด
ความเสี่ยง 5 ความเสี่ยง

3. การประเมินความเสี่ยง

- กำหนดรายละเอียดเกี่ยวกับโอกาสการเกิดเหตุ และ ระดับความรุนแรง ของแต่ละความเสี่ยง (บางความเสี่ยงสามารถใช้ตารางเดียวกันได้)
  - ระบุโอกาส 5 ระดับ
  - ระบุระดับความรุนแรง 5 ระดับ
- ใช้ Scenario Analysis เพื่อให้สามารถระบุความรุนแรงได้แม่นยำมากขึ้น

ให้นักศึกษาเขียน

(2) ตารางโอกาส

(3) ตารางความรุนแรง

และ

(4) ตารางประเมินความเสี่ยง

โอกาสการเกิดความเสี่ยง

ระดับของโอกาส	รายละเอียด
5	เกิดบ่อยมาก หมายถึงอะไร .. กำหนดรายละเอียด
4	
3	
2	
1	เกิดน้อยมาก หมายถึงอะไร .. กำหนดรายละเอียด

ความรุนแรงของความเสี่ยง

ระดับความรุนแรง	รายละเอียด
5	ผลกระทบสูงมาก .. หมายถึงอะไร กำหนดรายละเอียด
4	
3	
2	
1	ผลกระทบน้อยมาก .. หมายถึงอะไร กำหนดรายละเอียด

ผลลัพธ์ของการประเมินความเสี่ยง

No.	ความเสี่ยง	โอกาส	ความรุนแรง

ให้นักศึกษาเขียน

(5) Risk Map

Risk Map

5				#4,#5	High Risk
4					#3
3	#1		#2		
2				#6	
1	Low Risk				#7
โอกาส /ความรุนแรง	1	2	3	4	5

กำหนดระดับความเสี่ยง

No.	ความเสี่ยง	โอกาส	ความรุนแรง	ระดับความเสี่ยง
???	???	A	B	A x B

A x B
<= 9

ให้นักศึกษาเขียน

(6) ตารางระดับความเสี่ยง

4. กลยุทธที่ใช้ในการจัดการความเสี่ยง

- หลีกเลี่ยง – วางแผน ดำเนินการเพื่อไม่ให้ความเสี่ยงเกิดขึ้น
- ถ่ายโอน – วางแผน ดำเนินการเพื่อถ่ายโอนไปยังหน่วยงานอื่นๆ
- ลด – วางแผน ดำเนินการเพื่อลดความรุนแรง/โอกาส
- ยอมรับ – ยอมให้ความเสี่ยงดังกล่าวคงอยู่ในระบบได้ อาจไม่มีการดำเนินการอะไร แต่ต้องตรวจสอบว่าความเสี่ยงดังกล่าวยังคงอยู่ในขอบเขตที่ยอมรับอยู่หรือไม่

5. กิจกรรมการบริหารความเสี่ยง (Action Plan)

- ชื่องาน/กิจกรรม
- รายละเอียดกิจกรรม
- ผลที่คาดหวัง
- งบประมาณ
- ผู้รับผิดชอบ
- ระยะเวลาดำเนินการ

ให้นักศึกษาเขียน

(7) กิจกรรมบริหารความเสี่ยง

หลังกิจกรรมบริหารความเสี่ยงแล้ว ความเสี่ยงควรเป็นอย่างไร

6.ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง

ข้อมูลสำคัญในการบริหารความเสี่ยงคืออะไร จะสื่อสารให้ทราบโดยทั่วถึงได้อย่างไร

7.การติดตามและเฝ้าระวัง

กิจกรรมในการติดตามและเฝ้าระวัง มีอะไรบ้าง

สรุป / บทเรียน