บทที่ 2 กระบวนการรักษาความปลอดภัย

ความเสี่ยง

นโยบาย

การติดตั้งระบบรักษาความปลอดภัย

ความเสี่ยง(Risk)

- **การเสี่ยงหมายถึง “โอกาสหรือเหตุการณ์ที่ไม่พึงประสงค์ที่จะทำให้เราไม่บรรลุวัตถุประสงค์”**
- **ความเสี่ยง คือ สิ่งต่าง ๆที่อาจกีดกันองค์กรจากการบรรลุวัตถุประสงค์/เป้าหมาย**
- **ความเสี่ยงทำให้เราไม่บรรลุวัตถุประสงค์**
  - วัตถุประสงค์ที่เรากำลังทำเป็นประจำ(Operational Risk)
  - ทางด้านยุทธศาสตร์ (Strategy)
  - ทางด้านการแข่งขัน (Competitive)

ปัจจัยเสี่ยง(Risk Factor)

- หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การควบคุม(Control

- **หมายถึง นโยบาย แนวทาง หรือขั้นตอนปฏิบัติต่างๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ**

  - การควบคุมเพื่อการป้องกัน
  - การควบคุมเพื่อให้ตรวจพบ
  - การควบคุมโดยการชี้แนะ
  - การควบคุมเพื่อการแก้ไข

แนวคิดการบริหารความเสี่ยง

COSO

- ปัจจัยภายในองค์กร
- การตั้งวัตถุประสงค์
- การระบุเหตุการณ์หรือปัญหาที่จะเกิดขึ้น
- การประเมินความเสี่ยง
- การตอบสนองความเสี่ยง
- กิจกรรมของการควบคุม
- การสื่อสารและการส่งข้อมูลที่สำคัญและจำเป็น
- การตรวจติดตามการดำเนินงาน

FMEA

- กำหนดกระบวนการที่จะทำ FMEA
- ระบุขั้นตอนของแต่ละกระบวนการ
- ระดมความคิดเห็นเพื่อคาดหมายลักษณะข้อบกพร่อง
- ประเมินผลกระทบจากลักษณะข้อบกพร่อง
- กำหนดเกณฑ์ประเมินตัวเลขความเสี่ยงชี้นำ (RPN)
- คำนวณค่า RPN และจัดลำดับความสำคัญตามค่า RPN
- วางมาตรการเพื่อปรับปรุงและควบคุมกระบวนการ
- การสื่อสารและทำความเข้าใจทั่วทั้งองค์กร
- การตรวจติดตามการดำเนินการตามมาตรการ
- ทบทวนค่า RPN หลังการดำเนินการตามมาตรการ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

- <u>ความเสี่ยงด้านเทคโนโลยีสารสนเทศ</u> เป็นการวางระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ เพื่อกำจัด ป้องกันหรือลดการเกิดความเสียหาย โดยสามารถฟื้นฟูระบบสารสนเทศ และการสำรองและการกู้คืนข้อมูลจากความเสียหาย มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ มีระบบรักษาความมั่นคงและปลอดภัยของระบบฐานข้อมูล และมีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ

การประเมินความเสี่ยง (Risk Assessment)

- **หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็นระดับ**

การบริหารความเสี่ยง (Risk Management)

- **หมายถึง กระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง**

ขั้นตอนการบริหารความเสี่ยง

- **ขั้นตอนการบริหารความเสี่ยงอย่างง่าย 5 ข้อ ได้แก่**
  - การกำหนดวัตถุประสงค์ (Objective Establishment)
  - การระบุความเสี่ยง (Risk Identification)
  - การประเมินความเสี่ยง(Risk Assessment)
  - การสร้างแผนจัดการ(Risk Management Planning)
  - การติดตามสอบทาน (Monitoring & Review)

ปัจจัยการบริหารความเสี่ยง

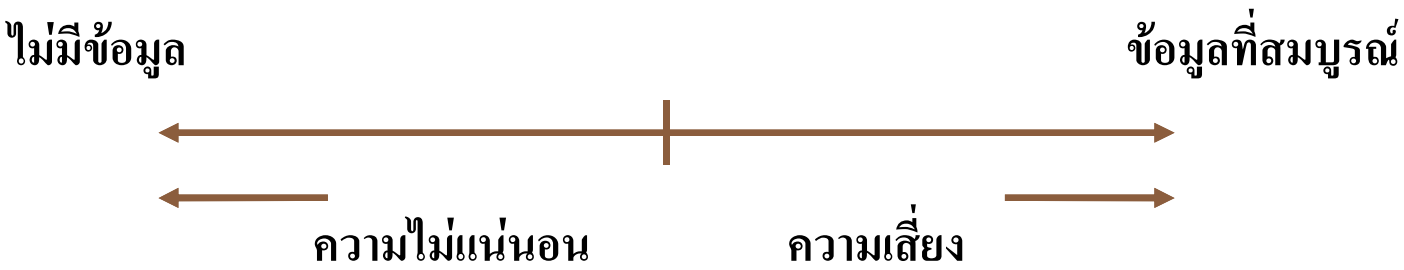
- **การบริหารความเสี่ยงเริ่มจาก..**
  - การกำหนดเหตุไม่พึงประสงค์ เหตุที่ไม่พึงประสงค์ที่ไม่ทำให้เรากระตือรือร้น
    - น้ำท่วม เกิดอุบัติเหตุกลางคัน รถเสีย ฝนตก
  - ความเสี่ยงระดับนี้ไม่เอามา Treat เป็นความเสี่ยงที่ไม่ควรควบคุม ก็ไม่ต้องทำแผนรับมือฝนตก
  - ถามตัวเองก่อนว่า เรายอมรับความจริงได้หรือไม่
  - มีความเสี่ยงอะไรที่ควบคุมได้

คำถามความเสี่ยง

- Q1 ท่านมีความฝัน ความหวังอะไรที่ต้องบรรลุให้ได้ยู่บ้างหรือไม่
- Q2 ท่านมีความกังวลใจอะไรบ้าง อุปสรรคที่จะทำให้ท่านไม่บรรลุความสำเร็จที่ตั้งไว้
- Q3 ท่านได้เตรียมการณ์ใดเพื่อป้องกัน
- Q4 ท่านคิดว่าการเตรียมการเหล่านั้นถ้ามีสิ่งที่เล็ดลอดได้จะน่ากังวลใจเพียงใด
- Q5 ท่านจะทราบได้อย่างไรว่า เหตุการณ์ ปัญหา อุปสรรค จำนวนมากนั้น ควรจะนำสิ่งใดมาพิจารณา
- Q6 ท่านคิดว่าจำเป็นต้องมีแนวทาง วิธีการ เพิ่มเติมในการรับมือ เหตุการณ์หรือผลที่เล็ดลอดมา อีกหรือไม่ อย่างไร
- Q7 ท่านจะทราบได้อย่างไรว่า เหตุการณ์นั้นได้เกิด หรือมีแนวโน้มที่จะเกิดมากน้อยหรือไม่เพียงไร

ความเสี่ยงและความไม่แน่นอน

ความเสี่ยงและความไม่แน่นอนตามปริมาณข้อมูลความสูญเสีย

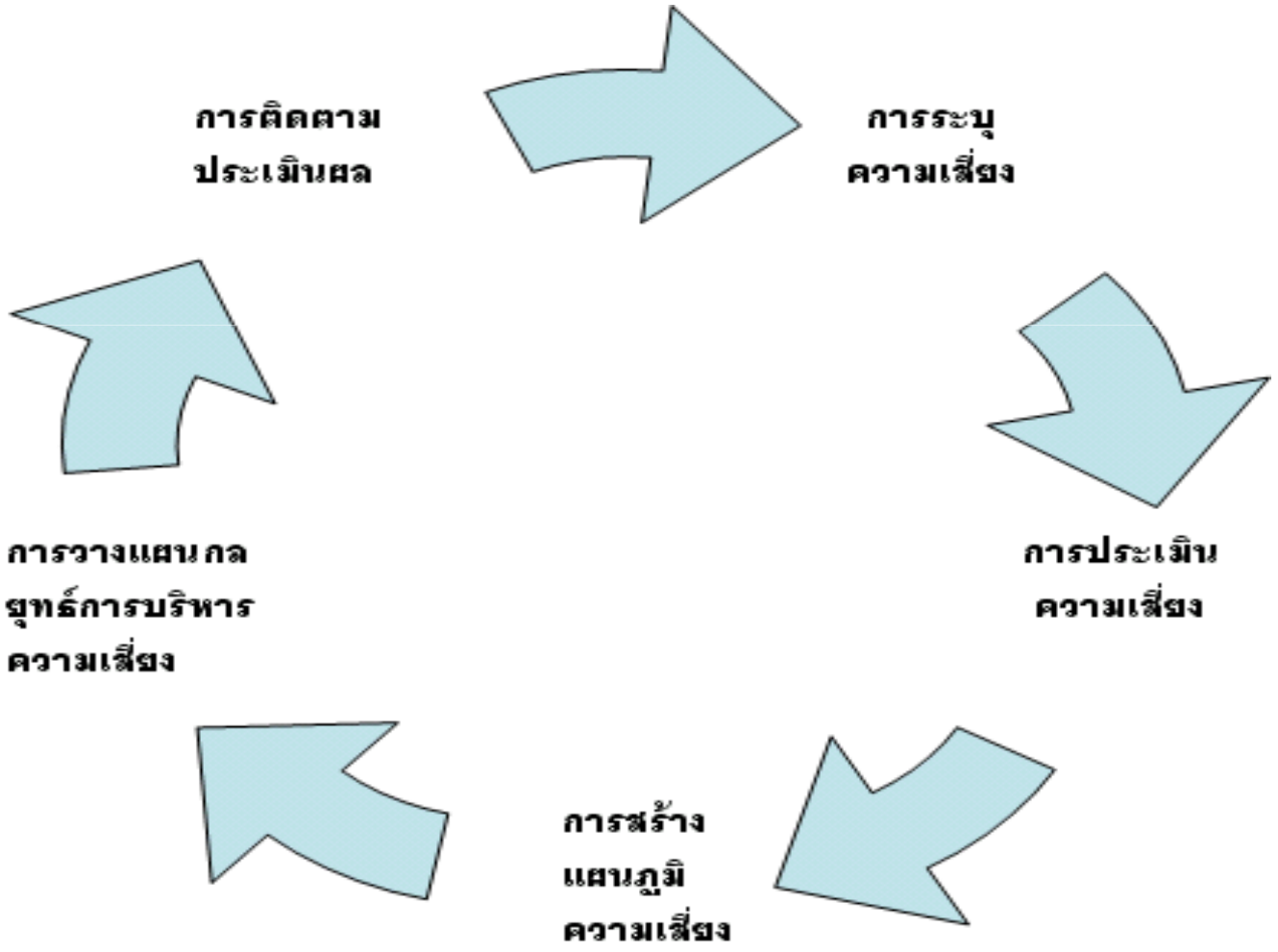


ภัย vs อันตราย

ศัพท์อีกสองคำที่เกี่ยวข้องกับคำว่า “ความเสี่ยง” (risk) คือ คำว่า “ภัย” (peril) และ “อันตราย” (hazard)

- **“ภัย”** หมายถึง สาเหตุของความสูญเสีย เช่น ถ้ากล่าวถึงไฟไหม้อาคาร ตัวภัย หมายถึง ไฟ ฉะนั้นสิ่งที่เป็นภัยพื้นฐาน ได้แก่ ไฟ ฟ้าผ่า พายุไต้ฝุ่น แผ่นดินไหว เป็นต้น
- **“อันตราย”** มีความหมายกว่างกว่าคำว่า “ภัย” กล่าวคือ “อันตราย” เป็นสภาวะที่สร้างหรือเสริมโอกาสที่ความไม่แน่นอนจะนำไปสู่ความสูญเสีย

การบริหารความเสี่ยง



วิธีการบริหารความเสี่ยง

- วิธีการบริหารความเสี่ยงสามารถสรุปได้เป็น 4 วิธีการหลักดังนี้
  - การหลีกเลี่ยงความเสี่ยง
  - การควบคุมความสูญเสีย
  - การรับความเสี่ยงไว้เอง
  - การถ่ายโอนความเสี่ยง

การวิเคราะห์ความเสี่ยง

- **โดยทั่วไปการแจกแจงของตัวแปรสุ่มความสูญเสียที่เราสามารถนำไปใช้ในการวิเคราะห์ความเสี่ยงมีอยู่ 2 ประเภทคือ**

  - การแจกแจงความถี่ของตัวแปรสุ่มความสูญเสีย
  - การแจกแจงความรุนแรงของตัวแปรสุ่มความสูญเสีย

แผนภูมิการประเมินความเสี่ยง

- การให้คะแนนระดับความถี่ที่เหตุการณ์จะเกิดเป็น 1 .. 5
- การให้คะแนนความรุนแรงเมื่อเหตุนั้นเกิดเป็น 1 .. 5
- นำคะแนนคูณกันจะได้ค่าผลกระทบที่เกิดต่อระบบ

Severity \ Frequency	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

การประเมิน : โอกาส

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ (Likelihood) เชิงปริมาณ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	1 เดือนต่อครั้งหรือมากกว่า
4	สูง	1-6 เดือนต่อครั้งแต่ไม่เกิน 5 ครั้ง
3	ปานกลาง	1 ปีต่อครั้ง
2	น้อย	2 - 4 ปีต่อครั้ง
1	น้อยมาก	5 ปีต่อครั้ง

การประเมิน : ผลกระทบ

ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) เชิงปริมาณ		
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	> 1 ล้านบาท
4	สูง	> 2.5 แสนบาท – 1 ล้านบาท
3	ปานกลาง	> 50,000 – 2.5 แสนบาท
2	น้อย	> 10,000 – 50,000 บาท
1	น้อยมาก	ไม่เกิน 10,000 บาท

การประเมิน : ผลกระทบด้าน IT

ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) ต่อระบบเทคโนโลยีสารสนเทศ		
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ
4	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
2	น้อย	เกิดเหตุที่แก้ไขได้
1	น้อยมาก	เกิดเหตุที่ไม่มีความสำคัญ

การประเมิน : ผลด้านการทำงาน

ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) ต่อการดำเนินงาน		
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	มีผลกระทบต่อกระบวนการและการดำเนินงานรุนแรงมาก เช่น หยุดดำเนินการมากกว่า 1 เดือน
4	สูง	มีผลกระทบต่อกระบวนการและการดำเนินงานรุนแรง เช่น หยุดดำเนินการ 1 เดือน
3	ปานกลาง	มีการชะงักงันอย่างมีนัยสำคัญของกระบวนการและการดำเนินงาน
2	น้อย	มีผลกระทบเล็กน้อยต่อกระบวนการและการดำเนินงาน
1	น้อยมาก	ไม่มีการชะงักงันของกระบวนการและการดำเนินงาน

ตัวอย่าง

ชื่อปัจจัยเสี่ยง: โปรแกรมสำเร็จรูปที่ใช้ปฏิบัติงานไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	
ปัจจัยภายใน	ประเภท: ความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ผลกระทบ: - ไม่สามารถอัพเดทข้อมูลหรือฟังก์ชันการใช้งานต่าง ๆ ให้เป็นปัจจุบันได้ - ไม่สามารถใช้งานโปรแกรมได้เต็มประสิทธิภาพ	
แนวทางตอบสนอง: - วางแผนการจัดหาโปรแกรมสำเร็จรูปที่ลิขสิทธิ์ถูกต้องตามกฎหมาย	
กิจกรรมตามแผนปฏิบัติการ: 1. จัดทำแผนการจัดหาโปรแกรมสำเร็จรูปที่ลิขสิทธิ์ถูกต้องตามกฎหมาย 2. จัดหาโปรแกรมสำเร็จรูปที่ลิขสิทธิ์ถูกต้องตามกฎหมาย	

ตัวอย่าง

ชื่อปัจจัยเสี่ยง: ข้อมูลสารสนเทศไม่ถูกต้องครบถ้วนและไม่สามารถใช้งานได้อย่างต่อเนื่อง

ปัจจัยภายใน	ประเภท: ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ผลกระทบ:

- การปฏิบัติงานล่าช้าหรือหยุดชะงัก

แนวทางตอบสนอง:

- จัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
- ควบคุมการเข้าออกห้องแม่ข่ายและการป้องกันความเสียหาย
- จัดทำแผนการสำรองและกู้คืนข้อมูลสารสนเทศ

กิจกรรมตามแผนปฏิบัติการ:

1. จัดทำประกาศและระเบียบ สป.กษ.
2. จัดหาระบบควบคุมการเปิด-ปิดประตูห้องแม่ข่ายอัตโนมัติ (Access Control System)
3. จัดหาระบบกล้องโทรทัศน์วงจรปิด (CCTV System)
4. จัดทำแผนการสำรองและกู้คืนข้อมูลสารสนเทศ

ตัวอย่าง

ชื่อปัจจัยเสี่ยง: ระบบคอมพิวเตอร์และเครือข่ายไม่สามารถใช้งานได้อย่างต่อเนื่อง

ปัจจัยภายนอก | **ประเภท: ความเสี่ยงด้านเทคโนโลยีสารสนเทศ**

ผลกระทบ:

- ทุกหน่วยงานที่ต่อเชื่อมไม่สามารถทำงานผ่านระบบการทำงานได้
- ผู้บริหารและผู้ปฏิบัติงานไม่สามารถติดต่อสื่อสารผ่านอินเตอร์เน็ตได้
- ผู้รับบริการและผู้ต้องการรับบริการข้อมูลข่าวสารของกระทรวงไม่สามารถได้รับบริการและข้อมูลข่าวสาร

แนวทางตอบสนอง:

- กำหนดสิทธิในการเข้าถึงเครือข่ายและติดตามเฝ้าดูการใช้เครือข่ายทั้งภายในและภายนอก
- จัดทำมาตรการรักษาความปลอดภัยของระบบเครือข่าย
- จัดทำแผนการบริหารงานต่อเนื่องในภาวะวิกฤต IT Continuity Plan)

กิจกรรมตามแผนปฏิบัติการ:

1. จัดทำระบบกำหนดสิทธิในการเข้าถึงเครือข่ายและระบบติดตาม เฝ้าดูการใช้เครือข่ายทั้งภายในและภายนอก
2. กำหนดมาตรการป้องกันไวรัสและการบุกรุกโจมตีที่มีประสิทธิภาพสำหรับเครื่องคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่อกับระบบเครือข่าย
3. จัดหาระบบสำรอง (Cool Site) และทำการจ้าง Outsource ในการบริหารความเสี่ยง

ตัวอย่าง

ชื่อปัจจัยเสี่ยง: สิ่งแวดล้อมและภัยพิบัติ

ปัจจัยภายนอก	ประเภท: ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ผลกระทบ:

- ข้อมูลสารสนเทศ ระบบคอมพิวเตอร์และเครือข่ายเกิดความเสียหาย

แนวทางตอบสนอง:

- จัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan)
- ปรับปรุงห้องคอมพิวเตอร์แม่ข่าย

กิจกรรมตามแผนปฏิบัติการ:

1. จัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan)
2. จัดหาอุปกรณ์วัดอุณหภูมิและความชื้น
3. จัดทำระบบป้องกันสัตว์กัดแทะสายไฟฟ้าและสายสัญญาณ
4. จัดทำระบบบริหารสายสัญญาณโดยจัดทำพื้นยกสำเร็จรูป