Contingency Planning

MS1 Thanin Muangpool

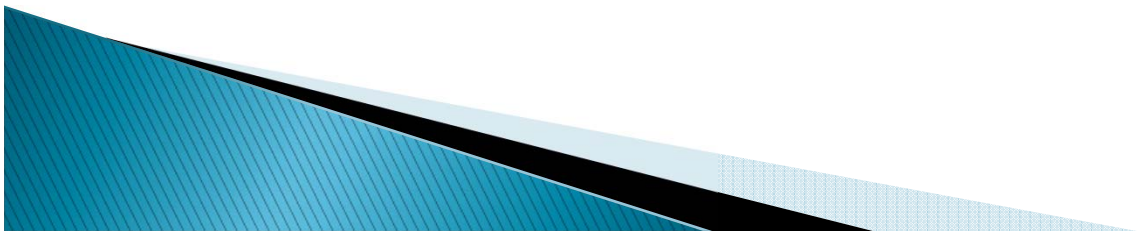
คุณลักษณะพิเศษของการจัดการความมั่นคงปลอดภัย

เพื่อให้การจัดการความมั่นคงปลอดภัยของสารสนเทศดำเนินการอย่างเป็นระบบ องค์กรสามารถใช้ มาตรฐานความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC17799 เป็นกรอบในการทำงานได้ มี 6 ด้าน ดังนี้

- **Planning** การวางแผน
- **Policy** การกำหนดนโยบาย
- **Program** หมายถึงโครงการต่าง ๆ ที่จัดทำขึ้น
- **Protection** การกำหนดมาตรการป้องกัน
- **People** บุคลากร
- **Project Management** การบริหารโครงการ

การวางแผนรับสถานการณ์ฉุกเฉินและภัยพิบัติ

- **การวางแผนรับสถานการณ์ฉุกเฉินและภัยพิบัติ (Contingency Planning)** คือกระบวนการที่ฝ่ายเทคโนโลยีสารสนเทศและฝ่ายความมั่นคงปลอดภัยของสารสนเทศ ร่วมกันเตรียมการตรวจหา โต้ตอบและฟื้นฟูระบบจากเหตุการณ์ที่เป็นภัยคุกคามทั้งจากมนุษย์และภัยธรรมชาติที่มีต่อความมั่นคงปลอดภัยของทรัพยากรสารสนเทศและทรัพย์สินที่เกี่ยวข้อง



การวางแผนรับสถานการณ์ฉุกเฉินและภัยพิบัติ

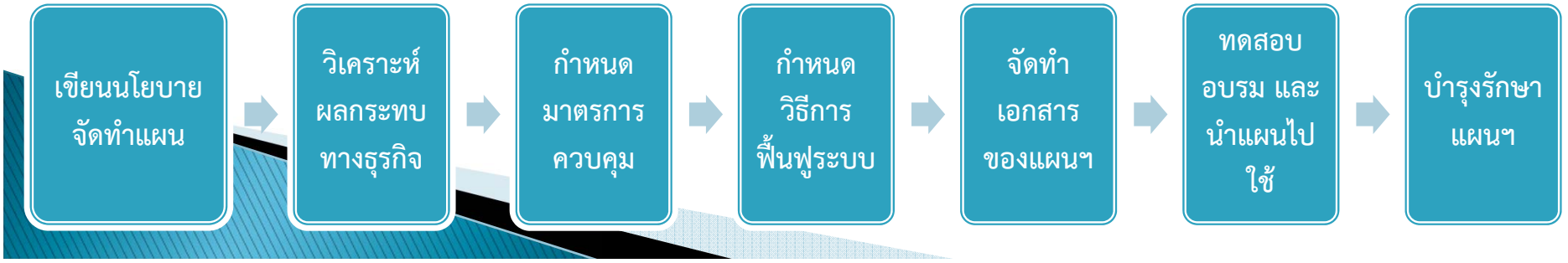
ประกอบด้วย 4 แผนงานคือ

- การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis)
- แผนรับมือเหตุการณ์ไม่คาดคิด (Incident Response Plan)
- แผนฟื้นฟูจากความเสียหาย (Disaster Recovery Plan)
- แผนดำเนินธุรกิจอย่างต่อเนื่องในสถานการณ์คับขัน (Business continuity)

ทั้ง 4 แผนงานจะต้องมีทีมงานที่รับผิดชอบในการดำเนินการจัดทำแผนงานโดยเฉพาะ เรียกว่า **Contingency Planning Management Team : CPMT**

กระบวนการวางแผนรับสถานการณ์ฉุกเฉินและภัยพิบัติ

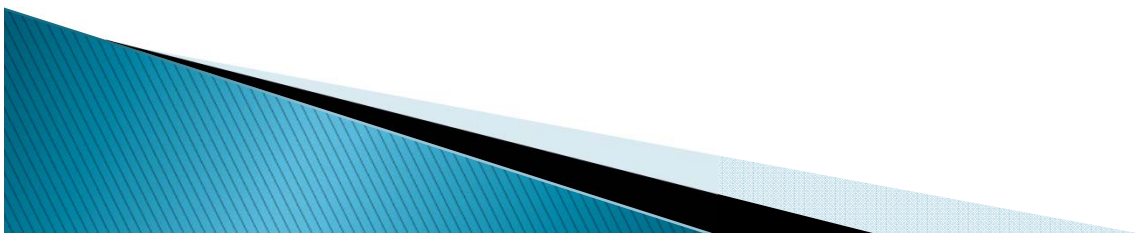
1. เขียนนโยบายจัดทำแผนรับมือสถานการณ์ฉุกเฉินและภัยพิบัติ
2. วิเคราะห์ผลกระทบทางธุรกิจ
3. ระบุมาตรการควบคุมเพื่อป้องกัน เพื่อลดผลกระทบที่อาจจะเกิดขึ้น
4. กำหนดกลยุทธ์การฟื้นฟูระบบ
5. จัดทำแผนรับสถานการณ์ฉุกเฉินและภัยพิบัติ
6. ทดสอบ ฝึกอบรม และนำแผนไปใช้
7. บำรุงรักษาแผน ทบทวนและปรับปรุงข้อมูลในแผนงานให้เป็นปัจจุบัน



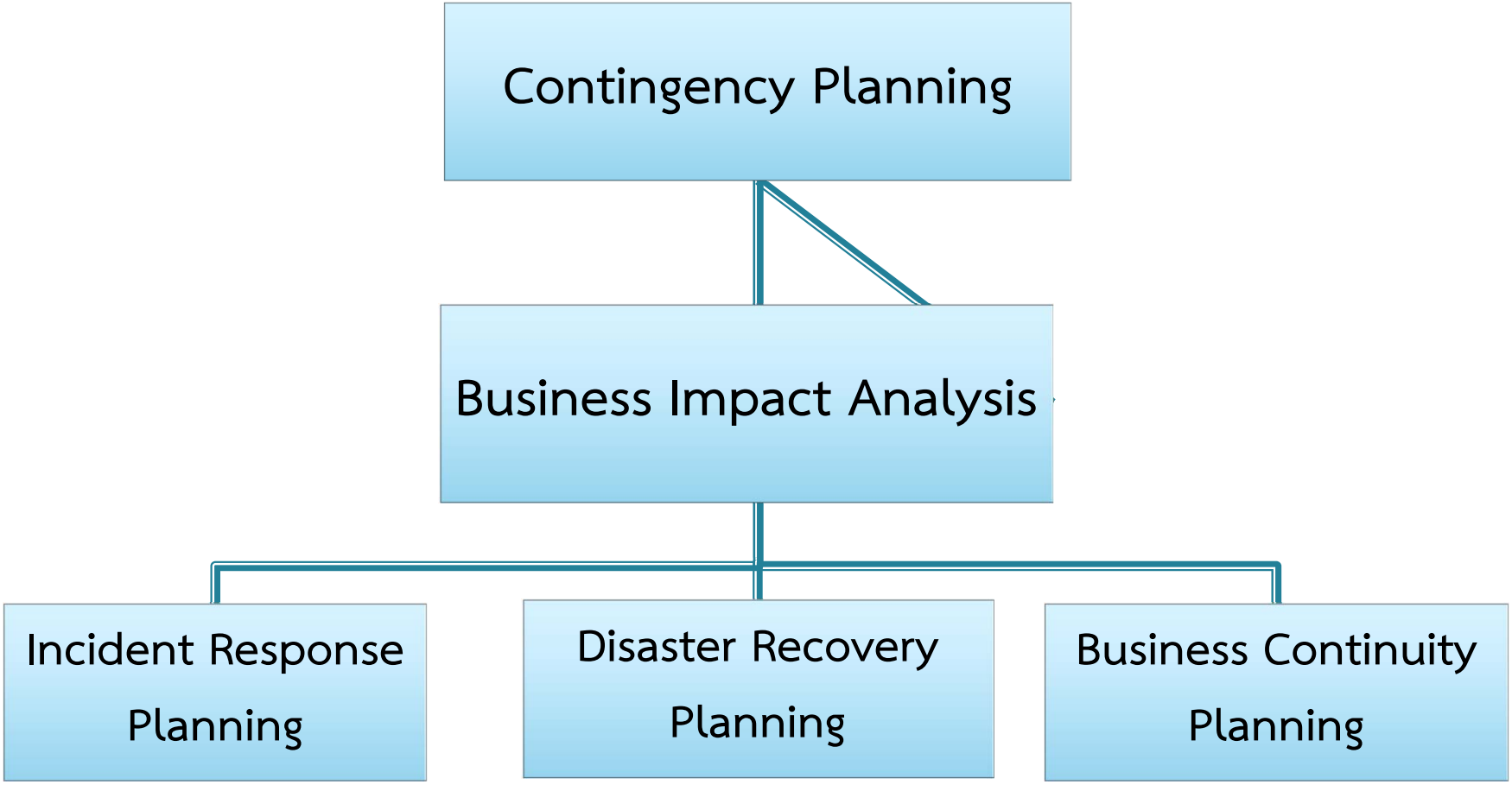
ส่วนประกอบของแผนรับสถานการณ์ฉุกเฉินและภัยพิบัติ

ประกอบด้วยแผนย่อย 4 แผน

1. การวิเคราะห์ผลกระทบทางธุรกิจ Business Impact Analysis
2. แผนรับมือเหตุการณ์ไม่คาดคิด Incident Response Plan
3. แผนฟื้นฟูจากความเสียหาย Disaster Recovery Plan
4. แผนดำเนินธุรกิจอย่างต่อเนื่องในสถานการณ์คับขัน Business Continuity Plan

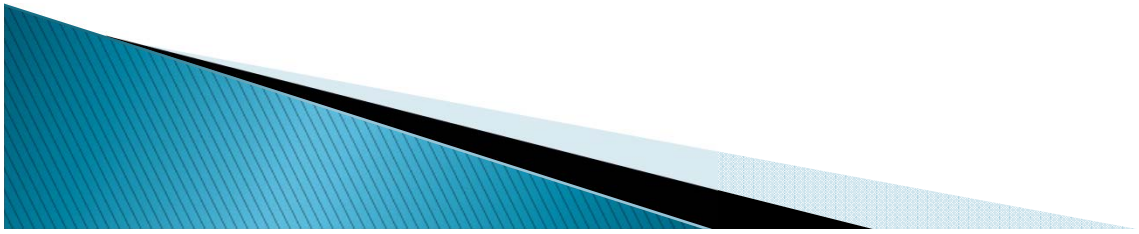


ส่วนประกอบของแผนรับสถานการณ์ฉุกเฉินและภัยพิบัติ



การวิเคราะห์ผลกระทบทางธุรกิจ

- **การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis)** คือ การประเมินผลที่อาจเกิดจากเหตุการณ์ไม่พร้อมใช้ต่าง ๆ หรือเหตุการณ์ที่ไม่คาดคิด
- **สรุป** คือ การประเมินความเสียหายจากเหตุการณ์ไม่คาดคิดนั่นเอง



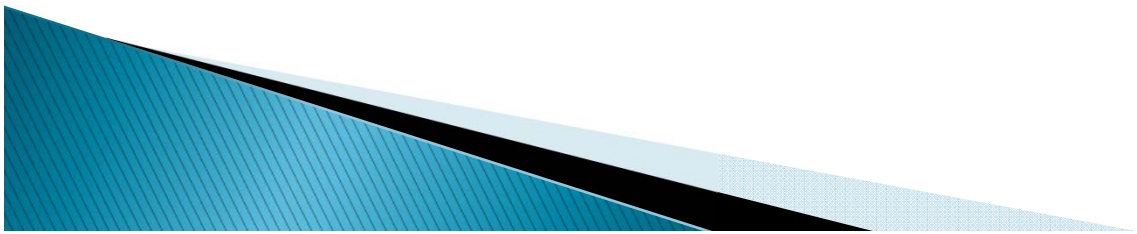
การวิเคราะห์ผลกระทบทางธุรกิจ

ขั้นตอนวิเคราะห์ผลกระทบทางธุรกิจ

ประกอบด้วยขั้นตอน 5 ขั้นตอนดังนี้

1. จำแนกและจัดลำดับการโจมตีจากภัยคุกคาม

องค์กรใดมีการจัดทำการวิเคราะห์ความเสี่ยง หรือดำเนินงานความมั่นคงปลอดภัยตามวงจร SecSDLC จะผ่านกิจกรรมการจำแนกและจัดลำดับการโจมตีจากภัยคุกคาม ทีมงานจะต้องนำรายการภัยคุกคาม มาเพิ่มเติมรายละเอียดในส่วนที่เรียกว่า Attack Profile หมายถึง รายละเอียดที่แสดงให้ทราบถึงพฤติกรรมการโจมตีภัยคุกคามประเภทต่างๆ ตัวอย่างเช่น



การวิเคราะห์ผลกระทบทางธุรกิจ

วันที่:	22/05/2008
ประเภทการโจมตี/รายละเอียด:	Malicious Code via e-mail
ภัยคุกคาม/ตัวแทน:	- Vandalism/Script Kiddies - Theft/Experience Hacker
ช่องโหว่:	- E-mail ของผู้ใช้ - พนักงานใช้ E-mail ไม่เหมาะสม - E-mail Server หรือ Gateway
พฤติกรรม:	- มีปริมาณ E-mail จำนวนมาก - ระบบของ Client ทำงานล้มเหลวผิดปกติ - การทำงานของ Server ล้มเหลวผิดปกติ - มีการแจ้งเตือนจาก E-mail ของผู้รับที่ไม่รู้จัก
ความเสี่ยง:	อาจแพร่กระจายไปยังทุกระบบที่เกี่ยวข้อง
ความเสียหายหรือสูญเสียของสารสนเทศ:	- ระบบปฏิเสธการให้บริการแก่ผู้ใช้ - ระบบปฏิเสธการให้บริการแก่ Server อื่น - ข้อมูลบางอย่างอาจสูญหาย
ความเสี่ยงของสินทรัพย์อื่นๆ:	ไม่มี
ความเสียหายหรือสูญเสียของสินทรัพย์อื่นๆ:	ไม่มี
การตอบสนองเมื่อพบการโจมตี:	- ตัดการเชื่อมต่อของ E-mail Gateway - กู้คืน Client ที่ถูกโจมตี - กู้คืน Server ที่ถูกโจมตี
การติดตาม:	กำหนดช่วงเวลาการอัพเดท Pattern ใหม่
ความคิดเห็นอื่นๆ:	ไม่มี

ขั้นตอนวิเคราะห์ผลกระทบทางธุรกิจ

2. **วิเคราะห์หน่วยธุรกิจ Business Unit Analysis** หรือหน้าท่าทางธุรกิจ แผนก ฝ่าย หรือส่วนงานใด ๆจะถูกวิเคราะห์ว่าหน้าที่ทางธุรกิจใดสำคัญที่สุด หน้าที่ใดรองลงมา และทำการจัดลำดับความสำคัญ
3. **สร้างสถานการณ์โจมตีประสบผลสำเร็จ Attack Success Scenario Development** ทีมงามจะนำ Attack Profile ที่เขียนไว้ มาสร้างสถานการณ์การโจมตีที่เป็นผลสำเร็จ คือ เป็นการเขียนผลกระทบที่เกิดขึ้นจากการโจมตีแต่ละประเภทในแต่ละหน้าที่ทางธุรกิจ เพื่อให้ทราบว่าแต่ละหน้าที่ทางธุรกิจนั้นได้รับผลกระทบอะไรบ้าง เอกสารที่ได้จะเรียกว่า Attack Success Scenario

ขั้นตอนวิเคราะห์ผลกระทบทางธุรกิจ

4. ประเมินผลความเสียหายที่อาจเกิดขึ้น Potential Damage Assessment นำ Attack Success Scenario มาจัดทำเอกสารที่แสดงถึงมูลค่าความเสียหายที่เกิดขึ้นกับหน้าที่ทางธุรกิจแต่ละประเภท และในแต่ละระดับของอันตรายที่เกิดขึ้น เอกสารที่เกิดขึ้นเรียกว่า Attack Scenario End Case

5. จำแนกเหตุการณ์ที่เกี่ยวข้องกับแผนอย่างต่อเนื่อง (Subordinate Plan Classification) นำ Attack Success Scenario และ Attack Scenario End Case มาพิจารณา เพื่อจำแนกว่าแต่ละ Case และแต่ละ Scenario มีความเกี่ยวข้องกับแผนอย่างไรบ้าง เช่น เหตุเพลิงไหม้ ย่อมเกี่ยวข้องกับแผนฟื้นฟูจากความเสียหาย (Disaster Recovery Plan) และ แผนดำเนินธุรกิจอย่างต่อเนื่องในสถานการณ์คับขัน (Business Continuity) เนื่องจากทั้งสองแผนเกี่ยวข้องกับเหตุการณ์ที่สร้างความเสียหายอย่างรุนแรง

แผนรับมือกับเหตุการณ์ไม่คาดคิด

- **แผนรับมือเหตุการณ์ไม่คาดคิด Incident Response Plan** ประกอบด้วยรายละเอียดของกระบวนการและขั้นตอนที่ต้องดำเนินการเมื่อตรวจพบเหตุการณ์ไม่คาดคิด ดังนั้นการวางแผนรับมือเหตุการณ์ไม่คาดคิด Incident Response Planning จึงหมายถึง การเตรียมตัวรับมือเหตุการณ์
- **เหตุการณ์ไม่คาดคิด Incident** คือเหตุการณ์ที่เกิดขึ้น ทั้งโดยธรรมชาติและมนุษย์ แล้วส่งผลต่อสารสนเทศและสินทรัพย์อื่น ๆ ขององค์กร การรับมือเหตุการณ์ไม่คาดคิด Incident Response ก็คือการดำเนินการต่างๆ ที่ต้องกระทำเมื่อตรวจพบเหตุการณ์ไม่คาดคิด

ร่างเอกสารสำคัญก่อนจัดทำแผนรับมือเหตุการณ์ไม่คาดคิด

มีขั้นตอน ดังนี้

1. **During The Incident** ทีมงานจะต้องทำเอกสารแสดงขั้นตอนการดำเนินงานที่จะต้องกระทำในระหว่างที่เกิดเหตุการณ์ไม่คาดคิดขึ้น โดยแบ่งขั้นตอนการดำเนินงานออกเป็นกลุ่มตามกลุ่มของผู้เกี่ยวข้อง เช่น ขั้นตอนที่ผู้ใช้ต้องกระทำ ขั้นตอนที่เจ้าหน้าที่ฝ่ายเทคนิคต้องกระทำ เป็นต้น
2. **After The Incident** จากข้อ 1 ให้นำมาประกอบจัดทำเอกสารแสดงขั้นตอนการดำเนินงานของผู้เกี่ยวข้องแต่ละฝ่าย หลังเหตุการณ์ไม่คาดคิดได้เกิดขึ้นและสงบลงแล้ว
3. **Before The Incident** จากข้อ 1 และ 2 ให้นำมาประกอบจัดทำเอกสารแสดงการดำเนินงานเพื่อการเตรียมตัวรับมือเหตุการณ์ไม่คาดคิด เช่น กำหนดตารางเวลาสำรองข้อมูล วิธีการเตรียมตัว เพื่อฟื้นฟูระบบจากความเสียหาย จัดตารางฝึกอบรม แผนการทดสอบเหตุการณ์ฉุกเฉิน ระดับการให้บริการของระบบและผู้ให้บริการ เป็นต้น

ตัวอย่างเอกสารทั้ง 3 ช่วงเวลาเหตุการณ์ไม่คาดคิด

ระหว่างการโจมตี

ผู้ใช้ระบบ (Users):

1. หากโปรแกรม Antivirus ของผู้ใช้ตรวจพบการโจมตี โปรแกรมจะลบหรือกักไวรัสไว้ ให้ผู้ใช้จดบันทึกข้อความแจ้งเตือนจากโปรแกรมไว้ และแจ้งไปยังเจ้าหน้าที่ฝ่ายเทคนิค
2. หากผู้ใช้พบว่าคอมพิวเตอร์ทำงานผิดปกติ หรือสงสัยว่าจะติดไวรัส ให้ปิดเครื่องคอมพิวเตอร์ และแจ้งไปยังเจ้าหน้าที่ฝ่ายเทคนิคทันที

เจ้าหน้าที่ฝ่ายเทคนิค (Technical Service):

1. บันทึกข้อมูลการติดไวรัสที่ผู้ใช้แจ้งมา
2. ตัดการเชื่อมต่อกับเครือข่ายชั่วคราวสำหรับเครื่องผู้ใช้ที่ติดไวรัส
3. สแกนไวรัสทุกระบบที่ต้องสงสัย
4. ให้ทีมงานออกตรวจสอบระบบของผู้ใช้ที่ติดไวรัส

หลังการโจมตี

ผู้ใช้ระบบ (Users):

1. สแกนไวรัสที่เครื่องคอมพิวเตอร์ของผู้ใช้เพื่อตรวจหาไวรัสประเภทอื่นๆ
2. เช็คอีเมล์เพื่อดูความผิดปกติ (เช่น Subject, Attach File) และตรวจหาอีเมล์ต้นเหตุของไวรัส
3. เขียนอธิบายอาการผิดปกติก่อนตรวจพบไวรัส
4. ตรวจสอบโปรแกรม Antivirus ว่าอัพเดทหรือไม่

เจ้าหน้าที่ฝ่ายเทคนิค (Technical Service):

1. บันทึกเหตุการณ์ไม่คาดคิดที่เกิดขึ้น
2. สอบถามผู้ใช้ทุกคนเพื่อตรวจหาสาเหตุ
3. ตรวจสอบการทำงานของระบบงานทุกระบบ พร้อมทั้งอัพเดท Signature ในระบบตรวจจับการบุกรุก
4. เชื่อมต่อเครื่องของผู้ใช้ที่ติดไวรัสเข้ากับเครือข่ายอีกครั้ง ตรวจสอบการทำงานให้กลับสู่สภาพปกติ
5. สรุปสถานการณ์ให้ผู้ใช้ฟัง
6. ประกาศแจ้งเตือนไปยังผู้ใช้คนอื่นๆ ให้ทราบโดยทั่วกัน พร้อมให้ผู้ใช้อัพเดทโปรแกรม Antivirus ด้วย

ก่อนการโจมตี

ผู้ใช้ระบบ (Users):

1. ห้ามนำ Flash Drive ที่ติดไวรัสมาใช้งาน หรือควรสแกน Flash Drive ก่อนใช้งานเสมอ
2. ห้ามดาวน์โหลดโปรแกรม/เกมส์/อื่นๆ ก่อนได้รับอนุญาตจากเจ้าหน้าที่ทางเทคนิค
3. ห้ามเปิดไฟล์ที่แนบมากับอีเมล์ หากมีการแจ้งเตือนว่าไฟล์ดังกล่าวไม่ปลอดภัย
4. อย่าฟอร์เวิร์ดอีเมล์เตือนไวรัสจากผู้ส่งที่ไม่รู้จัก

เจ้าหน้าที่ฝ่ายเทคนิค (Technical Service):

1. หมั่นตรวจสอบโปรแกรม Antivirus ว่าทำงานได้ตามปกติ และอัพเดทโปรแกรมเป็นระยะ
2. จัดหลักสูตรฝึกอบรม ให้ความรู้ด้านความมั่นคงปลอดภัยแก่ผู้ใช้ และสร้างระเบียบวินัย จิตสำนึกในการใช้งานอุปกรณ์ต่างๆ อย่างระมัดระวัง

ขั้นตอนการจัดทำแผนรับมือเหตุการณ์ไม่คาดคิด

1. เตรียมตัววางแผน Prepare to Plan
2. ตรวจหาเหตุการณ์ไม่คาดคิด Incident Detection

    2.1 Possible Indicator เหตุการณ์ต้องสงสัยอาจเป็นไปได้ว่าเป็นเหตุการณ์ไม่คาดคิด

    2.2. Probable Indicator เหตุการณ์ต้องสงสัยที่เกิดขึ้น ค่อนข้างแน่ใจ (Probable) ว่าเป็นเหตุการณ์ไม่คาดคิด

    2.3. Definite Indicator เหตุการณ์ต้องสงสัยที่เกิดขึ้น จัดว่าเป็นเหตุการณ์ไม่คาดคิด แน่นอน Definite

3. รับมือเหตุการณ์ไม่คาดคิด Incident Response

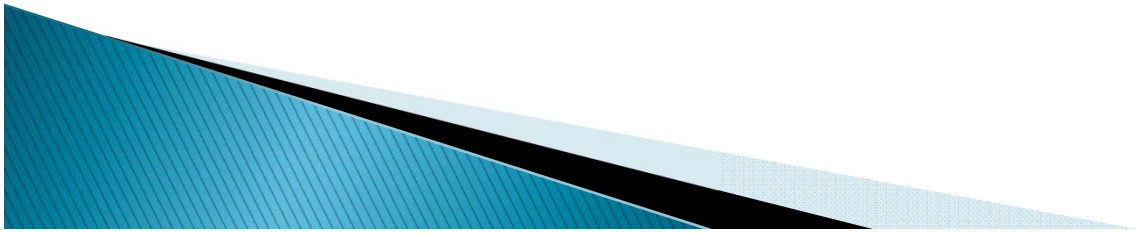
ขั้นตอนการจัดทำแผนรับมือเหตุการณ์ไม่คาดคิด

4. ฟื้นฟูระบบจากเหตุการณ์ไม่คาดคิด Incident Recovery เป็นขึ้นตอนกำหนดวิธีการฟื้นฟู ทีมงานจะต้องประเมินสถานการณ์ความเสียหายที่เกิดขึ้น ซึ่งจะพิจารณาตามขอบเขตของการรักษาความมั่นคงปลอดภัยของสารสนเทศ ได้แก่

    4.1 ความเสียหายด้านการปกปิดข้อมูลที่เป็นความลับ Confideniality

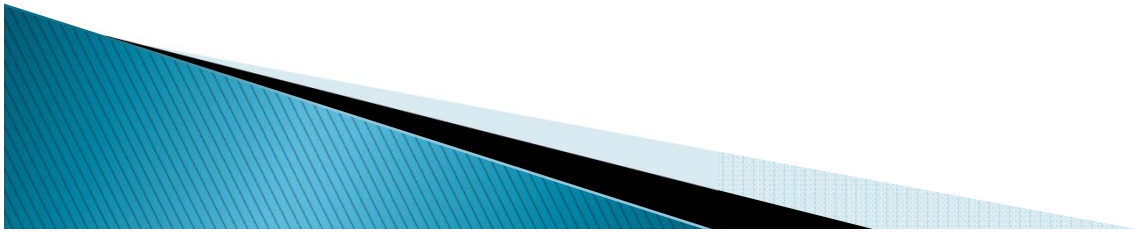
    4.2 ความถูกต้อง Integrity

    4.3 ความพร้อมใช้ Availability



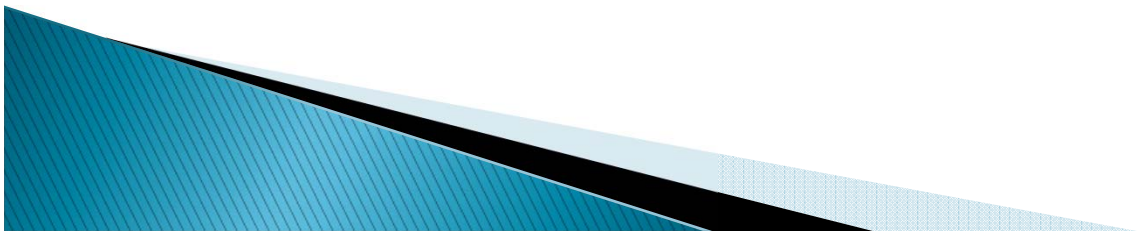
7 ขั้นตอนเพื่อกำหนดวิธีการฟื้นฟูระบบ

- ตรวจหาช่องโหว่ของระบบ
- ตรวจหาโปรแกรม Antivirus และโปรแกรมป้องกันการโจมตีอื่น ๆ
- ประเมินและปรับปรุงประสิทธิภาพของระบบติดตามการโจมตี
- กู้คืนข้อมูลจากแหล่งข้อมูลสำรอง
- กู้คืน Service และ Process ที่กำลังงานในขณะเกิดเหตุการณ์ไม่คาดคิด
- ติดตามการทำงานของระบบทันที
- แจ้งข่าวการเกิดเหตุการณ์ไม่คาดคิดแก่ทุกฝ่าย



แผนฟื้นฟูจากความเสียหาย

- **แผนฟื้นฟูจากความเสียหาย Disaster Recovery Plan** เป็นการกำหนดรายละเอียดในการเตรียมตัวฟื้นฟูการดำเนินงานจากความเสียหายหรือภัยพิบัติทั้งที่เกิดจากธรรมชาติและมนุษย์
- เช่นเดียวกับแผนงานชนิดอื่น ๆ ที่จะต้องมีทีมงามย่อยรับผิดชอบในการจัดทำโดยเฉพาะ เริ่มต้นจากการจัดทำนโยบายการฟื้นฟูจากความเสียหาย เรียกว่า Disaster Recovery Policy

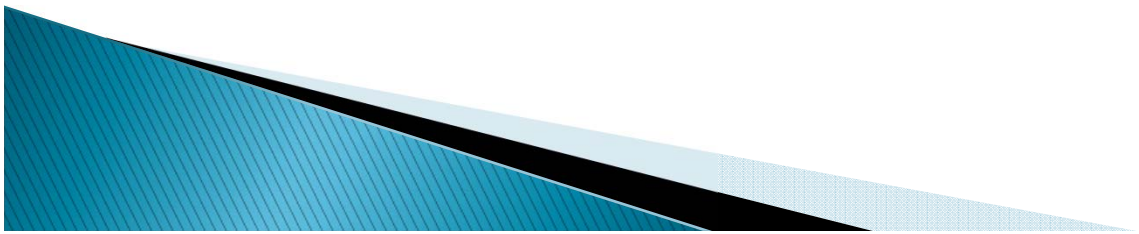


รายละเอียดสำคัญของแผนฟื้นฟูจากความเสียหาย

- **วัตถุประสงค์** บอกถึงวัตถุประสงค์ของแผนฯ เพื่อเป็นแนวทางในการปฏิบัติเมื่อเกิดขึ้นจริง
- **ขอบเขต** ระบุหน่วยงาน หรือหน้าที่ทางธุรกิจและกลุ่มบุคคลที่ต้องนำแผนฯ ไปใช้ได้จริง
- **บทบาทและความรับผิดชอบ** ระบุบทบาทและความรับผิดชอบของบุคลากรในการฟื้นฟูจากความเสียหาย
- **ทรัพยากรที่ต้องใช้** ระบุทรัพยากรที่ต้องใช้ในการฟื้นฟูการดำเนินงาน
- **การฝึกอบรม** ระบุโปรแกรมการฝึกอบรมที่จำเป็นต่อทุกฝ่ายและจำเป็นต่อผู้ใช้ทุกกลุ่ม

รายละเอียดสำคัญของแผนฟื้นฟูจากความเสียหาย

- **ตารางการทดสอบและฝึกซ้อม** จัดตารางการทดสอบแผนฟื้นฟูและการฝึกซ้อมฟื้นฟูการดำเนินงาน
- **ตารางบำรุงรักษา** จัดตารางทบทวนและปรับปรุงข้อมูลในแผนฟื้นฟูเป็นระยะ
- **ข้อควรระวัง** ระบุเรื่องที่ผู้เกี่ยวข้องควรระวังหรือควรให้ความสนใจเป็นพิเศษ



แผนฟื้นฟูจากความเสียหาย

กิจกรรมที่จำเป็นต่อการจัดทำแผนฟื้นฟูจากความเสียหาย คือ การจำแนกประเภทของความเสียหาย Disaster Classification ซึ่งทีมงานสามารถจำแนกประเภทได้หลายกลุ่ม เช่น

- **ความเสียหายที่เกิดจากมนุษย์** เช่น ลัทธิก่อการร้าย และสงคราม เป็นต้น
- **ความเสียหายที่เกิดจากธรรมชาติ** เช่น เพลิงไหม้ น้ำท่วม ฟ้าผ่า แผ่นดินยุบ พายุโคลน ทอร์นาโด ใต้ฝุ่น สึนามิ ไฟช๊อต เป็นต้น

ขั้นตอนการปฏิบัติงานของสมาชิกในทีมเพื่อลดความเสียหายเมื่อพบว่าเกิดภัยพิบัติขึ้น เช่น สมาชิกในทีมต้องรีบปิด server หรือการขนย้ายทรัพย์สินทันทีที่ทราบการแจ้งเตือน

วิธีการจัดหาระบบหรืออุปกรณ์ใหม่มาแทนอุปกรณ์เดิมที่ได้รับความเสียหาย เช่น การเช่า ซื้อ เป็นต้น

แผนดำเนินธุรกิจอย่างต่อเนื่องในสถานการณ์คับขัน

แผนดำเนินธุรกิจอย่างต่อเนื่องในสถานการณ์คับขัน Business Continuity Plan คือ แผนงานที่จะทำให้มั่นใจได้ว่า หน้าที่ทางธุรกิจที่สำคัญ จะสามารถดำเนินไปได้ แม้จะมีความเสียหายเกิดขึ้น สำหรับไซต์งานสำรอง เพื่อความต่อเนื่องของธุรกิจ เมื่อเกิดสถานการณ์คับขัน สามารถแบ่งได้เป็น 3 ประเภท

- **Hot site** คือ ไซต์งานที่องค์ประกอบในการทำงานครบถ้วนเหมือนเดิมทุกประการ การส ารองจะเป็นแบบ real time
- **Warm site** มีอุปกรณ์ครบเหมือนกับ Hot Site แต่เล็กกว่า การสำรองข้อมูลจะไม่เป็นแบบ real time เหมือนกับ Hot site แต่จะเป็นช่วงระยะเวลาที่กำหนด
- **Cold Site** เป็นไซต์งานที่คืนสภาพการทำงานช้าที่สุด เนื่องจากไซต์งานที่มีเพียงสถานที่ว่างเปล่าที่ได้ถูกจัดทำไว้เท่านั้น แต่จะไม่มีระบบคอมพิวเตอร์และข้อมูลสำรองไว้

ความแตกต่างระหว่างแผนงานแต่ละชนิด

การจำแนกความแตกต่างแผนงาน 3 ชนิด ที่เป็นองค์ประกอบของแผนรับสถานการณ์ฉุกเฉินและภัยพิบัติ Contingency Plan จะใช้ เวลา Time เป็นเงื่อนไขในการพิจารณา สามารถสรุปได้ดังนี้

1. **แผนรับมือเหตุการณ์ไม่คาดคิด Incident Reponses Plan** นำไปใช้ทันทีที่พบการโจมตีประเภทต่างๆ หากเหตุการณ์ไม่คาดคิดนั้นทำให้ระบบเสียหายมาก ให้นำแผนฟื้นฟูจากความเสียหายมาใช้
2. **แผนฟื้นฟูจากความเสียหาย Disaster Recovery Plan** มีวัตถุประสงค์เพื่อการฟื้นฟูระบบให้กลับมาท างานได้ ตามปกติหลังจากที่ระบบมีความเสียหายเกิดขึ้น
3. **แผนดำเนินธุรกิจอย่างต่อเนื่องในสถานการณ์ดับขัน Business Continuity Plan** นำมาใช้ควบคู่กับแผนฟื้นฟูจากความเสียหาย หากพบว่าต้องใช้เวลานานหรือต้องใช้ความพยายามอย่างมากในการฟื้นฟูระบบ

การทดสอบแผนรับสถานการณ์ฉุกเฉินและภัยพิบัติ

มีกลยุทธ์ ที่ใช้ในการทดสอบแผนรับสถานการณ์ฉุกเฉินและภัยพิบัติ ดังนี้

1. **Desk Check** โดยการกระจายแผนงานไปยังบุคลากรที่ได้รับมอบหมายให้รับผิดชอบหน้าที่ต่าง ๆ ในแผนงาน จากนั้นบุคลากรแต่ละคนจะทำการทดสอบแบบ Desk Check โดยการทบทวนรายละเอียดในแผน และทำเครื่องหมายหรือสัญลักษณ์ใด ๆ เพื่อแสดงให้เห็นว่ารายละเอียดใด ถูก หรือ ผิด เป็นเพียงการทบทวนรายละเอียดในแผนเท่านั้น เหมาะแก่การนำไปประกอบการพิจารณาความเป็นไปได้และความคุ้มค่าในการลงทุน
2. **Structured Walk-through** การทดสอบวิธีนี้ บุคลากรที่ได้รับมอบหมายจะทำการทดสอบแผนตามขั้นตอนต่าง ๆ ที่ระบุไว้ในแผน

การทดสอบแผนรับสถานการณ์ฉุกเฉินและภัยพิบัติ

3. Simulation การทดสอบวิธีนี้ บุคลากรได้รับมอบหมายในแผนงานจะต้องทดสอบแผนงานโดยจำลองการดำเนินงานทุกกิจกรรมที่ได้รับมอบหมาย จากนั้นบันทึกข้อผิดพลาดที่เกิดจากการทดสอบเพื่อปรับปรุงต่อไป บุคลากรในการทดสอบนี้จะรับผิดชอบเฉพาะงานที่ตนได้รับมอบหมายเท่านั้น

4. Parallel Testing บุคลากรจะปฏิบัติหน้าที่เสมือนเกิดหตุการณ์ขึ้นจริงและดำเนินกิจกรรมตามขั้นตอนต่าง ๆ ตามความจำเป็น โดยไม่รบกวนการดำเนินงานตามปกติของธุรกิจ

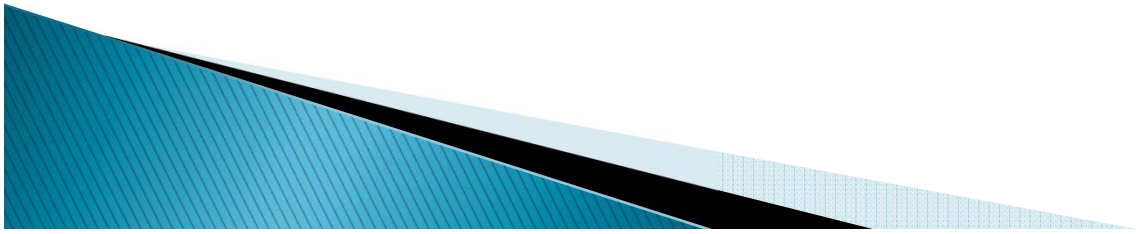
5. Full Interruption จึงควรทดสอบหลังเวลางาน การทดสอบวิธีนี้จะมีความเสี่ยงมากกว่าวิธีอื่น

มาตรฐานการรักษาความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC17799

มาตรฐานการรักษาความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC17799 เป็นมาตรฐานการจัดความมั่นคงปลอดภัยของสารสนเทศ ที่กำหนดขึ้นโดย British Standard Institute ของประเทศอังกฤษ แต่เดิมใช้ชื่อว่า BS7799 จากนั้นในปี ค.ศ. 2000 ได้ถูกนำมาดัดแปลงโดยองค์กรมาตรฐานสากล International Organization for Standard: ISO และคณะกรรมาธิการระหว่างประเทศว่าด้วยมาตรฐานสาขาอิเล็กทรอนิกส์ International Electrotechnical Commision : IEC จึงได้เปลี่ยนชื่อใหม่เป็น ISO/IEC17799

มาตรฐานการรักษาความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC17799

- **ISO/IEC17799** ได้ให้แนวทางในการจัดการความมั่นคงปลอดภัยของสารสนเทศอย่างมีระบบ แก่ผู้ที่รับผิดชอบหน้าที่ในการเริ่มต้น (Initiation) พัฒนา (Implementation) หรือบำรุงรักษา (Maintaining) ความมั่นคงปลอดภัยในองค์กร
- **ISO/IEC17799** มี 2 ฉบับ



ฉบับที่ 1

มีเนื้อหาครอบครุมทุกด้านของงานการจัดการความมั่นคงปลอดภัยของสารสนเทศ ประกอบด้วยหัวข้อการควบคุมความมั่นคงปลอดภัยทั้งหมด จัดเป็น 10 หมวดหลัก ดังนี้

1. Security Policy : นโยบายความมั่นคงปลอดภัยของสารสนเทศ
2. Security Infrastructure หรือ Organization of Information Security : โครงสร้างทางด้านความมั่นคงปลอดภัยของสารสนเทศสำหรับองค์กร
3. Asset Classification and Control : การจำแนกทรัพย์สินและการควบคุม
4. Personnel Security : ความมั่นคงปลอดภัยของบุคคล

ฉบับที่ 1

5. Physical and Environmental Security : ความมั่นคงปลอดภัยทางด้านสภาพแวดล้อมและกายภาพ

6. Communications and Operations Management : การจัดการการติดต่อสื่อสารและการดำเนินงาน

7. System Access Control : การควบคุมการเข้าถึงระบบ

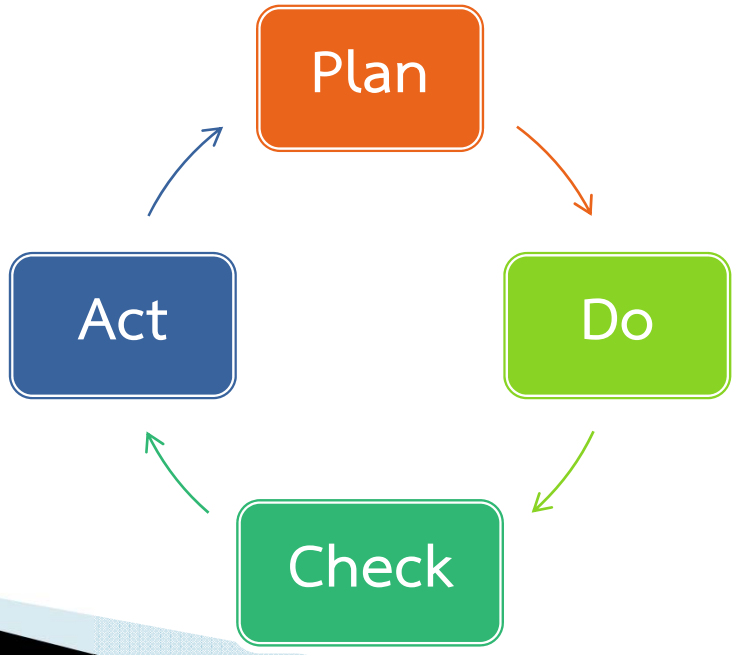
8. System Development and Maintenance : การพัฒนาและการบำรุงรักษา

9. Business Continuity Planning : การวางแผนดำเนินธุรกิจอย่างต่อเนื่องในสถานการณ์คับขัน

10. Compliancy : การยอมรับและปฏิบัติตามข้อกำหนดของกฎหมาย

ฉบับที่ 2

ได้ให้คำแนะนำที่เน้นวิธีการดำเนินงานตามฉบับที่ 1 และอธิบายถึงการจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ **Information Security Management System: ISMS** โดยมีกระบวนจัดทำเป็นวงจร เรียกว่า วงจร **PDCA (Plan-Do-Check-Action)**



Plan คือขั้นตอนของการวางแผนจัดตั้ง (Establish)ระบบ ISMS แต่ละขั้นตอนประกอบด้วย

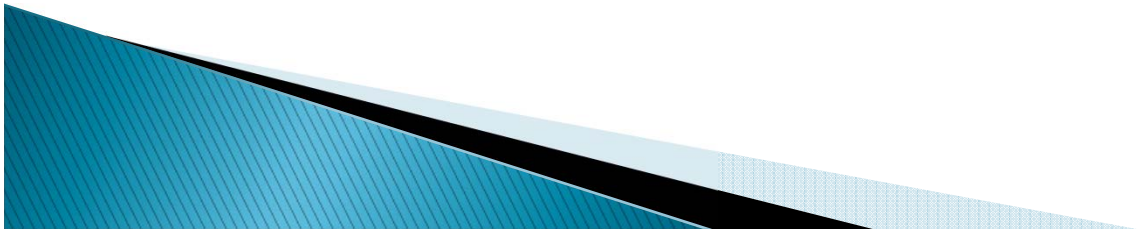
- กำหนดขอบเขตของระบบ
- กำหนดนโยบายของระบบ
- กำหนดแนวทางการประเมินความเสี่ยง
- ระบุความเสียง
- ประเมินความเสี่ยง
- ระบุและประเมินวิธีการลดความเสี่ยง
- เลือกวัตถุประสงค์และการควบคุม
- จัดเตรียมเอกสารมาตรการใช้งาน Statement of Applicability : SO

Do คือขั้นตอนการลงมือทำ คือพัฒนาระบบให้ดีขึ้นและนำไปใช้งาน Implement and Operate : ISMS ประกอบด้วยกิจกรรมย่อย ดังนี้

- จัดทำแผนการลดความเสี่ยง
- นำแผนการลดความเสี่ยงไปปฏิบัติ
- ใช้วิธีการควบคุมแบบต่าง ๆ
- จัดการฝึกอบรม ให้ความรู้ และสร้างความตะหนัก
- จัดการดำเนินงาน
- จัดการทรัพยากร
- ดำเนินในขั้นตอนการตรวจจับและตอบสนองต่อเหตุการณ์ไม่คาดคิดด้านความมั่นคง

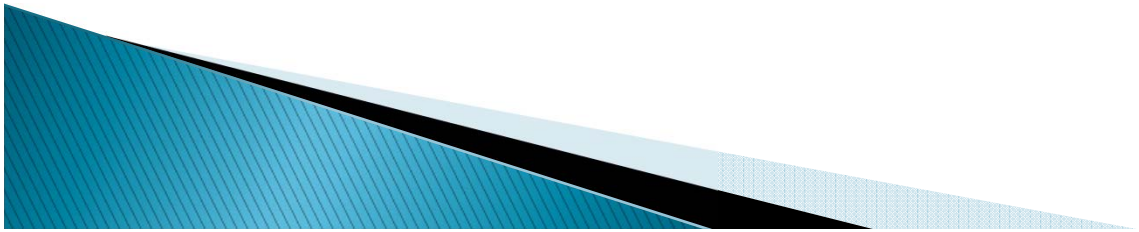
Check คือขั้นตอนของการติดตามและทบทวน Monitor and Review การดำเนินงานระบบ ISMS ประกอบด้วยกิจกรรมย่อยดังนี้

- เข้าสู่กระบวนการติดตามการทำงานของระบบ ISMS
- ประเมินประสิทธิภาพของระบบ ISMS
- ตรวจสอบระดับความเสี่ยง
- จัดทำการตรวจสอบภายในของระบบ ISMS
- ประเมินการบริหารจัดการระบบ ISMS
- บันทึกกิจกรรมและเหตุการณ์ที่ส่งผลกระทบต่อระบบ ISMS



Act คือขั้นตอนของการบำรุงรักษาและปรับปรุง Maintain and Improve ระบบ ISMS ประกอบด้วยกิจกรรมย่อยดังนี้

- ปรับปรุงระบบในส่วนที่มีข้อบกพร่อง
- ดำเนินการแก้ไขและป้องกัน
- นำบทเรียนหรือกรณีศึกษาที่ประสบผลสำเร็จจากที่อื่นมาปรับใช้
- รายงานผลการใช้งานระบบแก่ทุกฝ่ายที่มีส่วนเกี่ยวข้อง
- สร้างความมั่นใจว่าการปรับปรุงตรงตามวัตถุประสงค์



Questions and Answers

MS1 Thanin Muangpool

Thank you