9 การกู้คืนทรัพย์สินและการดำเนินงาน

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ดร.สุรเชษฐ์ สุชัยยะ
ผู้อำนวยการ
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ (CIPAT)

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.1 จุดประสงค์และปัจจัยการกู้คืนทรัพย์สินในระบบสารสนเทศ

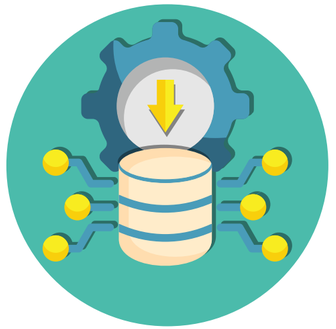
9.2 ระยะของการกู้คืนระบบ (Disaster Recovery Phases)

9.3 แผนฟื้นฟูภัยพิบัติ/แผนการกู้คืนจากภัยคุกคามทางไซเบอร์ (Disaster Recovery Plan - DRP)

9.4 การสำรองข้อมูล (Backup)

9.5 แหล่งกู้คืนภัยพิบัติ (Disaster Recovery Sites)

9.6 แผนการสื่อสารช่วงกู้คืนภัยพิบัติ (Disaster Recovery Communication Plan)



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.1 จุดประสงค์และปัจจัยการกู้คืนทรัพย์สินในระบบสารสนเทศ

- จุดประสงค์ของการกู้คืนระบบ
- ปัจจัยที่จำเป็นสำหรับกระบวนการกู้คืนระบบ

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.1 จุดประสงค์และปัจจัยการกู้คืนทรัพย์สินในระบบสารสนเทศ

- จุดประสงค์ของการกู้คืนระบบ
  - Short-Term Recovery Objective
  - Medium-Term Recovery Objectives
  - Long-Term Recovery Projects

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.1 จุดประสงค์และปัจจัยการกู้คืนทรัพย์สินในระบบสารสนเทศ

- ปัจจัยที่จำเป็นสำหรับกระบวนการกู้คืนระบบ
  - ข้อมูลที่ได้รับ การบำรุงรักษา และค่าใช้จ่ายในการปฏิบัติงาน
  - งบประมาณการกู้คืนระบบขององค์กร
  - ระยะเวลาที่ใช้ไปกับการกู้คืนระบบ
  - ความพร้อมของบุคลากรเพื่อปฏิบัติงานและการจัดการ
  - ความพร้อมและโซลูชันจาก Third Party

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.2 ระยะของการกู้คืนระบบ (Disaster Recovery Phases)

- Activation Phase
- Notification Phase
- Damage Assessment Phase
- Execution Phase
- Reconstitution Phase

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.2 ระยะของการกู้คืนระบบ (Disaster Recovery Phases)

- Activation Phase
  - ประกาศแจ้งเตือน
  - ประเมินความเสียหาย
  - กระตุ้นการกู้คืน

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.2 ระยะของการกู้คืนระบบ (Disaster Recovery Phases)

- Notification Phase
  - แจ้งข่าวสาร
  - รายงานความสูญเสีย
  - รายละเอียดการตอบสนองครั้งแรก
  - ประเมินเวลาในการกู้คืน
  - ข้อมูลแผนงานโดยสรุป
  - ข่าวสารและข้อแนะนำ
  - รายละเอียดการติดต่อ

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.2 ระยะของการกู้คืนระบบ (Disaster Recovery Phases)

- Damage Assessment Phase
  - ระบุสาเหตุและธรรมชาติของภัยพิบัติ
  - ประเมินความเสียหายและผลกระทบ
  - ประเมินความเป็นไปได้ของความเสียหายต่อเนื่อง
  - ประเมินเวลาที่คาดว่าจะใช้ในการกู้คืน
  - ประเมินความสามารถของอุปกรณ์

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.2 ระยะของการกู้คืนระบบ (Disaster Recovery Phases)

- Execution Phase
  - จัดลำดับความสำคัญของกิจกรรมกูGคืนระบบ
  - กระบวนการกู้คืน

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.2 ระยะของการกู้คืนระบบ (Disaster Recovery Phases)

- Reconstitution Phase
  - เรียกคืนระบบสู่สภาวะปกติ
  - ทดสอบระบบที่กู้คืน
  - ตรวจสอบและทดสอบการปฏิบัติงานเป็นระยะ ๆ

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.3 แผนฟื้นฟูภัยพิบัติ/แผนการกู้คืนจากภัยคุกคามทางไซเบอร์ (Disaster Recovery Plan - DRP)

ขั้นตอนในการวางแผนฟื้นฟูภัยพิบัติ

- กำหนดทีมกู้คืน
- ประเมินและจัดลำดับความสำคัญของความเสี่ยง
- พัฒนาแผนและขั้นตอนการกู้คืน
- ออกแบบและดำเนินการสำรองข้อมูล
- ทดสอบและปรับแผนการกู้คืน

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.3 แผนฟื้นฟูภัยพิบัติ/แผนการกู้คืนจากภัยคุกคามทางไซเบอร์ (Disaster Recovery Plan - DRP)

ขั้นตอนในการวางแผนฟื้นฟูภัยพิบัติ

- กำหนดทีมกู้คืน
  - Operations Recovery Director
  - ผู้จัดการฝ่ายปฏิบัติการและทีมกู้คืนระบบ
  - Facility Recovery Team
  - ทีมงานกู้คืน Platform

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.3 แผนฟื้นฟูภัยพิบัติ/แผนการกู้คืนจากภัยคุกคามทางไซเบอร์ (Disaster Recovery Plan – DRP)

ขั้นตอนในการวางแผนฟื้นฟูภัยพิบัติ

- ประเมินและจัดลำดับความสำคัญของความเสี่ยง

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.3 แผนฟื้นฟูภัยพิบัติ/แผนการกู้คืนจากภัยคุกคามทางไซเบอร์ (Disaster Recovery Plan – DRP)

ขั้นตอนในการวางแผนฟื้นฟูภัยพิบัติ

- ประเมินและจัดลำดับความสำคัญของความเสี่ยง
  - Business Impact Analysis (BIA) กระบวนการวิเคราะห์ปัจจัยเสี่ยงและผลกระทบจากในช่วงเวลาหนึ่งที่ระบบงานขององค์กรถูกทำให้หยุดชะงัก
  - Recovery Point Objective (RPO) ปริมาณข้อมูลสูญหายที่องค์กรยอมรับได้ในช่วงเวลาหนึ่ง (Acceptable Loss)

9 การกู้คืนทรัพย์สินและการดำเนินงาน

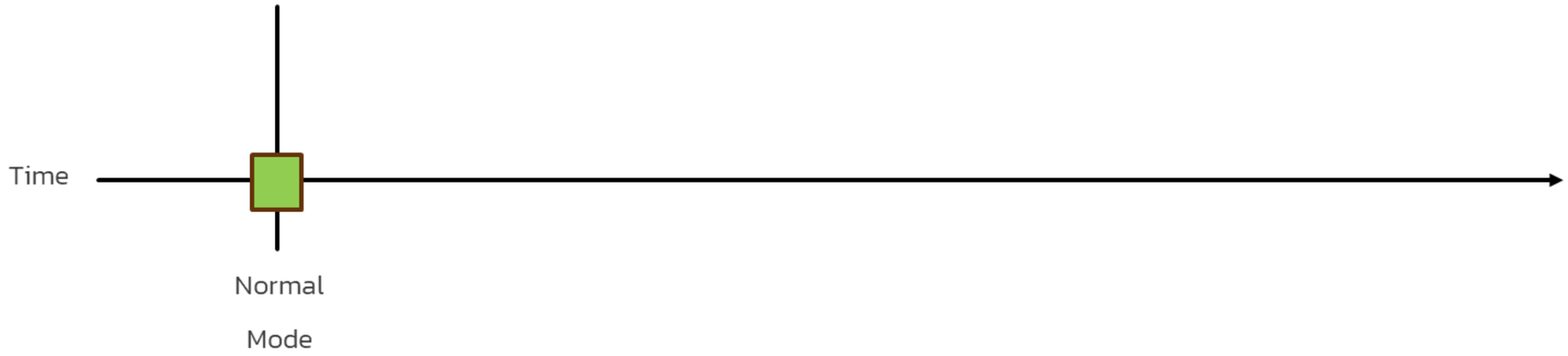
9.3 แผนฟื้นฟูภัยพิบัติ/แผนการกู้คืนจากภัยคุกคามทางไซเบอร์ (Disaster Recovery Plan – DRP)

ขั้นตอนในการวางแผนฟื้นฟูภัยพิบัติ

- ประเมินและจัดลำดับความสำคัญของความเสี่ยง
  - Recovery Time Objective (RTO) ระยะเวลาที่องค์กรยอมรับได้ในการกู้คืนระบบในกรณีที่เกิดเหตุฉุกเฉินขึ้น ซึ่งเป็นค่าที่ถูกกำหนดโดยเจ้าของระบบ ต้องให้ผู้บริหารระดับสูงรับรู้ และยอมรับในค่า RTO ที่ถูกกำหนดขึ้น
  - Maximum Tolerable Period of Disruption (MTPD) ช่วงเวลานานที่สุดที่ธุรกิจหยุดชะงัก หากเกินกำหนดช่วงเวลา นี้แล้วจะไม่สามารถทำให้ธุรกิจฟื้นคืนสู่สภาพปกติได้

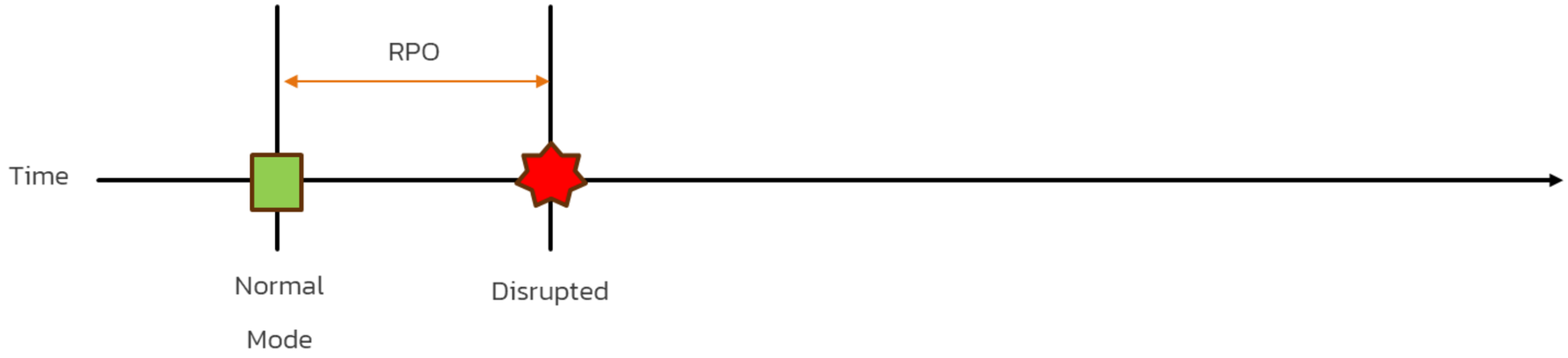
9 การกู้คืนทรัพย์สินและการดำเนินงาน

การวิเคราะห์ผลกระทบทางธุรกิจหลัก (BIA : Business Impact Analysis)
อ้างอิง ISO/IEC 22301:2019



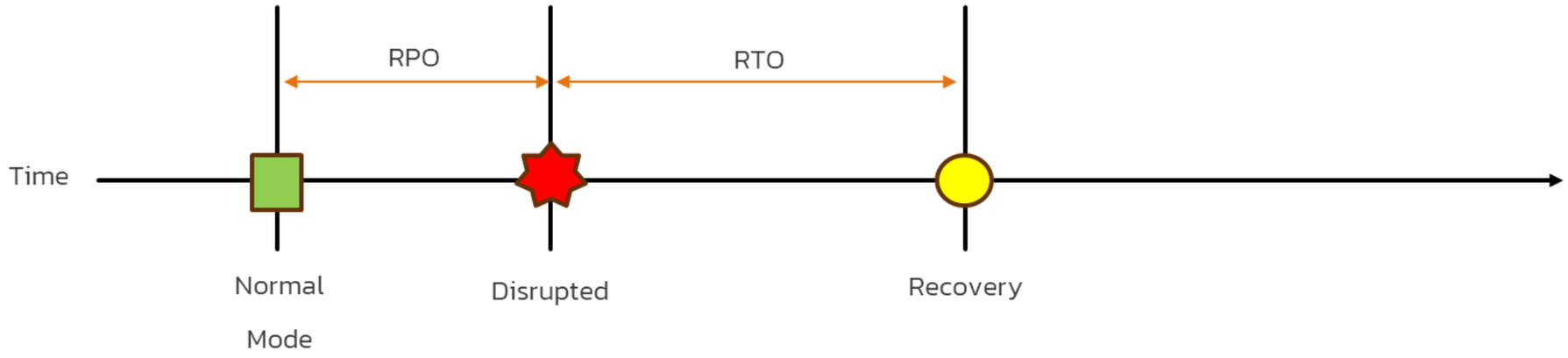
9 การกู้คืนทรัพย์สินและการดำเนินงาน

การวิเคราะห์ผลกระทบทางธุรกิจหลัก (BIA : Business Impact Analysis)
อ้างอิง ISO/IEC 22301:2019



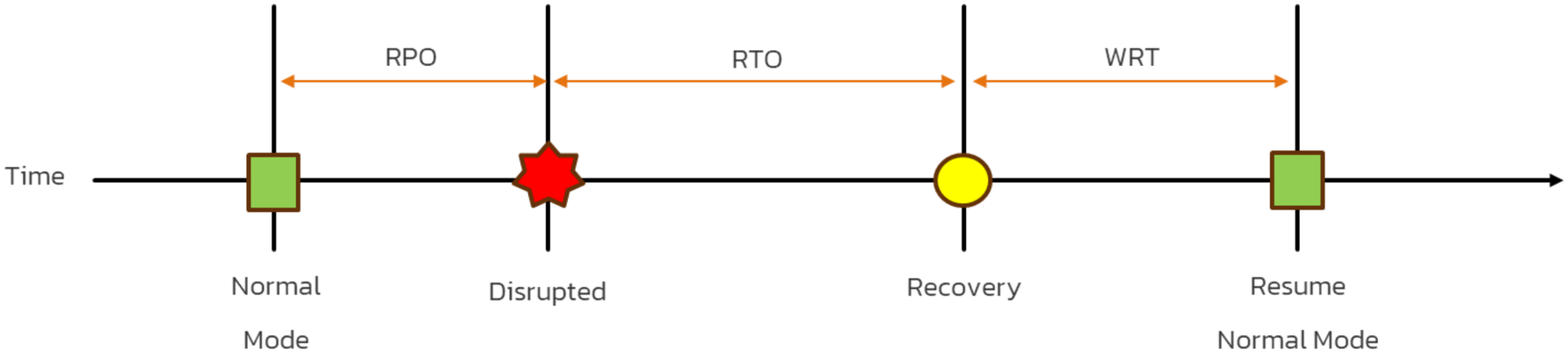
9 การกู้คืนทรัพย์สินและการดำเนินงาน

การวิเคราะห์ผลกระทบทางธุรกิจหลัก (BIA : Business Impact Analysis)
อ้างอิง ISO/IEC 22301:2019



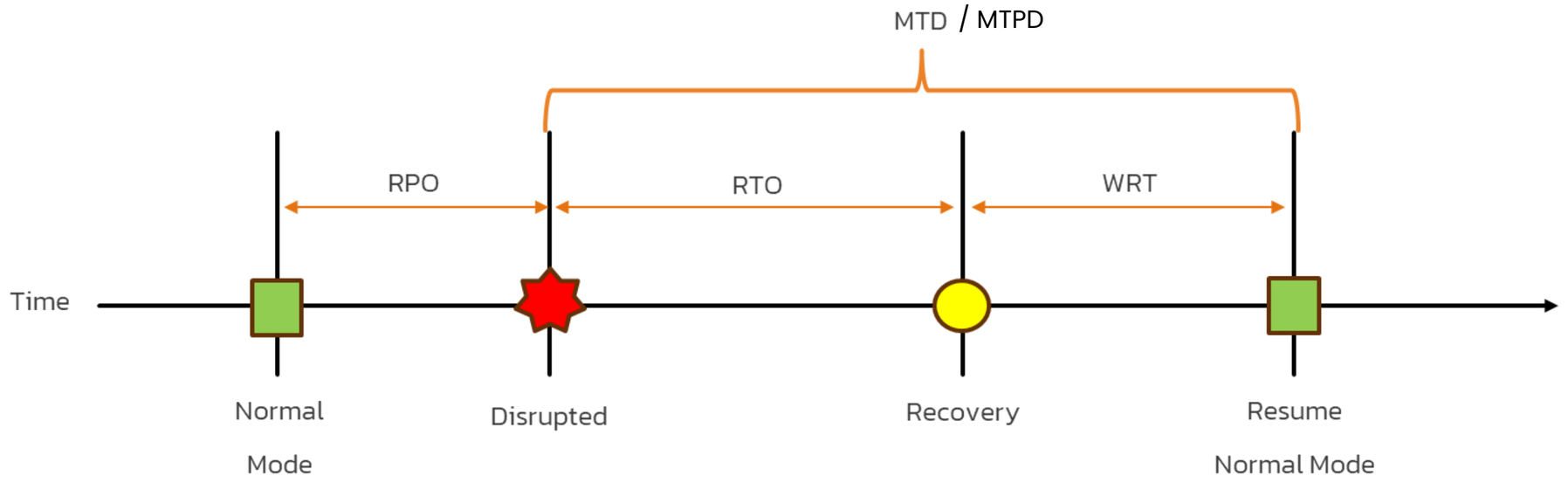
9 การกู้คืนทรัพย์สินและการดำเนินงาน

การวิเคราะห์ผลกระทบทางธุรกิจหลัก (BIA : Business Impact Analysis)
อ้างอิง ISO/IEC 22301:2019



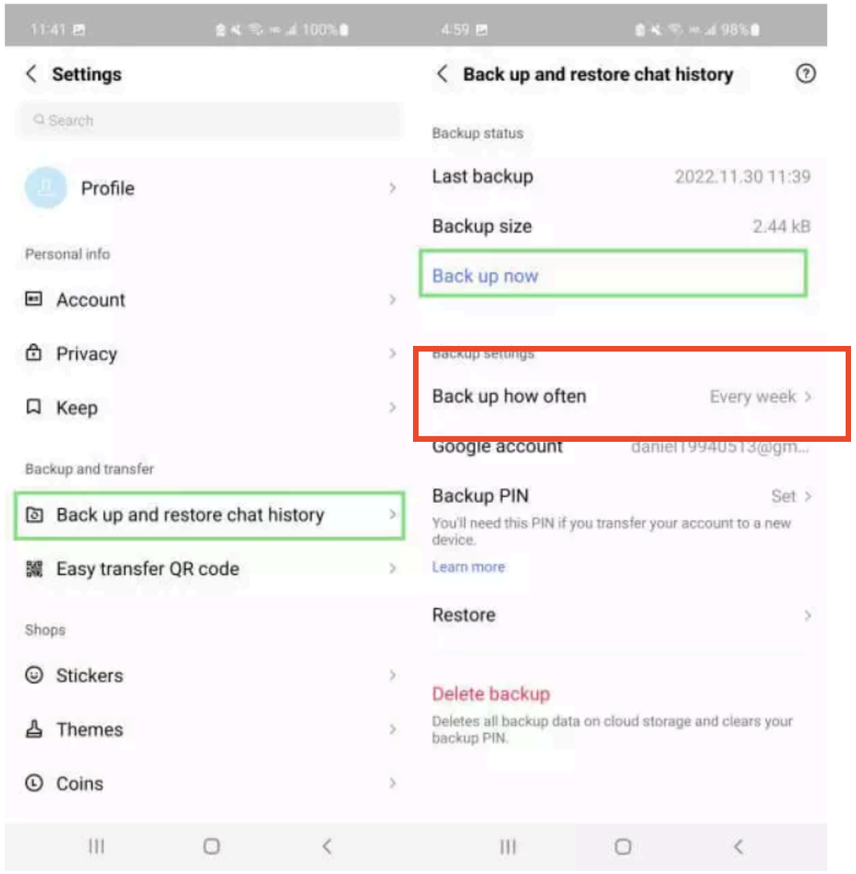
9 การกู้คืนทรัพย์สินและการดำเนินงาน

การวิเคราะห์ผลกระทบทางธุรกิจหลัก (BIA : Business Impact Analysis)
อ้างอิง ISO/IEC 22301:2019



9 การกู้คืนทรัพย์สินและการดำเนินงาน

ตัวอย่าง Back and Recovery Plan บน Digital Device ที่ใกล้ตัวทุกคน



Line : Instat Message

RPO (Recover Point Objective)

- Everyday
- Every 3 day
- Every week
- Every 2 weeks
- Every Month

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

9 การกู้คืนทรัพย์สินและการดำเนินงาน

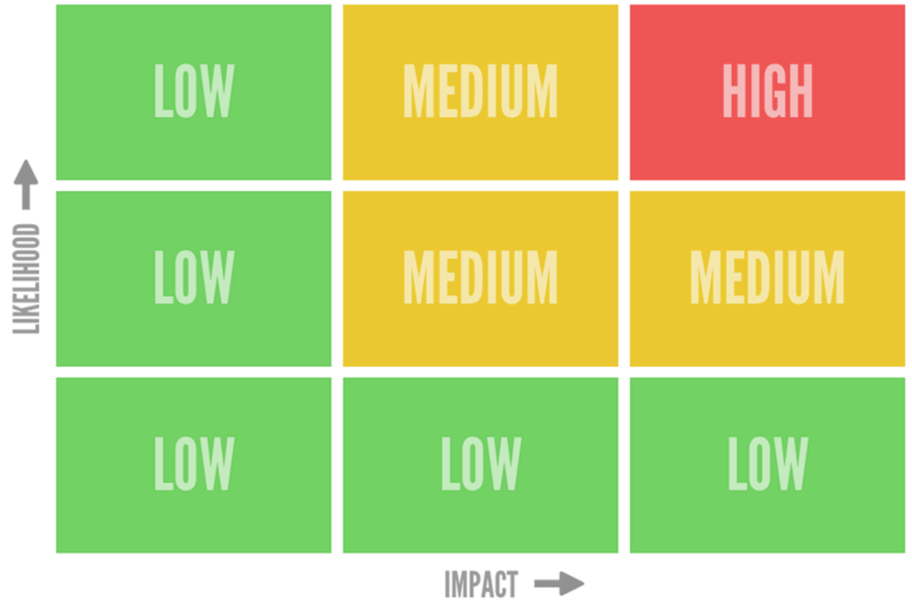
9.3 แผนฟื้นฟูภัยพิบัติ/แผนการกู้คืนจากภัยคุกคามทางไซเบอร์ (Disaster Recovery Plan - DRP)

ขั้นตอนในการวางแผนฟื้นฟูภัยพิบัติ

- ประเมินและจัดลำดับความสำคัญของความเสี่ยง

พิจารณาระดับความเสี่ยง(Risk) = ผลกระทบ (I) x โอกาสที่จะเกิดภัย (L)

- Impact : ผลกระทบ
- Likelihood : โอกาสที่จะเกิดภัย



9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.3 แผนฟื้นฟูภัยพิบัติ/แผนการกู้คืนจากภัยคุกคามทางไซเบอร์ (Disaster Recovery Plan - DRP)

ขั้นตอนในการวางแผนฟื้นฟูภัยพิบัติ

- พัฒนาแผนและขั้นตอนการกู้คืน

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.3 แผนฟื้นฟูภัยพิบัติ/แผนการกู้คืนจากภัยคุกคามทางไซเบอร์ (Disaster Recovery Plan - DRP)

ขั้นตอนในการวางแผนฟื้นฟูภัยพิบัติ

- ออกแบบและดำเนินการสำรองข้อมูล

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.3 แผนฟื้นฟูภัยพิบัติ/แผนการกู้คืนจากภัยคุกคามทางไซเบอร์ (Disaster Recovery Plan - DRP)

ขั้นตอนในการวางแผนฟื้นฟูภัยพิบัติ

- ทดสอบและปรับแผนการกู้คืน

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.4 การสำรองข้อมูล (Backup)

- ประเภทการสำรองข้อมูล
- กลยุทธ์การสำรองข้อมูล
- แนวทางปฏิบัติการสำรองข้อมูล

9 การกู้คืนทรัพย์สินและการดำเนินงาน

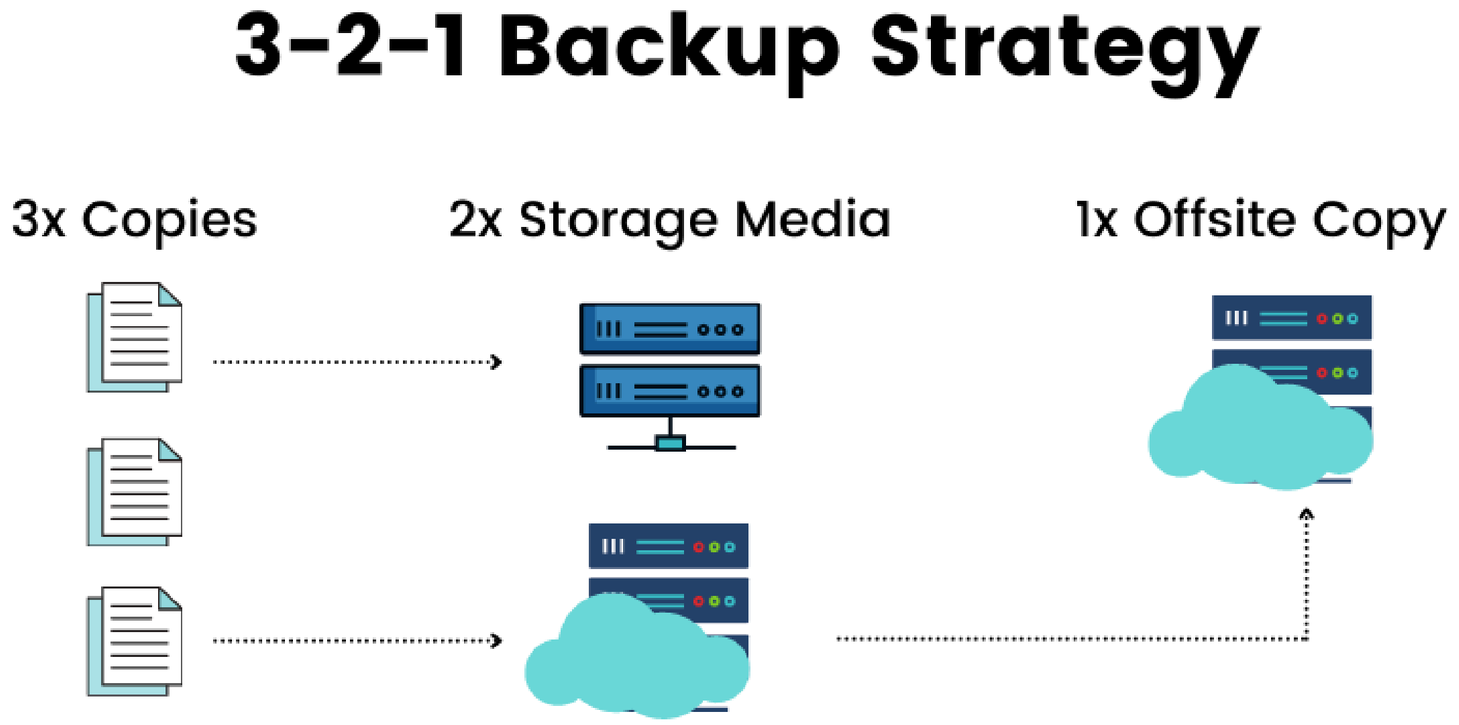
9.4 การสำรองข้อมูล (Backup)

- ประเภทการสำรองข้อมูล
  - การสำรองข้อมูลแบบเต็ม (Full Backup)
  - การสำรองข้อมูลส่วนเพิ่ม (Incremental Backup)
  - การสำรองข้อมูลที่แตกต่างกัน (Differential Backup)
  - การเลือกประเภทการสำรองข้อมูลที่เหมาะสม

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.4 การสำรองข้อมูล (Backup)

- กลยุทธ์การสำรองข้อมูล : การปรับใช้ 3-2-1 Backup Strategy



ข้อมูลจาก https://stonefly.com/blog/3-2-1-vs-3-2-1-1-0-vs-4-3-2-backup-strategies/

9 การกู้คืนทรัพย์สินและการดำเนินงาน

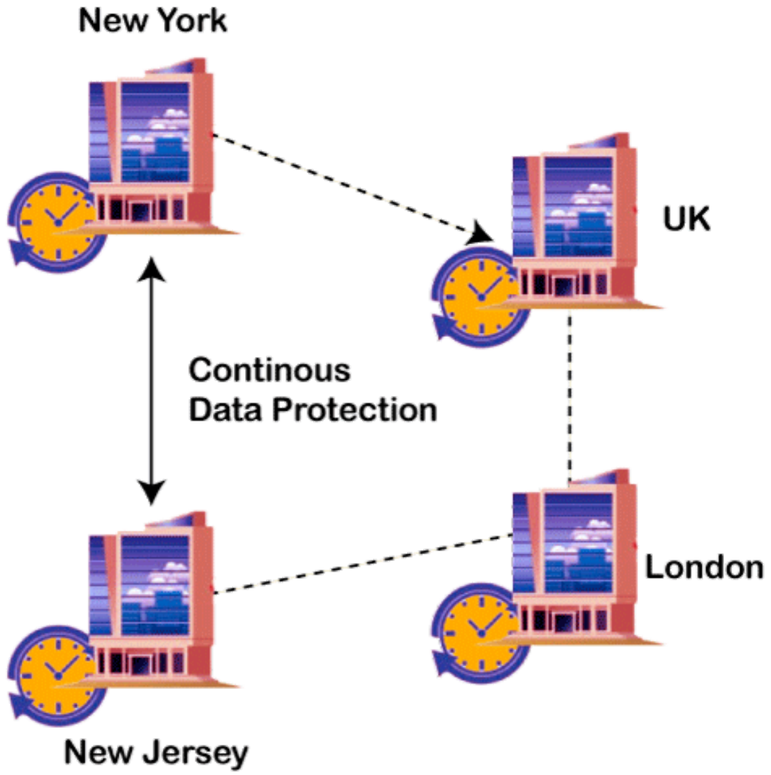
9.4 การสำรองข้อมูล (Backup)

- กลยุทธ์การสำรองข้อมูล : การปรับใช้ 3-2-1 Backup Strategy
  - การปกป้องข้อมูลอย่างต่อเนื่อง (Continuous Data Protection – CDP) และการลดความซ้ำซ้อนของข้อมูล (Deduplication)
  - บริการกู้คืนข้อมูล (Disaster Recovery as a Service – DRaaS)

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.4 การสำรองข้อมูล (Backup)

- กลยุทธ์การสำรองข้อมูล : การปรับใช้ 3-2-1 Backup Strategy
  - การปกป้องข้อมูลอย่างต่อเนื่อง (Continuous Data Protection – CDP)

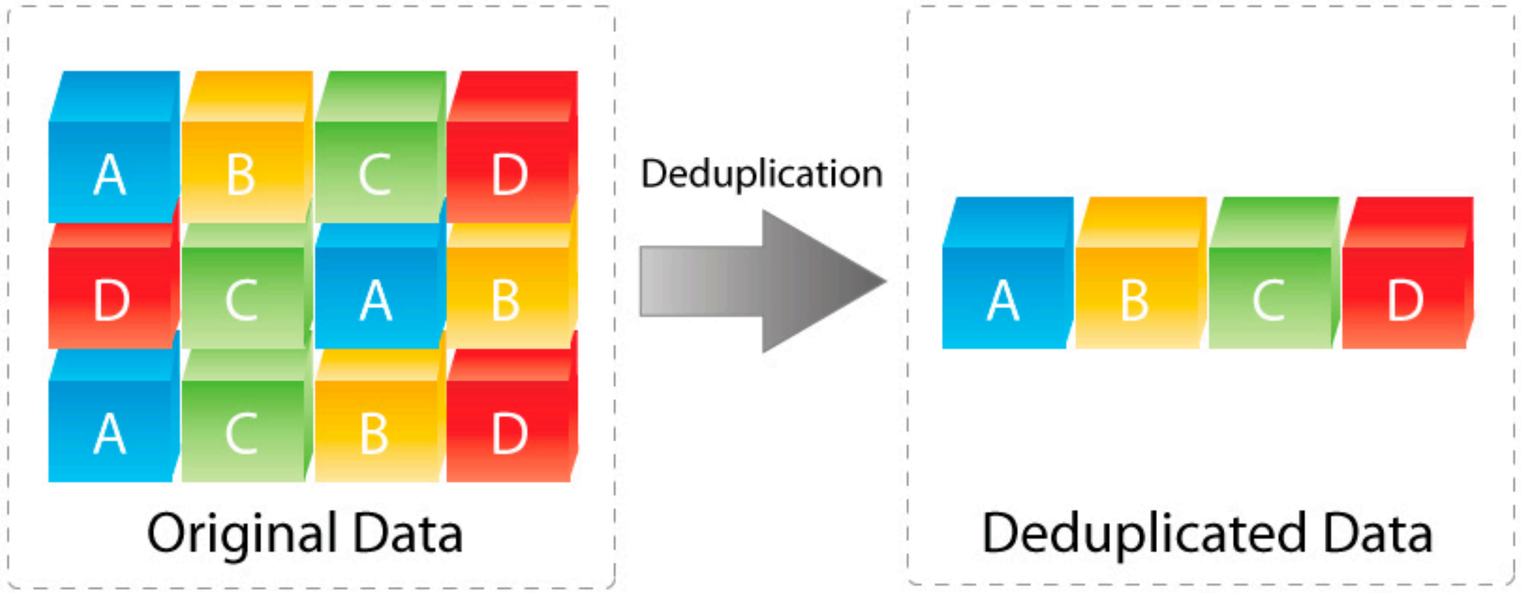


ข้อมูลจาก https://www.javatpoint.com/continuous-data-protection

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.4 การสำรองข้อมูล (Backup)

- กลยุทธ์การสำรองข้อมูล : การปรับใช้ 3-2-1 Backup Strategy
  - การลดความซ้ำซ้อนของข้อมูล (Deduplication)

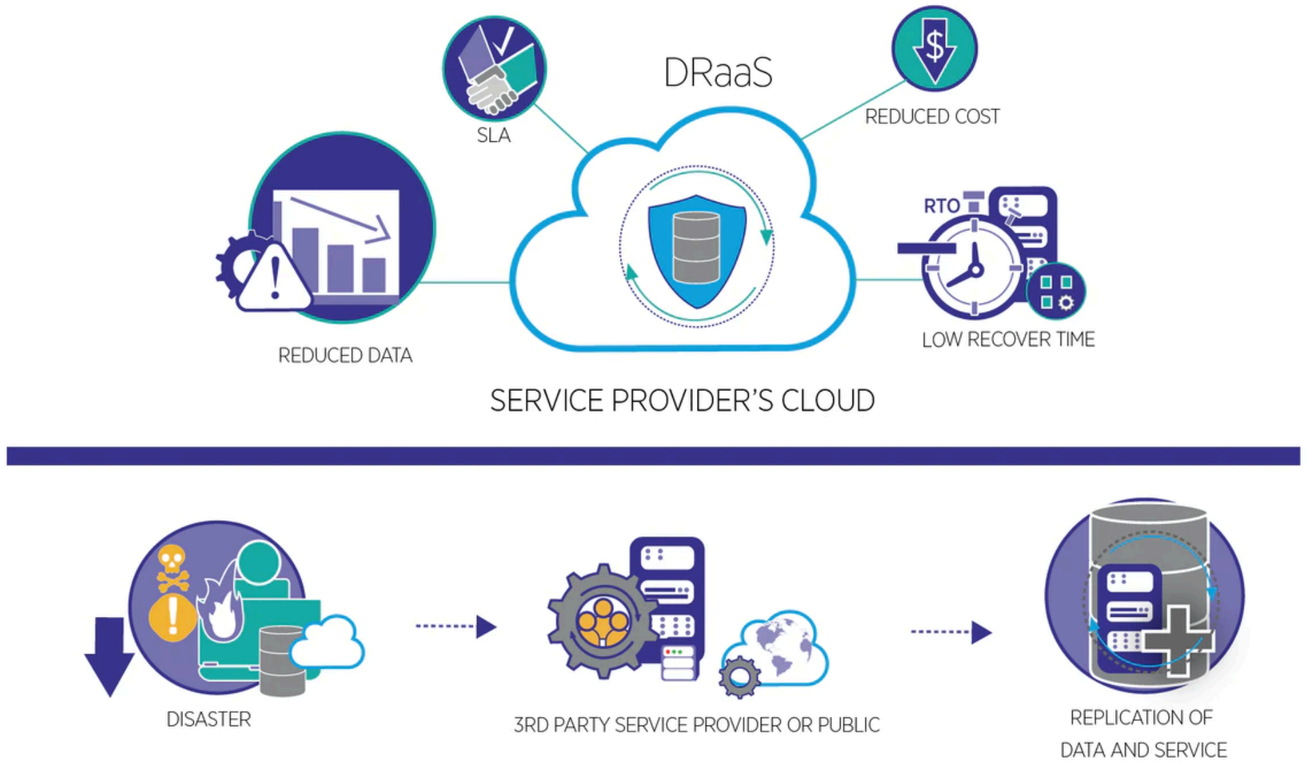


ข้อมูลจาก https://www.hsb.nl/the-importance-of-deduplication/

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.4 การสำรองข้อมูล (Backup)

- กลยุทธ์การสำรองข้อมูล : การปรับใช้ 3-2-1 Backup Strategy
  - บริการกู้คืนข้อมูล (Disaster Recovery as a Service – DRaaS)



ข้อมูลจาก https://www.rubrik.com/insights/what-is-disaster-recovery-as-a-service/

9 การกู้คืนทรัพย์สินและการดำเนินงาน

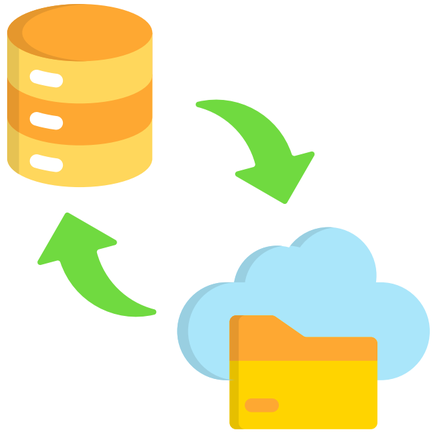
9.4 การสำรองข้อมูล (Backup)

- แนวทางปฏิบัติการสำรองข้อมูล
  - กำหนดกรอบโครงสร้างและกลยุทธ์การสำรองข้อมูล
  - ระบุข้อมูลใดคือทรัพย์สินที่สำคัญ
  - ดำเนินกาสำรองข้อมูล ตามกลยุทธ์ที่กำหนด
  - จัดเก็บ/เฝ้าระวัง สื่อบันทึกข้อมูล ตามกลยุทธ์ที่กำหนด
  - ทดสอบการกู้คืนสภาพข้อมูล ระยะเวลาและความถี่ตามกลยุทธ์ที่กำหนด
  - ทบทวนแนวทางปฏิบัติการสำรองข้อมูลและพัฒนาอย่างต่อเนื่อง

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.5 แหล่งกู้คืนภัยพิบัติ (Disaster Recovery Sites)

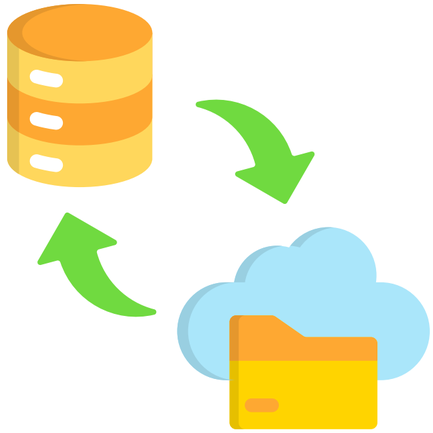
- Hot site
- Cold site
- Warm site
- ปัจจัยที่ส่งผลต่อการเลือกประเภทแหล่งการกู้คืนภัยพิบัติ
- การเลือกสถานที่ตั้งของแหล่งกู้คืนภัยพิบัติ



9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.5 แหล่งกู้คืนภัยพิบัติ (Disaster Recovery Sites)

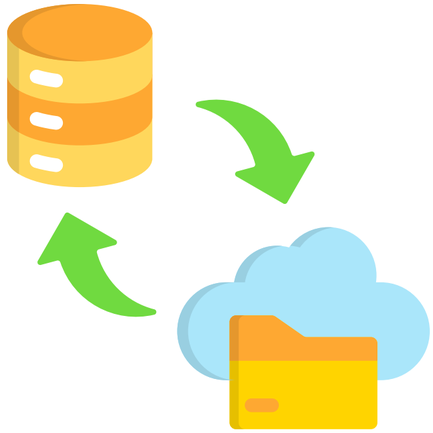
- Hot site
  - Hardware , Software , Network , Human Resource , Knowledge
  - Distance
  - Fast Recovery



9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.5 แหล่งกู้คืนภัยพิบัติ (Disaster Recovery Sites)

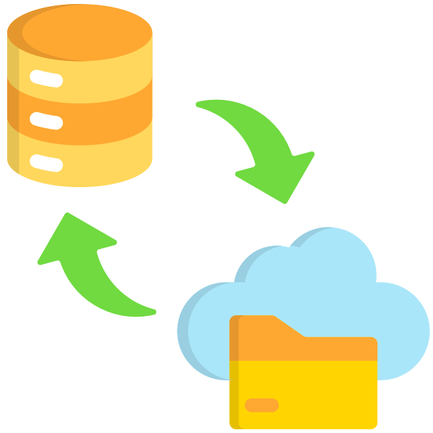
- Cold site
  - Resource Limit
  - Facility Limit
  - Slow Recovery



9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.5 แหล่งกู้คืนภัยพิบัติ (Disaster Recovery Sites)

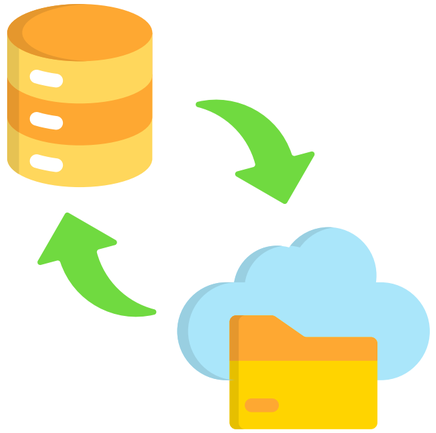
- Warm site
  - Normal Resource
  - Normal Facility
  - Normal Recovery



9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.5 แหล่งกู้คืนภัยพิบัติ (Disaster Recovery Sites)

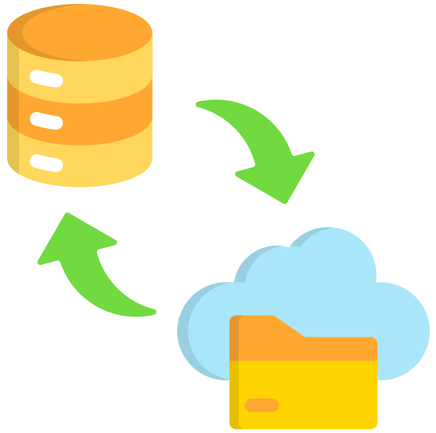
- ปัจจัยที่ส่งผลต่อการเลือกประเภทแหล่งการกู้คืนภัยพิบัติ
  - เวลา (Time)
  - สิ่งที่สำคัญต่อธุรกิจหรือองค์กร (Business or Organization Priorities)
  - งบประมาณ (Budget)



9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.5 แหล่งกู้คืนภัยพิบัติ (Disaster Recovery Sites)

- การเลือกสถานที่ตั้งของแหล่งกู้คืนภัยพิบัติ
  - ระดับความสำคัญของข้อมูล
  - ระยะเวลากู้คืนสภาพที่กำหนดไว้
  - งบประมาณ
  - ระยะทาง



9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.6 แผนการสื่อสารช่วงกู้คืนภัยพิบัติ (Disaster Recovery Communication Plan)

- ทำการสำรองข้อมูล (Data backups)
- สร้างทีมการสื่อสาร (Create Communication Team)
- การเข้าใจความสำคัญของการรายงานสิ่งจำเป็นต่อผู้มีส่วนได้ส่วนเสีย
- การคิดค้นกลยุทธ์การสื่อสาร
- การรวมข้อความสื่อสารเป็นหนึ่งเดียว
- การทดสอบแผนการสื่อสาร
- ขั้นตอนปฏิบัติสำหรับการสื่อสารไปยังผู้ที่เกี่ยวข้อง

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.6 แผนการสื่อสารช่วงกู้คืนภัยพิบัติ (Disaster Recovery Communication Plan)

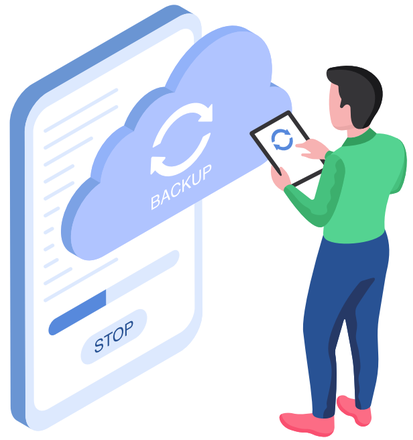
- ทำการสำรองข้อมูล (Data backups)

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.6 แผนการสื่อสารช่วงกู้คืนภัยพิบัติ (Disaster Recovery Communication Plan)

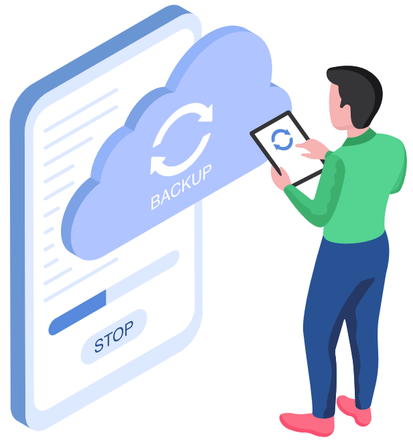
- สร้างทีมการสื่อสาร (Create Communication Team)
  - ควรกำหนดหน้าที่ความรับผิดชอบสมาชิกในทีม
  - กำหนดให้มีช่องทางติดต่อสมาชิกในทีมมากกว่า 1 ช่องทาง
  - ควรมีตารางที่มีชื่อ เบอร์โทร และช่องทางการติดต่ออื่นของสมาชิกในทีมทุกคน เพื่อสะดวกรวดเร็วในการสื่อสารกรณีเกิด Incident ขึ้น



9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.6 แผนการสื่อสารช่วงกู้คืนภัยพิบัติ (Disaster Recovery Communication Plan)

- การเข้าใจความสำคัญของการรายงานสิ่งจำเป็นต่อผู้มีส่วนได้ส่วนเสีย
  - ข้อมูลเกี่ยวกับสถานการณ์ปัจจุบัน
  - แผนการฟื้นฟู และระยะเวลาในการคืนสภาพให้ใช้งานได้ดังเดิม



9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.6 แผนการสื่อสารช่วงกู้คืนภัยพิบัติ (Disaster Recovery Communication Plan)

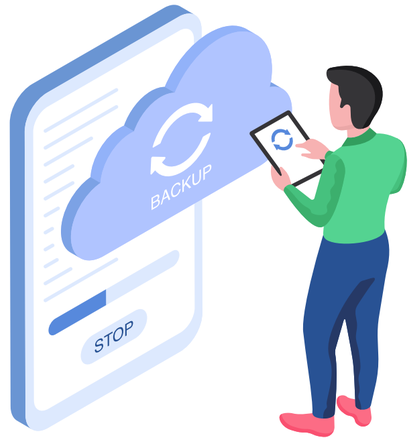
- การคิดค้นกลยุทธ์การสื่อสาร
  - ใครคือผู้สั่งการ (Commander)
  - ใครคือทำหน้าที่ประสานงาน (Co-Ordinator)
  - ใครคือทำหน้าที่ผู้สื่อสารหลัก (Communicator)
  - ต้องการความช่วยเหลือจากใคร/หน่วยงานใดบ้าง (Cooperation)

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.6 แผนการสื่อสารช่วงกู้คืนภัยพิบัติ (Disaster Recovery Communication Plan)

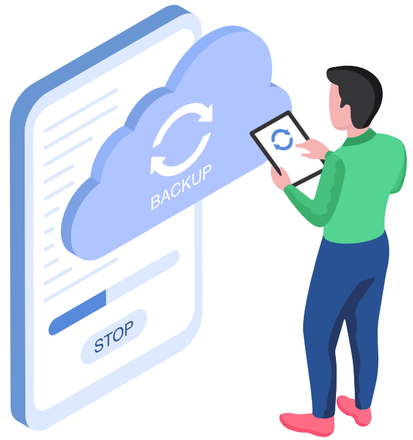
- การรวมข้อความสื่อสารเป็นหนึ่งเดียว
  - มี Dialog ในการสื่อสารที่ชัดเจนเข้าใจง่าย สำหรับผู้มีส่วนได้เสียแต่ละระดับ
  - สื่อสารรายละเอียดที่จำเป็นเท่านั้น
  - มีการแถลงข่าวอย่างเป็นทางการ



9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.6 แผนการสื่อสารช่วงกู้คืนภัยพิบัติ (Disaster Recovery Communication Plan)

- การทดสอบแผนการสื่อสาร
  - ทดสอบตามแผนกลยุทธ์ความต่อเนื่องทางธุรกิจ (BCP Strategy) ความถี่และระยะเวลา ตามที่กำหนดไว้ในแผน
  - ทบทวนแผนการสื่อสาร
  - นำผลการทดสอบมาพัฒนาปรับปรุงอย่างต่อ



9 การกู้คืนทรัพย์สินและการดำเนินงาน

9.6 แผนการสื่อสารช่วงกู้คืนภัยพิบัติ (Disaster Recovery Communication Plan)

- ขั้นตอนปฏิบัติสำหรับการสื่อสารไปยังผู้ที่เกี่ยวข้อง
  - อยู่ในอาการที่สงบเมื่อทำการสื่อสารไปยังผู้ที่เกี่ยวข้อง
  - หลีกเลี่ยงการสนทนาที่ยาวนานโดยไม่จำเป็น
  - กรณีที่ติดต่อบุคคลตามที่กำหนดไว้ไม่ได้ให้ดำเนินการดังนี้
    - กรณีมีผู้รับสายแทน
    - ทิ้งข้อความไว้เพื่อให้ติดต่อกลับ
    - บันทึกข้อมูลที่เกี่ยวข้องกับการติดต่อนั้น

9 การกู้คืนทรัพย์สินและการดำเนินงาน

สรุปบทเรียน : การกู้คืนทรัพย์สินและการดำเนินงาน

- มุ้งเน้นที่การฟื้นฟูระบบและข้อมูลให้กลับมาใช้งานได้ตามปกติอย่างรวดเร็ว
- รักษาความต่อเนื่องในการดำเนินธุรกิจขององค์กร
  - การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA)
  - การประเมินความเสี่ยง (Risk Assessment – RA)
  - การวางแผนฟื้นฟู (Disaster Recovery Plan : DRP)
  - การทดสอบแผนฟื้นฟู (Disaster Recovery Plan Test)
  - สำรองข้อมูล (Backup)
  - การจัดเตรียมแหล่งกู้คืนภัยพิบัติ (Disaster Recovery Sites)

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ดร.สุรเชษฐ์ สุชัยยะ
ผู้อำนวยการ
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ (CIPAT)

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.1 กลยุทธ์การบรรเทาความเสี่ยง (Risk Mitigation)

10.2 การควบคุมความเสี่ยง (Risk Control)

10.3 มาตรการควบคุมด้านเทคนิค (Technical Controls)

10.4 มาตรการควบคุมด้านการบริหารจัดการ (Administrative Controls)

10.5 มาตรการควบคุมด้านกายภาพ (Physical Controls)

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

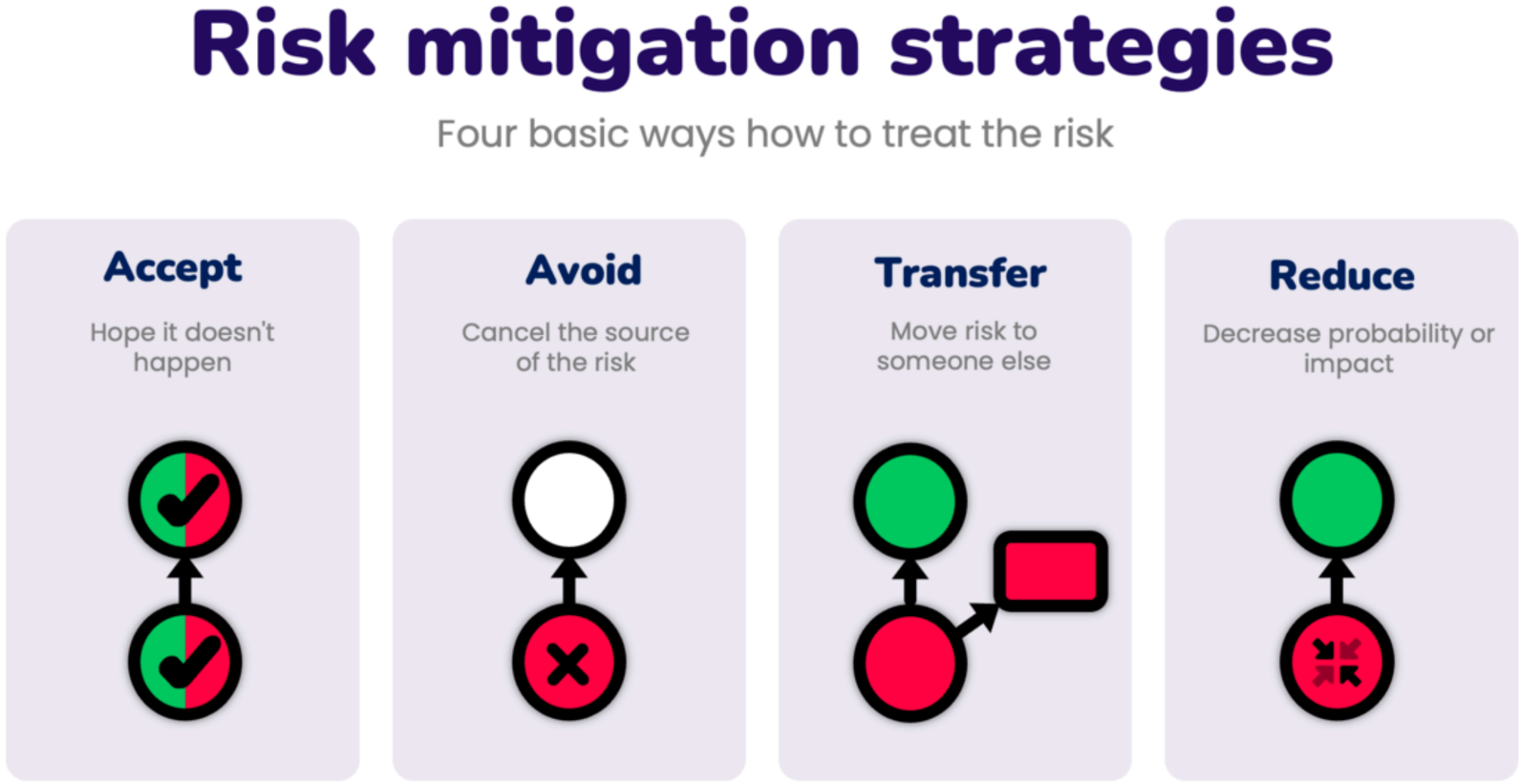
10.1 กลยุทธ์การลดความเสี่ยง (Risk Mitigation)

- วิธีการวางกลยุทธ์การลดความเสี่ยง
- ประเมินโอกาสเกิดและผลกระทบ

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.1 กลยุทธ์การบรรเทาความเสี่ยง (Risk Mitigation)

- วิธีการวางกลยุทธ์การบรรเทาดความเสี่ยง



10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.1 กลยุทธ์การบรรเทาความเสี่ยง (Risk Mitigation)

- ประเมินโอกาสเกิดและผลกระทบ
  - จัดทำโครงร่างของความเสี่ยง (Risk Profile)
  - เปรียบเทียบความเสี่ยงกับระดับความเสี่ยงที่องค์กรยอมรับได้
  - วิเคราะห์ต้นทุนและประโยชน์จากการจัดการความเสี่ยง
  - ระบุความต้องการของโครงการหรือระบบงาน
  - ประเมินผลการวิเคราะห์ความเสี่ยงก่อนการตัดสินใจดำเนินการ
  - การทำประกันภัย (Insurance)
  - การฝึกอบรมและสร้างความตระหนัก (Training and Awareness)

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.2 การควบคุมความเสี่ยง (Risk Control)

- การควบคุมเชิงป้องกัน (Preventive Controls)
- การควบคุมเชิงตรวจจับ (Detective Controls)
- การควบคุมเชิงแก้ไข

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.2 การควบคุมความเสี่ยง (Risk Control)

- การควบคุมเชิงป้องกัน (Preventive Controls)
  - การใช้มาตรการควบคุมการเข้าถึง (Access Control)
  - การใช้ซอฟต์แวร์ป้องกันไวรัสและมัลแวร์(Antivirus/Antimalware Software)

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.2 การควบคุมความเสี่ยง (Risk Control)

- การควบคุมเชิงตรวจจับ (Detective Controls)
  - การตรวจสอบระบบ (System Monitoring)
  - การบันทึกและตรวจสอบเหตุการณ์(Event Logging and Monitoring)
  - การใช้ระบบตรวจจับการบุกรุก (Intrusion Detection System - IDS)

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

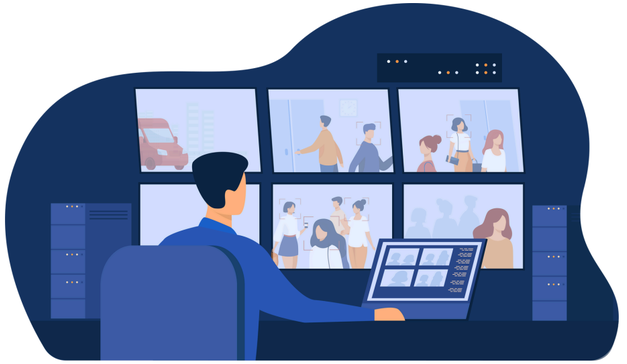
10.2 การควบคุมความเสี่ยง (Risk Control)

- การควบคุมเชิงแก้ไข
  - การกู้คืนระบบ (System Recovery)
  - การปรับปรุงมาตรการความมั่นคงปลอดภัย (Security Updates)
  - การวิเคราะห์เหตุการณ์ (Incident Analysis)

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.3 มาตรการควบคุมด้านเทคนิค (Technical Controls)

- ไฟร์วอลล์(Firewall)
- ระบบตรวจจับการบุกรุก (Intrusion Detection System - IDS)
- ระบบป้องกันไวรัส (Antivirus Systems)
- การเข้ารหัส (Encryption)



10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.3 มาตรการควบคุมด้านเทคนิค (Technical Controls)

- ไฟร์วอลล์(Firewall)
  - Statefull inspection
  - Proxy Services
  - Deep Packet Inspection
  - Advanced Threat Protection
  - Identity-Based Access Control
  - Secure VPN Support
  - AI & Cloud Integration
  - Real-Time Monitoring and Analytics

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

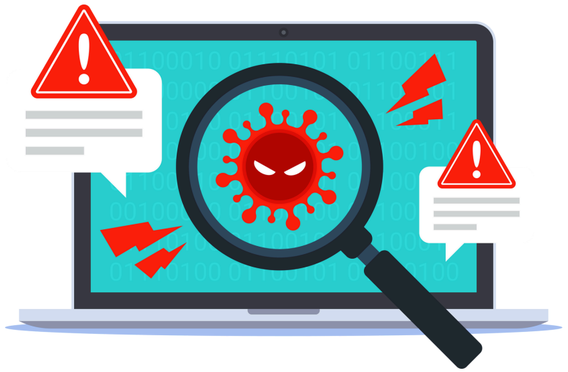
10.3 มาตรการควบคุมด้านเทคนิค (Technical Controls)

- ระบบตรวจจับการบุกรุก (Intrusion Detection System - IDS)
  - Deep Packet Inspection - DPI
  - Signature-Based Detection
  - Network-Based and Host-Based Detection
  - Policy Management and Customization
  - Alerting and Reporting
  - Real-Time Detection
  - Post-Incident Analysis

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.3 มาตรการควบคุมด้านเทคนิค (Technical Controls)

- ระบบป้องกันไวรัส (Antivirus Systems)



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.3 มาตรการควบคุมด้านเทคนิค (Technical Controls)

- การเข้ารหัส (Encryption)
  - SSL/TLS

ข้อมูลจาก https://medium.com/@jayampathiadhikari/ssl-tls-simplified-c3c1f08051b2

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.4 มาตรการควบคุมด้านการบริหารจัดการ (Administrative Controls)

- นโยบายและขั้นตอน (Policies and Procedures)
- การฝึกอบรมและสร้างความตระหนัก (Training and Awareness)
- การตรวจสอบและประเมิน (Audit and Assessment)

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.4 มาตรการควบคุมด้านการบริหารจัดการ (Administrative Controls)

- นโยบายและขั้นตอน (Policies and Procedures)
  - ลักษณะของนโยบายและขั้นตอนสำหรับมาตรการควบคุมด้านการบริหารจัดการ(Characteristics of Policies and Procedures)
  - การพัฒนานโยบายและขั้นตอน (Policy and Procedure Development):การฝึกอบรมและสร้างความตระหนัก (Training and Awareness)

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

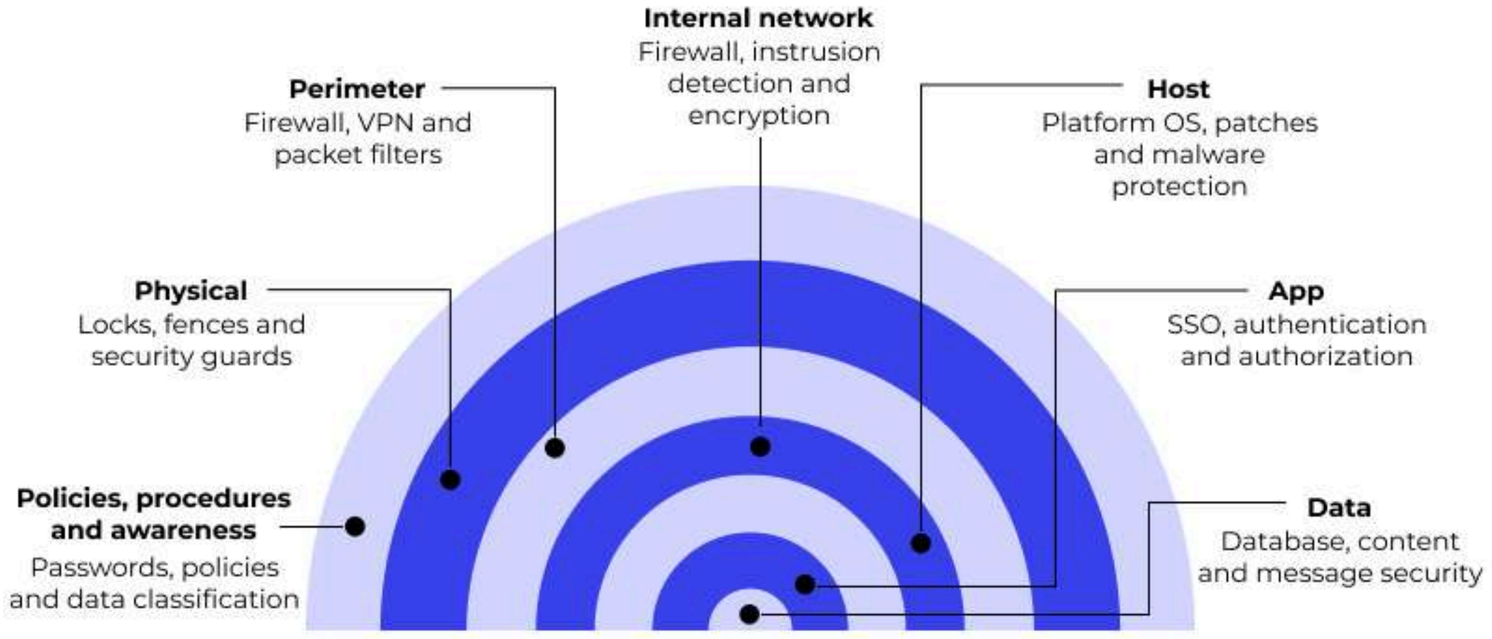
10.4 มาตรการควบคุมด้านการบริหารจัดการ (Administrative Controls)

- การฝึกอบรมและสร้างความตระหนัก (Training and Awareness)
  - การฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ
  - โปรแกรมสร้างความตระหนัก

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.4 มาตรการควบคุมด้านการบริหารจัดการ (Administrative Controls)

- การฝึกอบรมและสร้างความตระหนัก (Training and Awareness)



Elements of Defense in Depth (DiD)

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลจาก https://www.wallarm.com/what/defense-in-depth-concept

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.4 มาตรการควบคุมด้านการบริหารจัดการ (Administrative Controls)

- การตรวจสอบและประเมิน (Audit and Assessment)
  - การตรวจสอบภายใน (Internal Audit)
  - การประเมินความเสี่ยง (Risk Assessment)

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.5 มาตรการควบคุมด้านกายภาพ (Physical Controls)

- ระบบควบคุมการเข้าออก (Access Control Systems)
- กล้องวงจรปิด (CCTV)
- ระบบป้องกันอัคคีภัย (Fire Protection Systems)

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

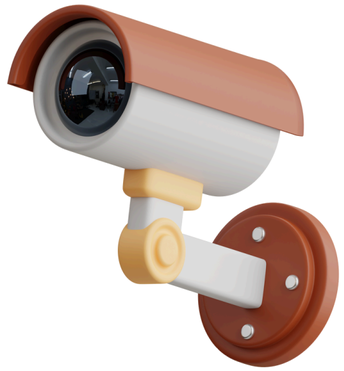
10.5 มาตรการควบคุมด้านกายภาพ (Physical Controls)

- ระบบควบคุมการเข้าออก (Access Control Systems)
  - การใช้บัตรผ่าน (Access Cards)
  - การใช้รหัสผ่าน (PIN)
  - การใช้ระบบสแกนลายนิ้วมือหรือใบหน้า (Biometric Systems)

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.5 มาตรการควบคุมด้านกายภาพ (Physical Controls)

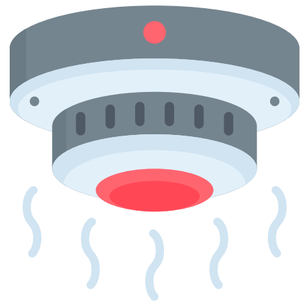
- กล้องวงจรปิด (CCTV)
  - การติดตั้งกล้องวงจรปิดในบริเวณที่มีความเสี่ยงสูง
  - การตรวจสอบภาพจากกล้องวงจรปิด
  - การบันทึกภาพจากกล้องวงจรปิด

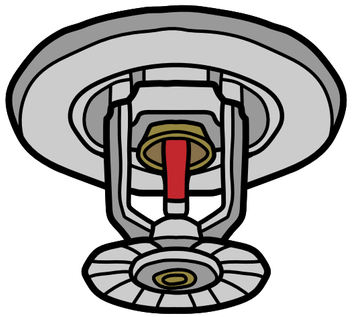


10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

10.5 มาตรการควบคุมด้านกายภาพ (Physical Controls)

- ระบบป้องกันอัคคีภัย (Fire Protection Systems)
  - การติดตั้งระบบดับเพลิงอัตโนมัติ (Automatic Fire Suppression Systems)
  - การติดตั้งเครื่องตรวจจับควัน (Smoke Detectors)
  - การติดตั้งระบบพ่นน้ำ (Sprinkler Systems)




CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

10 การนำกลยุทธ์การลดความเสี่ยงไปใช้

สรุปบทเรียน : การนำกลยุทธ์การลดความเสี่ยงไปใช้

- กลยุทธ์การบรรเทาความเสี่ยง (Risk Mitigation)
- การควบคุมความเสี่ยง (Risk Control)
- มาตรการควบคุมด้านเทคนิค (Technical Controls)
- มาตรการควบคุมด้านการบริหารจัดการ (Administrative Controls)
- มาตรการควบคุมด้านกายภาพ (Physical Controls)

สรุปและตอบคำถาม

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

Questions & Answer

www.MySurachet.com

085 636 2551

surachet@catinfonet.com

Thank you

LINE

LINE