รายงานการเข้าร่วมโครงการเอพีโอ

15-IN-08-GE-TRC-B

Training Course on Information Security Management System Based on ISO 27000

ระหว่างวันที่ 11-15 พฤษภาคม 2558

ณ กรุงจาการ์ตา ประเทศอินโดนีเซีย

จัดทำโดย นายไพโรจน์ แสงสุทธิจริตกุล

หัวหน้าแผนกโครงสร้างเทคโนโลยีสารสนเทศ ส่วนเทคโนโลยีสารสนเทศ สถาบันเพิ่มผลผลิตแห่งชาติ

วันที่ 16 กรกฎาคม 2558

ส่วนที่ 1 ข้อมูลทั่วไปของโครงการ

1.1 รหัสและชื่อโครงการ

15-IN-08-GE-TRC-B: Training Course on Information Security Management System Based on ISO 27000

1.2 ระยะเวลา

5 วัน ตั้งแต่วันที่ 11 ถึงวันที่ 15 พฤษภาคม 2558

1.3 สถานที่จัด

กรุงจาการ์ตา ประเทศอินโดนีเซีย

1.4 ชื่อเจ้าหน้าที่ APO ประจำโครงการ

Mr. Muhammad Idham (Program officer, APO)

Ms. Ratna Kurniasari (NPO Indonesia)

1.5 จำนวนและรายชื่อวิทยากรบรรยาย

วิทยากรบรรยาย ทั้งหมด 3 ท่าน

1. Mr. Siddharth Sharma
2. Mr. Lizuan Latif
3. Mr. Mohd Nazim Harun

1.6 จำนวนผู้เข้าร่วมโครงการและประเทศที่เข้าร่วมโครงการ

จำนวนผู้เข้าร่วมโครงการ ทั้งหมด 20 ท่าน จาก 14 ประเทศ ได้แก่ สาธารณรัฐประชาชนบังคลาเทศ (2 ท่าน), ราชอาณาจักรกัมพูชา (2 ท่าน), สาธารณรัฐฟิจิ (2 ท่าน), สาธารณรัฐอิสลามอิหร่าน (1 ท่าน), สาธารณรัฐอินเดีย (1 ท่าน), สาธารณรัฐอินโดนีเซีย (2 ท่าน), สาธารณรัฐประชาธิปไตยประชาชนลาว (1 ท่าน),สาธารณรัฐมองโกเลีย (1 ท่าน), สหพันธ์สาธารณรัฐประชาธิปไตยเนปาล (1 ท่าน), สาธารณรัฐอิสลามปากีสถาน (1 ท่าน), สาธารณรัฐฟิลิปปินส์ (2 ท่าน),สาธารณรัฐสังคมนิยมประชาธิปไตยศรีลังกา (1 ท่าน), ราชอาณาจักรไทย (2 ท่าน) และสาธารณรัฐสังคมนิยมเวียดนาม (1 ท่าน)

ส่วนที่ 2 เนื้อหา/องค์ความรู้จากการเข้าร่วมโครงการ

2.1 เนื้อหา / องค์ความรู้ที่ได้จากการฟังบรรยาย

หัวข้อ Introduction to Information Security Management System ISO/IEC 27001:2013 Concept and Fundamental

บรรยายโดย Mr. Siddharth Sharma

ความมั่นคงปลอดภัยสารสนเทศ

- ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศเป็นเพียง 50% ของ ความมั่นคงปลอดภัยสารสนเทศ
- ความมั่นคงปลอดภัยสารสนเทศประกอบด้วยสามด้าน ได้แก่
  (1) ด้านกายภาพ ตัวอย่างความเสี่ยงที่เป็นไปได้ เช่น ภัยธรรมชาติ
  (2) ด้านเทคนิค ตัวอย่างความเสี่ยงที่เป็นไปได้ เช่น การล้มเหลวของระบบสารสนเทศและระบบเครือข่าย การโจมตีโดยไวรัสคอมพิวเตอร์
  (3) ด้านการบริหารจัดการ ตัวอย่างความเสี่ยงที่เป็นไปได้ เช่น การขาดความรู้เกี่ยวกับระบบสารสนเทศ การขาดคู่มือการใช้งาน
- วัตถุประสงค์หลักของความมั่นคงปลอดภัยสารสนเทศ คือ ป้องกันความเสี่ยงที่เป็นไปได้ทั้งหมดที่เกี่ยวข้องกับข้อมูลสารสนเทศ (ทั้งที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และ ไม่เกี่ยวข้อง)

การควบคุมความปลอดภัย

- การควบคุมความปลอดภัยเป็นมาตรการปกป้องเพื่อหลีกเลี่ยง ตอบโต้ หรือ ลดความเสี่ยงด้านความปลอดภัยที่เกี่ยวกับทรัพย์สินส่วนบุคคลหรือทรัพย์สินองค์กรให้น้อยที่สุด
- การควบคุมความปลอดภัยแบบเป็นสามหมวดหลัก ได้แก่
  (1) การควบคุมด้านกายภาพ
  (2) การควบคุมด้านเทคนิค
  (3) การควบคุมด้านบริหารจัดการ

การควบคุมด้านกายภาพ

- การควบคุมด้านกายภาพเป็นการจัดเตรียมมาตรการรักษาความปลอดภัยที่พร้อมใช้งานภายใต้รูปแบบโครงสร้างที่มีการกำหนดไว้ เพื่อจุดประสงค์สำหรับใช้ป้องกันการเข้าถึงข้อมูลที่มีความสำคัญโดยไม่ได้รับอนุญาต
- ตัวอย่างของการควบคุมด้านกายภาพ
  (1) การใช้กล้องวงจรปิด
  (2) ระบบแจ้งเตือนโดยการตรวจจับการเคลื่อนไหวหรือตรวจจับความร้อน
  (3) เจ้าหน้าที่รักษาความปลอดภัย

(4) การใช้บัตรรูปภาพ

(5) ประตูเหล็กพร้อมกุญแจลิ้นตาย

(6) ระบบตรวจจับทางชีวภาพ เช่น การตรวจลายนิ้วมือ เสียง ใบหน้า ม่านตา ลายมือ และ วิธีการแบบอัตโนมัติอื่นๆที่ใช้สำหรับจดจำความเป็นตัวตน

การควบคุมด้านการบริหารจัดการ

- เป็นการควบคุมที่มองไปถึงปัจจัยด้านตัวบุคคลที่มีผลต่อความปลอดภัย
- ตัวอย่างของการควบคุมด้านการบริหารจัดการ
  (1) นโยบายทางด้านเทคโนโลยีสารสนเทศสำหรับผู้ใช้งาน นโยบายในการเข้าใช้งาน
  (2) การฝึกอบรมและสร้างความตะหนักรู้
  (3) การเตรียมความพร้อมสำหรับภัยพิบัติและแผนการกู้คืนระบบ
  (4) การสรรหาพนักงานและกลยุทธ์การแบ่งแยกงาน

การควบคุมด้านเทคนิค

- การควบคุมทางด้านเทคนิคใช้เทคโนโลยีเป็นหลักพื้นฐานในการควบคุมการเข้าถึงและการใช้งานข้อมูลสำคัญที่อยู่บนโครงสร้างทางกายภาพและอยู่ในระบบเครือย่าย
- ตัวอย่างของการควบคุมทางด้านเทคนิค
  (1) บัญชีและรหัสผ่านของระดับผู้ใช้งาน
  (2) การเข้ารหัสข้อมูล
  (3) Smart card
  (4) ระบบยืนยันตัวตนเพื่อเข้าเครือข่าย

องค์ประกอบที่สำคัญของความมั่นคงปลอดภัยสารสนเทศ

ISO 27001 มุ่งเน้นไปที่การป้องกันในเรื่องของ

- ความลับของข้อมูลสารสนเทศ (Confidentiality)
- ความถูกต้องของข้อมูลสารสนเทศ (Integrity)
- ความพร้อมใช้ของข้อมูลสารสนเทศ (Availability)

คำจำกัดความของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ(Information Security Management System หรือ ISMS)

ISMS เป็น Framework ของนโยบายและวิธีปฏิบัติซึ่งรวมไปถึงการควบคุมด้านกายภาพ การควบคุมด้านเทคนิค และ การควบคุมด้านการบริหารจัดการ ทั้งหมดที่เกี่ยวข้องกับกระบวนการบริหารความเสี่ยงสำหรับข้อมูลสารสนเทศขององค์กร

ข้อเท็จจริงพื้นฐาน

- ISO 27001 เป็นมาตรฐานสากลที่เผยแพร่โดย International Standardization Organization (ISO)
- ISO 27001 อธิบายถึง วิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในองค์กร
- ISO 27001 สามารถนำมาประยุกต์ใช้งานจริงในองค์กรได้ทุกรูปแบบ ไม่ว่าจะเป็น องค์กรแสวงหากำไรหรือไม่แสวงหากำไร องค์กรเอกชนหรือองค์กรภาครัฐ องค์กรขนาดเล็กหรือองค์กรขนาดใหญ่

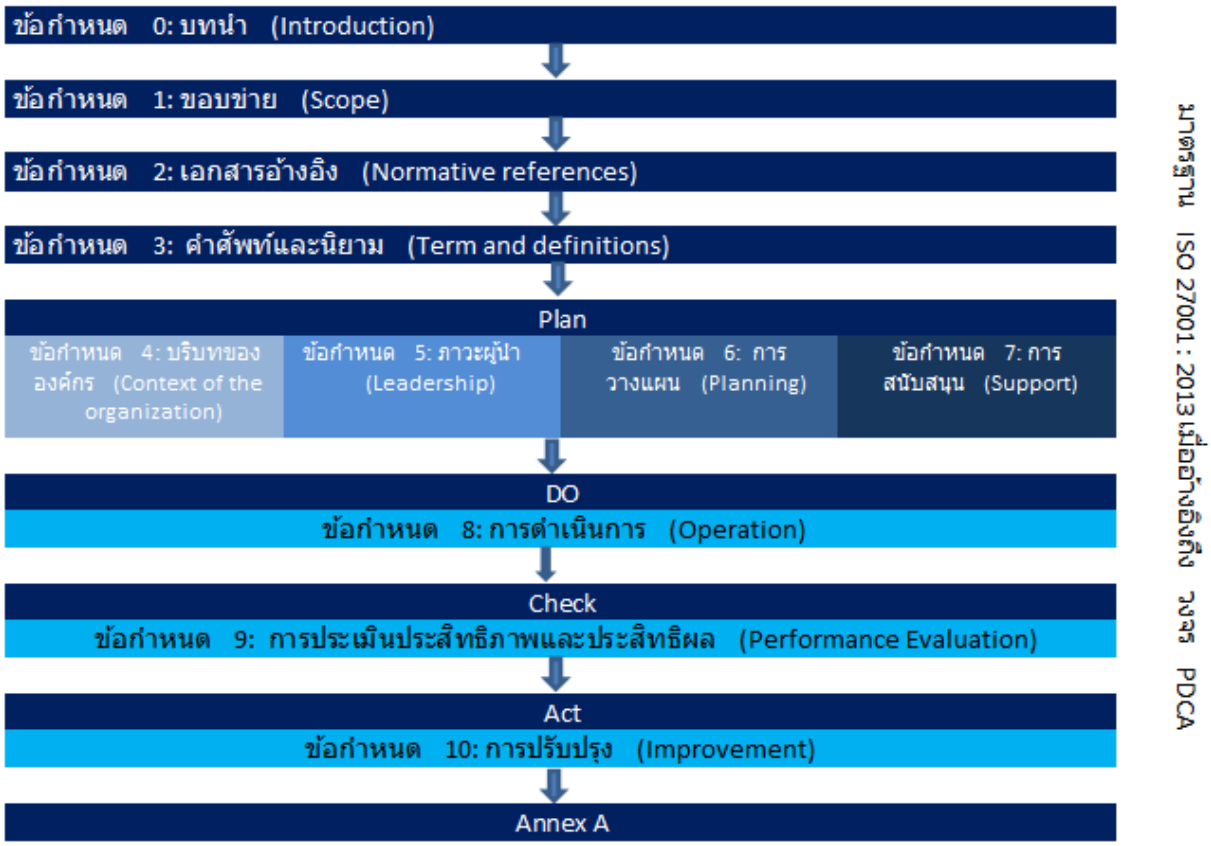
ปรัชญาของ ISO 27001

- ทรัพย์สินด้านข้อมูลสารสนเทศขององค์กรต้องได้รับการประเมินความเสี่ยงทั้งหมด
- มีการเลือกตัวควบคุมที่เหมาะสมสำหรับกำจัดหรือลดความเสี่ยงเหล่านั้นให้เหลือน้อยที่สุด

ความแตกต่างที่สำคัญ ของ ISO 27001:2013 กับ ISO 27001:2005

การเปลี่ยนแปลงที่สำคัญระหว่างเวอร์ชัน 2005 และ 2013 เกี่ยวข้องกับ

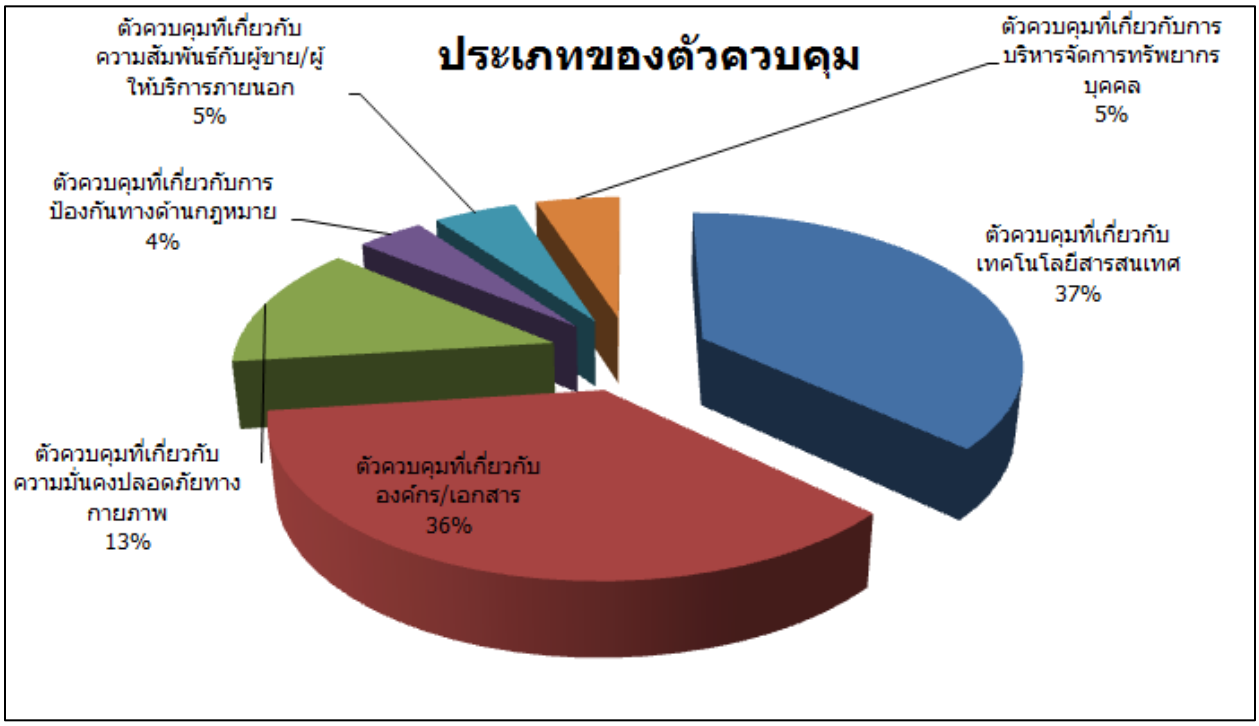
- โครงสร้างขององค์ประกอบหลักของมาตรฐาน
- ผู้มีส่วนได้ส่วนเสีย วัตถุประสงค์
- การเฝ้าติดตาม และการวัด
- Annex A มีการลดจำนวนของ ตัวควบคุมจาก 133 ไปเป็น 114 ตัว และ เพิ่มจาก 11 โดเมน เป็น 14 โดเมน
- ความเปลี่ยนแปลงในเรื่องของข้อกำหนด
    - ข้อกำหนดบางอย่างได้ถูกลบออกจากการปรับปรุงเป็น version 2013 เช่น การปฏิบัติการป้องกัน และ ข้อกำหนดในการจัดทำเอกสารสำหรับระเบียบปฏิบัติ
    - ข้อกำหนดบางอย่างได้ถูกเพิ่มเข้ามา เช่น ผู้ที่เกี่ยวข้อง (interested parties) เจ้าของความเสี่ยง (risk owner)
- ไม่มุ่งเน้น กระบวนการ PDCA (Plan-Do-Check-Act)
- เวอร์ชัน 2013 ถูกออกแบบให้มีความสอดคล้องกับมาตรฐานการจัดการอื่นๆมากยิ่งขึ้น



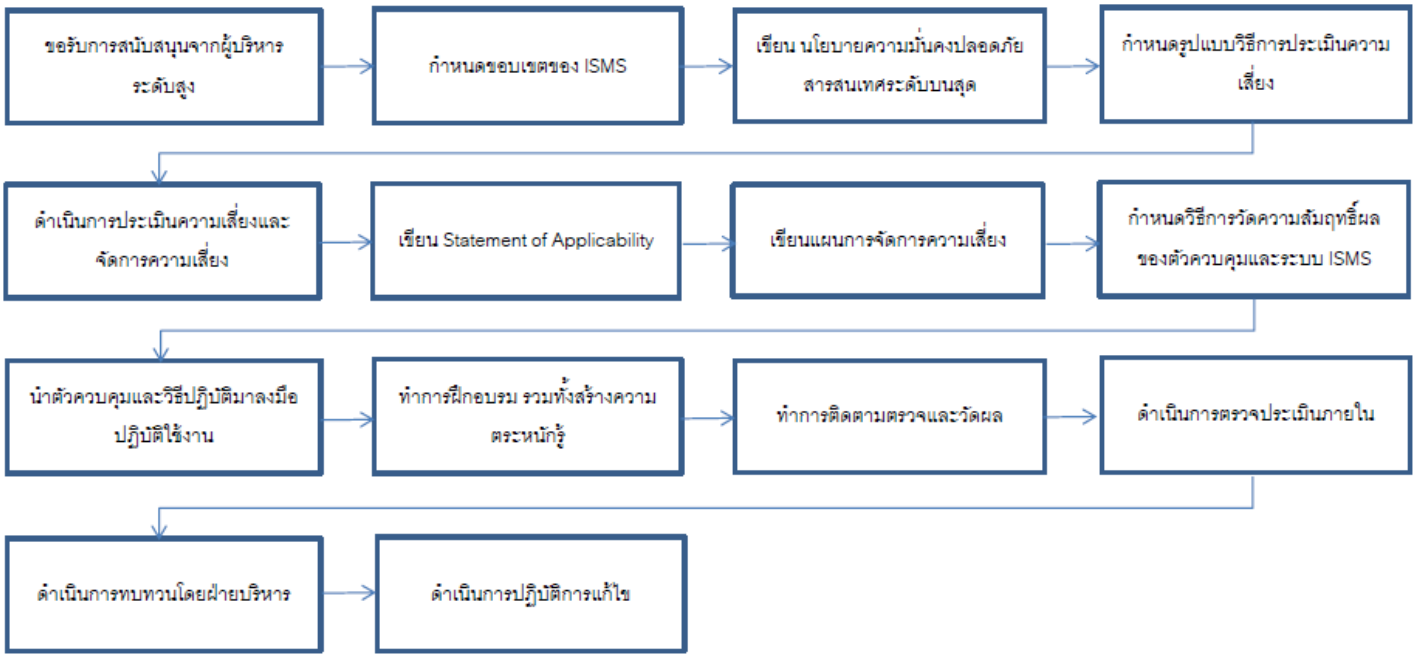
คำอธิบายโดยย่อของ ISO 27001 : 2013 Annex A

A.5	นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)
A.6	โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of information security)
A.7	ความมั่นคงปลอดภัยของทรัพยากรบุคคล (Human resource security)
A.8	การบริหารจัดการทรัพย์สิน (Asset Management)
A.9	การควบคุมการเข้าถึง (Access Control)
A.10	การเข้ารหัสข้อมูล (Cryptography)
A.11	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)
A.12	ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation security)
A.13	ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)
A.14	การจัดหา พัฒนา และ บำรุงรักษาระบบ (System acquisition, development and maintenance)
A.15	ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)
A.16	การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information security incident management)
A.17	ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องของธุรกิจ (information security aspects of business continuity management)
A.18	ความสอดคล้อง (Compliance)

ประเภทของตัวควบคุมใน Annex A ของ ISO 27001



ขั้นตอนโดยย่อของการนำ ISO 27001 มาลงมือปฏิบัติใช้งาน



หัวข้อ Introduction to Information Security Management System ISO/IEC 27001:2013 Impact towards Organisation

บรรยายโดย Mr. Lizuan Latif

- ระบบสารสนเทศเพื่อการบริหารจัดการเปรียบเสมือนระบบประสาทขององค์กร
- การทำงานที่ผิดปกติของระบบสารสนเทศอาจส่งผลกระทบต่อหน่วยงานต่างๆภายในองค์กร
- การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเป็นเครื่องมือสำหรับการรับประกันเรื่องความลับของข้อมูลสารสนเทศ ความพร้อมใช้ของข้อมูลสารสนเทศและ ความถูกต้องของข้อมูลสารสนเทศ
- ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่มีประสิทธิภาพจะช่วยลดความเสี่ยงของวิกฤตในองค์กร นอกจากนี้ ยังช่วยลดผลกระทบของวิกฤตที่เกิดขึ้นภายนอกองค์กร
- ข้อมูลจากผู้บริหารระดับสูงจากหลายๆองค์กรพบว่า องค์กรเหล่านี้ได้รับการปกป้องเป็นอย่างดี จากไฟร์วอลล์ แอนตี้ไวรัส การเข้ารหัสข้อมูล และ ระบบรหัสผ่าน อย่างไรก็ตาม ระบบความปลอดภัยทางด้านเทคนิคไม่เพียงพอที่จะยับยั้งผู้ที่มีความประสงค์ที่จะได้ทรัพย์สินขององค์กร

ผลกระทบของช่องโหว่ทางด้านความปลอดภัย

- ช่องโหว่ทางด้านความปลอดภัยมีผลที่ตามมาทั้งทางตรงและทางอ้อมกับตัวองค์กร
- การล่มของระบบ ค่าใช้จ่ายในการกู้คืนระบบ และ ความสูญเสียโดยตรงทางด้านการเงิน สามารถคำนวณเป็นตัวเลขได้ง่าย
- ค่าใช้จ่ายทางอ้อม เช่น การเสียชื่อเสียง ผลในทางกฎหมาย และ การสูญเสียรายได้ เป็นเรื่องยากในการประมาณการ
- องค์กรทุกขนาดจะมีประสบการณ์เกี่ยวกับเหตุการณ์ร้ายแรง

เหตุผลสำคัญที่ผลักดันให้มีการนำมาตรการความมั่นคงปลอดภัยสารสนเทศมาใช้งาน

การปกป้องข้อมูลของลูกค้า	31%
การปกป้องชื่อเสียงขององค์กร	14%
การดำเนินการเพื่อให้เป็นไปตามกฎหมาย ข้อกำหนดของภาครัฐ	13%
การป้องกันการล่มของระบบ	13%
การป้องกันทรัพย์สินทางปัญญา	12%
การดูแลความถูกต้องของข้อมูล	7%
การดำเนินธุรกิจอย่างต่อเนื่องในช่วงที่เกิดภัยพิบัติ	4%
เพิ่มพูนประสิทธิภาพและการลดค่าใช้จ่าย	3%
การสร้างโอกาสทางด้านธุรกิจ	2%
การปกป้องสินทรัพย์อื่นๆ (เช่น เงินสด) จากการโจรกรรม	1%

- จำนวนเหตุการณ์ที่เกี่ยวกับความปลอดภัยทางด้านข้อมูลสารสนเทศที่กระทบกับธุรกิจต่างๆในประเทศอังกฤษที่เกิดขึ้นในปี 2015 ลดลงเล็กน้อยเมื่อเทียบกับปี 2014 อย่างไรก็ตามความเสียหายที่เกิดขึ้นกับแต่ละเหตุการณ์รุนแรงมากขึ้น 10% ขององค์กรที่โดนโจมตี ได้รับความเสียหายรุนแรงมากจนจะต้องเปลี่ยนแปลงแนวทางการดำเนินธุรกิจ
- ความเสียหายจากการโจมตีในรูปของมูลค่าเงินเพิ่มขึ้นเป็นสองเท่าจากปีก่อน โดยค่าใช้จ่ายเฉลี่ยของการโจมตีที่รุนแรงที่สุดเพิ่มขึ้นอย่างมีนัยยะสำคัญ องค์กรขนาดใหญ่ในอังกฤษได้รับความเสียหายจากการโจมตีเป็นมูลค่าโดยเฉลี่ย 31.73 – 60.81 ล้านบาท องค์กรขนาดเล็กในอังกฤษได้ความเสียหายจากการโจมตีเป็นมูลค่าโดยเฉลี่ย 3.44-6.08 ล้านบาท
- องค์กรทุกขนาดยังคงได้รับความเดือดร้อนที่เกิดจากการโจมตีที่มาจากภายนอกอย่างต่อเนื่อง
- การโจมตีจากภายนอกยังคงเป็นสาเหตุสำคัญในเรื่องของปัญหาความมั่นคงปลอดภัยสารสนเทศ
- ช่องโหว่ที่เกิดจากพนักงานภายในยังมีบทบาทสำคัญในเรื่องช่องโหว่ทางด้านความปลอดภัย
- เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ 31% มีสาเหตุมาจาก ความผิดพลาดที่ไม่ได้ตั้งใจของผู้ใช้งาน และ อีก 20% เกิดจากเจตนาในการใช้ระบบอย่างไม่เหมาะสมของพนักงาน
- การทำความเข้าใจ การสื่อสารและ การสร้างความตระหนักรู้นำไปสู่ระบบความปลอดภัยที่มีประสิทธิภาพ
- หลายเหตุการณ์ทางด้านความมั่นคงปลอดภัยมีสาเหตุจากผู้บริหารให้ความสำคัญไม่เพียงพอกับเรื่องความปลอดภัย ซึ่งสามารถสังเกตได้จากงบประมาณทางด้านความปลอดภัย
- หลายๆธุรกิจเริ่มมีความตระหนักรู้เกี่ยวกับความสำคัญของการให้การศึกษาในเรื่องความปลอดภัย มีองค์กรจำนวนมากขึ้นที่อธิบายความเสี่ยงด้านความปลอดภัยขององค์กรให้กับพนักงานทราบเพื่อให้มั่นใจได้ว่าพนักงานจะปฏิบัติได้อย่างถูกต้องในการปกป้องสารสนเทศขององค์กร
- องค์กรธุรกิจจำเป็นต้องบริหารจัดการความเสี่ยงเกี่ยวกับเทคโนโลยีใหม่ การใช้เทคโนโลยียังคงเป็นส่วนสำคัญของการดำเนินการธุรกิจในแต่ละวันดังนั้นจึงเป็นสิ่งสำคัญอย่างยิ่งที่จะทำให้มั่นใจได้ว่ามีแนวทางดำเนินการที่ยืดหยุ่นสำหรับเรื่องความปลอดภัย
- การประเมินความเสี่ยงและทักษะด้านความปลอดภัยขององค์กรมีการพัฒนาดีขึ้นแต่หลายๆองค์กรก็ยังพยายามประเมินประสิทธิผลของกิจกรรมทางด้านความปลอดภัย

ประเภทของเหตุการณ์ทางด้านความมั่นคงปลอดภัยสารสนเทศ

- การติดไวรัสคอมพิวเตอร์และโปรแกรมไม่พึงประสงค์
- การบ่อนทำลายระบบหรือข้อมูลด้วยความตั้งใจของพนักงาน
- การโจรกรรมหรือฉ้อโกงทางด้านคอมพิวเตอร์
- เหตุการณ์ด้านความปลอดภัยอื่นๆที่เกิดจากการเข้าถึงระบบหรือข้อมูลโดยผู้ใช้งานที่ไม่มีสิทธิ (เช่น ใช้ ID ของบุคคลอื่นๆ)
- การเข้าถึงโดยไม่มีสิทธิโดยบุคคลภายนอก

ผลกระทบที่เกิดขึ้น

- การชะงักงันของการดำเนินธุรกิจ

- ในปัจจุบันผลกระทบที่เกี่ยวกับการใช้งาน อินเตอร์เน็ตและ E-mail อย่างไม่ถูกต้องของพนักงานเริ่มเป็นตัวการสำคัญที่สร้างปัญหาให้กับธุรกิจ การละเมิดกฎหมายและการขโมยหรือการเปิดเผยข้อมูลความลับโดยปราศจากสิทธิ์เป็นตัวการที่สร้างความเสียหายรุนแรงให้กับธุรกิจ
- เมื่อเปรียบเทียบกันการโจมตีเว็บไซต์และการติดไวรัสคอมพิวเตอร์เป็นตัวการที่ส่งผลกระทบน้อยกว่าสำหรับธุรกิจ
- ผลทางด้านกฎหมาย

ตัวอย่างเหตุการณ์ภัยคุกคามทางด้านคอมพิวเตอร์ในต่างประเทศ

บริษัท/ระบบที่โดนโจมตี ระบบการชำระเงินของบริษัท Heartland

เวลาที่เกิดเหตุการณ์ เดือนพฤษภาคม 2551

ผลกระทบ ข้อมูลบัตรเครดิต 134 ล้านใบรั่วไหล

วิธีการโจมตี เป็นการโจมตีผ่านช่องโหว่ของ SQL ทำให้สามารถติดตั้งโปรแกรมสปายแวร์ลงบนระบบสารสนเทศของบริษัท Heartland

บริษัท/ระบบที่โดนโจมตี บริษัท TJX

เวลาที่เกิดเหตุการณ์ เดือนธันวาคม 2549

ผลกระทบ ข้อมูลบัตรเครดิต 94 ล้านใบรั่วไหล

วิธีการโจมตี กลุ่ม Hacker อาศัยประโยชน์จากการเข้ารหัสข้อมูลที่ไม่แข็งแรง ขโมยข้อมูลบัตรเครดิตระหว่างการส่งถ่ายข้อมูลแบบไร้สายระหว่างร้านค้าสองแห่งของบริษัท Marshall ที่ตั้งอยู่ในไมอามี่ Hacker คนอื่นเจาะระบบของ TJX โดยใช้เครื่อง kiosk ตามร้านค้าที่อนุญาตให้ผู้คนทั่วไปสามารถใช้เครื่องสำหรับสมัครงานผ่านระบบ ตามความเห็นของผู้ร่วมก่อตั้งโครงการ KNOS และ หัวหน้าด้านสถาปัตยกรรม คุณ Kevin McAleavey การโจมตีนี้เกิดขึ้นเนื่องจากเครือข่ายของ TJX ไม่ได้ถูกปกป้องด้วยไฟร์วอลล์ใดๆ

บริษัท/ระบบที่โดนโจมตี บริษัท Epsilon

เวลาที่เกิดเหตุการณ์ เดือนมีนาคม 2554

ผลกระทบ การรั่วไหลข้อมูล ชื่อและ E-mail ของลูกค้าหลายล้านราย ที่เก็บบันทึกไว้ในร้านค้าปลีกมากกว่า 108 แห่ง รวมไปถึงองค์กรด้านการเงิน เช่น CitiGroup และ College Board ซึ่งเป็นองค์กรการศึกษาแบบไม่แสวงหากำไร ความสูญเสียที่เกิดขึ้น คิดเป็นมูลค่า 135 พันล้านบาท เนื่องจากบริษัท Epsilon มีรายชื่อของลูกค้าที่เป็นแบรนด์นานาชาติมากกว่า 2,200 รายและ มี E-mail ที่ต้องบริหารจัดการมากกว่า 4 หมื่นล้านฉบับต่อปี ดังนั้น แม้ว่าเหตุการณ์ดังกล่าวจะไม่ใช่เหตุการณ์ที่สร้างความเสียหายทางการเงินมากที่สุด แต่สามารถถือได้ว่าเป็นการละเมิดความปลอดภัยที่มีขนาดใหญ่ที่สุดในทุกๆเหตุการณ์ที่ผ่านมา

วิธีการโจมตี วิธีการโจมตียังไม่ชัดเจน แต่ผู้เชี่ยวชาญทางด้านเทคโนโลยีกล่าวว่าการโจมตีน่าจะมาจากวิธี Phishing และ การปลอมแปลงเป็นบุคคลอื่น

บริษัท/ระบบที่โดนโจมตี ระบบความปลอดภัย RSA

เวลาที่เกิดเหตุการณ์ เดือนมีนาคม 2554

ผลกระทบ เป็นไปได้ที่ข้อมูลลูกค้า 40 ล้านรายการถูกโจรกรรม ซึ่งการเยียวยามีค่าใช้จ่ายถึง 2,229 ล้านบาท และสิ่งที่น่ากลัวสำหรับผู้บริหารระดับสูงด้านความปลอดภัยคือ การที่แม้แต่บริษัทที่มีระบบความปลอดภัยที่ดีอย่าง RSA ก็ยังไม่สามารถต้านทานการโจมตีได้

บริษัท/ระบบที่โดนโจมตี กรมการทหารผ่านศึก

เวลาที่เกิดเหตุการณ์ เดือนพฤษภาคม 2549

ผลกระทบ ฐานข้อมูลที่ไม่ได้เข้ารหัสซึ่งมีข้อมูลของชื่อ หมายเลขประกันสังคม วันเกิด และข้อมูลอื่นๆของทหารผ่านศึกถูกโจรกรรม

สาเหตุ การคุกคามเกิดจากความผิดพลาดของมนุษย์ คอมพิวเตอร์ Notebook และ External Hard Disk ที่มีฐานข้อมูลดังกล่าวถูกโจรกรรม ความเสียหายที่เกิดขึ้น ประมาณการณ์แล้วคิดเป็นมูลค่า 3,378 – 16,890 ล้านบาท

บริษัท/ระบบที่โดนโจมตี ระบบเครือข่าย PlayStation ของโซนี่

เวลาที่เกิดเหตุการณ์ วันที่ 20 เมษายน 2554

ผลกระทบ บัญชีผู้ใช้งานเครือข่าย PlayStation 77 ล้านบัญชีถูกโจรกรรม โซนี่เสียหายเป็นมูลค่าหลายล้านในช่วงที่ระบบไม่สามารถให้บริการได้เป็นเดือน

บริษัท/ระบบที่โดนโจมตี บริษัท ESTsoft

เวลาที่เกิดเหตุการณ์ เดือนกรกฎาคมถึงเดือนสิงหาคม 2554

ผลกระทบ ข้อมูลส่วนบุคคลของชาวเกาหลีใต้ 35 ล้านรายรั่วไหลหลังจากที่ Hacker โจมตีช่องโหว่ด้านความปลอดภัยของผู้ให้บริการ Software ที่มีชื่อเสียง

บริษัท/ระบบที่โดนโจมตี บริษัท Gawker Media

เวลาที่เกิดเหตุการณ์ เดือนธันวาคม 2553

ผลกระทบ E-mail และ รหัสผ่านของผู้แสดงความคิดเห็นกว่า 1.3 ล้านคนบนหน้าเว็บไซต์ LifeHacker Gizmodo และ Jezebel ถูกโจรกรรม ซึ่งรวมไปถึงการขโมย source code ระบบ CMS ของ Gawker

วิธีการโจมตี Online forum และ Blog ต่างๆ เป็นเป้าหมายยอดนิยมของเหล่าบรรดา Hacker ทั้งหลาย บริษัท Gawker จับเก็บรหัสผ่านในรูปแบบที่ Hacker ทำความเข้าใจได้ง่ายมาก

บริษัท/ระบบที่โดนโจมตี CardSystems Solutions

เวลาที่เกิดเหตุการณ์ เดือนมิถุนายน 2548

ผลกระทบ ข้อมูลบัญชีบัตรเครดิต 40 ล้านบัญชีรั่วไหล

วิธีการโจมตี บริษัท CSS ซึ่งเป็นระบบที่ประมวลผลการชำระเงินรายใหญ่ให้กับ VISA, MasterCard และ American Express ไม่ปฏิบัติตามมาตรฐานในการจัดเก็บข้อมูลอย่างปลอดภัยหลังจากที่ได้รับใบรับรอง

บริษัท/ระบบที่โดนโจมตี AOL

เวลาที่เกิดเหตุการณ์ 6 สิงหาคม 2549

ผลกระทบ ข้อมูลการเข้าใช้ website กว่า 20 ล้านรายการจากผู้ใช้งานมากกว่า 650,000 รายซึ่งรวมไปถึงข้อมูลการจับจ่ายซื้อขายและข้อมูลทางด้านธนาคารถูกนำไปเผยแพร่บนหน้าเว็บไซต์แห่งหนึ่ง

บริษัท/ระบบที่โดนโจมตี monster.com

เวลาที่เกิดเหตุการณ์ เดือนสิงหาคม 2550

ผลกระทบ ข้อมูลความลับของผู้หางาน 1.3 ล้านคนถูกขโมยและถูกใช้ในการทำ Phishing โดย hacker เพื่อข่มขู่โดยการหลอกลวงผู้คนเหล่านั้นว่าเครื่องคอมพิวเตอร์ติดไวรัสและจะโดนลบไฟล์ถ้าไม่จ่ายเงินให้

บริษัท/ระบบที่โดนโจมตี Fidelity National Information Services

เวลาที่เกิดเหตุการณ์ เดือนกรกฎาคม 2550

ผลกระทบ ข้อมูลลูกค้า 3.2 ล้านรายการซึ่งรวมไปถึง ข้อมูลบัตรเครดิต ข้อมูลธนาคารและ ข้อมูลส่วนบุคคลถูกขโมยโดยพนักงานของบริษัทในเครือของ FIS

บริษัท/ระบบที่โดนโจมตี บริษัท Target Stores

เวลาที่เกิดเหตุการณ์ เดือนธันวาคม 2556

ผลกระทบ ข้อมูลบัตรเครดิต/เดบิตและข้อมูลสำหรับติดต่อของประชาชนถึง 110 ล้านคนถูกบุกรุก ความเสียหายคิดเป็นมูลค่า 5,473 ล้านบาท

วิธีการโจมตี Hacker โจมตีผ่านเครื่อง card reader ณ จุด POS และขโมยหมายเลขบัตรเครดิตและบัตรเดบิตไป 40 ล้านหมายเลข

บริษัท/ระบบที่โดนโจมตี Anthem

เวลาที่เกิดเหตุการณ์ กุมภาพันธ์ 2558

ผลกระทบ การขโมยข้อมูลส่วนบุคคลของลูกค้าปัจจุบันและลูกค้าเก่ารวมมากถึง 78.8 ล้านราย ตัวเลขความเสียหายทางด้านการเงินที่เกิดขึ้นประมาณ 3,370 ล้านบาท

บริษัท/ระบบที่โดนโจมตี Home Depot

เวลาที่เกิดเหตุการณ์ กันยายน 2557

ผลกระทบ การขโมยข้อมูลบัตรเครดิต/เดบิตของลูกค้า 56 ล้านราย คิดเป็นมูลค่าความเสียหาย 1,115 ล้านบาท

วิธีการโจมตี การติดตั้งโปรแกรมไม่พึงประสงค์ลงบนระบบ POS โดยหลอกว่าเป็นโปรแกรม Antivirus

บริษัท/ระบบที่โดนโจมตี COCA-COLA

วิธีการโจมตี อดีตพนักงานในแอตแลนต้าขโมยเครื่องคอมพิวเตอร์ notebook 55 ตัวที่มีข้อมูลแบบไม่เข้ารหัสของผู้คนจำนวน 74,000 คนซึ่งส่วนใหญ่เป็นพนักงานของบริษัท Coca Cola

บริษัท/ระบบที่โดนโจมตี SONY

เหตุการณ์ การโจมตีขนาดใหญ่ทางไซเบอร์ไปยังบริษัท Sony Picture Entertainment สร้างความเสียหายถึง 1,183 ล้านบาท

หัวข้อ Introduction to Information Security Management System ISO/IEC 27001:2013 PDCA Approach

บรรยายโดย Mr. Lizuan Latif

PDCA เป็นเครื่องมือบริหารจัดการคุณภาพ สร้างขึ้นโดย Dr W. Edwards Deming

การวางแผน (PLAN)

ค้นหาปัญหาที่แท้จริง

- เลือกปัญหาที่จะนำมาวิเคราะห์
- กำหนดเป้าหมายที่วัดได้
- จัดทำกระบวนการเพื่อขอรับการรับรองจากผู้บริหาร

วิเคราะห์ปัญหา

- ระบุและคัดเลือกกระบวนการที่ส่งผลกระทบกับปัญหา
- จัดทำรายการขั้นตอนในกระบวนการ
- จัดทำแผนผังกระบวนการ
- ตรวจสอบความถูกต้องของแผนผังกระบวนการ
- ระบุสาเหตุที่เป็นไปได้ของปัญหา
- รวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวกับปัญหา
- ทบทวนปัญหาที่ตั้งต้นไว้
- ระบุสาเหตุหลักของปัญหา
- รวบรวมข้อมูลเพิ่มเติมหากจำเป็นเพื่อตรวจสอบยืนยันความถูกต้องของสาเหตุหลักของปัญหา

พัฒนาแนวทางต่างๆในการแก้ไขปัญหา

- จัดทำเกณฑ์ในการเลือกแนวทาง
- จัดทำแนวทางที่จะสามารถจัดการสาเหตุหลักของปัญหา
- เลือกแนวทาง
- ขอรับการสนับสนุนแนวทางการแก้ไขปัญหาที่คัดเลือกไว้จากผู้มีอำนาจ

ปฏิบัติตามแผน (DO)

นำแนวทางแก้ไขปัญหามาลงมือปฏิบัติใช้งาน

- ดำเนินแนวทางการแก้ไขปัญหาที่คัดเลือกไว้ตามแผน
- การดำเนินการใช้รูปแบบของการ Trial หรือเป็น Pilot

ตรวจสอบการปฏิบัติตามแผน (CHECK)

ประเมินผลลัพธ์

- เก็บข้อมูลจากแนวทางแก้ไขปัญหา
- วิเคราะห์ข้อมูลจากแนวทางแก้ไขปัญหา

ปรับปรุงแก้ไข (ACT)

พิจารณากำหนดขั้นตอนลำดับถัดไป

- ระบุถึง การเปลี่ยนแปลงระบบและการฝึกอบรมที่จำเป็นสำหรับการนำแนวทางแก้ไขปัญหามาใช้อย่างเต็มรูปแบบ
- ประยุกต์ใช้แนวทางแก้ไขปัญหา
- วางแผนการตรวจติดตามแนวทางการแก้ไขปัญหาที่ดำเนินการอย่างต่อเนื่อง
- มองหาหนทางในการปรับปรุงแนวทางการแก้ไขปัญหาให้ดีขึ้น
- มองหาโอกาสในการปรับปรุงหรือ ตัดสินใจทบทวนแผนและลงมือปฏิบัติใหม่

การนำ PDCA มาใช้กับ ISMS

1. *การวางแผน (การจัดทำ ISMS)*
   จัดทำ แผนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ วัตถุประสงค์ กระบวนการ และ ขั้นตอนการปฏิบัติงานเพื่อจัดการความเสี่ยงและปรับปรุงประสิทธิภาพของความมั่นคงปลอดภัยสารสนเทศ

2. *ปฏิบัติตามแผน (การนำ ISMS มาลงมาปฏิบัติ)*
   นำ แผนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ วัตถุประสงค์ กระบวนการ และ ขั้นตอนการปฏิบัติงาน มาลงมือปฏิบัติใช้งาน

3. *ตรวจสอบการปฏิบัติตามแผน (ตรวจติดตามและทบทวน ISMS)*
   ประเมินและตรวจติดตามวัดประสิทธิผลของกระบวนการเมื่อเทียบกับนโยบาย วัตถุประสงค์ และ ประสบการณ์จากการใช้งานจริง และรายงานให้ทางฝ่ายบริหารพิจารณา

4. *ปรับปรุงแก้ไข (บำรุงรักษาและปรับปรุง ISMS)*
   ปฏิบัติการป้องกันและแก้ไข โดยดูจากผลของการตรวจประเมินภายในและการทบทวนโดยฝ่ายบริหารเพื่อให้เกิดการพัฒนาISMS ให้ดีขึ้นอย่างต่อเนื่อง

บทสรุป

- องค์กรจำเป็นต้องมีความเข้าใจอย่างถ่องแท้ในการนำ วงจร PDCA มาประยุกต์ใช้งานเพื่อให้สามารถควบคุมค่าใช้จ่ายของโครงการได้
- ตรวจติดตามเวลาที่ใช้ในการดำเนินโครงการ
- ตั้งเป้าหมายที่ชัดเจนสำหรับทีม

หัวข้อ Standard ISO/IEC 27001:2013 Standard Requirements

บรรยายโดย Mr. Mohd Nazim Harun

(4) เข้าใจบริบทขององค์กร (Context of the organization)

(4.1) การทำความเข้าใจองค์กรและบริบทขององค์กร (Understanding the organization and its context)

- กำหนดผลลัพธ์ที่ต้องการ
- กำหนดประเด็นภายในและภายนอกที่เกี่ยวข้อง

(4.2) การทำความเข้าใจความต้องการและความคาดหวังของผู้ที่เกี่ยวข้อง (Understanding the needs and expectations of interested parties)

- กำหนดผู้ที่เกี่ยวข้อง ซึ่งเป็นผู้ที่เกี่ยวข้องกับ ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และ
- กำหนดความต้องการของผู้ที่เกี่ยวข้องเหล่านั้น ที่เกี่ยวกับ ความมั่นคงปลอดภัยสารสนเทศ

(4.3) การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Determining the scope of the information security management system)

- กำหนดกรอบและการประยุกต์ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
- ระบุขอบเขตการดำเนินการ

(4.4) ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security management system)

- กำหนด ลงมือปฏิบัติ บำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง
- ต้องสอดคล้องกับข้อกำหนดของมาตรฐาน ISO 27001

(5) ภาวะผู้นำ (Leadership)

(5.1) ภาวะผู้นำ และ การให้ความสำคัญ (Leadership and commitment)

- ผู้บริหารระดับสูงต้องแสดงให้เห็นถึงภาวะผู้นำและการให้ความสำคัญกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(5.2) นโยบาย (Policy)

- ผู้บริหารระดับสูงต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ

(5.3) บทบาท หน้าที่ความรับผิดชอบ และ อำนาจหน้าที่ (Organization roles, responsibilities and authorities)

- ผู้บริหารระดับสูงต้องทำให้หน้าที่ความรับผิดชอบและอำนาจหน้าที่ตามบทบาทที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศมีการมอบหมายและสื่อสารให้ได้รับทราบกัน

(6) การวางแผน (Planning)

(6.1) การดำเนินการเพื่อจัดการความเสี่ยงและโอกาส (Actions to address risks and opportunities)

(6.1.1) ทั่วไป (General)

- เมื่อมีการวางแผนความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องพิจารณาถึงประเด็นที่อ้างถึงใน 4.1 และ ความต้องการที่อ้างถึงใน 4.2 และกำหนดความเสี่ยงและโอกาสที่ต้องจัดการ

(6.1.2) การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment)

- การประยุกต์กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเพื่อระบุถึงความเสี่ยงที่เกี่ยวกับการสูญเสียความลับ ความถูกต้องและ ความพร้อมใช้งานของสารสนเทศภายใต้ขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(6.1.3) การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information System risk treatment)

- องค์กรต้องกำหนดและประยุกต์กระบวนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเพื่อกำหนดทางเลือกที่เหมาะสมในการจัดการความเสี่ยงโดยนำผลลัพธ์จากการประเมินความเสี่ยงมาพิจารณา

(6.2) วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและการวางแผนเพื่อให้บรรลุวัตถุประสงค์ (Information security objectives and planning to achieve them)

- องค์กรต้องกำหนดวัตถุประสงค์ของความมั่นคงปลอดภัยที่เกี่ยวกับฟังก์ชันงานและระดับ วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศต้องสอดคล้องกันนโยบายความมั่นคงปลอดภัยสารสนเทศ

(7) การสนับสนุน (Support)

(7.1) ทรัพยากร (Resources)

- องค์กรต้องกำหนดและให้ทรัพยากรที่จำเป็นสำหรับการกำหนด การปฏิบัติ การบำรุงรักษาและ การปรับปรุงอย่างต่อเนื่องสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(7.2) ความรู้ความเชี่ยวชาญ (Competence)

- องค์กร ต้องกำหนดความรู้ความเชี่ยวชาญที่จำเป็นของบุคลากรที่ปฏิบัติงานภายใต้การควบคุมดูแลขององค์กรซึ่งส่งผลต่อประสิทธิภาพในการปฏิบัติงานความมั่นคงปลอดภัยสารสนเทศ

(7.3) การสร้างความตระหนักรู้ (Awareness)

- บุคลากรที่ปฏิบัติงานภายใต้การควบคุมดูแลขององค์กรต้องตระหนักรู้ถึงนโยบายความมั่นคงปลอดภัยสารสนเทศ

(7.4) การสื่อสาร (Communication)

- องค์กรต้องกำหนดความจำเป็นสำหรับการสื่อสารภายในและภายนอกองค์กรที่เกี่ยวกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(7.5) สารสนเทศที่เป็นลายลักษณ์อักษร (Documented information)

(7.5.1) ทั่วไป (General)

- ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรต้องรวมถึง สารสนเทศที่เป็นลายลักษณ์อักษรตามข้อกำหนดของมาตรฐาน ISO และ สารสนเทศที่เป็นลายลักษณ์อักษรที่ทางองค์กรพิจารณาเห็นถึงจำเป็นสำหรับความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(7.5.2) การสร้างและปรับปรุง (Creating and updating)

(7.5.3) การควบคุมสารสนเทศที่เป็นลายลักษณ์อักษร (Control of documented information)

(8) การดำเนินการ (Operation)

(8.1) การวางแผนและการควบคุมการดำเนินการ (Operational planning and control)

- องค์กรต้องวางแผน ลงมือปฏิบัติ และ ควบคุมกระบวนการที่จำเป็นเพื่อให้สอดคล้องกับความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

(8.2) การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment)

- องค์กรต้องดำเนินการประเมินความเสี่ยงตามรอบระยะเวลาที่วางแผน หรือ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยยะสำคัญ

(8.3) การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk treatment)

- องค์กรต้องลงมือปฏิบัติตามแผนจัดการความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ

(9) การประเมินประสิทธิภาพและประสิทธิผล (Performance evaluation)

(9.1) *การติดตามตรวจ การวัด การวิเคราะห์ และ การประเมิน (Monitoring, measurement, analysis and evaluation)*

- องค์กรต้องประเมินประสิทธิภาพและความสัมฤทธ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(9.2) *การตรวจประเมินภายใน (Internal audit)*

- องค์กรต้องจัดให้มีการตรวจประเมินภายในตามช่วงเวลาที่วางแผนไว้เพื่อให้มีสารสนเทศสำหรับการระบุว่า ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ สอดคล้องกับ
    1) ความต้องการขององค์กรเองสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
    2) ข้อกำหนดตามมาตรฐาน ISO 27001

(9.3) การทบทวนโดยฝ่ายบริหาร (Management review)

- ผู้บริหารระดับสูงต้องทำการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามช่วงเวลาที่วางแผนไว้เพื่อให้มั่นใจว่า ระบบยังคงความเหมาะสม เพียงพอ และ มีประสิทธิผลดี

(10) การปรับปรุง (Improvement)

(10.1) ความไม่สอดคล้องและการปฏิบัติการแก้ไข (Nonconformity and corrective action)

- เมื่อเกิดความไม่สอดคล้องขึ้น องค์กรต้อง
    a) ตอบกลับความไม่สอดคล้องนั้นอย่างเหมาะสม
    b) ประเมินความจำเป็นสำหรับการดำเนินการเพื่อขจัดสาเหตุของความไม่สอดคล้องเพื่อไม่ให้เกิดขึ้นอีก
    c) ดำเนินการแก้ไขตามความจำเป็น
    d) ทบทวนประสิทธิผลของการดำเนินการแก้ไขที่ได้ดำเนินการไป
    e) ทำการเปลี่ยนแปลงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามความจำเป็น

(10.2) การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)

- องค์กรต้องปรับปรุงความเหมาะสม ความเพียงพอ ความมีประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

หัวข้อ Introduction to Information Security Management System ISO/IEC 27001:2013 ISMS Document

บรรยายโดย Mr. Mohd Nazim Harun

ข้อกำหนดที่ต้องจัดทำเอกสารเป็นลักษณ์อักษรได้แก่

(4.3) การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Determining the scope of the information security management system)

(5.2) นโยบาย (Policy)

(6.1.2) การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment)

(6.1.3) การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information System risk treatment)

(6.2) วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและการวางแผนเพื่อให้บรรลุวัตถุประสงค์ (Information security objectives and planning to achieve them)

(7.2) ความรู้ความเชี่ยวชาญ (Competence)

(8.2) การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment)

(8.3) การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk treatment)

(9.1) การติดตามตรวจ การวัด การวิเคราะห์ และ การประเมิน (Monitoring, measurement, analysis and evaluation)

(9.2) การตรวจประเมินภายใน (Internal audit)

(9.3) การทบทวนโดยฝ่ายบริหาร (Management review)

(10.1) ความไม่สอดคล้องและการปฏิบัติการแก้ไข (Nonconformity and corrective action)

หัวข้อ Introduction to Information Security Management System ISO/IEC 27001:2013 Management review and audit
บรรยายโดย Mr. Mohd Nazim Harun

(9.2) *การตรวจประเมินภายใน (Internal audit)*

- องค์กรต้องจัดให้มีการตรวจประเมินภายในตามช่วงเวลาที่วางแผนไว้เพื่อให้มีสารสนเทศสำหรับการระบุว่า ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ สอดคล้องกับ
    1. ความต้องการขององค์กรเองสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
    2. ข้อกำหนดตามมาตรฐาน ISO 27001
- การวางแผน การจัด การลงมือปฏิบัติ และ การบำรุงรักษา โปรแกรมการตรวจประเมินภายใน รวมถึง ความถี่ วิธีการ ผู้รับผิดชอบ และ การรายงานผล
- โปรแกรมการตรวจประเมินภายใน ต้องพิจารณาถึง ความสำคัญของกระบวนการ และ ผลลัพธ์จากการตรวจประเมินภายในครั้งที่ผ่านมา
- ในการตรวจประเมินภายใน ต้องมีการระบุ เกณฑ์และ ขอบเขตการดำเนินการตรวจประเมินภายใน
- คัดเลือกผู้ตรวจประเมินภายในเพื่อให้การตรวจประเมินตรงกับวัตถุประสงค์ และ ไม่เกิดอคติใดๆ
- รายงานผลการตรวจประเมินภายในจะถูกรายงานไปยังฝ่ายบริหารและมีการเก็บสารสนเทศที่เป็นลายลักษณ์อักษรเพื่อใช้เป็นหลักฐาน

(9.3) การทบทวนโดยฝ่ายบริหาร (Management review)

- ผู้บริหารระดับสูงต้องทำการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามช่วงเวลาที่วางแผนไว้เพื่อให้มั่นใจว่า ระบบยังคงความเหมาะสม เพียงพอ และ มีประสิทธิผลดี
- จะต้องมีสถานะของการดำเนินการต่างๆที่เกิดจาก การทบทวนโดยฝ่ายบริหาร ครั้งก่อน และ ประเด็นภายในและภายนอกที่มีการเปลี่ยนแปลงไป
- จะต้องมีผลตอบกลับเกี่ยวกับประสิทธิภาพของระบบความปลอดภัย ได้แก่
    - ความไม่สอดคล้องกับข้อกำหนดและการปฏิบัติการแก้ไข
    - ผลของการตรวจติดตามและการวัด
    - ผลลัพธ์ของการตรวจประเมิน
    - การบรรลุตามวัตถุประสงค์
- จะต้องรวมถึง
    - ผลตอบกลับจากผู้เกี่ยวข้อง
    - ผลลัพธ์ของการประเมินความเสี่ยงและสถานะของการจัดการความเสี่ยง

        - โอกาสในการปรับปรุงให้ดียิ่งขึ้น
- ผลลัพธ์ของการทบทวนโดยฝ่ายบริหาร จะต้องมี
    - การตัดสินใจที่เกี่ยวกับการปรับปรุงให้ดีขึ้นอย่างต่อเนื่อง
    - โอกาสและความจำเป็นอื่นๆสำหรับการเปลี่ยนแปลง
- ต้องมีการจัดทำสารสนเทศที่เป็นลายลักษณ์อักษรเพื่อเก็บเป็นหลักฐาน

หัวข้อ Introduction to Information Security Management System ISO/IEC 27001:2013 The Benefit of ISMS Implementation

บรรยายโดย Mr. Siddharth Sharma

ประโยชน์ทางตรงของ ISMS

- เพิ่มความน่าเชื่อถือและความปลอดภัยของระบบสารสนเทศ
    - ธุรกิจต่างๆมีระบบสารสนเทศที่สลับซับซ้อน ISO 27001 ช่วยให้เห็นถึงตัวควบคุมที่จะช่วยให้ระบบธุรกิจพร้อมใช้งานได้ตลอดเวลา
    - ตัวควบคุมตามมาตรฐาน ISO 27001 ช่วยลดความเสี่ยงจากช่องโหว่ต่างๆ
    - การตรวจประเมินหลังได้รับใบรับรองทำให้มั่นใจได้ว่า ธุรกิจยังคงมีการปรับปรุงระบบความปลอดภัยให้ทันสมัย รองรับการป้องกันช่องโหว่ด้านความปลอดภัยใหม่ๆ และ ใช้แนวทางการปฏิบัติที่ดี
    - มาตรฐาน ISO 27001 เน้นการปรับปรุงระบบให้ดีขึ้นอย่างต่อเนื่องซึ่งช่วยให้ระบบมีความน่าเชื่อถือและทันสมัย
- เพิ่มผลกำไร
    - ISO 27001 ช่วยเพิ่มความสามารถในการทำกำไรให้กับองค์กรธุรกิจในระยะกลางถึงระยะยาว
    - เพิ่มความน่าเชื่อถือจากลูกค้า ลูกค้ามีความรู้สึกพอใจที่จะร่วมงานกับองค์กรที่ได้ใบรับรองมาตรฐานความปลอดภัย
- ระบบความมั่นคงปลอดภัยสารสนเทศที่คุ้มค่าและสอดคล้องกัน
    - การประเมินความเสี่ยงตามมาตรฐาน ISO 27001 ช่วยให้เห็น ประสิทธิภาพและประสิทธิผลของ ระบบความปลอดภัยที่องค์กรต่างๆนำมาใช้งานอยู่
    - การประเมินความเสี่ยงช่วยสรุปให้เห็นถึง ตัวควบคุมที่มีการนำมาใช้งานอยู่แต่ส่งผลประโยชน์ทางด้านธุรกิจน้อยมากหรือไม่มีเลย
    - การประเมินความเสี่ยงช่วยในเรื่องการปรับปรุงตัวควบคุมที่มีอยู่ให้ดียิ่งขึ้น อีกทั้งยังช่วยให้เห็นถึงตัวควบคุมอื่นๆที่สามารถนำมาใช้งานเพิ่มเติม
    - มาตรฐาน ISO 27001 ช่วยให้การพัฒนาระบบความปลอดภัยในองค์กรมีความสอดคล้องไปในทิศทางเดียวกัน และ เป็นไปตามมาตรฐานสากล
    - กระบวนการที่มีระเบียบแบบแผนช่วยทำให้เกิดความมั่นใจได้ว่า พนักงานจะปฏิบัติตามนโยบายซึ่งจะทำให้ได้ผลลัพธ์ที่ดีขึ้น
- ความสมเหตุสมผลของระบบ
    - ในขั้นตอนของการจัดทำ องค์กรต้องวิเคราะห์สารสนเทศและความต้องการเกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศ เพื่อให้ได้นโยบายที่สมเหตุสมผลและมีการลงทุนที่คุ้มค่า
- ความสอดคล้องกับข้อกำหนดกฎหมาย
    - การนำ ISO 27001 มาใช้งาน จะเป็นข้อบังคับให้องค์กรต้องปฏิบัติตามกฎหมาย ข้อกำหนดต่างๆ

ประโยชน์ทางอ้อมของ ISMS

- ปรับปรุงระบบบริหารจัดการให้ดียิ่งขึ้น
    - มาตรฐาน ISO 27001 มุ่งเน้นการกระจายอำนาจ ช่วยแบ่งเบาภาระในการบริหารจัดการ
    - ฝ่ายบริหารได้รับสารสนเทศที่มีคุณภาพดีขึ้นทำให้สามารถบริหารจัดการได้ดียิ่งขึ้น
- เพิ่มพูนความสัมพันธ์ที่ดีระหว่างบุคคล
    - นโยบาย วิธีปฏิบัติ และ แนวทางการดำเนินการที่ชัดเจน ช่วยให้ทุกสิ่งเป็นเรื่องที่ง่ายต่อการทำความเข้าใจของพนักงาน
    - ใบรับรองเป็นข้อได้เปรียบเหนือคู่แข่งทางธุรกิจที่พนักงานสามารถนำมาใช้เป็นเครื่องมือเพื่อการทำงานที่สะดวกสบายมากยิ่งขึ้น
    - พนักงานเข้าใจถึงความสำคัญของภาพลักษณ์ขององค์กร และใส่ใจมากขึ้นในเรื่องของบริการ ผลิตภัณฑ์ และ ลูกค้า
    - องค์กรมีทรัพยากรบุคคลที่มีคุณภาพสูงขึ้นเนื่องจาก องค์กรต้องจัดให้มีระบบการคัดกรองบุคลากรที่ดี
- ปรับปรุงระบบบริหารจัดการความเสี่ยงให้ดียิ่งขึ้น
    - ในขั้นตอนของการขอใบรับรอง ISO 27001 องค์กรต้องระบุช่องโหว่ ภัยคุกคาม และ ผลกระทบที่เป็นไปได้
    - องค์กรได้แนวทางที่เป็นระบบในการบริหารจัดการความเสี่ยง
    - การประเมินความเสี่ยงช่วยระบุความเสี่ยงที่สำคัญยิ่งกว่าสำหรับความสำเร็จของการดำเนินธุรกิจ
    - ISMS ช่วยในเรื่องการวางแผนเกี่ยวกับ Business Continuity และ Disaster Recovery ซึ่งจะช่วยลดโอกาสในการสูญเสียทางด้านการเงินและภาพลักษณ์ขององค์กร

2.2 เนื้อหา/องค์ความรู้ที่ได้จากการศึกษาดูงาน

ในวันพุธที่ 13 พฤษภาคม 2558 ทางผู้จัดได้พาผู้เข้าร่วมโครงการทุกท่านเดินทางออกจากกรุงจาการ์ตาไปยังเมืองบันดุงเพื่อเข้าเยี่ยมชมบริษัท Telkom Indonesia ซึ่งเป็นบริษัทที่ได้รับใบรับรอง ISO 27001:2013 โดยมีรายละเอียดของการบรรยายดังนี้

Telkom Indonesia หรือ Telkom Group เป็นองค์กรสื่อสารโทรคมนาคมเพียงแห่งเดียวที่ถือครองโดยภาครัฐ (ถือหุ้นโดยภาครัฐ 52.56%) และเป็นผู้ให้บริการระบบสื่อสารโทรคมนาคมและเครือข่ายต่างๆ จดทะเบียนอยู่ในตลาดหลักทรัพย์ด้วยชื่อ TLKM โดยมี Vision คือ “To become a leading Telecommunication, Information, Media, Edutainment and Services (“TIMES”) player in the region” ซึ่ง region ที่กล่าวถึงคือ Asia Pacific และ Mission คือ To provide “more for less” TIMES services และ To be the role model as the best managed corporation in Indonesia.

ความเป็นมาของการนำ ระบบ ISMS มาประยุกต์ใช้งานในองค์กร

- ปี 2006 เริ่มมี ISMS Policy ซึ่งเป็นไปตามกฎของตลาดหลักทรัพย์นิวยอร์ก (Stock compliance)
- ปี 2006-2011 มีการนำ ISMS มาประยุกต์ใช้งานจริงเฉพาะหน่วยงาน Information System Center (IT Department) ยังไม่มีการนำไปใช้กับหน่วยงานด้านเครือข่าย
- ปี 2011 เริ่มต้นกระบวนการขอใบรับรอง (certification) สาเหตุ คือ พลาดงานของลูกค้า 2 ราย สูญเสียโอกาสไป 40,000 ล้าน IDR เนื่องจากลูกค้ากำหนดให้บริษัทที่รับงานต้องมีใบรับรอง ISO 27001 / เพิ่มscope ของ ISMS ให้รวมระบบเครือข่าย / มีหน่วยงาน IT Strategy and Governance ทำหน้าที่เป็น Management Representative
- ปี 2013 ยังคงใช้ใบรับรองตามมาตรฐาน ISO27001 : 2005
- ปี 2014 ได้รับใบรับรอง ISO 27001 : 2013 พร้อมทั้ง จัดตั้ง Cyber Security Operation Center (ทำหน้าที่เป็น IT Security Incident Response Team)

- ความมุ่งมั่นของฝ่ายบริหาร (Management commitment) ช่วยให้การดำเนินการเป็นไปโดยราบรื่น
- กิจกรรมประจำปี
    - พิจารณาทบทวนนโยบายและวิธีปฏิบัติ (Policy & Procedure review)
    - ประเมินความเสี่ยง (Risk Assessment)
    - การทดสอบช่องโหว่ทางด้านความปลอดภัย (Vulnerability Test)
    - การทดสอบระบบบริหารความต่อเนื่องของธุรกิจ (Business Continuity Test)
    - การตรวจประเมินภายใน (Internal Audit)
    - การทบทวนโดยฝ่ายบริหาร (Management Review)
    - การตรวจติดตามผล (Surveillance Audit) โดย ผู้ตรวจประเมินภายนอก เป็นกิจกรรมที่ควรมีสำหรับองค์กรที่ได้ใบรับรองแล้ว
- ทรัพยากรบุคคล
    - การอบรมผู้ตรวจประเมิน ทาง Telkom มีผู้ตรวจประเมินที่ผ่านการรับรองสำหรับ ISO 27001 แล้วมากกว่า 15 ท่าน ISO2000 120 ท่าน และ มากกว่า 15 ท่าน สำหรับ CEH (Certified Ethical Hacker)
- การตรวจประเมินภายใน
    - การตรวจประเมินแบบข้ามพื้นที่ เนื่องจาก อินโดนีเซียประกอบด้วยหลายเกาะ เช่น สุมาตรา ชวา บอร์เนียว จึงใช้วิธีตรวจประเมินข้ามเกาะ เช่น ทีมจากสุมาตรา ทำหน้าที่ตรวจ หน่วยงานบนเกาะชวา ในแต่ละเกาะใช้ วิธีปฏิบัติ(procedure) เดียวกันแต่ปฏิบัติไม่เหมือนกัน lead auditor มาจากทีมตรวจประเมินภายใน
    - มี Information Security Awards เพื่อเพิ่มพูนขวัญกำลังใจให้ผู้ที่ปฏิบัติตาม ISMS

ขอบเขตการดำเนินการตามมาตรฐาน ISO 27001:2013

Scope :

1) Implementation of *Information Security Management System* based on ISO 27001:2013 and *Business Continuity Management System* based on ISO 22301:2012 on product and service infrastructure for IP Connectivity, focus on processes :
    a) Fulfilment
    b) Assurance
    c) Technical Operation
    d) Network Performance
2) Implementation of *Quality Management System* based on ISO 9001:2008 on product and service infrastructure for POTS dan Non POTS pada proses :
    a) Fulfilment
    b) Assurance
    c) Technical Operation
    d) Network Performance
    e) Service Development

เทคนิคในการขอใบรับรอง

- เริ่มด้วยขอบเขตการดำเนินการ(Scope) เล็กๆ
- วัตถุประสงค์ของการลงมือดำเนินการควรสอดคล้องกับความต้องการทางด้านธุรกิจขององค์กร

- การทบทวนและปรับปรุงให้ดียิ่งขึ้น มีการกำหนดหน้าที่ความรับผิดชอบอย่างชัดเจน

บทเรียนจากการนำ ISO 27001 มาใช้งาน

1. วัตถุประสงค์ที่ชัดเจน
2. ความมุ่งมั่นของฝ่ายบริหาร
3. พนักงานมีความตระหนักรู้เกี่ยวกับเรื่องความปลอดภัย
4. ระเบียบวินัย (Discipline)
5. สิ่งสำคัญที่สุดคือ การสร้าง Change Agents ซึ่งจะเป็นตัวแทนของแต่ละหน่วยงานที่รับผิดชอบทั้งหมดเกี่ยวกับเรื่องความปลอดภัย