บทที่ 9

ISO/IEC 27001:2013

ผู้ช่วยศาสตราจารย์ ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ
ภาควิชาการสื่อสารข้อมูลและเครือข่าย คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ (มจพ.)

บทนำ

- ISO หรือมาตรฐานที่กำหนดและควบคุมโดยองค์การนานาชาติเพื่อระบบมาตรฐาน (International Organization for standardization) เป็นที่รู้จักและให้ความสำคัญกันมากในวงการอุตสาหกรรม
- แต่ปัจจุบัน ISO กำลังก้าวสู่วงการอื่น ๆ ที่เกี่ยวข้อง เช่น
  - ISO 9000 มาตรฐานระบบบริหารงานคุณภาพ
  - ISO 14001 ด้านสิ่งแวดล้อมของอุตสาหกรรมการผลิต
  - ISO 50001 มาตรการด้านการจัดการอนุรักษ์พลังงาน
  - ISO 22000:2005 ระบบการจัดการความมั่นคงปลอดภัยของอาหาร
  - ISO 26000 มาตรฐานสากลที่ว่าด้วยความรับผิดชอบต่อสังคมให้เป็นไปในแนวทางเดียวกัน
  - ISO 14000 มาตรฐานการบริหารจัดการสิ่งแวดล้อม
  - ISO 17025 มาตรฐานการประเมินความสามารถทางวิชาการของห้องปฏิบัติการ
  - ISO 18000 มาตรฐานการจัดการอาชีวอนามัยและความมั่นคงปลอดภัย

บทนำ

- จะเห็นได้ว่ามาตรฐานตามกรอบของ ISO นั้นมีความละเอียดและครอบคลุมหลายวงการมากมาย
- จนหลายครั้งคนนอกวงการธุรกิจอุตสาหกรรมนั้น ๆ อาจจะไม่รู้จักมาตรฐานนั้นมาก่อนเลยก็เป็นไปได้
- และหลายครั้งแม้แต่มาตรฐานที่เกี่ยวโยงกับอุตสาหกรรมใด ๆ ก็อาจจะไม่ได้เป็นที่รับรู้หรือใส่ใจเพราะไม่ได้มีผลในทางปฏิบัติที่กระทบต่อการค้าขายหรือทำธุรกิจนั้น ๆ โดยตรงกับบริษัทในหมู่คู่ค้าและลูกค้า

บทนำ (ต่อ)

- แต่มาตรฐานหนึ่งที่ในปัจจุบันกำลังกลายเป็นมาตรฐานระดับโลกที่จำเป็นต่อทุกองค์กรก็คือ ISO/IEC 27001 ทั้งนี้ก็เพราะปัญหาและความเสี่ยงที่เคยเกิดขึ้นมาหลายครั้งทั้งเรื่องข้อมูลสถานพยาบาล สถาบันการเงินและภาครัฐรั่วไหล
- ISO/IEC 27001 (Information Security Management System: ISMS) เป็นมาตรฐานการจัดการข้อมูลที่มีความสำคัญเพื่อให้ธุรกิจดำเนินไปอย่างต่อเนื่อง ซึ่งข้อกำหนดต่าง ๆ กำหนดขึ้นโดยองค์กรที่มีชื่อเสียงและมีความน่าเชื่อถือระหว่างประเทศ คือ ISO (The International Organization for Standardization) และ IEC (The International Electrotechnical Commission) ร่วมกับองค์กรระหว่างประเทศอื่น ๆ อีกหลายองค์กร ประกอบด้วยองค์กรรัฐบาลและองค์กรอิสระต่าง ๆ
- การประยุกต์ใช้ ISMS จะช่วยให้กิจกรรมทางธุรกิจต่อเนื่องไม่สะดุด ช่วยป้องกันกระบวนการทางธุรกิจจากภัยร้ายแรงต่าง ๆ เช่น แผ่นดินไหว วาตภัย อุทกภัย ฯลฯ และความเสียหายของระบบข้อมูล โดยครอบคลุม ทุกกลุ่มอุตสาหกรรมและทุกกลุ่มธุรกิจ

Outline

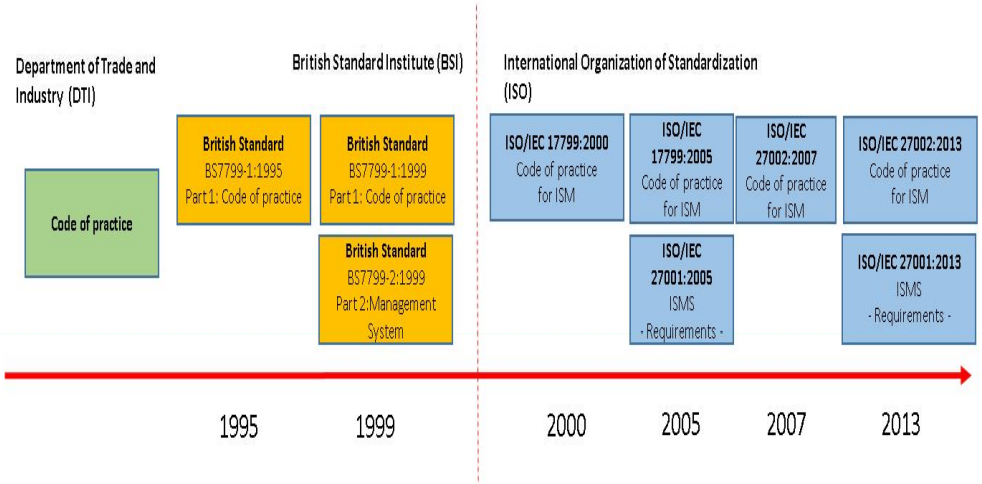
- 9.1 ทำความรู้จักกับ ISO/IEC 27001
- 9.2 ที่มาของความสำคัญสำหรับ ISO/IEC 27001
- 9.3 สิ่งที่ควรทราบก่อนนำมาตรฐานมาประยุกต์ใช้
- 9.4 เปรียบเทียบ ISO/IEC 27001:2005 และ ISO/IEC 27001:2013
- 9.5 โครงสร้างมาตรฐาน ISO (Annex SL)
- 9.6 การจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISMS)
- 9.7 โมเดล CIA และประเมินความเสี่ยงใน ISO/IEC 27001
- 9.8 เกร็ดน่ารู้เกี่ยวกับการทำ ISMS
- 9.9 บทสรุป

9.1 ทำความรู้จักกับ ISO/IEC 27001

9.1 มาทำความรู้จักกับ ISO/IEC 27001

- ISO/IEC 27001 คือ แนวทางหรือวิธีการเกี่ยวกับเรื่องความเสี่ยงด้านสารสนเทศเพื่อการกำหนด นโยบาย และกระบวนการทำงาน รวมทั้งเพื่อเลือกการควบคุมที่เหมาะสมในการบริหารความเสี่ยงด้วย กล่าวได้ว่าเป็นมาตรฐานเชิงระบบที่เน้นการปฏิบัติ จึงสามารถนำไปใช้อ้างอิงเพื่อการประเมินและขอรับการรับรองมาตรฐานต่อไปได้
- ในขณะที่ ISO 20000 นั้นเน้นเรื่องการบริหารบริการไอที แต่ ISO/IEC 27000 และ ISO/IEC 17799 จะเน้นเรื่องการบริหารข้อมูลสารสนเทศโดยตรง

ความเป็นมาของ ISO/IEC 27001



http://arafiandi.blogspot.com/

9.1 มาทำความรู้จักกับ ISO/IEC 27001 (ต่อ)

- Code of practice เรื่องการจัดการด้านความมั่นคงปลอดภัยของอังกฤษในปี 1992 เป็นต้นแบบของการพัฒนา ISO/IEC 27001
- BS7799-1 (ปี 1995) พัฒนามาจาก Code of practice เรื่องการจัดการด้านความมั่นคงปลอดภัย โดยหน่วยงานมาตรฐานของอังกฤษ (British Standard Institute)
- ต่อมา BS7799-1 กลายเป็น ISO/IEC 17799:2000 (หลัง: หมายถึงปีที่ประกาศใช้มาตรฐาน ในที่นี้ คือ ปี ค.ศ.2000)
- ก่อนจะขยายในส่วนของ BS7799-2 (ปี 2002) ครอบคลุมเรื่องระบบบริหารความมั่นคงปลอดภัยสารสนเทศและกลายเป็น ISO/IEC 27001:2005 ในเวลาต่อมาในปี 2005
- โดย ISO/IEC 17799 ได้เปลี่ยนรหัสเรียกมาเป็น ISO/IEC 27002
- มาตรฐาน ISO/IEC 27001:2013 คือมาตรฐานล่าสุดของ ISO/IEC 27001

9.1 มาทำความรู้จักกับ ISO/IEC 27001 (ต่อ)

ข้อแตกต่างระหว่าง ISO/IEC 17799 กับ ISO/IEC 27001

1. ISO/IEC 27001 เน้นเรื่องรายละเอียดเชิงเทคนิคมาตรฐานสำหรับการบริหารความมั่นคงปลอดภัยด้านสารสนเทศ ISMS (Information Security Management System)โดย ISO/IEC 27001:2005 เป็นรายละเอียดแบบมุ่งเน้นกระบวนการตามหลักการ PDCA (Plan-Do-Check-Act Process focused) สามารถใช้เป็นเกณฑ์เพื่อนำไปใช้งานจริง (Implement) และขอการรับรองได้ ส่วน ISO/IEC 27001:2013 นั้นไม่ได้มีการระบุแบบมุ่งเน้นกระบวนการตามหลักการ PDCA แต่แบบมุ่งเน้นกระบวนการตามหลักการพัฒนาอย่างต่อเนื่อง (Continual improvement) ตามที่องค์กรมีอยู่ หรือจะใช้ PDCA ก็ได้
2. ISO/IEC 17799 เป็นรายละเอียดการดำเนินการ (code of practice) เพื่อการควบคุมด้านความมั่นคงปลอดภัย (Security control) ต่อมาได้ถูกนำไปโยงความสัมพันธ์กับ ISO/IEC 27000 ซึ่งครอบคลุมเรื่องความมั่นคงปลอดภัยสารสนเทศทั้งหมดและถูกเรียกรหัสใหม่เป็น ISO/IEC 27002

Information Security Assurance Lifecycle

- ✓ The continual improvement process using PDCA concept is a requirement in ISO 27001:2005
- ✓ In ISO 27001:2013 there is no longer required to use PDCA only, each organization can use their existing continual improvement process
- ✓ Following description will still use PDCA as the continual improvement process for simplicity and general understanding purpose

PECB fedc

12

http://www.slideshare.net/PECBCERTIFICATION/pecb-webinar-ics-security-management-system-using-iso-27001-standard-as-the-strategic-management-foundation-integrated-with-nist-sp-80082-auditing-platform

9.1 มาทำความรู้จักกับ ISO/IEC 27001 (ต่อ)

- อาจกล่าวได้ว่า ISO/IEC 27001 นั้นเป็นส่วนขยายเพิ่มของ ISO/IEC 17799 เพื่อให้ครอบคลุมรายละเอียดในเชิงระบบทั้งหมด (โดยที่เดิมทีนั้น ISO/IEC 27001 มีชื่อเรียกว่า BS7799-2)
- ISO/IEC 27001 จะแสดงหลักการนำเอา code of practice เรื่องความมั่นคงปลอดภัยมาใช้งานจริงโดยเสนอภาพรวมการทำระบบบริหารและควบคุมความมั่นคงปลอดภัยสารสนเทศแบบบนลงล่าง (Top down) เริ่มตั้งแต่การวัดผล ติดตามตรวจสอบและควบคุมการบริหารความมั่นคงปลอดภัย ISO/IEC 27001 จึงเป็นรายละเอียดที่องค์กรไอทีจะต้องใช้เพื่อพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศเพื่อขอใบรับรอง (Certification) ต่อไป

9.2 ความสำคัญของ ISO/IEC 27001

9.2 ที่มาของความสำคัญสำหรับ ISO/IEC 27001

หัวใจสำคัญของระบบบริหารความมั่นคงปลอดภัยสารสนเทศนั้นอยู่ที่ 3 ปัจจัยหลักโดยพื้นฐานดังต่อไปนี้

1. ข้อมูลส่วนตัว ข้อมูลสำคัญขององค์กร
2. การบริหารความเสี่ยงจากเหตุการณ์และปัจจัยต่าง ๆ
3. บริหารระบบเพื่อป้องกันความมั่นคงปลอดภัยของข้อมูล

1. ข้อมูลส่วนตัว ข้อมูลสำคัญขององค์กร

- การรักษาความมั่นคงปลอดภัยด้านข้อมูลไม่ให้ถูกขโมย ลักลอบนำไปใช้ ดัดแปลง หรือทำให้เกิดข้อผิดพลาดอื่นใด ซึ่งสำหรับหลายหน่วยงานอาจเป็นอันตรายระดับวิกฤติได้ ซึ่งข้อมูลนี้ไม่เพียงเฉพาะข้อมูลสำคัญขององค์กรแต่ยังรวมถึงข้อมูลส่วนตัว ของลูกค้าหรือบุคคลที่สามที่เกี่ยวข้องอื่น ๆ ด้วย

2. การบริหารความเสี่ยงจากเหตุการณ์และปัจจัยต่าง ๆ

- การบริหารความเสี่ยงจากเหตุการณ์และปัจจัยต่าง ๆ ซึ่งปัจจุบันมีการคำนึงถึงการตั้งไซต์สำรอง ในลักษณะของศูนย์สำรองข้อมูลและดำเนินการกู้คืนระบบภายหลังภัยพิบัติหรือ Disaster Recovery Center (DRC) ซึ่งมีความสำคัญมากในหลายธุรกิจเช่น ธุรกิจการเงิน หรือบริการด้านสุขภาพ เพราะข้อมูลเหล่านั้นมีความสำคัญยิ่งยวดต่อความสามารถในการดำเนินธุรกิจให้ต่อเนื่องต่อไปได้ (Business continuity)

3. บริหารระบบเพื่อป้องกันความมั่นคงปลอดภัยของข้อมูล

ปัจจัยในการพิจารณาความมั่นคงปลอดภัยของระบบสารสนเทศ:

- ความลับของข้อมูล (Confidentiality)
- ความถูกต้องสมบูรณ์ของข้อมูล (Integrity)
- ความพร้อมใช้งานของข้อมูล (Availability)
- การยืนยันตัวตนของผู้ใช้ (Authentication)
- การควบคุมสิทธิในการใช้งานของผู้ใช้ (Authorization)
- การไม่สามารถปฏิเสธการกระทำ (Non repudiation)

ทำไมต้องนำมาตรฐานมาใช้

- มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานด้านการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศที่ผ่านการระดมสมอง อภิปราย และโหวตรับรองโดยประเทศที่เป็นสมาชิก นอกจากนี้มีในกระบวนการพัฒนามาตรฐานระดับสากลได้เปิดโอกาสให้ตัวแทนของแต่ละประเทศ องค์กรวิชาชีพ ได้เข้ามามีส่วนร่วม โดยมีเป้าหมายเพื่อให้เกิดการยอมรับในระดับสากล
- องค์กรที่ต้องการทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ หากต้องการสร้างระบบที่ได้รับการยอมรับอย่างแพร่หลาย ควรนำมาตรฐานสากลมาประยุกต์ใช้จะเป็นผลดีกว่าการกำหนดมาตรฐานเอง ซึ่งต้องใช้เวลาและผู้เชี่ยวชาญในการพัฒนา นอกจากนี้ยังอาจมีปัญหาเรื่องการยอมรับจากภายนอก
- การเลือกมาตรฐานมาใช้ ต้องพิจารณาถึงวัตถุประสงค์ ถ้าต้องการใบรับรอง ต้องดูว่าจะใช้ภายในหรือต่างประเทศด้วย

ข้อดีของการประยุกต์ใช้มาตรฐานสากล

- เป็นที่ยอมรับระดับสากล รู้จักแพร่หลายทั่วโลก
- มีการตรวจประเมินเพื่อรับรองมาตรฐาน โดยองค์กรที่ไม่มีส่วนได้เสีย (Third Party Certification Body)
- มีองค์ความรู้ หนังสือ การสัมมนา ที่ปรึกษาและผู้เชี่ยวชาญ
- เป็นมาตรฐานที่ไม่ผูกมัดกับเทคโนโลยี เทคนิค หรือ ขั้นตอนที่เฉพาะเจาะจง ผู้จัดทำระบบสามารถเลือกเทคโนโลยีได้ตามความเหมาะสมทำให้มาตรฐานมีความคล่องตัวสูง

9.3 สิ่งที่ควรทราบก่อนนำมาตรฐานมาประยุกต์ใช้

สิ่งที่ควรทราบก่อนนำมาตรฐานมาประยุกต์ใช้

- ISO/IEC 27001 เป็นภาษาอังกฤษ ส่วนของไทยก็มีมาตรฐานของคณะกรรมการธุรกรรมฯ องค์กรที่จัดทำระบบนี้ต้องมีความรู้ในภาษาอังกฤษระดับที่สามารถตีความข้อกำหนดได้อย่างถูกต้อง

- การประยุกต์ใช้มาตรฐาน ต้องมาตีความข้อกำหนดและวางแนวทางปฏิบัติให้สอดคล้อง หากตีความผิดหรือไม่ครบถ้วนก็อาจเกิดปัญหาในการตรวจประเมินเพื่อขอการรับรองได้

พื้นฐานความมั่นคงปลอดภัยของสารสนเทศ

- Information Security Management System (ISMS) Standard หรือที่รู้จักกันในนาม ISO/IEC 27001 เป็นมาตรฐานที่เกี่ยวกับการบริหารจัดการข้อมูลสารสนเทศให้มั่นคงปลอดภัย
- ซึ่งรวมถึงเรื่องไอที เรื่องคน เรื่องกฎระเบียบขององค์กร เรื่องจัดซื้อจัดจ้าง เรื่องการฝึกอบรมพนักงาน เป็นต้น เหล่านี้ล้วนเกี่ยวข้องกับการบริหารจัดการข้อมูลสารสนเทศให้มั่นคงปลอดภัย
- ต่อให้มีระบบไอทีล้ำเลิศแค่ไหนแต่ถ้าไม่มีกฎระเบียบควบคุมที่ชัดเจน ไม่มีการอบรมให้ความรู้ผู้ใช้ และไม่มีการควบคุม Outsource ที่ดีพอ องค์กรนั้นก็จะทำงานด้วยความยากลำบาก
- ยิ่งองค์กรมีระบบไอทีดีแต่ขาดมาตรการควบคุม พนักงานก็ใช้ทรัพยากรไปกับเรื่องที่ไม่สมควรและหลายคนทำผิดกฎหมาย เช่น พนักงานใช้คอมพิวเตอร์ขององค์กรโหลดหนังและแชร์ไฟล์ที่ละเมิดลิขสิทธิ์ แบบนี้เสี่ยงต่อการโดนจับและเสียหายต่อองค์กรแน่นอน

พื้นฐานความมั่นคงปลอดภัยของสารสนเทศ (ต่อ)

- การจัดทำระบบบริหารจัดการ (Management System) จะต้องพิจารณาหลายด้านที่มีความเกี่ยวข้อง
  - การบริหารคน (ภายในองค์กรและภายนอก เช่น Outsource)
  - กระบวนการและเทคโนโลยี (เข้าใจกระบวนการทำงาน และเทคโนโลยีที่เหมาะสมในการนำมาใช้งาน)
  - บริหารงบประมาณ (การลงทุนที่คุ้มค่า)
- ซึ่งเราต้องเข้าใจทั้ง 3 ด้านข้างต้น เพื่อที่จะหาจุดสมดุลย์และเกิดประโยชน์สูงสุด อย่างไรก็ตามเมื่อลงมือทำจริงมันมีอะไรเต็มไปหมดที่ต้องทำความเข้าใจ จะได้วางแนวทางปฏิบัติให้เหมาะสม ไม่เข้มงวดเกินไปจนทำอะไรไม่ได้ (มั่นคงปลอดภัยสูงสุด) หรือหลวมเกินไปจนแทบไม่ได้ควบคุมอะไรเลย

ISO/IEC 27001 มาตรฐานสากลที่ทั่วโลกยอมรับ

- องค์กร ISO - International Organization for Standardization เป็นหน่วยงานที่ให้กำเนิดมาตรฐาน ISO/IEC 27001 โดยเวอร์ชันล่าสุดคือ ISO/IEC 27001:2013 ประกาศเมื่อ 1 ต.ค. 2013
- ส่วนเวอร์ชันแรกประกาศใช้ครั้งแรกเมื่อปี 2550 (ISO/IEC 27001:2005) หลังจากประกาศใช้ก็ได้รับความสนใจจากองค์กรทั้งภาครัฐและเอกชนทั่วโลก นำมาใช้งานและขอการรับรอง (Certification)
- ประเทศไทยเองก็ไม่แพ้ชาติใดในโลก มีหน่วยงานรัฐและเอกชนเริ่มทำISO/IEC 27001 และขอการรับรองได้สำเร็จ เช่น บริษัท ไทยออยล์ จำกัด (มหาชน) บริษัท ทรูอินเทอร์เน็ต ดาต้าเซ็นเตอร์ จำกัด(True IDC) และรัฐวิสาหกิจอีกหลายแห่ง
- มาตรฐานนี้ออกแบบมาให้ใช้ได้ประเภทธุรกิจ หน่วยราชการ สถานศึกษา และใช้ได้กับองค์กรทั้งขนาดเล็กและขนาดใหญ่อย่างบริษัทข้ามชาติ ก็ทำได้เหมือนกัน

ทำไปทำไม

- สมมติ เราไปใช้บริการหน่วยงานราชการแห่งหนึ่ง ปรากฏว่าระบบไอทีล่มให้บริการไม่ได้ เจอแบบนี้ประชาชนผู้ใช้บริการเดือดร้อนแน่นอน ผู้บริหารหน่วยราชการนั้นคงเหงื่อตกและเร่งแก้ปัญหาเฉพาะหน้าเป็นการด่วน
- แน่นอนว่าระบบสารสนเทศทุกวันนี้เปรียบเสมือนเส้นเลือดของธุรกิจ คงไม่ดีแน่ถ้าไอทีล่มบ่อยหรือข้อมูลหาย
- จะดีกว่า ถ้ามีระบบอะไรซักอย่างที่ทำให้แน่ใจได้ว่า ระบบข้อมูลสารสนเทศสามารถให้บริการตามปกติ ข้อมูลได้รับการปกป้อง และหากเกิดขัดข้องก็สามารถรับมือและกู้ระบบคืนได้ ระบบที่ว่านี้ก็คือ ISO/IEC 27001
- ดังนั้นการที่จะมั่นใจได้ว่าระบบฯของเรามีความมั่นคงปลอดภัย ก็คือเราจะต้องรู้ว่ามีภัยคุกคามอะไรบ้างที่อาจมาโจมตี ทำให้สารสนเทศของเราเกิดความเสียหาย จากนั้นจึงประเมินความเสี่ยงและกำหนดมาตรการจัดการกับภัยคุกคาม ให้แน่ใจว่าสามารถรับมือภัยคุกคามเหล่านั้นได้อย่างเหมาะสม

ISO/IEC 27001 ทำยากหรือไม่ กลัวจะทำไม่สำเร็จ

ควรมีความรู้และความเข้าใจ 2 เรื่องใหญ่ ๆ คือ

1. เข้าใจองค์กรตัวเอง
2. เข้าใจมาตรฐานว่าต้องทำอะไรบ้าง

1. เข้าใจองค์กรตนเอง

- ต้องสำรวจข้อมูลซอฟต์แวร์ ฮาร์ดแวร์ บุคลากร ในขอบเขตที่จัดทำระบบ ข้อมูลนี้ยิ่งมีรายละเอียดยิ่งดี หากหน่วยงานเราเป็นราชการ บัญชีครุภัณฑ์เป็นจุดเริ่มต้นที่ดีในการรวบรวมข้อมูลซอฟต์แวร์และฮาร์ดแวร์
- เข้าใจภารกิจขององค์กร รู้ว่าระบบงานใดสำคัญที่สุดและระบบงานต่าง ๆ มีข้อจำกัดและจุดอ่อนอะไรบ้าง รู้ไปทำไม? ก็รู้เพื่อที่จะไปหามาตรการควบคุมมาจัดการกำจัดจุดอ่อน เช่น ระบบฐานข้อมูลทำงานอยู่บนเครื่อง Server ที่เก่าแก่มาก เก่าขนาดที่ไม่มี Spare part หาก Server นี้พังไปก็โบกมือลาได้เลยเพราะซ่อมไม่ได้ ในกรณีนี้จุดอ่อนก็คือ Server ที่เก่าบุโรทั่ง มีความเสี่ยงที่จะลาโลกไปเมื่อไหร่ก็ได้ ดังนั้นเราก็ต้องหามาตรการควบคุมมาจัดการความเสี่ยงนี้ โดยการจัดหาเครื่องใหม่ ซึ่งปัจจุบันนิยมใช้เทคโนโลยี Virtualization เข้ามาบริหารจัดการ ทั้งนี้ก็แล้วแต่แนวทางและขีดความสามารถของแต่ละองค์กร

2. เข้าใจมาตรฐาน:

- การนำมาตรฐาน ISO/IEC 27001 มาใช้งาน ก็ต้องทำความเข้าใจในตัวมาตรฐานเสียก่อน ว่าต้องทำอะไรบ้าง ทั้งเรื่องเอกสาร (Documents) และการนำไปใช้งานจริง (Implementation) ข้อกำหนดของ ISO/IEC 27001:2013 ฉบับของ ISO -International Organization for Standardization นั้นเป็นภาษาอังกฤษ หากเราต้องการศึกษามาตรฐานฉบับเต็ม มี 2 วิธี
  - ติดต่อซื้อมาตรฐาน ISO/IEC 27001 จากเว็บไซต์ของ ISO
  - ไปขออ่านได้ที่ห้องสมุดสำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม สมอ. ตั้งอยู่ที่กระทรวงอุตสาหกรรม ตรงข้าม รพ.รามาฯ

งบประมาณเท่าไหร่พอ

- ใช้งบประมาณมากหรือน้อยขึ้นอยู่กับสิ่งที่องค์กรเรายังขาด เช่น
  - ประเมินความเสี่ยงมาแล้วพบว่าเรายังไม่มีระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (log) แบบนี้เรื่องใหญ่ เพราะผิดกฎหมาย!! เราจำเป็นต้องจัดหามาโดยด่วน หรือพบว่าเครื่อง Server ของเราเก่าบุโรทั่ง มีโอกาสลาโลกไปแบบไม่ฟื้นเมื่อไหร่ก็ได้ แบบนี้เราจำเป็นต้องมีงบประมาณเพื่อจัดหาใหม่มาทดแทน และที่พบค่อนข้างมากในหลายองค์คือไม่มีมาตรการควบคุมหรือเครื่องมือเฝ้าระวังตรวจจับทางด้านความมั่นคงปลอดภัยของสารสนเทศ อันนี้ จำเป็นต้องลงทุนจัดหามาใช้งาน
- สุดท้ายหากจะขอใบรับรอง ISO/IEC 27001 ก็ต้องมีค่าตรวจประเมินรับรอง ระบบ (Certification) ซึ่งตรวจประเมินโดยหน่วยงานที่เรียกว่า Certified body

เริ่มต้นยังไงดี (ต่อ)

- Step1: ก่อนอื่นเราต้องกำหนดขอบเขต (Scope) ที่จะทำ ISO/IEC 27001
- Step2: ศึกษามาตรฐาน ISO/IEC 27001 ให้เข้าใจหลักการพื้นฐานและแนวทางการนำไปใช้งาน
- Step3: การทำ Gap Analysis หรือทำการประเมินองค์กรเบื้องต้นให้รู้ว่าองค์กรยังขาดอะไรบ้างเมื่อเทียบกับสิ่งที่ต้องมีตามมาตรฐาน ISO/IEC 27001

เริ่มต้นยังไงดี (ต่อ)

- ***Step1: ก่อนอื่น ต้องกำหนดขอบเขต (Scope) ที่จะทำ ISO/IEC 27001 หรือพูดอีกอย่างหนึ่ง คือ ต้องการให้ระบบงานหรือกิจกรรมอะไรบ้างที่ถูกควบคุมดูแลภายใต้ ISO/IEC 27001 เพื่อให้มั่นใจว่าสารสนเทศของระบบงาน หรือกิจกรรมนั้น ๆ มีความมั่นคงปลอดภัย***
  - ขอบเขตเป็นสิ่งที่สำคัญมาก เพราะถ้าขอบเขตเล็กเกินไปไม่สะท้อน Performance เพียงพอ อาจจะมีปัญหาในตอนยื่นขอตรวจรับรองระบบ แต่ถ้าใหญ่เกินไปจะทำให้สำเร็จได้ยาก

เริ่มต้นยังไงดี (ต่อ)

- *Step2: ศึกษามาตรฐาน ISO/IEC 27001 ให้เข้าใจหลักการพื้นฐาน และแนวทางการนำไปใช้งาน*
  - สามารถไปขออ่าน (หรือสำเนาไว้ศึกษา แต่เวลาขอการรับรองแนะนำให้ซื้อฉบับที่มีลิขสิทธิ์) ได้ที่ห้องสมุดสำนัก งานมาตรฐานผลิตภัณฑ์อุตสาหกรรม (สมอ) กระทรวงอุตสาหกรรม
  - หรือสั่งซื้อฉบับมีลิขสิทธิ์จากเว็บของ ISO
  - อ่านข้อกำหนดฉบับแปลภาษาไทยของ T-NET หรือ BSI

เริ่มต้นยังไงดี (ต่อ)

- *Step3: การทำ Gap Analysis หรือทำการประเมินองค์กรเบื้องต้นให้รู้ว่าองค์กรยังขาดอะไรบ้างเมื่อเทียบกับสิ่งที่ต้องมีตามมาตรฐาน ISO/IEC 27001 ขั้นตอนนี้เราจะต้องมีความรู้ในข้อกำหนดของ ISO/IEC 27001 พอสมควร ถึงจะประเมินได้ว่าข้อไหนมีแล้วข้อไหนยังขาด*
  - การทำ ISO/IEC 27001:2013 Gap analysis คือการสำรวจตรวจสอบและประเมินสิ่งที่เป็นอยู่ ณ ปัจจุบัน (ก่อนเริ่มทำระบบ) เปรียบเทียบกับข้อกำหนดของ ISO/IEC 27001:2013 พูดอีกอย่างก็คือ การตรวจประเมินด้วยข้อกำหนด ISO/IEC 27001:2013 เพื่อดูว่าหน่วยงานมีอะไรอยู่แล้ว และยังขาดอะไรที่ต้องทำเพิ่ม

สำหรับการเริ่มต้นมี 3 step ข้างต้น หลังจากการประเมินองค์กรเบื้องต้นใน Step3 เราก็จะรู้ว่ายังขาดอะไรบ้าง มีประเด็นอะไรที่ยังไม่สอดคล้องตามกฎหมายหรือไม่ ถ้ามีก็ให้สรุปประเด็นเสนอผู้บริหารเพื่อเร่งดำเนินการ

The ISO/IEC 27001:2013 Certification Process

There are Three Core Phases

Phase I : Before External Audit

1. Implementation of ISMS

Complete of implementation cycle of Information security management system (ISMS) Including mandatory Requirements and optional Controls

2. Conduct Internal Audit and review result by top management

The organization conduct periodic internal audits to ensure the ISMS incorporates adequate controls which operate effectively and review it by Top Management

3. Selection of a Certification body

Organization select a Certification body " BSI , DNV, SGS " to conduct External audit activity and Certified Organization ISMS Program

Phase II : External Audit

4. Stage 1 Audit

Conducted off or on site to determine if your ISMS system has met the requirements of the standard and is capable of being audited.

5. Stage 2 Audit

Conduct on site to audit the effectiveness of the ISMS system. Stage 1 and Stage 2 must be completed to become ISMS certified.

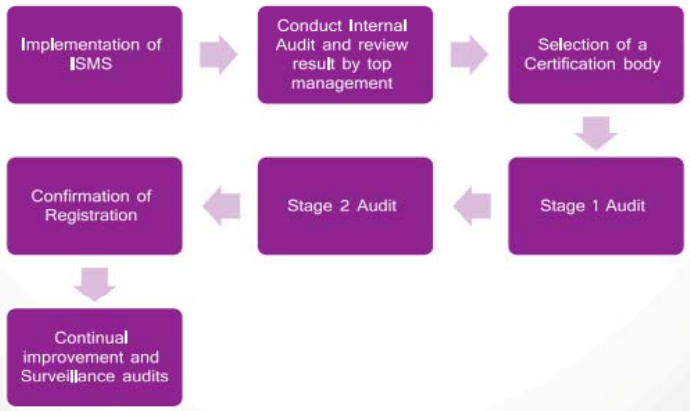
Phase III : Following the audit

6. Confirmation of Registration

Lead Auditor recommend to Certification Manager of Certification Body that Organization are certified.
The Certification Manager will review Organization file to ensure that the recommendation has been made in an impartial, fair and competent manner.
Upon completion of the above Organization will be officially certified to ISO/IEC 27001:2013 .

7. Continual improvement and Surveillance audits

Conduct Internal Audit Activity by Organization and Certification body auditor will conduct surveillance audit for organization every 6 months or 12 months for next three years after organization achieve ISO/IEC 27001:2013 Certification



www.bluekaizen.org

Example ISO 27001 Certification Implementation Approach

http://slideplayer.com/slide/8838138/

© Deloitte & Touche LLP and affiliated entities.

การออกใบรับรอง (Certification)

ในแง่ขององค์กร (Organization Certification)

- การออกใบรับรอง (Certification) เป็นวิธีหนึ่งที่จะสามารถรับรองได้ว่าองค์กรมีระบบบริหารความมั่นคงของข้อมูล (ISMS) ที่มีประสิทธิภาพ แต่การที่จะจัดทำระบบ ISMS จนถึงขั้นได้รับการรับรองนั้น ก็จะมีต้นทุนที่สูงพอสมควร ทั้งนี้ ขึ้นอยู่กับนโยบาย ความมุ่งมั่นของผู้บริหาร และความจำเป็นขององค์กร
- อย่างไรก็ตาม ถึงแม้ว่าองค์กรอาจจะไม่ได้มีความจำเป็นในการจัดทำระบบเพื่อให้ได้รับการรับรอง (Certification) แต่การนำแนวคิดของระบบ ISMS และหัวข้อการควบคุมที่กำหนดไว้ในมาตรฐาน ISO 27001 และ ISO 27002 ไปประยุกต์ใช้เพียงบางส่วน เพื่อปกป้องข้อมูลและระบบคอมพิวเตอร์ขององค์กรนั้น ก็มีประโยชน์ต่อองค์กรเป็นอย่างมาก โดยเฉพาะอย่างยิ่ง ต้นทุนของการดำเนินการเพื่อป้องกัน (Preventive) นั้น ย่อมน้อยกว่าและเทียบไม่ได้กับความเสียหายที่อาจเกิดขึ้นหรือต้นทุนที่ต้องใช้ในการแก้ปัญหาที่เกิดขึ้นแล้ว (Reactive)

การออกใบรับรอง (Certification) (ต่อ)

ในแง่ขององค์กร (Organization Certification) (ต่อ)

- สำหรับวิธีการยื่นขอใบรับรอง (Certification) ให้กับระบบบริหารความมั่นคงของข้อมูล (ISMS) นั้น จะมีขั้นตอนเหมือนกันกับการยื่นขอใบรับรองของระบบ ISO อื่น ๆ โดยต้องเริ่มจากการเลือกองค์กรที่จะเข้ามาทำการตรวจรับรองระบบ ซึ่งจะต้องเป็นองค์กรที่ได้รับการขึ้นทะเบียนอย่างถูกต้อง (Accredited)
- หลังจากนั้นจะต้องทำการกำหนดขอบเขตของระบบที่จะตรวจรับรอง เพื่อการวางแผนและดำเนินการตรวจรับรองอย่างมีประสิทธิภาพ ซึ่งเมื่อองค์กรได้รับการรับรองระบบ ISMS แล้วจะต้องได้รับการตรวจติดตามซ้ำ (Surveillance audit) ทุก ๆ 6 เดือน หรือ 1 ปี และทำการตรวจรับรองทั้งระบบใหม่ทั้งหมด (Re-Certification audit) ทุก ๆ 3 ปี

การออกใบรับรอง (Certification) (ต่อ)

ในแง่ของบุคคล (Individual Certification)

- เป็นการออกใบรับรอง (Auditor Certification) ให้กับบุคคลผู้ที่จะทำการตรวจรับรองระบบ (Auditor) เพื่อให้สามารถมั่นใจได้ว่าบุคคลผู้นั้นมีความรู้ ความชำนาญในระบบ ISMS และมีคุณสมบัติ เพียงพอที่จะดำเนินการตรวจสอบระบบ ISMS ได้ โดยองค์กรสากลที่ทำหน้าที่ควบคุมการออกใบรับรองให้กับผู้ตรวจสอบระบบ ก็คือ International Register of Certificated Auditors (IRCA)
- สำหรับคุณสมบัติของผู้ที่จะสามารถยื่นขอใบรับรอง (Auditor Certification) จาก IRCA ได้นั้นจะต้องผ่านการอบรมและการสอบในหลักสูตร ISO 27001 and ISO 27002 Information Security Management Systems Lead Auditor Training Course ที่ได้รับการรับรองจาก IRCA ซึ่งมีการจัดอบรมอยู่ในหลาย ๆ ประเทศทั่วโลก รวมทั้งในประเทศไทยด้วย พร้อมวุฒิการศึกษาขั้นต่ำในระดับปริญญาหรืออนุปริญญา และมีประสบการณ์อย่างน้อย 4 ปี

Estimated Time needed for Implementation and Certification ISO/IEC 27001:2013

Based on my Experience

Phase I : Estimated time needed for Implementation ISO/IEC 27001:2013

Estimated Duration needed for Implementation depend on Organization size

" Employees, Systems and Information "

- Small Organization : 50 - 150 Employee

Estimated time for Implementation of Standard from 6-8 Months

- Medium Organization : 150 - 400 Employee

Estimated time for Implementation of Standard from 10-12 Months

- Large Organization : 400 to 1000+ Employee

Estimated time for Implementation of Standard from 13-16 Months

Phase II : Estimated Time needed for Certification ISO/IEC 27001:2013

Case 1 : if there is one or more Minor Nonconformity and the organization try to Correct them accordingly the Certificate can be Issued around a Month

Case 2 : if there is one or more Major Nonconformity and the organization try to Correct them accordingly the Certificate can be Issued around 3-5 Months

9.4 เปรียบเทียบ ISO/IEC 27001:2005 และ ISO/IEC 27001:2013

เปรียบเทียบ ISO/IEC 27001:2005 และ ISO/IEC 27001:2013

ISO/IEC 27001:2005	ISO/IEC 27001:2013
132 “shall” statements (section 4-8)	125 “shall” statements (section 4-10)
Annexure A	Annexure A
-11 clauses	-14 clauses
-39 categories	-35 categories
-133 controls	-114 controls

ข้อกำหนดหลัก ๆ มีการเปลี่ยนแปลงไหม?

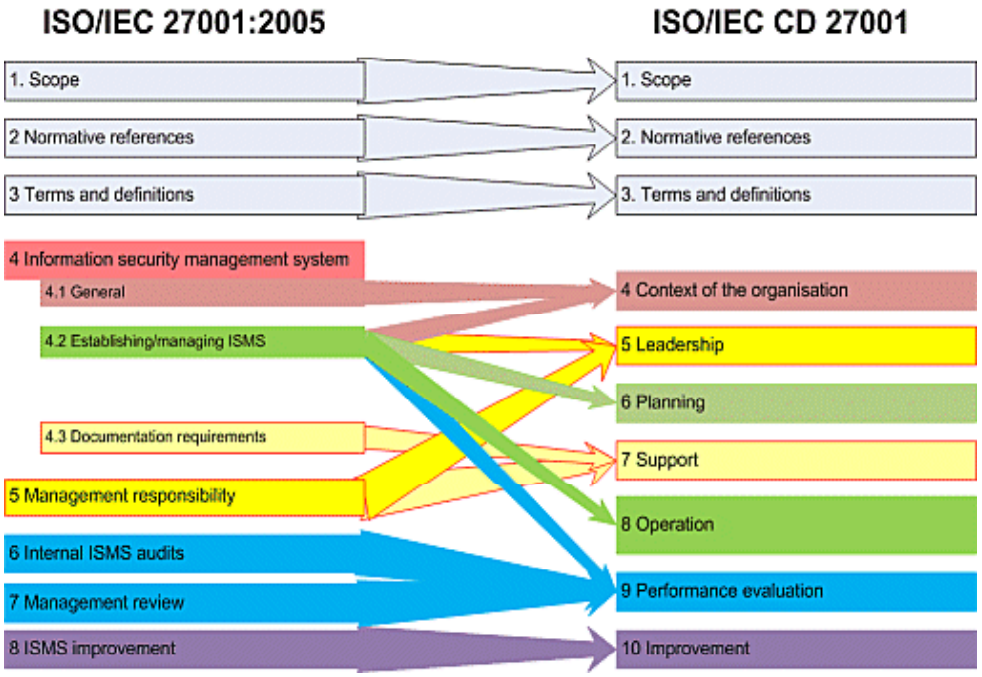
- จุดประสงค์โดยทั่ว ๆ ไปและสิ่งที่เน้น ของมาตรฐาน ISO/IEC 27001:2013 ยังคงเหมือนเดิมคือการระบุถึงความเสี่ยงของความมั่นคงปลอดภัยของข้อมูลที่อาจเกิดขึ้นกับองค์กร
- Version ใหม่นี้จะให้ความสำคัญในแง่มุมธุรกิจมากขึ้น โดยมุ่งเน้นที่ความจำเป็นในการให้ความสำคัญกับสภาพแวดล้อม/บริบทขององค์กร มากยิ่งขึ้น และให้สอดคล้องกับความต้องการทางธุรกิจทั้งภายในและภายนอกมากขึ้น
- อย่างไรก็ตาม มีมาตรฐานบางส่วนที่มีการเปลี่ยนโครงสร้างใหม่เพื่อให้เป็นไปตามข้อกำหนดของ มาตรฐานระบบบริหารจัดการยุคใหม่ นอกจากนี้มาตรฐาน ISO/IEC 27001:2013 New Version ยังสอดคล้องกับข้อปฏิบัติและ Risk Terminology ของมาตรฐานการบริหารจัดการความเสี่ยง ISO 31000 อีกด้วย

เปรียบเทียบ ISO/IEC 27001:2005 และ ISO/IEC 27001:2013 (ต่อ)

- มาตรฐาน ISO/IEC 27001:2013 มีการพัฒนา “กรอบความคิดในแง่ของการบริหารจัดการ” เพื่อให้มีการระบุถึงมุมมองของความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูลใน แง่มุมของการดำเนินธุรกิจ ซึ่งได้แก่ การระบุถึงภัยคุกคามต่าง ๆ ที่ธุรกิจในปัจจุบันต้องเผชิญ เช่น ภัยคุกคามจากโลกไซเบอร์ การโจมตีระบบโทรศัพท์เคลื่อนที่ การโจรกรรมข้อมูลส่วนบุคคล เป็นต้น

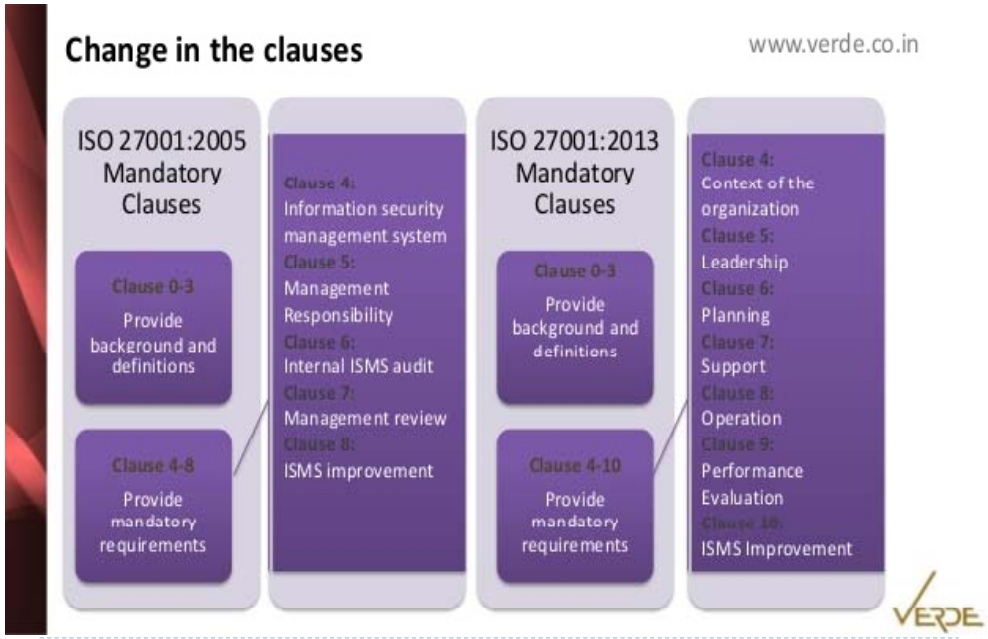
เปรียบเทียบ ISO/IEC 27001:2005 และ ISO/IEC 27001:2013 (ต่อ)

- ในเวอร์ชันใหม่ของ ISO/IEC 27001 ส่วนระบบบริหารจัดการ (management system) จะถูกปรับเปลี่ยนให้เป็นไปตาม Annex SL
- ซึ่งต่อไปจะโครงสร้างมาตรฐานใหม่ที่จะถูกใช้มาตรฐาน ISO ทั้งหมด
- โดยวัตถุประสงค์ของ Annex SL คือเพื่อทำให้โครงสร้าง คำจำกัดความและนิยามของมาตรฐานต่าง ๆ ในระบบบริหารจัดการที่เป็น ISO เป็นไปในทิศทางเดียวกัน อีกทั้งสนับสนุนให้องค์การที่มีการทำระบบบริหารจัดการ (Management system) มากกว่าหนึ่งมาตรฐานสามารถควบรวมและทำงานประสานกันได้เป็นอย่างดีในโครงสร้างมีข้อกำหนดทั้งหมด 10 ข้อ จากเดิม 8 ข้อ



 http://www.isotoyou.com/index.php/article/447-ISO/IEC 27001 -dis-what-change.html

เปรียบเทียบ ISO/IEC 27001:2005 และ ISO/IEC 27001:2013 (ต่อ)



 http://es.slideshare.net/VerdeVenturesPvtLtd/transition-to-ISO -27001-2013/5

Structure

All Below from 4 to 10 are Mandatory Requirements for Implementation and Certification of ISO/IEC 27001:2013

0. Introduction
The Objective of an Information Security Management System (ISMS)

1. Scope
State the Applicability of Standard within Context of Organization

2. Normative References
Overview and Vocabulary

3. Terms and Definitions
a brief, formalized glossary Including Common Terms and Definition of ISMS

4. Context of Organization
It has to determine organization needs and Expectations and Interested Parities

5. Leadership
Establish role of Top management toward ISMS

6. Planning
Establish Organization Strategic Objects and Risk Management

7. Support
Determined Organizational Resources and Competencies Requirements and Standard Documentation Required

8. Operation
The Information Security Requirements of the ISMS and way to address it

9. Performance Evaluation
Measurement of ISMS Performance

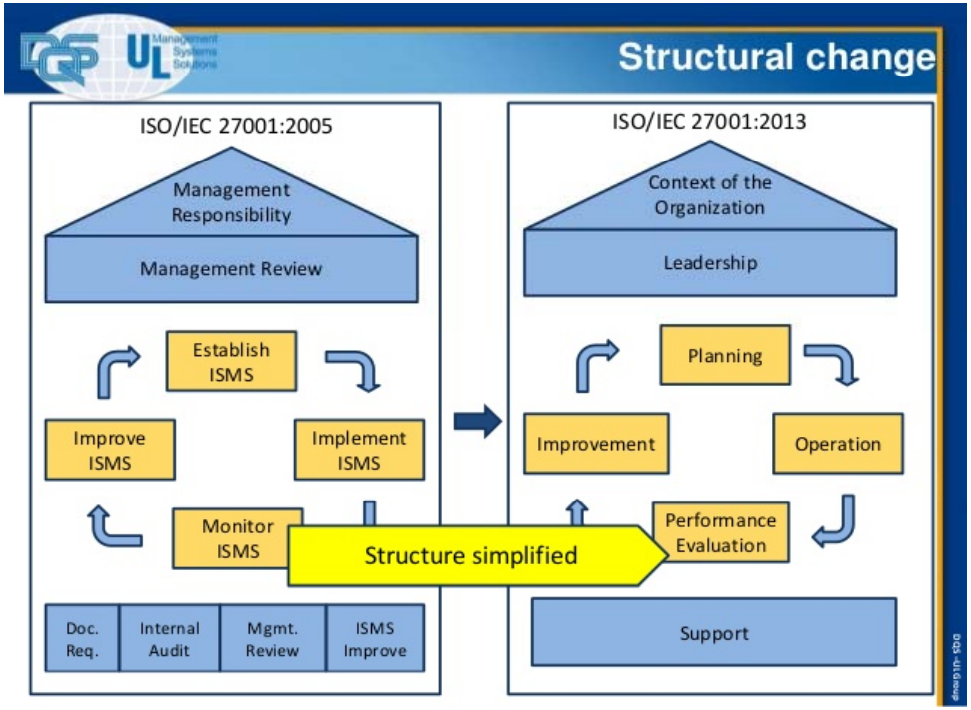
10. Improvement
Identify and act toward nonconformity of ISMS through Corrective Action and Ensure of Continual improvement of ISMS

สิ่งที่เปลี่ยนไปในตัวระบบบริหารจัดการ (ข้อกำหนด Clause 1-10) สรุปได้ดังนี้

- คำจำกัดความในเวอร์ชัน 2005 ทั้งหมดถูกย้ายไปอยู่ใน มาตรฐาน ISO/IEC 27000 เปลี่ยนเทอมที่ใช้ เช่น “ISMS Policy” เป็น “Information Security Policy” ให้ชื่อเป็นกลาง ๆ มากขึ้น เปลี่ยนชื่อหัวข้อ ข้อกำหนดการบวนการประเมินความเสี่ยงก็ลงรายละเอียดน้อยลง นั่นหมายความว่าเรามีทางเลือกสำหรับวิธีการในการประเมินความเสี่ยงที่หลากหลายขึ้น แต่ถ้าองค์กรของเรา คิดว่าการประเมินความเสี่ยงที่ทำอยู่ดี/เหมาะอยู่แล้วก็ไม่จำเป็นต้องปรับเปลี่ยนอะไรซึ่งเราสามารถใช้ทั้ง ISO/IEC 27005 และ ISO 31000 (Enterprise Risk Management) เป็นไกด์ในสร้างวิธีการประเมินความเสี่ยง ข้อกำหนดที่เกี่ยวกับพันธสัญญาของผู้บริการ (Management commitment) เป็น “Leadership”
- ข้อกำหนดที่เกี่ยวกับการบริหารจัดการทรัพยากร (Resource management) เป็น “Support”

ข้อกำหนดใหม่ในส่วนที่เกี่ยวกับเรื่อง “Top Management Leadership”

- ในหมวดที่เกี่ยวกับ บทบาทของผู้นำองค์กร ที่เพิ่มขึ้นมาในมาตรฐาน ISO/IEC 27001:2013
- เป็นการให้ผู้บริหารแสดงถึงความรับผิดชอบและการมีนโยบายเชิงรุกในแนวทาง ปฏิบัติและกิจกรรมต่างๆที่เกี่ยวข้องกับ การสร้าง การนำไปปฏิบัติ การดำเนินการ การติดตามการดำเนินงาน การทบทวนผลการดำเนินงาน การดูแลให้มีการดำเนินงานอย่างต่อเนื่อง และการพัฒนาระบบการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลให้เป็นไปตามข้อกำหนดของมาตรฐาน ISO/IEC 27001:2013



http://www.slideshare.net/ULDQSInc/iso-27001-transition-to-2013-03202014

เอกสารที่ต้องจัดทำ (Documentation) เวอร์ชันใหม่ไม่เน้นว่าต้องจัดทำเอกสารอะไรบ้าง

- ไม่ต้องมีการตั้งคำถามว่า ต้องทำเอกสาร/คู่มืออะไรบ้าง เอกสารชื่ออะไร ถ้าจะทำระบบ ISO/IEC 27001 ไม่ต้องถามหาบัญชีรายชื่อเอกสารที่ต้องจัดทำ
- เวอร์ชันใหม่เน้นไปที่เน้นหาของเอกสารไม่ใช่ชื่อ และเน้นไปที่ผลลัพธ์ในการดำเนินงานของระบบ
- เกิดคำใหม่ คือ “Documented information” แทนที่ เอกสาร และบันทึก แต่วิธีการควบคุมก็ไม่ต่างจากของเดิม

ข้อกำหนดเรื่องการพัฒนา (Improvement)

- การป้องกัน (Preventive action) ถูกตัดออกจากข้อกำหนดนี้ และเข้าไปรวมเป็นส่วนหนึ่งของการประเมินความเสี่ยง เพราะการทำงานเชิงป้องกันนั้นถือเป็นแนวคิดหนึ่งในการประเมินความเสี่ยง
- ข้อกำหนดย่อยจะเหลือแค่ความไม่สอดคล้องและการปรับปรุงแก้ไข (Nonconformity and corrective action) และการพัฒนาอย่างต่อเนื่อง (Continual improvement) เท่านั้น

ข้อกำหนดของ ISO/IEC 27001:2013

ภาพรวมของข้อกำหนดมาตรฐาน ISO/IEC 27001:2013 Information Security Management System (ISMS)

- บริบทขององค์กร (Context of the organization)
- ภาวะผู้นำ (Leadership)
- การวางแผน (Planning)
- การสนับสนุน (Support)
- การดำเนินการ (Operation)
- การประเมินประสิทธิภาพและประสิทธิผล (Performance evaluation)
- การปรับปรุง (Improvement)

4. บริบทขององค์กร (Context of the organization)

4.1 ทำความเข้าใจองค์กรและบริบทขององค์กร (Understanding the organization and its context)

- พื้นฐานสำคัญในการวางระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013 คือความเข้าใจบริบทขององค์กร โดยต้องระบุประเด็นภายใน(Internal issues) และประเด็นภายนอก (External issues) นำทั้ง 2 ประเด็นนี้มาพิจารณาในการวางระบบให้ครอบคลุมอย่างเหมาะสมไม่ตกหล่นประเด็นสำคัญ

4. บริบทขององค์กร (Context of the organization) (ต่อ)

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

- ในการทำ ISO/IEC 27001 จะต้องรู้ว่าใครคือผู้เกี่ยวข้อง (Interested parties) และพวกเขามีความต้องการและคาดหวังอะไร (Needs and expectations) จากองค์กรของเรา ระบบงานใดมีความสำคัญเพราะเป็นงานที่เกี่ยวข้องกับการส่งมอบสินค้าหรือบริการให้กับผู้เกี่ยวข้อง บริบทขององค์กรเป็นข้อมูลสำคัญในการกำหนดขอบเขตของการจัดทำระบบ (Scope)

4. บริบทขององค์กร (Context of the organization) (ต่อ)

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

- ขอบเขต (Scope) ของการทำ ISO/IEC 27001:2013 ต้องพิจารณาถึงข้อกำหนดและความต้องการของผู้เกี่ยวข้อง (Interested parties) ตรงนี้เป็นเงื่อนไขสำคัญที่องค์กรต้องทำความเข้าใจและกำหนดขอบเขตให้เหมาะสมและเพียงพอคือไม่กำหนดขอบเขตเล็กเกินไปจนตกหล่นผู้เกี่ยวข้อง หรือขอบเขตกว้างเกินกว่าความสามารถในการบริหารจัดการส่งผลให้ระบบขาดประสิทธิภาพ

4. บริบทขององค์กร (Context of the organization) (ต่อ)

4.4 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security management system)

- จัดทำระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) โดยกำหนดนโยบาย จัดทำเอกสารที่เกี่ยวข้อง นำไปปฏิบัติและรักษาไว้ รวมถึงปรับปรุงอย่างต่อเนื่อง โดย ISMS ต้องสอดคล้องตามข้อกำหนดของ ISO/IEC 27001:2013 Information Security Management System

5. ภาวะผู้นำ (Leadership)

5.1 ภาวะผู้นำและการให้ความสำคัญ (Leadership and commitment)

ผู้บริหารระดับสูงต้องแสดงให้เห็นถึงภาวะผู้นำและให้ความสำคัญต่อระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)

5.2 นโยบาย (Policy)

ผู้บริหารระดับสูงกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับจุดประสงค์ขององค์กรและสอดคล้องกับข้อกำหนด

5.3 บทบาท หน้าที่ความรับผิดชอบ และอำนาจหน้าที่ (Organizational roles, responsibilities and authorities)

กำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยของสารสนเทศ

6. การวางแผน (Planning)

6.1 การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส (Actions to address risks and opportunities)

- การวางแผนงานสำหรับระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ จะต้องพิจารณาถึงบริบทขององค์กร พิจารณาความเสี่ยงที่เกี่ยวข้องจากนั้นวางแนวทางจัดการอย่างเหมาะสม

6.2 วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและแผนการบรรลุวัตถุประสงค์ (Information security objectives and plans to achieve them)

- กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ(Information Security Objectives) และแผนการบรรลุวัตถุประสงค์ โดยวัตถุประสงค์นี้จะต้องวัดผลได้ และสอดคล้องกับนโยบายความมั่นคงปลอดภัยของสารสนเทศ (Information Security Policy)

7. การสนับสนุน (Support)

7.1 ทรัพยากร (Resources)

- การทำระบบให้สำเร็จจำเป็นต้องมีทรัพยากรเพียงพอและเหมาะสม ประกอบด้วย บุคลากร เวลา งบประมาณ และการสนับสนุนจากผู้บริหารอย่างเป็นรูปธรรม

7.2 สมรรถนะ (Competence)

- บุคลากรที่มีส่วนร่วมในการจัดทำระบบจะต้องมีความรู้ความสามารถ ซึ่งต้องมีการให้ความรู้ที่ตรงกับภาระหน้าที่เพื่อให้บุคลากรสามารถปฏิบัติได้อย่างถูกต้อง

7.3 การสร้างความตระหนัก (Awareness)

- ความตระหนักเป็นเรื่องสำคัญในด้านความมั่นคงปลอดภัยของสารสนเทศ เพราะหากบุคลากรมีความตระหนักที่เพียงพอ ย่อมจะลดความเสี่ยงได้โดยปริยาย เช่น เรื่องการใช้รหัสผ่านที่แข็งแรงเดายาก ถ้าบุคลากรมีความตระหนักก็จะเข้าใจและปฏิบัติตามส่งผลการความเสี่ยงลดลง

7. การสนับสนุน (Support) (ต่อ)

7.4 การสื่อสาร (Communication)

- การสื่อสารประกอบด้วยสื่อสารภายใน (Internal Communication) และการสื่อสารภายนอก (External Communication) เพื่อให้ความรู้ ข่าวสารที่เป็นประโยชน์ เป็นวิธีในการสร้างความตระหนักที่ได้ผลดี

7.5 เอกสารสารสนเทศ (Documented information)

- เอกสารมีความจำเป็นในการทำงานร่วมกันเพื่อให้เกิดความชัดเจนแก่ผู้ปฏิบัติและผู้ตรวจสอบ (Auditor) เอกสารในระบบ ISO/IEC 27001:2013 นั้นจะต้องผ่านการจัดทำโดยผู้ที่มีความรู้ มีผู้ทบทวน และอนุมัติก่อนจะนำไปใช้งาน

8. การดำเนินการ (Operation)

8.1 การวางแผนที่เกี่ยวข้องกับการดำเนินการและการควบคุม (Operational planning and control)

- ข้อนี้กล่าวถึงการปฏิบัติตามแผนที่วางไว้ โดยลงมือปฏิบัติตามแผนจัดการความเสี่ยง

8.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment)

- ประเมินความเสี่ยงต้องทำเป็นระยะ ไม่ใช่ทำครั้งเดียวจบ เพราะเมื่อเวลาผ่านไปก็จะมีความเสี่ยงใหม่เกิดขึ้นมา ไม่ว่าจะเป็นความเสี่ยงจากเทคโนโลยีใหม่ ๆ หรือสภาพแวดล้อม สังคมและการเมือง

8. การดำเนินการ (Operation) (ต่อ)

8.3 การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk treatment)

- Information Security Risk Treatment เป็นเครื่องมือการจัดการความเสี่ยงที่จัดทำขึ้นภายหลังการประเมินความเสี่ยงของทรัพย์สินสารสนเทศ โดยกำหนดรายละเอียดขั้นตอนวิธีการต่าง ๆ เพื่อนำไปปฏิบัติให้ได้ผลลัพธ์ตามที่กำหนดไว้

9. การประเมินประสิทธิภาพและประสิทธิผล (Performance evaluation)

9.1 การเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมิน (Monitoring, measurement, analysis and evaluation)

- เรื่องสำคัญที่พลาดไม่ได้คือ การเฝ้าระวัง (Monitor) การวัด (Measure) การวิเคราะห์ (Analyze) และการประเมิน (Evaluate) performance ของระบบ ทำให้รู้ได้ว่าผลลัพธ์เป็นไปตามที่วางแผนหรือไม่อย่างไร

9.2 การตรวจประเมินภายใน (Internal audit)

- การตรวจประเมินภายใน (Internal Audit) เป็นเครื่องมือสำคัญที่ทำให้รู้ว่าระบบที่เราจัดทำขึ้นมานั้น มีความสมบูรณ์จัดทำครบถ้วนตามข้อกำหนด มีการนำไปปฏิบัติหรือไม่ และได้ผลลัพธ์เป็นอย่างไร ตรวจสอบความเข้าใจ การปฏิบัติและเอกสารบันทึกที่เกี่ยวข้อง

9. การประเมินประสิทธิภาพและประสิทธิผล (Performance evaluation) (ต่อ)

9.3 การทบทวนของผู้บริหาร (Management review)

- Management Review เป็นการประชุมเพื่อรายงานผลของการจัดทำระบบ ISO/IEC 27001:2013 Information Security Management (ISMS) ต่อผู้บริหารระดับสูง (Top Management) โดยรายงานถึงการเปลี่ยนแปลงภายในและภายนอกที่มีผลกระทบต่อระบบฯ ผลการประเมินความเสี่ยงและการจัดการความเสี่ยง ผลการเฝ้าระวังด้าน Information Security ผลการตรวจประเมินภายใน (Internal Audit) ข้อบกพร่องจากการตรวจประเมินภายใน เป็นต้น

10. การปรับปรุง (Improvement)

10.1 ความไม่สอดคล้องและการดำเนินการแก้ไข (Nonconformity and corrective action)

- การระบุความไม่สอดคล้อง (Nonconformity: NC) และแก้ไขความไม่สอดคล้อง (Corrective action) อย่างเป็นระบบ มีผู้รับผิดชอบและมีบันทึกที่เป็นลายลักษณ์อักษรเกี่ยวกับความไม่สอดคล้องและแนวทางการแก้ไข

10.2 การปรับปรุงอย่างต่อเนื่อง (Continual improvement)

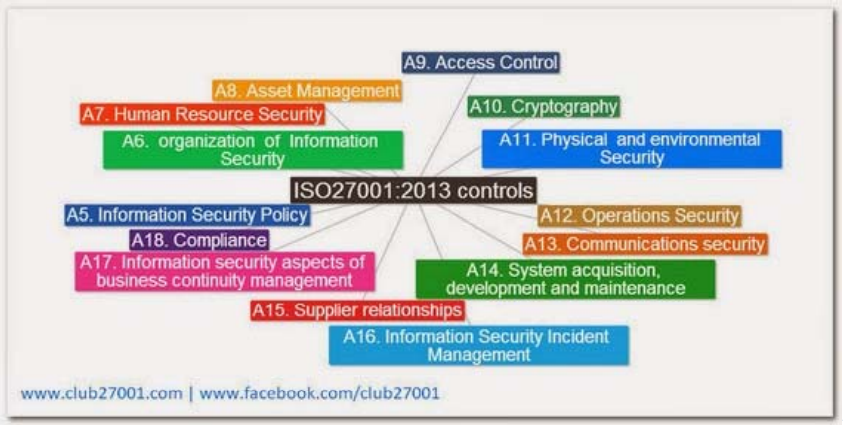
- ข้อกำหนดระบุให้องค์กรปรับปรุงระบบให้มีความเหมาะสม เพียงพอ และมีการปรับปรุงอย่างต่อเนื่อง

ประโยชน์ที่ได้จาก ISO/IEC 27001:2013

- โครงสร้างมาตรฐาน ISO/IEC 27001:2013 จะช่วยให้องค์กรต่าง ๆ สามารถใช้ระบบการบริหารจัดการได้มากกว่า 1 ระบบในคราวเดียวกัน
- เพราะโครงสร้างระบบบริหารของมาตรฐานต่าง ๆ มีความเหมือนกันมากขึ้น ซึ่งจะช่วยให้ประหยัดงบประมาณและเวลาในการนำมาตรฐานเหล่านี้มาใช้พร้อม ๆ กัน เนื่องจากสามารถนำนโยบายและกระบวนการดำเนินงานมาปรับใช้ร่วมกันได้
- เช่น องค์กรอาจใช้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001) มาใช้ร่วมกับระบบบริหารจัดการอื่นๆ เช่น ระบบการบริหารจัดการความต่อเนื่องทางธุรกิจ (มาตรฐาน ISO/IEC 22301) การบริหารจัดการการให้บริการระบบเทคโนโลยี (ISO/IEC 20001-1) หรือระบบการบริหารจัดการคุณภาพ (ISO 9001) เป็นต้น

มาตรการควบคุม (Control) จัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013

- การบริหารจัดการสารสนเทศในองค์กรให้มั่นคงปลอดภัยตามมาตรฐาน **ISO/IEC 27001:2013** นั้น จำเป็นต้องมีมาตรการควบคุมที่เหมาะสมกับ**ความเสี่ยงของสารสนเทศ (Information Security Risk)**



มาตรการควบคุม (Control) จัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013 (ต่อ)

- ในการจัดทำและดำเนินระบบ (ISMS Establishment and Implementation) ISO/IEC 27001:2013 มีมาตรการควบคุมให้เราเลือกมาใช้มากมายครอบคลุมตั้งแต่เรื่องคน (Human) เรื่อง Hardware Software และอื่น ๆ
- เราสามารถนำมาตรการควบคุมเหล่านี้มาใช้งาน (Implementation) และวางระบบเฝ้าระวังตรวจสอบ (ISMS Monitoring and Measurement) เพื่อวัดผลว่ามาตรการควบคุมนั้น ๆ มีประสิทธิภาพเพียงพอที่จัดการความเสี่ยงได้อย่างเหมาะสมหรือไม่
- ซึ่งในที่นี้จะขอนำเสนอมาตรการควบคุมจัดการความมั่นคงปลอดภัยของสารสนเทศตาม **Annex A** ของ ISO/IEC 27001:2013

Annex A

- สำหรับ Annex A ใน ISO/IEC 27001 มีการจับกลุ่มใหม่ เปลี่ยนจาก 11 โดเมน เป็น 14 โดเมน แต่ลด control ลงจาก 133 เป็น 114 ถ้าองค์กรของคน ได้การรับรอง ISO/IEC 27001:2005 อยู่แล้วก็แทบจะไม่ต้องปรับอะไรเลย สำหรับ Annex A การจับกลุ่มใหม่มีรายละเอียดดังนี้
  - ดึงหัวข้อ A.12.3 Cryptographic controls มาตั้งเป็น โดเมนใหม่ คือ A.10 Cryptography
  - แยกหัวข้อ A.10 Communications and operations management ออกเป็นสองหัวข้อย่อย คือ A.12 Operations Security และ A.13 Communications Security
  - รวมหัวข้อที่เกี่ยวข้องกับ Supplier โดยรวมข้อย่อย A.6.2 External parties และ A.10.2 Third party service delivery management และตั้งเป็นโดเมนใหม่ที่เรียกว่า A.15 Supplier relationships

ISO/IEC 27001:2005 vs ISO/IEC 27001:2013

ISO/IEC 27001:2005
A.5 Security policy
A.6 Organisation of information security
A.7 Asset management
A.8 Human resources security
A.9 Physical and environmental security
A.10 Communications and operations management
A.11 Access control
A.12 Information systems acquisition,development and maintenance
A.13 Incident management
A.14 Business continuity management
A.15 Compliance

ISO/IEC 27001:2013
A.5 Security policies
A.6 Organisation of information security
A.7 Human resource security
A.8 Asset management
A.9 Access control
A.10 Cryptography (NEW)
A.11 Physical and environmental security
A.12 Operations security
A.13 Communications security
A.14 Systems acquisition, development and maintenance
A.15 Supplier relationships (NEW)
A.16 Incident management
A.17 Business continuity management
A.18 Compliance

http://flipscloud.com/iso-27001-2013/

Annex A Control Objective and Controls : 114 Security Controls

Annex A is the best known series of security control objectives for Implementation ISO/IEC 27001:2013

All Controls are Optional to be implemented

Annex A Consist of

- **»14 Control Area :** Core topic areas that Covered Most Aspects of Information Security
- **» 34 Control Objective :** Objectives of Control
- **» 114 Control :** Applicable Controls to be Implemented on ISMS Program

A.5: Information Security Policies
Manage and Update of Organization Information Security Policies

A.6: Organization of Information Security
Manage of Organization Information including: Identified Role and Responsibilities, Segregation of Duties, Mobile Devices and teleworking

A.7: Human resources security
Manage of Organization Human Resource including: During, prior Employment Relationship

A.8: Asset management
Manage of Organization Assets

A.9: Access Control
Manage and Control Access of Organization Information

A.10: Cryptographic
Control of Using Cryptographic inside Organization

A.11: Physical and environmental Security
Manage and Control of Organization Physical and environmental Access

A.12: Operations security
Manage and control all Operation security including : Operational Procedure and Responsibilities , logging and Monitoring , Technical vulnerability management and information systems audit

A.13: Communications Security
Manage and control Organization Communication Security including : Network security management and information transfer Controls

A.14: System acquisition, development, and maintenance
Manage and control System Development Cycle Including: identified and enforce security requirements , Secure of development system

A.15: Supplier Relationship
Manager suppliers relationship including : apply information security for supplier relationship and service delivery management

A.16: Information Security Incident management
Manage information security incident

A.17: Information Security aspects of Business Continuity Management
Manage information security Continuity and Redundancies

A.18: Compliance
Manage organization compliance with legal and contractual requirements

มาตรการควบคุม (Control) จัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013 (ต่อ)

มาตรการควบคุมมีทั้งหมด 14 ข้อ ได้แก่

- A5. นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)
- A6. โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of Information Security)
- A7. ความมั่นคงปลอดภัยสำหรับบุคลากร (Human Resource Security)
- A8. การบริหารจัดการทรัพย์สิน (Asset Management)
- A9. การควบคุมการเข้าถึง (Access Control)
- A10. การเข้ารหัสข้อมูล (Cryptography)
- A11. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)
- A12. ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations Security)

มาตรการควบคุม (Control) จัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013 (ต่อ)

- A13. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)
- A14. การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)
- A15. ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationships)
- A16. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)
- A17. ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)
- A18. ความสอดคล้อง (Compliance)

Annex A ของ ISO/IEC 27001:2005 และ ISO/IEC 27001:2013

ISO 27001:2013 ISMS Control Point and Control Objective Summary

ISO27k ref.		Description	Control Total
Discretionary	A5	Management direction for information security,	2
	A6	Organisation of information security,	7
	A7	Human Resource security,	6
	A8	Asset Management,	10
	A9	Access control,	13
	A10	Cryptography,	2
	A11	Physical and Environmental security,	15
	A12	Operations Security,	14
	A13	Communications Security,	7
	A14	System acquisition, Development and Maintenance,	13
	A15	Supplier Relationships,	5
	A16	Information Security Incident Management,	7
	A17	Information Security Aspects of Business Continuity	4
	A18	Compliance	8
		Total Control Points :	113

ISO 27001:2005 ISMS Control Point and Control Objective Summary

ISO27k ref.		Description	Control Total
Discretionary	A5	Information Security Policy	2
	A6	Internal Information Security Organization	11
	A7	Asset Management	5
	A8	Human Resource Security	9
	A9	Physical and Environmental Security	13
	A10	Communications and Operations Management	32
	A11	Access Control	25
	A12	Information Systems Acquisition, Development and Maintenance	16
	A13	Information Security Incident Management	5
	A14	Business Continuity Management	5
	A15	Compliance	10
		Total Control Points :	133

http://www.itworldcanada.com/blog/the-new-isms-isoiec-270012013-expert-insight/84379

ISO 27001:2013 ISMS Requirements

Standard	High-Level Overview	High-Level Limitations
ISO 27001:2013	• Built on the same premise of any quality management ISO standard -continually improving performance. • Specifies the requirements for establishing, implementing and documenting an ISMS. • Specifies requirements for security controls to be implemented according to the business requirements, risk, and legal and contractual obligations. • Two Main Components of ISO: Clauses 4-10 and Annex A (Controls)	• Compliance with, or certification against ISO 27001:2013 does not, itself, guarantee that an organization is secure.

ISO 27001:2013 (clauses 4-10)

4. Context of the organization | 5. Leadership | 6. Planning | 7. Support | 8. Operation | 9. Performance evaluation | 10. Improvement

ISO 27001:2013 (Annex A Controls)

5. Information security policies | 6. Organisation of information security | 7. Human resources security | 8. Asset management | 9. Access control

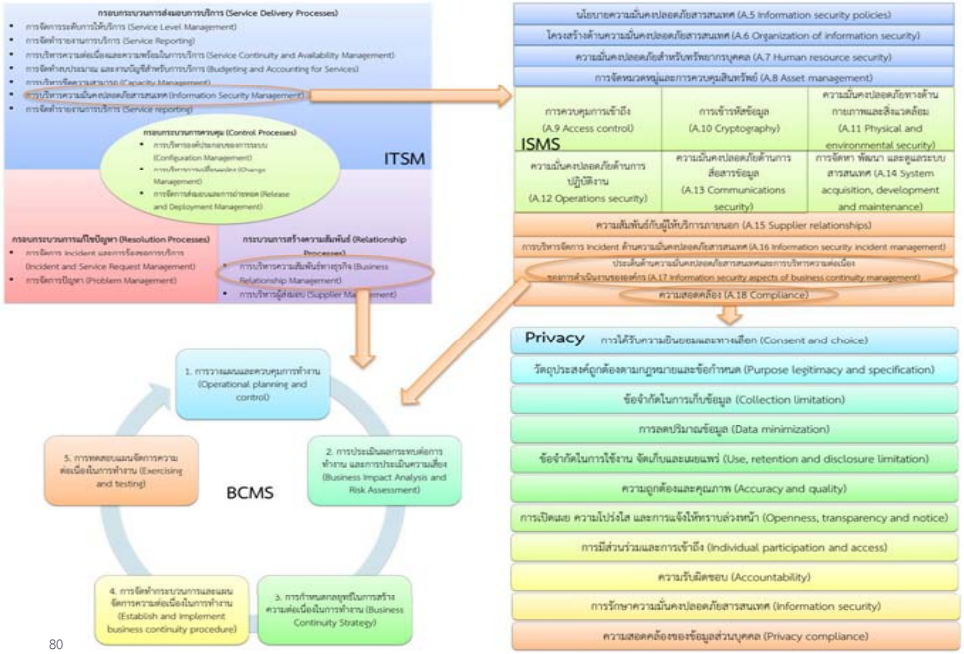
10. Cryptography | 11. Physical and environmental security | 12. Operations security | 13. Communications security | 14. Systems acquisition development & maintenance

15. Supplier relationships | 16. Information security incident management | 17. Information security aspects of business continuity management | 18. Compliance

http://slideplayer.com/slide/8838138/

© Deloitte & Touche LLP and affiliated entities.

ความสัมพันธ์ระหว่าง ITSM-ISMS-BCMS-Privacy



http://patanakul.blogspot.com/2015/06/itsm-isms-bcms-privacy.html

รายการเอกสารจำเป็นที่ต้องมีสำหรับ ISO/IEC 27001:2013

- รายการเอกสารที่จำเป็น (Mandatory documents) และสิ่งที่ต้องบันทึกเป็นหลักฐาน (Mandatory records) ตามข้อกำหนดของมาตรฐาน ISO/IEC 27001:2013
- เอกสารในที่นี้ไม่จำกัดเฉพาะเอกสารที่เป็นกระดาษ **แต่รวมถึงข้อมูลในคอมพิวเตอร์ด้วย**

http://ovthai.miss.in.th/2014/02/09/54321/

รายการเอกสารจำเป็นที่ต้องมีสำหรับ ISO/IEC 27001:2013 (ต่อ)

สำหรับเอกสารภาคบังคับว่าต้องจัดทำ เมื่อองค์กรต้องการขอรับรองระบบความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC27001:2013 มีรายการดังต่อไปนี้ (ต่อ)

1. ขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย: Scope of the ISMS (clause 4.3)
2. นโยบายความมั่นคงปลอดภัยสารสนเทศ และวัตถุประสงค์: Information security policy and objectives (clauses 5.2 and 6.2)
3. วิธีการประเมินความเสี่ยงและการปรับระดับความเสี่ยง: Risk assessment and risk treatment methodology (clause 6.1.2)
4. เอกสารแสดงมาตรการควบคุมที่นำไปใช้งาน: Statement of Applicability (clause 6.1.3 d)
5. แผนปรับระดับความเสี่ยง: Risk treatment plan (clauses 6.1.3 e and 6.2)
6. รายงานการประเมินความเสี่ยง: Risk assessment report (clause 8.2)
7. นิยามของบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัย: Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4)

http://ovthai.miss.in.th/2014/02/09/54321/

รายการเอกสารจำเป็นที่ต้องมีสำหรับ ISO/IEC 27001:2013 (ต่อ)

สำหรับเอกสารภาคบังคับว่าต้องจัดทำ เมื่อองค์กรต้องการขอรับรองระบบความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC27001:2013 มีรายการดังต่อไปนี้ (ต่อ)

8. รายการบัญชีทรัพย์สิน: Inventory of assets (clause A.8.1.1)
9. การยอมรับการใช้งานทรัพย์สิน: Acceptable use of assets (clause A.8.1.3)
10. นโยบายการควบคุมการเข้าถึง: Access control policy (clause A.9.1.1)
11. ขั้นตอนปฏิบัติงาน สำหรับการบริหารจัดการเทคโนโลยีสารสนเทศ: Operating procedures for IT management (clause A.12.1.1)
12. Secure system engineering principles (clause A.14.2.5)
13. นโยบายความมั่นคงปลอดภัยสำหรับผู้ให้บริการหรือจัดหาปัจจัยหลักของธุรกิจ: Supplier security policy (clause A.15.1.1)
14. ขั้นตอนการบริหารจัดการเหตุขัดข้อง: Incident management procedure (clause A.16.1.5)
15. ขั้นตอนการสร้างความต่อเนื่องทางธุรกิจ: Business continuity procedures (clause A.17.1.2)
16. การปฏิบัติตามกฎระเบียบ ข้อกำหนดทางกฎหมาย และสัญญา: Statutory, regulatory, and contractual requirements (clause A.18.1.1)

http://ovthai.miss.in.th/2014/02/09/54321/

รายการเอกสารจำเป็นที่ต้องมีสำหรับ ISO/IEC 27001:2013 (ต่อ)

รายการสิ่งที่ต้องบันทึกเป็นหลักฐานภาคบังคับ (Mandatory records):

1. บันทึกการฝึกอบรม ทักษะ ประสบการณ์และคุณสมบัติ: Records of training, skills, experience and qualifications (clause 7.2)
2. การเฝ้าระวังและการวัดผล: Monitoring and measurement results (clause 9.1)
3. แนวทางการปฏิบัติงานตรวจสอบ: Internal audit program (clause 9.2)
4. ผลการตรวจสอบภายใน: Results of internal audits (clause 9.2)
5. ผลการทบทวนการดำเนินการโดยผู้บริหาร: Results of the management review (clause 9.3)
6. ผลดำเนินการเพื่อแก้ไขความบกพร่อง: Results of corrective actions (clause 10.1)
7. ข้อมูลบันทึกกิจกรรมของผู้ใช้งาน ความผิดปกติและเหตุการณ์ด้านความมั่นคงปลอดภัย : Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3)

รายการเอกสารจำเป็นที่ต้องมีสำหรับ ISO/IEC 27001:2013 (ต่อ)

สำหรับเอกสารที่ไม่ได้ระบุในข้อกำหนดว่าเป็นสิ่งที่ต้องมี (Non-mandatory documents) แต่มักเป็นเอกสารที่ถูกนำไปใช้ในทางปฏิบัติตามข้อกำหนดของมาตรฐาน ISO/IEC27001:2013 โดยเฉพาะมาตรการที่ใช้ควบคุมด้านความมั่นคงปลอดภัยจาก Annex A

1. ขั้นตอนปฏิบัติเพื่อควบคุมเอกสาร: Procedure for document control (clause 7.5)
2. การควบคุมเพื่อบริหารจัดการบันทึกการปฏิบัติ: Controls for managing records (clause 7.5)
3. ขั้นตอนปฏิบัติในการตรวจสอบภายใน: Procedure for internal audit (clause 9.2)
4. ขั้นตอนปฏิบัติเพื่อแก้ไขข้อบกพร่อง: Procedure for corrective action (clause 10.1)
5. นโยบายการใช้งานอุปกรณ์พกพาส่วนตัว Bring your own device (BYOD) policy (clause A.6.2.1)
6. นโยบายการใช้งานอุปกรณ์พกพาและการทำงานจากระยะไกล: Mobile device and teleworking policy (clause A.6.2.1)
7. นโยบายการแบ่งระดับชั้นข้อมูล: Information classification policy (clauses A.8.2.1, A.8.2.2, and A.8.2.3)

รายการเอกสารจำเป็นที่ต้องมีสำหรับ ISO/IEC 27001:2013 (ต่อ)

8. นโยบายการตั้งรหัสผ่าน: Password policy (clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3)
9. นโยบาย Disposal and destruction policy (clauses A.8.3.2 and A.11.2.7)
10. ขั้นตอนปฏิบัติสำหรับทำงานในพื้นที่ควบคุม: Procedures for working in secure areas (clause A.11.1.5)
11. Clear desk and clear screen policy (clause A.11.2.9)
12. นโยบายการบริหารจัดการการเปลี่ยนแปลง: Change management policy (clauses A.12.1.2 and A.14.2.4)
13. นโยบายการสำรองข้อมูล: Backup policy (clause A.12.3.1)
14. นโยบายการโอนย้ายสารสนเทศ: Information transfer policy (clauses A.13.2.1, A.13.2.2, and A.13.2.3)
15. การวิเคราะห์ผลกระทบทางธุรกิจ: Business impact analysis (clause A.17.1.1)
16. แผนการซ้อมและทดสอบ: Exercising and testing plan (clause A.17.1.3)
17. แผนการบำรุงรักษาและการทบทวน: Maintenance and review plan (clause A.17.1.3)
18. กลยุทธ์การสร้างความต่อเนื่องทางธุรกิจ: Business continuity strategy (clause A.17.2.1)

สรุปภาพรวม

- ในส่วนที่เป็นกระบวนการ/คู่มือปฏิบัติงานต่างๆ ที่เกี่ยวข้องกับผู้ดูแลระบบ หรือการปฏิบัติงานเชิงเทคนิค แทบไม่ต้องปรับเปลี่ยนอะไร
- ส่วนที่จะต้องปรับปรุง จะอยู่ในส่วนระบบบริหารจัดการ (Management System) เป็นส่วนใหญ่เช่นต้องเปลี่ยนโครงสร้างเอกสาร SOA (Statement of Applicability) แน่ ๆ ให้เป็นไปตามโครงสร้างของ Annex A ใหม่ที่มี 14 โดเมน
- การควบคุมเอกสารและบันทึกก็ไม่จำเป็นต้องแยกกระบวนการแต่ให้มองเป็นการบริหารจัดการข้อมูล (Documented Information)
- การบริหารจัดการทรัพยากรจะมีการแยกออกมาเป็นหัวข้อชัดเจน เช่น ทรัพยากร (Resource) ความรู้ความสามารถ (Competence) ความตระหนัก (Awareness) และการสื่อสาร (Communication)

9.5 โครงสร้างมาตรฐาน ISO (Annex SL)

บริษัท ไอเอสโอ สมาร์ทโปร จำกัด www.ISO smartpro.com

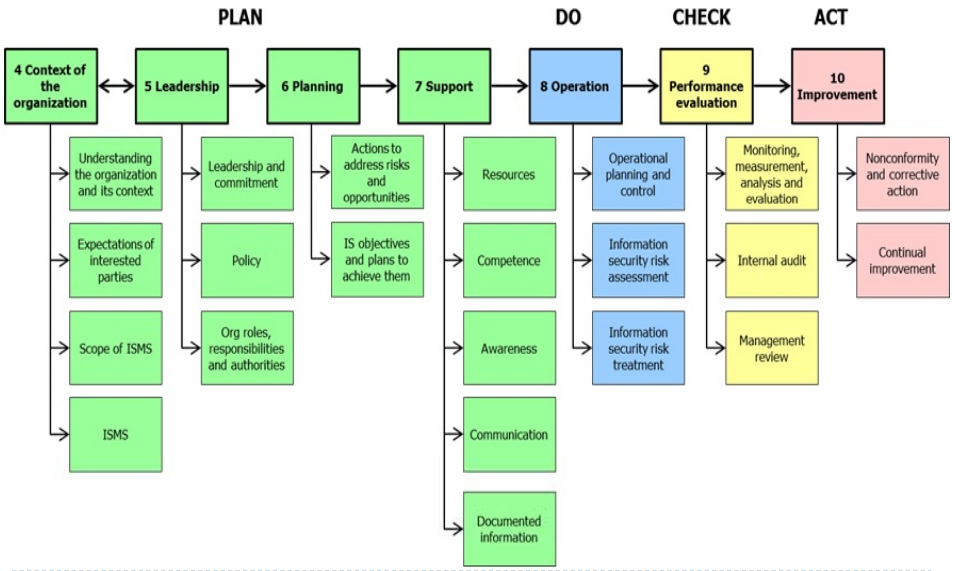
Annex SL

- คณะกรรมการ ISO ได้ตกลงกันว่าจะใช้โครงสร้างที่เรียกว่า Annex SL เป็นรูปแบบเอกสารสำหรับมาตรฐานการจัดการ ISO ทุกตัว (เรียกเป็นภาษาอังกฤษว่า MSS ย่อมาจาก Management System Standards)
- ทั้งนี้เพื่อให้มาตรฐานทุกตัวมีรูปแบบที่สอดคล้องกัน มีทิศทางเดียวกัน ชัดเจน ง่ายต่อการเข้าใจและการนำไปใช้ โดยเฉพาะกับองค์กรที่นำมาตรฐานหลายๆ ตัวมาใช้ด้วยกัน
- เริ่มตั้งแต่ประมาณปี 2012 เราจะเห็นได้ว่ารูปแบบของ Annex SL นี้ได้ถูกใช้ใน ISO 22301:2012 (Business Continuity Management System) แล้ว และ รวมถึง ISO/IEC 27001:2013 (Information Security Management System) ก็ใช้รูปแบบตาม Annex SL ด้วยเช่นกัน ในอนาคต มาตรฐานทุกตัวก็จะถูกปรับให้อยู่ในรูปแบบนี้เหมือนกันหมด

รูปแบบ Annex SL

- รายละเอียดของรูปแบบ Annex SL ที่เราควรจะรู้ก็คือใน Appendix 2 ของ Annex SL ที่ถูกนำมาใช้เป็นรูปแบบของมาตรฐานการจัดการ ISO นั้นประกอบด้วย 3 ส่วนคือ
  - High Level Structure จะเป็นหัวข้อหลักๆ ที่เหมือนกันในมาตรฐานการจัดการทุกตัว
  - Identical core text คือเนื้อหาที่อยู่ภายใต้หัวข้อหลักๆ 10 ตัว ข้างต้น
  - Common terms and core definitions

High level Standard structure – Annex SL



http://www.oaschina.com/zixun/a/bzwk/2014/0819/59.html

http://www.netgrowthltd.co.uk/ISO/IEC 27001 .aspx

High Level Structure

- Introduction
- 1. Scope
- 2. Normative references
- 3. Terms and conditions
- 4. Context of the organization
- 5. Leadership
- 6. Planning
- 7. Support
- 8. Operation
- 9. Performance evaluation
- 10.Improvement

เนื้อหาใน หัวข้อของ Introduction Scope และ Normative references จะแตกต่างกันไปตามมาตรฐานแต่ละตัว และในแต่ละมาตรฐานก็จะมีบรรณานุกรมที่เฉพาะเจาะจงลงไปได้

Identical core text

- **คือเนื้อหาที่อยู่ภายใต้หัวข้อหลักๆ 10 ตัว ข้างต้น ใน identical core text จะมีคำว่า "shall" 45 ตัว (ก่อให้เกิด 84 requirements) แต่อย่างไรก็ดี ในมาตรฐานแต่ละตัวก็จะมี requirements ของตนเองได้ ซึ่งก็ทำให้เกิดมากกว่า 84 requirements แน่ๆ เราลองมาดูตัวอย่างของ identical core text กัน**

1. Scope

- The scope should define what the 'intended outcome(s)' are of the discipline. The term 'expected outcome' will not be used.

2. Normative references

- Provides details of the reference standards or publications relevant to the particular standard.

Identical core text (ต่อ)

3. Terms & definitions

- Details terms and definition applicable to the specific standard in addition to any formal related terms and definitions standard.

4. Context of the organization

- 4.1 Understanding the organization and its context
- 4.2 Understanding the needs and expectations of interested parties
- 4.3 Determining the scope of the XXX* management system
- 4.4 XXX management system

Identical core text (ต่อ)

5. Leadership

- 5.1 Leadership and commitment
- 5.2 Policy
- 5.3 Organizational roles, responsibilities and authorities

6. Planning

- 6.1 Actions to address risks and opportunities
- 6.2 XXX objectives and planning to achieve them

Identical core text (ต่อ)

7. Support

- 7.1 Resources
- 7.2 Competence
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented information
- 7.5.1 General
- 7.5.2 Creating and updating
- 7.5.3 Control of documented information

8. Operation

- 8.1 Operational planning and control

(ข้อนี้จะเป็นข้อกำหนดที่ลงรายละเอียดในแต่ละมาตรฐานการจัดการ)

Identical core text (ต่อ)

9. Performance evaluation

- 9.1 Monitoring, measurement, analysis and evaluation
- 9.2 Internal audit
- 9.3 Management review

10.Improvement

- 10.1 Nonconformity and corrective action
- 10.2 Improvement

(* XXX หมายถึง มาตรฐานของแต่ละด้าน เช่น ISO 9001 คือ Quality, ISO 14001 คือ Environmental)

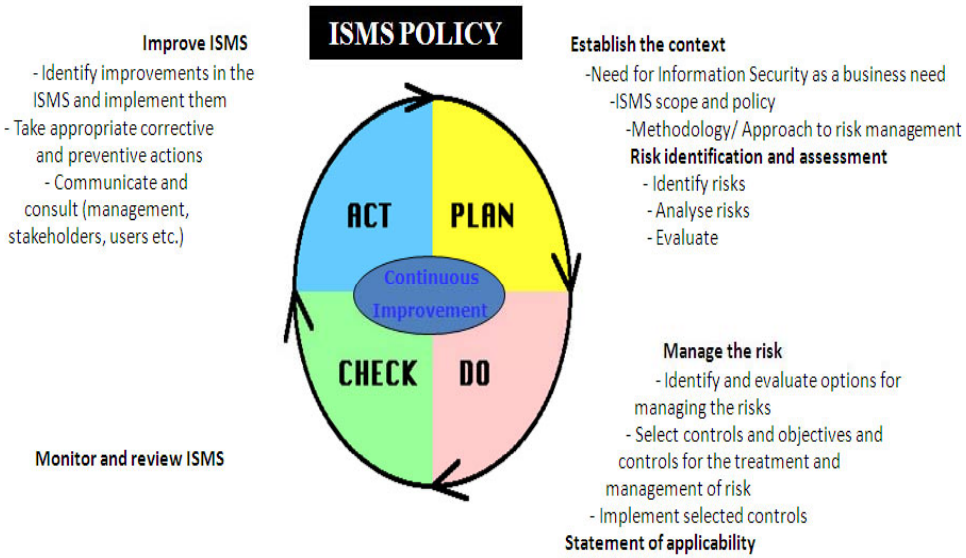
9.6 การจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISMS)

การจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISMS)

มี 4 องค์ประกอบใหญ่คือ

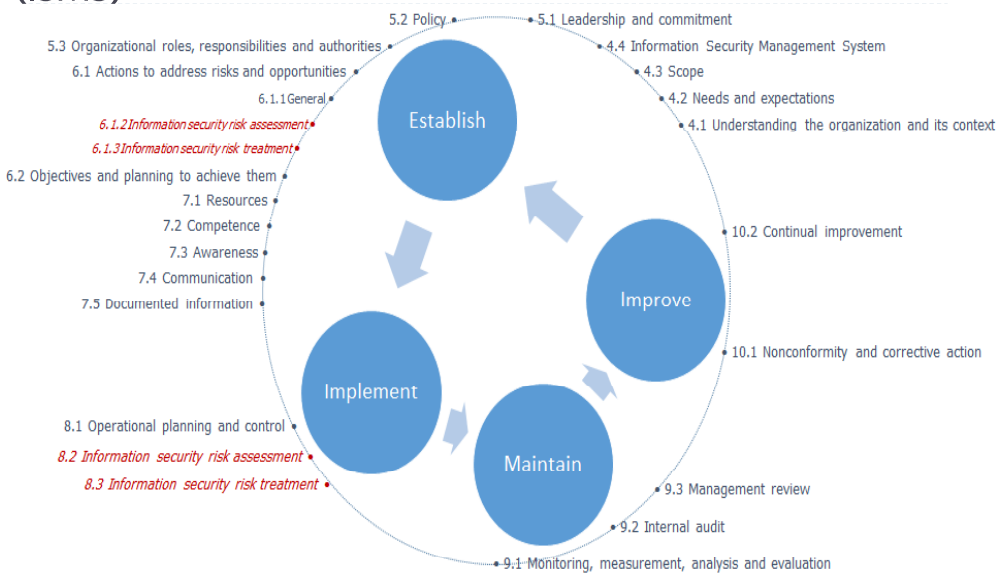
- **การวางแผนจัดทำระบบ ISMS (Establish ISMS)** การจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System-ISMS) คือ การเตรียมการวางแผนเพื่อปกป้องสารสนเทศ
- **การนำไปปฏิบัติ (Implement and operate ISMS)** คือ นำแผนจากขั้นตอนการจัดทำระบบ (Establish) ไปปฏิบัติจริงหน้างาน ทำตามเอกสารคู่มือและลงบันทึกในแบบฟอร์ม
- **การรักษามาตรฐาน การเฝ้าระวังและทบทวน (Maintain, monitor and review ISMS)** คือ ปฏิบัติควบคู่ไปกับการทำงานปกติ (ไม่ใช่ทำเฉพาะก่อนจะโดนตรวจ Audit) การเฝ้าระวังและทบทวนผลการทำระบบ
- **การพัฒนาปรับปรุง (Continual improve ISMS)** คือ การพยายามปรับปรุงอย่างต่อเนื่องเพื่อลดข้อผิดพลาดที่พบในข้อ 3 หรือปรับปรุงระบบให้มีประสิทธิภาพยิ่งขึ้น ไม่ใช่ทำครั้งเดียวจบ

Requirements of ISO 27001 ISMS



http://www.hybridtp.ie/ISO -27001-standard-on-information-security/

การจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISMS)



http://docplayer.net/7642634-Iso-iec-27001-2013-launch-event.html

การจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISMS) (ต่อ)

- การทำระบบ ISO/IEC 27001 ให้มีประสิทธิภาพ เราต้องทำตาม 4 ข้อ ข้างต้นให้ครบถ้วน และต้องมีหลักฐาน (ทั้งเอกสารและผลการปฏิบัติ) ที่น่าเชื่อถือ สะท้อนความเป็นจริงและตรวจสอบย้อนหลังได้

1. การวางแผนจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (Plan: Establish the ISMS)

- เริ่มต้นด้วยการกำหนดขอบเขตของการจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศให้ชัดเจน โดยแสดงถึงลักษณะของธุรกิจ องค์กร ทำเลที่ตั้ง ทรัพย์สิน และเทคโนโลยี หากไม่ครอบคลุมส่วนงานใด ต้องระบุรายละเอียดและเหตุผลดังกล่าว

- จากนั้นผู้บริหารระดับสูงกำหนดนโยบายการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System Policy: ISMS Policy) พร้อมทั้งอนุมัติและประกาศใช้นโยบายดังกล่าว เป็นกลไกให้มั่นใจว่าโครงการนี้ได้รับการสนับสนุนอย่างเป็นรูปธรรม และเป็นสัญญาณว่า ISMS ได้เริ่มอย่างเป็นทางการแล้ว

1. การวางแผนจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (Plan: Establish the ISMS) (ต่อ)

- การกำหนดคณะทำงานให้เหมาะสมและเพียงพอเป็นเรื่องสำคัญที่ต้องพิจารณา
- ตัวแทนหน่วยงานที่อยู่ในขอบเขตการจัดทำระบบควรเข้าร่วมเป็นคณะทำงานเพื่อให้มีส่วนร่วมในการจัดทำระบบที่สอดคล้องกับลักษณะการทำงาน
- เมื่อได้คณะทำงานเรียบร้อยแล้วก็เริ่มสำรวจภัยคุกคามและช่องโหว่ที่ก่อให้เกิดความเสี่ยงต่อสารสนเทศในขอบเขตการจัดทำระบบขององค์กร
- ตัวแทนหน่วยงานที่เป็นคณะทำงานก็รับผิดชอบสำรวจภัยคุกคามและช่องโหว่ในหน่วยงานของตนเอง
- ผลการประเมินความเสี่ยงจะบอกถึงระดับความเสี่ยงจากภัยคุกคามและช่องโหว่ในระบบสารสนเทศ
- คณะทำงานและผู้เกี่ยวข้องต้องกำหนดมาตรการควบคุมจัดการกับความเสี่ยงนั้นให้ชัดเจนและมีประสิทธิภาพเพียงพอ

2. การนำไปปฏิบัติ (Do: Implement and Operate the ISMS)

- ขั้นตอนการปฏิบัติ (Do) เป็นการนำผลลัพธ์ของขั้นตอนวางแผน (Plan) มาปฏิบัติให้เกิดผลตามวัตถุประสงค์ เช่น มาตรการป้องกันการบุกรุกระบบ มาตรการสำรองข้อมูล เป็นต้น ซึ่งก่อนจะปฏิบัติได้อย่างถูกต้องนั้นจำเป็นต้องมีการฝึกอบรม ถ่ายทอดความรู้แนวทางปฏิบัติที่ถูกต้องให้รับทราบทั่วกัน

3. การเฝ้าระวังและทบทวน (Check: Monitoring and Review the ISMS)

- หลังจากปฏิบัติตามมาตรการควบคุมที่กำหนดแล้ว เราจะรู้ได้อย่างไรว่ามาตรการควบคุมที่ปฏิบัตินั้นได้ผลตามเป้าหมายที่ต้องการ
- คำตอบคือต้องมีการวัดผลของมาตรการควบคุมที่ใช้ควบคุมดูแล แนวทางการวัดผลและความถี่ในการเฝ้าระวังต้องสอดคล้องกับความเสี่ยง
- ดังนั้นกระบวนการ ระบบงาน หรือทรัพย์สินสารสนเทศที่มีความเสี่ยงสูงควรได้รับการเฝ้าระวังและวัดผลการปฏิบัติงานที่เข้มงวดกว่า เพื่อให้มั่นใจว่าหากเกิดเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ระบบการตรวจวัดและเฝ้าระวังสามารถรายงานผลได้ทันเวลา

4. การรักษามาตรฐานและปรับปรุงให้ดีขึ้น (Act: Maintain and Improve the ISMS)

- หลังจากที่ตรวจพบปัญหาหรือสิ่งผิดปกติในขั้นตอนการตรวจสอบ (Check: Monitoring and Review the ISMS)
- ผู้ที่เกี่ยวข้องทุกระดับจำเป็นต้องร่วมกันแก้ไขปัญหาที่เกิดขึ้นและป้องกันปัญหาที่อาจเกิดซ้ำในอนาคต
- รวมถึงหาแนวทางปรับปรุงระบบการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศให้มีประสิทธิภาพยิ่งขึ้น
- กลไกสำคัญที่ช่วยให้ผลักดันให้การแก้ไขปัญหาและปรับปรุงดำเนินการได้อย่างเป็นรูปธรรม คือการมีส่วนร่วมของผู้บริหารระดับสูง บ่อยครั้งที่พบว่าปัญหาเกิดจากการขาดความชัดเจนในนโยบายการบริหารจัดการ ซึ่งผู้บริหารจะต้องให้ความกระจ่างและตัดสินใจแก้ไขปัญหาเชิงนโยบายให้เป็นรูปธรรม เพื่อให้คณะทำงานยึดถือเป็นแนวปฏิบัติต่อไป

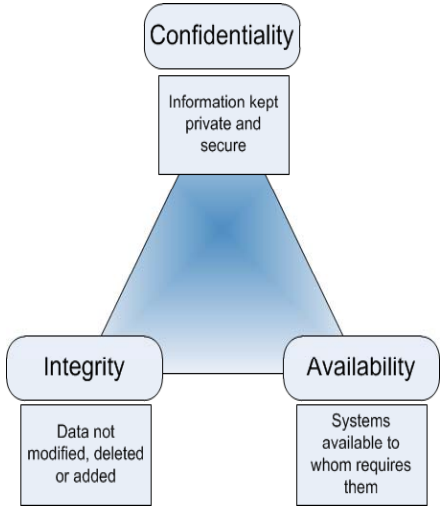
9.7 โมเดล CIA และการประเมินความเสี่ยง ใน ISO/IEC 27001

โมเดล CIA ใน ISO/IEC 27001

ISO/IEC 27001 เน้นการปกป้องข้อมูลสารสนเทศ (Information) ให้มีคุณสมบัติ 3 ประการคือ

- Confidential: การปกป้องสารสนเทศให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ ถ้าหากข้อมูลรั่วไหลแสดงว่าขาดคุณสมบัติในข้อนี้
- Integrity: ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความเป็นจริง เช่น การแฮ็กระบบเพื่อแก้ไขข้อมูล เป็นต้น
- Availability: สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน

ทรัพย์สิน (Asset) ที่มีความมั่นคงปลอดภัยนั้นต้องประกอบด้วยองค์ประกอบทั้งสามอย่างครบถ้วน ไม่ว่าทรัพย์สินนั้นจะเป็นสิ่งที่จับต้องได้ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย หรือทรัพย์สินที่จับต้องไม่ได้ เช่น ข้อมูล เป็นต้น



http://geraintw.blogspot.com/2012/09/cia-infosec.html

ความลับ (Confidentiality)

- การรักษาความลับให้กับข้อมูลเป็นองค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยของสารสนเทศ หลักการสำคัญของการรักษาความลับคือ ผู้ที่มีสิทธิหรือได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ ภาคธุรกิจให้ความสำคัญกับการรักษาความลับทางธุรกิจ ประชาชนทั่วไปก็ต้องการปกป้องข้อมูลส่วนตัวตามสิทธิขั้นพื้นฐานเช่นเดียวกัน
- ข่าวการละเมิดมาตรการควบคุมป้องกันของระบบคอมพิวเตอร์เข้าไปเจาะระบบทั้งในประเทศและต่างประเทศ แสดงให้เห็นว่ามาตรการควบคุมที่มีอยู่ยังมีจุดอ่อนที่ ผู้ไม่ประสงค์ดีที่มีความรู้บุกรุกผ่านช่องโหว่ดังกล่าว แรงจูงใจของการกระทำการดังกล่าวมีหลายเหตุปัจจัย เช่น ทำเพื่อเงิน เพื่อสร้างชื่อเสียง การยอมรับในกลุ่ม และทำไปด้วยความคึกคะนอง ปฏิเสธไม่ได้ว่าแฮ็กเกอร์ที่สามารถเจาะทะลุระบบรักษาความมั่นคงปลอดภัยของหน่วยงานสำคัญระดับประเทศ จะกลายเป็นฮีโร่ในสายตาของแฮ็กเกอร์มือใหม่ทั่วโลก

ความลับ (Confidentiality) (ต่อ)

- ระบบรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีประสิทธิภาพ ต้องมีมาตรการควบคุมตรวจสอบสิทธิก่อนเข้าถึง เพื่อยืนยันให้แน่ใจก่อนว่าผู้ที่ร้องขอนั้นมีสิทธิหรือได้รับอนุญาตให้เข้าถึงสารสนเทศ หรือระบบงานนั้นได้ กลไกพื้นฐานที่คุ้นเคยกันเป็นอย่างดี คือการใช้รหัสผ่าน (Password) ในการพิสูจน์ตัวตนและสิทธิที่ได้รับอนุญาต
- นอกจากมาตรการควบคุมตรวจสอบสิทธิแล้วการกำหนดชั้นความลับเป็นระดับต่างๆ ตามความสำคัญช่วยให้บริหารจัดการมีประสิทธิภาพมากขึ้น

ความลับ (Confidentiality) (ต่อ)

- ในบางหน่วยงานกำหนดชั้นความลับของสารสนเทศออกเป็น 4 ระดับ ประกอบด้วย ระดับชั้นความลับสุดยอด (Top Secret) ระดับชั้นความลับ (Secret) ระดับชั้นข้อมูลสำหรับใช้ภายในองค์กร (Internal Use) และระดับชั้นสารธารณะ (Public)
- ชั้นความลับนี้จะต้องมีเกณฑ์พิจารณาที่ชัดเจนว่าสารสนเทศลักษณะใดอยู่ในชั้นความลับที่กำหนด พร้อมทั้งกำหนดแนวทางการ การระบุชั้นความลับ การจัดเก็บและการสื่อสารข้อมูลสารสนเทศในแต่ละชั้นความลับอย่างชัดเจน มาตรการควบคุมทางเทคนิคที่ใช้ในการปกป้องความลับ เช่น การเข้ารหัส (Encryption) อาจถูกนำมาใช้เสริมความแข็งแกร่งให้กับมาตรการควบคุมปกป้องสารสนเทศที่ต้องการมาตรการควบคุมดูแลอย่างเข้มงวด

ความถูกต้องสมบูรณ์ (Integrity)

- การปกป้องสารสนเทศให้มีความถูกต้องสมบูรณ์ (Integrity) เป็นสิ่งสำคัญส่งผลถึงความน่าเชื่อถือของสารสนเทศนั้น ๆ
- ทำอย่างไรให้ข้อมูลมีความถูกต้องและน่าเชื่อถือเป็นสิ่งที่ผู้ดูแลระบบต้องหาคำตอบและดำเนินการให้เกิดขึ้น คำตอบในเชิงหลักการคือระบบต้องมีกลไกการตรวจสอบสิทธิหรือการได้รับอนุญาตให้ดำเนินการเปลี่ยนแปลงแก้ไขหรือกระทำการใด ๆ ต่อข้อมูลนั้น

ความถูกต้องสมบูรณ์ (Integrity) (ต่อ)

- ยิ่งเทคโนโลยีสารสนเทศพัฒนาก้าวหน้าไปมากเท่าไร มนุษย์ก็ยิ่งจำเป็นต้องพึงพาเทคโนโลยีมากขึ้นตามไปด้วย
- บัตรประชาชนอัจฉริยะเป็นตัวอย่างใกล้ตัวเราที่ชี้ให้เห็นว่า ประชาชนทุกคนไม่ว่าจะยากดีมีจนอย่างไร ก็ต้องเกี่ยวข้องกับเทคโนโลยีสารสนเทศอย่างเลี่ยงไม่ได้ อย่างน้อยข้อมูลส่วนตัวของเราก็ถูกจัดเก็บในฐานข้อมูลของรัฐบาล
- ลองนึกดูว่าจะเกิดอะไรขึ้นหากชื่อของนาย ก. ถูกลบออกจากบัญชีทะเบียนราษฎร์ นั่นหมายถึง นาย ก. ไม่มีตัวตนและไม่สามารถใช้สิทธิของประชาชนในการรับบริการรัฐได้
- จะเห็นได้ว่าข้อมูลนี้มีความสำคัญมากเพราะเป็นหลักฐานในการพิสูจน์ตัวตนของเรา
- หากมองในแง่ความมั่นคงปลอดภัยของสารสนเทศแล้ว ข้อมูลนี้จำเป็นต้องได้รับการปกป้องดูแลความถูกต้องสมบูรณ์และความน่าเชื่อถือ หากข้อมูลถูกเปลี่ยนแปลงโดยผู้ไม่ประสงค์ดีย่อมส่งผลเสียต่อเจ้าของข้อมูลอย่างหลีกเลี่ยงไม่ได้

ความพร้อมใช้งาน (Availability)

- การทำให้ระบบตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิเข้าถึงระบบได้เมื่อต้องการ อุปสรรคที่บั่นทอนความพร้อมใช้งานของระบบคอมพิวเตอร์จำแนกได้ 2 แบบ คือ
  - การที่ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ (Denial of Service)
  - ระบบคอมพิวเตอร์ทำงานด้อยประสิทธิภาพในการทำงาน (Loss of data processing capability)

ความพร้อมใช้งาน (Availability) (ต่อ)

- ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ อาจเกิดจากการกระทำของผู้ใช้ระบบ ผู้บุกรุกที่มีเจตนาร้าย หรือเกิดจากภัยธรรมชาติ เช่น น้ำท่วม ไฟไหม้ แผ่นดินไหวทำให้ระบบคอมพิวเตอร์เสียหายก็เป็นได้
- องค์กรที่ตระหนักถึงภัยคุกคามดังกล่าวอาจเตรียมแผนกู้คืนจากความเสียหาย (Disaster Recovery Plan) ไว้รองรับ
- หน่วยงานรัฐที่ให้บริการสารธารณะต่างใช้ระบบคอมพิวเตอร์ควบคุมการทำงาน เช่น ไฟฟ้า ประปา โทรศัพท์ เป็นต้น หากคอมพิวเตอร์ที่ควบคุมระบบเหล่านี้เกิดความเสียหายไม่สามารถให้บริการได้ ทำให้บริการต่าง ๆ หยุดชะงักย่อมส่งผลเสียต่อประชาชนในวงกว้าง

ความพร้อมใช้งาน (Availability) (ต่อ)

- นอกจากนี้ หากไฟฟ้าดับเป็นเวลานาน ระบบต่าง ๆ จะเกิดความเสียหายอย่างใหญ่หลวง
- ตัวอย่างจริงที่เคยเกิดขึ้นในต่างประเทศ เมื่อหลายปีก่อนระบบคอมพิวเตอร์ของศูนย์กระจายสินค้าเกิดความเสียหาย ไม่สามารถจ่ายกระแสไฟฟ้าไปยังคอนเทนเนอร์ที่ติดตั้งระบบทำความเย็นเป็นเวลาหลายวัน ส่งผลให้สินค้าในตู้คอนเทนเนอร์ดังกล่าวเสียหายทั้งหมด นอกจากนี้ยังทำให้ลูกค้าขอยกเลิกสัญญาเนื่องจากไม่ไว้วางใจในการบริการ เกิดความสูญเสียมูลค่ามหาศาล

การปกป้อง Confidentiality Integrity Availability

- ถึงตรงนี้หลายเราคงสงสัยว่าแล้วจะต้องป้องกัน Confidentiality Integrity Availability เข้มงวดแค่ไหน ข้อมูลก็มีมากมายหลายประเภท ต้องป้องกันอย่างเข้มข้นเท่ากันหมดทุกข้อมูลยังเปล่า?
- การปกป้องข้อมูล(Information) จะเข้มงวดมากหรือน้อย ขึ้นอยู่กับ "ความเสี่ยง (Risk)"
- หลักการ คือ ข้อมูลใดที่เสี่ยงสูงย่อมต้องมีมาตรการควบคุมปกป้องเข้มงวดกว่าข้อมูลที่มีความเสี่ยงต่ำ ตัวอย่างเช่น ข้อมูล username & password สำหรับเข้าสู่ระบบสารสนเทศขององค์กร ต้องมีมาตรการควบคุมปกป้องที่เข้มงวดไม่น้อยกว่าข้อมูลทั่วไปที่ประกาศในเว็บไซต์องค์กร เป็นต้น

ประเมินความเสี่ยงนั้นสำคัญไฉน

ประเมินความเสี่ยงนั้นสำคัญไฉน

- "การประเมินความเสี่ยงของสารสนเทศ (Information Security Risk Assessment)" เป็นหัวใจสำคัญของการทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001
- หากเราประเมินความเสี่ยงไม่ถูกต้อง หรือไม่ครอบคลุม ก็จะทำให้การจัดการความเสี่ยงที่ตามมานั้นแก้ปัญหาไม่ตรงจุด และไม่ครอบคลุมตามไปด้วย
- การประเมินความเสี่ยงก็เหมือนการตรวจร่างกาย ถ้าตรวจไม่ครบหรือตรวจไม่ละเอียดก็ไม่พบอาการป่วยและไม่ได้รักษา ปล่อยทิ้งไว้จนสุกงอม อาการป่วยก็แสดงออกมาในที่สุด!!

แนวทางจัดการความเสี่ยง

- เมื่อประเมินความเสี่ยงของสารสนเทศ จนทราบแล้วว่ามีเรื่องอะไรบ้างที่มีความเสี่ยง ไม่ว่าจะเสี่ยงมาก เสี่ยงปานกลางหรือเสี่ยงน้อย ทุกความเสี่ยงต้องมีคำตอบรองรับว่าความเสี่ยงแต่ละระดับจะจัดการอย่างไร
- โดยทั่วไปความเสี่ยงสูงจะมีการทำแผนงานจัดการความเสี่ยง (Risk Treatment) โดยมีมาตรการควบคุมต่าง ๆ มาดูแลจัดการ จากนั้นเขียนเป็นคู่มือการปฏิบัติก็เป็นวิธีการที่นิยมใช้กัน
- **ตรงนี้สำคัญ** เพราะว่าผลประเมินความเสี่ยงจะเป็นตัวกำหนดว่าจะต้องทำแผนงานจัดการความเสี่ยง (Risk Treatment) เพื่อจัดการความเสี่ยงอะไรบ้าง
- ประเด็นเรื่องกฎหมายเป็นหัวข้อหนึ่งที่สำคัญในการประเมินความเสี่ยง หากพบว่าประเมินความเสี่ยงแล้วพบว่าเป็นเรื่องผิดกฎหมาย แบบนี้จัดเป็นความเสี่ยงสูงต้องรีบแก้ไขโดยด่วน

การประเมินและบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

- การประเมินและบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เป็นกระบวนการที่สำคัญที่องค์กรทุกระดับพึงจัดให้มีขึ้น เพื่อปกป้องธุรกิจและสร้างความสอดคล้องกับกฎหมาย รวมถึงเป็นกระบวนการพื้นฐานที่มาตรฐานสากลต่าง ๆ กำหนดให้มีการปฏิบัติใช้ภายในองค์กร เช่น ISO 27001, ISO 20000, ISO22301 เป็นต้น
- โดยวิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่นิยมใช้งานอย่างแพร่หลายในองค์กรต่างๆ ที่ Implement ISO 27001:2005 คือวิธีการที่เรียกว่า Asset-based Risk Assessment ซึ่งประกอบด้วยขั้นตอนหลัก ๆ ดังนี้
  - จัดทำทะเบียนทรัพย์สิน (Inventory of Asset) เพื่อระบุทรัพย์สินสารสนเทศที่สำคัญที่ต้องได้รับการปกป้อง
  - พิจารณาถึงภัยคุกคาม (Threat) ที่อาจทำอันตรายต่อทรัพย์สินสารสนเทศ และจุดอ่อน (Vulnerability) ในตัวทรัพย์สิน กระบวนการ หรือมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ ที่อาจเป็นช่องทางให้ภัยคุกคามเหล่านั้นเข้าทำอันตรายต่อทรัพย์สินได้
  - ประเมินระดับผลกระทบ (Impact) ต่อองค์กร และโอกาส (Probability) ที่จะเกิดเหตุการณ์ความเสี่ยงขึ้น
  - คำนวณระดับความเสี่ยง โดยสูตรพื้นฐานที่นิยมใช้กัน คือ
    - **ผลกระทบ (Impact) x โอกาส (Probability) = ระดับความเสี่ยง (Risk)**

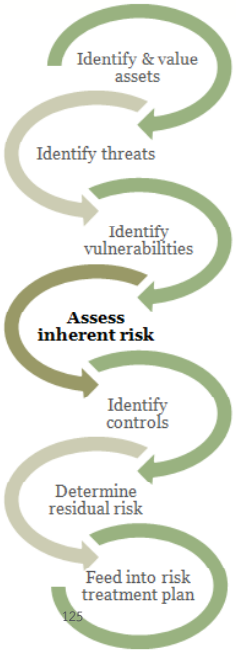
http://www.acinfotec.com/2014/06/05/learn-scenario-based-risk-assessment-suitable/

Asset-based Risk Assessment

ข้อดี	ข้อเสีย
•เข้าใจง่าย เนื่องจากผู้ประเมินความเสี่ยงเห็นภาพที่ชัดเจน ว่ากำลังพิจารณาความเสี่ยงที่เกี่ยวข้องกับทรัพย์สินใด •มั่นใจได้ว่าการบริหารความเสี่ยงจะครอบคลุมทุกทรัพย์สิน	•ต้องใช้ระยะเวลาและทรัพยากรจำนวนมากในการประเมินความเสี่ยงให้ครอบคลุมทุกทรัพย์สิน และผลที่ได้คือข้อมูลที่มากเกินความจำเป็น และนำไปใช้งานจริงได้น้อย •การประเมินความเสี่ยงที่เกี่ยวข้องกับทรัพย์สินจำนวนมาก เช่น การเปลี่ยน Platform ของระบบงานหลัก หรือความเสี่ยงที่ไม่เกี่ยวข้องกับทรัพย์สินโดยตรง เช่น การปรับเปลี่ยนกระบวนการทางธุรกิจ อาจทำได้ยาก หรือถึงขั้นไม่สามารถทำได้เลย

RISKMANAGEMENT

Determine Risk Probability



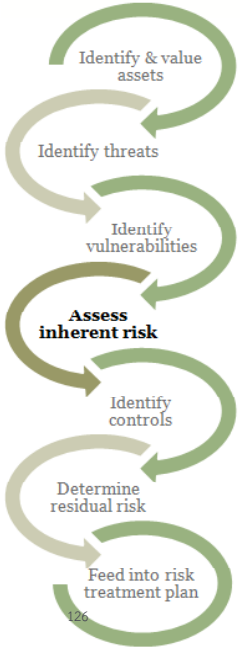
For each asset/threat/vulnerability combination, determine the probability of the specific risk materialising:

Probability	Guidance
Certain	• History of regular occurrence. • The event will occur (recur) • No special skills or determination required; information asset easily available.
Likely	• The event will occur (recur) in most circumstances
Possible	• Has occurred in the past. • The event may well occur (recur) at some time • No special skills required except for time and determination.
Unlikely	• The event could occur (recur) at some time
Rare	• No history of occurrence. • The event may only happen in exceptional circumstances • High level of technical or social engineering skill and determination required.

http://www.slideshare.net/tschraider/iso27001-risk-assessment-approach

RISKMANAGEMENT

Determine Risk Impact



For each asset/threat/vulnerability combination, consider the business impact should the risk materialise: (to be determined per organisation)

Business Impact Rating	Characteristics
Catastrophic	For example: Service disruption / failure – > 1 week; Direct financial loss – > 50% PBT / > 10% fall in share price; Business/ reputation impact – e.g. legal action (including custodial sentence) / extensive external media attention / failure to achieve 1 or more corporate objective
Major	For example: Service disruption / failure – 1-5 days; Direct financial loss – 15-50% PBT; Health & safety incident – e.g. fatality / permanent disability; Business/ reputation impact – e.g. legal action / national attention from media or regulators
Moderate	For example: Service disruption / failure – 1 day; Direct financial loss – 5-15% PBT; Health & safety incident – e.g. fractures / time off; Business/ reputation impact – e.g. legal action / local media or regulatory attention
Minor	For example: Service disruption – <1 day; Direct financial loss – < 5% PBT; Health & safety incident – e.g. cuts / bruises; Business / reputation impact – e.g. complaint or legal action
Insignificant	For example: Service disruption – none / minor; Direct financial loss – negligible; Health & safety incident – none / very minor; Business / reputation impact- systems could be improved

http://www.slideshare.net/tschraider/iso27001-risk-assessment-approach

Level	Likelihood
A	Remote
B	Unlikely
C	Likely
D	Highly Likely
E	Near Certainty

ASSESSMENT GUIDE

Likelihood	a	b	c	d	e
E	M	M	H	H	H
D	L	M	M	H	H
C	L	L	M	M	H
B	L	L	L	M	M
A	L	L	L	L	M

Consequence

RISK ASSESSMENT

High (Red)
Unacceptable. Major disruption likely. Different approach required. Priority management attention required

Moderate (Yellow)
Some disruption. Different approach may be required. Additional management attention may be needed

Low (Green)
Minimum impact. Minimum oversight needed to ensure risk remains low

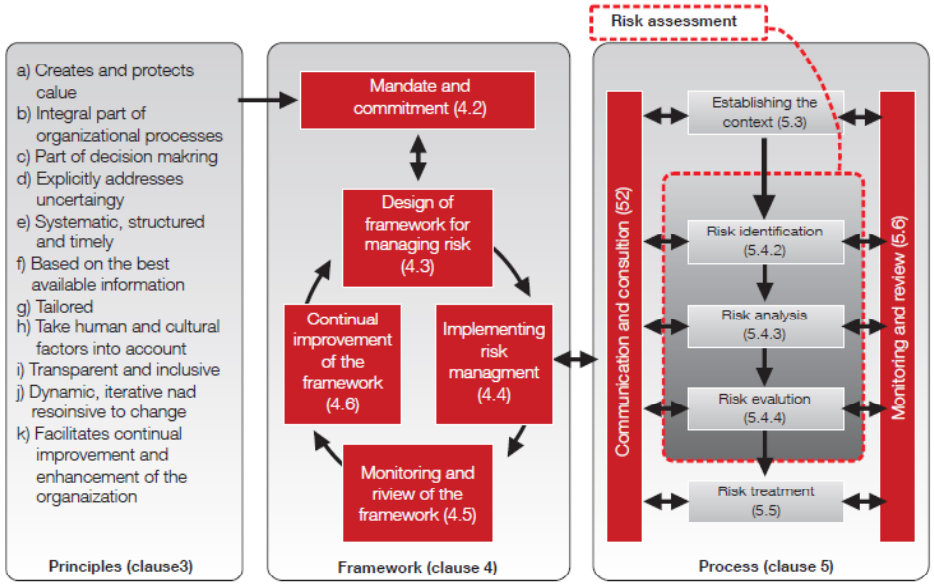
Level	Schedule	and/or	Cost
a	Minimal or no impact		Minimal or no impact
b	Additional resources required; able to meet		<5%
c	Minor slip in key milestones; not able to meet need date		5-7%
d	Major slip in key milestone or critical path impacted		7-10%
e	Can't achieve key team or major program milestone		>10%

https://www.fhwa.dot.gov/environment/climate_change/adaptation/resilience_pilots/2010-2011_pilots/conceptual_model62410.cfm

ISO 31000:2009

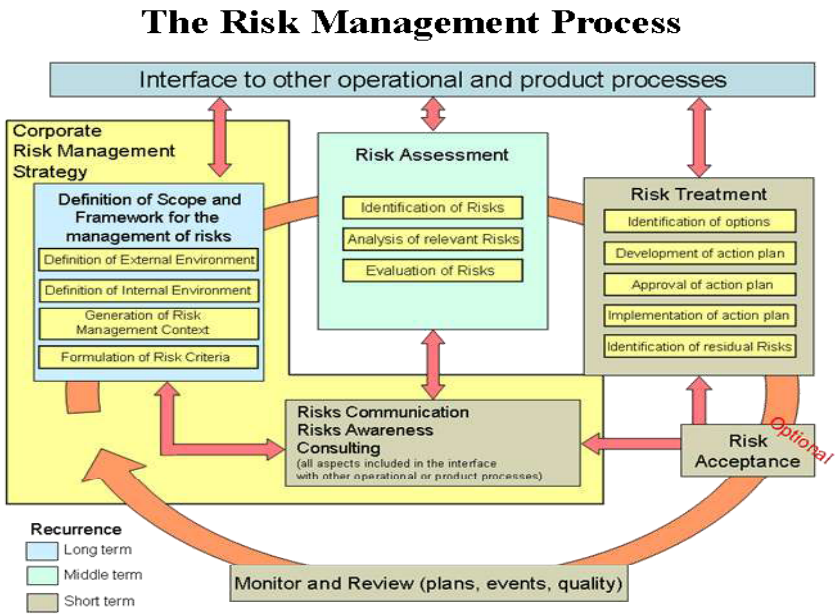
- ในปี 2009 องค์กร ISO ได้ตีพิมพ์มาตรฐาน ISO 31000 ซึ่งเป็นแนวปฏิบัติ (Guideline) ในการบริหารความเสี่ยงขององค์กร โดยใช้วิธีการประเมินความเสี่ยงในลักษณะ Scenario-based Risk Assessment ซึ่งประกอบด้วยขั้นตอนหลัก ๆ ดังนี้
  - ระบุความเสี่ยง (Risk Identification) โดยการพิจารณาถึงเหตุการณ์ความเสี่ยง (Risk Scenario) ที่เป็นไปได้ โดยเหตุการณ์ความเสี่ยงอาจเกี่ยวข้องกับทรัพย์สิน (Asset-related) หรือไม่ก็ได้
  - วิเคราะห์ความเสี่ยง (Risk Analysis) เป็นการประเมินระดับผลกระทบ (Impact) ต่อองค์กร และโอกาส (Probability) ที่จะเกิดเหตุการณ์ความเสี่ยงขึ้น รวมถึงคำนวณระดับความเสี่ยง (Risk Level)
- จากขั้นตอนข้างต้นจะเห็นว่าไม่จำเป็นต้องจัดทำทะเบียนทรัพย์สินก่อนการประเมินความเสี่ยง และไม่จำเป็นต้องแยกพิจารณาภัยคุกคาม (Threat) และจุดอ่อน (Vulnerability) ของแต่ละความเสี่ยง หากแต่สามารถกำหนดเหตุการณ์ความเสี่ยง (Risk Scenario) และทำการวิเคราะห์ความเสี่ยงได้เลย

ISO 31000 Risk Management

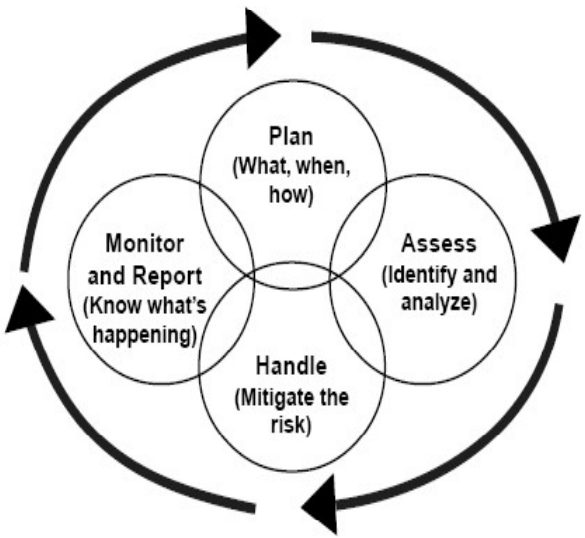


 https://www.pecb.com/whitepaper/iso-31000-risk-management--principles-and-guidelines

ENISA: The Risk Management Process, according to ISO Standard 13335



https://en.wikipedia.org/wiki/IT_risk_management



A Continuous Interlocked Process—Not an Event

https://en.wikipedia.org/wiki/IT_risk_management

ตัวอย่าง Asset-based Risk Assessment และ Scenario-based Risk Assessment

Asset-based Risk Assessment

Asset	Threat	Vulnerability	Impact	Probability	Risk
Application Server	การโจมตีทางเครือข่าย	ไม่ได้ทำการติดตั้ง Patch อย่างเหมาะสม	High	High	High
	ฮาร์ดแวร์เสียหรือทำงานผิดพลาด	ไม่ได้ทำการบำรุงรักษาอย่างเหมาะสม	High	Low	Medium

Scenario-based Risk Assessment

Risk Scenario	Impact	Probability	Risk
ความเสี่ยงจาก Heartbleed Bug เนื่องจากมีหลายระบบงานขององค์กรที่ใช้งาน OpenSSL version ที่ได้รับผลกระทบจากช่องโหว่นี้	High	High	High

***หมายเหตุ** ตัวอย่างข้างต้นเป็นการอธิบายองค์ประกอบที่เกี่ยวข้องกับการประเมินความเสี่ยงแบบง่ายเท่านั้น การประเมินความเสี่ยงในสถานการณ์จริงยังมีองค์ประกอบอื่น ๆ ที่เกี่ยวข้อง และมีความซับซ้อนมากกว่านี้ เช่น ต้องมีการพิจารณามาตรการควบคุม (Existing Controls) ที่มีอยู่เดิมภายในองค์กรด้วย

Scenario-based Risk Assessment

ข้อดี	ข้อเสีย
•ประหยัดเวลาและทรัพยากรที่ต้องใช้ในการประเมินความเสี่ยง •จำนวนข้อมูลที่ได้มีความเหมาะสมและมีคุณภาพ •สามารถประเมินความเสี่ยงได้ทุกรูปแบบ (ไม่จำกัดเฉพาะความเสี่ยงที่เกี่ยวข้องกับทรัพย์สิน)	•การระบุเหตุการณ์ความเสี่ยงทำได้ยาก โดยเฉพาะกับผู้ประเมินความเสี่ยงมือใหม่ •ไม่มีขอบข่ายที่ชัดเจน ที่จะทำให้มั่นใจได้ว่าได้ทำการประเมินความเสี่ยงอย่างครอบคลุมแล้ว (ต่างจากการประเมินความเสี่ยงแบบ Asset-based ซึ่งจะทราบชัดเจนว่าได้ประเมินความเสี่ยงครบทุกทรัพย์สินแล้ว)

วิธีการประเมินความเสี่ยง

- วิธีการประเมินความเสี่ยงทั้งสองแบบ ล้วนมีข้อดี-ข้อเสีย ที่แตกต่างกัน
- ดังนั้นองค์กรควรเลือกวิธีการที่เหมาะสมกับลักษณะงานและความต้องการขององค์กร อย่างไรก็ตาม ด้วยข้อเท็จจริงที่ว่า**วิธีการประเมินความเสี่ยงแบบ Scenario-based Risk Assessment มีความยืดหยุ่น และสามารถประยุกต์ใช้ได้กับความเสี่ยงทุกรูปแบบ องค์กรชั้นนำส่วนใหญ่จึงเริ่มปรับวิธีการประเมินความเสี่ยงของตนตามแนวทาง Scenario-based Risk Assessment ของ ISO 31000** เพื่อให้มีกระบวนการบริหารความเสี่ยงที่เป็นมาตรฐานกลางสำหรับความเสี่ยงของทั้งองค์กร (Enterprise Risk Management หรือ ERM)
- **นอกจากนี้ มาตรฐาน ISO 27001:2013 (เวอร์ชันใหม่) หรือมาตรฐาน ISO ฉบับใหม่ ๆ ที่มีข้อกำหนดเรื่องการประเมินความเสี่ยง ยังได้อ้างถึง ISO 31000 ว่าเป็นวิธีการประเมินความเสี่ยงที่แนะนำ (Recommended) ให้ใช้งานอีกด้วย** การประเมินความเสี่ยงแบบ Scenario-based Risk Assessment จึงถือได้ว่าเป็นทิศทางที่องค์การต่าง ๆ ควรมุ่งไปอย่างแท้จริง

แนวทางการทำแผนจัดการความเสี่ยง ISO/IEC 27001 (Risk Treatment Plan)

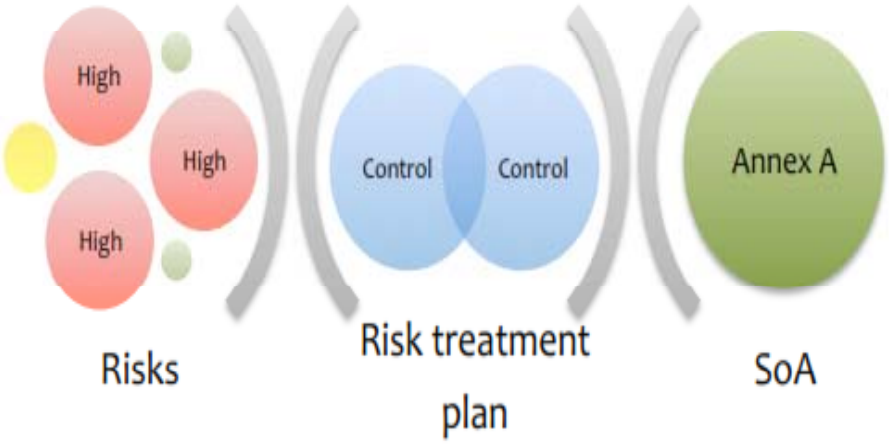
- ขั้นตอนที่สำคัญมากในการทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System - ISMS) ตาม ISO/IEC 27001 นั้น คือการประเมินความเสี่ยง (Risk Assessment)
- หลังจากประเมินความเสี่ยงตามเกณฑ์ (Risk Criteria) ที่กำหนดแล้ว ก็จะได้ได้ผลลัพธ์ออกมาเป็นความเสี่ยงระดับต่างๆ (ในที่นี้กำหนดความเสี่ยงเป็น 2 ระดับ คือ ความเสี่ยงที่ยอมรับได้ และความเสี่ยงสูง)

แนวทางการทำแผนจัดการความเสี่ยง ISO/IEC 27001 (Risk Treatment Plan)

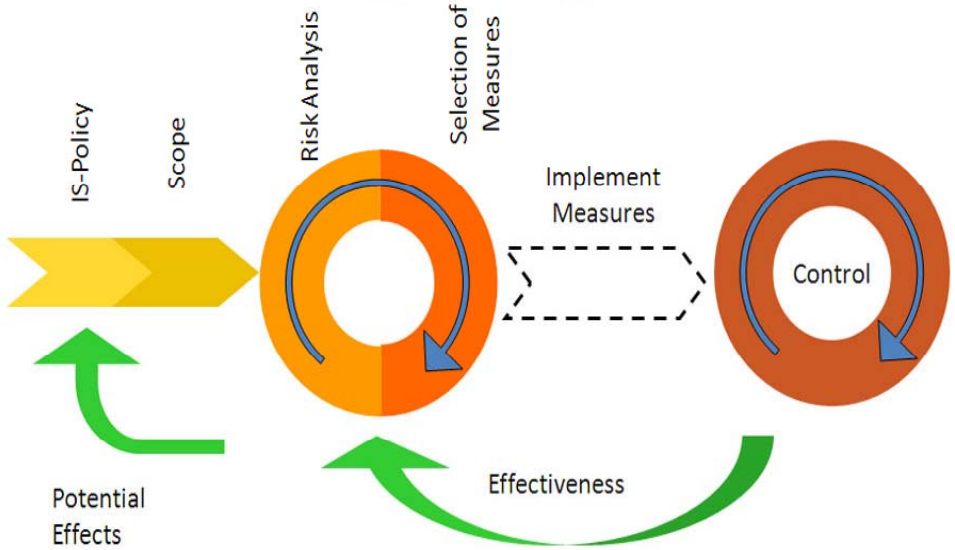
โดยความเสี่ยงแต่ละระดับก็จะมีแนวทางการจัดการที่เหมาะสม เช่น

- **ความเสี่ยงที่ยอมรับได้**: ดำเนินการกำหนดขั้นตอนการปฏิบัติงาน ชี้แจงสร้างความเข้าใจ ปลูกฝังจิตสำนึก และเฝ้าระวังอย่างต่อเนื่อง
- **ความเสี่ยงสูง**: จัดทำ**แผนจัดการความเสี่ยง (Risk Treatment Plan)** โดยในการทำแผนนี้ให้เลือกมาตรการควบคุม (Controls) จาก Annex A ที่เหมาะสมมาใช้งานให้ตรงกับภัยคุกคาม ช่องโหว่ และความเสี่ยง

แนวทางการทำแผนจัดการความเสี่ยง ISO/IEC 27001 (Risk Treatment Plan) (ต่อ)

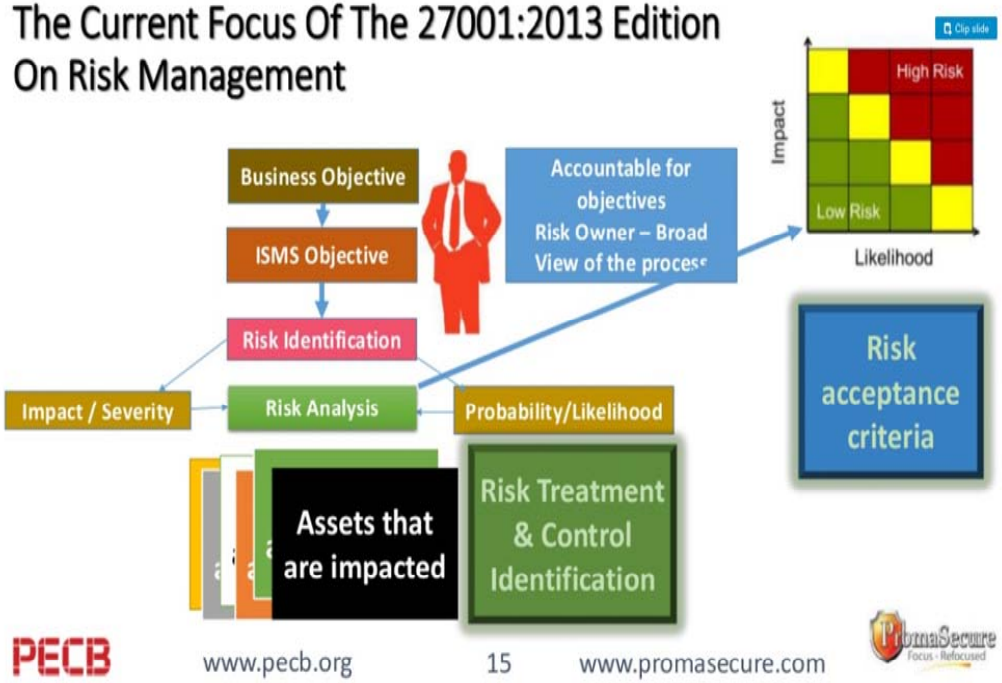


ISO 27001 Information Security Management system



https://avkashk.wordpress.com/information-security-management-systemISO -27001/

The Current Focus Of The 27001:2013 Edition On Risk Management



http://www.slideshare.net/PECBCERTIFICATION/the-significance-of-the-shift-to-risk-management-from-threat-vulnerability-assessment-in-isms

Statement of Applicability

Current as of: DD/MM/YYYY

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Annex A controls			Current controls	Remarks (with justification for exclusions)	Selected controls and reasons for selection				Remarks (overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	Sec	Control Objective/Control							
5 Security Policies	5.1	Management direction for information security							
	5.1.1	Policies for information							
	5.1.2	Review of the policies for information security							
6 Organisation of information security	6.1	Internal organisation							
	6.1.1	Information security roles and responsibilities							
	6.1.2	Segregation of duties							
	6.1.3	Contact with authorities							
	6.1.4	Contact with special interest groups							
	6.1.5	Information security in project management							
	6.2	Mobile devices and teleworking							
	6.2.1	Mobile device policy							
	6.2.2	Teleworking							
7 Human resource security	7.1	Prior to employment							
	7.1.1	Screening							
	7.1.2	Terms and conditions of employment							
	7.2	During employment							
	7.2.1	Management responsibilities							
	7.2.2	Information security awareness, education and training							
	7.2.3	Disciplinary process							
	7.3	Termination and change of employment							
	7.3.1	Termination or change of employment responsibilities							

www.ISO27001security.com

แผนจัดการความเสี่ยง (Risk Treatment Plan)

- มีวัตถุประสงค์เพื่อจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยแผนฯนี้มีคุณสมบัติสำคัญ 2 อย่างคือ
  - จัดการลดโอกาสที่ภัยคุกคามจะใช้ช่องโหว่มาทำอันตรายต่อองค์กร
  - การลดผลกระทบของ Incident ที่เกิดจากความเสี่ยงดังกล่าว
- ในการเขียนแผนจัดการความเสี่ยง ให้โฟกัสไปที่ภัยคุกคามและช่องโหว่ แล้วนำมาตรการควบคุม (Controls) ที่เกี่ยวข้องมาประยุกต์ใช้งาน
- เพื่อการลดโอกาสเกิด และลดผลกระทบจากภัยคุกคามเหล่านั้น เช่น ผลประเมินความเสี่ยงพบว่ามีความเสี่ยงของการเข้าถึงห้อง Server โดยไม่มีการควบคุม ซึ่งผลการประเมินพบว่ามีความเสี่ยงสูงจำเป็นต้องทำแผนจัดการความเสี่ยง

มาตรการควบคุมควบคุมที่เลือกใช้:

1. ในกรณีนี้เป็นเรื่องของการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) จึงเลือกมาตรการควบคุมข้อ **A11.1.2 Physical entry controls (การควบคุมการเข้าออกทางกายภาพ)** โดยเพิ่มอุปกรณ์ Key Card และกล้องวงจรปิด ที่หน้าห้อง Server และเก็บข้อมูลผู้ที่ผ่านเข้าออกทุกครั้งเพื่อตรวจสอบภายหลัง
2. กำหนดนโยบายการเข้าถึงห้อง Server เป็นลายลักษณ์อักษร ซึ่งตรงกับมาตรการควบคุมเรื่อง ข้อ **A9.1.1 Access control policy** โดยอนุญาตให้ผู้เกี่ยวข้องเท่านั้นมีสิทธิผ่านเข้าออกได้ กรณีอื่นให้ร้องขอเป็นลายลักษณ์อักษร เช่น กรณี Vendor มา Maintenance ต้องมีเจ้าหน้าที่ขององค์กรเป็นผู้ร้องขอและนำเข้าไป เป็นต้น (รายละเอียดในการควบคุมนี้ ขึ้นอยู่กับบริบทของแต่ละองค์กร)

- หลังจากกำหนดรายละเอียดการดำเนินงานแล้ว ก็ต้องกำหนดผู้รับผิดชอบปฏิบัติ และงบประมาณที่ต้องใช้ในการจัดหาอุปกรณ์ เครื่องมือต่างๆ ในกรณีนี้ได้แก่ ระบบ Key Card และกล้องวงจรปิด เป็นต้น

มาตรการควบคุมควบคุมที่เลือกใช้: (ต่อ)

อย่างไรก็ตาม แม้ความเสี่ยงจะลดลงแต่ก็มิได้หมายความว่าเราเลิกสนใจไปเลย ตรงกันข้าม เราจำเป็นต้องกำกับดูแล ควบคุมให้เป็นไปตามนโยบายอย่างเคร่งครัด ได้แก่

- ให้สิทธิผ่านเข้าออกเฉพาะผู้ที่เกี่ยวข้องเท่านั้น ตามหน้าที่ความรับผิดชอบ
- บำรุงรักษาอุปกรณ์ระบบ Key Card และกล้องวงจรปิด อย่างสม่ำเสมอ
- ตรวจสอบการจัดเก็บข้อมูล Log ทั้งของ Key card และกล้องวงจรปิดให้แน่ใจว่าจัดเก็บได้ครบถ้วน
- ตรวจสอบย้อนหลัง ว่าผู้ที่ผ่านเข้าออกนั้นเป็นผู้ที่ได้รับอนุญาตตามนโยบาย

9.8 เกร็ดน่ารู้เกี่ยวกับการทำ ISMS

เกร็ดน่ารู้เกี่ยวกับการทำ ISMS

- แนวทางการทำ ISO/IEC 27001:2013 Project Master Plan
- ขั้นตอนการทำ ISO/IEC 27001:2013 Gap Analysis
- ประเด็นน่ารู้เกี่ยวกับคณะทำงานระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013
- Key Success Factors เบื้องหลังการทำระบบ ISO/IEC 27001 ให้สำเร็จจากประสบการณ์จริง
- เคล็ดลับการเตรียมตัวสำหรับผู้ตรวจประเมินภายใน ISO/IEC 27001 Internal Auditor
- ขั้นตอนวางแผนตรวจประเมินภายใน (Internal Audit) ISO/IEC 27001:2013
- ISO/IEC 27001:2013 Human Resource Security – กรณีศึกษา ICANN โดย Hacker ล้วงตับ
- Physical Access Control กับความมั่นคงปลอดภัยตาม ISO/IEC 27001:2013
- การบริหารจัดการระบบ CCTV อย่างมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001:2013
- หลากหลายคำถามที่องค์กรต้องตอบเพื่อป้องกันปัญหา “ข้อมูลรั่วไหล”
- การควบคุมความมั่นคงของข้อมูล และการวัดประสิทธิผลตามข้อกำหนดของมาตรฐาน ISO/IEC 27001

แนวทางการทำ ISO/IEC 27001:2013 Project Master Plan

ISO/IEC 27001:2013 Project Master Plan คือ แผนงานที่กำหนดรายละเอียดกิจกรรมต่าง ๆ เพื่อสร้างระบบการจัดการความมั่นคงปลอดภัยให้เกิดขึ้นในองค์กร แผนงานนี้จะกำหนดช่วงเวลาและผู้รับผิดชอบแต่ละงานทำให้เห็นภาพรวมของเนื้องานในช่วงเวลาต่าง ๆ ช่วยให้บริหารจัดการได้มีประสิทธิภาพมากขึ้น

แนวทางการทำ ISO/IEC 27001:2013 Project Master Plan (ต่อ)

ข้อดีของการทำ Project Plan

- ใช้ประกอบการวางแผนงานประจำปี ทำให้หน่วยงานรู้ว่ามีอะไรต้องทำในช่วงเวลาใด มีประโยชน์อย่างยิ่งในการเตรียมการล่วงหน้าเพื่อจัดสรรเวลาและคนทำงานให้เหมาะสม โดยเฉพาะอย่างยิ่งในกรณีที่องค์กรทำหลายโครงการพร้อมกัน
- ใช้เตรียมงบประมาณ การทำโครงการเพิ่มประสิทธิภาพใด ๆ ก็ตาม จำเป็นต้องใช้งบประมาณมากบ้าง น้อยบ้างแล้วแต่เนื้องาน ISO/IEC 27001:2013 ก็เช่นเดียวกัน การมีแผนงานล่วงหน้าจะทำให้สามารถเตรียมงบประมาณล่วงหน้า เมื่อถึงเวลาทำงานจริงจะได้ไม่ติดขัดเรื่องการใช้งบประมาณที่จำเป็น
- เตรียมบุคลากร คณะทำงานระบบการจัดการความมั่นคงปลอดภัยเป็นตัวแทนของหน่วยงานที่เข้าระบบ *ISO/IEC 27001* ซึ่งส่วนใหญ่ก็จะหนีไม่พ้นหน่วยงานไอที ธุรการ ซ่อมบำรุง และหน่วยงานOperationต่าง ๆ ที่เกี่ยวข้อง Project Master Plan ทำให้รู้ว่ามีกิจกรรมอะไรบ้าง ในช่วงเวลาใด ทำให้คณะทำงานสามารถวางแผนการทำงานของตนเองได้ล่วงหน้า

ISO/IEC 27001:2013 PRJECT MASTER PLAN

ลำดับ	กิจกรรม	ผู้รับผิดชอบ	ช่วงเวลาดำเนินการ							
			1	2	3	4	5	6	7	8
1	รวบรวมกฎหมาย กฎระเบียบด้านเทคโนโลยีสารสนเทศที่ต้องปฏิบัติ									
2	รวบรวมข้อมูลเอกสารความรู้ และศึกษามาตรฐานระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013									
3	รวบรวม Incident ของระบบสารสนเทศ เช่น ระบบล่ม, รายงานปัญหาไวรัส มัลแวร์ต่าง ๆ เป็นต้น									
4	สรุปเหตุผลและความจำเป็นในการจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013									
5	(ร่าง)กำหนดขอบเขตการจัดทำระบบฯ โดยกำหนดเป็นระบบงาน หน่วยงาน หรือทั้งองค์กร									
6	นำเสนอข้อมูลต่อผู้บริหารเพื่อพิจารณา									
7	กำหนดคณะทำงานระบบฯ ประกอบด้วยตัวแทนหน่วยงานที่อยู่ในขอบเขตระบบ ISO/IEC 27001									

ISO/IEC 27001:2013 PRJECT MASTER PLAN										
ลำดับ	กิจกรรม	ผู้รับผิดชอบ	ช่วงเวลาดำเนินการ							
			1	2	3	4	5	6	7	8
8	คณะทำงานฯ ศึกษาข้อกำหนดของมาตรฐาน ISO/IEC 27001									
9	คณะทำงานฯ สำรวจสถานะปัจจุบันของระบบสารสนเทศ เปรียบเทียบกับข้อกำหนด ISO/IEC 27001 (Gap Analysis)									
10	กำหนดนโยบายความมั่นคงปลอดภัยของสารสนเทศ และจัดทำเอกสารต่างๆ									
11	ฝึกอบรมให้ความรู้แก่พนักงาน และผู้เกี่ยวข้อง (รวมผู้รับเหมา)									
12	ดำเนินระบบตามแนวทางที่กำหนด และเฝ้าระวังตรวจวัดตามแผนงาน									
13	ตรวจประเมินภายในระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศและแก้ไขข้อบกพร่อง									
14	รายงานผลการทำระบบ ISO/IEC 27001 ต่อผู้บริหาร									

ขั้นตอนการทำ ISO/IEC 27001:2013 Gap Analysis

ISO/IEC 27001:2013 Gap analysis **คืออะไร**

- คือการสำรวจตรวจสอบและประเมินสิ่งที่เป็นอยู่ ณ.ปัจจุบัน (ก่อนเริ่มทำระบบ) เปรียบเทียบกับข้อกำหนดของ ISO/IEC 27001:2013

พูดอีกอย่างก็คือ การตรวจประเมินด้วยข้อกำหนด ISO/IEC 27001:2013 เพื่อดูว่าหน่วยงานมีอะไรอยู่แล้ว และยังขาดอะไรที่ต้องทำเพิ่ม

ขั้นตอนการทำ ISO/IEC 27001:2013 Gap Analysis

1. **ชี้แจงสื่อสารทำความเข้าใจวัตถุประสงค์ของการทำ Gap Analysis** ให้ทราบทั้งองค์กร โดยเฉพาะหน่วยงานที่จะถูกประเมิน
2. **ผู้ทำ Gap Analysis ศึกษาข้อกำหนด (ISO/IEC 27001 Requirements)** ของ ISO/IEC 27001:2013 ให้เข้าใจ
3. **จัดทำ Checklist ตามข้อกำหนด** - ควรใช้คำถามที่เกี่ยวข้อง และถ้าให้ดีควรถามให้ตรงกับบริบท (Context) ของหน่วยงานที่ไปประเมิน (การที่ใช้ Standard checklist ไปสอบถาม อาจทำให้คนที่ถูกถามไม่เข้าใจคำถาม จำเป็นต้องมีการปรับ Checklist ให้เหมาะกับบริบทขององค์กร)
4. **สอบถามขั้นตอน ความเข้าใจของผู้ตอบ และเรียกดูหลักฐาน** ทั้งเอกสารและข้อมูลในระบบที่เกี่ยวข้อง

ขั้นตอนการทำ ISO/IEC 27001:2013 Gap Analysis (ต่อ)

5. **บันทึกสิ่งที่พบให้ชัดเจน** เช่น สัมภาษณ์ใคร ชื่อ ตำแหน่ง หน่วยงาน เอกสารอะไร (ชื่อเอกสาร, รหัส) ที่พบว่าไม่สอดคล้อง
6. **สรุปผลและทำรายงาน** - โดยสรุปตามข้อกำหนด ISO/IEC 27001:2013 ทุกข้อ เช่น เรื่องประเมินความเสี่ยง องค์กรมีหรือไม่มี ถ้ามีแล้วมีครบตามข้อกำหนดหรือไม่ เป็นต้น
7. **นำเสนอต่อผู้บริหารสูงสุด (Top Management)** เพื่อรายงานให้ทราบถึงสถานะปัจจุบัน ว่าอยู่ในระดับใด ยังขาดอะไรบ้างที่จะได้มาตรฐาน ตาม ISO/IEC 27001:2013

ISO/IEC 27001:2013 Gap Analysis

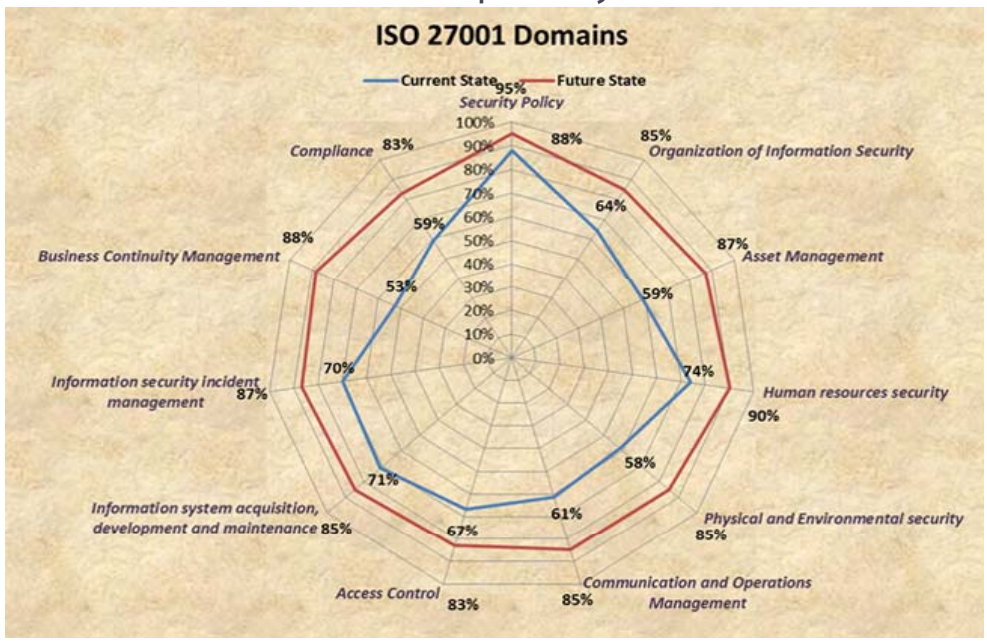
- หัวใจสำคัญของ ISO/IEC 27001:2013 Gap Analysis คือ ข้อมูลทำให้รู้ว่าองค์กรของเรายังขาดอะไร แค่ไหน
- ที่สำคัญคือ มีอะไรที่ยังไม่สอดคล้องตามกฎหมายบ้าง
- Report ที่ได้จากกิจกรรมนี้ เป็นจุดตั้งต้นของการปรับปรุงองค์กรให้มีความมั่นคงปลอดภัย ให้ผู้บริหารหยิบไปใช้วางแผนเตรียมงาน เตรียมคน เตรียมงบประมาณ เพื่อปิด Gap เหล่านี้

ประเมินความพร้อมด้านระบบบริหารความมั่นคงปลอดภัยด้วย ISO/IEC 27001:2013
ด้วยระบบ Information Security Management System Self Assessment จาก ACIS Professional Center

1.การประเมินส่วนที่ 1 ระบบบริหารจัดการ (Management Systems)

	0	1	2	3	4	5
1) บริบทขององค์กร (Context)	0	1	2	3	4	5
มีการกำหนดประเด็นที่เกี่ยวข้องกับผลลัพธ์ที่ต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ทั้งที่เป็นประเด็นภายใน และประเด็นภายนอก						
มีการกำหนดกลุ่มผู้ที่ต้องให้ความสนใจ (Interested parties) ซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และรวบรวมความต้องการ ความคาดหวังจากกลุ่ม						
มีการกำหนดขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยพิจารณาจาก 1.1 และ 1.2 พร้อมทั้งระบุกิจกรรมที่เชื่อมโยงหรือเกี่ยวข้องซึ่งดำเนินการโดยภายในองค์กรและภายนอกองค์กร						
2) ความเป็นผู้นำ (Leadership)	0	1	2	3	4	5
ผู้บริหารระดับสูงได้กำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศและวัตถุประสงค์ที่สอดคล้องกับทิศทางเชิงกลยุทธ์ขององค์กร						
มีการบูรณาการข้อกำหนดของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเข้ากับกระบวนการขององค์กร						
มีการจัดเตรียมทรัพยากรที่จำเป็นสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ						
มีการส่งเสริมให้มีการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง						
3) นโยบาย (Policy)	0	1	2	3	4	5
มีนโยบายที่อยู่ในรูปแบบข้อมูลเชิงเอกสาร (Documented information)						
มีการสื่อสารภายในองค์กร						
มีการสื่อสารและพร้อมให้เข้าถึงได้อย่างเหมาะสม สำหรับผู้ที่ต้องให้ความสนใจ						
4) บทบาท หน้าที่ความรับผิดชอบและอำนาจ (Organizational roles, responsibilities and authorities)	0	1	2	3	4	5
ภายในองค์กรที่ทำให้มั่นใจว่าสามารถดำเนินระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามข้อกำหนดของมาตรฐาน						
มีการรายงานสมรรถนะการดำเนินการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต่อผู้บริหารระดับสูง						
4) การวางแผน (Planning)	0	1	2	3	4	5
มีการกำหนดกระบวนการสำหรับประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศที่ทำให้มั่นใจว่าสามารถประเมินซ้ำได้ตลอดที่ผลลัพธ์สามารถนำมาเปรียบเทียบได้ มีความสอดคล้องและถูกต้อง						
มีการกำหนดหลักเกณฑ์ในการยอมรับความเสี่ยงและหลักเกณฑ์สำหรับดำเนินการประเมินความเสี่ยง						
มีการประเมินความเสี่ยงตามหลักเกณฑ์ที่กำหนด โดยครอบคลุมขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ						
มีการพิจารณาระดับความเสี่ยงและจัดทำแผนการลดความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ สำหรับความเสี่ยงที่เกินกว่าระดับการ						
มีการจัดการแผนการดำเนินความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับวัตถุประสงค์						
5) การปฏิบัติการ (Operation)	0	1	2	3	4	5
มีการนำแผนการลดความเสี่ยงและแผนการดำเนินความมั่นคงปลอดภัยสารสนเทศมาดำเนินการเพื่อให้บรรลุตามเป้าหมาย						
มีการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ ตามเกณฑ์สำหรับดำเนินการประเมินความเสี่ยงที่กำหนดขึ้น						
6) การประเมินสมรรถนะ (Performance evaluation)	0	1	2	3	4	5

ตัวอย่างผลลัพธ์ที่ได้จาก Gap Analysis



 http://www.isaca.org/COBIT/focus/Pages/iso-iec-27001-process-mapping-to-cobit-4-1-to-derive-a-balanced-scorecard-for-it-governance.aspx

ประเด็นน่ารู้เกี่ยวกับคณะทำงานระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013

- บทบาทหน้าที่ของคณะทำงาน (Working Committee) ระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001 โดยทั่วไปมีดังนี้ (รวบรวมจากประสบการณ์ บางองค์กรอาจมีหน้าที่มากหรือน้อยกว่านี้ก็ได้ ไม่ได้เป็นกฎตายตัวแต่อย่างใด)

ประเด็นน่ารู้เกี่ยวกับคณะทำงานระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013 (ต่อ)

1. คณะทำงานระบบฯคือทีมงานที่มีหน้าที่สร้างระบบให้เกิดขึ้นเป็นรูปธรรม จัดทำเอกสารและนำไปปฏิบัติ รวมถึงมีส่วนร่วมในการกำกับดูแลด้านความมั่นคงปลอดภัยของสารสนเทศในหน่วยงานตนเอง

2. คณะทำงานฯ ควรประกอบด้วยตัวแทนจากหน่วยงานต่าง ๆ ที่อยู่ในขอบเขตของการจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001

3. คณะทำงานฯ มีหน้าที่ในการประเมินความเสี่ยงของสารสนเทศในหน่วยงานตนเอง และมีส่วนร่วมในการกำหนดมาตรการจัดการความเสี่ยงที่เหมาะสม

4. คณะทำงานฯจะต้องมีความรู้ในข้อกำหนดของมาตรฐาน ISO/IEC 27001:2013 มีความรู้ในหลักการและวิธีการประเมินความเสี่ยงของสารสนเทศ

ประเด็นน่ารู้เกี่ยวกับคณะทำงานระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013 (ต่อ)

5. มีบทบาทสำคัญในการชี้แจง แนะนำ สื่อสารประชาสัมพันธ์ในหน่วยงานตนเองถึงการปฏิบัติตามมาตรการต่าง ๆ ที่เกี่ยวข้องกับการป้องกันสารสนเทศให้มั่นคงปลอดภัย

6. จัดทำหรือมีส่วนร่วมในการจัดทำเอกสารเกี่ยวกับการปฏิบัติงานของหน่วยงานตนเอง ตามมาตรการด้านความมั่นคงปลอดภัยของสารสนเทศ เช่น หน่วยงาน HR ก็จัดทำเอกสารขั้นตอนการดำเนินงานกรณีพนักงานลาออกหรือโอนย้ายหน่วยงาน ซึ่งขั้นตอนการดำเนินงานก็จะมีรายละเอียดครอบคลุมตั้งแต่ การเรียกคืนทรัพย์สินขององค์กร การถอดถอนสิทธิการเข้าถึงระบบงาน เป็นต้น

7. มีส่วนร่วมในการปิดช่องโหว่ของระบบ (Vulnerability) โดยอาจเป็นผู้ดำเนินการเองหรือควบคุมการดำเนินการก็ได้

ประเด็นน่ารู้เกี่ยวกับคณะทำงานระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013 (ต่อ)

8. มีส่วนร่วมในการตรวจประเมินภายในระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISO27001 Internal Audit)

9. เป็นผู้รับการตรวจประเมินภายในระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (Internal Auditee)

10. เป็นรับการตรวจประเมิน (Auditee) เพื่อขอการรับรอง (ISO/IEC 27001:2013 Certification Audit) ซึ่งในกรณีนี้ จะมีผู้ตรวจจากภายนอกเข้ามาตรวจประเมินในองค์กรของเรา ถ้าผลการตรวจผ่านก็จะได้ใบรับรองมาตรฐานระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001

Key Success Factors เบื้องหลังการทำระบบ ISO/IEC 27001 ให้สำเร็จจากประสบการณ์จริง

Key Success factors ของการทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001

1. ได้รับการสนับสนุนจากผู้บริหารระดับสูง (Top Management) อย่างเป็นรูปธรรม

- การทำระบบ Information Security Management System (ISMS) - ISO/IEC 27001 นั้นทำให้ผู้เกี่ยวข้องโดยเฉพาะผู้ใช้งานทั่วไป (User) รู้สึกยุ่งยากกว่าเดิม และจะเริ่มบ่น เริ่มดื้อ
- บางครั้งคนที่บ่นและดื้อก็เป็นระดับบริหารซะเอง แบบนี้ทำให้คณะทำงานงานสร้างระบบฯทำงานลำบาก ร้อนถึงผู้บริหารระดับสูง (Top Management) ต้องแสดงจุดยืนชัด ๆ ว่าสนับสนุนให้ทำระบบฯ ให้สำเร็จ เพราะหากเบอร์ 1 ไม่ทุบโต๊ะเสียงบ่นก็จะเริ่มดังขึ้น การดื้อไม่ให้ความร่วมมือก็จะมากขึ้นและลงท้ายด้วยการเลิกทำระบบในที่สุด

Key Success factors ของการทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001 (ต่อ)

2. กำหนดขอบเขตของระบบ (Scope) ให้ชัดเจน

- ขอบเขตการทำระบบ (Scope) เป็นตัวกำหนดว่าผู้เกี่ยวข้องมีใครบ้าง ระบบงานใดบ้าง สถานที่และระบบสนับสนุนที่เกี่ยวข้อง ในการกำหนดขอบเขต (Scope) มาตรฐานISO/IEC 27001:2013 กำหนดให้พิจารณาบริบท (Context) ขององค์กรซึ่งต้องพิจารณาถึง **Interested parties** ที่เกี่ยวข้องด้วย
- ประเด็นสำคัญคือ ขอบเขตที่จัดทำระบบฯต้องสมเหตุผล ตอบโจทย์ของ Interested parties และไม่ควรกว้างเกินไปจนไม่สามารถกำกับดูแลได้อย่างมีประสิทธิภาพ เช่น บางบริษัทฯ มีสาขากระจายอยู่ทั่วประเทศ และสาขาต่างจังหวัดหลายแห่งก็ขาดบุคลากรที่มีความรู้ความสามารถเพียงพอ แบบนี้ถ้าทำระบบทั้งหมดครอบคลุมทุกสาขาก็มีแนวโน้มว่าจะสำเร็จได้ยาก เป็นต้น

Key Success factors ของการทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001 (ต่อ)

3. ตัวแทนผู้บริหาร หรือ Information Security Management Representative (ISMR) กำกับดูแลควบคุมและติดตามงาน

- Project Leader ของการทำ ISO/IEC 27001 ก็คือ ตัวแทนฝ่ายบริหาร หรือ ISMR นี่แหละ ถ้าจะบอกว่าความสำเร็จของการทำระบบฯมาจากการเอาจริงเอาจังทั้งบุ๋นและบู๊ของ ISMR ก็ไม่ใช่เรื่องเกินจริงแต่อย่างใด เพราะว่า ISMR นั้นกำกับทุกขั้นตอนตั้งแตเริ่มทำระบบ (Establish) นำไปใช้ (Implement) ตรวจประเมิน (Audit) เฝ้าระวังและตรวจสอบ (Monitor and Measurement) รวมถึงการแก้ไขปรับปรุงอย่างต่อเนื่อง (Continual Improvement)
- ISMR นั้นควรมีความรู้ในบริบทขององค์กรเป็นอย่างดีและควรมีความรู้เกี่ยวกับข้อกำหนดของ ISO/IEC 27001 ในระดับปานกลางขึ้นไป คือ เข้าใจภาพรวมและการนำไปใช้จริงในองค์กร ที่สำคัญ ISMR ควรมี Power ในระดับที่สามารถตามงานจากหน่วยงานต่าง ๆ สามารถเชิญประชุม และตัดสินใจได้ (ยกเว้นบางเรื่องที่ต้องขอไฟเขียวจาก Top Management เช่นเรื่องงบประมาณ ฯลฯ)

Key Success factors ของการทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001 (ต่อ)

4. กระจายงานให้คณะทำงานอย่างเหมาะสม

- ปัญหาที่เจอบ่อยมาก ๆ ในการทำระบบฯ คือ งานกระจุกตัวอยู่ที่คนใดคนหนึ่งมากเกินไป อาจเป็นเพราะแบ่งงานไม่ดีหรือมีปัญหาในการกระจายงาน (เกี่ยงไม่ยอมรับงาน) เจอแบบนี้ ISMR ต้อง Action และบางกรณีอาจต้องขอให้ Top Management สั่งลงมาเป็นทางการก็เคยเจอ หากปล่อยไว้แบบนี้งานไม่เดินและคนที่รับโหลดงานเยอะก็จะล้าและถอดใจ สุดท้ายระบบนี้ fail

Key Success factors ของการทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001 (ต่อ)

5. สร้างแรงจูงใจให้คณะทำงาน

- จากประสบการณ์ในฐานะที่ปรึกษา (Consultant) พบว่าส่วนใหญ่คณะทำงานระบบฯ มีงานประจำในตำแหน่งต่าง ๆ ไม่ใช่ทำระบบฯแบบ Full Time พูดแบบไม่เกรงใจ การทำระบบฯ คือ งานที่เพิ่มขึ้นมานั่นเอง! ดังนั้นการ**สร้างแรงจูงใจ**ให้คณะทำงานฯ จึงสำคัญไม่แพ้เรื่องอื่น ๆ

- หลายบริษัทฯ มีแต้มพิเศษให้คณะทำงานในฐานะที่ Contribute ให้กับองค์กร บางแห่งมีมีงบฯ สำหรับเลี้ยงขนม อาหารให้คณะทำงานฯในกรณีอยู่ดึกหรือทำงานวันหยุด บางที่แจกเสื้อ Jacket ฯลฯ เรื่องนี้อาจดูไม่สำคัญในสายตาผู้บริหาร แต่เชื่อหรือไม่ว่าเรื่องเล็ก ๆ น้อยนี่แหละมีส่วนช่วยให้หลาย ๆ ที่ทำระบบสำเร็จและรักษาระบบไว้ได้หลังจากได้ใบรับรองแล้ว

เคล็ดลับการเตรียมตัวสำหรับผู้ตรวจประเมินภายใน ISO/IEC 27001 Internal Auditor

เคล็ดลับการเตรียมตัวสำหรับผู้ตรวจประเมินภายใน ISO/IEC 27001 Internal Auditor (ต่อ)

1. ทำความเข้าใจข้อกำหนด (ISO/IEC 27001 Requirements):

ข้อนี้เป็นหัวใจสำคัญเลยทีเดียวของการเป็นผู้ตรวจประเมินภายใน ISO/IEC 27001 (ISO/IEC 27001 Internal auditor) ย้ำว่าเข้าใจข้อกำหนด (ISMS Requirements) ไม่ถึงขนาดท่องจำได้ทุกข้อเพราะเรามี Checklist เป็นตัวช่วยสำคัญ

การที่ผู้ตรวจประเมิน (Auditor) มีความเข้าใจสามารถจับประเด็นสำคัญที่เป็น keyword ของข้อกำหนด จะช่วยให้ประเมินสิ่งที่ตรวจพบ (Evidence) ได้อย่างมีประสิทธิภาพ และที่สำคัญเมื่อผู้ตรวจประเมินมีความเข้าใจ จะสามารถอธิบายสิ่งที่ไม่สอดคล้อง (หรือข้อบกพร่อง) ที่พบให้ผู้ถูกตรวจยอมรับได้

เคล็ดลับการเตรียมตัวสำหรับผู้ตรวจประเมินภายใน ISO/IEC 27001 Internal Auditor (ต่อ)

2. ทำความเข้าใจหน่วยงานที่จะต้องไปตรวจ (Auditee):

- อย่างน้อยควรเข้าใจและเห็นภาพรวมพอสมควร เช่น หน่วยงานมีหน้าที่อะไร มีระบบงานอะไรบ้าง น่าจะมีภัยคุกคามและความเสี่ยงอะไรบ้าง (คร่าว ๆ) ตรงนี้ผู้ตรวจประเมินฯ อาจพอเดาได้ว่าน่าจะใช้เวลามากกับจุดไหนมากน้อยเท่าไร เช่น สัมภาษณ์และตรวจสอบเอกสาร 1 ชม. สำรวจสถานที่ปฏิบัติงาน 45 นาที เป็นต้น (จะใช้เวลามากหรือน้อยขึ้นอยู่กับภัยคุกคาม ความเสี่ยงและความซับซ้อน)

เคล็ดลับการเตรียมตัวสำหรับผู้ตรวจประเมินภายใน ISO/IEC 27001 Internal Auditor (ต่อ)

3. เตรียมคำถามหรือเช็คลิสต์ (ISO/IEC 27001:2013 Checklist):

- หลังจากที่ทำความเข้าใจหน่วยงานที่ได้รับมอบหมายให้ตรวจแล้ว auditor ก็มีภารกิจสำคัญคือการเตรียมคำถาม ที่เรียกกันติดปากว่า Checklist นั่นเอง นี่ถือเป็นยาขมอย่างหนึ่งของการเป็นผู้ตรวจประเมิน เพราะหากไม่เข้าใจข้อกำหนดเพียงพอ ก็จะไม่รู้ว่าอะไรคือ Keyword สำคัญที่จะใช้เป็นคำถาม วิธีแก้ง่าย ๆ คือ ย้อนกลับไปดูข้อ 1:)

เคล็ดลับการเตรียมตัวสำหรับผู้ตรวจประเมินภายใน ISO/IEC 27001 Internal Auditor (ต่อ)

- หรือจะใช้ checklist จากคนอื่น (หาในอินเทอร์เน็ต หรือจากที่ปรึกษา) ก็เป็นอีกทางเลือกหนึ่งที่นิยมเพราะประหยัดเวลา
- จากประสบการณ์ในฐานะที่ปรึกษา ISO/IEC 27001 พบว่าหลายคนได้ Checklist มาก็ลุยเลย คือ ไม่ได้ทำความเข้าใจข้อกำหนด พอถึงวันตรวจก็ถือ Checklist ไปหน้างานแล้วอ่านคำถามจาก Checklist ทั้งดุ้น ปรากฏว่าคนถูกถามไม่เข้าใจ ไม่เข้าใจคำถามว่าอยากรู้อะไร จึงย้อนถามกลับมา คราวนี้งงกันทั้งคู่!!
- ทางแก้คือ ผู้ตรวจประเมิน (Internal Auditor) จะต้องทำความเข้าใจคำถาม และควรปรับภาษาจากภาษาเขียนให้เป็นภาษาพูด จะขอดูเอกสารอะไรหรือสัมภาษณ์ใครก็จดไว้ใน Checklist ให้ชัดเจน

เคล็ดลับการเตรียมตัวสำหรับผู้ตรวจประเมินภายใน ISO/IEC 27001 Internal Auditor (ต่อ)

4. เรียบเรียงคำถาม: ควรเรียบเรียงคำถามให้เป็นไปตามลำดับงาน หรือกระบวนการทำงาน

เช่น การถามเพื่อ Audit ระบบงานจัดซื้อ ก็ควรวางคำถามตามลำดับขั้นตอนการจัดซื้อ โดยเริ่มจาก Purchase request แล้วไปต่อที่ Review และตามด้วย Approve เป็นต้น อย่าวางคำถามโดดไปโดดมา เพราะจะทำให้จับประเด็นได้ยาก และจะงงทั้งคนตรวจและคนถูกตรวจ .....

4 เคล็ดลับการเตรียมตัวสำหรับผู้ตรวจประเมินภายใน ISO/IEC 27001 Internal Auditor (ต่อ)

- การเป็นผู้ตรวจประเมินภายใน ISO/IEC 27001 นั้นจำเป็นต้องมีความรู้และทักษะเพียงพอ ซึ่งต้องเตรียมความพร้อมกันล่วงหน้าพอสมควร ในหลายองค์กรนิยมให้ผู้ตรวจประเมินระบบอื่นเช่น ระบบคุณภาพ ISO 9001 (ผ่านการอบรมข้อกำหนดหรือ หลักสูตรการตรวจประเมินภายใน ISO/IEC 27001) มาร่วมทีมตรวจ ซึ่งมีข้อดี คือ
  - มีประสบการณ์และทักษะในการถาม การเรียกดูเอกสาร แต่อาจไม่มีความรู้เชิงลึกในด้านไอที ปัญหานี้แก้ได้ด้วยการจัดทีมให้มีผู้รู้ด้านไอทีร่วมทีมไปด้วยเป็นการเรียนรู้ไปด้วยกัน

ขั้นตอนวางแผนตรวจประเมินภายใน (Internal Audit) ISO/IEC 27001:2013

- การตรวจประเมินภายใน (Internal Audit ISO/IEC 27001:2013) เป็นกิจกรรมบังคับสำหรับหน่วยงานที่จัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System: ISMS) ISO/IEC 27001:2013 ภาพรวมของการวางแผนแบ่งเป็น 7 ขั้นตอน

ขั้นตอนวางแผนตรวจประเมินภายใน (Internal Audit) ISO/IEC 27001:2013 (ต่อ)

1. เตรียมบุคลากรที่จะทำหน้าที่เป็นผู้ตรวจประเมินภายใน (Internal auditor) ISO/IEC 27001:2013

- โดยผู้ตรวจประเมินเหล่านี้จะต้องมีความรู้และเข้าใจในข้อกำหนด (Requirements) ของ ISO/IEC 27001:2013 ว่าแต่ละข้อกำหนดมีเจตนารมณ์อย่างไร และควรจะดูหลักฐานอะไรเพื่อยืนยันว่าได้ปฏิบัติตามข้อกำหนดเหล่านั้น (ไม่เน้นจำข้อกำหนด ขอเพียงเข้าใจและทำ Checklist ล่วงหน้าก็ตรวจประเมินได้ระดับหนึ่งแล้ว)

2. กำหนดช่วงเวลาที่จะทำการตรวจประเมินไว้ล่วงหน้า

- โดยส่วนใหญ่นิยมตรวจปีละ 2 ครั้ง และมีการแจ้งกำหนดการตรวจประเมิน (Audit Schedule) ล่วงหน้าไปยังหน่วยงานที่อยู่ภายในขอบเขต (Scope) ของการทำระบบ เพื่อให้หน่วยงานได้รับทราบและเตรียมตัว เตรียมข้อมูลไว้รับการตรวจ

ขั้นตอนวางแผนตรวจประเมินภายใน (Internal Audit) ISO/IEC 27001:2013 (ต่อ)

3. กำหนดขอบเขตของการตรวจประเมิน

- โดยกำหนดเป็นพื้นที่ หน่วยงาน หรือระบบงาน ให้ชัดเจน เพื่อจะได้วางแผนตรวจประเมินโดยพิจารณาถึงขนาดและความซับซ้อนของระบบงานหรือหน่วยงานที่ไปตรวจ รวมถึงการจัดเวลาและผู้ตรวจประเมินที่มีทักษะและความสามารถตรงกับภารกิจได้อย่างเหมาะสม

4. หากเป็นการตรวจประเมินภายในครั้งแรก (มือใหม่หัดตรวจ) แนะนำให้นำ Gap Analysis ISO/IEC 27001:2013 มาเป็นแนวทางการวางแผน

- โดยให้ list สิ่งที่รายงาน Gap Analysis ระบุว่ายังไม่ได้ทำ หรือยังไม่มี เช่น ยังไม่มีนโยบายความมั่นคงปลอดภัยของสารสนเทศเป็นลายลักษณ์อักษร นี่คือสิ่งที่จะต้อง Focus เวลาไปตรวจประเมิน ส่วนที่รายงาน Gap Analysis ระบุว่ามีแล้ว ก็ให้ Internal Auditor ไปตรวจว่ายังรักษาอยู่ได้หรือไม่ เป็นต้น

ขั้นตอนวางแผนตรวจประเมินภายใน (Internal Audit) ISO/IEC 27001:2013 (ต่อ)

5. ถ้าเป็นการตรวจประเมินครั้งที่ 2 เป็นต้นไป เวลาวางแผนตรวจประเมินควรดูผล Audit คราวก่อนด้วย จะได้รู้ว่าตอนตรวจประเมินความก่อนมีปัญหาอุปสรรคอะไร

- เช่น ในแผนให้เวลามากไป น้อยไป ผู้ตรวจถามตรงประเด็นหรือไม่ ฯลฯ นอกจากนี้ให้ดูว่าการตรวจประเมินคราวก่อนพบข้อบกพร่องที่หน่วยงานใดมากที่สุด ตรวจคราวนี้จะได้ไปทวนสอบดูว่าได้แก้ปัญหาเหล่านั้นเรียบร้อยหรือยัง แก้ตรงจุดได้ผลชะงัดหรือไม่ เป็นต้น

6. วางแผนการตรวจประเมินภายใน (Internal Audit) โดยพิจารณาว่าแต่ละหน่วยงานจะถูกตรวจข้อกำหนด ISO/IEC 27001:2013 ใดบ้าง

- จุดสำคัญคือผู้ที่วางแผนนี้จะต้องเข้าใจในข้อกำหนด และบริบทของหน่วยงานที่ถูกตรวจ ผลที่ได้คือ วางแผนตรวจประเมินภายในได้ครอบคลุม ครบถ้วนและกำหนดเวลาได้เหมาะสม

ขั้นตอนวางแผนตรวจประเมินภายใน (Internal Audit) ISO/IEC 27001:2013 (ต่อ)

7. เสนอตัวแทนฝ่ายบริหาร (Management Representative) พิจารณาและแนะนำให้เสนอต่อ Top Management ลงนามในแผนให้มีผลบังคับใช้อย่างเป็นทางการ

- เมื่อจัดทำแผนการตรวจประเมินภายใน (Internal audit ISO/IEC 27001:2013) เรียบร้อยแล้ว ให้เสนอตัวแทนฝ่ายบริหาร (Management Representative) พิจารณาและแนะนำให้เสนอต่อ Top Management ลงนามในแผนให้มีผลบังคับใช้อย่างเป็นทางการ (ไม่มีใครกล้าเบี้ยว ถ้าไม่มีเหตุจำเป็นจริง ๆ)
- ในที่นี้กล่าวถึงขั้นตอนการวางแผนตรวจประเมินเพื่อให้เข้าใจภาพรวมกว้าง เวลาที่วางแผนจริงจะต้องอ้างอิงระเบียบปฏิบัติ (Procedure) ซึ่งจะกำหนดหน้าที่ไว้อย่างชัดเจนว่าใครเป็นผู้จัดทำ Audit Plan ใช้แบบฟอร์มอะไร ใครเป็นผู้อนุมัติ และแจ้งหน่วยงานให้ทราบล่วงหน้าอย่างน้อยกี่วัน รวมถึงอาจกำหนดคุณสมบัติของผู้ตรวจประเมิน (ISO/IEC 27001:2013 Internal auditor) ไว้เป็นลายลักษณ์อักษรด้วย

ISO/IEC 27001:2013 Human Resource Security – กรณีศึกษา ICANN โดย Hacker ล้วงตับ

ISO/IEC 27001:2013 Human Resource Security – กรณีศึกษา ICANN โดย Hacker ล้วงตับ (ต่อ)

- เรียบร้อยโรงเรียน Hacker ไปอีกราย เมื่อ ICANN หรือ The Internet Corporation for Assigned Names and Numbers (ICANN) โดนมือดีฝ่าระบบป้องกัน (Information & Network Security) เข้าไปล้วงตับองค์กรสำคัญระดับโลกนี้
- ภารกิจ Hacking นี้ใช้เทคนิค **spear phishing attack** คือปลอม Email ว่ามาจาก Trusted source **หลอกให้ Staffs ป้อนข้อมูลที่ sensitive เช่น username, password etc.** เมื่อได้ข้อมูลลับแล้ว Hacker ก็นำไปขยายผลไปยังระบบเหล่านี้
  - Centralized Zone Data System (CZDS)
  - ICANN Governmental AdvISO ry Committee (GAC) Wiki
  - ICANN Blog
  - ICANN WHOIS information portal
- ที่น่าตกใจคือ Hacker เข้าถึงข้อมูลของระบบ Centralized Zone Data System (CZDS) **ด้วยสิทธิ Admin !!!**

ISO/IEC 27001:2013 Human Resource Security – กรณีศึกษา ICANN โดย Hacker ล้วงตับ (ต่อ)

- รายงานข่าวอ้างอิงจาก http://www.esecurityplanet.com/network-security/icann-hacked.html เผยถึงสิ่งที่ Hacker ได้โชว์สเตปไว้ คือ การ Copy ไฟล์เหล่านี้ออกไป
  - Zone files
  - Username and hashed password
  - Mailing address
  - Fax number
  - Phone number
- โฆษกของ ICANN ได้แถลงยอมรับถึงเหตุการณ์นี้ และบอกว่า ณ ตอนนี้ยังไม่พบความเสียหาย!! (แต่อนาคตตัวใครตัวมัน - โฆษกไม่ได้กล่าว)

ISO/IEC 27001:2013 Human Resource Security – กรณีศึกษา ICANN โดย Hacker ล้วงตับ (ต่อ)

- นอกจากนี้ยังแถ-ลง ว่า ช่วงก่อนนี้ทาง ICANN ได้ปรับปรุง Security มาแล้วระดับหนึ่ง ทำให้ Hacker เจาะได้แค่นี้ **หักมุมซะงั้น...**
- หลังเหตุการณ์ ICANN ได้ **reset password** ใหม่พร้อมแจ้งให้ user รับทราบและดำเนินการเปลี่ยน password
- จากเนื้อข่าว ปัญหานี้น่าจะเกิดจาก Staffs ของ ICANN แต่การแก้ปัญหาเราไม่ได้บอกว่าจะแก้ปัญหาที่ Staffs อย่างไร บอกแต่ reset password ของ user ซึ่งจริง ๆ แล้ว กรณีนี้เขาไม่ได้ผิดอะไรเลย

ISO/IEC 27001:2013 Human Resource Security – กรณีศึกษา ICANN โดย Hacker ล้วงตับ (ต่อ)

- ISO/IEC 27001:2013 ให้ความสำคัญกับการสร้าง Awareness ให้กับพนักงานทุกระดับ และ Outsources รวมถึงผู้เกี่ยวข้องซึ่งรวมถึงนักศึกษาฝึกงาน แม่บ้าน รปภ. เป็นต้น เพราะบุคคลเหล่านี้เป็น Attack surface ที่ Hacker โจมตีได้ง่าย ดังเช่นกรณีของ ICANN
- มาตรการควบคุม (Controls) ที่เกี่ยวข้องกับการควบคุมพนักงานขององค์กร ได้แก่ **A.7 Human resource security** ซึ่งครอบคลุมตั้งแต่ก่อนจ้างงาน (Prior Employment) ระหว่างการจ้างงาน (During Employment) และการออกจากงานหรือโอนย้าย (Termination and Change of employment)

ISO/IEC 27001:2013 - A7 Human Resource Security มาตรการควบคุมบริหารจัดการคน

- วัตถุประสงค์ของมาตรการควบคุมด้าน Information Security Management ตาม ISO/IEC 27001:2013 ในเรื่อง Human Resource Security คือให้เรากำหนดวิธีการให้มั่นใจว่าพนักงาน (Employees) และผู้รับจ้างช่วง (Contractors) นั้นเข้าใจหน้าที่และความรับผิดชอบของตน รวมถึงการสรรหาคนทำงานที่มีความเหมาะสมกับบทบาทที่ได้รับมอบหมาย

ISO/IEC 27001:2013 - A7 Human Resource Security มาตรการควบคุมบริหารจัดการคน (ต่อ)

คนหรือบุคลากรเป็นโจทย์ข้อหนึ่งที่องค์กรต้องบริหารจัดการให้สอดคล้องกับระบบความมั่นคงปลอดภัยของสารสนเทศ ซึ่งตรงกับมาตรการควบคุมข้อ **A7 Human Resource Security** โดยครอบคลุมเป็น 3 ประเด็น ได้แก่

A7.1 Prior to employment: ก่อนที่จะจ้างงาน

- การเลือกคนเข้าทำงาน เรื่องนี้สำคัญไม่แพ้เรื่องอื่น เพราะหลายกรณีเกิดปัญหาจากคนทำงานนี่แหละ ไม่ว่าจะเป็นกรณีจอมแฉบันลือโลก Edward Snowden ที่เอาความลับของหน่วยงานมาเผยแพร่ เล่นเอาป่วนไปทั่วโลก

ISO/IEC 27001:2013 - A7 Human Resource Security
มาตรการควบคุมบริหารจัดการคน (ต่อ)

A7.2 During employment: ระหว่างที่ยังเป็นพนักงาน

- องค์กรต้องกำกับดูแลและมีแนวทางที่ชัดเจนให้พนักงานและผู้รับจ้างช่วง (Contractors) มีความตระหนักและมีความรับผิดชอบในหน้าที่ของตน **ความตระหนักด้าน Information Security** เป็นอะไรที่ต้องรณรงค์กันอย่างต่อเนื่อง เรียกว่าปลูกฝังให้ขึ้นใจได้ยิ่งดี เข้าทำนองกันไว้ดีกว่าแก้ คือ ถ้าพนักงานมีความตระหนักก็จะไม่ทำอะไรที่เสี่ยง ปัญหาก็จะลดน้อยลง

ISO/IEC 27001:2013 - A7 Human Resource Security
มาตรการควบคุมบริหารจัดการคน (ต่อ)

A7.3 Termination and change of employment: ลาออกหรือโอนย้าย

- หลายองค์กรมีการจัดการกรณีพนักงานลาออกเป็นระเบียบปฏิบัติชัดเจน เริ่มตั้งแต่การเรียกคืนทรัพย์สินขององค์กรเช่น Notebook, External Harddisk จากนั้นก็แจ้งไอทีระงับสิทธิการเข้าระบบสารสนเทศภายในช่วงเวลาที่กำหนด มาตรการควบคุมเหล่านี้ช่วยป้องกันปัญหาข้อมูลรั่วไหล
- กรณีโอนย้าย ไม่ว่าจะเป็นย้ายระดับใด ก็ควรทบทวนสิทธิการเข้าถึงระบบสารสนเทศให้เหมาะสมกับภาระหน้าที่และความรับผิดชอบ ส่วนเรื่องทรัพย์สินที่องค์กรมอบให้ไว้ใช้งานก็เช่นกัน ควรทบทวนว่าตำแหน่งใหม่จำเป็นต้องใช้ทรัพย์สินเหล่านั้นหรือไม่ การทำเช่นนี้จะช่วยให้มั่นใจได้ว่าผู้ปฏิบัติงานมีสิทธิเข้าถึงระบบงานที่เหมาะสมกับหน้าที่ และมีอุปกรณ์ที่เหมาะสมกับการทำงานนั้น ๆ

Physical Access Control กับความมั่นคงปลอดภัยตาม ISO/IEC 27001:2013

- การติดตั้ง **ระบบควบคุมการเข้าถึงทางกายภาพ** หรือ Physical Access Control นั้น ได้รับความนิยมอย่างแพร่หลายเป็นอย่างมากในปัจจุบัน ทั้งในอาคารสำนักงาน ตึกคอนโดมีเนียม และบ้านพักอาศัย อีกทั้งยังมีให้เลือกใช้งานกันอยู่หลากหลายรูปแบบ ซึ่งเจ้าของสถานที่หรือผู้บริหารองค์กรจะต้องพิจารณาเลือกใช้งานอย่างรอบคอบและเหมาะสมกับสภาพแวดล้อมและเงื่อนไขของตนเอง โดยคำนึงถึงความเสี่ยงและความมั่นคงปลอดภัยเป็นหลัก

 http://destinationonecounselor.blogspot.com/2015/03/physical-access-control-ISO -270012013.html

10 สิ่งสำคัญที่ต้องพิจารณาในการบริหารจัดการระบบ Access Control (ต่อ)

1. **ตำแหน่งที่ติดตั้ง** เป็นจุดเริ่มต้นที่สำคัญในการบริหารจัดการระบบ Physical Access Control การตัดสินใจเลือกตำแหน่งที่ติดตั้งอย่างถูกต้องเหมาะสมจะช่วยเพิ่มประสิทธิภาพในการจัดการ และเสริมความมั่นคงปลอดภัยมากยิ่งขึ้น
2. **ประเภท** การเลือกประเภทของระบบ Physical Access Control นั้น จะต้องพิจารณาตามความเสี่ยงของพื้นที่ และความเหมาะสมในการใช้งาน อาทิ การใช้บัตร Smart Card, การสแกนลายนิ้วมือ, การสแกนรูม่านตา เป็นต้น
3. **การกำหนดสิทธิ์การเข้าถึงพื้นที่** พนักงานทุกคนไม่สมควรได้รับสิทธิ์ในการเข้าถึงพื้นที่ที่ไม่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของตนเอง ดังนั้น เพื่อให้สอดคล้องตามมาตรการด้านความมั่นคงปลอดภัย เจ้าของพื้นที่จึงควรจะมีการจำกัดสิทธิ์การเข้าถึงให้เฉพาะผู้ที่จำเป็นเท่านั้น

10 สิ่งสำคัญที่ต้องพิจารณาในการบริหารจัดการระบบ Access Control (ต่อ)

4. **ระยะเวลาการจัดเก็บข้อมูล** จำเป็นต้องมีการเก็บบันทึกข้อมูลการผ่านเข้าออกไว้อย่างน้อยเป็นระยะเวลา 90 วัน หรือพิจารณาให้สอดคล้องกับวัตถุประสงค์และความต้องการด้านความมั่นคงปลอดภัยขององค์กรเป็นหลัก
5. **การตั้งค่าเวลา** เวลาของระบบ Access Control นั้น จะต้องได้รับการตั้งค่าตามหน่วยเวลามาตรฐานสากล รวมถึงสอดคล้องกับระบบอื่นๆ ที่เกี่ยวข้อง เพื่อให้สามารถอ้างอิงและตรวจสอบได้หากมีการสืบสวนเกิดขึ้น และจะต้องได้รับการทบทวนความเที่ยงตรงของค่าเวลาอย่างสม่ำเสมอ
6. **การเฝ้าระวัง** การติดตั้งระบบ Access Control นั้นจะไม่เกิดประโยชน์อย่างใดเลยหากขาดการเฝ้าระวัง และจะต้องมีการกำหนดขั้นตอนการปฏิบัติงานอย่างเหมาะสม เช่น หากพบตรวจพบความผิดปกติจะต้องแจ้งไปยังใคร ผ่านทางช่องทางใด วิธีการแจ้งเป็นอย่างไร เป็นต้น

10 สิ่งสำคัญที่ต้องพิจารณาในการบริหารจัดการระบบ Access Control (ต่อ)

7. **พนักงาน** จะต้องมีการตระหนักรู้และมีความตื่นตัวด้านความมั่นคงปลอดภัยอยู่ตลอดระยะเวลาในการปฏิบัติงาน และจะต้องหมั่นสังเกต ตั้งข้อสงสัยอยู่เสมอ เพื่อตรวจหาความผิดปกติ
8. **การสำรองข้อมูล** แนวทางในการสำรองข้อมูลนั้นจะขึ้นอยู่กับความจำเป็นและความเสี่ยงของแต่ละพื้นที่ และจะต้องมีการกำหนดขั้นตอนในการสำรองข้อมูล เช่น ประเภทของสื่อบันทึกข้อมูล ระยะเวลาการจัดเก็บข้อมูลสำรอง การดูแลรักษาข้อมูลสำรอง ฯลฯ อย่างมั่นคงปลอดภัยอีกด้วย

10 สิ่งสำคัญที่ต้องพิจารณาในการบริหารจัดการระบบ Access Control (ต่อ)

9. **โปรแกรม/ซอฟต์แวร์** ที่ใช้เพื่อจัดการระบบ Access Control นั้น จะต้องใช้งานได้ง่ายและมีความมั่นคงปลอดภัย โดยจะต้องผ่านการตรวจหาจุดอ่อนและช่องโหว่อย่างสม่ำเสมอ และจะต้องมีการจัดการผู้ใช้งาน, รหัสผ่าน รวมถึงมีการทบทวนประวัติการเข้าใช้งานอย่างรอบคอบเหมาะสม
10. **สัญญาการให้บริการ** องค์กรจะต้องมีการกำหนดข้อตกลงในสัญญาการให้บริการของผู้ให้บริการภายนอกที่ดูแลอุปกรณ์และระบบ Access Control อย่างเหมาะสม เช่น มีการกำหนดรอบระยะเวลาการบำรุงรักษา เงื่อนไขการแก้ปัญหาหากระบบเกิดการหยุดชะงัก เป็นต้น โดยจะต้องคำถึงความต้องการด้านความมั่นคงปลอดภัยเป็นสำคัญเสมอ

การบริหารจัดการระบบ CCTV อย่างมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001:2013

- ในปัจจุบันมีการใช้งานระบบ CCTV เพื่อเพิ่มความมั่นคงปลอดภัยตามสถานที่ต่าง ๆ ทั้งสถานที่ราชการ สำนักงานเอกชน ร้านค้า รวมถึงที่พักอาศัย ซึ่งระบบ CCTV เองนั้นก็มีความหลากหลายแตกต่างกันไป ดังนั้น ผู้บริหารขององค์กรหรือเจ้าของสถานที่จึงจำเป็นที่จะต้องพิจารณาเลือกติดตั้ง CCTV ชนิดที่มีความเหมาะสมกับสภาพแวดล้อมและเงื่อนไขของตนเอง
- ข้อมูลที่น่าสนใจเพื่อประกอบการบริหารจัดการระบบ CCTV ของเราให้มีความมั่นคงปลอดภัย และสอดคล้องตามมาตรฐาน ISO/IEC 27001:2013 มีดังต่อไปนี้

http://destinationonecounselor.blogspot.com/2015/03/cctv-ISO -270012013.html

12 สิ่งที่ต้องให้ความสำคัญเมื่อมีการติดตั้งระบบ CCTV

1. **ตำแหน่งที่ติดตั้งกล้อง** เป็นสิ่งแรกสุดที่เราต้องพิจารณาให้ความสำคัญ เพราะตำแหน่งการติดตั้งที่ถูกต้องจะช่วยให้เราสามารถบันทึกภาพได้อย่างมีประสิทธิภาพ
2. **ประเภทของกล้อง** ควรเลือกให้เหมาะสมตามระดับความเสี่ยงของพื้นที่ เช่น กล้องปกติ, กล้องที่มีเซ็นเซอร์จับการเคลื่อนไหว, กล้องแบบที่ถูกดัดแปลงรูปลักษณ์ไม่ให้ทราบว่าเป็นกล้อง เป็นต้น
3. **ความละเอียดและความคมชัด** จะต้องเลือกให้สัมพันธ์กับระดับความเสี่ยงของพื้นที่
4. **มุมมองของกล้อง** จะต้องกำหนดว่าในพื้นที่บริเวณนั้น จำเป็นจะต้องจับภาพเป็นมุมกว้างเท่าไร ถ้าหากมุมมองของกล้องยังไม่ครอบคลุมพื้นที่ อาจจะต้องพิจารณาเพิ่มจำนวนกล้องที่ติดตั้ง

12 สิ่งที่ต้องให้ความสำคัญเมื่อมีการติดตั้งระบบ CCTV (ต่อ)

5. **ระยะเวลาการจัดเก็บข้อมูลภาพ** ควรจะจัดเก็บข้อมูลเอาไว้อย่างน้อยไม่ต่ำกว่า 90 วัน หรือสอดคล้องตามงบประมาณขององค์กร
6. **การตั้งค่าเวลา** ควรจะตั้งค่าเวลาของกล้องให้สอดคล้องตามเวลาสากล รวมถึงตรวจสอบค่าเวลาของทุกระบบขององค์กรให้ถูกต้องตรงกันอีกด้วย
7. **การควบคุมการเข้าถึง** ต้องมีการควบคุม และตรวจสอบผู้ที่ต้องการเข้าถึงหรือใช้งานระบบอย่างเข้มงวด เพื่อปกป้องความถูกต้องของข้อมูลภาพที่ระบบ CCTV บันทึกไว้
8. **การตรวจสอบและเฝ้าระวัง** ข้อมูลภาพที่บันทึกไว้นั้นจะไม่มีประโยชน์ใดๆ เลย หากไม่มีการตรวจสอบและเฝ้าระวังสิ่งผิดปกติอย่างเหมาะสม ดังนั้น จึงควรจะมีการกำหนดขั้นตอนการปฏิบัติงานอย่างชัดเจน

12 สิ่งที่ต้องให้ความสำคัญเมื่อมีการติดตั้งระบบ CCTV (ต่อ)

9. **การสำรองข้อมูล** จะต้องมีการพิจารณาวิธีการสำรองข้อมูล ระยะเวลาการเก็บบันทึกข้อมูลสำรอง อย่างเหมาะสมตามระดับความเสี่ยง และจะต้องมีการตรวจสอบความถูกต้องและความพร้อมใช้งานของข้อมูลสำรองตามรอบระยะเวลาเพื่อความมั่นใจอีกด้วย
10. **ซอฟต์แวร์หรือระบบบริหารจัดการ** จะต้องได้รับการพิจารณาว่าสามารถใช้งานได้ง่ายหรือไม่ สามารถตั้งค่าให้เหมาะสมกับการใช้งานได้หรือเปล่า และมีจุดอ่อนหรือช่องโหว่ใดๆ หรือไม่
11. **บุคลากร** จะต้องมีทักษะความรู้และมีความตื่นตัวเกี่ยวกับความมั่นคงปลอดภัยอยู่ตลอดเวลา และต้องหมั่นสังเกตหรือตั้งข้อสงสัยอยู่เสมอ
12. **สัญญาการให้บริการ** องค์กรจะต้องกำหนดข้อตกลงในการให้บริการของผู้ให้บริการภายนอกอย่างชัดเจน เช่น กำหนดรอบระยะเวลาบำรุงรักษา การจัดหาอุปกรณ์สำรอง เป็นต้น

หลากหลายคำถามที่องค์กรต้องตอบเพื่อป้องกันปัญหา “ข้อมูลรั่วไหล”

- ในปัจจุบัน **“ข้อมูลรั่วไหล”** กลายเป็นปัญหาพื้นฐานที่ทุกองค์กรต้องเผชิญ ไม่ว่าจะเป็นองค์กรขนาดเล็กหรือขนาดใหญ่ แม้ว่าจะมีการจัดซื้อหรือใช้งานเทคโนโลยีที่ทันสมัยและเข้มแข็งมากสักเพียงใด ก็ยังคงไม่สามารถหลีกเลี่ยงความเสี่ยงของการรั่วไหลของข้อมูลได้ เพราะสาเหตุอาจจะเกิดจากความพยายามโจมตีจากผู้มุ่งร้าย การทำงานที่ประมาทเลินเล่อของบุคลากร ฯลฯ ซึ่งล้วนแต่นำมาซึ่งผลเสียหาย
- ดังนั้น แนวทางการแก้ปัญหาข้อมูลรั่วไหลที่ดีที่สุด ก็คือการป้องกันการเกิดเหตุ และการลดผลกระทบที่อาจจะเกิดขึ้นจากเหตุนั้น - จึงนำเสนอ **“รายการคำถาม”** เพื่อให้ผู้บริหารของทุกองค์กรได้พิจารณา คำถามเหล่านี้จะช่วยให้เราได้ทบทวนการดำเนินการและการปฏิบัติงานต่าง ๆ ในระหว่างค้นหาคำตอบ ซึ่งจะเป็นประโยชน์ต่อการวางแผนพัฒนาและปรับปรุงต่อไป

http://destinationonecounselor.blogspot.com/2015/03/blog-post.html

คำถามที่องค์กรต้องตอบเพื่อเป็นการป้องกันหรือเตรียมการในการรับมือปัญหา “ข้อมูลรั่วไหล (ต่อ)

คำถามที่องค์กรต้องตอบเพื่อเป็นการป้องกันหรือเตรียมการในการรับมือปัญหา “ข้อมูลรั่วไหล” (ต่อ)

- องค์กรมีการจัดลำดับชั้นความลับอย่างไร
- องค์กรกำหนดวิธีในการดูแลรักษาและการใช้งานข้อมูลตามชั้นความลับอย่างไร
- องค์กรมีการควบคุมการเข้าถึงอย่างไร
- องค์กรมีมาตรฐานรหัสผ่านอย่างไร
- องค์กรมีนโยบายการนำข้อมูลหรือทรัพย์สินเข้าออกพื้นที่อย่างไร
- องค์กรมีการควบคุมการเข้าถึงพื้นที่ทางกายภาพอย่างไร
- องค์กรมีการติดตั้งระบบกล้องวงจรปิดอย่างไร
- องค์กรมีการมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศอะไรบ้าง
- องค์กรมีการกำหนดกฎระเบียบการใช้งานทรัพย์สินแต่ละประเภทอย่างไร
- องค์กรมีการควบคุมการใช้งานสื่อบันทึกข้อมูลอย่างไร
- องค์กรมีการทำลายข้อมูลอย่างมั่นคงปลอดภัยอย่างไร

คำถามที่องค์กรต้องตอบเพื่อเป็นการป้องกันหรือเตรียมการในการรับมือปัญหา “ข้อมูลรั่วไหล” (ต่อ)

- องค์กรมีการเข้ารหัสข้อมูลสำคัญอย่างไร
- องค์กรมีการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยอย่างไร
- องค์กรมีการบริหารจัดการเหตุละเมิดความมั่นคงปลอดภัยอย่างไร
- องค์กรมีการบริหารจัดการการเปลี่ยนแปลงอย่างไร
- องค์กรมีการทบทวนประวัติการเข้าถึง ประวัติการใช้งานระบบและเหตุการณ์ต่างๆ ทางด้านความมั่นคงปลอดภัยอย่างไร
- องค์กรมีวิธีการในการคัดเลือกหรือตรวจสอบประวัติของพนักงานอย่างไร
- องค์กรมีการให้พนักงานลงนามในเอกสารสัญญาการรักษาความลับของข้อมูลอย่างไร
- องค์กรมีการสร้างความตระหนักรู้และให้ความรู้ทางด้านความมั่นคงปลอดภัยอย่างไร
- องค์กรมีบทลงโทษในกรณีมีการละเมิดความมั่นคงปลอดภัยอย่างไร

การตั้งคำถามเป็นจุดเริ่มต้นของการพัฒนาปรับปรุงที่ดีเสมอ!!

การควบคุมความมั่นคงของข้อมูล และการวัดประสิทธิผลตามข้อกำหนดของมาตรฐาน ISO/IEC 27001

- การควบคุมความมั่นคงของข้อมูลนั้นจำเป็นต้องใช้ทรัพยากรในการดำเนินการ ผู้บริหารขององค์กรย่อมคาดหวังให้วิธีการควบคุมนั้นได้ผลตามวัตถุประสงค์ และคุ้มค่ากับงบประมาณที่ได้ลงทุนไป ยกตัวอย่างเช่น การติดตั้งโปแกรมป้องกันไวรัสต้องสามารถลดอัตราความเสี่ยงที่ข้อมูลสำคัญในเครื่องคอมพิวเตอร์จะถูกโจมตีจากไวรัสต่าง ๆ โดยมีค่าบำรุงรักษาและค่าลิขสิทธิ์ของโปรแกรมอยู่ภายในงบประมาณที่ได้กำหนดไว้
- ฉะนั้น เพื่อให้ทราบว่าวิธีการควบคุมความมั่นคงของข้อมูลต่าง ๆ ที่องค์กรนำมาใช้นั้นบรรลุตามวัตถุประสงค์ และความคาดหวังหรือไม่ องค์กรจึงต้องมีการนำเครื่องมืออย่างหนึ่งมาใช้ ซึ่งก็คือ “การวัดประสิทธิผลของการควบคุมความมั่นคงของข้อมูล” (Effectiveness Measurement) นั่นเอง

http://www.acinfotec.com/2008/08/14/การควบคุมความมั่นคงของ

การควบคุมความมั่นคงของข้อมูล และการวัดประสิทธิผลตามข้อกำหนดของมาตรฐาน ISO/IEC 27001 (ต่อ)

- การวัดมีจุดประสงค์เพื่อให้ได้ผลที่มีความถูกต้องแม่นยำ และสามารถนำมาใช้ในการเปรียบเทียบได้
- ดังนั้น การวัดที่ดีจึงต้องมีการอ้างอิงกับมาตรฐานอย่างหนึ่งอย่างใดเสมอ ยกตัวอย่างเช่น การวัดความยาวโดยอ้างอิงมาตรฐานระบบเมตริก
- นอกจากนี้ ยังต้องนำวิธีการ และเครื่องมือสำหรับการวัดที่เหมาะสมมาใช้งานอีกด้วย เช่น การใช้ไม้บรรทัดวัดความยาวที่ต้องการความแม่นยำในระดับเซนติเมตร หรือใช้เวอร์เนียวัดความยาวเมื่อต้องการความแม่นยำในระดับมิลลิเมตร เป็นต้น
- ในทำนองเดียวกัน การวัดประสิทธิผลของวิธีการควบคุมความมั่นคงของข้อมูลก็อาศัยหลักการดังกล่าวข้างต้น และได้รับการบรรจุให้เป็นหนึ่งในข้อกำหนดของมาตรฐาน ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems – Requirements

การควบคุมความมั่นคงของข้อมูล และการวัดประสิทธิผลตามข้อกำหนดของมาตรฐาน ISO/IEC 27001 (ต่อ)

- องค์กรจำเป็นต้องกำหนดตัววัด (Metric) สำหรับแต่ละวิธีการควบคุมที่ต้องการวัดประสิทธิผล เพื่อให้การวัดประสิทธิผลมีความถูกต้องแม่นยำ และได้ผลลัพธ์ที่ตรงกันไม่ว่าการวัดนั้นได้รับการดำเนินการโดยผู้ใดก็ตาม โดยตัววัดจะต้องประกอบไปด้วย 3 ส่วนหลัก ดังนี้

1. รายละเอียดของวิธีการควบคุมความมั่นคงของข้อมูลที่ต้องการวัดประสิทธิผล เป็นการระบุรายละเอียดที่จำเป็นเกี่ยวกับวิธีการควบคุมที่องค์กรต้องการวัดประสิทธิผล เช่น ชื่อวิธีการควบคุม วัตถุประสงค์ และขอบเขตของการวัดผลประสิทธิผล เป็นต้น
2. รายละเอียดของวิธีการที่ใช้ในการวัดประสิทธิผล เป็นการระบุรายรายละเอียดที่จำเป็นเกี่ยวกับวิธีการที่องค์กรนำมาใช้ในการวัดประสิทธิผล เช่น แหล่งข้อมูลที่จะนำมาใช้ วิธีการรวบรวมข้อมูล ตารางเวลาที่จะทำการวัดประสิทธิผล ผู้รับผิดชอบ และวิธีการประมวลผลข้อมูล เป็นต้น

การควบคุมความมั่นคงของข้อมูล และการวัดประสิทธิผลตามข้อกำหนดของมาตรฐาน ISO/IEC 27001 (ต่อ)

3. การตั้งเป้าหมาย เป็นการกำหนดระดับของผลการวัด เพื่อใช้เป็นตัวชี้วัดว่าวิธีการควบคุมความมั่นคงของข้อมูลนั้นบรรลุตามวัตถุประสงค์หรือไม่ เช่น การวัดประสิทธิผลของการฝึกอบรมด้วยการทดสอบความรู้ความเข้าใจของพนักงาน หากได้คะแนนเฉลี่ยมากกว่าเป้าหมายที่ 80% หมายถึง การฝึกอบรมนั้นบรรลุตามวัตถุประสงค์ หรือ การวัดด้วยจำนวนชั่วโมงของการฝึกอบรมด้านความมั่นคงของข้อมูล โดยในปีแรกกำหนดเป้าหมายเป็น 10 ชั่วโมง/คน/ปี และปีที่สองกำหนดเป็น 15 ชั่วโมง/คน/ปี หากผลการวัดเป็นไปตามเป้าหมายนี้ ถือว่าการวางแผนและการจัดฝึกอบรมนั้นบรรลุตามวัตถุประสงค์

การควบคุมความมั่นคงของข้อมูล และการวัดประสิทธิผลตามข้อกำหนดของมาตรฐาน ISO/IEC 27001 (ต่อ)

- การกำหนดตัววัดประสิทธิผลของการควบคุมความมั่นคงของข้อมูลนั้น ต้องได้รับการพิจารณาอย่างรอบคอบโดยผู้เกี่ยวข้องแต่ละฝ่ายภายในองค์กรอย่างเหมาะสม เพื่อให้ตัววัดนั้นสามารถสะท้อนให้เห็นประสิทธิผลของวิธีการควบคุมความมั่นของข้อมูลได้อย่างแท้จริง โดยต้องระมัดระวังไม่ให้วิธีการวัดสลับซับซ้อนจนเกินไป และไม่กำหนดเป้าหมายสูง หรือต่ำจนเกินไป ฯลฯ อันเป็นปัญหาที่พบบ่อยครั้งในการกำหนดรายละเอียดของตัววัด

การควบคุมความมั่นคงของข้อมูล และการวัดประสิทธิผลตามข้อกำหนดของมาตรฐาน ISO/IEC 27001 (ต่อ)

- การวัดประสิทธิผลของการควบคุมความมั่นคงของข้อมูลมีประโยชน์หลายประการ เช่น การแสดงให้เห็นถึงประสิทธิผลของวิธีการควบคุมความมั่นคงของข้อมูลว่าเป็นไปตามที่ต้องการหรือไม่
- การแสดงให้เห็นถึงแนวโน้มการพัฒนาของวิธีการควบคุมความมั่นคงของข้อมูลว่าดีขึ้นหรือด้อยลงเมื่อเปรียบเทียบผลการวัดในแต่ละช่วงเวลา ซึ่งผู้บริหารสามารถนำมาใช้เป็นข้อมูลประกอบการตัดสินใจในการจัดสรรงบประมาณ และทรัพยากรสนับสนุนสำหรับแต่ละส่วนงานได้อย่างเหมาะสม
- นอกจากนี้ ผลการวัดยังสามารถยืนยันได้ว่า องค์กรมีการควบคุมความมั่นคงของข้อมูลในระดับที่ดี และมีการวัดประสิทธิผลเพื่อการปรับปรุงอยู่อย่างสม่ำเสมอ

9.9 บทสรุป

- ISO/IEC27001 (Information Security Management System: ISMS) เป็นมาตรฐานการจัดการข้อมูลที่มีความสำคัญเพื่อให้ธุรกิจดำเนินไปอย่างต่อเนื่อง ซึ่งข้อกำหนดต่าง ๆ กำหนดขึ้นโดยองค์กรที่มีชื่อเสียงและมีความน่าเชื่อถือระหว่างประเทศ คือ ISO/IEC (The International Electrotechnical Commission)
- ในการจัดทำระบบบริหารจัดการ (Management System) จะต้องพิจารณาหลายด้านที่มีความเกี่ยวข้อง
  - การบริหารคน (ภายในองค์กรและภายนอก เช่น Outsource)
  - กระบวนการและเทคโนโลยี (เข้าใจกระบวนการทำงาน และเทคโนโลยีที่เหมาะสมในการนำมาใช้งาน)
  - บริหารงบประมาณ (การลงทุนที่คุ้มค่า)

9.9 บทสรุป (ต่อ)

- ซึ่งเราต้องเข้าใจทั้ง 3 ด้านข้างต้น เพื่อที่จะหาจุดสมดุลและเกิดประโยชน์สูงสุด อย่างไรก็ตามเมื่อลงมือทำจริงมันมีอะไรเต็มไปหมดที่ต้องทำความเข้าใจ จะได้วางแนวทางปฏิบัติให้เหมาะสม ซึ่งเนื้อหาในบทนี้ได้กล่าวในประเด็นต่าง ๆ ที่จำเป็นซึ่งสามารถใช้เป็นแนวทางในการปฏิบัติงานได้

Assignment

- **Can ISO 27001 help protect your organization from cyber attack? – A Hacker's view on ISO 27001 standard?**
- http://www.acinfotec.com/2014/12/11/can-iso-27001-help-protect-your-organization-from-cyber-attack-a-hackers-view-on-iso-27001-standard/

เอกสารอ้างอิง

- รีวิว ISO/IEC 27001: 2013 - ตอนที่1 พื้นฐานความมั่นคงปลอดภัยของสารสนเทศ, Pryn Sereepong, 14 มกราคม พ.ศ. 2557 http://www.club27001.com/2014/01/review-ISO/IEC 27001 -2013-part1.html
- รีวิว ISO/IEC 27001:2013 - ตอนที่2 ความสำคัญของการประเมินความเสี่ยงสารสนเทศ, Pryn Sereepong, 20 มกราคม พ.ศ. 2557 http://www.club27001.com/2014/01/ISO/IEC 27001 -2013-Information-Risk-Assessment.html
- Overview ข้อกำหนด ISO/IEC 27001:2013 ตอนที่ 1, Pryn Sereepong, 3 กุมภาพันธ์ พ.ศ. 2557 http://www.club27001.com/2014/02/27001-2013-requirement-overview-part1.html
- Overview ข้อกำหนด ISO/IEC 27001:2013 ตอนที่2 (จบ), Pryn Sereepong, 5 กุมภาพันธ์ พ.ศ. 2557 http://www.club27001.com/2014/02/ISO -27001-Requirement-overview-part2.html
- บันได 4 ขั้นสู่มาตรฐาน ISO/IEC 27001 Information Security Managment, Pryn Sereepong, 25 สิงหาคม พ.ศ. 2556 http://www.club27001.com/2013/08/4-ISO iec-27001.html
- แนวทางการทำแผนจัดการความเสี่ยง ISO/IEC 27001 (Risk Treatment Plan), Pryn Sereepong, 11 เมษายน พ.ศ. 2557 http://www.club27001.com/2014/04/risk-treatment-plan.html
- มาตรการ (Control) จัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001: 2013, Pryn Sereepong, 9 กุมภาพันธ์ พ.ศ. 2557 http://www.club27001.com/2014/02/ISO -27001-2013-Controls-requirement.html

เอกสารอ้างอิง (ต่อ)

- 10 ประเด็นน่ารู้เกี่ยวกับคณะทำงานระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001:2013, Pryn Sereepong, 12 มิถุนายน พ.ศ. 2557 http://www.club27001.com/2014/06/10-ISO/IEC 27001 2013.html
- แนวทางการทำ ISO/IEC 27001:2013 Project Master Plan, Pryn Sereepong, 3 สิงหาคม พ.ศ. 2557 http://www.club27001.com/2014/08/ISO/IEC 27001 -2013-project-master-plan.html
- 7 ขั้นตอนการทำ ISO/IEC 27001:2013 Gap Analysis, Pryn Sereepong, 27 พฤศจิกายน พ.ศ. 2557 http://www.club27001.com/2014/11/7-steps-to-ISO -27001-2013-Gap-Analysis.html
- เล่าสู่กันฟัง Key Success Factors เบื้องหลังการทำระบบ ISO/IEC 27001ให้สำเร็จจากประสบการณ์จริง, Pryn Sereepong, 11 กุมภาพันธ์ พ.ศ. 2557 http://www.club27001.com/2014/02/iso27001-2013-key-success-factors.html
- รู้จัก ISO/IEC 27001 มาตรฐานระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ, Pryn Sereepong, 7 สิงหาคม พ.ศ. 2556 http://www.club27001.com/2013/08/ISO iec-27001.html
- http://www.british-assessment.co.uk/articles/isos-annex-sl-explained
- http://www.share4shine.com/ISO/IEC 27001 /Document2.pdf
- http://www.isosmartpro.com/private_folder/ISO _new_vesion/Annex_SL_by_ISO_Smart_PRO.pdf
- http://www.slideshare.net/LRQA_Nederland/webinar-veranderingen-en-impact-ISO -27001-informatiebeveiliging

เอกสารอ้างอิง (ต่อ)

- องค์ประกอบของความมั่นคงปลอดภัยของสารสนเทศ, Pryn Sereepong, 10 สิงหาคม พ.ศ. 2556 http://www.club27001.com/2013/08/normal-0-false-false-false-en-us-x-none.html
- 4 เคล็ดลับการเตรียมตัวสำหรับผู้ตรวจประเมินภายใน ISO/IEC 27001 Internal Auditor, Pryn Sereepong, 16 ธันวาคม พ.ศ. 2557 http://www.club27001.com/2014/12/4-secrets-of-ISO -27001-internal-auditor.html
- 7 ขั้นตอนวางแผนตรวจประเมินภายใน(Internal Audit) ISO/IEC 27001:2013, Pryn Sereepong, 11 ธันวาคม พ.ศ. 2557 http://www.club27001.com/2014/12/7-Steps-to-planning-ISO -27001-2013-Audit-Plan.html
- ISO/IEC 27001:2013 Human Resource Security - กรณีศึกษา ICANN โดยHacker ล้วงตับ, Pryn Sereepong, 23 ธันวาคม พ.ศ. 2557 http://www.club27001.com/2014/12/ISO -27001-2013-icann-hacked-Human-resource-security.html
- ISO/IEC 27001:2013 - A7 Human Resource Security มาตรการบริหารจัดการคน, Pryn Sereepong, 22 มกราคม พ.ศ. 2558 http://www.club27001.com/2015/01/ISO -27001-2013-human-resource-security.html
- ISO/IEC 27001:2013 An Overview, Securitykaizen Magazine Best Practice, Ahmed Riad, www.bluekaizen.org
- http://pannoppamad.blogspot.com/2014/01/ISO -27001-information-security.html
- http://www.ISO/IEC 27001 standard.com/webinar/ISO -27001-an-overview-of-isms-implementation-process-free-webinar/

เอกสารอ้างอิง (ต่อ)

- http://www.iso27001standard.com/free-downloads/
- http://www.iso27001.info/news-articles/resources/a-12-step-process-for-planning-your-transition-fro.aspx
- http://www.netgrowthltd.co.uk/ISO/IEC 27001 .aspx
- http://www.itnews24hrs.com/2014/04/ISO-270001-isms/
- http://ovthai.miss.in.th/2014/02/09/54321/
- http://www.acinfotec.com/2006/10/06/risk-management-the-key-process-for-ISO -27001-implementation/
- https://www.acisonline.net/?p=1771&lang=th
- http://www.acinfotec.com/2008/09/11/overview-of-ISO -27001-and-ISO -27002-the-international-standards-for-information-security-management-part-i/
- http://www.isotoyou.com/index.php/article/447-ISO/IEC 27001-dis-what-change.html
- http://www.itnews24hrs.com/2014/04/ISO -270001-isms/
- http://ovthai.miss.in.th/2014/02/09/54321/
- http://www.acinfotec.com/2006/10/06/risk-management-the-key-process-for-ISO -27001-implementation/
- https://www.acisonline.net/?p=1771&lang=th