เรียนรู้มาตรฐาน ISO 27001 :2013 การจัดการความมั่นคงปลอดภัยของสารสนเทศแบบง่ายๆ

เราชาวมหิดลทราบหรือไม่ว่าปัจจุบันนี้องค์กรของเรามีระบบงานสารสนเทศที่สำคัญหลายๆ ระบบ ซึ่งเป็นระบบงานหลักขององค์กร เช่น ระบบสารสนเทศเพื่อการบริหารจัดการ MU-ERP ระบบสารสนเทศทางโรงพยาบาล ระบบสารสนเทศเพื่อการศึกษา ฯลฯ

ลองนึกภาพสมมุติขณะที่เราออกใบเสร็จรับเงิน ปรากฏว่าระบบไอทีล่มไม่สามารถออกใบเสร็จรับเงินได้ ผู้ที่เดือดร้อนอาจจะเป็นนักศึกษา ผู้ปกครอง ผู้มาติดต่อ ผู้บริหารและงานไอทีต้องเร่งแก้ปัญหาเฉพาะหน้าเป็นการด่วน ซึ่งแน่นอนว่าระบบสารสนเทศทุกวันนี้เปรียบเสมือนเส้นเลือดขององค์กร คงไม่ดีแน่ถ้าระบบไอทีล่มบ่อย หรือข้อมูลสูญหาย จะดีกว่ามั้ยถ้ามีระบบอะไรซักอย่างที่ทำให้แน่ใจได้ว่า ระบบข้อมูลสารสนเทศสามารถให้บริการตามปกติ ข้อมูลได้รับการปกป้อง และหากเกิดขัดข้องก็สามารถรับมือและกู้ระบบคืนได้ ระบบที่ว่านี้ก็คือ ISO27001

ดังนั้นการที่จะมั่นใจได้ว่าระบบฯ ของเรามีความมั่นคงปลอดภัย ก็เราจะต้องรู้ว่ามีภัยคุกคามอะไรบ้างที่อาจมาโจมตี ทำให้สารสนเทศของเราเกิดความเสียหาย จากนั้นจึงประเมินความเสี่ยงและกำหนดมาตรการจัดการกับภัยคุกคาม ให้แน่ใจว่าสามารถรับมือภัยคุกคามเหล่านั้นได้อย่างเหมาะสม ทั้งนี้จะขอแนะนำมาตรฐาน ISO27001

ISO27001 มาตรฐานสากลที่ทั่วโลกยอมรับ

องค์กร ISO - International Organization for Standardization เป็นหน่วยงานที่ให้กำเนิดมาตรฐาน ISO27001 โดยเวอร์ชั่นล่าสุดคือ ISO27001:2013 ประกาศเมื่อ 1 ต.ค. 2013 ส่วนเวอร์แรกประกาศใช้ครั้งแรกเมื่อปี 2550 (ISO27001:2005) หลังจากประกาศใช้ก็ได้รับความสนใจจากองค์กรทั้งภาครัฐและเอกชนทั่วโลก นำมาใช้งานและขอการรับรอง (Certification) ประเทศไทยเองก็ไม่แพ้ชาติใดในโลก มีหน่วยงานรัฐและเอกชนเริ่มทำISO27001 และขอการรับรองได้สำเร็จ เช่น บริษัท ไทยออยล์ จำกัด (มหาชน) บริษัท ทรู อินเทอร์เน็ต ดาต้าเซ็นเตอร์ จำกัด(True IDC) และรัฐวิสาหกิจอีกหลายแห่ง องค์กรอย่างเราสามารถทำได้ มาตรฐานนี้ออกแบบมาให้ใช้ได้ประเภทธุรกิจ หน่วยราชการ สถานศึกษา และใช้ได้กับองค์กรทั้งขนาดเล็กและขนาดใหญ่อย่างบริษัทข้ามชาติ

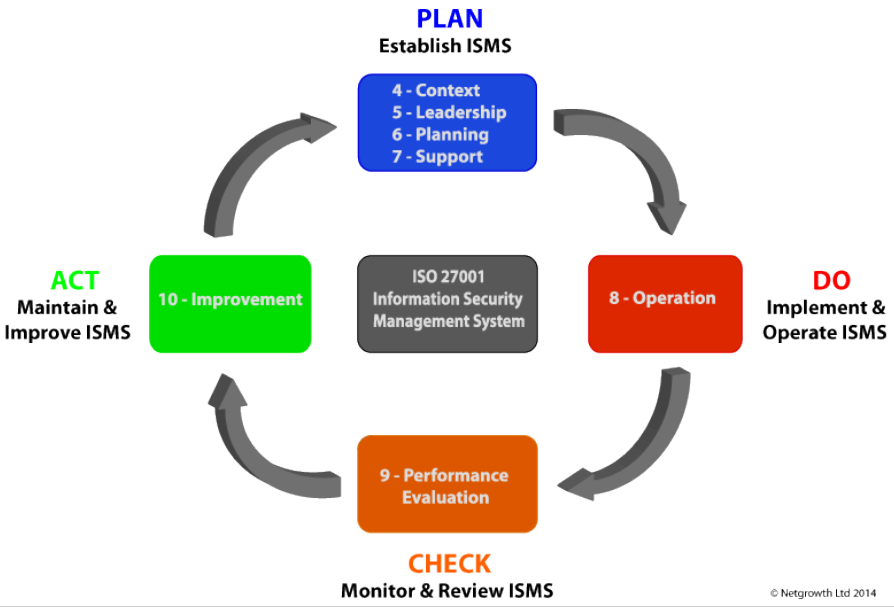
ISO27001 (Information Security Management System-ISMS)

มาตรฐานการจัดการความมั่นคงปลอดภัยของสารสนเทศ พอกล่าวถึงข้อมูลสารสนเทศท่านอาจคิดว่าคงเป็นเรื่องไอทีล้วนๆ ถูกต้องแล้ว แต่ถูกเพียงครึ่งเดียว!! จริงๆ แล้วมีเรื่องอื่นที่ต้องบริหารจัดการเช่นเดียวกัน ทั้งเรื่องคน เรื่องกฎระเบียบขององค์กร เรื่องจัดซื้อจัดจ้าง เรื่องการฝึกอบรมพนักงาน เป็นต้น เหล่านี้ล้วนเกี่ยวข้องกับการบริหารจัดการข้อมูลสารสนเทศให้มั่นคง ปลอดภัย ต่อให้มีระบบไอทีล้ำเลิศแค่ไหน แต่ถ้าไม่มีกฎระเบียบควบคุมที่ชัดเจน ไม่มีการอบรมให้ความรู้ผู้ใช้ และไม่มีการควบคุม Outsource ที่ดีพอ บอกได้เลยว่าองค์กรนี้เหนื่อย !!

ยิ่งองค์กรมีระบบไอทีดีแต่ขาดมาตรการควบคุม พนักงานก็ใช้ทรัพยากรไปกับเรื่องที่ไม่สมควรและหลายคนทำผิดกฎหมาย เช่น พนักงานใช้คอมพิวเตอร์ขององค์กรโหลดหนังและแชร์ไฟล์ที่ละเมิดลิขสิทธิ์ แบบนี้เสี่ยงต่อการโดนจับและเสียหายต่อองค์กรแน่นอน

มาตรฐานนี้ใช้แนวทาง PDCA (Plan-Do-Check-Act) เป็นโครงสร้างเช่นเดียวกับมาตรฐานที่รู้จักกันอย่างแพร่หลาย เช่น ISO 9001(Quality Management System-QMS) ISO14001(Environmental Management System-EMS) ดังนั้นองค์กรที่มีระบบ QMS,EMS อยู่แล้วสามารถเข้าใจแนวทางของ ISMS ได้ไม่ยากนัก เพียงแต่เปลี่ยนมุมมองมาสนใจที่ Information และวางแนวทางบริหารให้เกิดความมั่นคงปลอดภัยโดยผ่านกระบวนการ วางแผน (Plan) นำไปปฏิบัติ(Do) ทบทวนและตรวจสอบ(Check) และแก้ไขปรับปรุง (Act)

จะเห็นได้ว่าหลักการ PCDA สอดคล้องกับสามัญสำนึกทั่วไป คือก่อนทำอะไรควรมีการวางแผนล่วงหน้า พิจารณาให้รอบคอบแล้วลงจึงมือทำตามแผน หลังจากนั้นก็ตรวจสอบผลลัพธ์ว่าเป็นไปตามแผนที่วางไว้หรือไม่ หากไม่เป็นไปตามแผนก็ต้องแก้ไขปรับปรุง และนำบทเรียนมาพิจารณาในการวางแผนก่อนทำงานครั้งต่อไป ซึ่งแนวคิดนี้สามารถประยุกต์ใช้ในการทำมาตรฐาน ISO/IEC 27001 ได้เป็นอย่างดี



การที่องค์กรหนึ่งผ่านการรับรองมาตรฐานระบบการความมั่นคงปลอดภัยของสารสนเทศ ISO 27001 นั้นหมายถึง องค์กรดังกล่าวได้นำข้อกำหนดของมาตรฐาน ISO 27001 มาประยุกต์ใช้อย่างครบถ้วน และมีหลักฐานที่เป็นรูปธรรมให้เชื่อได้ว่าองค์กรดังกล่าวมีระบบการจัดการ ความมั่นคงปลอดภัยของสารสนเทศที่ได้มาตรฐานสากล

การจัดทำระบบบริหารจัดการ(Management System)จะต้องพิจารณาหลายด้านที่มีความเกี่ยวข้อง

- การบริหารคน(ภายในองค์กรและภายนอก เช่น Outsource)
- กระบวนการและเทคโนโลยี (เข้าใจกระบวนการทำงาน และเทคโนโลยีที่เหมาะสมในการนำมาใช้งาน)
- บริหารงบประมาณ (การลงทุนที่คุ้มค่า)

ซึ่งท่านต้องเข้าใจทั้ง 3 ด้านข้างต้น เพื่อที่จะหาจุดสมดุลย์และเกิดประโยชน์สูงสุด อย่างไรก็ตามเมื่อลงมือทำจริงมันมีอะไรเต็มไปหมดที่ต้องทำความเข้าใจ จะได้วางแนวทางปฏิบัติให้เหมาะสม ไม่เข้มงวดเกินไปจนทำอะไรไม่ได้(ปลอดภัยสูงสุด) หรือหลวมเกินไปจนแทบไม่ได้ควบคุมอะไรเลย

ISO27001 ทำยากมั้ย ตอบได้เลยว่าไม่ยาก ถ้ามีความรู้และความเข้าใจ 2 เรื่องใหญ่ๆ คือ

1. เข้าใจองค์กรตนเอง : ต้องสำรวจข้อมูล ซอฟแวร์ ฮาร์ดแวร์ บุคลากร ในขอบเขตที่จัดทำระบบ ข้อมูลนี้ยิ่งมีรายละเอียดยิ่งดี ทะเบียนคุมทรัพย์สินเป็นจุดเริ่มต้นที่ดีในการรวบรวมข้อมูล Hardware ,Software

เข้าใจภาระกิจขององค์กร รู้ว่าระบบงานใดสำคัญที่สุดและระบบงานต่างๆ มีข้อจำกัดและจุดอ่อนอะไรบ้าง เพื่อที่จะไปหามาตรการมาจัดการกำจัดจุดอ่อน เช่น ระบบฐานข้อมูลทำงานอยู่บนเครื่องServer ที่

เก่าแก่มาก เก่าขนาดที่ไม่มี Spare part หาก Server นี้พังไปก็โบกมือลาได้เลยเพราะซ่อมไม่ได้ !! ในกรณีนี้จุดอ่อนก็คือ Server ที่เก่าบุโรทั่ง มีความเสี่ยงที่จะลาโลกไปเมื่อไหร่ก็ได้ ดังนั้นท่านก็ต้องหามาตรการมาจัดการความเสี่ยงนี้ โดยจัดหาเครื่องใหม่ ซึ่งปัจจุบันนิยมใช้เทคโนโลยี Virtualization เข้ามาบริหารจัดการ ทั้งนี้ก็แล้วแต่แนวทางและขีดความสามารถของแต่ละองค์กร

2.เข้าใจมาตรฐาน : จะนำมาตรฐาน ISO27001 มาใช้งาน ก็ต้องทำความเข้าใจในตัวมาตรฐานเสียก่อนว่าต้องทำอะไรบ้าง ทั้งเรื่องเอกสาร(Documents) และการนำไปใช้งานจริง (Implementation) ข้อกำหนดของ ISO27001:2013 ฉบับของ ISO-International Organization for Standardization นั้นเป็นภาษาอังกฤษ

งบประมาณเท่าไหร่ถึงจะพอ

งบประมาณจำเป็นต้องมี แต่ใช้งบประมาณมากหรือน้อยขึ้นอยู่กับสิ่งที่องค์กรยังขาด เช่น ประเมินความเสี่ยงมาแล้วพบว่ายังไม่มีระบบจัดเก็บข้อมูลจราจรทาง คอมพิวเตอร์(log) แบบนี้งานเข้า เพราะผิดกฎหมาย!! จำเป็นต้องจัดหามาโดยด่วน หรือพบว่าเครื่อง Server เก่าบุโรทั่ง มีโอกาสลาโลกไปแบบไม่ฟื้นเมื่อไหร่ก็ได้ แบบนี้จำเป็นต้องมีงบประมาณเพื่อจัดหาใหม่มาทดแทน และที่พบค่อนข้างมากในหลายองค์คือไม่มีมาตรการหรือเครื่องมือเฝ้าระวังตรวจ จับทางด้านความมั่นคงปลอดภัยของสารสนเทศ อันนี้ก็จำเป็นต้องลงทุนจัดหามาใช้งาน และสุดท้ายหากจะขอใบรับรองISO27001ก็ต้องมีค่าตรวจประเมินรับรอง ระบบ(Certification) ซึ่งตรวจประเมินโดยหน่วยงานที่เรียกว่า Certified body

เริ่มต้นยังไงดี

Step1 : ก่อนอื่นท่านต้องกำหนดขอบเขต(Scope)ที่จะทำ ISO27001 หรือพูดอีกอย่างหนึ่งก็คือ ท่านต้องการให้ระบบงานหรือกิจกรรมอะไรบ้างที่ถูกควบคุมดูแลภายใต้ ISO27001 เพื่อให้มั่นใจว่าสารสนเทศของระบบงาน หรือกิจกรรมนั้นๆ มีความมั่นคงปลอดภัย

Step2 : ศึกษามาตรฐาน ISO27001 ให้เข้าใจหลักการพื้นฐานและแนวทางการนำไปใช้งาน

Step3 : ทำการประเมินองค์กรเบื้องต้นให้รู้ว่าองค์กรยังขาดอะไรบ้างเมื่อเทียบกับ สิ่งที่ต้องมีตามมาตรฐานISO27001 ขั้นตอนนี้ท่านจะต้องมีความรู้ในข้อกำหนดของ ISO27001 พอสมควร ถึงจะประเมินได้ว่าข้อไหนมีแล้วข้อไหนยังขาด

สำหรับการเริ่มต้นมี 3 step ข้างต้น หลังจากการประเมินองค์กรเบื้องต้นใน Step3 ท่านก็จะรู้ว่ายังขาดอะไรบ้าง มีประเด็นอะไรที่ยังไม่สอดคล้องตามกฎหมายหรือไม่ ถ้ามีก็ให้สรุปประเด็นเสนอผู้บริหารเพื่อเร่งดำเนินการ

การนำมาตรฐานISO27001มาใช้งาน มี4 องค์ประกอบใหญ่คือ

- จัดทำระบบ(Establish) การจัดการความมั่นคงปลอดภัยของ สารสนเทศ(Information Security Management System -ISMS) คือ การเตรียมการ วางแผนเพื่อปกป้องสารสนเทศ
- นำไปปฏิบัติ(Implement) คือ นำแผนจากขั้นตอนการจัดทำระบบ(Establish) ไปปฏิบัติจริงหน้างานทำตามเอกสารคู่มือและลงบันทึกในแบบฟอร์ม
- รักษาไว้(Maintain) คือปฏิบัติควบคู่ไปกับการทำงานปกติ(ไม่ใช่ทำเฉพาะก่อนจะโดนตรวจAudit)
- ปรับปรุงอย่างต่อเนื่อง(Continual Improvement) คือ ทบทวนผลการทำระบบและหาจุดปรับปรุงอย่างต่อเนื่อง ไม่ใช่ทำครั้งเดียวจบ

การทำระบบ ISO27001 ให้มีประสิทธิภาพ ท่านต้องทำตาม 4 ข้อข้างต้นให้ครบถ้วน ตั้งแต่ จัดทำระบบ(Establish), นำไปปฏิบัติ(Implement) , รักษาไว้(Maintain) และ Continual Improvement และต้องมีหลักฐาน(ทั้งเอกสารและผลการปฏิบัติ) ที่น่าเชื่อถือ สะท้อนความเป็นจริงและตรวจสอบย้อนหลังได้

โมเดล CIA ใน ISO27001

- ***Confidential:*** การปกป้องสารสนเทศให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ ถ้าหากข้อมูลรั่วไหลแสดงว่าขาดคุณสมบัติในข้อนี้
- ***Integrity:*** ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความเป็นจริง เช่น การแฮกระบบเพื่อแก้ไขข้อมูล เป็นต้น
- ***Availability***: สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน

ถึงตรงนี้หลายท่านคงสงสัยว่าแล้วจะต้องป้องกันConfidentiality , Integrityเข้มงวดแค่ไหน ข้อมูลก็มีมากมายหลายประเภท ต้องป้องกันอย่างเข้มข้นเท่ากันหมดทุกข้อมูลยังเปล่า ??? การปกป้องข้อมูล(Information) จะเข้มงวดมากหรือน้อย ขึ้นอยู่กับ**"ความเสี่ยง"** หลักการคือ ข้อมูลใดที่เสี่ยงสูงย่อมต้องมีมาตรการปกป้องเข้มงวดกว่าข้อมูลที่มีความ เสี่ยงต่ำ ตัวอย่างเช่น ข้อมูล username & password สำหรับเข้าสู่ระบบสารสนเทศขององค์กร ต้องมีมาตรการปกป้องที่เข้มงวดไม่น้อยกว่าข้อมูลทั่วไปที่ประกาศในเวบไซต์องค์กร เป็นต้น

ประเมินความเสี่ยงนั้นสำคัญไฉน

"การประเมินความเสี่ยงของสารสนเทศ(Information Security Risk Assessment) " เป็นหัวใจสำคัญของการทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศISO27001 นั่นคือ หากท่านประเมินความเสี่ยงไม่ถูกต้อง หรือไม่ครอบคลุม ก็จะทำให้การจัดการความเสี่ยงที่ตามมานั้นแก้ปัญหาไม่ตรงจุด และไม่ครอบคลุมตามไปด้วย ว่าไปแล้วการประเมินความเสี่ยงก็เหมือนการตรวจร่างกายนั่นแหละ ถ้าตรวจไม่ครบหรือตรวจไม่ละเอียดก็ไม่พบอาการป่วยและไม่ได้รักษา ปล่อยทิ้งไว้จนสุกงอมอาการป่วยก็แสดงออกมาในที่สุด!!

แนวทางจัดการความเสี่ยง

เมื่อประเมินความเสี่ยงของสารสนเทศ จนทราบแล้วว่ามีเรื่องอะไรบ้างที่มีความเสี่ยง ไม่ว่าจะเสี่ยงมาก เสี่ยงปานกลางหรือเสี่ยงน้อย ทุกความเสี่ยงต้องมีคำตอบรองรับว่าความเสี่ยงแต่ละระดับจะจัดการอย่างไร โดยทั่วไปความเสี่ยงสูงจะมีการทำ**แผนงานจัดการความเสี่ยง(Risk Treatment)** โดยมีมาตรการต่างๆ มาดูแลจัดการ

“ตรงนี้สำคัญเพราะว่าผลประเมินความเสี่ยงจะเป็นตัวกำหนดว่าจะต้องทำแผนงานจัดการความ เสี่ยง (Risk Treatment) เพื่อจัดการความเสี่ยงอะไรบ้าง ประเด็นเรื่องกฎหมายเป็นหัวข้อหนึ่งที่สำคัญในการประเมินความเสี่ยง หากพบว่าประเมินความเสี่ยงแล้วพบว่าเป็นเรื่องผิดกฎหมาย แบบนี้จัดเป็นความเสี่ยงสูงต้องรีบแก้ไขโดยด่วน” โปรดติดตามฉบับต่อไป

ที่มา ผู้เขียน : ปริญญ์ เสรีพงศ์ CISA, CEH, ISMS(IRCA)

http://www.club27001.com/2013/08/isoiec-27001_21.html

http://www.club27001.com/2014/01/review-iso27001-2013-part1.html

http://www.club27001.com/2014/01/iso27001-2013-Information-Risk-Assessment.html

ผู้รวบรวม โดย นันทนิตร์ มีพร้อม
นักตรวจสอบภายใน
มหาวิทยาลัยมหิดล