บทที่ 2
แนวความคิดและทฤษฎีที่เกี่ยวข้อง

2.1 แนวความคิด

ปัจจุบันระบบเทคโนโลยีสารสนเทศเข้ามามีบทบาทมากมายในองค์กรต่างๆ ทั้งในด้านระบบการทำงานขององค์กร ซึ่งในระบบองค์กรทั้งในภาครัฐและภาคเอกชน ต่างมีข้อมูลซึ่งเป็นความลับของแต่ละหน่วยงานโดยถ้าจะพูดถึงระบบการป้องกันความปลอดภัยสารสนเทศของแต่ล่ะหน่วยงาน จะมีรูปแบบและวิธีการที่แต่งต่างกันออกไป โดยระเบียบการจัดการมาตรฐานหลักของระบบบริหารป้องกันความปลอดภัยสารสนเทศหลักๆ คือ มาตรฐาน ISO 27001:2013 (ISMS : Information Security Management Systems) ที่ได้รับการยอมรับเป็นมาตรฐานสากล เพื่อให้องค์กรต่างๆปฏิบัติให้เป็นไปตามมาตรฐานเดียวกัน เพื่อลดความเสี่ยงและความปลอดภัยในระบบสารสนเทศ

ตารางที่ 2.1 สาเหตุของปัญหาด้านความปลอดภัยของระบบสารสนเทศ

เทคโนโลยี	กระบวนการ	บุคลากร
ขาดคุณสมบัติด้านความปลอดภัย	ไม่ได้ออกแบบกระบวนการให้รองรับด้านความปลอดภัย	ขาดความรู้ที่เกี่ยวกับเรื่องความปลอดภัย
มี Bugs มีช่องโหว่ด้านความปลอดภัย และขาด Patch แก้ไข	ไม่มีบทบาทความรับผิดชอบด้านความปลอดภัยชัดเจน	ขาดความใส่ใจจริงจังในการแก้ปัญหา
ไม่มีมาตรฐาน	ขาดการตรวจประเมินและติดตามตรวจสอบ	ขาดการสื่อสารที่ดีในเรื่องที่เกี่ยวกับความปลอดภัย
ยากที่จะปรับปรุงปัญหาความเสี่ยงด้านความปลอดภัยให้ทันต่อเหตุการณ์	ไม่มีแผนรองรับภัยพิบัติ	มีข้อผิดพลาดที่เกิดจากการทำงานของบุคลากรเอง
	ไม่มีกระบวนการรองรับการปรับความทันสมัยเรื่องความปลอดภัยให้ระบบ	

ISO 27001:2013 หรือ Information Security Management System (ISMS) เป็นมาตรฐานที่เกี่ยวกับการบริหารจัดการข้อมูลสารสนเทศให้มั่นคงปลอดภัย กำหนดขึ้นโดยองค์กรการระหว่างประเทศ คือ ISO (International Organization for Standardization) และ IEC (International Electrotechnical Commission) มาตรฐานนี้เป็นมาตรฐานสากลที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรและใช้เป็นมาตรฐานอ้างอิงเพื่อเป็นแนวทางในการเสริมสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรอย่างแพร่หลาย สามารถนำไปประยุกต์ใช้เพื่อรักษาความมั่นคงให้กับระบบสารสนเทศขององค์กร

2.2 ทฤษฎีที่เกี่ยวข้อง

รู้จัก ISO/IEC 27001 มาตรฐานระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ

ISO/IEC 27001 เป็นมาตรฐานที่เกิดจากความร่วมมือระหว่างหน่วยงาน ISO (The International Organization for Standardization) กับหน่วยงาน IEC (The International Electrotechnical Commission) ร่วมกับองค์กรระหว่างประเทศอื่นๆ อีกหลายองค์กร ประกอบด้วยองค์กรรัฐบาลและองค์กรอิสระต่างๆ

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 การสัมนา ที่ปรึกษาและผู้เชี่ยวชาญ

- เป็นมาตรฐานที่ไม่ผูกมัดกับเทคโนโลยี เทคนิค หรือ ขั้นตอนที่เฉพาะเจาะจง ผู้จัดทำระบบสามารถเลือกเทคโนโลยีได้ตามความเหมาะสมทำให้มาตรฐานมีความคล่องตัวสูง
- สิ่งที่ควรทราบก่อนนำมาตรฐานมาประยุกต์ใช้
- ISO/IEC 27001 เป็นภาษาอังกฤษ ส่วนของไทยก็มีมาตรฐานของคณะกรรมการธุรกรรมฯ องค์กรที่จัดทำระบบนี้ต้องมีความรู้ในภาษาอังกฤษระดับที่สามารถตีความข้อกำหนดได้อย่างถูกต้อง
- การประยุกต์ใช้มาตรฐาน ต้องมาตีความข้อกำหนดและวางแนวทางปฏิบัติให้สอดคล้อง หากตีความผิดหรือไม่ครบถ้วนก็อาจเกิดปัญหาในการตรวจประเมินได้

(Pryn Sereepong, 2556)

โครงสร้างของมาตรฐาน ISO 27001

ISO 27001 (Information Security Management System-ISMS) มาตรฐานการจัดการความมั่นคงปลอดภัยของสารสนเทศ ประกอบด้วยข้อกำหนดที่ครอบคลุมถึงการ จัดทำ นำไปปฏิบัติ ทบทวนและเฝ้าระวัง รักษาความต่อเนื่อง รวมถึงปรับปรุงระบบให้สอดคล้องกับสถานะการณ์ ผู้ที่ประยุกต์ใช้มาตรฐานนี้ต้องจัดทำเอกสารให้ครอบคลุมข้อกำหนดข้างต้นและระบบที่จัดทำขึ้นนี้จะต้องเหมาะสมกับความเสี่ยงเชิงธุรกิจขององค์กร

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

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

การที่องค์กรหนึ่งผ่านการรับรองมาตรฐานระบบการความมั่นคงปลอดภัยของสารสนเทศ ISO 27001นั้นหมายถึง องค์กรดังกล่าวได้นำข้อกำหนดของมาตรฐาน ISO 27001 มา

ประยุกต์ใช้อย่างครบถ้วน และมีหลักฐานที่เป็นรูปธรรมให้เชื่อได้ว่าองค์กรดังกล่าวมีระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศที่ได้มาตรฐานสากล (Pryn Sereepong, 2556)

องค์ประกอบของความมั่นคงปลอดภัยของสารสนเทศ

ความมั่นคงปลอดภัยของสารสนเทศนั้นมีองค์ประกอบด้วยกัน 3 ประการ คือ ความลับ (Confidentiality) ความถูกต้องสมบูรณ์(Integrity) และความพร้อมใช้งาน(Availability) ทรัพย์สิน (Asset) ที่มีความมั่นคงปลอดภัยนั้นต้องประกอบด้วยองค์ประกอบทั้งสามอย่างครบถ้วน ไม่ว่าทรัพย์สินนั้นจะเป็นสิ่งที่จับต้องได้ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย หรือทรัพย์สินที่จับต้องไม่ได้ เช่น ข้อมูล เป็นต้น

- ความลับ (Confidentiality)

การรักษาความลับให้กับข้อมูลเป็นองค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยของสารสนเทศ หลักการสำคัญของการรักษาความลับคือ ผู้ที่มีสิทธิหรือได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ ภาคธุรกิจให้ความสำคัญกับการรักษาความลับทางธุรกิจ ประชาชนทั่วไปก็ต้องการปกป้องข้อมูลส่วนตัวตามสิทธิขั้นพื้นฐานเช่นเดียวกัน

ข่าวการละเมิดมาตรการป้องกันของระบบคอมพิวเตอร์เข้าไปเจาะระบบทั้งในประเทศและต่างประเทศ แสดงให้เห็นว่ามาตรการที่มีอยู่ยังมีจุดอ่อนที่ ผู้ไม่ประสงค์ดีที่มีความรู้บุกรุกผ่านช่องโหว่ดังกล่าว แรงจูงใจของการกระทำการดังกล่าวมีหลายเหตุปัจจัย เช่น ทำเพื่อเงิน เพื่อสร้างชื่อเสียง การยอมรับในกลุ่ม และทำไปด้วยความคึกคะนอง ปฏิเสธไม่ได้ว่าแฮกเกอร์ที่สามารถเจาะทะลุระบบรักษาความปลอดภัยของหน่วยงานสำคัญระดับประเทศ จะกลายเป็นฮีโร่ในสายตาของแฮกเกอร์มือใหม่ทั่วโลก

ระบบความมั่นคงปลอดภัยของสารสนเทศที่มีประสิทธิภาพ ต้องมีมาตรการตรวจสอบสิทธิก่อนเข้าถึง เพื่อยืนยันให้แน่ใจก่อนว่าผู้ที่ร้องขอนั้นมีสิทธิหรือได้รับอนุญาตให้เข้าถึงสารสนเทศ หรือระบบงานนั้นได้ กลไกพื้นฐานที่คุ้นเคยกันเป็นอย่างดี คือการใช้รหัสผ่าน(Password) ในการพิสูจน์ตัวตนและสิทธิที่ได้รับอนุญาต

นอกจากมาตรการตรวจสอบสิทธิแล้วการกำหนดชั้นความลับเป็นระดับต่างๆ ตามความสำคัญช่วยให้บริหารจัดการมีประสิทธิภาพมากขึ้น ในบางหน่วยงานกำหนดชั้นความลับของสารสนเทศออกเป็น 4 ระดับ ประกอบด้วย ระดับชั้นความลับสุดยอด (Top Secret) ระดับชั้นความลับ (Secret) ระดับชั้นข้อมูลสำหรับใช้ภายในองค์กร(Internal Use) และระดับชั้นสารธารณะ(Public) ชั้นความลับนี้จะต้องมีเกณฑ์พิจารณาที่ชัดเจนว่าสารสนเทศลักษณะใดอยู่ในชั้นความลับที่กำหนด พร้อมทั้งกำหนดแนวทางการการระบุชั้นความลับ การสื่อสารและการจัดเก็บข้อมูลสารสนเทศในแต่ละชั้นความลับ

อย่างชัดเจน มาตรการทางเทคนิคที่ใช้ในการปกป้องความลับ เช่น การเข้ารหัส (Encryption) อาจถูกนำมาใช้เสริมความแข็งแกร่งให้กับมาตรการปกป้องสารสนเทศที่ต้องการมาตรการดูแลอย่างเข้มงวด

- ความถูกต้องสมบูรณ์ (Integrity)

การปกป้องสารสนเทศให้มีความถูกต้องสมบูรณ์ (Integrity) เป็นสิ่งสำคัญส่งผลถึงความน่าเชื่อถือของสารสนเทศนั้นๆ ทำอย่างไรให้ข้อมูลมีความถูกต้องและน่าเชื่อถือเป็นสิ่งที่ผู้ดูแลระบบต้องหาคำตอบและดำเนินการให้เกิดขึ้น คำตอบในเชิงหลักการคือระบบต้องมีกลไกการตรวจสอบสิทธิหรือการได้รับอนุญาตให้ดำเนินการเปลี่ยนแปลงแก้ไขหรือกระทำการใดๆ ต่อข้อมูลนั้น

ยิ่งเทคโนโลยีสารสนเทศพัฒนาก้าวหน้าไปมากเท่าไร มนุษย์ก็ยิ่งจำเป็นต้องพึ่งพาเทคโนโลยีมากขึ้นตามไปด้วย บัตรประชาชนอัจฉริยะเป็นตัวอย่างใกล้ตัวเราที่ชี้ให้เห็นว่า ประชาชนทุกคนไม่ว่าจะยากดีมีจนอย่างไร ก็ต้องเกี่ยวข้องกับเทคโนโลยีสารสนเทศอย่างเลี่ยงไม่ได้ จะเห็นได้ว่าข้อมูลนี้มีความสำคัญมากเพราะเป็นหลักฐานในการพิสูจน์ตัวตนของเรา หากมองในแง่ของสารสนเทศแล้ว ข้อมูลนี้จำเป็นต้องได้รับการปกป้องดูแลความถูกต้องสมบูรณ์และความน่าเชื่อถือ หากข้อมูลถูกเปลี่ยนแปลงโดยผู้ไม่ประสงค์ดีย่อมส่งผลเสียต่อเจ้าของข้อมูลอย่างหลีกเลี่ยงไม่ได้

- การพร้อมใช้งาน (Availability)

การทำให้ระบบตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิเข้าถึงระบบได้เมื่อต้องการ อุปสรรคที่บั่นทอนความพร้อมใช้งานของระบบคอมพิวเตอร์จำแนกได้ 2 แบบ คือ

- การที่ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ (Denial of Service)
- ระบบคอมพิวเตอร์ทำงานด้อยประสิทธิภาพในการทำงาน (Loss of data processing capability)

ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ อาจเกิดจากการกระทำของผู้ใช้ระบบ ผู้บุกรุกที่มีเจตนาร้าย หรือเกิดจากภัยธรรมชาติ เช่น น้ำท่วม ไฟไหม้ แผ่นดินไหวทำให้ระบบคอมพิวเตอร์เสียหายก็เป็นได้ องค์กรที่ตระหนักถึงภัยคุกคามดังกล่าวอาจเตรียมแผนกู้คืนจากความเสียหาย (Disaster Recovery Plan)ไว้รองรับ หน่วยงานรัฐที่ให้บริการสารธารณะต่างใช้ระบบคอมพิวเตอร์ควบคุมการทำงาน เช่นไฟฟ้า ประปา โทรศัพท์ เป็นต้น หากคอมพิวเตอร์ที่ควบคุมระบบเหล่านี้เกิดความเสียหายไม่สามารถให้บริการได้ ทำให้บริการต่างๆ หยุดชะงักย่อมส่งผลเสียต่อประชาชนในวงกว้าง นอกจากนี้หากไฟฟ้าดับเป็นเวลานาน ระบบต่างๆ จะเกิดความเสียหายอย่างใหญ่หลวง ตัวอย่างจริงที่เคยเกิดขึ้นในต่างประเทศ เมื่อหลายปีก่อนระบบคอมพิวเตอร์ของศูนย์

กระจายสินค้าเกิดความเสียหาย ไม่สามารถจ่ายกระแสไฟฟ้าไปยังคอนเทนเนอร์ที่ติดตั้งระบบทำความเย็นเป็นเวลาหลายวัน ส่งผลให้สินค้าในตู้คอนเทนเนอร์ดังกล่าวเสียหายทั้งหมด นอกจากนี้ยังทำให้ลูกค้าขอยกเลิกสัญญาเนื่องจากไม่ไว้วางใจในการบริการ เกิดความสูญเสียมูลค่ามหาศาล (Pryn Sereepong, 2556)

ภัยคุกคาม และช่องโหว่ (Threat and Vulnerability)

ภัยคุกคาม(Threat) อาจเป็นมนุษย์ ภัยธรรมชาติ หรือปัจจัยอื่นๆ ที่มีแนวโน้มที่จะก่อให้เกิดความเสียหายได้ ทั้งที่เจตนาสร้างความเสียหายหรือไม่ก็ตาม การทำความเข้าใจและตระหนักถึงภัยคุกคามจะช่วยให้เข้าใจองค์ประกอบที่เกี่ยวข้องกันทั้งระบบได้เป็นอย่างดี หากจำแนกแหล่งกำเนิดของภัยคุกคาม อาจแบ่งได้ดังนี้

- มนุษย์ เช่น แฮกเกอร์ สายลับ ผู้ก่อการร้าย ผู้ไม่ประสงค์ดีที่โจมตีระบบสารสนเทศ ไวรัส โปรแกรมไม่ประสงค์ดีต่างๆ เป็นต้น
- ภัยธรรมชาติ เช่นน้ำท่วม ฟ้าผ่า พายุ แผ่นดินไหว เป็นต้น
- ข้อผิดพลาดทางเทคนิค เช่น อุปกรณ์ชำรุด เสื่อมสภาพ หรือทำงานผิดพลาด เป็นต้น

ช่องโหว่(Vulnerability) เป็นองค์ประกอบที่สำคัญของการศึกษาเรื่องความมั่นคงปลอดภัยของสารสนเทศ ภัยคุกคามที่กล่าวมาข้างต้นจะใช้ประโยชน์จากช่องโหว่นี้เพื่อสร้างความเสียหาย ดังนั้นหากช่องโหว่มีจำนวนมาก โอกาสที่ภัยคุกคามจะสร้างความเสียหายจากช่องโหว่ดังกล่าวก็มากตามไปด้วย กล่าวได้ว่าหากไม่มีช่องโหว่หรือจุดอ่อน ภัยคุกคามก็ไม่สามารถทำอันตรายแก่ระบบสารสนเทศได้ (Pryn Sereepong, 2556)

บันได 4 ขั้นสู่มาตรฐาน ISO 27001 Information Security Management

การจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISMS) แบ่งเป็น 4 ขั้นตอน ดังนี้

บันไดขั้นที่ 1 การวางแผนจัดทำระบบ ISMS (Establish ISMS)

บันไดขั้นที่ 2 การนำไปปฏิบัติ (Implement and operate ISMS)

บันไดขั้นที่ 3 การเฝ้าระวังและทบทวน (Monitor an review ISMS)

บันได้ขั้นที่ 4 การรักษามาตรฐานและพัฒนาปรับปรุง (Maintain and improve ISMS)

รูปที่ **2.1** บันไดขั้นสู่มาตรฐาน ISO 27001 Information Security Management

บันไดขั้นที่ 1 การวางแผนจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (Plan : Establish the ISMS)

เริ่มต้นด้วยการกำหนดขอบเขตของการจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศให้ชัดเจน โดยแสดงถึงลักษณะของธุรกิจ องค์กร ทำเลที่ตั้ง ทรัพย์สิน และเทคโนโลยี หากไม่ครอบคลุมส่วนงานใด ต้องระบุรายละเอียดและเหตุผลดังกล่าว จากนั้นผู้บริหารระดับสูงกำหนดนโยบายการจัดการความปลอดภัยของสารสนเทศ (Information Security Management System Policy : ISMS Policy) พร้อมทั้งอนุมัติและประกาศใช้นโยบายดังกล่าว เป็นกลไกให้มั่นใจว่าโครงการนี้ได้รับการสนับสนุนอย่างเป็นรูปธรรม และเป็นสัญญาณว่า ISMSได้เริ่มอย่างเป็นทางการแล้ว

การกำหนดคณะทำงานให้เหมาะสมและเพียงพอเป็นเรื่องสำคัญที่ต้องพิจารณา ตัวแทนหน่วยงานที่อยู่ในขอบเขตการจัดทำระบบควรเข้าร่วมเป็นคณะทำงานเพื่อให้มีส่วนร่วมในการจัดทำระบบที่สอดคล้องกับลักษณะการทำงาน เมื่อได้คณะทำงานเรียบร้อยแล้วก็เริ่มสำรวจภัยคุกคามและช่องโหว่ที่ก่อให้เกิดความเสี่ยงต่อสารสนเทศในขอบเขตการจัดทำระบบขององค์กร ตัวแทนหน่วยงานที่เป็นคณะทำงานก็รับผิดชอบสำรวจภัยคุกคามและช่องโหว่ในหน่วยงานของตนเอง ผลการประเมินความเสี่ยงจะบอกถึงระดับความเสี่ยงจากภัยคุกคามและช่องโหว่ในระบบสารสนเทศ คณะทำงานและผู้เกี่ยวข้องต้องกำหนดมาตรการจัดการกับความเสี่ยงนั้นให้ชัดเจนและมีประสิทธิภาพเพียงพอ

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

ขั้นตอนการปฏิบัติ (Do) เป็นการนำผลลัพธ์ของขั้นตอนวางแผน(Plan) มาปฏิบัติให้เกิดผลตามวัตถุประสงค์ เช่น มาตรการป้องกันการบุกรุกระบบ มาตรการสำรองข้อมูล เป็นต้น ซึ่ง

ก่อนจะปฏิบัติได้อย่างถูกต้องนั้น จำเป็นต้องมีการฝึกอบรม ถ่ายทอดความรู้แนวทางปฏิบัติที่ถูกต้องให้รับทราบทั่วกัน

บันไดขั้นที่ 3 การเฝ้าระวังและทบทวน (Check : Monitoring and Review the ISMS) หลังจากปฏิบัติตามมาตรการที่กำหนดแล้ว เราจะรู้ได้อย่างไรว่ามาตรการที่ปฏิบัตินั้นได้ผลตามเป้าหมายที่ต้องการ คำตอบคือต้องมีการวัดผลของมาตรการที่ใช้ควบคุมดูแล แนวทางการวัดผลและความถี่ในการเฝ้าระวังต้องวิเคราะห์คู่กับความเสี่ยง ดังนั้นกระบวนการ ระบบงาน หรือทรัพย์สินสารสนเทศที่มีความเสี่ยงสูงควรได้รับการวัดผลการปฏิบัติงานที่เข้มงวดกว่า เพื่อให้มั่นใจว่าหากเกิดเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ระบบการตรวจวัดและเฝ้าระวังสามารถรายงานผลได้ทันเวลา

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

หลังจากที่ตรวจพบปัญหาหรือสิ่งผิดปกติในขั้นตอนการตรวจสอบ(Check : Monitoring and Review the ISMS) ผู้ที่เกี่ยวข้องทุกระดับจำเป็นต้องร่วมกันแก้ไขปัญหาที่เกิดขึ้นและป้องกันปัญหาที่อาจเกิดซ้ำในอนาคต รวมถึงหาแนวทางปรับปรุงระบบการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศให้มีประสิทธิภาพยิ่งขึ้น กลไกสำคัญที่ช่วยให้ผลักดันให้การแก้ไขปัญหาและปรับปรุงดำเนินการได้อย่างเป็นรูปธรรม คือการมีส่วนร่วมของผู้บริหารระดับสูง บ่อยครั้งที่พบว่าปัญหาเกิดจากการขาดความชัดเจนในนโยบายการบริหารจัดการ ซึ่งผู้บริหารจะต้องให้ความกระจ่างและตัดสินใจแก้ไขปัญหาเชิงนโยบายให้เป็นรูปธรรม เพื่อให้คณะทำงานยึดถือเป็นแนวปฏิบัติต่อไป (Pryn Sereepong, 2556)

พื้นฐานความมั่นคงปลอดภัยของสารสนเทศ

Information Security Management System (ISMS) Standard หรือ ISO 27001 เป็นมาตรฐานที่เกี่ยวกับการบริหารจัดการข้อมูลสารสนเทศให้มั่นคงปลอดภัย

ถึงองค์กรมีระบบสารสนเทศดีแต่ขาดมาตรการควบคุม พนักงานใช้ทรัพยากรไปกับเรื่องที่ไม่สมควร และทำผิดกฎหมาย เช่น พนักงานใช้คอมพิวเตอร์ขององค์กรโหลดหนังและแชร์ไฟล์ที่ละเมิดลิขสิทธิ์ เสี่ยงต่อการโดนจับและเสียหายต่อองค์กร

การจัดทำระบบบริหารจัดการ(Management System) จะต้องพิจารณาหลายด้านที่มีความเกี่ยวข้อง

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

ซึ่งต้องเข้าใจทั้ง 3 ด้านข้างต้น เพื่อที่จะหาจุดสมดุลและเกิดประโยชน์สูงสุด อย่างไรก็ตามเมื่อลงมือทำจริงมันมีอะไรเต็มไปหมดที่ต้องทำความเข้าใจ จะได้วางแนวทางปฏิบัติให้เหมาะสม ไม่เข้มงวดเกินไปจนทำอะไรไม่ได้(ปลอดภัยสูงสุด) หรือหลวมเกินไปจนไม่ได้ควบคุมอะไรเลย

รูปที่ **2.2** ISO2700 12013 (ISMS)

<u>ISO27001 มาตรฐานสากลที่ทั่วโลกยอมรับ</u>

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

ดังนั้นการที่จะมั่นใจได้ว่าระบบสารสนเทศของเรามีความมั่นคงปลอดภัย ก็คือเราจะต้องรู้ว่ามีภัยคุกคามอะไรบ้างที่อาจมาโจมตี ทำให้สารสนเทศของเราเกิดความเสียหาย จากนั้น

จึงประเมินความเสี่ยงและกำหนดมาตรการจัดการกับภัยคุกคาม ให้แน่ใจว่าสามารถรับมือภัยคุกคามเหล่านั้นได้อย่างเหมาะสม

เตรียมความรู้และความเข้าใจ 2 เรื่องใหญ่ๆ คือ

1. เข้าใจองค์กรตนเอง

ต้องสำรวจข้อมูล ซอฟแวร์ ฮาร์ดแวร์ บุคลากร ในขอบเขตที่จัดทำระบบ ข้อมูลนี้ยิ่งมีรายละเอียดยิ่งดี หากหน่วยงานท่านเป็นราชการ บัญชีครุภัณฑ์เป็นจุดเริ่มต้นที่ดีในการรวบรวมข้อมูล Hardware ,Software

เข้าใจภาระกิจขององค์กร รู้ว่าระบบงานใดสำคัญที่สุดและระบบงานต่างๆ มีข้อจำกัดและจุดอ่อนอะไรบ้าง รู้เพื่อที่จะไปหามาตรการมาจัดการกำจัดจุดอ่อน เช่น ระบบฐานข้อมูลทำงานอยู่บนเครื่อง Server เก่า หาก Server นี้เสีย ในกรณีนี้จุดอ่อนก็คือ Server ที่เก่า มีความเสี่ยงที่จะเสียเมื่อไหร่ก็ได้ ดังนั้นต้องหามาตรการ จัดการความเสี่ยงนี้ โดยจัดหาเครื่องใหม่ ซึ่งปัจจุบันนิยมใช้เทคโนโลยี Virtualization เข้ามาบริหารจัดการ ทั้งนี้ก็แล้วแต่แนวทางและขีดความสามารถของแต่ละองค์กร

2. เข้าใจมาตรฐาน

การนำมาตรฐาน ISO27001 มาใช้ ต้องทำความเข้าใจในตัวมาตรฐานเสียก่อน ว่าต้องทำอะไรบ้าง ทั้งเรื่องเอกสารและการนำไปใช้งานจริง ข้อกำหนดของ ISO27001:2013

ต้องใช้งบประมาณเท่าไหร่

งบประมาณมีความจำเป็น แต่ใช้งบประมาณมากหรือน้อยขึ้นอยู่กับสิ่งที่องค์กรยังขาด เช่น ประเมินความเสี่ยงมาแล้วพบว่าท่านยังไม่มีระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์(log) องค์กรจำเป็นต้องจัดหามาโดยด่วน เพราะผิดกฎหมาย หรือพบว่าเครื่อง Server อายุการใช้งานมาก มีโอกาสเสียเมื่อไหร่ก็ได้ แบบนี้องค์กรจำเป็นต้องมีงบประมาณเพื่อจัดหาใหม่มาทดแทน และที่พบค่อนข้างมากในหลายองค์คือไม่มีมาตรการหรือเครื่องมือเฝ้าระวังตรวจจับทางด้านความมั่นคงปลอดภัยของสารสนเทศ จำเป็นต้องลงทุนจัดหามาใช้งาน และหากจะขอใบรับรอง ISO 27001 ก็ต้องมีค่าตรวจประเมินรับรองระบบ (Certification) ซึ่งตรวจประเมินโดยหน่วยงานที่เรียกว่า Certified body

เริ่มต้นอย่างไร

Step1: กำหนดขอบเขต (Scope) ที่จะทำ ISO 27001 หรือ ต้องการให้ระบบงานหรือกิจกรรมอะไรบ้างที่ถูกควบคุมดูแลภายใต้ ISO 27001 เพื่อให้มั่นใจว่าสารสนเทศของระบบงานหรือกิจกรรมนั้นๆ มีความมั่นคงปลอดภัย

Step2: ศึกษามาตรฐาน ISO27001 ให้เข้าใจหลักการพื้นฐานและแนวทางการนำไปใช้

Step3: ทำการประเมินองค์กรเบื้องต้นให้รู้ว่าองค์กรยังขาดอะไรบ้างเมื่อเทียบกับสิ่งที่ต้องมีตามมาตรฐาน ISO 27001 ขั้นตอนนี้องค์กรจะต้องมีความรู้ในข้อกำหนดของ ISO 27001 พอสมควร ถึงจะประเมินได้ว่าข้อไหนมีแล้วข้อไหนยังขาด

หลังจากการประเมินองค์กรเบื้องต้น องค์กรจะรู้ว่ายังขาดอะไรบ้าง มีประเด็นอะไรที่ยังไม่สอดคล้องตามกฎหมาย และสรุปประเด็นเสนอผู้บริหารเพื่อเร่งดำเนินการ (Pryn Sereepong, 2557)

ความสำคัญของการประเมินความเสี่ยงสารสนเทศ

การนำมาตรฐานISO27001มาใช้งาน มี 4 องค์ประกอบใหญ่คือ

- จัดทำระบบ(Establish)การจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System -ISMS) คือ การเตรียมการวางแผนเพื่อปกป้องสารสนเทศ
- นำไปปฏิบัติ(Implement) คือ นำแผนจากขั้นตอนการจัดทำระบบ (Establish)ไปปฏิบัติจริงหน้างาน ทำตามเอกสารคู่มือและลงบันทึกในแบบฟอร์ม
- รักษาไว้(Maintain) คือปฏิบัติควบคู่ไปกับการทำงานปกติ (ไม่ใช่ทำเฉพาะก่อนจะโดนตรวจAudit)
- ปรับปรุงอย่างต่อเนื่อง(Continual Improvement) คือ ทบทวนผลการทำระบบและหาจุดปรับปรุงอย่างต่อเนื่อง ไม่ใช่ทำครั้งเดียวจบ

การทำระบบ ISO27001ให้มีประสิทธิภาพ ท่านต้องทำตาม 4 ข้อข้างต้นให้ครบถ้วน ตั้งแต่ จัดทำระบบ(Establish), นำไปปฏิบัติ(Implement) , รักษาไว้(Maintain) และ Continual Improvement และต้องมีหลักฐาน(ทั้งเอกสารและผลการปฏิบัติ) ที่น่าเชื่อถือ สะท้อนความเป็นจริง และตรวจสอบย้อนหลังได้

โมเดล CIA ในISO27001

ISO 27001 เน้นการปกป้องข้อมูลสารสนเทศ (Information) ให้มีคุณสมบัติ 3 ประการ คือ

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

การปกป้องข้อมูล(Information) จะเข้มงวดมากหรือน้อย ขึ้นอยู่กับ"ความเสี่ยง" หลักการคือ ข้อมูลใดที่เสี่ยงสูงย่อมต้องมีมาตรการปกป้องเข้มงวดกว่าข้อมูลที่มีความเสี่ยงต่ำ ตัวอย่างเช่น ข้อมูล username & password สำหรับเข้าสู่ระบบสารสนเทศขององค์กร ต้องมีมาตรการปกป้องที่เข้มงวดไม่น้อยกว่าข้อมูลทั่วไปที่ประกาศในเว็บไซท์องค์กร เป็นต้น

รูปที่ **2.3** ISO27001-2013 Risk Assessment

ประเมินความเสี่ยงนั้นสำคัญอย่างไร

การประเมินความเสี่ยงของสารสนเทศ (Information Security Risk Assessment) เป็นหัวใจสำคัญของการทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศISO27001 นั่นคือ หากองค์กรประเมินความเสี่ยงไม่ถูกต้อง หรือไม่ครอบคลุม ก็จะทำให้การจัดการความเสี่ยงที่ตามมานั้นแก้ปัญหาไม่ตรงจุด และไม่ครอบคลุมตามไปด้วย

แนวทางจัดการความเสี่ยง

เมื่อประเมินความเสี่ยงของสารสนเทศ จนทราบแล้วว่ามีเรื่องอะไรบ้างที่มีความเสี่ยง ไม่ว่าจะเสี่ยงมาก เสี่ยงปานกลางหรือเสี่ยงน้อย ทุกความเสี่ยงต้องมีคำตอบรองรับว่าความเสี่ยงแต่ละระดับจะจัดการอย่างไร โดยทั่วไปความเสี่ยงสูงจะมีการทำแผนงานจัดการความเสี่ยง(Risk Treatment) โดยมีมาตรการต่างๆ มาดูแลจัดการ จากนั้นเขียนเป็นคู่มือการปฏิบัติก็เป็นวิธีการที่นิยมใช้กันครับ

เพราะว่าผลประเมินความเสี่ยงจะเป็นตัวกำหนดว่าจะต้องทำแผนงานจัดการความเสี่ยง (Risk Treatment) เพื่อจัดการความเสี่ยงอะไรบ้าง ประเด็นเรื่องกฎหมายเป็นหัวข้อหนึ่งที่สำคัญในการประเมินความเสี่ยง หากพบว่าประเมินความเสี่ยงแล้วพบว่าเป็นเรื่องผิดกฎหมาย แบบนี้จัดเป็นความเสี่ยงสูงต้องรีบแก้ไขโดยด่วน (Pryn Sereepong, 2557)

ข้อกำหนด ISO 27001:2013

บทความนี้อธิบายภาพรวมของข้อกำหนดมาตรฐาน ISO27001:2013 Information Security Management System (ISMS) เพื่อให้ผู้อ่านได้เข้าใจภาพกว้างของมาตรฐานเป็นพื้นฐานสำหรับศึกษารายละเอียดเพิ่มเติมในเอกสารมาตรฐานฉบับเต็มได้ง่ายขึ้น

1. บริบทขององค์การ (Context of the organization)

1.1 ทำความเข้าใจเกี่ยวกับองค์กรและบริบทขององค์กร (Understanding the organization and its context)

พื้นฐานสำคัญในการวางระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO27001:2013 คือความเข้าใจบริบทขององค์กร โดยต้องระบุประเด็นภายใน(Internal issues) และประเด็นภายนอก(External issues) นำทั้ง2ประเด็นนี้มาพิจารณาในการวางระบบให้ครอบคลุมอย่างเหมาะสมไม่ตกหล่นประเด็นสำคัญ

1.2 กำหนดความจำเป็นและความคาดหมายของบุคคลที่เกี่ยวข้อง (Understanding the needs and expectations of interested parties)

ในการทำ ISO27001 จะต้องรู้ว่าใครคือผู้เกี่ยวข้อง (Interested parties) และพวกเขามีความต้องการและคาดหวังอะไร(needs and expectations)จากองค์กรของเรา ระบบงานใดมีความสำคัญเพราะเป็นงานที่ข้องเกี่ยวกับการส่งมอบสินค้าหรือบริการให้กับผู้เกี่ยวข้อง บริบทขององค์กรเป็นข้อมูลสำคัญในการกำหนดขอบเขตของการจัดทำระบบ(Scope)

1.3 การกำหนดขอบเขตของระบบการจัดการความปลอดภัยสารสนเทศ (Determining the scope of the information security management system)

ขอบเขต(Scope) ของการทำ ISO27001:2013 ต้องพิจารณาถึงข้อกำหนด(Interested parties) ตรงนี้เป็นเงื่อนไขสำคัญที่องค์กรต้องทำความเข้าใจและกำหนดขอบเขตให้เหมาะสมและเพียงพอคือไม่กำหนดขอบเขตเล็กเกินไปจนตกหล่นผู้เกี่ยวข้อง หรือขอบเขตกว้างเกินกว่าความสามารถในการบริหารจัดการส่งผลให้ระบบขาดประสิทธิภาพ

1.4 ระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security management system)

จัดทำระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ(ISMS) โดยกำหนดนโยบาย จัดทำเอกสารที่เกี่ยวข้อง นำไปปฏิบัติและรักษาไว้ รวมถึงปรับปรุงอย่างต่อเนื่อง โดยISMSต้องสอดคล้องตามข้อกำหนดของ ISO27001:2013 Information Security Management System

2. ความเป็นผู้นำ (Leadership)

2.1 ความเป็นผู้นำและความมุ่งมั่น (Leadership and commitment)

ผู้บริหารต้องแสดงให้เห็นถึงภาวะผู้นำและให้ความสำคัญกบระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ(ISMS)

2.2 นโยบาย (Policy)

ผู้บริหารเป็นผู้กำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับจุดประสงค์ขององค์กรและสอดคล้องกับข้อกำหนด

2.3 บทบาทขององค์กรและหน่วยงานที่รับผิดชอบ (Organizational roles, responsibilities and authorities)

กำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยของสารสนเทศ

3. การออกแบบ (Planning)

3.1 การดำเนินการเพื่อรับมือกับความเสี่ยงและโอกาส (Actions to address risks and opportunities)

การวางแผนงานสำหรับระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ จะต้องพิจารณาถึงบริบทขององค์กร พิจารณาความเสี่ยงที่เกี่ยวข้องจากนั้นวางแนวทางจัดการอย่างเหมาะสม

3.2 การรักษาความปลอดภัยสารสนเทศและวางแผนบรรลุวัตถุประสงค์ (Information security objectives and plans to achieve them)

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

4. การสนับสนุน (Support)

4.1 แหล่งที่มา (Resources)

การทำระบบให้สำเร็จจำเป็นต้องมีทรัพยากรเพียงพอและเหมาะสม ประกอบด้วย บุคลากร เวลา งบประมาณ และการสนับสนุนจากผู้บริหารอย่างเป็นรูปธรรม

4.2 สมรรถนะ (Competence)

บุคลากรที่มีส่วนร่วมในการจัดทำระบบจะต้องมีความรู้ความสามารถ ซึ่งต้องมีการให้ความรู้ที่ตรงกับภาระหน้าที่เพื่อให้บุคลากรสามารถปฏิบัติได้อย่างถูกต้อง

4.3 ความตระหนัก (Awareness)

ความตระหนักเป็นเรื่องสำคัญในด้านความมั่นคงปลอดภัยของสารสนเทศ เพราะหากบุคลกรมีความตระหนักที่เพียงพอ ย่อมจะลดความเสี่ยงได้โดยปริยาย เช่น เรื่องการใช้รหัสผ่านที่แข็งแรงเดายาก ถ้าบุคลากรมีความตระหนักก็จะเข้าใจผลการความเสี่ยงลดลง

4.4 การสื่อสาร (Communication)

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

4.5 เอกสารสารสนเทศ (Documented information)

เอกสารมีความจำเป็นในการทำงานร่วมกันเพื่อให้เกิดความชัดเจนแก่ผู้ปฏิบัติและผู้ตรวจสอบ (Auditor) เอกสารในระบบISO27001:2013 นั้นจะต้องผ่านการจัดทำโดยผู้ที่มีความรู้ มีผู้ทบทวน และอนุมัติก่อนจะนำไปใช้งาน

5. การดำเนินการ (Operation)

5.1 การวางแผนที่เกี่ยวข้องกับการดำเนินการและการควบคุม (Operational planning and control)

ข้อนี้กล่าวถึงการปฏิบัติตามแผนที่วางไว้ โดยลงมือตามแผนจัดการความเสี่ยง

5.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment)

ประเมินความเสี่ยงต้องทำเป็นระยะ ไม่ใช่ทำครั้งเดียวจบ เพราะเมื่อเวลาผ่านไปก็จะมีความเสี่ยงใหม่เกิดขึ้นมา ไม่ว่าจะเป็นความเสี่ยงจากเทคโนโลยีใหม่ๆ หรือสภาพแวดล้อม สังคม และการเมือง

5.3 การรักษาความเสี่ยงด้านความปลอดภัยสารสนเทศ (Information security risk treatment)

Information Security Risk Treatment เป็นเครื่องมือการจัดการความเสี่ยงที่จัดทำขึ้นภายหลังการประเมินความเสี่ยงของทรัพย์สินสารสนเทศ โดยกำหนดรายละเอียด ขั้นตอนวิธีการต่างๆ เพื่อนำไปปฏิบัติให้ได้ผลลัพธ์ตามที่กำหนดไว้

6. การประเมินประสิทธิภาพและประสิทธิผล (Performance evaluation)

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

เรื่องสำคัญที่พลาดไม่ได้คือ การเฝ้าระวัง (Monitor) การวัด (measure) การวิเคราะห์ (Analyze) และการประเมิน (evaluate) performance ของระบบ ทำให้รู้ได้ว่าผลลัพธ์เป็นไปตามที่วางแผนหรือไม่อย่างไร

6.2 การตรวจประเมินภายใน (Internal audit)

การตรวจประเมินภายใน (Internal Audit) เป็นเครื่องมือสำคัญที่ทำให้รู้ว่าระบบที่เราจัดทำขึ้นมานั้น มีความสมบูรณ์จัดทำครบถ้วนตามข้อกำหนด มีการนำไปปฏิบัติหรือไม่ และได้ผลลัพธ์เป็นอย่างไร ตรวจสอบความเข้าใจ การปฏิบัติและเอกสารบันทึกที่เกี่ยวข้อง

6.3 การตรวจสอบการจัดการ (Management review)

Management Review เป็นการประชุมเพื่อรายงานผลของการจัดทำระบบ ISO 27001:2013 Information Security Management (ISMS) ต่อผู้บริหารระดับสูง (Top Management) โดยรายงานถึงการเปลี่ยนแปลงภายในและภายนอกที่มีผลกระทบต่อระบบ ผลการประเมินความ

เสี่ยงและการจัดการความเสี่ยง ผลการเฝ้าระวังด้านInformation Security ผลการตรวจประเมินภายใน (Internal Audit) ข้อบกพร่องจากการตรวจประเมินภายใน เป็นต้น

7. การแก้ไข (Improvement)

7.1 ความไม่คล้อยตามและการดำเนินการแก้ไข (Nonconformity and corrective action)

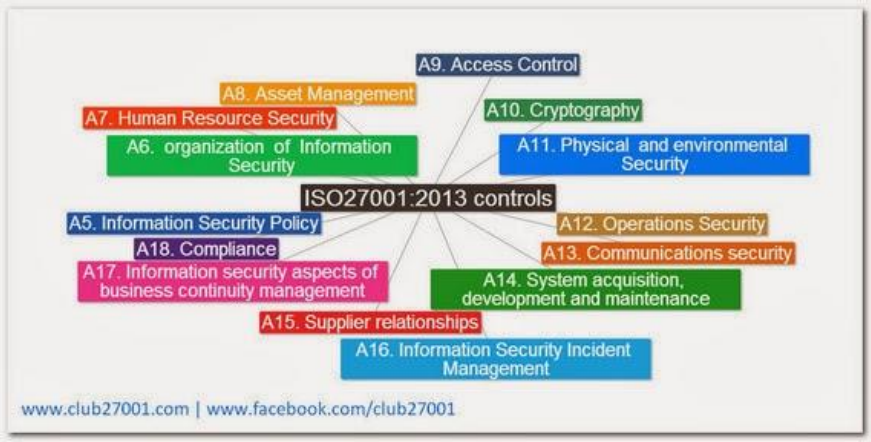
การระบุความไม่คล้อยตาม(Nonconformity) และแก้ไข (corrective action) อย่างเป็นระบบ มีผู้รับผิดชอบและมีบันทึกที่เป็นลายลักษณ์อักษรเกี่ยวกับความไม่คล้อยตามและแนวทางการแก้ไข

7.2 การแก้ไขอย่างต่อเนื่อง (Continual improvement)

ข้อกำหนดระบุให้องค์กรปรับปรุงระบบให้มีความเหมาะสม เพียงพอ และมีการปรับปรุงอย่างต่อเนื่อง (Pryn Sereepong, 2557)

มาตรการ(Control) จัดการความมั่นคงปลอดภัยของสารสนเทศ ISO 27001 :2013

การบริหารจัดการสารสนเทศในองค์กรให้มั่นคงปลอดภัยตามมาตรฐานISO 27001:2013นั้น จำเป็นต้องมีมาตรการที่เหมาะสมกับความเสี่ยงของสารสนเทศ (Information Security Risk)



รูปที่ **2.**4 มาตรการ (Control) จัดการความปลอดภัยของสารสนเทศ ISO 27001 :2013

ในการจัดทำและดำเนินระบบ (ISMS) ISO27001:2013 มีมาตรการให้ท่านเลือกมาใช้มากมายครอบคลุมตั้งแต่เรื่องคน (Human) เรื่องHardware ,Software และอื่นๆ

ท่านสามารถนำมาตรการเหล่านี้มาใช้งาน (Implementation) และวางระบบเฝ้าระวังตรวจสอบ (ISMS Monitoring and Measurement) เพื่อวัดผลว่ามาตรการนั้นๆมีประสิทธิภาพเพียงพอที่จัดการความเสี่ยงได้อย่างเหมาะสมหรือไม่

บทความนี้ขอนำเสนอมาตรการจัดการความปลอดภัยของสารสนเทศ ตาม Annex A ของ ISO 27001:2013

มาตรการมีทั้งหมด 14 ข้อได้แก่

A5. นโยบายความปลอดภัยสารสนเทศ (Information Security Policy)

A6. โครงสร้างความปลอดภัยสารสนเทศ (organization of Information Security)

A7. ความปลอดภัยสำหรับบุคลากร (Human Resource Security)

A8. การบริหารจัดการทรัพย์สิน (Asset Management)

A9. การควบคุมการเข้าถึง (Access Control)

A10. การเข้ารหัสข้อมูล (Cryptography)

A11. ความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)

A12. ความปลอดภัยสำหรับการดำเนินการ (Operations Security)

A13. ความปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

A14. การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)

A15. ความสัมพันธ์กับผู้ขายภายนอก (Supplier relationships)

A16. การบริหารจัดการความเป็นมาด้านความปลอดภัยสารสนเทศ (Information Security Incident Management)

A17. ด้านความปลอดภัยข้อมูลสารสนเทศของการจัดการต่อเนื่องทางการค้า (Information security aspects of business continuity management)

A18. ความสอดคล้อง (Compliance)

(Pryn Sereepong, 2557)

แนวทางการทำแผนจัดการความเสี่ยง ISO 27001 (Risk Treatment Plan)

ขั้นตอนที่สำคัญมากในการทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System - ISMS) ตาม ISO 27001 นั้นคือการประเมินความเสี่ยง(Risk Assessment) หลังจากประเมินความเสี่ยงตามเกณฑ์(Risk Criteria)ที่กำหนดแล้ว ก็จะได้ได้ผลลัพธ์ออกมาเป็นความเสี่ยงระดับต่างๆ (ในที่นี้กำหนดความเสี่ยงเป็น 2 ระดับคือความเสี่ยงที่ยอมรับได้ และความเสี่ยงสูง) โดยความเสี่ยงแต่ละระดับก็จะมีแนวทางการจัดการที่เหมาะสม เช่น

1. ความเสี่ยงที่ยอมรับได้ : ดำเนินการกำหนดขั้นตอนการปฏิบัติงาน ชี้แจงสร้างความเข้าใจ ปลูกฝังจิตสำนึก และเฝ้าระวัง

2. ความเสี่ยงสูง : จัดทำแผนจัดการความเสี่ยง (Risk Treatment Plan) โดยในการทำแผนนี้ให้เลือกมาตรการ (Controls) จาก Annex A ที่เหมาะสมมาใช้งานให้ตรงกับภัยคุกคาม ช่องโหว่ และความเสี่ยง

<u>แผนจัดการความเสี่ยง (Risk Treatment Plan)</u>

มีวัตถุประสงค์เพื่อจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยแผนฯนี้มีคุณสมบัติสำคัญ 2 อย่างคือ

1. จัดการลดโอกาสที่ภัยคุกคามจะใช้ช่องโหว่มาทำอันตรายต่อองค์กร
2. การลดผลกระทบของ Incident ที่เกิดจากความเสี่ยงดังกล่าว

ในการเขียนแผนจัดการความเสี่ยง ให้โฟกัสไปที่ภัยคุกคามและช่องโหว่ แล้วนำมาตรการ(Controls) ที่เกี่ยวข้อง มาประยุกต์ใช้งาน เพื่อการลดโอกาสเกิด และลดผลกระทบจากภัยคุกคามเหล่านั้น เช่น ผลประเมินความเสี่ยงพบว่ามีความเสี่ยงของการเข้าถึงห้อง Server โดยไม่มีการควบคุม ซึ่งผลการประเมินพบว่ามีความเสี่ยงสูงจำเป็นต้องทำแผนจัดการความเสี่ยง

<u>มาตรการที่เลือกใช้</u>

1. ในกรณีนี้เป็นเรื่องของการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) จึงเลือกมาตรการข้อ A11.1.2 Physical entry controls (ควบคุมการเข้าออกทางกายภาพ) โดยเพิ่มอุปกรณ์ Kay Card และกล้องวงจรปิด ที่หน้าห้อง Server และเก็บข้อมูลผู้ที่ผ่านเข้าออกทุกครั้งเพื่อตรวจสอบภายหลัง

2. กำหนดวิถีทางการเข้าถึงห้อง Server ซึ่งตรงกับมาตรการเรื่อง ข้อ A9.1.1 Access control policy โดยอนุญาตให้ผู้เกี่ยวข้องเท่านั้นมีสิทธิผ่านเข้าออกได้ กรณีอื่นให้ร้องขอเป็นหนังสือ เช่น กรณี Vendor มา Maintenance ต้องมีเจ้าหน้าที่ขององค์กรเป็นผู้ร้องขอและนำเข้าไป เป็นต้น (รายละเอียดในการควบคุมนี้ ขึ้นอยู่กับบริบทของแต่ละองค์กร)

หลังจากกำหนดรายละเอียดการดำเนินงานแล้ว ก็ต้องกำหนดผู้รับผิดชอบปฏิบัติ และงบประมาณที่ต้องใช้ในการจัดหาอุปกรณ์ เครื่องมือต่างๆ ในกรณีนี้ได้แก่ ระบบ Key Card และกล้องวงจรปิด เป็นต้น

จะเห็นได้ว่าหลังจากที่เราได้กำหนดการเข้าถึงห้อง Server อย่างชัดเจน และมีอุปกรณ์ควบคุมเป็นรูปธรรม โอกาสที่คนไม่เกี่ยวข้องจะเข้าไปในห้อง Server จึงเป็นไปได้ยาก ทำให้ความเสี่ยงในกรณีนี้ก็ลดลงอย่างเห็นได้ชัด กล่าวได้ว่า ความเสี่ยงลดลงบรรลุตามวัตถุประสงค์

อย่างไรก็ตาม แม้ความเสี่ยงจะลดลงแต่ก็มิได้หมายความว่าเราเลิกสนใจไปเลย ตรงข้ามเราจำเป็นต้องกำกับดูแล ควบคุมให้เป็นไปตามนโยบายอย่างเคร่งครัด ได้แก่

- ให้สิทธิผ่านเข้าออกเฉพาะผู้ที่เกี่ยวข้องเท่านั้น ตามหน้าที่ความรับผิดชอบ
- บำรุงรักษาอุปกรณ์ระบบ Key Card ,และกล้องวงจรปิด อย่างสม่ำเสมอ

- ตรวจสอบการจัดเก็บข้อมูล Log ทั้งของ Key card และกล้องวงจรปิดให้แน่ใจว่าจัดเก็บได้ครบถ้วน
- ตรวจสอบย้อนหลัง ว่าผู้ที่ผ่านเข้าออกนั้นเป็นผู้ที่ได้รับอนุญาตตามนโยบาย

(Pryn Sereepong, 2557)

แนวทางการทำ ISO27001:2013 Project Master Plan

ISO27001:2013 Project Master Plan คือ แผนงานที่กำหนดรายละเอียดกิจกรรมต่างๆ เพื่อสร้างระบบการจัดการความมั่นคงปลอดภัยให้เกิดขึ้นในองค์กร แผนงานนี้จะกำหนดช่วงเวลาและผู้รับผิดชอบแต่ละงานทำให้เห็นภาพรวมของเนื้องานในช่วงเวลาต่างๆ ช่วยให้บริหารจัดการได้มีประสิทธิภาพมากขึ้น

ข้อดีของการทำ Project Plan

- ใช้ประกอบการวางแผนงานประจำปี ทำให้หน่วยงานรู้ว่ามีอะไรต้องทำในช่วงเวลาใด มีประโยชน์อย่างยิ่งในการเตรียมการล่วงหน้าเพื่อจัดสรรเวลาและคนทำงานให้เหมาะสม โดยเฉพาะอย่างยิ่งในกรณีที่องค์กรทำหลายโครงการพร้อมกัน
- ใช้เตรียมงบประมาณ การทำโครงการเพิ่มประสิทธิภาพใดๆก็ตาม จำเป็นต้องใช้งบประมาณมากบ้าง น้อยบ้างแล้วแต่เนื้องาน ISO27001-2013 ก็เช่นเดียวกัน การมีแผนงานล่วงหน้าจะทำให้สามารถเตรียมงบประมาณล่วงหน้า เมื่อถึงเวลาทำงานจริงจะได้ไม่ติดขัดเรื่องการใช้งบประมาณที่จำเป็น
- เตรียมบุคลากร คณะทำงานระบบการจัดการความมั่นคงปลอดภัยเป็นตัวแทนของหน่วยงานที่เข้าระบบ ISO27001 ซึ่งส่วนใหญ่ก็จะหนีไม่พ้นหน่วยงานไอที ธุรการ ซ่อมบำรุง และหน่วยงานOperationต่างๆ ที่เกี่ยวข้อง Project Master Plan ทำให้รู้ว่ามีกิจกรรมอะไรบ้าง ในช่วงเวลาใด ทำให้คณะทำงานสามารถวางแผนการทำงานของตนเองได้ล่วงหน้า

(Pryn Sereepong, 2557)

7 ขั้นตอนการทำ ISO 27001:2013 Gap Analysis

ISO 27001:2013 Gap analysis คือการสำรวจตรวจสอบและประเมินสิ่งที่เป็นอยู่ ณ ปัจจุบัน (ก่อนเริ่มทำระบบ) เปรียบเทียบกับข้อกำหนดของ ISO 27001:2013

การตรวจประเมินด้วยข้อกำหนด ISO 27001:2013 เพื่อดูว่าหน่วยงานมีอะไรอยู่แล้วและยังขาดอะไรที่ต้องทำเพิ่ม

7 ขั้นตอนการทำ ISO 27001:2013 Gap Analysis

1. ชี้แจงสื่อสารทำความเข้าใจวัตถุประสงค์ของการทำ Gap Analysis ให้ทราบทั้งองค์กร โดยเฉพาะหน่วยงานที่จะถูกประเมิน
2. ผู้ทำ Gap Analysis ศึกษาข้อกำหนด (ISO 27001 Requirements) ของ ISO 27001:2013 ให้เข้าใจ
3. จัดทำ Checklist ตามข้อกำหนด - ควรใช้คำถามที่เกี่ยวข้อง และถ้าให้ดีควรถามให้ตรงกับ context ของหน่วยงานที่ไปประเมิน (จากการเป็นที่ปรึกษา เจอบ่อยมาก ที่ใช้ standard checklist ไปตาม ปรากฏว่าคนถูกถามไม่เข้าใจว่าอยากรู้อะไร ??)
4. สอบถามขั้นตอน ความเข้าใจของผู้ตอบ และเรียกดูหลักฐาน ทั้งเอกสารและข้อมูลในระบบที่เกี่ยวข้อง
5. บันทึกสิ่งที่พบให้ชัดเจน เช่น สัมภาษณ์ใคร ชื่อ,ตำแหน่ง หน่วยงาน เอกสารอะไร(ชื่อเอกสาร,รหัส)ที่พบว่าไม่สอดคล้อง
6. สรุปผลและทำรายงาน - โดยสรุปตามข้อกำหนด ISO 27001:2013 ทุกข้อ เช่น เรื่องประเมินความเสี่ยง องค์กรมีหรือไม่มี ถ้ามีแล้วมีครบตามข้อกำหนดหรือไม่ เป็นต้น
7. นำเสนอต่อผู้บริหารสูงสุด (Top Management) เพื่อรายงานให้ทราบถึงสถานะปัจจุบัน ว่าอยู่ในระดับใด ยังขาดอะไรบ้างที่จะได้มาตรฐาน ตามISO 27001:2013

หัวใจสำคัญของ ISO 27001:2013 Gap Analysis คือ ข้อมูลทำให้รู้ว่าองค์กรของเรายังขาดอะไร แค่ไหน ที่สำคัญคือ มีอะไรที่ยังไม่สอดคล้องตามกฎหมายบ้าง Report ที่ได้จากกิจกรรมนี้ เป็นจุดตั้งต้นของการปรับปรุงองค์กรให้มีความมั่นคงปลอดภัย ให้ผู้บริหารหยิบไปใช้วางแผน เตรียมงาน เตรียมคน เตรียมงบประมาณ เพื่อปิด Gap เหล่านี้ (Pryn Sereepong, 2557)

7 ขั้นตอนวางแผนตรวจประเมินภายใน (Internal Audit) ISO 27001:2013

ได้กล่าวไว้ว่า การตรวจประเมินภายใน(Internal Audit ISO 27001:2013) เป็นกิจกรรมบังคับสำหรับหน่วยงานที่จัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ(Information Security Management System : ISMS) ISO 27001:2013 ภาพรวมของการวางแผนแบ่งเป็น 7 ขั้นตอนดังนี้

1. เตรียมบุคลากรที่จะทำหน้าที่เป็นผู้ตรวจประเมินภายใน (Internal auditor ISO 27001:2013) โดยผู้ตรวจประเมินเหล่านี้จะต้องมีความรู้และเข้าใจในข้อกำหนด (Requirements) ของ ISO 27001:2013 ว่าแต่ละข้อกำหนดมีเจตนารมณ์อย่างไร และควรจะดูหลักฐานอะไรเพื่อ

ยืนยันว่าได้ปฏิบัติตามข้อกำหนดเหล่านั้น (ไม่เน้นจำข้อกำหนด ขอเพียงเข้าใจและทำ Checklist ล่วงหน้าก็ตรวจประเมินได้ระดับหนึ่งแล้ว)

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

3. กำหนดขอบเขตของการตรวจประเมิน โดยกำหนดเป็นพื้นที่ หน่วยงาน หรือระบบงาน ให้ชัดเจน เพื่อจะได้วางแผนตรวจประเมินโดยพิจารณาถึงขนาดและความซับซ้อนของระบบงานหรือหน่วยงานที่ไปตรวจ รวมถึงการจัดเวลาและผู้ตรวจประเมินที่มีทักษะและความสามารถตรงกับภาระกิจได้อย่างเหมาะสม

4. หากเป็นการตรวจประเมินภายในครั้งแรก (มือใหม่หัดตรวจ) แนะนำให้นำ Gap Analysis ISO 27001:2013 มาเป็นแนวทางการวางแผน โดยให้list สิ่งที่รายงาน Gap Analysis ระบุว่ายังไม่ได้ทำ หรือยังไม่มี เช่น ยังไม่มีนโยบายความมั่นคงปลอดภัยของสารสนเทศเป็นลายลักษณ์อักษร นี่แหละคือสิ่งที่จะต้องFocus เวลาไปตรวจประเมิน ส่วนที่รายงานGap Analysis ระบุว่ามีแล้ว ก็ให้ Internal Auditor ไปตรวจว่ายังรักษาอยู่ได้หรือไม่ เป็นต้น

5. ถ้าเป็นการตรวจประเมินครั้งที่ 2เป็นต้นไป เวลาวางแผนตรวจประเมินควรดูผล Audit คราวก่อนด้วย จะได้รู้ว่าตอนตรวจประเมินความก่อนมีปัญหาอุปสรรคอะไร เช่น ในแผนให้เวลามากไป น้อยไป ผู้ตรวจถามตรงประเด็นมั้ย ฯลฯ นอกจากนี้ให้ดูว่าการตรวจประเมินคราวก่อนพบข้อบกพร่องที่หน่วยงานใดมากที่สุด ตรวจคราวนี้จะได้ไปทวนสอบดูว่าได้แก้ปัญหาเหล่านั้นเรียบร้อยหรือยัง แก้ตรงจุดได้ผลชงัดหรือไม่ เป็นต้น

6. วางแผนการตรวจประเมินภายใน (Internal Audit) โดยพิจารณาว่าแต่ละหน่วยงานจะถูกตรวจข้อกำหนด ISO 27001:2013ใดบ้าง จุดสำคัญคือผู้ที่วางแผนนี้จะต้องเข้าใจในข้อกำหนดและบริบทของหน่วยงานที่ถูกตรวจ ผลที่ได้คือ วางแผนตรวจประเมินภายในได้ครอบคลุมครบถ้วนและกำหนดเวลาได้เหมาะสม

7. เมื่อจัดทำแผนการตรวจประเมินภายใน (Internal audit ISO 27001:2013) เรียบร้อยแล้ว ให้เสนอตัวแทนฝ่ายบริหาร (Management Representative) พิจารณาและแนะนำให้เสนอต่อ Top Management ลงนามในแผนให้มีผลบังคับใช้อย่างเป็นทางการ (ไม่มีใครกล้าเบี้ยว ถ้าไม่มีเหตุจำเป็นจริงๆ)

บทความนี้กล่าวถึงขั้นตอนการวางแผนตรวจประเมินเพื่อให้เข้าใจภาพรวมกว้าง เวลาที่วางแผนจริงจะต้องอ้างอิงระเบียบปฏิบัติ(Procedure) ซึ่งจะกำหนดหน้าที่ไว้อย่างชัดเจนว่าใครเป็นผู้จัดทำ Audit Plan ใช้แบบฟอร์มอะไร ใครเป็นผู้อนุมัติ และแจ้งหน่วยงานให้ทราบล่วงหน้า

อย่างน้อยกี่วัน รวมถึงอาจกำหนดคุณสมบัติของผู้ตรวจประเมิน (ISO 27001:2013 Internal auditor) ไว้เป็นลายลักษณ์อักษรด้วย (Pryn Sereepong, 2557)

4 เคล็ดลับการเตรียมตัวสำหรับผู้ตรวจประเมินภายใน ISO 27001 Internal Auditor

4 เคล็ดลับการเตรียมตัวสำหรับผู้ตรวจประเมินภายใน ได้แก่

1. ทำความเข้าใจข้อกำหนด (ISO 27001 Requirements): ข้อนี้เป็นหัวใจสำคัญของการเป็นผู้ตรวจประเมินภายใน ISO 27001 (Internal auditor ISO 27001) เข้าใจข้อกำหนด (ISMS Requirements)

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

2. ทำความเข้าใจหน่วยงานที่จะต้องไปตรวจ (Audit) : ควรเข้าใจและเห็นภาพรวมพอ เช่น หน่วยงานมีหน้าที่อะไร มีระบบงานอะไรบ้าง น่าจะมีภัยคุกคามและความเสี่ยงอะไรบ้าง ตรงนี้ผู้ตรวจประเมินสารสนเทศ อาจพอเดาได้ว่าน่าจะใช้เวลามากกับจุดไหนมากน้อยเท่าไร เช่น สัมภาษณ์และตรวจสอบเอกสาร 1 ชม. สำรวจสถานที่ปฏิบัติงาน 45 นาที เป็นต้น (จะใช้เวลามากหรือน้อยขึ้นอยู่กับภัยคุกคาม ความเสี่ยงและความซับซ้อน)

3. เตรียมคำถาม (ISO 27001:2013 Checklist) : หลังจากที่ทำความเข้าใจหน่วยงานที่ได้รับมอบหมายให้ตรวจแล้ว auditor ก็มีภาระกิจสำคัญคือการเตรียมคำถาม ที่เรียกกันว่า Checklist นี่ถือเป็นยาขมอย่างหนึ่งของการเป็นผู้ตรวจประเมิน เพราะหากไม่เข้าใจข้อกำหนดเพียงพอ ก็จะไม่รู้ว่าอะไรคือ Keyword สำคัญที่จะใช้เป็นคำถาม

4. เรียบเรียงคำถาม : ควรเรียบเรียงคำถามให้เป็นไปตามลำดับงาน หรือกระบวนการทำงาน เช่น ถาม Audit ระบบงานจัดซื้อ ก็ควรวางคำถามตามลำดับขั้นตอนการจัดซื้อ เช่น เริ่มจาก Purchase request แล้วไปต่อที่ Review , approve เป็นต้น อย่าวางคำถามโดดไปโดดมา เพราะจะทำให้จับประเด็นได้ยาก

การเป็นผู้ตรวจประเมินภายใน ISO 27001 นั้นจำเป็นต้องมีความรู้และทักษะเพียงพอ ซึ่งต้องเตรียมความพร้อมกันล่วงหน้าพอสมควร ในหลายองค์กรนิยมให้ผู้ตรวจประเมินระบบอื่นเช่น ระบบคุณภาพ ISO 9001 (ผ่านการอบรมข้อกำหนดหรือ หลักสูตรการตรวจประเมินภายใน ISO 27001 มาร่วมทีมตรวจ ซึ่งมีข้อดีคือ มีประสบการณ์และทักษะในการถาม การเรียกดูเอกสาร แต่อาจไม่มีความรู้เชิงลึกในด้านไอที ปัญหานี้แก้ได้ด้วยการจัดทีมให้มีผู้รู้ด้านไอทีร่วมทีมไปด้วยเป็นการเรียนรู้ไปด้วยกัน (Pryn Sereepong, 2557)

ประโยชน์ในการเข้าจดทะเบียนตลาดหลักทรัพย์

เป็นแหล่งระดมทุนระยะยาวสำหรับธุรกิจขนาดใหญ่ที่มีผลการดำเนินงานมาอย่างต่อเนื่อง เพื่อใช้เป็นเงินทุนหมุนเวียนหรือขยายธุรกิจ รวมทั้งช่วยให้มีโครงสร้างทางการเงินที่เหมาะสมต่อการดำเนินกิจการ ซึ่งก่อให้เกิดความได้เปรียบในด้านการแข่งขัน เพิ่มพลังให้ธุรกิจและตอบสนองโอกาสทางการเงิน

ประโยชน์ในการเข้าจดทะเบียน

1. ประโยชน์ต่อบริษัท

1.1 แหล่งระดมเงินทุนระยะยาว

บริษัทสามารถระดมทุนจากประชาชนเพื่อนำไปใช้ เป็นเงินทุนหมุนเวียนหรือขยายธุรกิจได้โดยง่ายและรวดเร็ว ซึ่งก่อให้เกิดความได้เปรียบในด้านการแข่งขัน รวมทั้งช่วยให้มีโครงสร้างทางการเงินที่เหมาะสมต่อการดำเนินกิจการ นอกจากนี้ยังเป็นการเปิดโอกาสในการเลือกระดมทุนผ่านการออกหลักทรัพย์ประเภทอื่นๆ ได้ง่ายขึ้นภายหลังการเข้าจดทะเบียน เช่น หุ้นกู้ หุ้นกู้แปลงสภาพ เป็นต้น

1.2 ภาพลักษณ์

การเข้าเป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์ฯ จะช่วยเสริมสร้างภาพลักษณ์ที่ดีในฐานะที่บริษัทได้ผ่านการพิจารณาจาก สำนักงานคณะกรรมการ ก.ล.ต. และคณะกรรมการตลาดหลักทรัพย์ฯ ซึ่งถือได้ว่าเป็นบริษัทที่มีผลการดำเนินงานที่ดี และมีฐานะมั่นคงในระดับหนึ่ง รวมทั้งมีการเปิดเผยข้อมูลที่โปร่งใส ภาพลักษณ์ที่ดีนี้จะก่อให้เกิดคุณประโยชน์ในด้านต่าง ๆ ที่เกี่ยวข้องกับการประกอบธุรกิจของบริษัท เช่น ความน่าเชื่อถือ อำนาจในการต่อรอง และสร้างความตระหนักตลอดจนความนิยมในผลิตภัณฑ์/บริการของกิจการโดยทางอ้อม นอกจากนี้การเผยแพร่ข่าวสารและความเคลื่อนไหวของบริษัทผ่านสื่อต่าง ๆ ของตลาดหลักทรัพย์ฯ ล้วนเป็นสิ่งที่สามารถเกื้อกูลต่อกิจการของบริษัทให้เป็นที่รู้จักและยอมรับของสาธารณชนมากยิ่งขึ้น คุณประโยชน์นี้หากสามารถตีค่าเป็นตัวเงินแล้วย่อมหมายถึงค่าใช้จ่ายมูลค่ามหาศาลสำหรับคู่แข่งที่มิได้อยู่ในตลาดหลักทรัพย์ฯ ที่จะต้องใช้ในการโฆษณาหรือประชาสัมพันธ์ให้เป็นที่รู้จักและยอมรับของสาธารณชน

1.3 จุดเริ่มต้นในการเชื่อมโยงหรือขยายธุรกิจกับธุรกิจต่างประเทศ

ในยุคโลกาภิวัฒน์การประกอบธุรกิจระหว่างประเทศได้ทวีความสำคัญมากขึ้น การมีแนวร่วมโดยเฉพาะแนวร่วมจากกิจการในต่างประเทศที่สามารถเกื้อกูลระหว่างกันทั้งในด้านการตลาด การผลิต เทคโนโลยี การเงิน และบุคลากร ย่อม

ส่งผลให้เกิดความได้เปรียบในเชิงแข่งขัน การเป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์ฯ ย่อมเป็นจุดเริ่มต้นที่ดี และเป็นแรงจูงใจให้เกิดความสนใจในการเข้าร่วมลงทุนจากธุรกิจต่างชาติซึ่งจะเกื้อหนุนให้เกิดการขยายตัวทางธุรกิจอย่างต่อเนื่องและสามารถเพิ่มความแข็งแกร่งให้แก่บริษัทมากยิ่งขึ้น

1.4 การสร้างความรับผิดชอบและการบริหารแบบมืออาชีพ

การเข้าจดทะเบียนในตลาดหลักทรัพย์ฯ จะมีส่วนช่วยกระตุ้นให้บริษัทบริหารงานได้อย่างมีประสิทธิภาพ และรัดกุมมากขึ้นเนื่องจากบริษัทจะอยู่ในความสนใจของผู้ลงทุนโดยมีราคาหุ้นของบริษัทเป็นตัวสะท้อนความเชื่อมั่นของสาธารณชนที่มีต่อกิจการในระดับหนึ่ง ในขณะเดียวกันการเข้าจดทะเบียนก็จะเป็นเครื่องมือ ในการกำกับดูแลการบริหารกิจการให้เป็นไปในทิศทางที่ควรจะเป็น ซึ่งจะช่วยเสริมสร้างประสิทธิภาพตลอดจนเพิ่มพูนประสิทธิผลในการประกอบธุรกิจอันจะเป็นผลประโยชน์แก่ทุกฝ่ายที่มีส่วนเกี่ยวข้องกับบริษัทโดยรวม

1.5 ความภาคภูมิใจของบุคลากรของบริษัท

คุณประโยชน์ที่สำคัญประการหนึ่งที่มักจะถูกมองข้ามจากการที่บริษัทเข้าจดทะเบียนในตลาดหลักทรัพย์ฯ คือ ความภาคภูมิใจของพนักงานของบริษัท โดยหากบริษัทนั้นมีผลประกอบการและภาพลักษณ์ที่ดีมีชื่อเสียงเป็นที่ยอมรับ และรู้จักกันอย่างแพร่หลายย่อมทำให้บุคลากรของบริษัทเกิดความรู้สึกที่ดีต่อบริษัท หากผู้บริหารรู้จักใช้สิ่งนี้ให้เป็นประโยชน์โดยการสร้างความยึดมั่นหรือค่านิยมร่วม (shared value) ให้เกิดขึ้นในลักษณะของการกระตุ้นให้บุคลากรทุกฝ่ายได้ตระหนัก และมีส่วนร่วมต่อการสร้างชื่อเสียงและเกียรติคุณของบริษัท คุณประโยชน์อันมหาศาลย่อมจะเกิดขึ้นกับบริษัทในระยะยาว

1.6 สิทธิประโยชน์ทางภาษีเงินปันผล

บริษัทจดทะเบียนจะได้รับสิทธิประโยชน์ทางภาษีในกรณีที่บริษัทจดทะเบียนไปถือหุ้นของบริษัทอื่นที่จัดตั้งตามกฎหมายไทยหรือกองทุนรวม เงินปันผลที่ได้รับจากบริษัทอื่นดังกล่าวจะได้รับการยกเว้นภาษีเงินได้ แต่เงินที่ได้รับดังกล่าวต้องเป็นเงินที่ได้รับจากหุ้นหรือหน่วยลงทุนที่ถือไว้ไม่น้อยกว่า 3 เดือนก่อน และหลังวันที่ได้รับเงินได้

2. ประโยชน์ต่อผู้ถือหุ้น

2.1 เสริมสร้างสภาพคล่อง

การเป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์ฯ ช่วยเสริมสร้างสภาพคล่องให้กับผู้ถือหุ้นของบริษัท เนื่องจากผู้ถือหุ้นสามารถซื้อขายเปลี่ยนมือหรือเปลี่ยนเป็น

เงินสดได้สะดวก และง่ายในเวลาที่ต้องการตลอดจนทราบมูลค่าที่แท้จริงของหุ้นตามความต้องการของตลาด และใช้เป็นหลักประกันในการกู้ยืมได้

2.2 ความคุ้มครองในการลงทุน

ผู้ถือหุ้นจะได้รับความคุ้มครองในการลงทุน เนื่องจากตลาดหลักทรัพย์ฯ มีกฎระเบียบในการกำกับการซื้อขายหลักทรัพย์ และการเปิดเผยข้อมูลเพื่อให้เกิดความเป็นธรรมต่อผู้ถือหุ้น ตลอดจนให้ผู้ถือหุ้นและผู้ลงทุนได้รับข้อมูลที่ถูกต้องพอเพียงทันเวลา และเท่าเทียมกัน

2.3 สิทธิประโยชน์ทางภาษี

บุคคลธรรมดาที่เป็นผู้ถือหุ้นในบริษัทจดทะเบียนจะได้รับสิทธิประโยชน์ทางภาษี ดังนี้

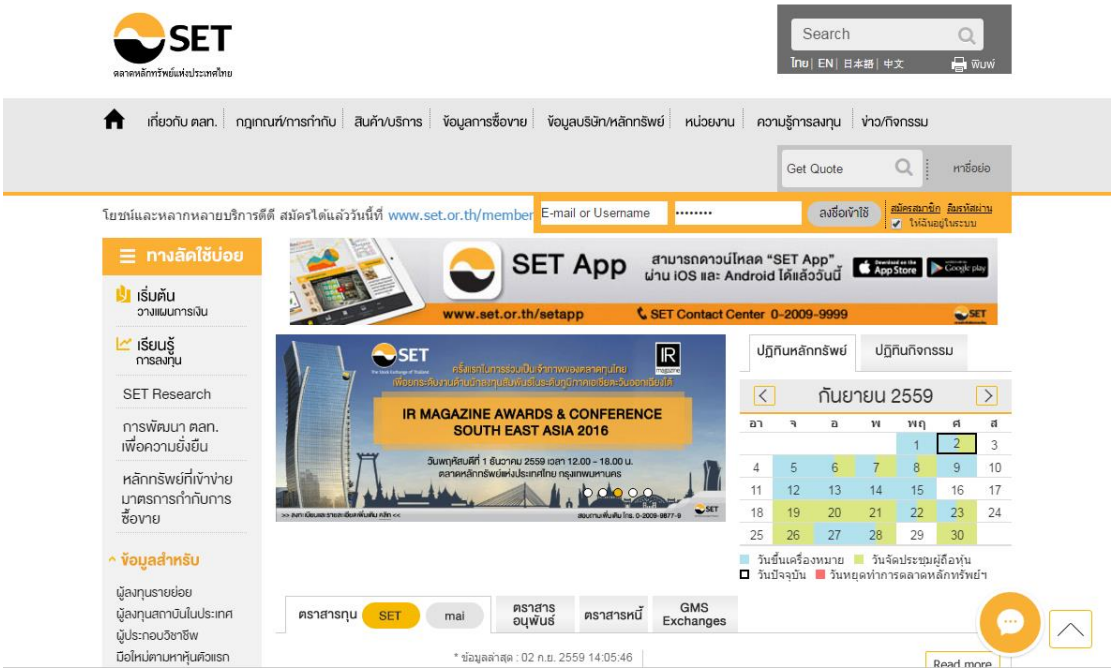
- เงินได้จากการขายหลักทรัพย์ในตลาดหลักทรัพย์ฯ ได้รับยกเว้นไม่ต้องนำมารวมคำนวณเพื่อเสียภาษี
- ผู้มีเงินได้ซึ่งได้รับเงินปันผลจากบริษัทจดทะเบียนจะถูกหักภาษี ณ ที่จ่าย 10% โดยผู้มีเงินได้ซึ่งอยู่ในประเทศไทย มีสิทธิที่จะเลือกดำเนินการดังนี้
  - ไม่นำเงินปันผลดังกล่าวมารวมคำนวณเพื่อเสียภาษีเงินได้ เฉพาะผู้มีเงินได้ที่ไม่ขอรับเงินภาษีที่ถูกหักไว้คืนหรือไม่ขอเครดิตภาษีที่ถูกหักไว้นั้นไม่ว่าทั้งหมดหรือบางส่วน หรือ
  - นำเงินปันผลดังกล่าวมารวมคำนวณเพื่อเสียภาษีเงินได้ โดยจะได้รับการเครดิตภาษีคืนในภายหลัง ยกตัวอย่างเช่น ผู้มีเงินได้จะได้รับการเครดิตภาษี 3 ใน 7 ของเงินปันผลที่ได้รับในกรณีที่บริษัทจดทะเบียนที่มีการจ่ายเงินปันผลนั้นได้เสียภาษีเงินได้นิติบุคคล (มูลค่าของการเครดิตภาษีสามารถคำนวณได้จากสูตร X/(100 - x) โดย x คืออัตราภาษีเงินได้ที่บริษัทได้เสียอยู่)

(ตลาดหลักทรัพย์แห่งประเทศไทย, ม.ป.ป.)

2.3 เว็บไซต์ที่เกี่ยวข้อง

รูปที่ 2.5 http://www.club27001.com

เป็นเว็บไซต์ที่ให้ความรู้และข้อมูล เกี่ยวกับเรื่องมาตรฐานความมั่นคงปลอดภัยระบบสารสนเทศ ISO 27001:2013 บอกถึงความเป็นมา โครงสร้าง ข้อกำหนดของมาตรฐานและแนวทางการตรวจสอบมาตรฐาน



รูปที่ 2.6 http://www.set.or.th

เป็นเว็บไซต์ที่ให้ความรู้และข้อมูลเกี่ยวกับเรื่องตลาดหลักทรัพย์ ความเป็นมาของตลาดหลักทรัพย์และประโยชน์ของการเข้าตลาดหลักทรัพย์