เรื่อง: มาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติต่างๆ ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ
เรียบเรียงโดย: น.ส.ดวงกมล ทรัพย์พิทยากร
ตรวจทานโดย: ดร.บรรจง หะรังษี ดร.โกเมน พิบูลย์โรจน์ นายพุธ นาฑีสุวรรณ และ น.ส.ศิริวรรณ อภิสิริเดช
เผยแพร่วันที่: 28 กุมภาพันธ์ 2550

บทนำ

ปัจจุบันเรื่องของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guidance) และกรอบวิธีปฏิบัติ (Framework) ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเริ่มได้รับความสนใจจากองค์กรที่ใช้งานระบบเทคโนโลยีสารสนเทศเพิ่มมากขึ้น ทั้งนี้ องค์กรมุ่งหวังว่าสิ่งเหล่านี้จะสามารถนำมาช่วยประเมินการวัดประสิทธิภาพและประสิทธิผลของการจัดทำและพัฒนาระบบสารสนเทศเพื่อใช้งานในองค์กร ช่วยปรับปรุงกระบวนการด้านเทคโนโลยีสารสนเทศ ช่วยบริหารจัดการด้านคุณภาพของระบบตลอดจนช่วยเสริมสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศขององค์กร

อย่างไรก็ดี ความมุ่งหวังขององค์กรจะเป็นไปตามที่กล่าวมาข้างต้นหรือไม่ ขึ้นอยู่กับการจะเลือกใช้มาตรฐาน แนวทางปฏิบัติ หรือกรอบวิธีปฏิบัติใดมาสนับสนุนวิสัยทัศน์ ยุทธศาสตร์ และพันธกิจขององค์กร องค์กรต้องศึกษาและพิจารณาคัดเลือกมาตรฐาน แนวทางปฏิบัติ หรือกรอบวิธีปฏิบัติ ที่เหมาะสมตามรูปแบบและแนวทางที่สิ่งเหล่านั้นได้รับการพัฒนามา และควรต้องนำมาประยุกต์ใช้แบบค่อยเป็นค่อยไปตามแต่กำลังขององค์กร

นอกจากนี้ยังมีปัจจัยอื่นที่ควรพิจารณาร่วมด้วย อาทิ วัตถุประสงค์ของมาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติที่กลุ่มผู้จัดทำได้นิยามไว้ การได้คัดเลือกมาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติที่ตรงกับสิ่งที่องค์กรต้องการจะนำมาซึ่งประโยชน์และความคุ้มค่าต่อไป เช่น องค์กรที่ดำเนินธุรกิจเกี่ยวกับการเงินหรือการให้บริการชำระเงินผ่านสื่ออิเล็กทรอนิกส์ จะให้ความสำคัญกับมาตรฐานด้านความมั่นคงปลอดภัยเป็นหลัก เนื่องจากต้องปฏิบัติตามข้อกำหนดของธนาคารแห่งประเทศไทย ซึ่งได้แก่ มาตรฐาน ISO 27001 เป็นต้น

บทความนี้จึงได้รวบรวม มาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ประกอบด้วย COBIT Framework, COSO, ITIL, ISO/IEC 27001, 17799:2005, FIPS PUB 200, ISO/IEC 13335, ISO/IEC 15408-2005/Common Criteria /ITSEC, PRINCE2, PMBOK, TickIT, TOGAF8.1, IT Baseline Protection Manual และ มาตรฐาน NIST 800-14 มาแนะนำในเบื้องต้น และได้จัดทำแหล่งข้อมูลสำหรับศึกษาเพิ่มเติมไว้ในย่อหน้าสุดท้ายของสิ่งที่กล่าวถึง สำหรับแหล่งข้อมูลหลักผู้ศึกษาได้อ้างอิงมาจากบทความเรื่อง COBIT Mapping Overview of International IT Guidance, 2rd Edition เผยแพร่โดย IT Governance Institute (ITGI) ประเทศสหรัฐอเมริกา

จากที่ได้กล่าวมาข้างต้นแวดวงเทคโนโลยีสารสนเทศนอกจากจะมีพัฒนาการอย่างต่อเนื่องแล้ว มาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติที่นำมากล่าวถึงก็ได้รับการพัฒนาตามมาและล้วนมีสาระสำคัญที่ผู้ใช้งานระบบเทคโนโลยีสารสนเทศทั้งหลายควรได้ศึกษา ทำความเข้าใจไปพร้อมๆ กับการใช้งานและแน่นอนว่าเมื่อได้ทำการศึกษาและทำความเข้าใจแล้ว ผู้อ่านจะได้คัดสรร หรือเลือกสิ่งเหล่านี้ไปประยุกต์ใช้ได้ตรงกับงาน และท้ายที่สุดก็จะเป็นการช่วยเสริมสร้างให้ระบบสารสนเทศขององค์กรได้รับการบริหารจัดการ หรือพัฒนาปรับปรุงอย่างต่อเนื่องด้วยความเหมาะสมต่อไป

บทแนะนำ มาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติต่างๆ

COBIT

กรอบวิธีปฏิบัติ COBIT (Control Objectives for Information and related Technology) เป็นรูปแบบวิธีปฏิบัติที่ถูกพัฒนาขึ้นโดยกลุ่มความร่วมมือที่ชื่อว่า Information Systems Audit and Control Association (ISACA) ใช้สำหรับองค์กรที่ต้องการมุ่งสู่การพัฒนาให้ระบบเทคโนโลยีสารสนเทศมีความเป็น "ไอทีภิบาล" หรือ "IT Governance" กล่าวคือ สามารถบริหารจัดการระบบสารสนเทศขององค์กรให้สามารถใช้งานได้อย่างมีประสิทธิภาพ มีความคุ้มค่ากับการลงทุน ดังนั้น กรอบวิธีปฏิบัตินี้จึงมีตัววัดในระดับของการดำเนินการในแต่ละกระบวนการ และได้รับความนิยมใช้กันโดยแพร่หลายในกลุ่มธุรกิจด้านการเงินและการธนาคาร สำหรับเนื้อหาของกรอบวิธีปฏิบัติ COBIT เวอร์ชั่น 3 มีเนื้อหาหลักๆ แบ่งเป็น 4 ด้านดังนี้

1) Planning and Organization (PO) ประกอบด้วยวัตถุประสงค์จำนวน 10 ข้อ
2) Acquisition and Implementation (AI) ประกอบด้วยวัตถุประสงค์จำนวน 7 ข้อ
3) Delivery and Support (DS) ประกอบด้วยวัตถุประสงค์จำนวน 13 ข้อ
4) Monitoring (M) ประกอบด้วยวัตถุประสงค์จำนวน 4 ข้อ

กรอบวิธีปฏิบัติ COBIT นั้น แรกเริ่มเดิมทีได้รับการเผยแพร่ในรูปแบบของกระบวนการด้านเทคโนโลยีสารสนเทศ (IT process) และใช้เป็นกรอบวิธีปฏิบัติเพื่อควบคุมกระบวนการด้านเทคโนโลยีสารสนเทศที่เชื่อมโยงกับความต้องการทางธุรกิจ

ขณะเดียวกันกรอบวิธีปฏิบัติ COBIT ก็ถูกนำไปใช้เป็นแนวทางในการระบุการดำเนินงานทางธุรกิจแต่ละกระบวนการกับเจ้าของกระบวนการด้านเทคโนโลยีสารสนเทศนั้นๆ เช่น กระบวนการพัฒนาแอพพลิเคชั่น มีเจ้าของกระบวนการคือผู้ที่เป็นผู้ให้ requirement แก่ผู้พัฒนาระบบและเป็นผู้ใช้งานโดยตรง แต่สำหรับภาครัฐอาจมีการจ้างบริษัทรับจ้างเหมาพัฒนาแอพพลิเคชั่น แต่กระนั้น เมื่อระบุผู้ที่เป็นเจ้าของกระบวนการ การระบุก็จะต้องระบุถึงหน่วยงานภาครัฐนั้นว่าเป็นเจ้าของกระบวนการพัฒนาแอพพลิเคชั่น ไม่ใช่ผู้รับเหมา

การมีเจ้าของกระบวนการที่ชัดเจนทำให้การดำเนินการภายในต้องมีความชัดเจนด้วย ต้องมีการกำหนดความต้องการของระบบ โดยผู้เป็นเจ้าของระบบ เช่น แอพพลิเคชั่นนี้มี requirement อะไรบ้างที่พัฒนาแล้วต้องสามารถสอดรับกับภารกิจของหน่วยงานที่เป็นเจ้าของระบบ หรือต้องมีการกำหนดหัวข้อ security requirement ไว้เป็นหัวข้อหนึ่งใน Term of Reference (TOR) เพื่อกำหนดเป็น requirement ให้กับผู้รับเหมาในการพัฒนาว่าแอพพลิเคชั่นนี้ต้องรองรับการกรอกข้อมูลที่เป็นการรันคำสั่งทางไกลเพื่อบุกรุกระบบ เป็นต้น

ดังนั้น การมีเจ้าของกระบวนการหรือการที่สามารถระบุได้ว่าหน่วยงานใดเป็นเจ้าของกระบวนการบ้าง การระบุดังกล่าวจะช่วยให้มีผู้รับผิดชอบเป็นเจ้าของกระบวนการ และจะต้องมีหน้าที่ผูกพันกับกระบวนการนั้นๆ ในการดูแลรับผิดชอบและรักษาความปลอดภัยของสารสนเทศในแต่ละกระบวนการ

ภายหลัง ผู้พัฒนา COBIT ได้มีการเพิ่มเติมแนวทางปฏิบัติ (Management Guidelines) เพื่อเสริมสร้างการให้บริการด้านเทคโนโลยีสารสนเทศให้มีคุณภาพมากยิ่งขึ้น เมื่อมีผู้ใช้กรอบวิธีปฏิบัติ COBIT มากขึ้น กลุ่มผู้พัฒนาจึงได้มีการจัดทำเครื่องมือช่วยในการบริหารจัดการ เช่น บรรดา Checklist ที่ระบุไว้ในกระบวนการต่างๆ ซึ่งจะช่วยในเรื่องของการกำหนดตัวชี้วัดและเป็นการยกระดับในการพัฒนาตัวชี้วัดเหล่านี้สามารถคำนวณเป็นตัวเลขที่สามารถวัดประสิทธิภาพและประสิทธิผลได้อีกด้วย (Metrics and Maturity models)

ด้วยเหตุนี้ COBIT จึงกลายเป็นมาตรฐานหรือกรอบวิธีปฏิบัติที่ใช้งานด้านธุรกิจกันอย่างแพร่หลายและถูกนำไปประยุกต์ใช้มากขึ้นในด้านของการใช้เป็นกรอบวิธีปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพและประสิทธิผลหรือมีความคุ้มค่าในการใช้งานระบบเทคโนโลยีสารสนเทศ หรือ IT Governance นั่นเอง

กล่าวโดยสรุป กรอบวิธีปฏิบัติ COBIT สามารถอธิบายเป็นภาพกว้างๆ โดยพิจารณาจากระดับบนลงล่าง (Top-Down approach) หัวข้อใหญ่ (Domains) -> กระบวนการต่างๆ (Processes) -> กิจกรรมหรือหน้าที่งานต่างๆภายใต้กระบวนการนั้น (Activities/Tasks) อย่างไรก็ตาม กรอบวิธีปฏิบัตินี้มุ่งเน้นในการยกระดับประสิทธิภาพของระบบเทคโนโลยีสารสนเทศที่เป็นส่วนผลักดันงานขององค์กรมากกว่าความมุ่งเน้นทางด้านการรักษาความมั่นคงปลอดภัยเท่ากับมาตรฐาน ISO/IEC 27001

แหล่งข้อมูลเพิ่มเติม

http://www.isaca.org/cobit
http://www.itgi.org/
http://www.sei.cmu.edu/cmmi

COSO

COSO ย่อมาจาก ได้รับการจัดทำและเผยแพร่โดย Committee of Sponsoring Organisations of the Treadway Commission กล่าวอีกนัยหนึ่ง COSO เป็นกรอบวิธีปฏิบัติที่จะช่วยส่งเสริมให้การตรวจสอบกิจการภายในองค์กรหรือ Internal Control ให้มีความเที่ยงตรงต่อหลักการและโปร่งใสมากขึ้น โดยเฉพาะอย่างยิ่งองค์กรด้านการเงิน

ประเด็นที่กรอบวิธีปฏิบัติ COSO เน้น ได้แก่ เรื่องของคุณภาพในการจัดทำงบการเงินซึ่งหมายถึง ความน่าเชื่อถือถูกต้องและก็เป็นไปตามหลักความจริงนั่นเอง และอีกสองส่วนสำคัญคือ จริยธรรมต่อการตรวจสอบภายในอย่างมีประสิทธิภาพหรือการรายงานตามสิ่งที่พบนั่นเอง ผู้ตรวจสอบจะต้องมีจริยธรรม รักษาจรรยาชีพของตน ไม่ใช่เอาหูไปนา เอาตาไปไร่ไม่สนใจที่จะทำการตรวจสอบอย่างแท้จริง เช่น กรณีที่เห็นว่างบการเงินมีกำไรผิดสังเกตแต่ก็มิได้ทักท้วง เป็นต้น

เมื่อนำกรอบวิธีปฏิบัติ COSO ไปใช้แล้วจะช่วยในการลดความเสี่ยงต่อไปนี้ได้ กล่าวคือ

- ความเสี่ยงเกี่ยวกับมาตรการที่ขาดการควบคุมอย่างเป็นระบบ (Non-systematic approach for controls)
- มาตรการควบคุมที่ไม่สมบูรณ์ (Incomplete control)
- มาตรการควบคุมที่ไม่มีประสิทธิภาพ (Inefficient controls)
- การจัดทำรายงาน หรือขั้นตอนปฏิบัติที่มีอยู่ไม่รัดกุมเพียงพอ อันเนื่องมาจากขาดมาตรการในการควบคุม (Inadequate processes and reporting due to a lack of controls) COSO ประกอบด้วยเนื้อหาหลักๆ 4 ประเภท ดังนี้

1) Executive summary
2) Framework
3) Reporting to External parties
4) Evaluation tools

เนื้อหาส่วนใหญ่จะเน้นไปในด้านของคุณภาพในการจัดทำรายงานงบการเงินและจรรยาบรรณแห่งวิชาชีพผู้ตรวจสอบ ที่ผู้ตรวจสอบภายในต้องเคร่งครัดในการตรวจสอบเพื่อควบคุมทั้งสถานะทางการเงิน และจริยธรรมในการทำงานของผู้บริหารเพื่อป้องกันการเกิดคอรับชั่นภายในองค์กร

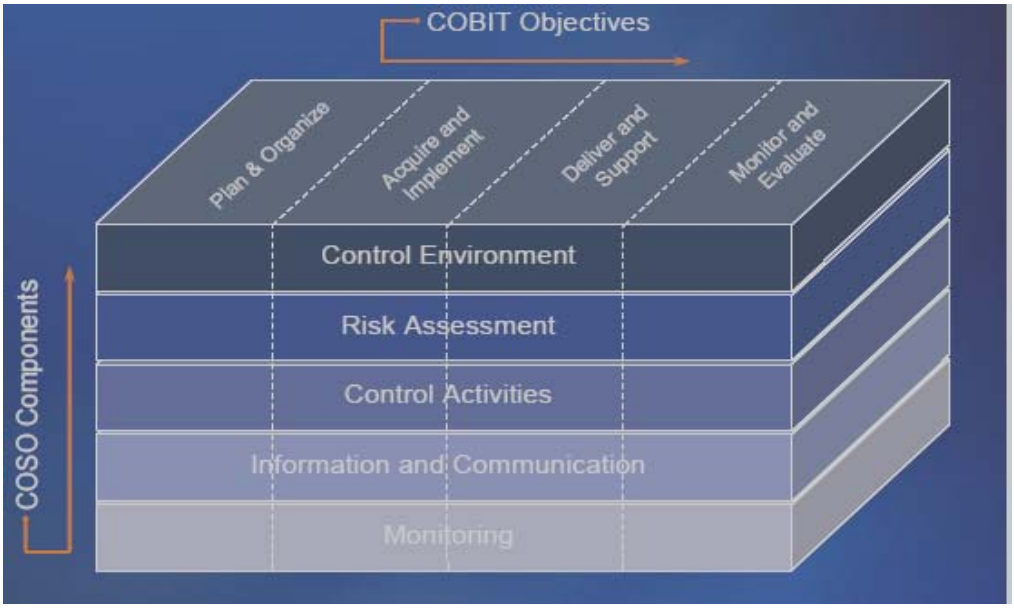
เป้าหมายของการใช้กรอบควบคุม COSO เพื่อที่จะปรับปรุงวิธีการต่างๆ ที่ใช้ควบคุมผู้ประกอบการโดยนำไปผนวกรวมกับระบบควบคุม/ตรวจสอบกิจการภายใน กรอบควบคุม COSO สามารถทำให้ผู้บริหารอาวุโสจัดทำการควบคุมภายในให้มีขึ้นในองค์กรเพื่อที่จะแน่ใจได้ว่าองค์กรกำลังดำเนินงานอย่างเป็นไปตามเป้าประสงค์ และองค์กรได้มีการบริหารจัดการความเสี่ยงในด้านต่างๆ อย่างเหมาะสมแล้ว หรืออาจกล่าวได้ว่า COSO จะช่วยเสริมศักยภาพของการควบคุมตรวจสอบกิจการภายใน

เพื่อให้เข้าใจถึงกรอบวิธีปฏิบัติของ COSO มากยิ่งขึ้น ได้มีการนำเสนอเป็นภาพเปรียบเทียบเป็นมิติระหว่างกรอบ COBIT และ COSO โดยนำ COBIT Objective เป็นตัวตั้ง และภายในจะมีองค์ประกอบของกรอบ COSO บรรจุอยู่ องค์ประกอบของ COSO มี 5 องค์ประกอบหลัก ได้แก่

1) การควบคุมสภาพแวดล้อม
2) การประเมินความเสี่ยง
3) การควบคุมการดำเนินงานหรือกิจกรรมต่างๆ
4) สารสนเทศและการสื่อสาร
5) การติดตามผล

องค์ประกอบทั้ง 5 นี้จะมีสอดแทรกไว้ในแต่ละด้านของ COBIT ซึ่งเริ่มตั้งแต่ การวางแผนและริเริ่ม (Planning &Organize) การกำหนดความต้องการและลงมือปฏิบัติ (Acquire and Implement) การส่งมอบและให้การสนับสนุน (Deliver and Support) การติดตามและประเมินผล (Monitor and Evaluate) ซึ่งในส่วนนี้จะเป็นหัวข้อตาม COBIT เวอร์ชั่น 4 ที่เพิ่งเผยแพร่เมื่อต้นปี 2549

การผสมผสานระหว่างกรอบวิธีปฏิบัติทั้งสองสามารถแสดงเป็นภาพให้ชัดเจนได้ดังนี้



<u>แผนภาพที่ 2</u> แสดงมิติความสัมพันธ์ระหว่างกรอบ COSO และ COBIT เวอร์ชั่น 4

แหล่งข้อมูลเพิ่มเติม www.cpa2biz.com

มาตรฐาน ISO/IEC27001, ISO/IEC17799

มาตรฐานนี้เป็นมาตรฐานสากลที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร และใช้เป็นมาตรฐานอ้างอิงเพื่อเป็นแนวทางในการเสริมสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรอย่างแพร่หลาย โดยแบ่งเนื้อหาออกเป็น 11 หัวข้อใหญ่ๆ (Domain) ซึ่งแต่ละหัวข้อประกอบด้วยวัตถุประสงค์จำนวนแตกต่างกัน รวมแล้วจำนวน 39 วัตถุประสงค์ (Control objectives) และภายใต้วัตถุประสงค์แต่ละข้อประกอบด้วยมาตรการในการรักษาความมั่นคงปลอดภัยแตกต่างกัน รวมแล้วจำนวน 133 ข้อ (Controls) ซึ่งสามารถนำไปประยุกต์ใช้เพื่อรักษาความมั่นคงให้กับระบบสารสนเทศขององค์กรได้

ก่อนจะมาเป็นมาตรฐานสากลนี้ มาตรฐาน ISO/IEC 27001 และ ISO/IEC 17799:2005 ได้รับการแก้ไขปรับปรุงมาจากมาตรฐานเดิมที่ชื่อว่า BS 7799-1 และ ISO/IEC 17799:2000 ตามลำดับ มาตรฐานนี้จะประกอบด้วยเลขหมายในตระกูล 27000 อีกหลายเลขลำดับและองค์กรมาตรฐานสากลจะพัฒนามาตรฐานตระกูล 27000 ออกมาในเร็วๆ นี้ ล่าสุดมาตรฐานที่เป็นข้อกำหนดหรือ specification ของการจัดทำระบบ ISMS ได้ถูกตีพิมพ์และเผยแพร่ในลำดับของ ISO/IEC 27001 เมื่อเดือนตุลาคม 2548 ซึ่งทีมงานพัฒนามาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ภายใต้ โครงการ ThaiCERT และศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ได้จัดทำและเผยแพร่ไว้บนเว็บไซต์ของโครงการเป็นภาษาไทยแล้ว และสามารถศึกษาได้ตามลิ้งค์ที่ปรากฏในแหล่งข้อมูลเพิ่มเติม

ความแตกต่างระหว่างมาตรฐาน ISO/IEC27001 กับ ISO/IEC17799-2005 สามารถอธิบายโดยย่อได้ดังนี้

มาตรฐาน ISO/IEC27001 ว่าด้วยเรื่องของข้อกำหนดในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยหรือ ISMS ให้กับองค์กร มีหัวข้อที่เกี่ยวข้องได้แก่

1) ขอบเขต (Scope)
2) ศัพท์เทคนิคและนิยาม (Terms and definitions)
3) โครงสร้างของมาตรฐาน (Structure of this standard)
4) การประเมินความเสี่ยงและการจัดการกับความเสี่ยง ลด/ โอนย้าย/ ยอมรับความเสี่ยง (Risk assessment and treatment)

มาตรฐาน ISO/IEC 27001 นี้ปัจจุบันได้รับความนิยมอย่างแพร่หลายเนื่องจากประกอบด้วยวงจร Plan-Do-Check-Act และใช้แนวทางการประเมินความเสี่ยงมาประกอบการพิจารณาหาวิธีการหรือมาตรการเพื่อป้องกัน ลดความเสี่ยง และรักษาทรัพย์สินสารสนเทศที่มีค่าขององค์กรให้มีความมั่นคงปลอดภัยในระดับที่เหมาะสม

สำหรับมาตรฐาน ISO/IEC 17799-2005 ว่าด้วยเรื่องของวิธีปฏิบัติที่จะนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัยที่องค์กรได้จัดทำขึ้น ซึ่งจะต้องเป็นไปตามข้อกำหนดในมาตรฐาน ISO/IEC 27001 รายละเอียดของมาตรฐานนี้จะบอกถึงวิธีปฏิบัติในการลดความเสี่ยงที่เกิดจากจุดอ่อนของระบบโดยแบ่งเป็นหัวข้อหลักที่เกี่ยวข้องกับระบบ และให้แนวทางว่าผู้จัดทำควรปฏิบัติอย่างไร ซึ่งผู้ใช้สามารถเพิ่มเติมมาตรการหรือใช้วิธีการที่มีความมั่นคงปลอดภัยเพียงพอ หรือเหมาะสมตามที่องค์กรได้ประเมินไว้

หัวข้อสำคัญหรือ 11 โดเมนหลักในมาตรฐาน ISO/IEC 17799-2005 มีดังนี้

1) นโยบายความมั่นคงปลอดภัยขององค์กร (Security policy)
2) โครงสร้างความมั่นคงปลอดภัยภายในองค์กร (Organization of information security)
3) การจัดหมวดหมู่และการควบคุมทรัพย์สินขององค์กร (Asset management)
4) มาตรฐานของบุคลากรเพื่อสร้างความมั่นคงปลอดภัยให้กับองค์กร (Human resources security)
5) ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร (Physical and environmental security)
6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)
7) การควบคุมการเข้าถึงระบบสารสนเทศขององค์กร (Access control)
8) การพัฒนาและดูแลระบบสารสนเทศ (Information systems acquisition, development and maintenance)
9) การบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัย (Information security incident management)
10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)
11) การปฏิบัติตามข้อกำหนดทางด้านกฎหมายและบทลงโทษของการละเมิดนโยบาย (Compliance)

นอกจากมาตรฐาน ISO/IEC 27001 นี้จะเป็นมาตรฐานสากลที่ใช้กันอย่างแพร่หลายแล้ว ในด้านข้อมูลเชิงลึกพบว่ามีบริษัทหรือองค์กรทั่วโลกที่ผ่านการรับรองตามมาตรฐานนี้ ประมาณสองพันกว่ารายแล้ว

ดังนั้นความพร้อมใช้ของมาตรฐานนี้ และความสำคัญของการเป็นมาตรฐานที่ว่าด้วยเรื่องของความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ มาตรฐานนี้จึงควรศึกษาและให้ความสำคัญเป็นอันดับต้นๆ

แหล่งข้อมูลเพิ่มเติม

- http://www..iso27001security.com/html/iso17799.html
- http://www.thaicert.nectec.or.th
- Information technology—Security techniques—Information security management systems—Requirements, ISO/IEC27001:2005(E) International Standard, First Edition 2005-10-15.
- Information technology—Security techniques—Code of practice for information security management, ISO/IEC17799:2005(E) International Standard, Second Edition 2005-06-15.

ISO/IEC TR 13335

มาตรฐานนี้ ย่อมาจาก Guidelines for the Management of IT Security ซึ่งเป็น technical report และมาตรฐาน ISO/IEC 27001 ได้มีการอ้างอิงมายังมาตรฐาน ISO/IEC 13335 ในเรื่องของการจัดทำ technical report ซึ่งเริ่มต้นจากการระบุภัยคุกคาม จุดอ่อนหรือช่องโหว่ของระบบเทคโนโลยีสารสนเทศ แนวทางการประเมินความเสี่ยงต่างๆ จนสามารถระบุแนวทางเพื่อลดความเสี่ยงได้ สำหรับเนื้อหาหลักของมาตรฐานนี้จะแบ่งเป็น 5 ส่วนสำคัญ ดังนี้

1. การบริหารจัดการหน้าที่งานต่างๆของความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศที่ได้รับการวางโครงร่างไว้ รวมถึงจัดหาแนวคิดด้านความมั่นคงปลอดภัยให้เป็นไปตามโครงร่างที่ได้ตั้งไว้ ทั้งรูปแบบสารสนเทศและเทคโนโลยีที่ใช้ในการติดต่อสื่อสาร
2. การนำไปปฏิบัติและการบริหารจัดการด้านความมั่นคงปลอดภัยต้องได้รับการจัดทำด้วยวิธีการที่เหมาะสมที่สุด
3. เทคนิคสำหรับการบริหารจัดการด้านความมั่นคงปลอดภัยต้องได้รับการจัดการให้จากผู้จัดทำระบบเทคโนโลยีสารสนเทศ
4. ต้องให้แนวทางปฏิบัติสำหรับการเลือกวิธีการรักษาความมั่นคงปลอดภัย ซึ่งพิจารณาจากประเภทของระบบไอทีนั้นๆ รวมถึงความตระหนักด้านความมั่นคงปลอดภัยและภัยคุกคามที่อาจมีขึ้นในอนาคต
5. สารสนเทศที่อยู่บนระบบกรณีที่ต้องมีการส่งผ่านสายสื่อสาร ต้องได้รับการรักษาความมั่นคงปลอดภัยในระหว่างการส่งและต้องจัดให้เครือข่ายมีความมั่นคงปลอดภัยด้วย

แหล่งข้อมูลเพิ่มเติม www.nist.org
http://csrc.nist.gov/publications

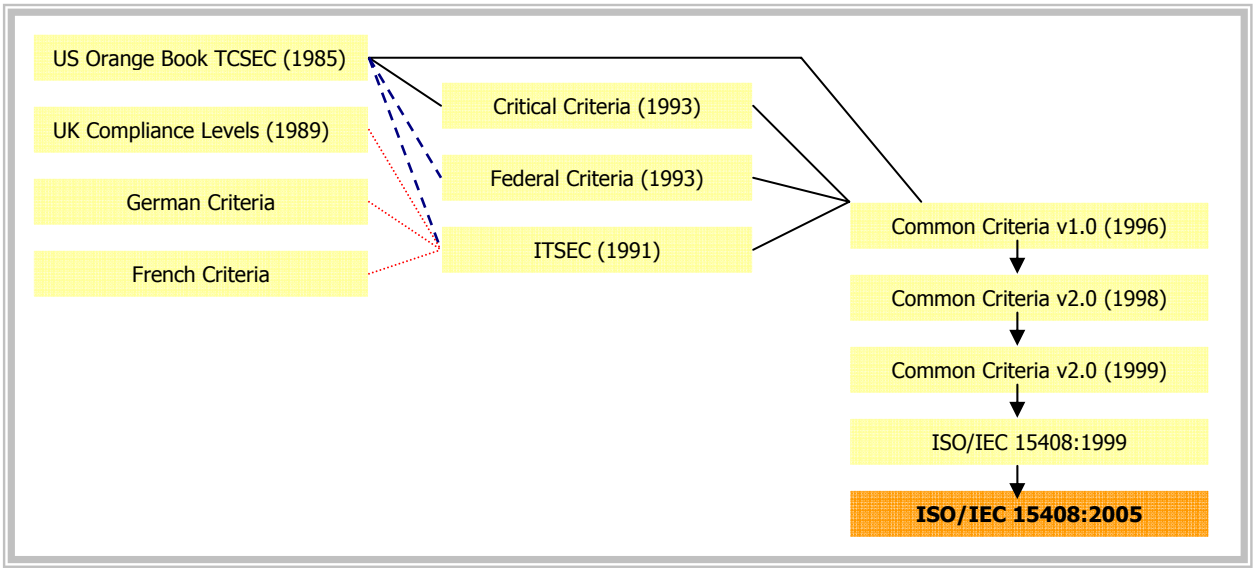
ISO/IEC 15408:2005/Common Criteria/ ITSEC

มาตรฐานนี้ได้รับการพิมพ์เผยแพร่โดย ISO/IEC JTC1 กลุ่มองค์กรที่ให้ความร่วมมือกันจัดทำมาตรฐานกลางหรือข้อกำหนดร่วมที่เรียกว่า Common Criteria โดยส่วนใหญ่เป็นองค์กรในกลุ่มประเทศยุโรป เป้าหมายในการร่างมาตรฐานกลางหรือข้อกำหนดร่วมนี้จัดทำขึ้นเพื่อใช้เป็นเกณฑ์กลางในการวัดระดับความมั่นคงปลอดภัยว่าระบบต่างๆ ที่จัดทำขึ้นเมื่อนำมาเปรียบเทียบกับเกณฑ์นี้แล้วระบบนั้นจะมีความมั่นคงปลอดภัยอยู่ในระดับใด

ทั้งนี้ การที่มีตัวแทนองค์กรมาร่วมกันกำหนดมาตรฐานกลางนี้ก็เพื่อความยุติธรรมในการสร้างข้อกำหนดองค์กรต่างๆ ที่เข้ามาร่วมกันดำเนินการในเรื่องนี้ได้แก่

- องค์กร Communication Security Establishment จากประเทศแคนาดา
- องค์กร Central Service of the Information จากประเทศฝรั่งเศส
- องค์กร Federal Office for Security in Information Technology จากประเทศเยอรมันนี
- องค์กร The Netherlands National Communications Security Agency จากประเทศเนเธอร์แลนด์
- องค์กร Communications-Electronics Security Group จากประเทศสหราชอาณาจักรอังกฤษ และ
- องค์กร National Institute of Standards and Technology and National Security Agency จากประเทศสหรัฐอเมริกา

แผนผังต่อไปนี้จะแสดงพัฒนาการของมาตรฐานกลาง ISO/IEC 15408:2005 ที่ได้รับการพัฒนามาจากมาตรฐานกลางของกลุ่มความร่วมมือดังกล่าว จนในที่สุดได้กลายเป็นมาตรฐานกลางในเวอร์ชั่นปัจจุบัน



<u>แผนภาพที่ 3</u> แสดงพัฒนาการของมาตรฐานกลาง ISO/IEC 15408:2005 ที่มีพัฒนามาจากมาตรฐานกลางต่างๆ ของกลุ่มความร่วมมือ ISO/IEC JTC1

แหล่งข้อมูลเพิ่มเติม www.iso.org
http://isotc.iso.ch/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm

ITIL

ITIL มาจากคำเต็มว่า IT Infrastructure Library ได้รับการจัดทำเผยแพร่โดยหน่วยงานรัฐบาล คือ Central Computer and Telecommunications Agency หรือ CCTA ซึ่งขณะนี้กลายเป็นองค์กร The British Office of Government Commerce (OGC) แต่ก็มิได้ประกาศบังคับว่าทุกองค์กรที่เกี่ยวข้องจะต้องปฏิบัติตาม ITIL

ITIL เป็นแนวทางปฏิบัติ (Guidance) ที่ว่าด้วยเรื่องเกี่ยวกับโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ แบ่งเป็น 8 เรื่อง ดังนี้

1) การบริหารจัดการซอฟต์แวร์และทรัพย์สินขององค์กร (Software and Asset Management)
2) การส่งมอบผลิตภัณฑ์หรือบริการที่ได้มาตรฐาน (Service Delivery)
3) คุณภาพของการบริการหลังส่งมอบ (Service Support)
4) การวางแผนสำหรับการบริหารจัดการการให้บริการ (Planning to Implement Service Management)
5) การบริหารจัดการโครงสร้างพื้นฐานด้านไอซีที (ICT Infrastructure Management)
6) การบริหารจัดการแอพพลิเคชั่น (Application Management)
7) การบริหารจัดการด้านความมั่นคงปลอดภัย (Security Management)
8) มุมมองทางธุรกิจ (Business Perspective, Volume II)

แต่ ITIL ได้ชื่อว่าเป็นแนวทางปฏิบัติที่ดีเยี่ยม (best practice) ในการบริหารจัดการด้าน IT Service ให้แก่ผู้บริโภคอย่างเปี่ยมคุณภาพ แนวทางปฏิบัตินี้เหมาะกับองค์กร ไม่ว่าจะขนาดเล็กหรือใหญ่ โดยเฉพาะอย่างยิ่ง องค์กรที่เน้นเรื่องของการบริการด้าน IT Service

ITIL เป็นแนวทางปฏิบัติปัจจุบันยังไม่สามารถขอใบรับรองได้ เนื่องจากปัจจุบัน ITIL เป็นเอกสารอ้างอิงสำหรับใช้เป็นแนวทางปฏิบัติ แต่ในอนาคตก็อาจมีการคัดเอาเฉพาะส่วนนี้มาทำข้อกำหนด และมีการออกใบรับรองภายใต้ชื่อ ISO 20000 (มาตรฐานการให้บริการด้านสารสนเทศ)

แหล่งข้อมูลเพิ่มเติม www.tso.co.uk/itil/
www.ogc.gov.uk
www.itil.co.uk
www.itsmf.com

FIPS PUB 200

มาตรฐาน FIPS PUB 200 ว่าด้วยเรื่องของข้อกำหนดขั้นต่ำสำหรับความต้องการด้านความมั่นคงปลอดภัย ซึ่งเป็นภาคบังคับขององค์กรบริหารจัดการสารสนเทศและระบบสารสนเทศกลางของประเทศสหรัฐอเมริกา ซึ่งทุกองค์กรที่เป็นหน่วยงานภาครัฐจะต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยนี้เป็นอย่างน้อย โดยมาตรฐานนี้จะมีการระบุประเภท ของระบบสารสนเทศต่างๆ และวิธีปฏิบัติที่จำเป็นสำหรับควบคุมเพื่อให้เกิดความมั่นคงปลอดภัยของสารสนเทศในระบบนั้นๆ

FIPS PUB 200 เป็นมาตรฐานที่ได้รับการพิมพ์เผยแพร่จากองค์กรกลางที่กำกับดูแลมาตรฐานต่างๆ ของระบบประมวลผลสารสนเทศในประเทศสหรัฐอเมริกา The Federal Information Processing Standards (FIPS) มาตรฐานนี้ได้รับการปรับปรุงและพิมพ์เผยแพร่ล่าสุดเดือนมีนาคม 2006

การที่ FIPS PUB 200 ได้รับการกำหนดให้เป็นมาตรฐานขั้นต่ำและองค์กรภาครัฐต้องปฏิบัติตามเป็นภาคบังคับ เนื่องมาจากรัฐบาลของประเทศสหรัฐอเมริกา ต้องการสนับสนุนเรื่องความมั่นคงปลอดภัย ดังนั้น จึงได้บัญญัติกฎหมาย Federal Information Security Management Act (FISMA) ซึ่งส่งผลให้หน่วยงานต่างๆ ต้องปฏิบัติตามโดยปริยาย

สำหรับเนื้อหาโดยสรุปของมาตรฐานนี้ ได้แก่

- การระบุข้อกำหนดขั้นต่ำของระบบประมวลผลสารสนเทศขององค์กรกลางในประเทศสหรัฐอเมริกา
- การจัดทำข้อกำหนดนี้เพื่อสนับสนุนการพัฒนา
- การลงมือปฏิบัติ
- การดำเนินการเพื่อสร้างความมั่นคงปลอดภัยระบบสารสนเทศ โดยหน่วยงานสามารถคัดเลือกเฉพาะส่วนที่เกี่ยวข้องกับองค์กรของตนมาปฏิบัติตาม มาตรฐานนี้จึงได้มีการจัดทำแนวทางในการคัดเลือกและกำหนดมาตรการด้านความมั่นคงปลอดภัยที่จำเป็นและเหมาะสมสำหรับระบบประมวลผลสารสนเทศของแต่ละหน่วยงาน

มาตรฐานนี้กล่าวได้ว่าเป็นข้อกำหนดตามกฎ หรือข้อบังคับที่องค์กรภาครัฐหรือองค์กรกลางของรัฐบาลสหรัฐฯ ต้องปฏิบัติตามให้ได้ และมาตรฐานนี้ยังเป็นเพียงข้อกำหนดขั้นต่ำและไม่มีการให้ใบรับรอง สำหรับมาตรฐานของระบบสารสนเทศที่ต้องการความมั่นคงปลอดภัยในระดับที่สูงกว่านี้ จะมีองค์กรอีกองค์กรหนึ่งที่ช่วยพัฒนามาตรฐานด้านเทคโนโลยีต่างๆ และได้จัดทำไว้เพื่อเสริมสร้างมาตรฐานความมั่นคงปลอดภัยทางด้านเทคนิค หน่วยงานที่ดูแลในส่วนนี้มีชื่อว่า (National Institute of Security Technology หรือ NIST) ดังนั้นระบบที่มีข้อมูลสารสนเทศที่ต้องรักษาความลับ ความถูกต้อง และความสมบูรณ์ของข้อมูลในระดับสูงจำเป็น จะต้องใช้มาตรฐานที่รัดกุมและเข้มแข็งมากกว่ามาตรฐาน FIPS PUB 200 นี้ หรืออาจต้องอาศัยความเฉพาะด้านทางเทคโนโลยีและใช้มาตรฐานของ NIST เป็นมาตรฐานหลัก ทั้งนี้ ผู้ศึกษาจะได้กล่าวถึงมาตรฐาน NIST โดยละเอียดต่อไป

แหล่งข้อมูลเพิ่มเติม www.nist.org
http://csrc.nist.gov/publications

NIST 800-14

สถาบันมาตรฐานเทคโนโลยีสารสนเทศแห่งชาติของสหรัฐอเมริกา ได้พิมพ์เผยแพร่หนังสือมาตรฐานในชื่อว่า Generally Accepted Principles and Practices for Securing Information Technology Systems มาตรฐานนี้เป็นเกณฑ์กลางที่ได้รับการจัดทำและเผยแพร่ขึ้นโดยสถาบันดังกล่าว เพื่อเสริมสร้างองค์กรที่ใช้ระบบสารสนเทศให้นำมาตรฐานเทคโนโลยีทีได้จัดพิมพ์นี้ไปใช้ เพื่อเสริมสร้างความมั่นคงปลอดภัยให้แก่ระบบเทคโนโลยีสารสนเทศขององค์กรหรือหน่วยงานต่างๆ ในประเทศสหรัฐอเมริกาให้มากที่สุด

ทั้งนี้ เพื่อเป็นการป้องกันภัยคุกคามด้านอาชญากรรมคอมพิวเตอร์และการละเมิดความมั่นคงปลอดภัยข้อมูลสารสนเทศโดยเฉพาะอย่างยิ่งสารสนเทศบนระบบโครงสร้างพื้นฐานของประเทศ
การเผยแพร่ในครั้งแรกเมื่อปี 1996 ได้จัดทำเป็นกฎพื้นฐานด้าน Computer Security จำนวน 8 ข้อดังนี้

1) ในพันธกิจขององค์กรต้องให้การสนับสนุนเรื่องของความมั่นคงปลอดภัยคอมพิวเตอร์
2) ในการบริหารจัดการองค์กรต้องผนวกเรื่องของความมั่นคงปลอดภัยคอมพิวเตอร์ไว้เป็นสาระสำคัญด้วย
3) ควรมีการลงทุนที่เหมาะสมในเรื่องของความมั่นคงปลอดภัยคอมพิวเตอร์
4) ผู้เป็นเจ้าของระบบต้องแสดงความรับผิดชอบต่อการรักษาความมั่นคงปลอดภัยของระบบโดยตลอด
5) ความรับผิดชอบและการดูแลเอาใจใส่ในเรื่องของความมั่นคงปลอดภัยคอมพิวเตอร์ต้องได้รับการดำเนินการอย่างชัดแจ้ง
6) การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ต้องการแนวทางที่ผสมผสานในวิธีปฏิบัติ เช่น การรักษาความมั่นคงปลอดภัยทางกายภาพ ทางด้านฮาร์ดแวร์ ซอฟต์แวร์ และผู้ใช้ เป็นต้น
7) ความมั่นคงปลอดภัยคอมพิวเตอร์ต้องได้รับการปรับปรุงให้ดีขึ้นอย่างต่อเนื่องและสม่ำเสมอ
8) ปัจจัยแวดล้อมสามารถส่งผลต่อการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ได้เสมอ

NIST เป็นแนวทางปฏิบัติที่องค์กรที่จัดทำมีเจตนาให้ใช้เป็นเอกสารอ้างอิงและเป็นเสมือนเครื่องมือในการตรวจสอบระบบเทคโนโลยีสารสนเทศขององค์กร แนวทางปฏิบัตินี้จัดเป็นเกณฑ์พื้นฐานที่หลายองค์กรเห็น

ร่วมกันว่าควรจะต้องจัดให้มีและสามารถตรวจสอบได้โดยฝ่ายตรวจสอบทั้งภายในและภายนอกองค์กร เช่น ผู้ตรวจสอบกิจการภายใน ผู้จัดการ ผู้ใช้หรือลูกค้า พนักงานด้านความมั่นคงปลอดภัยคอมพิวเตอร์ เป็นต้น แนวทางที่ NIST ได้จัดทำนั้นสามารถประยุกต์ใช้ได้ทั้งภาครัฐและเอกชน

อ้างอิงจาก Marianne Swanson, Barbara Guttman, Special Publication 800–14, Generally Accepted Principles and Practices for Securing Information Technology Systems, Published 1996, National Institute of Standards and Technology (NIST)

แหล่งข้อมูลเพิ่มเติม www.nist.gov
http://csrc.nist.gov

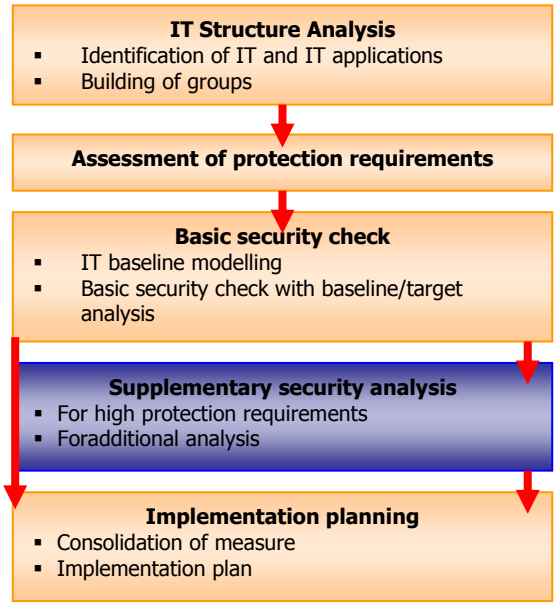
IT Baseline Protection Manual

มาตรฐาน IT Baseline Protection Manual หรือเรียกย่อๆ ว่า IT BPM เป็นหนังสือคู่มือที่แนะนำการรักษาความมั่นคงปลอดภัยระบบอย่างมีมาตรฐาน แต่อาจกำหนดไว้เป็นมาตรฐานขั้นต่ำ คู่มือนี้พิมพ์เผยแพร่โดย BSI ซึ่งเป็นองค์กรกลางที่กำกับดูแลเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยจะจัดทำเฉพาะระบบสารสนเทศที่มีใช้ในองค์กรทั่วไป อาทิ ระบบสารสนเทศเกี่ยวกับบุคลากรขององค์กร ระบบสารสนเทศสำหรับสื่อสารด้วยไปรษณีย์อิเล็กทรอนิกส์ เป็นต้น คู่มือนี้จะให้การแนะนำว่าระบบที่ยกตัวอย่างนี้ ควรมีเกราะป้องกันหรือวิธีการด้านความมั่นคงปลอดภัยอย่างน้อยต้องดำเนินการอย่างไรบ้าง

หนังสือคู่มือนี้แต่ละองค์กรอาจนำไปประยุกต์ใช้ด้วยวัตถุประสงค์ที่แตกต่างกันออกไป เช่น ต้องการที่จะใช้เป็นเกณฑ์ระบุว่าความปลอดภัยขั้นต่ำขององค์กรคืออะไร องค์กรต้องการใช้เป็นแนวทางปฏิบัติด้านความมั่นคงปลอดภัยที่ดีระดับหนึ่ง การปรับปรุงความมั่นคงปลอดภัยระบบข้อมูลสารสนเทศ หรือบางองค์กรอาจต้องการได้รับใบรับรอง เป็นต้น

อย่างไรก็ดี หนังสือคู่มือนี้ จะได้รับการปรับปรุงทุกๆ หกเดือน การจะปรับปรุงในหัวข้อใดจะได้รับความเห็นชอบจากการลงมติของกลุ่มความร่วมมือ หนังสือคู่มือนี้มีความหนาถึง 2,300 หน้าและเน้นหนักด้านเทคนิคเป็นอย่างมาก เนื้อหาประกอบด้วย

- ระบบต้องมีการบริหารจัดการด้านความมั่นคงปลอดภัยตั้งแต่ขั้นการออกแบบ ประสานงานและติดตามสถานะของความมั่นคงปลอดภัยของระบบที่เกี่ยวกับหน้าที่งานนั้น
- ระบบต้องมีการวิเคราะห์และจัดทำเป็นเอกสารเกี่ยวกับโครงสร้างที่มีอยู่ของทรัพย์สินที่เป็นเทคโนโลยีสารสนเทศในองค์กร
- ระบบต้องได้รับการประเมินถึงมาตรการและระบบบริหารจัดการด้านความมั่นคงปลอดภัยเดิมที่ได้จัดทำไว้แล้วนั้น ว่ามีประสิทธิภาพเพียงพอและเหมาะสมแล้วหรือยัง
- องค์กรต่างๆ สามารถนำโครงสร้างของเครือข่ายที่มีความมั่นคงปลอดภัย ซึ่งได้ออกแบบไว้เหมาะสมแล้วตามคู่มือนี้ มาเป็นแนวทางในการจัดทำเครือข่ายขององค์กร
- ระบบต้องได้รับการดำเนินการปรับปรุงแก้ไขกรณีที่พบว่ามาตรการหรือแนวทางการรักษาความมั่นคงปลอดภัยเหล่านั้นไม่เพียงพอหรือมีการดำเนินการบางอย่างที่ยังไม่รัดกุม เป็นต้น



<u>แผนภาพที่ 4</u> แสดงแนวคิดการวางรูปแบบการรักษาความมั่นคงปลอดภัยระบบ

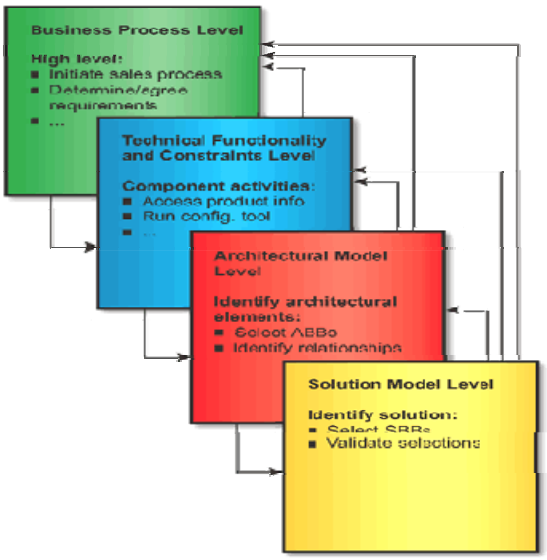
แหล่งข้อมูลเพิ่มเติม www.sei.cmu.edu/cmmi
www.iso.org

TOGAF 8.1

TOGAF มาจากคำเต็มว่า The Open Group Architecture Forum เป็นกลุ่มองค์กรที่แบ่งปันข้อมูล ความรู้ ค่ามาตรฐาน ต่างๆ ของสถาปัตยกรรมทางด้านฮาร์ดแวร์และซอฟต์แวร์ เพื่อให้เครื่องใช้ไฟฟ้า หรือผลิตภัณฑ์อิเล็กทรอนิกส์ที่ผลิตต่างค่าย ต่างบริษัท มีพื้นฐานของสถาปัตยกรรมด้าน ฮาร์ดแวร์และซอฟต์แวร์ไปในทางเดียวกันมีความเข้ากันได้ โดยอาศัยการประชุมหารือระหว่างกลุ่มผู้ผลิต กลุ่มผู้ใช้ กลุ่มที่ทดสอบ เพื่อลงความเห็นให้ใช้สถาปัตยกรรมพื้นฐานที่มีมาตรฐานเดียวกัน ทั้งนี้ เพื่อให้สามารถรองรับในเรื่องของความเข้ากันได้ทั้งในด้านของความต้องการทางธุรกิจ โครงสร้างข้อมูล โครงสร้างเกี่ยวกับแอพพลิเคชัน และสถาปัตยกรรมด้านเทคโนโลยีต่างๆ เพื่อประโยชน์ในการพัฒนาต่อยอดผลิตภัณฑ์อิเล็กทรอนิกส์ต่างๆ ซึ่งในระยะหลังได้มีการเสริมเรื่องของการรักษาความมั่นคงปลอดภัยข้อมูลมากขึ้น

สถาปัตยกรรมที่กลุ่มผู้ผลิตร่วมกันปฏิบัติ ประกอบด้วย Business Architecture, Data Architecture, Applications Architecture, Technology Architecture เป็นต้น ปัจจุบัน TOGAF เป็นเครื่องมือที่ช่วยผู้ผลิตหรือผู้ประกอบการในการจัดทำฮาร์ดแวร์และซอฟต์แวร์ในเรื่องของค่าใช้จ่าย มีกลุ่มความร่วมมือเป็นฐานช่วยสร้างความสมบูรณ์ให้กับผลิตภัณฑ์และเกิดผลิตภัณฑ์ใหม่ๆ ขึ้น ผู้ผลิตที่มีความร่วมมือกันได้แก่ HP, IBM, HITACHI, NEC, Fujitsu, Capgimini เป็นต้น

กลุ่มความร่วมมือนี้ เริ่มเกิดขึ้นเมื่อปี 1995 ในระหว่างที่มีเวทีสำหรับการจัดทำระบบให้กับองค์กรด้านความมั่นคงทางทหารของประเทศสหรัฐอเมริกา หรือ DoD (Department of Defense) และมีการแบ่งปันข้อมูลข่าวสารที่เป็นความรู้และแนวทางระหว่างกัน นอกจากนี้ได้มีการเผยแพร่ความรู้และข้อกำหนดเหล่านั้นบนเว็บไซต์ของกลุ่มความร่วมมือนี้ด้วย



<u>แผนภาพที่ 5</u> แสดงกรอบแนวทางปฏิบัติในแต่ละระดับของกลุ่มความร่วมมือ TOGAF

สำหรับการให้ใบรับรอง โดยตัวบุคคลแล้ว สามารถสมัครเข้ารับการอบรมและรับการทดสอบ หากผ่านจะสามารถได้ใบรับรองได้ สำหรับในนามองค์กรสามารถมีผลิตภัณฑ์/บริการ ที่ได้รับการรับรองว่าเป็นผลิตภัณฑ์/บริการ ภายใต้การรับรองของ TOGAF เช่นกัน

ขณะนี้ท่านที่สนใจอ่านมาตรฐานอุตสาหกรรมเปิดของ TOGAF สามารถดาวน์โหลดได้จากเว็บไซต์ในลิ้งก์ด้านล่างนี้ ซึ่งมีตั้งแต่เวอร์ชั่น TOGAF version 8 (Enterprise Edition) เผยแพร่เมื่อเดือนธันวาคม 2002 และปรับเป็นเวอร์ชั่น 8.1 เมื่อเดือนธันวาคม 2003 สำหรับ TOGAF version 7 (Technical Edition) พิมพ์เผยแพร่เมื่อเดือนธันวาคม 2001 จัดพิมพ์เกี่ยวกับด้านเทคนิค สำหรับ TOGAF version 8 จะเน้นเรื่องของสถาปัตยกรรมทางเทคนิคและใช้วิธีพัฒนาจากของเดิม สำหรับเวอร์ชั่น 9 ซึ่งน่าจะเผยแพร่ปี 2006 เป็นอย่างช้า จะมีการเพิ่มเติมในประเด็นต่อไปนี้ด้วย

- The enterprise, culture and stakeholders
- Enterprise architecture creation
- Enterprise architecture-based transformation

- Enterprise architecture deployment
- Enterprise architecture realisation
- Enterprise architecture management and governance

แหล่งข้อมูลเพิ่มเติม www.opengroup.org
www.opengroup.org/architecturel
www.opengroup.org/togaf8-doc/arh

PRINCE2

PRINCE2 เป็นเครื่องมือที่ได้รับการพัฒนาขึ้นเพื่อเป็นการช่วยให้ผู้มีหน้าที่เป็น Project Manager สามารถทำงานได้สะดวกขึ้น เครื่องมือนี้จะรวมสภาวะแวดล้อมทางธุรกิจที่เกี่ยวข้องกับการจัดทำโครงการด้านเทคโนโลยีสารสนเทศที่หลากหลาย และสามารถแจกแจงออกมาเป็นกิจกรรมที่ต้องกระทำ เพื่อช่วยในการบริหารจัดการโครงการด้านไอที ให้สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล และสิ่งที่เครื่องมือ PRINCE2 นี้ได้รวบรวมไว้นั้นเป็นกิจกรรมที่เป็นพื้นฐานและสามารถปรับแต่งให้เหมาะสมกับเงื่อนไขต่างๆ ตามการบริหารจัดการโครงการได้

อาจกล่าวได้ว่า ผู้บริหารที่ใช้เครื่องมือนี้ จะสามารถบริหารโครงการได้สัมฤทธิผลอย่างแน่นอนอย่างไรก็ดี เครื่องมือดังกล่าวแม้จะได้รับการยอมรับว่าเป็นเครื่องมือที่ใช้กันจนเป็นที่นิยมและเกือบจะกลายเป็นมาตรฐานของการบริหารจัดการโครงการด้านไอทีไปแล้วก็ตามแต่ก็ไม่ได้ประกาศให้เป็นมาตรฐานที่ทุกองค์กรควรต้องนำไปใช้ เนื่องด้วยข้อจำกัดในการประยุกต์ให้เหมาะสมกับองค์กรซึ่งบางองค์กรที่มีขนาดใหญ่ก็จะสามารถใช้งานเครื่องมือนี้ได้อย่างคุ้มค่า แต่หากไม่ใช่องค์กรขนาดใหญ่ก็อาจไม่คุ้มที่จะนำเครื่องมือนี้ไปประยุกต์ใช้

สำหรับเครื่องมือ PRINCE2 ได้จัดพิมพ์เผยแพร่เป็นครั้งแรกโดย the Central Computer and Telecommunications Agency (CCTA) และได้รับการนำไปพัฒนาต่อโดย British Office of Government Commerce (OGC) และตีพิมพ์เป็นภาษาอังกฤษเท่านั้น

แหล่งข้อมูลเพิ่มเติม www.ogc.gov.uk
www.apmgroup.co.uk

PMBOK

PMBOK เป็นแนวทางปฏิบัติของการบริหารจัดการโครงการที่เป็นองค์ความรู้ หรือ Body of Knowledge ย่อมาจาก A Guide to the Project Management Body of Knowledge แนวทางปฏิบัตินี้ได้ถูกอธิบายไว้ว่าเป็นข้อสรุปของความรู้ที่เกี่ยวกับการบริหารจัดการโครงการอย่างมืออาชีพ และเป็นหนึ่งในมาตรฐานของสหรัฐอเมริกาภายใต้ชื่อว่า ANSI/PMI 99-001-2004

แม้ว่าแนวทางปฏิบัติเกี่ยวกับการบริหารจัดการโครงการเป็นเรื่องที่หลายคนต่างให้ความสนใจแต่เนื่องจากการขาดแคลนเครื่องมืออัตโนมัติที่จะสามารถนำมาช่วยอำนวยความสะดวกในการบริหารจัดการกลุ่มผู้เห็นความจำเป็นของการบริหารจัดการโครงการ โดยเฉพาะอย่างยิ่งโครงการเกี่ยวกับระบบเทคโนโลยีสารสนเทศซึ่งมีความซับซ้อน มีความต้องการทางธุรกิจที่ต่างกัน สภาวแวดล้อมทางธุรกิจต่างกัน ความต้องการในการจัดทำระบบจึงต่างกันไปด้วย จึงกลายเป็นเรื่องยากที่จะจัดการนำความรู้เหล่านี้มารวมกัน

อย่างไรก็ตาม เมื่อเริ่มจัดทำโครงการมากขึ้น วิธีการบริหารจัดการก็มากขึ้นเป็นลำดับ กลุ่มผู้เห็นความสำคัญจึงได้รวบรวมองค์ความรู้เหล่านี้ขึ้น และเริ่มมีการนำไปใช้ และเห็นว่าสามารถใช้งานได้ดี เหมาะกับการบริหารจัดการโครงการโดยส่วนใหญ่ แม้จะไม่ทั้งหมด แต่ก็สามารถรวบรวมเอากระบวนการด้านไอทีที่เป็นพื้นฐานมาใช้ได้

ตารางต่อไปนี้ จะแสดงความสัมพันธ์ระหว่างกระบวนการกับความรู้ที่เกี่ยวข้องกับกระบวนการนั้น ต่อการบริหารจัดการโครงการต่างๆ

Project Management Phases	Project Management Process Groups				
	Initiating Process Group	**Planning Process Group**	**Executing Process Group**	**Monitoring and Controlling Process Group**	**Closing Process Group**
Project integration management	▪ Project charter development ▪ Preliminary project scope statement development	▪ Project management plan development	▪ Project execution direction and management	▪ Project work monitoring and control ▪ Integrated change control	▪ Project closure
Project scope management		▪ **Scope planning** ▪ **Scope definition** ▪ **WBS creation**		▪ **Scope verification** ▪ **Scope change control**	

Project Management Phases	Project Management Process Groups				
	Initiating Process Group	**Planning Process Group**	**Executing Process Group**	**Monitoring and Controlling Process Group**	**Closing Process Group**
Project time management		▪ Activity definition ▪ Activity sequencing ▪ Activity resource estimating ▪ Activity duration estimating ▪ Development scheduling		▪ Schedule control	
Project cost management		▪ Cost estimating ▪ Cost budgeting		▪ Cost control	
Project quality management		▪ Quality planning	▪ Quality assurance performance	▪ Quality control performance	
Project HR management		▪ Human Resource planning	▪ Project team acquisition ▪ Team development	▪ Project team management	
Project communication management		▪ Communication planning	▪ Information distribution	▪ Performance reporting ▪ Stakeholders management	
Project risk management		▪ Risk management planning ▪ Risk identification ▪ Qualitative risk analysis ▪ Quantitative risk analysis ▪ Risk response planning	▪	▪ Risk monitoring and control	
Project procurement management		▪ Procurement and acquisitions planning ▪ Contract planning	▪ Seller responses request ▪ Seller selection	▪ Contract administration	▪ Contract close-out

อ้างอิง Project Management Institute**, A Guide to the Project Management Body of Knowledge (PMBOK® Guide)**, 3rd Edition, 2004, figure 3-45.

แหล่งข้อมูลเพิ่มเติม www.pmi.org

TickIT

TickIT เป็นมาตรฐานกลุ่มอุตสาหกรรม และเป็นกรอบสำหรับการให้การรับรองระบบบริหารจัดการคุณภาพสำหรับการพัฒนาซอฟต์แวร์ วัตถุประสงค์หลักของมาตรฐานนี้คือต้องการสร้างหรือปรับปรุงในเรื่องของระบบบริหารจัดการคุณภาพสำหรับการพัฒนาซอฟต์แวร์ให้เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล และเป็นไปตามระบบบริหารจัดการคุณภาพ

กลุ่มเป้าหมายของมาตรฐาน TickIT ที่ควรศึกษาและทำความเข้าใจได้แก่ กลุ่มลูกค้าผลิตภัณฑ์ซอฟต์แวร์ โดยเฉพาะอย่างยิ่งระดับผู้บริหารที่ควรทราบว่าจะจัดทำข้อกำหนดในการจัดซื้อจัดจ้างและระบุความต้องการที่ถูกต้องให้กับผู้ผลิตซอฟต์แวร์ได้อย่างไร เป็นต้น กลุ่มต่อมาคือกลุ่มผู้ให้บริการจัดหาซอฟต์แวร์ต่างๆ ซึ่งเป็นผู้ที่ต้องพัฒนาระบบบริหารจัดการคุณภาพสำหรับการพัฒนาซอฟต์แวร์ของตนให้ได้มาตรฐานและมีการพัฒนาอย่างต่อเนื่อง นอกจากนี้ กลุ่มผู้ตรวจสอบ (auditor) ควรให้ความสนใจในมาตรฐานนี้ด้วยเนื่องจากมาตรฐานนี้สามารถให้การรับรองได้ ซัพพลายเออร์ รวมถึงการรับรองคุณภาพและช่วยสร้างกระบวนการพัฒนาอย่างต่อเนื่องให้กับผู้ผลิตซอฟต์แวร์

ที่มาหลักของการพัฒนามาตรฐาน TickIT มาจากกลุ่มอุตสาหกรรมชาวอังกฤษและสวีดิช โดย บรรดาผู้พัฒนาได้จำลองสถานการณ์ในการพัฒนาระบบซอฟต์แวร์โดยคำนึงถึงประเด็นเกี่ยวกับ

- อะไรคือคุณภาพในกระบวนการพัฒนาซอฟต์แวร์
- การจะพัฒนาซอฟต์แวร์ให้ได้คุณภาพนั้นต้องทำอย่างไร และ
- ระบบบริหารจัดการต่างๆ ที่เกี่ยวข้องเพื่อให้ได้มาซึ่งคุณภาพเหล่านั้นต้องได้รับการปรับปรุงเพื่อรองรับการพัฒนาซอฟต์แวร์อย่างมีคุณภาพด้วยวิธีการใดบ้าง

แนวทาง TickIT เป็นแนวทางพัฒนาคุณภาพ ซึ่งเสมือนกับระบบบริหารจัดการคุณภาพ ISO 9001 ดังนั้น การพัฒนาซอฟต์แวร์อย่างมีคุณภาพซึ่งเป็นข้อกำหนดทางสัญญาสำหรับผู้ผลิตและจัดหาซอฟต์แวร์ในตลาดหลักๆ ผลจากการระบุเป็นข้อกำหนดทำให้การคำนึงถึงเรื่องคุณภาพกลายเป็นผลพลอยได้ของการพัฒนาซอฟต์แวร์ให้มีคุณภาพและกลายเป็นข้อกำหนดพื้นฐาน และเป็นแนวทางการปรับปรุงคุณภาพและบริการจัดส่งให้ลูกค้าได้อย่างเป็นที่พอใจ

จากความเกี่ยวข้องดังกล่าวทำให้องค์กรผู้ผลิตซอฟต์แวร์ต้องพัฒนาความเชื่อมั่นทางการตลาดแม้ว่าจะมีการแบ่งช่วงสัญญาไปให้บริษัทหรือผู้รับเหมาอื่นทำการผลิตซอฟต์แวร์หรือระบบเทคโนโลยีสารสนเทศก็ตาม สัญญามีผลผูกพันไปถึงบุคคลที่สามที่เข้ามามีส่วนร่วมนี้ด้วย จึงทำให้ภาคการผลิตซอฟต์แวร์ต้องได้รับการรับรองคุณภาพจาก Certification Bodies (CB)

นอกจากนี้ ยังมีการพัฒนาแนวทางปฏิบัติ TickIT ต่อยอด โดยผู้ตรวจสอบด้านคุณภาพในการพัฒนาซอฟต์แวร์และระบบ ประกอบกับผู้ผลิตซอฟต์แวร์มืออาชีพต่างๆ และทั้งสองฝ่ายได้พิมพ์เผยแพร่ในเรื่องของแนวทางปฏิบัติ TickIT เพื่อประโยชน์ต่อผู้ใช้ต่อไป สำหรับขั้นตอนปฏิบัติของ TickIT ที่ได้กลายเป็นข้อกำหนดในมาตรฐานสากล ISO 9001:2000 ได้มีการพิมพ์เผยแพร่วิธีปฏิบัติไว้ใน TickIT Guide no. 5

แหล่งข้อมูลเพิ่มเติม www.tickit.org
www.iso.org

บทวิเคราะห์

จากข้อมูลข้างต้น ผู้ศึกษาต้องการนำเสนอเป็นข้อมูลเบื้องต้นในระดับแนะนำตัวของ มาตรฐาน แนวทางปฏิบัติ หรือกรอบวิธีปฏิบัติแต่ละชนิดเท่านั้น หากองค์กรต้องการนำไปประยุกต์ใช้ ต้องศึกษาเพิ่มเติมอีกมาก และการจะลงมือศึกษาสิ่งใด ก็ควรพิจารณาปัจจัยด้านความเหมาะสมเหล่านี้ประกอบด้วย ปัจจัยดังกล่าว ได้แก่

- ปัจจัยเรื่องความสอดคล้องกับข้อกำหนด กฎหมาย กล่าวคือ มาตรฐานหรือกรอบวิธีปฏิบัติ หรือแนวทางปฏิบัติเหล่านั้น ได้รับการกำหนดเป็น พันธะสัญญา กฎหมายระหว่างประเทศ กฎหมายในประเทศ หรือถูกกำหนดเป็นระเบียบด้านการกำกับดูแลที่องค์กรต้องปฏิบัติหรือไม่ เช่น องค์กรกลางในประเทศสหรัฐอเมริกา ต้องปฏิบัติตามมาตรฐาน FIPS PUB 200 ซึ่งว่าด้วยเรื่องความมั่นคงปลอดภัยขั้นต่ำของระบบสารสนเทศขององค์กรกลางในประเทศสหรัฐอเมริกา เป็นต้น
- ปัจจัยเรื่องพันธะผูกพันทางสัญญา ทั้งในระดับคู่สัญญา และในระดับคู่สัญญารายย่อย กล่าวคือ กรณีผู้ประกอบการด้านการผลิตรถยนต์ ผู้ผลิตรายใหญ่จะมีการรับส่วนประกอบมาจากผู้ผลิตรายย่อย ผู้ผลิตรายย่อยนั้นต้องมีมาตรฐานที่เป็นที่ยอมรับตามที่ผู้ผลิตรายใหญ่ต้องการ จึงจะสามารถดำเนินงานในส่วนนั้นได้ ตัวอย่างมาตรฐานที่ต้องปฏิบัติตามในลักษณะนี้ ได้แก่ มาตรฐาน ITIL เป็นต้น
- ปัจจัยที่เกี่ยวข้องกับแผนแม่บท หรือนโยบายด้าน ICT ของประเทศ เช่น ประเทศไทยเมื่อเริ่มให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศ ก็ได้มีองค์กรต่างๆ หยิบเอามาตรฐาน ISO/IEC 27001, 17799-2005 มาใช้เป็นกรอบในการวางแผนและนำไปสู่การปฏิบัติให้องค์กรมีระบบเทคโนโลยีสารสนเทศที่มีความปลอดภัย เป็นต้น
- ปัจจัยด้านพันธกิจ ภารกิจ และกลยุทธ์ขององค์กร กล่าวคือ หากองค์กรใดต้องการความได้เปรียบบางประการและพิจารณาเห็นว่าความได้เปรียบนั้นจะกลายเป็นจุดขายขององค์กรต่อไป จึงวางแผนเพื่อให้องค์กรมีกรอบวิธีปฏิบัติในการสร้างความได้เปรียบดังกล่าว เช่น องค์กรภาครัฐ อาจกำหนดพันธกิจว่า ต้องเป็นองค์กรที่มีความโปร่งใสในการบริหารจัดการงบประมาณ องค์กรภาครัฐก็ควรจะพิจารณากรอบวิธีปฏิบัติ COSO มาเป็น Internal Control ให้กับองค์กร ขณะเดียวกัน หากต้องการเพิ่มความมีประสิทธิภาพ ประสิทธิผลของระบบเทคโนโลยีสารสนเทศ องค์กรอาจต้องพิจารณากรอบวิธีปฏิบัติ COBIT มาใช้เป็นเกณฑ์ประกอบการวางแผนปฏิบัติการในทั้งเรื่องของความคุ้มค่าในการลงทุน การวัดประสิทธิภาพการประเมินผล และการปรับปรุง เป็นต้น

ปัจจัยที่กล่าวมาเป็นเพียงข้อพิจารณาเบื้องต้น การนำไปปฏิบัติจริง องค์กรต้องเข้าใจก่อนว่าองค์กรของตนอยู่ในสถานะใด มีความจำเป็นต้องปฏิบัติตามมาตรฐานเหล่านี้มากหรือน้อยเพียงใด ความพร้อมของทรัพยากรขององค์กรมีมากน้อยเพียงใด ทั้งหลายเหล่านี้ ต้องได้รับการพิจารณาร่วมกันทั้งในระดับผู้บริหารและในระดับปฏิบัติการ เพื่อให้ผลที่ออกมาสัมฤทธิ์ตามวัตถุประสงค์ของมาตรฐาน แนวทางปฏิบัติ หรือกรอบวิธีปฏิบัติได้อย่างเหมาะสม

นอกจากปัจจัยที่กล่าวมาข้างต้นแล้ว องค์กรควรพิจารณาถึงประโยชน์ที่องค์กรจะได้รับ ความคุ้มค่า และกลยุทธ์ หรือวิธีกำหนดเส้นทางดำเนินการหรือการวางแผนไปสู่การปฏิบัติ ซึ่งควรหมายรวมถึงการเปลี่ยนแปลงสิ่งเหล่านั้นเข้าไปในวัฒนธรรมองค์กรอีกด้วย

อย่างไรก็ดี สิ่งหนึ่งที่ผู้ศึกษาเห็นว่าน่าจะเป็นการช่วยให้ผู้บริหารองค์กรสามารถเลือกหรือหยิบเอามาตรฐาน แนวทางปฏิบัติ หรือกรอบวิธีปฏิบัติไปใช้ได้เร็วขึ้น คือ การจัดประเภทความเหมือนและความต่างของวัตถุประสงค์ของมาตรฐาน แนวทางปฏิบัติ หรือกรอบวิธีปฏิบัติ ที่ได้ยกมากล่าวข้างต้น เพื่อให้อย่างน้อยที่สุดผู้บริหารองค์กรจะสำรวจได้อย่างรวดเร็วว่าองค์กรของตนควรเน้นในมาตรฐาน แนวทางปฏิบัติ หรือกรอบวิธีปฏิบัติใด เป็นต้น

ผู้ศึกษาจัดกลุ่มเหล่านี้เพื่อเป็นตัวอย่างแนวคิดอย่างง่ายๆ เท่านั้น หากองค์กรมีลักษณะที่ซับซ้อนกว่าปกติ ก็อาจจะเลือกมาตรฐาน กรอบวิธีปฏิบัติ และแนวทางปฏิบัติที่มีจุดอ่อนและจุดแข็งต่างกันมาประยุกต์เอาสิ่งที่ดีมารวมกัน และนำไปใช้ก็เป็นอีกแนวคิดหนึ่งที่สามารถทำได้ ผู้ศึกษาเห็นว่า การที่องค์กรจะต้องปรับจูนองค์ความรู้จาก มาตรฐาน กรอบวิธีปฏิบัติ และแนวทางปฏิบัติเหล่านี้ ให้ตอบโจทย์ของผู้บริหารและตอบโจทย์ในการทำงานได้น่าจะเป็นสิ่งที่ท้าทายต่อผู้ประกอบวิชาชีพที่เกี่ยวข้องในด้านนี้ มากกว่าการนำทั้งแบบไปปฏิบัติเพียงอย่างเดียว

ตาราง แสดงการจัดกลุ่ม มาตรฐาน กรอบวิธีปฏิบัติ แนวทางปฏิบัติหรือเครื่องมือช่วยบริหารจัดการ แบ่งตามลักษณะการประยุกต์ใช้

ตัวอย่าง กรอบวิธีปฏิบัติ *(คำอธิบาย จะบรรยายถึงกระบวนการและขั้นตอนที่ช่วยให้ผู้ปฏิบัติสามารถดำเนินการและพัฒนาขีดความสามารถของการนำเทคโนโลยีสารสนเทศไปใช้งานได้อย่างมีประสิทธิภาพ สำหรับแนวทางที่ให้จะเป็นลักษณะของ Best practice (แนวทางปฏิบัติชั้นดี))*	**COBIT** **COSO** **ITIL**
ตัวอย่าง มาตรฐานสากลที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ *(คำอธิบาย มาตรฐานเหล่านี้จะมีขอบเขตที่แตกต่างกันออกไป ได้แก่* • *ISO/IEC 27001 ว่าด้วยเรื่องการรักษาความมั่นคงปลอดภัยระบบ* • *ISO/IEC 13335 ว่าด้วยเรื่องแนวทางปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยระบบ* • *ISO/IEC 15408 ว่าด้วยเรื่องเทคนิควิธีด้านความมั่นคงปลอดภัยซึ่งจะถูกใช้เป็นเงื่อนไขกลางหรือเกณฑ์กลาง (Common Criteria) ในการประเมินระบบในเรื่องของความมั่นคงปลอดภัย)*	**ISO/IEC 27001** **ISO/IEC 13335** **ISO/IEC 15408**
ตัวอย่าง แนวทางปฏิบัติขั้นต่ำที่องค์กรภาครัฐต้องปฏิบัติตาม *(คำอธิบาย แนวทางปฏิบัติดังกล่าวได้พัฒนาขึ้นโดยหน่วยงานภาครัฐ เพื่อใช้เป็นแนวทางปฏิบัติทางเทคนิคให้กับหน่วยงานที่ต้องการความมั่นคงปลอดภัยเป็นพิเศษและมีมาตรฐานเทคโนโลยีเฉพาะทาง)*	**FIPS PUB 200** **NIST 800-14** **IT BPM Manual**
ตัวอย่าง เครื่องมือต่างๆ ที่ใช้สำหรับบริหารจัดการระบบเทคโนโลยีสารสนเทศ *(คำอธิบาย แนวทางปฏิบัติหรือเครื่องมือต่างๆ มีไว้เพื่อช่วยวิเคราะห์ความต้องการ ช่วยออกแบบ ช่วยจำลองแนวทาง และช่วยบริหารจัดการโครงการทางเทคโนโลยีสารสนเทศให้ดำเนินการได้ง่ายขึ้นและเป็นไปอย่างมีแบบแผน)*	**PRINCE2** **PMBOK** **TickIT** **TOGAF 8.1**

บทสรุป

กล่าวโดยสรุป บทความนี้จัดทำเพื่อเปรียบเทียบแนวทางปฏิบัติที่มีการพิมพ์เผยแพร่และเป็นที่รู้จักกันในแวดวงเทคโนโลยีสารสนเทศทั่วโลก ทั้งนี้ในบทความได้เน้นถึงประเด็นเกี่ยวกับการบริหารจัดการเกี่ยวกับระบบไอทีให้เป็นไปอย่างมีความคุ้มค่า ตรงตามวัตถุประสงค์และพันธกิจขององค์กรหรือเรียกอีกอย่างว่า "ไอทีภิบาล"

ประเด็นเกี่ยวกับไอทีภิบาลมิใช่มีเพียงกรอบวิธีปฏิบัติของ COBIT เท่านั้นที่ได้กล่าวถึง แต่ในมาตรฐานอื่นๆ และแนวทางปฏิบัติด้านไอทีที่ดีหลายๆ เรื่องเช่นที่กล่าวมาข้างต้นก็มีการกล่าวถึงประเด็นด้านไอทีภิบาลเช่นกัน การกล่าวถึงไอทีภิบาลของมาตรฐานและแนวทางปฏิบัติด้านไอทีที่ยกมาเป็นตัวอย่างนั้น ในบางตัวอย่างมีการบรรยายหรือสร้างความเข้าใจในข้อกำหนดตลอดจนระบุแนวทางในการปฏิบัติจริงโดยมีรายละเอียดที่ครอบคลุมและลงลึกทางเทคนิคมากกว่ากรอบวิธีปฏิบัติของ COBIT และบางตัวอย่างสามารถใช้เป็นเครื่องมือในการออกแบบ หรือ เครื่องมือช่วยในการบริหารจัดการโครงการด้านไอที ซึ่งตัวอย่างที่ดีเหล่านี้ต่างก็ได้รับการนำไปประยุกต์ใช้อย่างกว้างขวางเพราะสามารถช่วยให้ประเด็นไอทีภิบาลสามารถนำไปปฏิบัติได้จริง

อย่างไรก็ดี กรอบวิธีปฏิบัติ COBIT แม้จะไม่ใช่คำตอบสำหรับนักบริหารด้านไอทีทุกอย่างแต่ก็ยังเป็นกรอบวิธีปฏิบัติที่ใช้ได้สำหรับรวบรวมเอามาตรฐาน กรอบวิธีปฏิบัติ และแนวทางปฏิบัติ ตลอดจนบางอย่างอาจใช้เป็นเครื่องมือในการบริหารจัดการเพื่อช่วยผู้ปฏิบัติงานให้สามารถทำงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น นอกจากนี้ ในบทวิเคราะห์ผู้ศึกษาได้ให้ความเห็นเกี่ยวกับปัจจัยที่ต้องคำนึงถึงหากจะเลือก มาตรฐาน กรอบวิธีปฏิบัติ หรือแนวทางปฏิบัติใดไปใช้ย่อมต้องพิจารณาถึง

- ปัจจัยเรื่องความสอดคล้องกับข้อกำหนด กฎหมาย
- ปัจจัยเรื่องพันธะผูกพันทางสัญญา
- ปัจจัยที่เกี่ยวข้องกับแผนแม่บท หรือนโยบายด้าน ICT ของประเทศ
- ปัจจัยด้านพันธกิจ ภารกิจ และกลยุทธ์ขององค์กร

เป็นต้น

ท้ายสุดนี้ ตัวอย่างต่างๆ ที่นำมากล่าวนั้น ปัจจุบันอาจมีการเปลี่ยนแปลงหรืออัพเดตให้มีความทันสมัยตามแนวทางของเทคโนโลยีมากยิ่งขึ้น ดังนั้นการค้นหาข้อมูลเพิ่มเติมจะสามารถช่วยให้ผู้อ่านได้เห็นภาพที่เป็นปัจจุบันมากขึ้น และสื่ออินเทอร์เน็ตสามารถนำความรู้เหล่านี้เผยแพร่ให้นักบริหารด้านไอที ได้ทำศึกษาและทำความเข้าใจได้โดยง่าย ผู้ศึกษาเห็นว่าการได้ทดลองเข้าไปใช้งานเนื้อหาเหล่านี้ น่าจะช่วยอำนวยประโยชน์ให้กับระบบสารสนเทศขององค์กรของท่านไม่ทางใดก็ทางหนึ่ง

แหล่งข้อมูลอ้างอิง

[1] IT Governance Institute (ITGI), **COBIT Mapping Overview of International IT Guidance**, **2rd Edition**, www.itgi.org
[2] International Organization for Standardization (ISO), www.iso.org
[3] National Institute of Standards and Technology (NIST), www.nist.gov
[4] Project Management Institute**, A Guide to the Project Management Body of Knowledge (PMBOK® Guide)**, 3rd Edition, 2004, figure 3-45
[5] www.isaca.org/cobit
[6] www.ogc.gov.uk
[7] www.sei.cmu.edu/cmmi
[8] www.tickit.org