MASCIntelligence

วารสารความเคลื่อนไหวเกี่ยวกับการมาตรฐาน

ISSN 1905-842X
Vol. 2 / No. 13
July-September 2008

Supply Chain & Information Technology

CONTENT

สารบัญ

About Us

สถาบันรับรองมาตรฐานไอเอสโอ ได้รับมอบหมายภารกิจจากสำนักงานเศรษฐกิจอุตสาหกรรม กระทรวงอุตสาหกรรม ในการดำเนินโครงการสร้างระบบข้อมูลองค์ความรู้ และการเตือนภัยด้านมาตรฐานระบบการจัดการแก่ธุรกิจอุตสาหกรรมและหน่วยงานอื่นๆ ที่เกี่ยวข้อง ผู้สนใจสามารถสมัครเพื่อขอรับวารสาร MASCIntelligence เป็นประจำได้ โดยเขียนชื่อ-ที่อยู่ พร้อมหมายเลขโทรศัพท์ แล้ว Fax กลับมาที่หมายเลข 02-617-1708 โดยไม่เสียค่าใช้จ่ายใดๆ

ฝ่ายหน่วยตรวจ
สถาบันรับรองมาตรฐานไอเอสโอ

EDITOR'S NOTE

ในภาวะการณ์ปัจจุบันที่วิกฤติพลังงานส่งผลกระทบต่อภาคอุตสาหกรรมของไทย การจัดการห่วงโซ่อุปทานที่มีประสิทธิภาพได้เข้ามามีบทบาทเป็นตัวช่วยเหลือที่ทำให้ภาคอุตสาหกรรมฟันฝ่าวิกฤตินี้ไปได้ ขณะนี้ ISO ได้มีการกำหนดมาตรฐานเกี่ยวกับด้านห่วงโซ่อุปทาน เป็นอนุกรมมาตรฐาน ISO 28000 ซึ่งได้ประกาศใช้ล่าสุดเมื่อเดือนกันยายน 2550 ที่ผ่านมา ซึ่ง MASCIntelligence ฉบับนี้จะได้กล่าวถึงมาตรฐานดังกล่าว รวมทั้งความรู้หลากหลายเกี่ยวกับเรื่องของห่วงโซ่อุปทาน นอกจากนี้ ยังมีเนื้อหาที่น่าสนใจอื่นๆ เกี่ยวกับระบบการจัดการด้านเทคโนโลยีสารสนเทศ ซึ่งมีกระแสความตื่นตัวอย่างมาก โดย ISO ประกาศมาตรฐานต่างๆ ที่เกี่ยวข้องกว่า 30 มาตรฐาน นอกจากนี้ ในเล่มยังจะได้พบกับ สบทร. หน่วยงานที่ได้รับการรับรองระบบการจัดการความปลอดภัยสารสนเทศ หรือ ISO 27001 เป็นหน่วยงานแรกของประเทศไทย

ขอแถมท้ายอีกสักเรื่อง คือ มาตรฐานระบบบริหารงานคุณภาพ ISO 9001:2000 กำลังอยู่ระหว่างการดำเนินการปรับปรุงแก้ไข โดยขณะนี้อยู่ระหว่างการประกาศเป็น Version FDIS และคาดการณ์ว่าจะมีการประกาศเป็นมาตรฐานฉบับสมบูรณ์ในช่วงปลายปีนี้ถึงต้นปีหน้า ซึ่งรายละเอียดจะได้มีการนำเสนอในวาระต่อไป

ท้ายที่สุด ขอขอบคุณสำนักงานเศรษฐกิจอุตสาหกรรม กระทรวงอุตสาหกรรม ที่ให้การสนับสนุน MASCIntelligence ด้วยดีเสมอมา รวมทั้งผู้อ่านที่ให้ความสนใจใน MASCIntelligence

หากมีข้อติชมประการใด สามารถส่งข้อคิดเห็นมาได้ที่
E-mail : IBD@masci.or.th

BEST PRACTICE

แนวทางปฏิบัติที่ดี
ระบบการจัดการความปลอดภัยสำหรับห่วงโซ่อุปทาน

มาตรฐาน ISO 28001:2007 Security management systems for the supply chain - Best practices for implementing supply chain security- assessment and plans - Requirements and guidance นี้เป็นมาตรฐานที่สามารถขอรับการรับรองได้ จัดทำขึ้นเพื่อเป็นแนวทางสำหรับองค์กรในการกำหนดระดับของความปลอดภัยที่พอเพียงสำหรับห่วงโซ่อุปทานขององค์กร และใช้เป็นบรรทัดฐานในการพิจารณาหรือทวนสอบระบบความปลอดภัยของห่วงโซ่อุปทานที่มีอยู่แล้วในองค์กร นอกจากนั้น มาตรฐานฉบับนี้ยังช่วยในการดำเนินการให้สอดคล้องตามหลักเกณฑ์ของ Authorized Economic Operators (AEO) อีกด้วย มาตรฐานนี้ประกอบไปด้วย

ข้อ 1: ขอบข่าย (Scope)
ข้อ 2: เอกสารอ้างอิง (Normative reference)
ข้อ 3: บทนิยามและคำศัพท์ (Term and definitions)
ข้อ 4: ขอบเขตการนำไปประยุกต์ใช้ (Field of application)

1. ต้องมีคำอธิบายการนำไปประยุกต์ใช้ (Statement of Application) โดยอย่างน้อยต้องมีข้อมูลรายละเอียดเกี่ยวกับตัวองค์กร ขอบข่าย รายละเอียดการติดต่อกับพันธมิตรทางธุรกิจ วันที่ประเมินและระยะเวลาที่มีผลบังคับใช้ และลายมือชื่อผู้มีอำนาจลงนามขององค์กร
2. หากมีการใช้พันธมิตรทางธุรกิจมาเป็นส่วนหนึ่งในห่วงโซ่อุปทาน พันธมิตรทางธุรกิจจะต้องมีคำประกาศด้านความปลอดภัย
3. การได้รับการรับรองหรือการอนุมัติที่เป็นที่ยอมรับในระดับสากลโดยองค์กรที่มีใบรับรองตามสนธิสัญญาสากลฉบับบังคับในการบริหารจัดการความปลอดภัย โดยมีแนวทางปฏิบัติแผนงานและกระบวนการด้านความปลอดภัยเป็นไปตามข้อกำหนดของมาตรฐานฉบับนี้ ไม่จำเป็นต้องได้รับการตรวจประเมินความสอดคล้อง
4. พันธมิตรทางธุรกิจที่ได้รับการยกเว้นการแสดงขีดความสามารถด้านความปลอดภัย ได้แก่ ผู้ที่ได้รับการทวนสอบแล้วว่าสอดคล้องกับมาตรฐาน ISO 28001:2007 หรือ ISO 20858 ผู้ที่ได้รับการรับรองตามข้อ 3 ข้างต้น ผู้ที่ได้รับการแต่งตั้งเป็น AEO
5. การทบทวนความปลอดภัยของพันธมิตรทางธุรกิจ ต้องพิจารณาจากผลการประเมินความเสี่ยงเป็นสำคัญ

ข้อ 5: กระบวนการด้านความปลอดภัยห่วงโซ่อุปทาน (Supply chain security process)

1. องค์กรจะต้องบริหารจัดการความปลอดภัยครอบคลุมห่วงโซ่อุปทานที่เกี่ยวข้อง และต้องมีระบบการจัดการเพื่อสนับสนุนวัตถุประสงค์ดังกล่าว โดยจะต้องมีแนวทางปฏิบัติและกระบวนการเพื่อลดความเสี่ยงในห่วงโซ่อุปทาน ระบุอยู่ใน**คำอธิบายการนำไปประยุกต์ใช้** (Statement of Application) ที่กำหนดไว้ข้างต้น
2. การประเมินความปลอดภัยจะต้องครอบคลุมกิจกรรมทั้งหมดขององค์กรตามที่ระบุในคำอธิบายการนำไปประยุกต์ใช้ที่กำหนดไว้ข้างต้น โดยการประเมินความปลอดภัยจะต้องครอบคลุมระบบสารสนเทศเอกสารและเครือข่ายต่างๆ ที่เกี่ยวข้องกับการเคลื่อนย้ายหรือการขนถ่ายสินค้าที่อยู่ภายใต้การเก็บรักษาขององค์กร
3. การประเมินความปลอดภัย
   - ผู้ตรวจประเมินจะต้องมีทักษะและความรู้ที่เกี่ยวข้อง ได้แก่ เทคนิคการประเมินความเสี่ยงที่เกี่ยวข้องกับประเด็นด้านห่วงโซ่อุปทาน การประยุกต์ใช้มาตรการเพื่อหลีกเลี่ยงการเปิดเผยของวัตถุดิบที่ไวต่อความปลอดภัย ความเข้าใจต่อภัยคุกคามและวิธีการลดความรุนแรงและอื่นๆ
   - องค์กรต้องจัดทำขั้นตอนการปฏิบัติงานที่ระบุมาตรการในการตอบโต้เพื่อลดความรุนแรงของภัยคุกคาม จัดทำรายการของสถานการณ์ภัยคุกคามที่เกี่ยวข้อง และจะต้องประเมินมาตรการตอบโต้ที่มีอยู่ในการรับมือกับแต่ละสถานการณ์ รวมถึง พิจารณาความเป็นไปได้และผลที่จะตามมาจากแต่ละสถานการณ์ โดยอาจมีการเพิ่มมาตรการที่จำเป็นเพื่อลดความเสี่ยงให้ลงมาสู่ระดับที่ยอมรับได้
   - องค์กรต้องทบทวนคำประกาศด้านความปลอดภัยของพันธมิตรทางธุรกิจโดยใช้ความเป็นมืออาชีพ ความรู้ และกฎระเบียบของหน่วยงานที่เกี่ยวข้อง เป็นเกณฑ์ในการทบทวน
4. องค์กรจะต้องพัฒนาและคงไว้ซึ่งแผนความปลอดภัยตามที่ระบุในคำอธิบายการนำไปประยุกต์ใช้ที่กำหนดไว้ข้างต้น
5. เมื่อองค์กรได้จัดทำแผนแล้วเสร็จ จะต้องจัดทำระบบการจัดการเพื่อนำแผนดังกล่าวไปปฏิบัติใช้
6. องค์กรจะต้องจัดทำขั้นตอนการปฏิบัติงานการจัดทำเอกสาร การเฝ้าระวัง และการวัดสมรรถนะของระบบการจัดการและต้องดำเนินการตรวจติดตามตามช่วงเวลาที่กำหนด ผลของการตรวจติดตามต้องจัดทำเป็นเอกสารและเก็บรักษาไว้ นอกจากนั้นองค์กรจะต้องประเมินโอกาสในการปรับปรุงอย่างต่อเนื่องเพื่อเพิ่มขีดความสามารถด้านความปลอดภัย
7. องค์กรจะต้องทบทวนแผนความปลอดภัยภายหลังจากการเกิดอุบัติการณ์ด้านความปลอดภัยที่เกี่ยวข้องในส่วนของห่วงโซ่อุปทานที่องค์กรควบคุมอยู่ โดยการทบทวนจะต้อง
   - พิจารณาสาเหตุของอุบัติการณ์และหาแนวทางการแก้ไข
   - พิจารณาประสิทธิผลของมาตรการและขั้นตอนการปฏิบัติงานสำหรับการกู้ความปลอดภัยกลับคืน
   - ตรวจประเมินซ้ำตามกระบวนการตรวจประเมินโดยใช้ผลจากการพิจารณาข้างต้น

หากเกิดเหตุการณ์ที่ฝ่าฝืนความปลอดภัย องค์กรต้องดำเนินการตามขั้นตอนการปฏิบัติงานในการแจ้งไปยังศุลกากรหรือหน่วยงานผู้บังคับใช้กฎหมาย

• *ISO 28001: 2007 – Security Management Systems for the Supply Chain – Best Practices for implementing supply chain security, assessment and plans- Requirements and guidance*

บทความน่ารู้

เข้าใจโลจิสติกส์... ไม่ยาก อย่างที่คิด

คำว่า **"โลจิสติกส์ (Logistic)"** ได้ถูกใช้กันอย่างแพร่หลายในปัจจุบัน โดยคนส่วนใหญ่ยังมีความเข้าใจว่าโลจิสติกส์คือการขนส่งแต่เพียงอย่างเดียว หากพิจารณาคำจำกัดความโดย Council of Supply Chain Management Professionals (2004) **"โลจิสติกส์" ถือเป็นส่วนหนึ่งของกระบวนการห่วงโซ่อุปทาน** ซึ่งประกอบด้วย

- การวางแผน
- การนำไปปฏิบัติ
- การควบคุม
- การไหลทั้งไปและกลับ
- รวมถึง...**การจัดเก็บสินค้า บริการ และข้อมูลข่าวสาร** ที่เกี่ยวข้องอย่างมีประสิทธิภาพ จากต้นทางไปยังแหล่งบริโภค ปลายทาง

เพื่อตอบสนองความต้องการของลูกค้า ทั้งนี้ ได้มี**การแบ่งโลจิสติกส์ ออกเป็นกิจกรรมย่อยมากถึง 14 กิจกรรม**ด้วยกัน ได้แก่

1) การบริการลูกค้า
2) การพยาบาลอุปสงค์
3) การสื่อสารด้านการกระจายสินค้า
4) การจัดการสินค้าคงคลัง
5) การขนถ่ายวัสดุ
6) การดำเนินการกับคำสั่งซื้อ
7) การบริการหลังการขาย
8) การเลือกที่ตั้งของโรงงานและคลังสินค้า
9) การจัดหาวัตถุดิบและบริการ
10) การบรรจุภัณฑ์
11) การนำสินค้ากลับคืน
12) การกำจัดสิ่งปฏิกูลจากกระบวนการผลิต
13) การจราจรและขนส่ง
14) การบริหารคลังสินค้าและการจัดเก็บ

การจัดการโลจิสติกส์อย่างมีประสิทธิภาพได้เข้ามามีบทบาทสำคัญต่อการดำเนินธุรกิจในยุคโลกาภิวัตน์ที่มุ่งเน้นการสร้างขีดความสามารถในการแข่งขันจากการประหยัดต้นทุนและการสร้างความพึงพอใจแก่ลูกค้า ทั้งทางด้านความรวดเร็วและความถูกต้องแม่นยำในการส่งมอบสินค้า ตลอดจนการนำเสนอความหลากหลายของสินค้าตามความต้องการที่แตกต่างกัน (Mass Customization)

หลักการสำคัญในการจัดการโลจิสติกส์ คือ ความพยายามในการลดต้นทุน ในขณะที่ไม่ทำให้ระดับการให้บริการแก่ลูกค้าลดลง โดยมุ่งเน้นการปรับปรุงในทุกกระบวนการที่เกี่ยวข้องตามแนวคิด **"Total Cost Tradeoff" ที่ให้ความสำคัญกับการลดต้นทุนโลจิสติกส์รวม** แทนที่การลดต้นทุนในกิจกรรมใดกิจกรรมหนึ่งเพียงอย่างเดียว เนื่องจากกิจกรรมต่างๆในระบบโลจิสติกส์มีความสัมพันธ์และส่งผลกระทบซึ่งกันและกัน อาทิเช่น การตัดสินใจเปลี่ยนรูปแบบการขนส่งจากทางทะเลซึ่งมีค่าขนส่งต่ำ ไปใช้การขนส่งทางอากาศที่มีค่าขนส่งสูง แต่สามารถนำส่งสินค้าได้รวดเร็วกว่า ซึ่งระยะเวลาการขนส่งที่สั้นลงส่งผลให้ไม่ต้องถือครองสินค้าคงคลังไว้เป็นจำนวนมาก หากค่าใช้จ่ายในการถือครองสินค้าคงคลังลดลงมากกว่าค่าใช้จ่ายที่เพิ่มขึ้นจากการขนส่งทางอากาศ การตัดสินใจเปลี่ยนรูปแบบการขนส่งก็เป็นสิ่งที่พึงกระทำ เพราะสามารถลดต้นทุนโลจิสติกส์โดยรวมลงได้ **ดังนั้น เพื่อให้สามารถบริหารระบบโลจิสติกส์อย่างมีประสิทธิภาพ ผู้ตัดสินใจต้องมองผลกระทบต่อภาพรวมของระบบ (Holistic view) เป็นสำคัญ**

การเลือกใช้กลยุทธ์ด้านโลจิสติกส์ให้เหมาะสมยังขึ้นอยู่กับลักษณะของสินค้า สินค้าทั่วไปที่มีการใช้งานเป็นประจำ หรือที่เรียกว่า "Functional Products" เช่น สบู่ ยาสระผม ยาสีฟัน จะมีอุปสงค์ที่ค่อนข้างแน่นอนและสามารถคาดเดาได้ไม่ยาก วงจรชีวิตของสินค้ายาวเนื่องจากเป็นสินค้าที่มีความต้องการใช้อยู่เสมอ สินค้าต่างยี่ห้อกันสามารถนำมาใช้ทดแทนกันได้ และมีกำไรต่อหน่วยต่ำ ดังนั้น**กลยุทธ์ด้านโลจิสติกส์ที่เหมาะสมจึงเป็นการบริหารต้นทุนโลจิสติกส์ให้ต่ำที่สุด(Cost Efficiency) เพื่อให้สินค้าสามารถแข่งขันได้ในตลาดที่มีราคาเป็นปัจจัยหลัก**

ในขณะที่สินค้าแฟชั่นและ**สินค้าที่มีความทันสมัยหรือใช้เทคโนโลยีสูง (Fashionable and Innovative Products)** เช่น เสื้อผ้าแฟชั่นตามฤดูกาล อุปกรณ์อิเล็คโทรนิกส์และคอมพิวเตอร์ มักมีอุปสงค์ที่แปรปรวนและคาดเดาได้ยากกว่า สินค้ามีวงจรชีวิตค่อนข้างสั้นจากการผลิตรุ่นใหม่ออกมาบ่อยๆ ตามความก้าวหน้าทางเทคโนโลยี การมีสินค้าไม่เพียงพอต่อความต้องการของลูกค้าอาจทำให้สูญเสียโอกาสในการขายได้ เนื่องจากสินค้าประเภทนี้สามารถสร้างกำไรต่อหน่วยได้สูง **กลยุทธ์ด้านโลจิสติกส์จึงไม่มุ่งเน้นในเรื่องการลดต้นทุน แต่ให้ความสำคัญแก่การตอบสนองความต้องการของลูกค้า (Responsiveness) ทั้งทางด้านความหลากหลายของตัวสินค้า (Variety) การมีสินค้าพร้อมขายเสมอ (Availability) และความรวดเร็วในการจัดส่ง (Speed) เป็นสำคัญ**

การพัฒนาระบบโลจิสติกส์ของประเทศไทย ควรได้รับการดำเนินการทั้งในระดับมหภาคและจุลภาคควบคู่กัน โดยในระดับมหภาค **ภาครัฐต้องจัดหาระบบโครงสร้างพื้นฐานและสิ่งอำนวยความสะดวก**ที่มีความจำเป็นต่อผู้ประกอบการ ตลอดจน**ปรับปรุงกฎระเบียบข้อบังคับที่เกี่ยวข้อง** เพื่อให้ผู้ประกอบการสามารถร่วมใช้ประโยชน์จากโครงสร้างพื้นฐานอย่างคุ้มค่าและเป็นธรรม และขจัดอุปสรรคในการดำเนินงาน

นอกจากนี้ **การยกระดับประสิทธิภาพโลจิสติกส์** จำต้องอาศัยการมีโลจิสติกส์ ในระดับจุลภาคที่ดีโดยการพัฒนาผู้ประกอบการซึ่งถือเป็นตัวขับเคลื่อนสำคัญในระบบโลจิสติกส์ของประเทศ ให้มีความรู้ความเข้าใจในการจัดการโลจิสติกส์ที่ถูกต้องเพื่อนำมาใช้ในการเพิ่มขีดความสามารถในการแข่งขันของกิจการตนเองกับทั้งคู่แข่งภายในประเทศและบริษัทข้ามชาติซึ่งนับวันจะยิ่งทวีจำนวนมากขึ้นจากกระแสโลกาภิวัตน์และการเปิดเสรีทางการค้าที่ไม่สามารถหลีกเลี่ยงได้

เป็นที่ทราบว่า**การจัดการโลจิสติกส์ให้เกิดประสิทธิภาพสูงสุดต้องอาศัยการนำวิทยาการความรู้และเทคโนโลยีสมัยใหม่เข้ามาประยุกต์ใช้ในการวางแผนและควบคุมการทำงาน** วิธีปฏิบัติด้านโลจิสติกส์มากมายได้ถูกพัฒนาขึ้นจากการลองทำจริงแบบลองผิดลองถูกไปจนถึงการทำงานค้นคว้าวิจัยตามหลักทฤษฎี ในปัจจุบัน เทคนิคต่างๆ เช่น **Just-in-time, Postponement, Cross-docking และ Vendor managed inventory** ได้ถูกนำมาใช้กันอย่างแพร่หลาย รวมถึง**การนำความรู้ทางด้าน Operations Research และ Optimization Techniques มาใช้ในการช่วยวิเคราะห์หาแผนปฏิบัติการที่มีประสิทธิภาพที่สุด (Optimal Solution)**

การนำระบบเทคโนโลยีสารสนเทศ (IT) เช่น EDI และ RFID **มาใช้ในการส่งผ่านข้อมูลและติดตามสถานะการขนส่ง รวมถึงการพัฒนาซอฟท์แวร์สำหรับการวางแผนและควบคุม** เช่น ระบบ Enterprise Resource Planning (ERP) อย่างไรก็ตาม การจัดการโลจิสติกส์ที่ดีไม่ใช่การนำเทคนิคและเทคโนโลยีที่มีมาใช้ทั้งหมดโดยขาดการวางแผนและการเข้าใจถึงปัญหาที่แท้จริง

นอกจากนี้ ไม่มีเทคนิคใดๆ ที่สามารถนำมาใช้ได้กับทุกสถานการณ์และในทุกสภาพแวดล้อมของการทำงานได้ ตัวอย่างเช่น การผลิตแบบทันเวลา หรือ Just-in-time ไม่สามารถประสบความสำเร็จได้หากปราศจากผู้จัดหาวัตถุดิบที่มีระบบข้อมูลข่าวสารและการขนส่งที่มีประสิทธิภาพ ซึ่งหากการประยุกต์ใช้เทคนิคอย่างไม่เหมาะสม นอกจากจะทำให้เกิดการสิ้นเปลืองทั้งค่าใช้จ่ายและเวลาแล้ว ยังอาจส่งผลเสียต่อประสิทธิภาพในระบบโลจิสติกส์อีกด้วย

ดังจะเห็นได้ว่า หลายๆ หน่วยงานได้มีการติดตั้งระบบ IT ด้านโลจิสติกส์ด้วยเงินลงทุนมหาศาลแต่ไม่สามารถใช้ประโยชน์จากระบบดังกล่าวได้อย่างคุ้มค่า ดังนั้น **การเลือกรูปแบบของระบบการจัดการโลจิสติกส์ที่เหมาะสมจะต้องคำนึงถึงปัจจัยหลายๆ ด้านประกอบกัน**นอกเหนือจากงบประมาณที่มี เช่น ขนาดขององค์กร ขอบเขตของการใช้งาน ลักษณะของข้อมูลที่ต้องใช้ ความจำเป็น ความพร้อมของบุคลากรและเครื่องมือที่มีอยู่ รวมถึงการเข้าใจถึงสาเหตุที่แท้จริงของปัญหา เป็นต้น

ปัญหาที่องค์กรส่วนใหญ่ทั้งภาครัฐและเอกชนกำลังเผชิญอยู่ คือ การขาดข้อมูลที่สะท้อนถึงประสิทธิภาพของระบบโลจิสติกส์ หากแต่กลับมุ่งเน้นการลงทุนทางด้านโครงสร้างพื้นฐานและระบบ IT

ทั้งนี้ **การปรับปรุงระบบโลจิสติกส์ในเบื้องต้น** ควรเริ่มจากการประเมินระดับการดำเนินงานในปัจจุบันก่อน โดยการวิเคราะห์ขั้นตอนการทำงานทั้งหมด เพื่อให้เห็นถึงสภาพการปฏิบัติงานที่แท้จริงและสามารถ

ระบุปัญหาที่เกิดขึ้นพร้อมประเมินสาเหตุที่เป็นไปได้ ในขั้นตอนนี้การวิเคราะห์ต้นทุนโลจิสติกส์จำแนกตามประเภทของกิจกรรมที่เกี่ยวข้องจึงเป็นสิ่งจำเป็น โดยทั่วไปต้นทุนโลจิสติกส์สามารถจำแนกออกเป็น

- **ต้นทุนการขนส่ง** (Transportation Cost)
- **ต้นทุนสินค้าคงคลัง** (Inventory Holding Cost)
- **ต้นทุนการบริหารจัดการ** (Administration Cost)
- **ต้นทุนจากการขนถ่ายและดูแลสินค้า**(Material Handling and Warehousing Cost)

หลังจากนั้น จึง**หาแนวทางในการปรับปรุงประสิทธิภาพการทำงานให้ดีขึ้นบนพื้นฐานของทรัพยากรเดิม**ที่มีอยู่ โดย**พยายามขจัดกิจกรรมที่ไม่สร้างมูลค่า** (Non-value adding activities) ซึ่งเป็นกิจกรรมที่สร้างความสูญเปล่า (Waste) ออกไปให้ได้มากที่สุด หากจะมีการลงทุนเพิ่มเติมก็ต่อเมื่อเป็นการลงทุนที่คุ้มค่าและมีความจำเป็นต่อการเพิ่มศักยภาพโลจิสติกส์ให้ดีขึ้นเท่านั้น

ดังนั้น **โลจิสติกส์** จึงเป็นเรื่องของการประเมินประสิทธิภาพและการปรับปรุงวิธีการบริหารจัดการมากกว่าการเพิ่มขยายโครงสร้างพื้นฐาน ทั้งนี้ การลงทุนในโครงการต่างๆ จะก่อให้เกิดต้นทุนโลจิสติกส์ทางอ้อมถ้าหากไม่มีการใช้ประโยชน์จากโครงสร้างพื้นฐานนั้นๆ อย่างคุ้มค่า จะเห็นได้ว่า หากเพียงแค่เข้าใจว่าโลจิสติกส์คืออะไร การจัดการก็ไม่ใช่เรื่องยากอีกต่อไป....

ดร. สถาพร โอภาสานนท์ ภาควิชาบริหารธุรกิจระหว่างประเทศโลจิสติกส์ และการขนส่ง คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

บทความน่ารู้

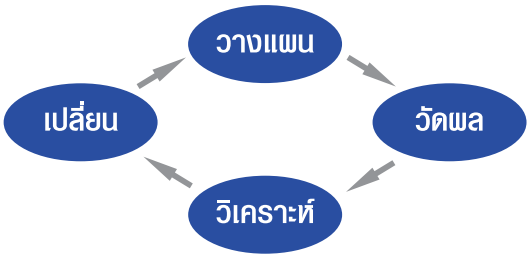
การวัดประสิทธิภาพ และการปรับปรุง ระบบโลจิสติกส์

หากพิจารณาจากคำจำกัดความที่เสนอโดย Council of Supply Chain Management Professionals จะพบว่าโลจิสติกส์มีความเกี่ยวข้องกับกระบวนการวางแผน (Plan) การนำไปปฏิบัติ (Implement) และการควบคุม (Control) การไหลทั้งไปและกลับของสินค้า บริการ และข้อมูลข่าวสาร ทั้งนี้ **องค์ประกอบที่มีความสำคัญต่อกระบวน การวางแผนและการควบคุม** คือ ข้อมูลที่สามารถสะท้อนให้เห็นถึงสถานภาพการดำเนินงานด้านโลจิสติกส์ขององค์กร ซึ่งตัวชี้วัด (Key performance indicators, KPIs) จะถูกใช้ในการประเมินระดับประสิทธิภาพ ณ ปัจจุบัน รวมถึงใช้เปรียบเทียบผลการดำเนินงานในกิจกรรมประเภทเดียวกันกับองค์กรอื่นๆ เพื่อนำมาประกอบการพิจารณาสาเหตุของปัญหาและแนวทางในการปรับปรุงแก้ไข นอกจากใช้ในการวางแผนเพื่อเพิ่มประสิทธิภาพของระบบแล้ว ข้อมูลตัวชี้วัดยังสามารถนำไปใช้ในการควบคุมการดำเนินงานว่าสามารถบรรลุตามเป้าหมายที่วางไว้หรือไม่

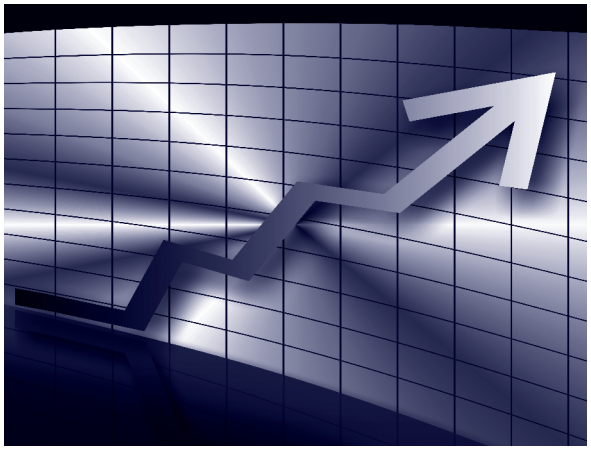
ก่อนที่จะกล่าวถึงการพัฒนาตัวชี้วัดประสิทธิภาพโลจิสติกส์ อยากจะขอชี้แจงถึงคำศัพท์อีกสองคำที่มักถูกใช้ประกอบกันเสมอ ได้แก่ Benchmarking หรือ การเทียบวัด และ Best Practice หรือวิธีปฏิบัติที่ดีที่สุด Benchmarking ได้ถูกนำมาใช้กันอย่างแพร่หลายในการจัดการโลจิสติกส์ ซึ่งเป็นเครื่องมือสำหรับใช้ในการปรับปรุงองค์กรตนเอง โดยทำการวัดและเปรียบเทียบประสิทธิภาพ ตลอดจนวิธีการปฏิบัติในกิจกรรมที่คล้ายคลึงกันกับองค์อื่นๆ เพื่อให้ทราบว่าประสิทธิภาพในการดำเนินงานขององค์กรตนเองเป็นอย่างไร และใครเป็นผู้ปฏิบัติได้ดีที่สุดและมีวิธีการปฏิบัติเป็นอย่างไร หลังจากนั้นจึงนำผลของการเปรียบเทียบกับวิธีปฏิบัติที่ดีที่สุดหรือที่เรียกว่า Best Practice มาประยุกต์ใช้ให้เหมาะสม เพื่อให้ได้วิธีการปฏิบัติที่สามารถทำให้องค์กรตนเองประสบความสำเร็จได้

การเทียบวัด (Benchmarking)

การทำ Benchmarking ประกอบด้วย 4 ขั้นตอนหลัก ได้แก่ **การวางแผน** (Plan) **การวัดผล** (Measure) **การวิเคราะห์** (Analyze) และ**การปรับเปลี่ยน** (Change)



การวางแผน – คัดเลือกกลุ่มตัวชี้วัดที่จะทำการวัดผล และระบุกลุ่มบริษัทที่จะเข้าร่วมโครงการ เพื่อทำการเทียบวัดและแลกเปลี่ยนข้อมูลระหว่างกัน ซึ่งอาจจะเป็นบริษัทคู่แข่งหรือไม่ใช่ก็ได้ และไม่จำกัดว่าจะต้องอยู่ในอุตสาหกรรมเดียวกันเท่านั้น ตัวอย่างเช่น ผู้ผลิตเสื้อผ้าส่งออกอาจต้องการเทียบวัดระยะเวลาและขั้นตอนในการรับคำสั่งซื้อลูกค้า (Order processing) กับบริษัทที่ทำธุรกิจด้านอาหารที่มีบริการส่งตามบ้าน ซึ่งอยู่ต่างอุตสาหกรรมกัน



ดร. สถาพร โอภาสานนท์ ภาควิชาบริหารธุรกิจระหว่างประเทศ โลจิสติกส์ และการขนส่ง คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

การวัดผล – ดำเนินการสำรวจและรวบรวมข้อมูลตัวชี้วัดและวิธีปฏิบัติขององค์กรตนเองและบริษัทที่เข้าร่วมโครงการ

การวิเคราะห์ – นำผลการปฏิบัติงานหรือตัวชี้วัดความสามารถในการปฏิบัติกิจกรรม ตลอดจนวิธีปฏิบัติของแต่ละองค์กรมาเปรียบเทียบและทำการวิเคราะห์หามาตรการในการลดช่องว่างด้านประสิทธิภาพระหว่างองค์กรตนเองกับบริษัทที่ถูกค้นพบว่ามีผลการปฏิบัติที่ดีที่สุด โดยทั่วไปแล้ว อาจจะไม่มีองค์กรใดเลยที่เป็นผู้ปฏิบัติที่ดีที่สุดในทุกๆ กิจกรรม ดังนั้น การวิเคราะห์จึงควรพิจารณา Best Practice แยกตามรายกิจกรรม มากกว่าการมุ่งเน้นไปที่องค์กรใดองค์กรหนึ่งเป็นพิเศษ

การปรับเปลี่ยน – นำมาตรการที่วิเคราะห์ได้มาทดลองปฏิบัติจริง พร้อมสังเกตการณ์ถึงอุปสรรคและผลลัพธ์ของการปฏิบัติ

ขั้นตอนทั้งสี่ควรถูกดำเนินการอย่างต่อเนื่องและสม่ำเสมอ เนื่องจาก Best Practice มีการเปลี่ยนแปลงอยู่ตลอดเวลาตามความพยายามของแต่ละองค์กรที่จะพัฒนาวิธีปฏิบัติให้ดีขึ้นอยู่เสมอ และยังขึ้นอยู่กับว่ามีผู้ทำได้ดีกว่ามากน้อยเพียงใด ดังนั้น เพื่อให้เกิดการพัฒนาอย่างต่อเนื่อง แต่ละองค์กรจึงควรทำการวัดประสิทธิภาพของตนเองและเปรียบเทียบกับผู้ประกอบการรายอื่นเป็นประจำ

จะเห็นได้ว่า หากปราศจากการทำ Benchmarking แล้ว องค์กรจะไม่สามารถทราบได้ว่าการดำเนินงานในส่วนไหนบ้างที่ควรได้รับการปรับปรุงให้ดีขึ้น ตัวอย่างเช่น บริษัทให้บริการโลจิสติกส์รายหนึ่งอาจพึงพอใจกับความสามารถในการเคลื่อนย้ายสินค้าภายในคลังสินค้าที่บริษัททำได้ในอัตรา 200 ชิ้นต่อชั่วโมง จวบจนกระทั่งได้ทำการเทียบวัดกับบริษัทอื่นที่สามารถปฏิบัติได้ดีกว่าในอัตรา 300 ชิ้นต่อชั่วโมง นอกจากนี้ Benchmarking ยังทำให้สามารถระบุได้ว่าใครคือ Best Practice ในแต่ละด้าน และองค์กรเหล่านั้นมีวิธีในการปฏิบัติเช่นไร

การพัฒนาตัวชี้วัดประสิทธิภาพด้านโลจิสติกส์

Benchmarking จะให้ความสำคัญแก่การสร้างกระบวนการเรียนรู้และทำความเข้าใจในรายละเอียดของขั้นตอนการดำเนินงานในแต่ละกิจกรรมเพื่อแสวงหาแนวทางในการปรับปรุงระบบให้ดีขึ้น โดยไม่ได้มุ่งเน้นเฉพาะการวัดประสิทธิภาพแต่เพียงอย่างเดียว อย่างไรก็ตาม เพื่อให้มีข้อมูลที่ชัดเจนในการประเมินผลของหน่วยงาน การพัฒนาตัวชี้วัดก็ยังคงถือว่ามีบทบาทสำคัญและเป็นขั้นตอนที่ขาดไม่ได้ในการวางแผนทำ Benchmarking โดยการจัดทำชุดตัวชี้วัดที่เหมาะสมจะช่วยให้สามารถวัดและเปรียบเทียบประสิทธิภาพการดำเนินงานด้านโลจิสติกส์กับองค์กรอื่นๆ ได้อย่างถูกต้องแม่นยำ ลดอคติและความคลาดเคลื่อนที่อาจเกิดขึ้นได้ ตลอดจนเป็นตัวบ่งชี้ทิศทางการพัฒนาปรับปรุงรูปแบบการทำงานในด้านต่างๆ เพื่อลดช่องว่างระหว่างองค์กรตนเองกับผู้ปฏิบัติที่ดี

การเลือกชุดตัวชี้วัด เพื่อทำการสำรวจข้อมูลจึงควรพิจารณาจากปัจจัยที่มีความสำคัญต่อขีดความสามารถในการดำเนินแผนกลยุทธ์หลักขององค์กรให้ประสบความสำเร็จได้ ทั้งนี้ กลยุทธ์ทางด้านการจัดการโลจิสติกส์และโซ่อุปทานสามารถแบ่งออกได้เป็น 2 แนวทาง ได้แก่ **การมีประสิทธิภาพทางด้านต้นทุน** (Cost Efficiency) **และการตอบสนองความต้องการของลูกค้า** (Responsiveness)

- ตัวอย่างของตัวชี้วัดประสิทธิภาพด้านต้นทุน ได้แก่
  - ต้นทุนการถือครองสินค้าคงคลัง
  - สัดส่วนของระยะทางการวิ่งรถเที่ยวเปล่า
  - อัตราการใช้ประโยชน์จากพื้นที่ในคลังสินค้า
  - ค่าใช้จ่ายในการบำรุงรักษายานพาหนะ
- ตัวอย่างของตัวชี้วัดประสิทธิภาพด้านการตอบสนอง ได้แก่
  - ร้อยละของการส่งมอบสินค้าได้ครบถ้วนตามจำนวนที่ลูกค้าสั่งและตรงเวลา
  - ระยะเวลาในการส่งมอบสินค้า
  - ระยะเวลาที่ใช้ในการตรวจปล่อยสินค้าและดำเนินพิธีศุลกากร
  - ความถูกต้องของใบแจ้งหนี้และเอกสารอื่นๆ

สำหรับการนำตัวชี้วัดมาใช้ในการควบคุมการดำเนินงานขององค์กรให้เป็นไปตามเป้าหมายที่วางไว้ การกำหนด KPI ควรอยู่ในวิสัยที่ผู้รับผิดชอบในกิจกรรมนั้นๆ สามารถควบคุมและจัดการได้ในช่วงระยะเวลาที่กำหนดไว้เท่านั้น

หัวใจสำคัญของการวัดประสิทธิภาพและการพัฒนากระบวนการทำงานด้านโลจิสติกส์ให้เป็นเลิศ คือ การได้รับความร่วมมือจากทุกฝ่ายที่เกี่ยวข้องทั้งภายในและภายนอกองค์กรตลอดจนต้องมีการสำรวจข้อมูลอย่างจริงจังเป็นประจำเพื่อส่งเสริมให้เกิดการพัฒนาอย่างต่อเนื่อง ดังที่ได้กล่าวไว้ข้างต้น เป็นไปได้ยากที่บริษัทหนึ่งๆ จะเป็นผู้ปฏิบัติที่ดีที่สุดในทุกๆ ด้าน ดังนั้น ความสำคัญของการทำ Benchmarking คือ การที่จะพยายามพัฒนาองค์กรของตนเองให้เป็น Best Practice ในกิจกรรมที่ส่งผลสำคัญต่อการประสบความสำเร็จขององค์กรโดยรวม ดังนั้น ตัวชี้วัดที่ใช้จึงต้องสะท้อนถึงความสำเร็จหรือล้มเหลว ตามวัตถุประสงค์หรือเป้าหมายขององค์กรเป็นสำคัญ

...ห่วงโซ่อุปทาน (Supply Chain)...

Supply Chain

ห่วงโซ่อุปทาน หรือ Supply Chain **หรือบางครั้งใช้คำว่า** Logistics Network หมายถึง ระบบขององค์กร มนุษย์ กิจกรรม สารสนเทศ และทรัพยากรที่เกี่ยวข้องในการเคลื่อนย้ายผลิตภัณฑ์ หรือบริการจากผู้ส่งมอบ (Supplier) ไปยังลูกค้า หรือผู้มีส่วนได้ส่วนเสียต่างๆ

กิจกรรมที่เกี่ยวข้องกับห่วงโซ่อุปทานนั้น จะแปลงทรัพยากรธรรมชาติ วัตถุดิบและองค์ประกอบต่างๆ ไปเป็นผลิตภัณฑ์สำเร็จรูปที่ส่งมอบไปยังลูกค้าสุดท้าย ซึ่งกิจกรรมต่างๆ ดังกล่าวมักจะมีความสับสนเกิดขึ้นระหว่างคำว่า "ห่วงโซ่อุปทาน" และ "โลจิสติกส์"

"โลจิสติกส์ (Logistic)" นั้น จะใช้กับกิจกรรมภายในองค์กรเพียงองค์กรเดียวในการกระจายสินค้า ในขณะที่ **"ห่วงโซ่อุปทาน** (Supply Chain)" จะครอบคลุมถึงการผลิต การจัดซื้อ และมีการมุ่งเน้นในมุมมองที่กว้างกว่า ซึ่งจะรวมถึงองค์กรที่หลากหลาย รวมทั้งผู้ส่งมอบ ผู้ผลิต ผู้ค้าปลีกที่จะทำงานร่วมกัน เพื่อสนองตอบความต้องการของลูกค้า

การจัดการห่วงโซ่อุปทาน (Supply Chain Management)

การจัดการห่วงโซ่อุปทาน (Supply Chain Management) คือ กระบวนการในการวางแผน การนำไปปฏิบัติใช้ และการควบคุมการดำเนินการของห่วงโซ่อุปทานให้มีประสิทธิภาพมากที่สุดเท่าที่จะเป็นไปได้

การจัดการห่วงโซ่อุปทานนั้น ครอบคลุมถึงการเคลื่อนย้ายและการจัดเก็บทั้งหมดตั้งแต่วัตถุดิบ สินค้าคงคลังในระหว่างผลิต จนกระทั่งผลิตภัณฑ์สำเร็จรูปจากแหล่งกำเนิดไปยังแหล่งบริโภค

บางองค์กรได้ให้คำจำกัดความของ**การจัดการห่วงโซ่อุปทาน** โดยหมายรวมถึงการวางแผนและการจัดการของทุกกิจกรรมที่เกี่ยวข้องกับการหาแหล่งวัตถุดิบหรือทรัพยากร การจัดซื้อ การแปรสภาพ และการจัดการด้านโลจิสติกส์ และยังรวมถึงการประสานงานและความร่วมมือกับพันธมิตรต่างๆ ไม่ว่าจะเป็นผู้ส่งมอบ คนกลาง บุคคลที่สาม และลูกค้า

วัตถุประสงค์เบื้องต้นของการจัดการห่วงโซ่อุปทานก็คือ เพื่อตอบสนองความต้องการของลูกค้าโดยใช้ทรัพยากรอย่างมีประสิทธิภาพ รวมทั้งขีดความสามารถในการกระจายสินค้า การเก็บสินค้าคงคลังและแรงงาน ดังนั้น แนวคิดในการเพิ่มประสิทธิภาพโดยการใช้การรับจ้างช่วงไปยังองค์กรอื่นที่สามารถดำเนินการได้ดีกว่า เพื่อลดการควบคุมเชิงการบริหารจัดการของการดำเนินงานประจำวัน ซึ่งการลดการควบคุมและเพิ่มพันธมิตรของห่วงโซ่อุปทานเป็นที่มาของแนวคิดด้านการจัดการห่วงโซ่อุปทาน

วัตถุประสงค์อีกประการหนึ่งของการจัดการห่วงโซ่อุปทานก็คือ ช่วยปรับปรุงพัฒนาความเชื่อมั่นและความร่วมมืออันดีระหว่างพันธมิตรของห่วงโซ่อุปทานอีกด้วย

พัฒนาการของการจัดการห่วงโซ่อุปทาน

วิวัฒนาการของการศึกษาการจัดการห่วงโซ่อุปทาน พบว่า แบ่งเป็น 6 ยุคหลักๆ ด้วยกันคือ

1. Creation Era: คำว่าการจัดการห่วงโซ่อุปทานเริ่มใช้ครั้งแรกโดยที่ปรึกษาด้านอุตสาหกรรมชาวอเมริกันในช่วงต้นทศวรรษที่ 1980 แต่อย่างไรก็ตาม แนวคิดด้านการจัดการห่วงโซ่อุปทานมีมานานแล้วตั้งแต่ต้นศตวรรษที่ 20 โดยเฉพาะในเรื่องการคิดค้นสายการประกอบ ลักษณะของการจัดการห่วงโซ่อุปทานในยุคนี้จะรวมถึงการเปลี่ยนแปลงในอุตสาหกรรมขนาดใหญ่ Re-engineering และการลดขนาดองค์กร (Downsizing) ซึ่งถูก

ขับเคลื่อนโดยการลดต้นทุนค่าใช้จ่ายและแนวคิดด้านการบริหารจัดการของญี่ปุ่น

2. **Integration Era:** การศึกษาการจัดการห่วงโซ่อุปทานมุ่งเน้นไปที่การพัฒนาระบบ Electronic Data Exchange (EDE) ในช่วงปี 1960 และพัฒนาจนถึงช่วงปี 1990 โดยการนำระบบ Enterprise Resource Planning (ERP) เข้ามา ในยุคนี้ยังคงมีการพัฒนาต่อมาเรื่อยๆ จนเข้าสู่ศตวรรษที่ 21 จนก้าวเข้าสู่ระบบ internet-based วิวัฒนาการของห่วงโซ่อุปทานในยุคนี้เป็นการผสานระหว่างการให้มูลค่าเพิ่มและการลดต้นทุนค่าใช้จ่าย

3. **Globalization Era:** พัฒนาการของการจัดการห่วงโซ่อุปทานให้ความสำคัญระบบที่มีการเชื่อมโยงผู้ส่งมอบทั่วโลกและการขยายห่วงโซ่อุปทานข้ามเขตแดนของประเทศไปยังประเทศอื่น ยุคนี้จัดว่าเป็นยุคโลกาภิวัฒน์ของการจัดการห่วงโซ่อุปทาน โดยมีเป้าหมายในการเพิ่มความสามารถในการแข่งขัน การให้มูลค่าเพิ่ม และการลดต้นทุนค่าใช้จ่ายโดยผ่านวิธีการ global sourcing

4. **Specialization Era—Phase 1— Outsourced Manufacturing and Distribution:** ในช่วงปี 1990 อุตสาหกรรมเริ่มมุ่งเน้นในเรื่องความสามารถหลักขององค์กรและการเลือกใช้แนวคิดเฉพาะใหม่ๆ เข้ามาใช้ในองค์กร โดยเริ่มที่จะไม่สนแนวคิดเรื่อง Vertical integration การปฏิบัติงานที่ไม่ใช่ความสามารถหลักขององค์กร และใช้วิธีการรับจ้างช่วงไปยังองค์กรเฉพาะอื่นๆ ผู้ผลิตแบบ OEM ได้กลายเป็นเจ้าของยี่ห้อสินค้า ซึ่งต้องควบคุมห่วงโซ่อุปทานทั้งสายจากผู้ส่งมอบสินค้ามากกว่าการควบคุมกระบวนการภายใน ดังนั้น ผู้รับจ้างผลิตจะต้องบริหารจัดการใบรายการวัตถุดิบ (BOM) โดยระบบการให้หมายเลขสำหรับ OEM หลายรายที่แตกต่างกัน

5. **Specialization Era—Phase 2— Supply Chain Management as a Service:** เริ่มต้นตั้งแต่ช่วงปี 1980 โดยเริ่มต้นจากค่าธรรมเนียมในการขนส่ง การจัดการคลังสินค้า และบริษัทขนส่ง และได้ก้าวหน้าเกินกว่าการเป็นเพียงแค่การขนส่งและโลจิสติกส์ กลายเป็นการวางแผน ความร่วมมือ การปฏิบัติการด้านอุปทานและการบริหารจัดการสมรรถนะ

ความสนใจเฉพาะด้านห่วงโซ่อุปทานจะช่วยให้องค์กรสามารถปรับปรุงความสามารถที่จะนำพาองค์กรไปสู่ความสำเร็จในทิศทางเดียวกันกับผู้ผลิตแบบรับจ้างช่วงและผู้กระจายสินค้า ทำให้สามารถพัฒนาให้คู่ค้าหรือพันธมิตรการค้ามาร่วมในการจัดการห่วงโซ่อุปทานเพื่อเพิ่มสมรรถนะและประสิทธิภาพการบริหารจัดการให้สูงขึ้น

เทคโนโลยีซอฟแวร์สำหรับห่วงโซ่อุปทานเริ่มต้นตั้งแต่ช่วงปลายทศวรรษ 1990 และได้ก้าวหน้าจาก Application Service Provider (ASP) model ในช่วงประมาณปี 1998 ถึง 2003 มาจนเป็น On-Demand model ในช่วงระหว่างปี 2003 ถึง 2006 และมาเป็น Software as a Service (SaaS) model จนถึงปัจจุบัน

6. **Supply Chain Management 2.0 (SCM 2.0):** ในยุคของ SCM 2.0 นี้จะกล่าวถึงการเปลี่ยนแปลงของทั้งยุค Globalization และ Specialization รวมทั้ง วิวัฒนาการของกระบวนการ วิธีการ และเครื่องมือในการบริหารจัดการ

จากการที่ Web 2.0 หมายถึงแนวโน้มในการใช้เทคโนโลยี World Wide Web ในการสร้างความคิดสร้างสรรค์ การแบ่งปันข้อมูล การร่วมไม่ร่วมมือกันระหว่างผู้ใช้ ซึ่ง Web 2.0 จะช่วยในการสืบค้นข้อมูลบน Web ดังนั้น SCM 2.0 จึงใช้แนวคิดนี้กับห่วงโซ่อุปทาน ซึ่งเป็นหนทางไปสู่การผสมผสานของกระบวนการ วิธีการ เครื่องมือ และช่องทางการส่งมอบ เพื่อให้ทันต่อการเปลี่ยนแปลงของห่วงโซ่อุปทานที่เพิ่มขึ้นตามการแข่งขันที่สูงขึ้น ราคาสินค้าที่เพิ่มขึ้น ราคาน้ำมันที่ทะยานสูงขึ้น วงจรชีวิตของสินค้าที่สั้นลง ฯลฯ

SCM 2.0 เป็นจุดเริ่มต้นของการผสานระหว่างซอฟแวร์และการบริการเพื่อสนับสนุนให้เกิดการค้าที่มีประสิทธิภาพระหว่างคู่ค้าหรือพันธมิตรที่อยู่ในห่วงโซ่อุปทาน ซึ่งจะช่วยให้กระบวนการในการรับจ้างช่วงสามารถทำได้อย่างมีประสิทธิภาพยิ่งขึ้น

ความปลอดภัยของห่วงโซ่อุปทาน (Supply Chain Security)

ความปลอดภัยของห่วงโซ่อุปทาน (Supply Chain Security) หมายถึง ความพยายามในด้านความปลอดภัยให้แก่ห่วงโซ่อุปทาน ซึ่งได้แก่ ระบบการขนส่งสินค้าและโลจิสติกส์ โดยรวมกิจกรรมด้านการจัดการห่วงโซ่อุปทานและข้อกำหนดด้านความปลอดภัยที่อาจจะเกิดจากภยันตรายต่างๆ เช่น การก่อการร้าย, การปล้นสะดมในน่านน้ำทะเล และการโจรกรรม

ความปลอดภัยของห่วงโซ่อุปทานโดยทั่วๆ ไป มีกิจกรรมที่ประกอบด้วย

- การรับรองผู้เกี่ยวข้องในห่วงโซ่อุปทาน
- การกลั่นกรองและการรับรองรายการสินค้าที่จะขนส่ง
- การแจ้งรายการสินค้าล่วงหน้าไปยังประเทศปลายทาง
- การสร้างความมั่นใจด้านความปลอดภัยของสินค้าในระหว่างการเปลี่ยนถ่ายสินค้าโดยใช้กุญแจและการปิดผนึก
- การตรวจสอบสินค้าเมื่อรับเข้า

ในปัจจุบันองค์การระหว่างประเทศว่าด้วยการมาตรฐาน (ISO) ได้กำหนดและประกาศใช้มาตรฐานเกี่ยวกับความปลอดภัยของห่วงโซ่อุปทาน (Supply Chain Security) ซึ่งก็คือ **ชุดมาตรฐาน ISO 28000** Security Management Systems for the Supply Chain

มาตรฐานที่ได้รับการอนุมัติและนำไปใช้อยู่ในขณะนี้ มีดังนี้

- ISO 28000:2007 Specification for security management systems for the supply chain (ซึ่งนำมาใช้แทนที่มาตรฐาน ISO/PAS 28000:2005 ภายหลังจากผ่านการนำไปใช้ในรูปของ publicly available specification และการทบทวนด้านเทคนิค) ประกาศใช้เมื่อวันที่ 15 กันยายน 2550 โดยการร่างมาตรฐานของคณะกรรมการวิชาการ ISO/TC 8 ships and marine technology และคณะกรรมการวิชาการอื่นๆ ที่รับผิดชอบด้านห่วงโซ่อุปทาน

  ซึ่งมาตรฐานฉบับนี้ได้รวมเอาแนวคิด Process-based ของมาตรฐานระบบบริหารงานคุณภาพ ISO 9001:2000 และมาตรฐานระบบการจัดการสิ่งแวดล้อม ISO 14001:2004 รวมทั้งวงจร PDCA ข้อกำหนดสำหรับการปรับปรุงอย่างต่อเนื่อง และประเด็นในการจัดการความเสี่ยงของ ISO 14001:2004 ซึ่งทำให้มาตรฐานนี้สามารถเข้ากันได้กับมาตรฐานทั้งสองดังกล่าว ดังนั้น องค์กรที่ได้มีการนำมาตรฐานทั้งสองไปปฏิบัติใช้แล้วก็จะสามารถใช้เป็นพื้นฐานในการพัฒนาระบบการจัดการด้านความปลอดภัยให้สอดคล้องกับ ISO 28000:2007

  ISO 28001:2007 Security management systems for the supply chain - Best practices for implementing supply chain security - Assessment and plans - Requirements and guidance

- ISO 28003:2007 Security management systems for the supply chain -Requirements for bodies providing audit and certification of supply chain security management systems

- ISO 28004:2007, Security management systems for the supply chain - Guidelines for the implementation of ISO 28000

ซึ่งชุดมาตรฐาน ISO 28000 สามารถเข้ากันได้กับโครงการด้านความปลอดภัยอื่นๆ รวมถึง

- The World Customs Organization (WCO) Supply Chain Security and ;Facilitation of Global Trade initiative

- The EU Security Program - Authorized Economic Operator (AEO)

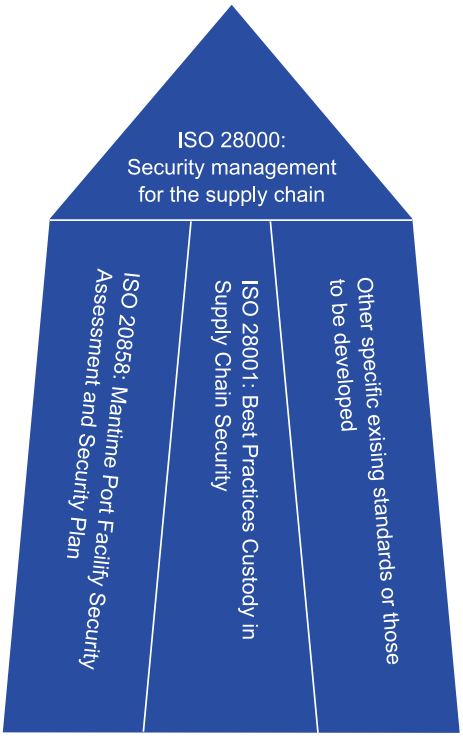
- The US Customs and Border Protection initiative - Customs Trade Partnership Against Terrorism (C-TPAT)

มาตรฐานระบบการจัดการความปลอดภัยสำหรับห่วงโซ่อุปทาน: ISO 28000:2007 - Specification for security management systems for the supply chain

บทนำ

มาตรฐานสากลฉบับนี้ ได้ถูกพัฒนาขึ้นตามอุปสงค์ของภาคอุตสาหกรรมสำหรับมาตรฐานด้านการจัดการความปลอดภัย **วัตถุประสงค์ของมาตรฐานนี้** เพื่อปรับปรุงความปลอดภัยของห่วงโซ่อุปทานให้ดียิ่งขึ้น มาตรฐานนี้เป็นมาตรฐานระบบการจัดการขั้นสูง ซึ่งสามารถทำให้องค์กรสร้างระบบการจัดการความปลอดภัยของห่วงโซ่อุปทานได้ทั่วทั้งองค์กร

องค์กรจะต้องประเมินสภาวะแวดล้อมด้านความปลอดภัยที่ซึ่งองค์กรได้ดำเนินการอยู่ และพิจารณาว่ามีมาตรการด้านความปลอดภัยเพียงพอหรือไม่ และมีข้อกำหนดกฎหมายอื่นที่องค์กรได้ดำเนินการอย่างสอดคล้องหรือไม่ ถ้ามีการชี้บ่งความจำเป็นด้านความปลอดภัย องค์กรจะต้องจัดทำกลไกและกระบวนการ เพื่อให้สามารถบรรลุความจำเป็นเหล่านั้น เนื่องจากโดยธรรมชาติแล้วห่วงโซ่อุปทานจะมีการเปลี่ยนแปลงอยู่เสมอที่สำคัญ องค์กรที่บริหารจัดการหลายห่วงโซ่อุปทานต้องให้ความสำคัญกับผู้ให้บริการ (Service provider) ขององค์กร เพื่อให้หน่วยงานเหล่านั้น มีการดำเนินการสอดคล้องตามมาตรฐานความปลอดภัยสำหรับห่วงโซ่อุปทาน ซึ่งเป็นเงื่อนไขที่รวมอยู่ในห่วงโซ่อุปทาน เพื่อให้สามารถบริหารจัดการได้ง่ายขึ้น ดังตัวอย่างในภาพที่ 1



ภาพที่ 1 - ความสัมพันธ์ระหว่าง ISO 28000 กับมาตรฐานอื่นที่เกี่ยวข้อง

โครงสร้างของมาตรฐาน

- **ข้อ 1 : ขอบข่าย** (Scope) – มาตรฐาน ISO 28000:2007 กำหนดข้อกำหนดสำหรับระบบการจัดการความปลอดภัย รวมทั้งประเด็นที่วิกฤติต่อการประกันความปลอดภัยของห่วงโซ่อุปทาน การจัดการความปลอดภัยถูกเชื่อมโยงกับประเด็นด้านการจัดการธุรกิจอื่นๆ นอกจากนี้ ประเด็นยังหมายรวมถึงทุกกิจกรรมที่ควบคุม หรือมีอิทธิพลจากองค์กรที่มีผลกระทบกับความปลอดภัยของห่วงโซ่อุปทาน และประเด็นอื่นที่มีผลกระทบไม่ว่าที่ใด หรือเมื่อใดกับการจัดการความปลอดภัยก็ต้องนำมาพิจารณาด้วย รวมทั้งการขนส่งสินค้าผ่านห่วงโซ่อุปทาน

  มาตรฐานสากลฉบับนี้สามารถใช้ได้กับองค์กรทุกขนาด ตั้งแต่ขนาดเล็กถึงองค์กรข้ามชาติ ธุรกิจประเภทการผลิต บริการ การจัดเก็บสินค้า หรือการขนส่งในทุกขั้นตอนของการผลิตหรือห่วงโซ่อุปทาน
- **ข้อ 2 : เอกสารอ้างอิง** (Normative reference)
- **ข้อ 3 : บทนิยามและคำศัพท์** (Term and definitions)

สำหรับข้อกำหนดมาตรฐาน ISO 28000:2007 ที่องค์กรต้องนำไปปฏิบัติ คือ ข้อกำหนดข้อ 4 โดยมีสาระสำคัญดังนี้

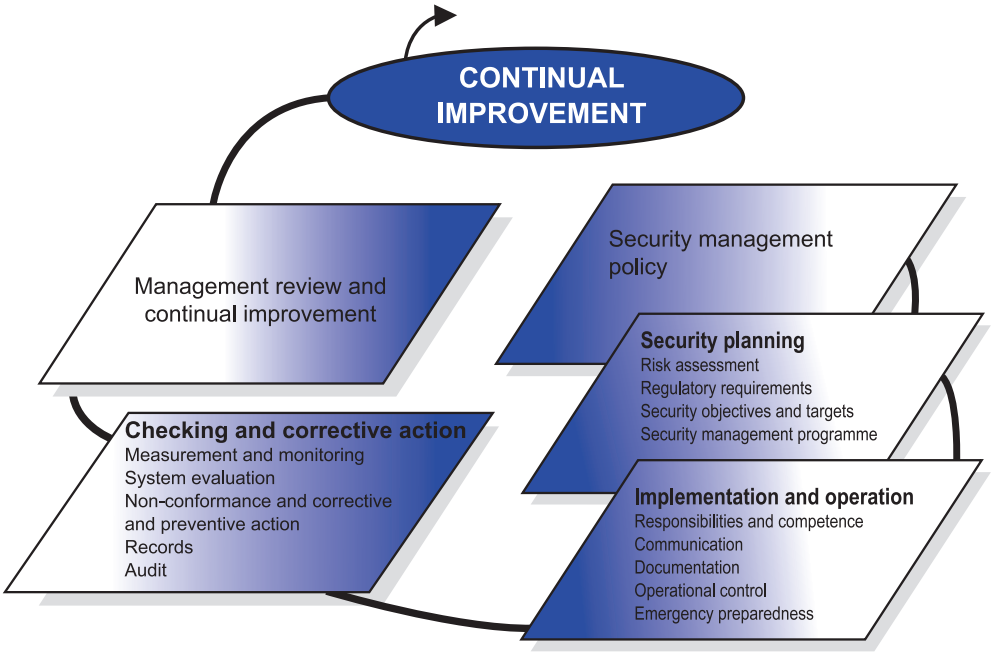
- **ข้อ 4 : องค์ประกอบระบบการจัดการความปลอดภัย** (security management system elements)

ข้อกำหนดทั่วไป (4.1)

- องค์กรจะต้องกำหนดขอบข่ายของระบบการจัดการความปลอดภัย
- หากมีการจ้างเหมาช่วง (outsource) ในกระบวนการใดจะต้องมีการควบคุมกระบวนการเหล่านั้น และต้องระบุการควบคุมและความรับผิดชอบที่จำเป็นในระบบการจัดการความปลอดภัยด้วย

นโยบายการจัดการความปลอดภัย (4.2)

- ผู้บริหารระดับสูงจะต้องกำหนดนโยบายการจัดการความปลอดภัย โดยนโยบายจะต้อง
  - สอดรับกับนโยบายอื่นๆ ขององค์กร
  - ให้กรอบในการสร้างวัตถุประสงค์ เป้าหมาย และโครงการ
  - สอดรับกับกรอบการจัดการความเสี่ยงและการคุกคามด้านความปลอดภัยขององค์กร
  - เหมาะกับภัยคุกคามที่เกิดขึ้นกับองค์กร ธรรมชาติและขนาดของการปฏิบัติงาน
  - กล่าวถึงวัตถุประสงค์ด้านการจัดการความปลอดภัยอย่างชัดเจน
  - แสดงความมุ่งมั่นในการปรับปรุงอย่างต่อเนื่อง
  - แสดงความมุ่งมั่นในการปฏิบัติตามข้อกำหนดกฎหมายอื่นๆ ที่เกี่ยวข้อง
  - ผ่านความเห็นชอบและรับรองจากผู้บริหารระดับสูง
  - จัดทำเป็นเอกสารนำไปปฏิบัติใช้ และรักษาไว้
  - มีการสื่อสารไปยังพนักงานและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง
  - มีพร้อมสำหรับผู้มีส่วนได้ส่วนเสียตามความเหมาะสม
  - สามารถทบทวนได้ หากมีกรณีที่มีผลกระทบต่อความต่อเนื่องหรือมีความเกี่ยวข้องกับระบบการจัดการความปลอดภัย



ภาพที่ 2 - องค์ประกอบของมาตรฐาน

การประเมินความเสี่ยงด้านความปลอดภัยและการวางแผน (4.3)

การประเมินความเสี่ยง (4.3.1)

- องค์กรจะต้องจัดทำคู่มือการปฏิบัติงานในการชี้บ่งและการประเมินภัยคุกคามความปลอดภัย ภัยคุกคามที่เกี่ยวข้องกับการจัดการความปลอดภัยและความเสี่ยง รวมทั้งชี้บ่งและนำไปปฏิบัติใช้ซึ่งมาตรการการควบคุม โดยการควบคุมนั้นต้องเหมาะสมกับธรรมชาติและขนาดของการปฏิบัติงาน การประเมินก็จะต้องพิจารณาความเป็นไปได้ของเหตุการณ์และผลลัพธ์ที่จะตามมาด้วย
- องค์กรจะต้องมั่นใจว่าจะมีการพิจารณาผลของการประเมินข้างต้น และผลกระทบจากการควบคุมต่างๆ ตามความเหมาะสม
- องค์กรจะต้องจัดทำเป็นเอกสาร และสารเทศต่างๆ จะต้องทันสมัยอยู่เสมอ
- วิธีการสำหรับการชี้บ่งและการประเมินภัยคุกคามและความเสี่ยงจะต้อง
  - o ถูกชี้บ่งให้สอดคล้องกับขอบข่าย ธรรมชาติ และระยะเวลา
  - o มีข้อมูลสารสนเทศที่เกี่ยวข้องกับภัยคุกคามและความเสี่ยง
  - o มีการจัดหมวดหมู่ของภัยคุกคามและความเสี่ยง รวมทั้งการชี้บ่งว่าภัยคุกคามและความเสี่ยงนั้นสามารถหลีกเลี่ยงได้ กำจัดได้ หรือ ควบคุมได้หรือไม่
  - o มีขั้นตอนการเฝ้าระวัง เพื่อให้เกิดความมั่นใจในประสิทธิผลและความเหมาะสมของช่วงเวลาในการนำไปปฏิบัติ

กฎหมายและกฎระเบียบต่าง ๆ ที่เกี่ยวข้อง (4.3.2)

- องค์กรจะต้องจัดทำคู่มือการปฏิบัติงานในการชี้บ่งและเข้าถึงกฎหมายและกฎระเบียบต่างๆ ที่เกี่ยวข้อง และพิจารณาว่ากฎหมายและกฎระเบียบต่างๆ ที่เกี่ยวข้องเหล่านั้นนำมาใช้กับภัยคุกคามและความเสี่ยงนั้นอย่างไร และข้อมูลสารสนเทศจะต้องทันสมัย และมีการสื่อสารไปยังพนักงานและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง

วัตถุประสงค์ของการจัดการความปลอดภัย (4.3.3)

- องค์กรจะต้องกำหนดวัตถุประสงค์ในทุกหน่วยงานและระดับที่เกี่ยวข้องขององค์กร โดยต้องมีความเชื่อมโยงกับนโยบาย โดยในการกำหนดวัตถุประสงค์จะต้องนำประเด็นต่างๆ เข้ามาพิจารณาด้วย เช่น กฎหมายและกฎระเบียบต่างๆ ภัยคุกคามและความเสี่ยงที่เกี่ยวข้อง มุมมองของผู้มีส่วนได้ส่วนเสีย เป็นต้น

เป้าหมายของการจัดการความปลอดภัย (4.3.4)

- องค์กรจะต้องกำหนดเป้าหมายที่เหมาะสมกับความต้องการขององค์กร โดยต้องมีความเชื่อมโยงกับวัตถุประสงค์ โดยเป้าหมายจะต้อง

- เหมาะสมในแต่ละระดับ
- เฉพาะเจาะจง วัดได้ ทำให้สำเร็จได้ และมีกรอบระยะเวลา
- สื่อสารไปยังพนักงานและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง
- ทบทวนตามช่วงระยะเวลาที่เหมาะสม

โครงการการจัดการความปลอดภัย (4.3.5)

- องค์กรจะต้องกำหนดโครงการเพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่ตั้งไว้ โดยโครงการจะต้องคุ้มค่าและต้องมีการจัดลำดับความสำคัญก่อนหลัง รวมทั้งต้องคำนึงถึงประสิทธิผลและประสิทธิภาพด้านราคาในการนำไปปฏิบัติด้วย นอกจากนั้น ต้องมีการจัดทำเป็นเอกสารเกี่ยวกับอำนาจหน้าที่และความรับผิดชอบ วิธีการ และระยะเวลาเพื่อให้บรรลุตามวัตถุประสงค์และเป้าหมายที่ตั้งไว้ รวมทั้งต้องได้รับการทบทวนตามช่วงระยะเวลาที่เหมาะสม

การนำไปปฏิบัติใช้และการดำเนินการ (4.4)

โครงสร้าง อำนาจหน้าที่ และความรับผิดชอบสำหรับการจัดการความปลอดภัย (4.4.1)

- องค์กรจะต้องกำหนดโครงสร้างและบทบาทขององค์กร อำนาจหน้าที่และความรับผิดชอบ เพื่อให้สามารถบรรลุนโยบาย วัตถุประสงค์ เป้าหมาย และโครงการที่ตั้งไว้ รวมทั้งสื่อสารไปยังผู้เกี่ยวข้อง
- ผู้บริหารระดับสูงจะต้องแสดงให้เห็นถึงความมุ่งมั่นในการพัฒนา การนำไปปฏิบัติใช้ และการปรับปรุงประสิทธิผลอย่างต่อเนื่องของระบบ โดยการ
  - มอบหมายหนึ่งในผู้บริหารระดับสูงเพื่อรับผิดชอบในการจัดทำระบบทั้งหมด
  - มอบหมายหนึ่งหรือมากกว่าหนึ่งในผู้บริหารเพื่อให้มั่นใจว่ามีการนำวัตถุประสงค์และเป้าหมายที่ตั้งไว้ไปปฏิบัติใช้
  - จัดหาทรัพยากรให้พอเพียง
  - พิจารณาผลกระทบของนโยบาย วัตถุประสงค์ เป้าหมาย และโครงการที่ตั้งไว้ ที่อาจจะมีต่อประเด็นอื่นๆ ในองค์กร
  - ทำให้มั่นใจว่าโครงการความปลอดภัยใดๆ ที่เกิดจากส่วนอื่นๆ ขององค์กร เสริมกับระบบการจัดการความปลอดภัย
  - สื่อสารถึงความสำคัญในการดำเนินการให้เป็นไปตามข้อกำหนดการจัดการความปลอดภัยเพื่อให้สอดคล้องกับนโยบายที่ตั้งไว้
  - ทำให้มั่นใจว่าภัยคุกคามหรือความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยได้ถูกรวมไว้ในการประเมินภัยคุกคามและความเสี่ยง
  - ทำให้มั่นใจถึงความเป็นไปได้ของวัตถุประสงค์ เป้าหมาย และโครงการที่ตั้งไว้

ความรู้ความสามารถ การฝึกอบรม และจิตสำนึก (4.4.2)

- องค์กรจะต้องมั่นใจว่าผู้ที่มีหน้าที่ในการดำเนินการจัดทำระบบอุปกรณ์และกระบวนการมีคุณสมบัติที่เหมาะสม ในเรื่องการศึกษา การฝึกอบรม และประสบการณ์ นอกจากนั้น องค์กรจะต้องจัดทำคู่มือการปฏิบัติงานเพื่อให้ผู้เกี่ยวข้องมีจิตสำนึกในเรื่อง
  - ความสำคัญในการปฏิบัติให้สอดคล้องกับนโยบาย ขั้นตอนการปฏิบัติงาน และข้อกำหนดของระบบการจัดการ ความปลอดภัย
  - บทบาทและหน้าที่ในการปฏิบัติให้สอดคล้องตามที่กำหนดไว้
  - ความเป็นไปได้ของผลที่จะตามมาต่อความปลอดภัยขององค์กรหากไม่ปฏิบัติตามขั้นตอนการปฏิบัติงาน
- จะต้องมีการจัดเก็บบันทึกความรู้ความสามารถและการฝึกอบรม

การสื่อสาร (4.4.3)

- องค์กรจะต้องกำหนดขั้นตอนการปฏิบัติงานเพื่อให้มั่นใจว่าสารสนเทศที่เกี่ยวข้องกับการจัดการความปลอดภัยถูกสื่อสารไปยังพนักงาน ผู้รับจ้างช่วงและผู้มีส่วนได้ส่วนเสีย รวมทั้งจะต้องมีการพิจารณาสารสนเทศก่อนการเผยแพร่ เนื่องจากโดยธรรมชาติแล้วจะมีความอ่อนไหวสูง

การจัดทำเป็นเอกสาร (4.4.4)

- องค์กรจะต้องจัดทำเอกสารระบบการจัดการความปลอดภัย ซึ่งรวมถึง (อาจจะมากกว่านี้ก็ได้)
  - นโยบาย วัตถุประสงค์ และเป้าหมาย
  - ขอบข่ายของระบบการจัดการความปลอดภัย
  - องค์ประกอบสำคัญและความเชื่อมโยงของระบบ และการอ้างอิงกับเอกสารที่เกี่ยวข้อง
  - เอกสาร บันทึก ที่กำหนดไว้ในมาตรฐาน
  - เอกสาร บันทึก ที่องค์กรพิจารณาแล้วว่าจำเป็นต่อประสิทธิผลของระบบ
- องค์กรจะต้องพิจารณาความอ่อนไหวของสารสนเทศเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

การควบคุมเอกสารและข้อมูล (4.4.5)

- องค์กรจะต้องจัดทำขั้นตอนการปฏิบัติงานในการควบคุมเอกสาร ข้อมูลและสารสนเทศ ตามที่กำหนดในข้อ 4 ของมาตรฐานฉบับนี้ เพื่อให้มั่นใจว่า
  - เอกสาร ข้อมูลและสารสนเทศถูกจัดเก็บและเข้าถึงโดยผู้ที่มีอำนาจ
  - เอกสาร ข้อมูลและสารสนเทศ มีการทบทวนในช่วงเวลาที่เหมาะสมและได้รับการอนุมัติโดยผู้ที่มีอำนาจ
  - เอกสาร ข้อมูลและสารสนเทศ version ปัจจุบันจะต้องมีไว้ ณ จุดปฏิบัติงานที่จำเป็น
  - เอกสาร ข้อมูลและสารสนเทศที่ล้าสมัย จะถูกนำออกนอกจุดปฏิบัติงาน เพื่อป้องการนำไปใช้โดยไม่ได้ตั้งใจ
  - มีการชี้บ่งเอกสาร ข้อมูลและสารสนเทศที่จัดเก็บไว้เพื่อวัตถุประสงค์ทางกฎหมายหรือความรู้
  - เอกสาร ข้อมูลและสารสนเทศมีความปลอดภัย และจะต้องสำรองข้อมูล และสามารถกู้ข้อมูลได้กรณีที่จัดเก็บในรูปแบบอิเล็กทรอนิกส์

การควบคุมการปฏิบัติการ (4.4.6)

- องค์กรจะต้องชี้บ่งการปฏิบัติการและกิจกรรมที่จำเป็นต่อความสำเร็จของ

STANDARD MOVEMENT

- นโยบายการจัดการความปลอดภัย
- การควบคุมกิจกรรมและการลดความรุนแรงของภัยคุกคามที่ชี้บ่งว่ามีความเสี่ยงที่มีนัยสำคัญ
- ความสอดคล้องกับกฎหมายและกฎระเบียบที่เกี่ยวข้อง
- วัตถุประสงค์การจัดการความปลอดภัย
- โครงการการจัดการความปลอดภัย
- ระดับความปลอดภัยของห่วงโซ่อุปทานที่จำเป็น

- องค์กรจะต้องมั่นใจว่าการปฏิบัติการและกิจกรรมจะประสบความสำเร็จ โดยการจัดทำเอกสารขั้นตอนการปฏิบัติงานประเมินภัยคุกคาม และควบคุมห่วงโซอุปทานตั้งแต่ต้นน้ำเพื่อลดผลกระทบที่ปลายน้ำ และกำหนดข้อกำหนดของสินค้าหรือบริการที่กระทบต่อความปลอดภัย

การเตรียมความพร้อมสำหรับเหตุฉุกเฉิน การตอบสนอง และการฟื้นฟู (4.4.7)

- องค์กรจะต้องมีแผนและขั้นตอนการปฏิบัติงานเพื่อชี้บ่งการตอบสนองต่ออุบัติการณ์เพื่อป้องกันและลดความรุนแรงของผลที่จะตามมา รวมทั้งวิธีการบำรุง รักษาเครื่องมือต่างๆ รวมทั้งมีการทบทวนประสิทธิผลในระยะเวลาที่เหมาะสม

การตรวจสอบและการปฏิบัติการแก้ไข (4.5)

การวัดและการเฝ้าระวังสมรรถนะ (4.5.1)

- องค์กรจะต้องมีขั้นตอนการปฏิบัติงานเพื่อวัดและเฝ้าระวังสมรรถนะของระบบการจัดการและสมรรถนะด้านความปลอดภัย และต้องพิจารณาภัยคุกคามและความเสี่ยง รวมทั้งผลกระทบที่ตามมาและความถี่ในการวัดและการเฝ้าระวัง

การประเมินระบบ (4.5.2)

- องค์กรจะต้องมีการประเมินแผน ขั้นตอนการปฏิบัติงาน และขีดความสามารถของการทบทวน การทดสอบ บทเรียนที่ได้รับ ฯลฯ รวมทั้งต้องมีการประเมินความสอดคล้องกับกฎหมายและกฎระเบียบต่างๆ แนวทางปฏิบัติที่ดี นโยบายและวัตถุประสงค์เป็นระยะ ๆ
- องค์กรจะต้องจัดเก็บบันทึกของการประเมินข้างต้น

ความผิดพลาด อุบัติการณ์, ความไม่สอดคล้อง และการปฏิบัติการแก้ไขและป้องกัน (4.5.3)

- องค์กรจะต้องจัดทำขั้นตอนการปฏิบัติงานในการกำหนดความรับผิดชอบและอำนาจหน้าที่ในการ
  - ประเมินและจัดทำการปฏิบัติการป้องกันเพื่อชี้บ่งความผิดพลาดที่อาจจะเกิดขึ้น
  - การสอบสวนหาสาเหตุของสิ่งที่เกิดขึ้น
  - ดำเนินการเพื่อลดความรุนแรงของผลที่ตามมา
  - ดำเนินการปฏิบัติการป้องกัน
  - ยืนยันประสิทธิผลของการปฏิบัติการป้องกัน
- การปฏิบัติการแก้ไขและป้องกันจะต้องเหมาะสมกับขนาดของปัญหาและพอเพียงสำหรับภัยคุกคามและความเสี่ยงที่เกี่ยวข้องกับการจัดการความปลอดภัย

การควบคุมบันทึก (4.5.4)

- องค์กรจะต้องจัดทำและเก็บรักษาบันทึกเพื่อแสดงถึงความสอดคล้องกับข้อกำหนด
- องค์กรจะต้องจัดทำขั้นตอนการปฏิบัติงานในการจัดการบันทึก
- สามารถจัดเก็บในรูปอิเล็กทรอนิกส์และดิจิตอล แต่ต้องมีการสำรองข้อมูลอย่างปลอดภัยและเข้าถึงได้เฉพาะผู้มีอำนาจ

การตรวจประเมิน (4.5.5)

- องค์กรจะต้องจัดทำกำหนดการตรวจประเมินและดำเนินการตรวจประเมินตามช่วงเวลาที่วางแผนไว้
- กำหนดการตรวจประเมินจะต้องขึ้นอยู่กับผลการประเมินภัยคุกคามและความเสี่ยง ถ้าเป็นไปได้ การตรวจประเมินจะต้องกระทำโดยผู้ที่มีอิสระจากหน้าที่ความรับผิดชอบโดยตรงกับกิจกรรมที่ถูกตรวจประเมิน

การทบทวนของฝ่ายบริหารและการปรับปรุงอย่างต่อเนื่อง (4.6)

- ผู้บริหารระดับสูงจะต้องทบทวนตามช่วงเวลาที่วางแผนไว้เพื่อให้มั่นใจถึงความเหมาะสม ความพอเพียง และประสิทธิผลของระบบการจัดการความปลอดภัย การประเมินโอกาสในการปรับปรุงและความจำเป็นในการเปลี่ยนแปลงระบบการจัดการความปลอดภัย รวมทั้งนโยบาย วัตถุประสงค์ ภัยคุกคามและความเสี่ยง
- องค์กรจะต้องจัดเก็บบันทึกของการทบทวน

อ้างอิง

- ISO 28000: 2007 – Specifications for security management systems for the Supply Chain
- “Securing the global supply chain” – ISO Focus 2007
- “ISO/PAS 28000 applies management system approach to security of global supply chains” – ISO Management Systems January – February 2006
- http://en.wikipedia.org/wiki/Supply_Chain
- http://en.wikipedia.org/wiki/Supply_Chain_Security
- http://en.wikipedia.org/wiki/Supply_Chain_Manageme

...หลากหลายมาตรฐาน ISO ด้านระบบเทคโนโลยีสารสนเทศ...

ปัจจุบัน **เทคโนโลยีสารสนเทศ** (Information Technology: IT) มีบทบาทสำคัญในธุรกิจขององค์กรเพิ่มมากขึ้น ทั้งองค์กรขนาดเล็ก ขนาดกลางและขนาดย่อม (SMEs) ไปจนถึงองค์กรขนาดใหญ่ ครอบคลุมทุกประเภทอุตสาหกรรมและการบริการ ซึ่งต่างก็ต้องอาศัยระบบเทคโนโลยีสารสนเทศเข้ามาเป็นส่วนหนึ่งของกระบวนการบริหารจัดการต่างๆ ขององค์กร อาทิ การบริหารจัดการกลยุทธ์ การประเมินผลการวัดประสิทธิภาพและประสิทธิผลการดำเนินการ เป็นต้น

นิยามของ "ระบบสารสนเทศเพื่อการบริหารจัดการ" (Management Information System: MIS)

ระบบสารสนเทศเพื่อการบริหารจัดการ หมายถึง ระบบที่รวบรวมและจัดเก็บข้อมูลจากแหล่งข้อมูลต่างๆ ทั้งภายในและภายนอกองค์กรอย่างมีหลักเกณฑ์ โดยมีวัตถุประสงค์เพื่อการประมวลผลและการจัดรูปแบบให้ได้ข้อมูลสารสนเทศที่ช่วยสนับสนุนการทำงาน และการตัดสินใจในด้านต่างๆ ของผู้บริหาร ทั้งนี้ เพื่อให้การดำเนินงานขององค์กรเป็นไปอย่างมีประสิทธิภาพ

ระบบสารสนเทศเพื่อการบริหารจัดการ ประกอบด้วยหน้าที่หลัก 2 ประการ ได้แก่

- สามารถเก็บรวบรวมข้อมูลจากแหล่งต่างๆ ทั้งจากภายในและภายนอกองค์กรมาไว้ด้วยกันอย่างเป็นระบบ
- สามารถทำการประมวลผลข้อมูลอย่างมีประสิทธิภาพ เพื่อให้ได้สารสนเทศที่ช่วยสนับสนุนการปฏิบัติงานและการบริหารงานของผู้บริหาร

ระบบสารสนเทศเพื่อการบริหารจัดการไม่จำเป็นที่จะต้องสร้างขึ้นจากระบบคอมพิวเตอร์ โดยอาจสร้างขึ้นมาจากอุปกรณ์อะไรก็ได้ แต่ต้องสามารถปฏิบัติหน้าที่หลักทั้ง 2 ประการได้อย่างครบถ้วนและสมบูรณ์ ดังนั้น ถ้าระบบใดประกอบด้วยหน้าที่หลัก 2 ประการดังกล่าว ตลอดจนสามารถปฏิบัติงานในหน้าที่หลักได้อย่างครบถ้วนและสมบูรณ์ ระบบนั้นก็สามารถถูกจัดเป็นระบบสารสนเทศเพื่อการบริหารจัดการ (MIS) ได้

แต่เนื่องจากปัจจุบันคอมพิวเตอร์เป็นอุปกรณ์ที่มีประสิทธิภาพในการจัดการข้อมูล นักวิเคราะห์และออกแบบระบบ (System Analyst and Designer) จึงออกแบบระบบสารสนเทศให้มีคอมพิวเตอร์เป็นอุปกรณ์หลักในการบริหารจัดการสารสนเทศ

"จุดมุ่งหมายของการจัดทำระบบการบริหารจัดการเทคโนโลยีสารสนเทศ" เพื่อ:

- ช่วยในการบริหารจัดการด้านระบบบริหารงานคุณภาพขององค์กร เช่น การปรับปรุงกระบวนการธุรกรรมต่างๆ ขององค์กรการสร้างกระบวนการตรวจสอบความถูกต้อง เป็นต้น
- ช่วยเสริมสร้างความมั่นคง - ความปลอดภัยในแง่ของ
  - การขัดจังหวะ/การหยุดชะงักการให้บริการ (Service disruption)
  - การลักลอบใช้บริการ (Theft of service)
  - การถูกโจมตี (Attack of the network)
  - การละเมิดสิทธิส่วนบุคคล (Privacy violation)
  - และอื่นๆ

  ให้กับระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อสร้างเสถียรภาพการดำเนินการต่างๆ
- ช่วยเสริมสร้างความมั่นใจให้แก่ผู้มีส่วนได้ส่วนเสียขององค์กร
- ช่วยเพิ่มศักยภาพในการแข่งขันด้านสินค้าและการบริการ

ซึ่งความสลับซับซ้อนและความยุ่งยากบางประการในเรื่องของการบริหารจัดการระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพนั้น เป็นจุดเริ่มต้นของการมีมาตรฐาน (Standard) แนวทางปฏิบัติ (Guidance) และกรอบวิธีการปฏิบัติ (Framework) ด้านระบบการรักษาความปลอดภัยและความมั่นคงให้กับระบบเทคโนโลยีสารสนเทศขององค์กร

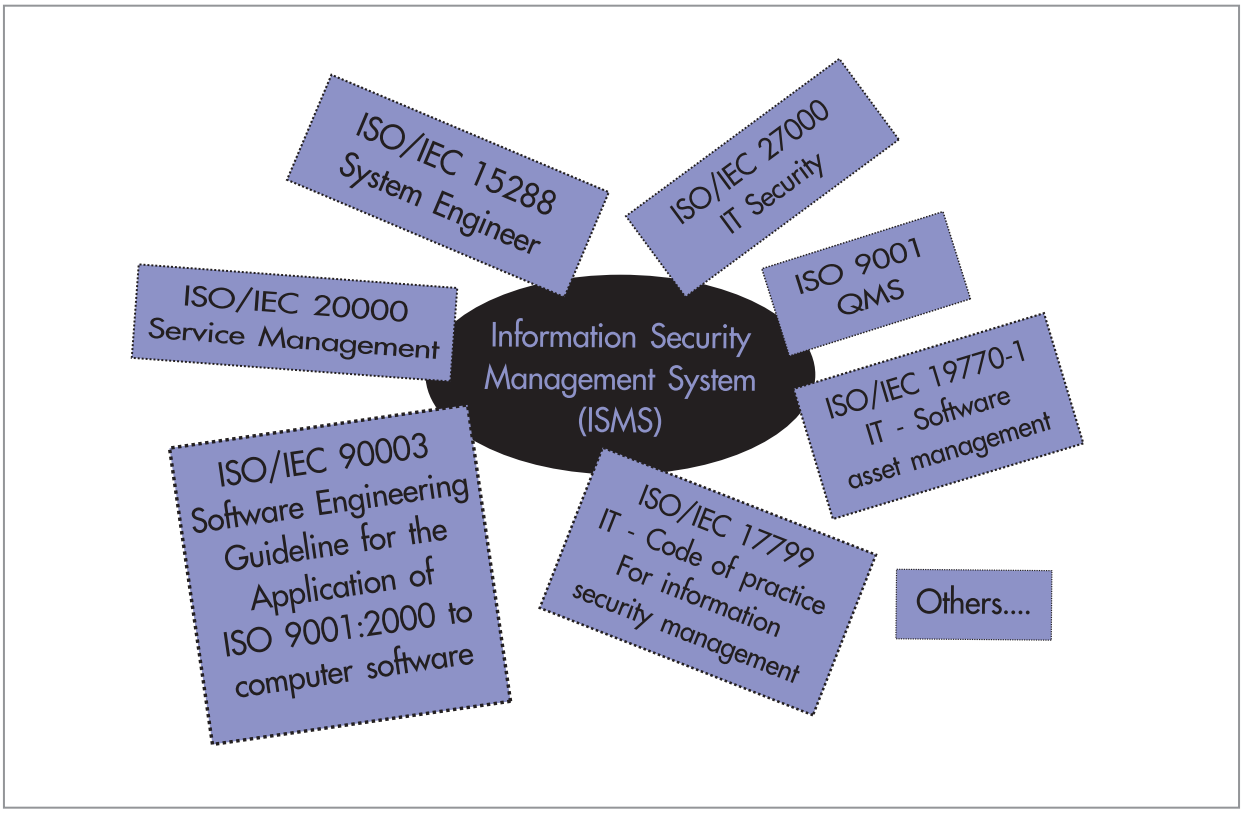
"การเลือกสรรให้เข้ากับลักษณะองค์กร"

องค์กรจะสามารถดำเนินการเป็นไปตามที่กล่าวมาแล้วข้างต้นได้หรือไม่นั้นขึ้นอยู่กับการเลือกใช้มาตรฐานที่เหมาะสมที่สามารถสนับสนุนวิสัยทัศน์และพันธกิจขององค์กร โดยองค์กรควรทำการศึกษาและพิจารณาคัดเลือกมาตรฐาน แนวทางปฏิบัติ และกรอบวิธีการปฏิบัติ ซึ่งถูกพัฒนาของหน่วยงานที่เป็นผู้ออกมาตรฐาน อาทิ องค์การระหว่างประเทศว่าด้วยการมาตรฐาน (International Organization for Standardization: ISO) ว่ามีความเหมาะสมและเข้ากันได้กับรูปแบบการดำเนินการขององค์กรหรือไม่ และควรพิจารณาปัจจัยอื่นในการคัดเลือกร่วมด้วย อาทิ

- วัตถุประสงค์ของมาตรฐาน (รวมถึงแนวทางปฏิบัติ และกรอบวิธีการปฏิบัติ) ที่ได้มีการกำหนดนิยามไว้
- จุดมุ่งหมายขององค์กรต่อการมีมาตรฐานสำหรับการดำเนินการเพื่อพิจารณาถึงประโยชน์และความคุ้มค่าที่เกี่ยวเนื่องกับการลงทุนด้านเทคโนโลยีสารสนเทศ

โดยองค์กรอาจต้องค่อยๆ นำมาตรฐาน (แนวทางปฏิบัติ และกรอบวิธีการปฏิบัติ) มาประยุกต์เข้ากับกระบวนการทำงานเดิมขององค์กรอย่างค่อยเป็นค่อยไป เพื่อให้เกิดการปรับตัวและสร้างการยอมรับให้แก่ผู้ที่เกี่ยวข้อง

“หลากหลายมาตรฐาน ISO ด้านระบบเทคโนโลยีสารสนเทศ”



ตัวอย่าง มาตรฐาน ISO ที่เกี่ยวข้องด้านระบบเทคโนโลยีสารสนเทศ

ISO/IEC 27001:2005 Information technology –– Security techniques –– Information security management systems –– Requirements

มาตรฐาน ISO/IEC 27001:2005 **ว่าด้วยเรื่องข้อกำหนดระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ** (Information Security Management Systems: ISMS) เป็นมาตรฐานสากลที่มุ่งเน้นการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร ได้รับการพัฒนามาจากมาตรฐาน BS 7799-2:2002 Information security management systems – Specification with guidance for use หรือที่รู้จักกันทั่วไปคือ BS 7799

โครงสร้างข้อกำหนด ISO/IEC 27001:2005

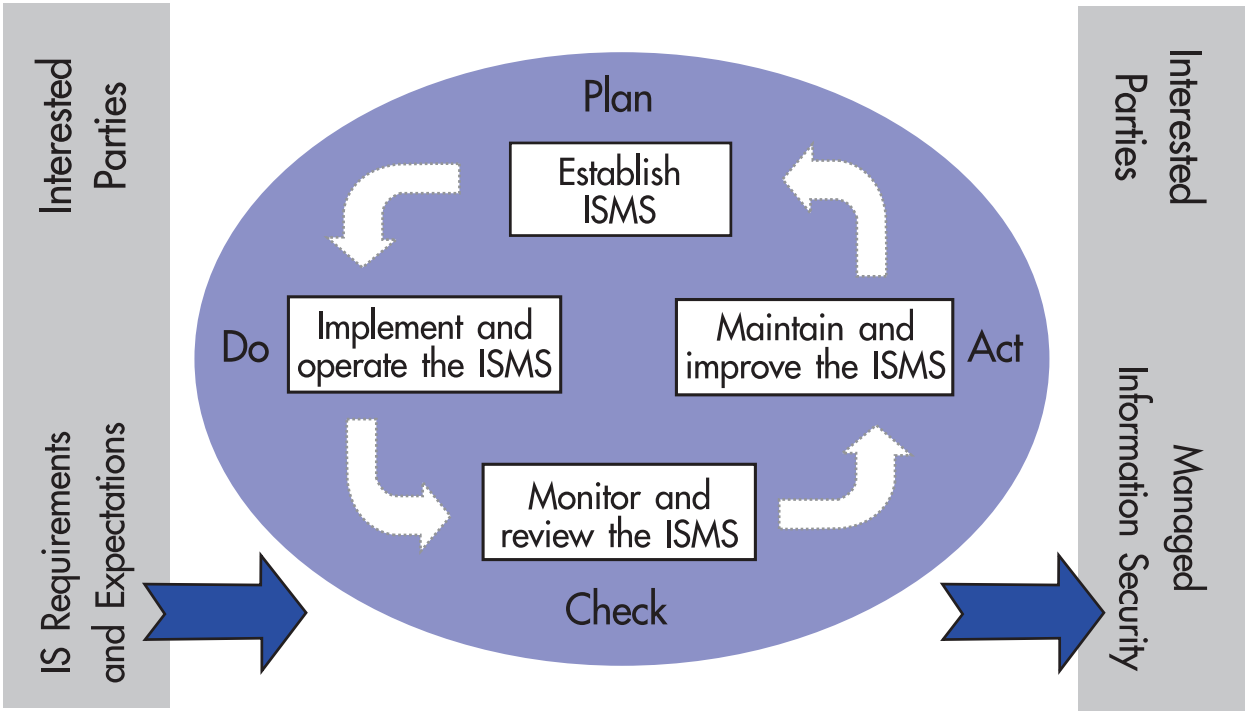
- ข้อ 0: บทนำ (Introduction)
- ข้อ 1: ขอบข่าย (Scope)
- ข้อ 2: มาตรฐานอ้างอิง (Normative references)
- ข้อ 3: บทนิยามและคำศัพท์ (Terms and definitions)
- ข้อ 4 ถึงข้อ 8: เป็นข้อกำหนดที่องค์กรต้องนำไปปฏิบัติประกอบด้วย
  - ข้อ 4: Information Security Management System (ISMS)
  - ข้อ 5: Management Responsibility
  - ข้อ 6: Internal ISMS Audits
  - ข้อ 7: Management Review of the ISMS
  - ข้อ 8: ISMS improvement

มาตรฐาน ISO/IEC 27001:2005 อาศัยหลักการพื้นฐานของ W. E. Deming นั่นก็คือ PDCA Model: Plan - Do - Check - Act เช่นเดียวกับมาตรฐานบริหารงานคุณภาพ ISO 9001 ในการบริหารจัดการระบบสารสนเทศให้เกิดความมั่นคงปลอดภัย ซึ่งองค์กรที่นำมาตรฐานนี้ไปปฏิบัติ (Implement) ต้องมีการดำเนินการตามแผนภาพ:

แผนภาพ: PDCA model applied to ISMS processes

“Plan” ( ) การกำหนดนโยบาย ISMS วัตถุประสงค์ กระบวนการปฏิบัติงาน และขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับการจัดการความเสี่ยงและการปรับปรุงด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศ

“Do” ( ) การนำไปปฏิบัติและการดำเนินการตามนโยบาย การควบคุม กระบวนการปฏิบัติงาน และขั้นตอนการปฏิบัติต่างๆ ที่องค์กรได้วางแผนไว้



"Check" () การตรวจสอบและการวัดผลการดำเนินการเทียบกับนโยบาย ISMS วัตถุประสงค์ และการดำเนินการต่างๆ ตลอดจนรายงานการประชุมทบทวนโดยฝ่ายบริหาร

"Act" () การปฏิบัติการแก้ไขและป้องกัน (Corrective and preventive actions) โดยอ้างอิงผลจากการตรวจติดตามภายใน (Internal audit) และการประชุมทบทวนโดยฝ่ายบริหาร (Management review) และข้อมูลอื่นๆ เพื่อการปรับปรุงระบบ ISMS อย่างต่อเนื่อง

สำหรับมาตรฐาน ISO/IEC 27000 Series ประกอบด้วยมาตรฐานสำคัญที่เกี่ยวข้อง ได้แก่

- ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for Information security management
- ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management
- ISO/IEC 27006:2007 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems

ปัจจุบัน ประเทศไทยมีองค์กรจำนวน 7 แห่ง (จำนวน 9 ใบรับรอง) ที่ได้รับการรับรองมาตรฐาน ISO/IEC 27001:2005 และสำหรับองค์กรต่างๆ ทั่วโลกมีจำนวนองค์กรที่ได้รับการรับรองแล้วจำนวนทั้งสิ้น 4,282 ใบรับรอง (ข้อมูล ณ วันที่ 14 กรกฎาคม 2551: www.iso27001certificates.com)

ISO/IEC 20000-1:2005 Information technology -- Service management -- Part 1: Specification

มาตรฐานการบริหารจัดการการให้บริการสารสนเทศ: ISO/IEC 20000-1:2005 ได้รับการพัฒนามาจากมาตรฐานเดิม นั่นก็คือ มาตรฐาน BS 15000

ความเป็นมาของมาตรฐาน ISO/IEC 20000 สืบเนื่องมาจากปัจจุบันหน่วยงานต่างๆ ทั้งองค์กรภาครัฐและภาคเอกชนมีการมอบหมายงานในส่วนที่เกี่ยวข้องกับระบบสารสนเทศขององค์กรตัวเองให้แก่หน่วยงานภาคนอกเข้ามาดูแลรับผิดชอบและดำเนินการแทน (Outsource หรือ IT Service Provider) สาเหตุสำคัญมาจากกระบวนการด้านสารสนเทศค่อนข้างมีความซับซ้อน ต้องอาศัยผู้เชี่ยวชาญที่มีประสบการณ์มาดำเนินการ และเพื่อลดค่าใช้จ่ายในการดำเนินการเกี่ยวกับการจัดการระบบสารสนเทศขององค์กร

ซึ่งจุดนี้เองจึงเป็นเหตุสำคัญและเป็นปัจจัยหลักที่หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ (IT Service Provider) จำเป็นต้องมีการดำเนินการและปฏิบัติให้สอดคล้องมาตรฐาน ISO/IEC 20000 เพื่อช่วยให้องค์กรที่เป็นผู้รับบริการ และ/หรือลูกค้า เกิดความมั่นใจว่าหน่วยงานให้บริการนั้นๆ มีประสิทธิภาพ-ประสิทธิผลการดำเนินการ มีเสถียรภาพการบริหารจัดการที่ดี สามารถดำเนินการได้อย่างมั่นคง ต่อเนื่อง เป็นไปตามสัญญา/ข้อตกลง และสามารถสร้างความพึงพอใจให้แก่ผู้รับบริการและลูกค้า ซึ่งสามารถสะท้อนให้เห็นว่าผู้ให้บริการมีมาตรฐานในการควบคุมคุณภาพของการให้บริการ

โครงสร้างข้อกำหนด ISO/IEC 20000-1:2005

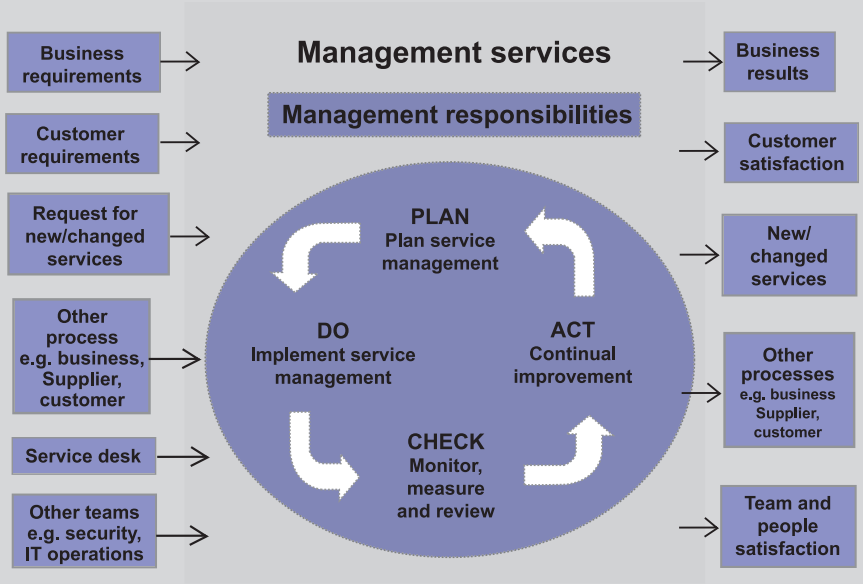
- ข้อ 1: ขอบข่าย (Scope)
- ข้อ 2: บทนิยามและคำศัพท์ (Terms and definitions)

สำหรับข้อกำหนดมาตรฐาน ISO/IEC 20000-1:2005 ที่องค์กรต้องนำไปปฏิบัติ คือ ข้อกำหนดตั้งแต่ข้อที่ 3 ถึงข้อกำหนดข้อที่ 10 ได้แก่

- ข้อ 3: ข้อกำหนดสำหรับการบริหารจัดการ (Requirements for a management system) ประกอบด้วย
  - ความรับผิดชอบของผู้บริหาร (Management responsibility)
  - ข้อกำหนดด้านเอกสาร (Documentation requirements)
  - ความรู้ความสามารถจิตสำนึกและการฝึกอบรม (Competence, awareness and training)
- ข้อ 4: การวางแผนและการบริหารจัดการการให้บริการ (Planning and implementing service management) ประกอบด้วย
  - การบริหารจัดการแผนการให้บริการ (Plan service management, Plan: P)
  - การบริหารจัดการการให้บริการและการบริการที่จัดให้มี (Implement service management and provide the service, Do: D)
  - การเฝ้าระวัง การวัด และการทบทวน (Monitoring, measuring and reviewing, Check: C)
  - การปรับปรุงอย่างต่อเนื่อง (Continual improvement, Act: A)

โดยมุ่งเน้นที่นโยบายและการปรับปรุงการบริหารจัดการ

จากการพิจารณาข้อกำหนด **มาตรฐาน** ISO/IEC 20000-1:2005 ข้อที่ 4 การวางแผนและการบริหารจัดการการให้บริการ พบว่า มาตรฐาน ISO/IEC 20000-1 อาศัยหลักการพื้นฐาน PDCA Model: Plan - Do - Check - Act เช่นเดียวกับมาตรฐาน ISO/IEC 27001:2005 โดยองค์กรที่นำมาตรฐานนี้ไปปฏิบัติ (Implement) ต้องมีการดำเนินการตามแผนภาพ:

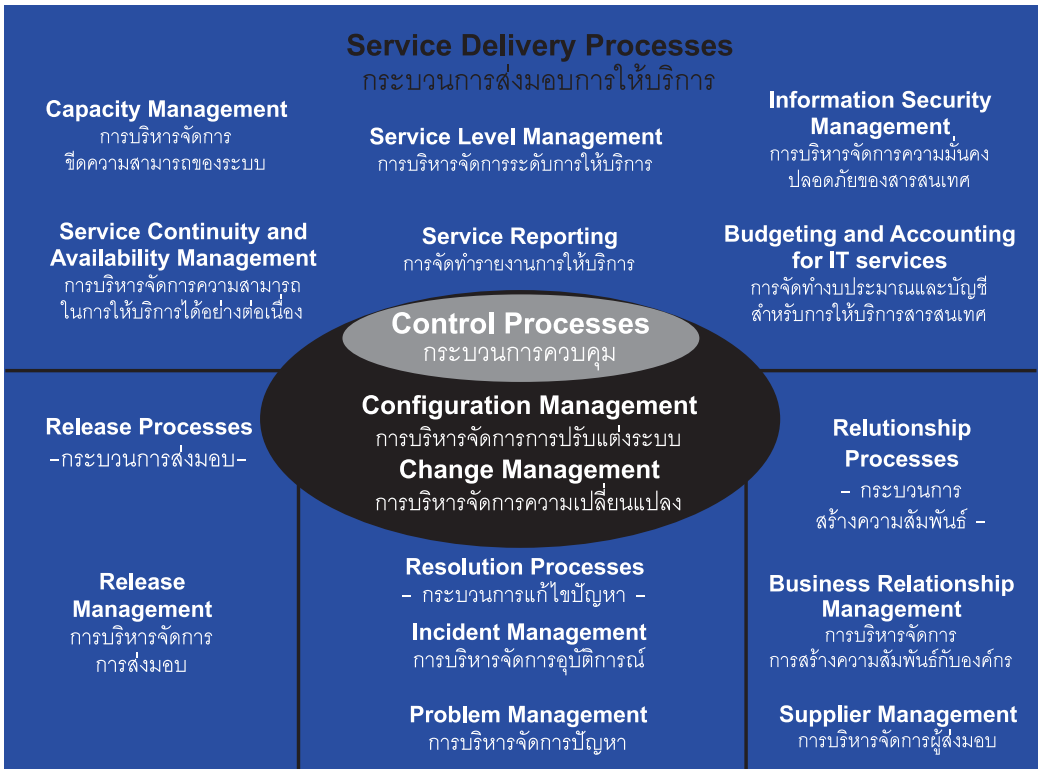


แผนภาพ : PDCA methodology for service management processes

- **ข้อ 5: การวางแผนและการดำเนินการปฏิบัติ กรณีที่มีการให้บริการใหม่หรือมีการเปลี่ยนแปลงการให้บริการ** (Planning and implementing new or changed services)
- **ข้อ 6: กระบวนการส่งมอบการให้บริการ** (Service delivery process) ประกอบด้วย
  - การบริหารจัดการระดับการให้บริการ (Service level management)
  - การจัดทำรายงานการให้บริการ (Service reporting)
  - การบริหารจัดการความสามารถในการให้บริการได้อย่างต่อเนื่อง (Service continuity and availability management)
  - การจัดทำงบประมาณและบัญชีสำหรับการให้บริการสารสนเทศ (Budgeting and accounting for IT services)
  - การบริหารจัดการขีดความสามารถของระบบ (Capacity management)
  - การบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information security management)
- **ข้อ 7: กระบวนการสร้างความสัมพันธ์** (Relationship processes) ประกอบด้วย
  - ข้อกำหนดทั่วไป (General)

- การบริหารจัดการการสร้างความสัมพันธ์กับองค์กร (Business relationship management)
- การบริหารจัดการผู้ส่งมอบ (Supplier management)

- **ข้อ 8: กระบวนการแก้ไขปัญหา** (Resolution processes) ประกอบด้วย
  - ที่มา (Background): องค์กรต้องแยกกระบวนการการบริหารจัดการอุบัติการณ์ออกจากกระบวนการการบริหารจัดการปัญหา แต่อย่างไรก็ตามทั้ง 2 กระบวนการนี้ ต้องคงความเชื่อมโยงกันไว้
  - การบริหารจัดการอุบัติการณ์ (Incident management)
  - การบริหารจัดการปัญหา (Problem management)
- **ข้อ 9: กระบวนการควบคุม** (Control processes) ประกอบด้วย
  - การบริหารจัดการการปรับแต่งระบบ (Configuration management)
  - การบริหารจัดการความเปลี่ยนแปลง (Change management)
- **ข้อ 10: กระบวนการส่งมอบ** (Release process) ประกอบด้วยกระบวนการบริหารจัดการการส่งมอบ (Release management process)



แผนภาพ: องค์ประกอบของกระบวนการบริหารจัดการการให้บริการ (Service Management Processes)

ประเด็นสำคัญของข้อกำหนด ISO/IEC 20000-1:2005

- **กระบวนการส่งมอบการให้บริการ - การบริหารจัดการระดับการให้บริการ** (Service level management) ประเด็นสำคัญของข้อกำหนด คือ ผู้ให้บริการ และผู้รับบริการ (ลูกค้า) รวมถึงผู้เกี่ยวข้องทั้งหมด ต้องทำการตกลงและกำหนดขอบเขตของการให้บริการแต่ละประเภท โดยข้อตกลงของการให้บริการนี้ เรียกว่า **"ข้อตกลงระดับการให้บริการ** (Service Level Agreements: SLAs)" เช่น การให้บริการแก้ไขปัญหาการใช้งานเรื่องการถูกโจมตีจากไวรัสของเครื่องคอมพิวเตอร์ ผู้ให้บริการต้องดำเนินแล้วเสร็จภายในระยะเวลา 4 ชั่วโมงนับจากเวลาที่ได้รับแจ้งจากผู้รับบริการ เป็นต้น

- **กระบวนการส่งมอบการให้บริการ - การจัดทำรายงานการให้บริการ** (Service reporting) โดยรายงานการให้บริการต้องประกอบด้วย:
  - ผลของการดำเนินการเทียบกับเป้าหมายระดับการบริการที่ได้กำหนดไว้
  - สิ่งที่ไม่สอดคล้องตามข้อกำหนดและประเด็นอื่นๆ ที่เกี่ยวข้อง เช่น NCs เทียบกับข้อตกลงระดับการให้บริการ (SLA) เป็นต้น
  - ข้อมูลด้านปริมาณ/ภาระงาน (Workload characteristics) เช่น ปริมาณการใช้ทรัพยากรต่าง ได้แก่ Disk / CPU / Server / และอื่นๆ เป็นต้น
  - รายงานการดำเนินการหลังจากการเกิดเหตุการณ์สำคัญ เช่น การเกิดอุบัติการณ์และการเปลี่ยนแปลง เป็นต้น
  - ข้อมูลแนวโน้ม เช่น ระบบปฏิบัติการใหม่ที่คาดว่าจะมีการประกาศใช้ เป็นต้น
  - การวิเคราะห์ความพึงพอใจ

▶ **กระบวนการส่งมอบการให้บริการ - การบริหารจัดการขีดความสามารถของระบบ** (Capacity management) ทั้งนี้เพื่อให้มั่นใจว่าองค์กรที่เป็นผู้ให้บริการมีขีดความสามารถในการดำเนินการ โดยองค์กรต้องมีการจัดทำแผนการดำเนินการประจำปี และมีการระบุสิ่งที่ธุรกิจต้องการ นอกจากนี้ การบริหารจัดการขีดความสามารถต้องมีการพิจารณาถึงองค์ประกอบต่างๆ ดังต่อไปนี้

- ความต้องการด้านประสิทธิผลและขีดความสามารถการดำเนินการในปัจจุบันและอนาคต
- การกำหนดช่วงระยะเวลาและค่าใช้จ่ายสำหรับการปรับปรุงและการพัฒนาการให้บริการ
- การประเมินผลกระทบของการปรับปรุงและการพัฒนาการให้บริการ ความต้องการด้านการเปลี่ยนแปลง และการนำเทคโนโลยี - เทคนิคใหม่ๆ เข้ามาพัฒนาขีดความสามารถของระบบ
- การคาดการณ์ผลกระทบของการเปลี่ยนแปลงภายนอก เช่น กฎหมาย เป็นต้น
- ข้อมูลและกระบวนการต่างๆ ที่ใช้ประกอบการการวิเคราะห์คาดการณ์ถึงขีดความสามารถของระบบ

▶ **กระบวนการส่งมอบการให้บริการ - การบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ** (Information security management) **สามารถอ้างอิงและนำแนวปฏิบัติของมาตรฐาน ISO/IEC 17799 หลักปฏิบัติสำหรับความมั่นคงปลอดภัยของสารสนเทศ** (Information technology – Security techniques – Code of practice for information security management) มาประยุกต์ใช้ร่วมกับกิจกรรมการให้บริการขององค์กรได้

การควบคุมความมั่นคงปลอดภัยของสารสนเทศที่เหมาะสมนั้น องค์กรต้องจัดทำและปฏิบัติตามนโยบายความมั่นคงปลอดภัยที่กำหนด และดำเนินการจัดการกับความเสี่ยงที่เกี่ยวข้องกับการให้บริการหรือระบบขององค์กร เช่น การกำหนดมาตรการความมั่นคงปลอดภัยที่จำเป็น อาทิ การติดตั้ง Server ป้องกันไวรัส การกำหนดผู้รับผิดชอบในการดูแลและรายงานปัญหาฉุกเฉิน เป็นต้น

▶ **กระบวนการแก้ไขปัญหา - การบริหารจัดการอุบัติการณ์** (Incident management) **และการบริหารจัดการปัญหา** (Problem management) เพื่อบริหารจัดการอุบัติการณ์ต่างๆ ที่มีผลกระทบต่อการบริการขององค์กร โดยมุ่งเน้นที่การกู้ระบบหรือธุรกรรมให้กลับคืนสู่สภาวะปกติอย่างรวดเร็วที่สุด และเพื่อลดการหยุดชะงักของธุรกิจและการให้การบริการ โดยมุ่งเน้นที่การวิเคราะห์หาสาเหตุของปัญหา หรืออุบัติการณ์ที่ทำให้ขาดความต่อเนื่อง เพื่อแก้ไขและป้องกันการเกิดซ้ำ (สามารถศึกษารายละเอียดเพิ่มเติมเกี่ยวกับ**การบริหารจัดการอุบัติการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศได้จากมาตรฐาน** ISO/IEC TR 18044 Information technology -- Security techniques -- Information security incident management)

▶ **กระบวนการควบคุม - การบริหารจัดการการปรับแต่งระบบ** (Configuration management) องค์กรต้องกำหนดและควบคุมองค์ประกอบของการให้บริการและโครงสร้างพื้นฐานและบำรุงรักษาข้อมูลของการปรับแต่งระบบให้มีความถูกต้อง

การบริหารจัดการการปรับแต่งระบบนั้น องค์กรต้องกำหนดกลไกสำหรับการชี้บ่ง การควบคุม และการสร้างร่องรอย Versions ขององค์ประกอบที่สามารถชี้บ่งการให้บริการและโครงสร้างพื้นฐาน เพื่อให้มั่นใจว่าระดับของการควบคุมเพียงพอและเหมาะสมต่อ:

- ความต้องการของธุรกิจ
- ความเสี่ยงอันเนื่องมาจากความล้มเหลวของการปรับแต่งระบบ
- ระดับความสำคัญของการให้บริการที่เกี่ยวข้อง

▶ **กระบวนการควบคุม - การบริหารจัดการความเปลี่ยนแปลง** (Change management) เพื่อให้มั่นใจว่าการเปลี่ยนแปลงต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศได้รับการตรวจสอบ การอนุมัติ การนำไปปฏิบัติ และการทบทวน

การเปลี่ยนแปลงต่างๆ ต้องมีการบันทึกและจัดประเภท เช่น ประเภทเร่งด่วน ประเภทเหตุการณ์ฉุกเฉิน ประเภทข้อบกพร่องสำคัญ ประเภทข้อบกพร่องย่อย เป็นต้น นอกจากนี้ การร้องขอให้มีการเปลี่ยนแปลงใดๆ นั้น องค์กรต้องทำการประเมินความเสี่ยง ผลกระทบ และประโยชน์ทางธุรกิจ

ในกรณีที่การเปลี่ยนแปลงไม่ประสบความสำเร็จด้วยสาเหตุใดสาเหตุหนึ่งนั้น กระบวนการบริหารจัดการการเปลี่ยนแปลงต้องสามารถทำการย้อนกลับ หรือทำการแก้ไขกลับคืนสู่ระบบเดิมได้

▶ **กระบวนการส่งมอบ - กระบวนการบริหารจัดการการส่งมอบ** (Release management process) ในข้อกำหนดนี้ คำว่า **"กระบวนการส่งมอบ"** นั้น หมายถึง การส่งมอบไปสู่การใช้งานจริงให้แก่ผู้รับบริการ (ลูกค้า)

องค์กรผู้ให้บริการต้องมีการวางแผนธุรกิจ/กิจกรรมการให้บริการระบบสารสนเทศ ซอร์ฟแวร์และฮาร์ดแวร์ โดยแผนที่วางไว้นั้น ต้องได้รับการเห็นชอบและการอนุญาตจากผู้เกี่ยวข้อง เช่น ลูกค้า ผู้ใช้งาน (Users) ผู้ปฏิบัติงาน เป็นต้น

สำหรับกรณีที่กระบวนการส่งมอบไม่ประสบความสำเร็จ ต้องสามารถทำการย้อนกลับ หรือทำการแก้ไขกลับคืนสู่ระบบเดิมได้ เช่นเดียวกับกระบวนการบริหารจัดการความเปลี่ยนแปลง ทั้งนี้ องค์กรผู้ให้บริการต้องเตรียมระบบสำหรับการทดสอบก่อนการส่งมอบให้แก่ผู้รับบริการไปใช้งานจริง

นอกจากนี้ ความสำเร็จและความล้มเหลวของการส่งมอบต้องมีการวัดผล โดยการวัดผลต้องรวมถึงอุบัติการณ์ที่เกี่ยวข้องในช่วงของกระบวนการส่งมอบ การวิเคราะห์และการตรวจสอบผลกระทบต่อธุรกิจ การดำเนินการด้านสารสนเทศ (IT) และทรัพยากรบุคคลที่เกี่ยวข้อง และที่สำคัญต้องสามารถใช้เป็นข้อมูลในการวางแผนสำหรับการปรับปรุงการให้บริการได้อีกด้วย

องค์กรที่มีความสนใจในข้อกำหนด**มาตรฐานการบริหารจัดการการให้บริการสารสนเทศ** ISO/IEC 20000-1:2005 และต้องการศึกษารายละเอียดของการปฏิบัติให้มีความสอดคล้อง สามารถศึกษาแนวทางเพิ่มเติมได้จากข้อกำหนดมาตรฐาน ISO/IEC 20000-2:2005 Information technology -- Service management -- Part 2: Code of practice

ISO/IEC 17799:2005 Information technology –– Security techniques –– Code of practice for information security management

ความเป็นมาของมาตรฐาน ISO/IEC 17799:2005 หลักปฏิบัติสำหรับความมั่นคงปลอดภัยของสารสนเทศ เป็นมาตรฐานที่มีจุดกำเนิดมาจากมาตรฐาน BS 7799-1 และถูกพัฒนาจากมาตรฐาน ISO/IEC 17799:2000 ภายใต้คณะกรรมการเทคนิคร่วมที่ 1 (Joint Technical Committee: ISO/IEC JTC 1) และคณะกรรมการย่อยที่ 27 (Sub-committee: SC 27) ซึ่งมาตรฐาน ISO/IEC 17799:2005 ที่ใช้กันในปัจจุบันนับเป็นฉบับปรับปรุงครั้งที่ 2

สำหรับความสมบูรณ์ของการบูรณาการ **ระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information security management systems: ISMS)** นั้น องค์กรควรมีการประยุกต์การปฏิบัติเข้ากับมาตรฐานตระกูล **ISO/IEC 27000** (A family of ISMS: Series of number 27000 et seq.)

โครงสร้างข้อกำหนด ISO/IEC 17799:2005

- ข้อ 1: ขอบข่าย (Scope)
- ข้อ 2: บทนิยามและคำศัพท์ (Terms and definitions)
- ข้อ 3: โครงสร้างของมาตรฐาน (Structure of this standard) ประกอบด้วย
  - ▶ ข้อกำหนดย่อย (Clauses) ที่องค์กรต้องถือปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศมีจำนวนทั้งสิ้น 11 ข้อกำหนดย่อย (ซึ่งก็คือข้อกำหนดข้อที่ 5 ถึงข้อกำหนดข้อที่ 15 ของมาตรฐาน ISO/IEC 17799 นั่นเอง)
  - ▶ ประเภทความปลอดภัยหลัก (Main security categories) ประกอบด้วยวัตถุประสงค์ควบคุม (สิ่งที่องค์กรต้องการ) และปัจจัยควบคุมอื่นๆ เพื่อให้องค์กรบรรลุวัตถุประสงค์ควบคุมและมีการกำหนดนิยามศัพท์สำคัญที่พบปรากฏในรายละเอียดของข้อกำหนดมาตรฐาน ISO/IEC 17799 แต่ละข้อ ได้แก่นิยามของคำว่า:
  - ▶ **การควบคุม** (Control)

- **แนวทางการปฏิบัติ** (Implementation guidance)
- **และข้อมูลอื่น ๆ** (Other information)"

ทั้งนี้ เนื่องจาก**ข้อกำหนดย่อยของมาตรฐาน** ISO/IEC 17799 เช่น ข้อกำหนดย่อยที่ 6.1.1 ความมุ่งมั่นของฝ่ายบริหารต่อความมั่นคงปลอดภัยของสารสนเทศ (Management commitment to information security) ข้อกำหนดย่อยที่ 7.1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of assets) ข้อกำหนดย่อยที่ 8.1.3 ระยะเวลาและเงื่อนไขของการจ้างงาน (Terms and conditions of employment) เป็นต้น **จะมีการระบุสิ่งที่องค์กรต้องปฏิบัติตามแยกตาม 3 คำนิยามดังกล่าว**

- **ข้อ 4: การประเมินความเสี่ยงและการจัดการความเสี่ยง** (Risk assessment and treatment) ประกอบด้วย
  - **การประเมินความเสี่ยง** (Assessing security risks) โดยองค์กรควรพิจารณาชี้บ่ง โอกาสของการเกิด และความสำคัญ (ความรุนแรง) ของความเสี่ยงเทียบกับระดับความเสี่ยงที่ยอมรับได้ขององค์กรและวัตถุประสงค์ขององค์กร
  - **การจัดการความเสี่ยง** (Treating security risks) โดยก่อนที่องค์กรจะพิจารณาดำเนินการจัดการใดๆ ต่อความเสี่ยง องค์กรควรมีการพิจารณาว่าความเสี่ยงนั้นๆ ยอมรับได้หรือไม่ (รายละเอียดเพิ่มเติม สามารถศึกษาได้จากมาตรฐาน ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management และมาตรฐาน ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management **นอกจากนี้ สามารถศึกษาคำศัพท์และนิยามต่าง ๆ ที่เกี่ยวข้องกับความเสี่ยง (Risk) ได้จากมาตรฐาน ISO/IEC Guide 73:2002 Risk management -- Vocabulary -- Guidelines for use in standards)**

สำหรับข้อกำหนดมาตรฐาน ISO/IEC 17799:2005 ที่องค์กรต้องนำไปปฏิบัติ คือ ข้อกำหนดตั้งแต่ข้อที่ 5 ถึงข้อกำหนดข้อที่ 15 ได้แก่

- **ข้อ 5: นโยบายความมั่นคงปลอดภัย** (Security policy) มีวัตถุประสงค์ในการกำหนดแนวทางการบริหารจัดการและสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยของสารสนเทศขององค์กรให้มีความสอดคล้องตามข้อกำหนดกฎหมาย และกฎระเบียบข้อบังคับที่เกี่ยวข้อง โดยข้อกำหนดข้อที่ 5 นโยบายความมั่นคงปลอดภัยนี้ ประกอบด้วยข้อกำหนดย่อยจำนวน 2 ข้อ ได้แก่
  - เอกสารนโยบายความมั่นคงปลอดภัยของสารสนเทศ (Information security policy document)
  - การทบทวนนโยบายความมั่นคงปลอดภัยของสารสนเทศ (Review of the information security policy)
- **ข้อ 6: โครงสร้างความมั่นคงปลอดภัยขององค์กร** (Organization of information security) มีวัตถุประสงค์เพื่อบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศภายในองค์กร ประกอบด้วย
  - **การบริหารจัดการภายในองค์กร** (Internal Organization) แบ่งย่อยออกเป็น
  - **ความมุ่งมั่นของฝ่ายบริหารต่อความมั่นคงปลอดภัยของสารสนเทศ** (Management commitment to information security)
  - **การประสานงานด้านความมั่นคงปลอดภัยของสารสนเทศ** (Information security co-ordination) โดยองค์กรต้องกำหนดให้มีผู้แทนจากหน่วยงานต่างๆ ในการดำเนินการที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศขององค์กร
  - **การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ** (Allocation of information security responsibilities) โดยเฉพาะอย่างยิ่งการกำหนดหน้าที่ความรับผิดชอบสำหรับการป้องกันทรัพย์สินส่วนบุคคล (Individual assets) และการดำเนินการที่เกี่ยวข้องกับกระบวนการความมั่นคงปลอดภัยเฉพาะทาง
  - **กระบวนการสำหรับการอนุมัติการใช้งานอุปกรณ์/สิ่งอำนวยความสะดวกด้านสารสนเทศ** (Authorization process for information processing facilities) ในกรณีที่มีอุปกรณ์/สิ่งอำนวยความสะดวกใหม่
  - **สัญญารักษาความลับ** (Confidentiality agreements)
  - **การติดต่อกับหน่วยงานอื่นในกรณีจำเป็น** (Contact with authorities) องค์กรต้องมีขั้นตอนการปฏิบัติงาน (Procedure) สำหรับการติดต่อกับหน่วยงานอื่นในกรณีจำเป็น เช่น หน่วยงานกฎหมาย (Law enforcement) หน่วยงานดับเพลิง (Fire department) และผู้รับผิดชอบในการดำเนินการขององค์กร (Supervisory authorities) นอกจากนี้ กรณีที่องค์กรมีการใช้อินเตอร์เน็ต องค์กรนั้นๆ จำเป็นต้องมีข้อมูลในการติดต่อกับหน่วยงานผู้ให้บริการอินเตอร์เน็ตหรือหน่วยงานที่ให้บริการโทรคมนาคมด้วย
  - **การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ** (Contact with special interest groups) องค์กรต้องเก็บรักษาการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ หรือหน่วยงานที่มีความเชี่ยวชาญเฉพาะทาง และสมาคม/องค์กรที่มีความชำนาญด้านความมั่นคงปลอดภัยของสารสนเทศ
  - **การทบทวนด้านความมั่นคงปลอดภัยของสารสนเทศ** (Independent review of information security) องค์กรที่มีการบริหารจัดการสารสนเทศ เช่น องค์กรมีการกำหนดวัตถุประสงค์ควบคุม มีการควบคุมการปฏิบัติงาน มีการกำหนดนโยบาย กระบวนการและขั้นตอนปฏิบัติงานด้านความมั่นคงปลอดภัยของสารสนเทศ เป็นต้น ต้องดำเนินการทบทวนตามช่วงเวลาที่กำหนด หรือในกรณีที่มีการเปลี่ยนแปลงที่สำคัญต่อการดำเนินการด้านความมั่นคงปลอดภัยของสารสนเทศ

- **หน่วยงานภายนอก** (External parties) มีจุดมุ่งหมายเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลองค์กรและกระบวนการต่างๆ ในส่วนที่มีความเกี่ยวเนื่องกับหน่วยงานภายนอก แบ่งย่อยออกเป็น
  - **การชี้บ่งความเสี่ยงที่เกี่ยวข้องกับหน่วยงานภายนอก** (Identification of risks related to external parties)
  - **การชี้แจงข้อกำหนดความมั่นคงปลอดภัยในกรณีที่มีการติดต่อกับลูกค้า**(Addressing security when dealing with customers) กรณีที่องค์กรให้ลูกค้าเข้าถึงระบบสารสนเทศหรือทรัพย์สินขององค์กรได้นั้น องค์กรต้องทำการชี้แจงข้อกำหนดความมั่นคงปลอดภัยให้ลูกค้ารับทราบ
  - **การชี้แจงข้อกำหนดความมั่นคงในกรณีที่มีการตกลงกับหน่วยงานภายนอก** (Addressing security in third party agreements)

- **ข้อ 7: การบริหารจัดการทรัพย์สิน** (Asset management) ประกอบด้วย
  - **หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร** (Responsibilities for assets) แบ่งย่อยออกเป็น
    - **การจัดทำบัญชีทรัพย์สินขององค์กร** (Inventory of assets) ในกรณีที่องค์กรมีการประเมินทรัพย์สินสำคัญ สามารถศึกษาเพิ่มเติมได้จากมาตรฐาน ISO/IEC TR 13335-3)
    - **การระบุผู้เป็นเจ้าของทรัพย์สิน** (Ownership of assets)
    - **การใช้งานทรัพย์สินที่เหมาะสม** (Acceptable use of assets)
  - **การจำแนกประเภทสารสนเทศ** (Information classification) แบ่งย่อยออกเป็น
    - แนวทางการจำแนกประเภท (Classification guidelines)
    - การควบคุมและการแสดงป้ายชื่อสารสนเทศ (Information labeling and handling)

- **ข้อ 8: ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล** (Human resources security) ประกอบด้วย
  - **ความมั่นคงปลอดภัยก่อนการจ้างงาน** (Prior to employment) ครอบคลุมลูกจ้าง คู่สัญญา และผู้ใช้งานจากหน่วยงานภายนอก แบ่งย่อยออกเป็น
    - การกำหนดบทบาทหน้าที่และความรับผิดชอบ (Rolesand responsibilities)
    - การตรวจสอบคุณสมบัติผู้สมัคร (Screening)
    - ระยะเวลาและเงื่อนไขการจ้างงาน (Terms and conditions of employment)
  - **ความมั่นคงปลอดภัยระหว่างการจ้างงาน** (During employment) ครอบคลุมลูกจ้าง คู่สัญญา และผู้ใช้งานจากหน่วยงานภายนอกเช่นเดียวกับความมั่นคงปลอดภัยช่วงก่อนการจ้างงาน แบ่งย่อยออกเป็น

- **การกำหนดหน้าที่ความรับผิดชอบในการบริหารจัดการ** (Management responsibilities)
- **การสร้างจิตสำนึก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยของสารสนเทศ** (Information security awareness, education and training)
- **กระบวนการทางวินัยเกี่ยวกับการลงโทษ** (Disciplinary process)

▶ **การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน** (Termination or change of employment) แบ่งย่อยออกเป็น

- **การกำหนดหน้าที่ความรับผิดชอบหลังการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน** (Termination responsibilities)
- **การส่งคืนทรัพย์สินขององค์กร** (Return of assets)
- **การถอดถอนสิทธิในการเข้าถึงระบบสารสนเทศขององค์กร** (Removal of access right)

● **ข้อ 9: ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม** (Physical and environmental security) ประกอบด้วย การกำหนดบริเวณปลอดภัย (Secure areas) และความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security)

● **ข้อ 10: การบริหารจัดการด้านการสื่อสารและการปฏิบัติการ** (Communications and operations management) ประกอบด้วย

▶ **การกำหนดหน้าที่ความรับผิดชอบและการจัดทำเอกสารขั้นตอนการปฏิบัติงาน** (Operational procedures and responsibilities)

▶ **การบริหารจัดการการส่งมอบการให้บริการของหน่วยงานภายนอก** (Third party service delivery management)

▶ **การวางแผนระบบสารสนเทศและการตรวจรับ** (System planning and acceptance) เพื่อลดความเสี่ยงจากความล้มเหลวของระบบโดยพิจารณาจากการบริหารจัดการขีดความสามารถของระบบสารสนเทศ (Capacity management)และการตรวจรับระบบ(System acceptance) ในกรณีที่มีระบบสารสนเทศใหม่ และการเปลี่ยนแปลง Version ใหม่

▶ **การป้องกันจากการถูกประสงค์ร้าย** (Protection against malicious and mobile code) เพื่อป้องกัน (Prevent) และรักษาความสมบูรณ์ (Integrity) ระหว่างซอร์ฟแวร์ (Software) และระบบเครือข่าย (Network) จากการถูกโจมตีจากโปรแกรมที่ไม่ประสงค์ดี หรือที่ไม่ได้รับอนุญาต (ในที่นี้หมายถึง Malicious code เช่น ไวรัส เป็นต้น) และจากโปรแกรมที่สามารถเคลื่อนที่ได้จากหน่วยความจำของคอมพิวเตอร์เครื่องหนึ่งเพื่อไปทำงาน (โจมตี) ในหน่วยความจำของคอมพิวเตอร์อีกเครื่องหนึ่ง หรือจากหน่วยความจำของคอมพิวเตอร์เครื่องหนึ่งไปทำงาน (โจมตี) ในระบบเครือข่าย/โปรแกรมที่เป็นเป้าประสงค์ ซึ่งก็คือ Mobile code นั่นเอง

▶ **การสำรองข้อมูล** (Back-up) เพื่อรักษาความสมบูรณ์และความพร้อมใช้ของระบบสารสนเทศและอุปกรณ์

▶ **การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย** (Network security management) เพื่อให้มั่นใจว่าองค์กรมีการดำเนินการป้องกันระบบสารสนเทศและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศ

▶ **การจัดการสื่อที่ใช้ในการบันทึกข้อมูล**(Media handling) เพื่อป้องกันจากการเปิดเผยข้อมูลสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต จากการแก้ไขเปลี่ยนแปลงข้อมูลสารสนเทศ จากการย้ายข้อมูลสารสนเทศ หรือจากการทำลายทรัพย์สินสารสนเทศ และจากภาวะที่ถูกขัดขวาง/การชะงักงัน (Interruption) ที่เกี่ยวข้องกับกิจกรรมธุรกิจ

▶ **การแลกเปลี่ยนข้อมูลสารสนเทศ** (Exchange information) เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและซอร์ฟแวร์ที่มีการแลกเปลี่ยนข้อมูลภายในและภายนอกองค์กร

▶ **การให้บริการธุรกรรมทางอิเล็กทรอนิกส์** (Electronic commerce services)

▶ **การเฝ้าระวัง** (Monitoring) เพื่อตรวจสอบ (Detect) กิจกรรมกระบวนการสารสนเทศที่ไม่ได้รับอนุญาต ตรวจสอบประสิทธิผลของการควบคุม และยืนยันความสอดคล้องของการดำเนินการระบบสารสนเทศขององค์กรเทียบกับนโยบาย

● **ข้อ 11: การควบคุมการเข้าถึงระบบสารสนเทศ** (Access control) ประกอบด้วย

▶ **ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึง** (Business requirement for access control)

▶ **การบริหารจัดการการเข้าถึงสารสนเทศของผู้ใช้งาน** (User access management)

▶ **หน้าที่ความรับผิดชอบของผู้ใช้งาน** (User responsibilities)

▶ **การควบคุมการเข้าถึงเครือข่ายสารสนเทศ** (Network access control)

▶ **การควบคุมการเข้าถึงระบบปฏิบัติการ** (Operating system access control)

▶ **การใช้งานและการควบคุมการเข้าถึงสารสนเทศ** (Application and information access control) เพื่อป้องกันการเข้าถึงสารสนเทศโดยไม่ได้รับอนุญาต องค์กรต้องจัดทำระบบการใช้งานของระบบสารสนเทศ เช่น การกำหนดสิทธิของผู้ใช้งาน เป็นต้น

▶ **อุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร** (Mobile computing and teleworking)

● **ข้อ 12: การเข้าถือสิทธิในระบบสารสนเทศ การพัฒนาและการบำรุงรักษา** (Information systems acquisition, development and maintenance) เพื่อให้มั่นใจในความมั่นคงปลอดภัยของทุกองค์ประกอบของระบบสารสนเทศองค์กร ประกอบด้วย

- **ข้อกำหนดความมั่นคงปลอดภัยของระบบสารสนเทศ** (Security requirements of information systems)
- **กระบวนการตรวจสอบความถูกต้องในการใช้งาน** (Correct processing in applications) เพื่อป้องกันความผิดพลาด การสูญหาย การเปลี่ยนแปลงโดยไม่ได้รับอนุญาต หรือการใช้งานที่ผิดวัตถุประสงค์ของสารสนเทศองค์กร
- **การควบคุมโดยระบบการเข้ารหัส** (Cryptographic controls) เพื่อป้องกันข้อมูลประเภทความลับ การยืนยันตัวตนของผู้ใช้งาน หรือรักษาความถูกต้องสมบูรณ์ของสารสนเทศโดยวิธีการเข้ารหัส
- **ความมั่นคงปลอดภัยของระบบไฟล์ข้อมูล** (Security of system files)
- **ความมั่นคงปลอดภัยในกระบวนการพัฒนาและกระบวนการสนับสนุนระบบสารสนเทศ** (Security in development and support processes) เพื่อรักษาความมั่นคงปลอดภัยของการใช้งานระบบซอร์ฟแวร์และสารสนเทศขององค์กร
- **การบริหารจัดการการถูกโจมตีทางเทคนิค** (Technical vulnerability management) เพื่อลดความเสี่ยงอันเกิดจากการถูกโจมตีทางเทคนิคโดยอาศัยช่องโหว่ของการเผยแพร่ข้อมูลสารสนเทศ โดยการกำหนดมาตรการ/วิธีการควบคุมจากการถูกโจมตี

- **ข้อ 13: การบริหารจัดการอุบัติการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ** (Information security incident management) เพื่อให้มั่นใจว่าเหตุการณ์ (Events) และจุดอ่อน (Weaknesses) ด้านความมั่นคงปลอดภัยของสารสนเทศขององค์กรได้รับปฏิบัติการแก้ไข (Corrective action) ในระยะเวลาที่เหมาะสม โดยต้องมีระบบการรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ และการบริหารจัดการอุบัติการณ์และการปรับปรุงด้านความมั่นคงปลอดภัยของสารสนเทศ (สามารถศึกษารายละเอียดเพิ่มเติมเกี่ยวกับการบริหารจัดการอุบัติการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศได้จากมาตรฐาน ISO/IEC TR 18044 Information technology – Security techniques – Information security incident management)
- **ข้อ 14: การบริหารจัดการความสามารถในการให้บริการได้อย่างต่อเนื่อง** (Business continuity management) เพื่อขัดขวางการหยุดชะงัก/ความไม่ต่อเนื่องที่มีต่อกิจกรรมทางธุรกิจ เพื่อป้องกันกระบวนการธุรกิจที่มีความสำคัญจากผลของความล้มเหลวของระบบสารสนเทศหรือจากการล่มของระบบสารสนเทศ และเพื่อให้มั่นใจว่าองค์กรสามารถดำเนินการกู้ระบบกลับคืนได้ภายในระยะเวลาที่เหมาะสม
- **ข้อ 15: ความสอดคล้อง** (Compliance) ประกอบด้วย
  - ความสอดคล้องตามข้อกำหนดกฎมาย (Compliance with legal requirements)
  - ความสอดคล้องกับนโยบายความมั่นคงปลอดภัยและมาตรฐาน และความสอดคล้องตามข้อกำหนดทางเทคนิค (Compliance with security policies and standards, and technical compliance)
  - การพิจารณาตรวจสอบระบบสารสนเทศ (Information systems audit considerations)

จากมาตรฐานทั้ง 3 มาตรฐานด้านความมั่นคงปลอดภัยของสารสนเทศดังกล่าวข้างต้นนั้น คงช่วยให้ผู้อ่านมองเห็นภาพของมาตรฐานด้านเทคโนโลยีสารสนเทศมากยิ่งขึ้น

อ้างอิง:

* องค์การระหว่างประเทศว่าด้วยการมาตรฐาน, www.iso.org
* ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย, www.thaicert.nectec.or.th
* กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, www.mict.go.th

รวบรวม ISO ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ

- ISO/IEC Guide 73:2002 Risk management -- Vocabulary -- Guidelines for use in standards
- ISO 10007:2003 Quality management systems -- Guidelines for configuration management
- ISO/IEC 11770-2:2008 Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques
- ISO/IEC 12207:2008 Systems and software engineering -- Software life cycle processes
- ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology
- ISO/IEC TR 14516:2002 Information technology -- Security techniques -- Guidelines for the use and management of trusted third party services
- ISO/IEC 14764:2006 Software engineering -- Software life cycle processes -- Maintenance
- ISO/IEC TR 15271:1998 Information technology -- Guide for ISO/IEC 12207 (Software life cycle processes)
- ISO/IEC 15288:2008 Systems and software engineering -- Systems life cycle processes
- ISO/IEC 15289:2006 Systems and software engineering -- Content of systems and software life cycle process information products (Documentation)
- ISO/IEC 15504-1:2004 Information technology -- Process assessment -- Part 1: Concepts and vocabulary
- ISO/IEC 15504-3:2004 Information technology -- Process assessment -- Part 3: Guidance on performing an assessment
- ISO/IEC 15504-4:2004 Information technology -- Process assessment -- Part 4: Guidance on use for process improvement and process capability determination
- ISO/IEC 15504-5:2006 Information technology -- Process assessment -- Part 5: An exemplar process assessment model
- ISO/IEC 15940:2006 Information technology -- Software engineering environment services
- ISO/IEC 16085:2006 Systems and software engineering -- Life cycle processes -- Risk management
- ISO/IEC TR 16326:1999 Software engineering -- Guide for the application of ISO/IEC 12207 to project management
- ISO/IEC 17799:2005 Information technology -- Security techniques -- Code of practice for information security management
- ISO/IEC 18028-1:2006 Information technology -- Security techniques -- IT network security -- Part 1: Network security management
- ISO/IEC 18028-4:2005 Information technology -- Security techniques -- IT network security -- Part 4: Securing remote access
- ISO/IEC 18028-5:2006 Information technology -- Security techniques -- IT network security -- Part 5: Securing communications across networks using virtual private networks
- ISO/IEC TR 18044:2004 Information technology -- Security techniques -- Information security incident management
- ISO/IEC TR 19760:2003 Systems engineering -- A guide for the application of ISO/IEC 15288 (Systems life cycle processes)
- ISO/IEC 20000-1:2005 Information technology -- Service management -- Part 1: Specification
- ISO/IEC 20000-2:2005 Information technology -- Service management -- Part 2: Code of practice
- ISO/TR 26122:2008 Information and documentation -- Work process analysis for records (แทนที่มาตรฐาน ISO 15489-1:2001 Information and documentation -- Record management -- Part 1: General ซึ่งถูกยกเลิก)
- ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements
- ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management
- ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management
- ISO/IEC 90003:2004 Software engineering -- Guidelines for the application of ISO 9001:2000 to computer software
- ISO/IEC TR 90005:2008 Software engineering -- Guidelines for the application of ISO 9001 to system life cycle processes
- .....

"ที่มา : www.iso27001certificate.com, 14 ก.ค. 51"

... สบทร. 1 ใน 7 องค์กรของประเทศไทย

กับการรับรอง ISO/IEC 27001 ...

สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ: สบทร. (Government Information Technology Services: GITS) เป็นหน่วยงานที่จัดตั้งขึ้นโดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ภายใต้สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ตามมติคณะรัฐมนตรี เมื่อวันที่ 21 พฤษภาคม 2540 ในการพัฒนาเครือข่าย GINet (Government Information Network) และกิจกรรมอื่นที่สนับสนุนการใช้เทคโนโลยีสารสนเทศแก่หน่วยงานภาครัฐ ต่อมาเมื่อวันที่ 18 กันยายน 2546 คณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติมีมติให้ สบทร. ดำเนินงานโดยใช้ข้อบังคับโครงการพิเศษ หรือระเบียบทุนประเดิม สังกัด สวทช. จนถึงปัจจุบัน

ตลอดระยะเวลา 10 ปีที่ผ่านมา สบทร. ได้ให้บริการด้านเทคโนโลยีสารสนเทศกับหน่วยงานภาครัฐตามภารกิจที่ได้รับมอบหมายไปแล้วเป็นจำนวนมาก ภายใต้วิสัยทัศน์ในการ "เป็นองค์กรพันธมิตร เพื่อยกระดับ e-Government ของประเทศไทยที่มีความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ (IT) อย่างมีคุณภาพและครบวงจร" (Your Dependable e-Government Partner)โดยให้บริการ 4 ด้านหลัก ได้แก่ บริการเครือข่ายสารสนเทศภาครัฐ (Government Network Services) บริการแอปพลิเคชั่นภาครัฐ (Government ASP Services) บริการระบบความมั่นคงปลอดภัยภาครัฐ (Government Information Security Services) และบริการซิสเต็มอินทิเกรชั่นสำหรับภาครัฐ (Government System Integration Services) ซึ่งนับได้ว่าครบทุกวงจรความต้องการด้านเทคโนโลยีสารสนเทศสำหรับหน่วยงานภาครัฐ

ISO กับกรอบการทำงานของ สบทร.:

ดร.ศักดิ์ เสกขุนทด ผู้อำนวยการสำนักบริการเทคโนโลยีสารสนเทศภาครัฐ และดำรงตำแหน่ง ISMR ได้นำระบบบริหารงานคุณภาพ ISO 9001:2000 มาประยุกต์ใช้เป็นกรอบการดำเนินงานของ สบทร. ร่วมกับมาตรฐาน ISO/IEC 27001:2005 โดยมาตรฐาน ISO 9001 นั้น เป็นพื้นฐานของการปฏิบัติตามข้อกำหนดมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ หรือ ISO/IEC 27001:2005 Information technology - Security techniques - Information Security Management Systems - Requirements เนื่องจากข้อกำหนดของทั้ง 2 มาตรฐานอิงตามหลักการ PDCA Model และมีโครงสร้างข้อกำหนดที่คล้ายคลึงกัน ซึ่งช่วยให้ สบทร. มีการทำงานเป็นระบบและมีประสิทธิภาพเพิ่มมากขึ้น สอดรับกับหลักการของข้อกำหนดมาตรฐานในเรื่อง **การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)** นอกจากนี้ จากการที่ สบทร. ได้รับการรับรองระบบงาน ทั้ง ISO 9001:2000 (ทั้งระบบ) และ ISO/IEC 27001:2005 (เฉพาะส่วนงานที่ดูแลเรื่องผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority: CA)) ยังเป็นการช่วยเสริมระดับความมั่นใจด้านความมั่นคงปลอดภัยของระบบสารสนเทศของการเป็นผู้ให้บริการ (Services Provider) ที่ดีตลอดมาของ สบทร.

เหตุผลและความจำเป็นของการทำ ISO/IEC 27001:2005 : สืบเนื่องจากการที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้มีมติเห็นชอบให้มีการใช้ระบบการมอบความไว้วางใจ (Trust Model) ในรูปแบบ Root CA ขึ้นในประเทศไทย ซึ่งกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้มอบหมายให้ สบทร.

BEST PRACTICE

ปฏิบัติหน้าที่ National Root CA หรือผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ระดับบนสุดของประเทศ ซึ่งจะเป็นศูนย์กลางในการสร้างความเชื่อมั่นในการติดต่อสื่อสารในรูปแบบอิเล็กทรอนิกส์ โดยเชื่อมโยงผู้ให้บริการออกใบรับรองทั้งในและต่างประเทศ ประกอบกับความมุ่งมั่นในเรื่องการปรับปรุงและการพัฒนาอย่างต่อเนื่อง ทำให้ สบทร. ก้าวสู่การเป็นองค์กรแห่งแรกของประเทศไทยที่ได้รับการรับรอง ISO/IEC 27001:2005 จาก British Standard Institution (BSI) เมื่อวันที่ 4 ธันวาคม 2549 จนทำให้ในวันนี้ สบทร. เป็นองค์กรที่มีระบบการบริหารจัดการภายในและระบบบริหารความมั่นคงปลอดภัยสารสนเทศในลักษณะเดียวกับองค์กรนานาชาติ สามารถให้บริการแก่หน่วยงานภาครัฐได้อย่างมีประสิทธิภาพและมีคุณภาพเป็นที่ยอมรับในระดับสากล

ความแตกต่างระหว่างก่อนและหลังของการทำ ISO/IEC 27001:2005 : สิ่งที่เห็นได้อย่างชัดเจนอันดับแรก คือ เรื่องของจิตสำนึก (Awareness) ของผู้ปฏิบัติงาน โดย ดร.ศักดิ์ ให้ความสำคัญในเรื่องของ **"คน"** โดยเน้นความสำคัญที่**การสร้างจิตสำนึก (Awareness)** โดยมีการรณรงค์ผ่านรูปแบบจดหมายอิเล็กทรอนิกส์ ป้าย และบอร์ดประชาสัมพันธ์ ร่วมกับการใช้ระยะเวลาในการสร้าง Awareness อีกทั้งได้ยกตัวอย่างการสร้าง Awareness เรื่องกลไกของการปรับปรุงทบทวน ซึ่งจำเป็นต้องคิดให้ละเอียดมากขึ้น การปรับเปลี่ยนจากการบังคับให้ปฏิบัติให้เป็น Practices ที่ต้องปฏิบัติเป็นปกติและพยายามทำให้ผู้ปฏิบัติงานรู้สึกว่าตัวเองเป็นส่วนหนึ่งของการทำงาน นอกจากนี้ ผอ.นันทนา พจนานันทกุล ผู้อำนวยการฝ่ายวิศวกรรมและปฏิบัติการ ได้กล่าวเสริมในอีกประเด็นที่เห็นถึงความเปลี่ยนแปลงได้อย่างเป็นรูปธรรม คือ **เรื่องการบริหารจัดการความเสี่ยง (Risk Management)**

ประโยชน์ที่ได้รับจากการทำ ISO/IEC 27001:2005 : คือ เรื่องการดำเนินธุรกิจได้อย่างต่อเนื่อง **(Business Continuity)** ไม่ว่าจะเป็นการตอบสนองและจัดการกับปัญหาหรือเหตุละเมิดความมั่นคง (Incidents) ต่างๆ ตลอดจน**กระบวนการภายใน** ของ สบทร. ในการดำเนินการเป็น National Root CA ก็มีความพร้อม ความชัดเจน และช่วยให้ขั้นตอนการปฏิบัติงานต่างๆ เป็นไปอย่างรวดเร็วและมีประสิทธิภาพมากขึ้น

Key(s) ของการทำ ISO/IEC 27001:2005 : หัวใจสำคัญของระบบ ISO/IEC 27001:2005 คือ "คน" เนื่องจากเป็นผู้ที่นำองค์กรไปสู่การปรับปรุงการให้บริการและกระบวนการทำงาน และที่สำคัญทุกคนที่มีส่วนเกี่ยวข้องกับการทำงาน **"ต้องมีความเชื่อมั่นในระบบ ISO/IEC 27001:2005 ซึ่งเกิดจากการระดมสมองของทีมงานในการนำข้อกำหนดมาประยุกต์ใช้ทั้งในเชิงเทคนิคและการจัดการ"**

และอีกประการหนึ่งที่จะขาดไปไม่ได้ นั่นก็คือ **Commitment** ของผู้บริหาร ตั้งแต่ คณะกรรมการบริหาร ผู้อำนวยการ จนถึงผู้ปฏิบัติงาน เนื่องจากในการปฏิบัติงานจริงนั้นต้องมีการเชื่อมโยงกระบวนการทำงานเข้าด้วยกัน หรือมีการประสานความร่วมมือกับฝ่ายอื่นๆ ด้วย และที่สำคัญ การดำเนินการเพื่อให้สอดคล้องกับมาตรฐาน ISO/IEC 27001:2005 นั้น จำเป็นต้องได้รับการสนับสนุนงบประมาณการลงทุนอย่างเพียงพอ ทั้งการจัดจ้างที่ปรึกษา การฝึกอบรมผู้ปฏิบัติงาน การจัดหาอุปกรณ์ด้านระบบเทคโนโลยีสารสนเทศ และอื่นๆ

นอกจากนี้ การจัดทำระบบ ISO/IEC 27001:2005 นั้น สบทร. ใช้ระยะเวลาประมาณ 1 ปีในการเตรียมการต่างๆ อาทิ การทำ Gap Analysis และการบริหารจัดการความเสี่ยง (Risk Management) เป็นต้น โดยพิจารณาจากหลักของ CIA (Confidentiality, Integrity, Availability) เพื่อให้สอดคล้องตามข้อกำหนดระบบการจัดการ ISMS (ISO/IEC 27001:2005)

ปัญหาและอุปสรรคของการทำ ISO/IEC 27001:2005 : ระยะเริ่มแรกของการดำเนินการจัดทำระบบนั้น พบ**อุปสรรคด้านระบบเอกสารและบันทึก** เนื่องจากการจัดทำระบบ ISO/IEC 27001:2005 นั้น สบทร. ขอการรับรองเฉพาะส่วนงานที่ดูแลเรื่อง CA เท่านั้น แต่ในการปฏิบัติงานจริงนั้น พบว่า เอกสารและบันทึกบางส่วนมีความเชื่อมโยงกับส่วนงานอื่น จำเป็นต้องขอความร่วมมือจากฝ่ายอื่นๆ ด้วยในการดำเนินการ แต่ด้วยความมุ่งมั่นของผู้บริหารและทีมงาน ISO/IEC 27001:2005 ได้แก้ไขปัญหาดังกล่าวโดยการเริ่มต้นการจัดทำเอกสารก่อน จากนั้น จึงค่อยแจกจ่ายไปยังฝ่ายอื่นๆ ที่เกี่ยวข้อง เพื่อให้เกิดบันทึกต่อไป และพยายามทำให้กลมกลืนไปกับการปฏิบัติงานของฝ่ายต่างๆ ที่เกี่ยวข้อง ซึ่งช่วยให้ผู้ปฏิบัติงานในฝ่ายอื่นเกิดความสะดวกในการปรับตัวต่อการปฏิบัติตามเอกสารดังกล่าว

BEST PRACTICE: สบทร. **ใช้กลไกของฝ่ายบริหาร**ในการเข้ามามีส่วนร่วม และกำหนดแนวทาง/วิธีการดำเนินการแก้ไขปัญหาที่พบผ่านการระดมความคิดเห็นในการประชุมฝ่ายบริหาร และการประชุมคณะกรรมการกำกับและดูแล (Steering Committee) เนื่องจากลักษณะของการทำงานนั้น มีความเกี่ยวข้องกับหลายฝ่าย แต่ทั้งนี้ ผู้ปฏิบัติงานสามารถนำเสนอประเด็นปัญหาเข้าที่ประชุมได้

การตั้ง Core Team ที่ดี ก็เป็นสิ่งสำคัญของแต่ละองค์กร สำหรับ Core Team ของ สบทร. นั้น ประกอบด้วย พนักงานและผู้จัดการส่วนงานที่อยู่ภายใต้ขอบเขตการจัดทำระบบ ซึ่งรวมไปถึงส่วนงานอื่นๆ ที่เกี่ยวข้อง อาทิเช่น ส่วนบริหารงานบุคคล และนิติกร ซึ่ง Core Team ต้องศึกษาทำความเข้าใจกับข้อกำหนดมาตรฐานอย่างละเอียด

ทั้งนี้ ดร.ศักดิ์ ได้แนะนำเพิ่มเติมว่า**การไปเยี่ยมชมดูงาน** หรือตัวอย่างการดำเนินงานขององค์กรอื่นที่มีการจัดทำระบบแล้ว จะสามารถช่วยให้เห็นภาพการดำเนินการอย่างชัดเจนและเป็นรูปธรรมได้ดีกว่าการจัดจ้างที่ปรึกษาเข้ามาช่วยดำเนินการ ซึ่งสำหรับ Core Team ของ สบทร. นั้น ได้ทำการศึกษาแนวทางปฏิบัติที่ดีที่เกี่ยวข้องของหน่วยงานต่างประเทศอื่นๆ เพิ่มเติม แล้วนำมาประยุกต์ให้เข้ากับลักษณะการทำงานของ สบทร.

และจากสิ่งต่างๆ เหล่านี้ ก็จะสามารถช่วยให้ Core Team และผู้ปฏิบัติงานเกิดความเข้าใจได้ว่า "Security" นั้นมีความสำคัญและจำเป็นกับการจัดทำระบบ ISO ขององค์กรอย่างไร สิ่งสำคัญที่ขาดไม่ได้อีกประการ คือ **การสื่อสาร** โดยเฉพาะการสื่อสารภายในองค์กรเพื่อสร้างความเข้าใจและกระตุ้น Awareness ของผู้ปฏิบัติงาน

สำหรับ**การนำระบบไปใช้งาน (Implement)** ระบบ ISO/IEC 27001:2005 นั้น สบทร. ยึดตามแนวทางที่ได้ทำ**การประเมินความเสี่ยง (Risk Assessment)** ขององค์กรว่ามีความเสี่ยงในแต่ละกระบวนการ/กิจกรรมการบริการมีอะไรบ้าง และแต่ละความเสี่ยงนั้นๆ อยู่ในระดับใด โดยความเสี่ยงใดที่ประเมินแล้วพบว่าอยู่ในระดับที่ยอมรับได้ ก็ไม่ต้องมีการแก้ไขความเสี่ยงนั้น

นอกจากนี้ การจัดเก็บเอกสารในระบบ ISO/IEC 27001:2005 อ้างอิงตาม ISO 9001 โดยมีการจัดทำในรูปแบบอิเล็กทรอนิกส์ เพื่อช่วยลดจำนวนของเอกสารที่ต้องจัดเก็บ และมีการกำหนดลำดับขั้นและสิทธิ์ในการเข้าถึงเอกสาร

มุมมองต่อวงการ IT ประเทศไทย:

ดร.ศักดิ์ กล่าวว่าในอดีต **โครงสร้างพื้นฐาน** (Infrastructure) ต่างๆ ด้านเทคโนโลยีสารสนเทศของประเทศไทยยังไม่พร้อม แต่ปัจจุบัน ความพร้อมทางด้านโครงสร้างพื้นฐานได้รับการพัฒนา ตลอดจนได้รับงบประมาณสนับสนุนจากหน่วยงานภาครัฐมากขึ้น แต่อย่างไรก็ตาม **ขีดจำกัดด้านจำนวนบุคลากรในวงการ IT** ไม่เพียงพอ ยังคงมีความต้องการบุคลากร/ผู้เชี่ยวชาญที่มีความรู้ความสามารถในการควบคุมการดำเนินการทั้งนี้ เนื่องจากระบบการจัดการได้เข้ามามีบทบาทในกระบวนการภายในขององค์กรต่างๆ มากขึ้น อาทิเช่น โครงการ Mega-Projects รถไฟฟ้าสายต่างๆ ก็จำเป็นต้องมีบุคลากรที่มีความเชี่ยวชาญด้าน IT เข้าไปควบคุมกระบวนการ หรือแม้กระทั่งด้านการจัดการพลังงาน เช่น การนำระบบ Mobile Office ระบบการจัดการ IT เข้ามาประยุกต์ใช้ร่วมกับการทำงาน ก็จะสามารถช่วยลดปริมาณการใช้พลังงานลงได้เช่นเดียวกัน

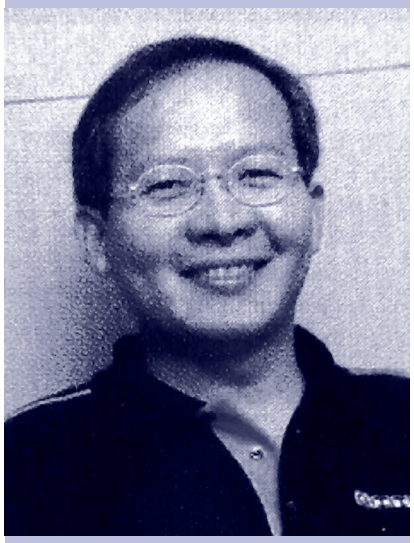
นอกจากนี้ **ทัศนคติของการทำงานเป็นทีม** เป็นสิ่งสำคัญต่อการดำเนินงาน เพื่อเสริมประสิทธิภาพการทำงาน รวมทั้ง**การจัดการ การทำงาน** เนื่องจากปัจจุบัน **เทคโนโลยีไร้สาย (Wireless)** ได้กลายเป็นปัจจัยสำคัญอันดับต้นๆ ของการทำงาน **ซึ่งการรักษาความมั่นคงปลอดภัย (Security)** ของข้อมูลก็ยิ่งต้องมีประสิทธิภาพที่ดีสอดคล้องตามกัน โดยเฉพาะความสำคัญ**เรื่องการจัดการความเสี่ยง** และเรื่องของ **ความเป็นส่วนตัว (Privacy)** ตลอดจนการจัดการ กับเหตุละเมิดความมั่นคง (Incident Management) ในเรื่องการโจมตีหรือการละเมิดความมั่นคงปลอดภัย เพื่อให้องค์กรเกิดความสูญเสียที่ส่งผลกระทบต่อธุรกิจน้อยที่สุด

สำหรับ **การจัดการ Security** ที่ดีเพื่อให้ได้ประสิทธิภาพและประสิทธิผลการดำเนินการนั้น องค์กรต้องจัดการที่กระบวนการ (Process) การทำงาน โดยองค์กรต้องพิจารณาก่อนว่า "SECURITY" ขององค์กรนั้นคืออะไร แล้วจึงดำเนินการ มิใช่รอให้ปัญหาเกิดแล้วจึงค่อยดำเนินการ

การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) เป็นอีกหนึ่งประเด็นที่สำคัญของระบบการรักษาความมั่นคงปลอดภัยของสารสนเทศ องค์กรจึงควรวิเคราะห์ผลกระทบที่ทำให้ธุรกิจหยุดนิ่งไม่สามารถดำเนินการต่อไปได้ ซึ่งการวิเคราะห์ผลกระทบนี้ต้องพิจารณาความเชื่อมโยงกับมูลค่าของการให้บริการ ตลอดจนพิจารณาถึงการบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity Management: BCM) ด้วย

โดย **"การเรียนลัด"** เช่น การศึกษาแนวทางปฏิบัติขององค์กรอื่น หรือการศึกษาดูงาน สามารถช่วยให้องค์กรนั้นๆ พร้อมสู่การพัฒนา ได้อย่างรวดเร็วและมีประสิทธิภาพมากกว่าการเริ่มต้นจากศูนย์

สุดท้ายนี้ ดร.ศักดิ์ ได้ให้ข้อคิดเตือนใจ...ประชาชนชาวไทยควรน้อมนำกระแส**พระราชดำรัสของพระบาทสมเด็จพระเจ้าอยู่หัวในเรื่องของ "เศรษฐกิจพอเพียง"** เข้ามาประยุกต์ใช้ให้เข้ากับทั้งการทำงานและการดำเนินชีวิตประจำวัน



ขอขอบพระคุณ ดร.ศักดิ์ เสกขุนทด (ผู้อำนวยการสำนักบริการเทคโนโลยีสารสนเทศภาครัฐ) ผอ.นันทนา พจนานันทกุล (ผู้อำนวยการฝ่ายวิศวกรรมและปฏิบัติการ) และคุณสันต์ทศน์ สุริยันต์ (ผู้จัดการส่วนปฏิบัติการ PKI) ในการเอื้อเฟื้อข้อมูลและเปิดโอกาสให้ทีมงานเข้าสัมภาษณ์มา ณ โอกาสนี้

การบริหารจัดการผู้ส่งมอบ – ข้อกำหนดที่ 7.3

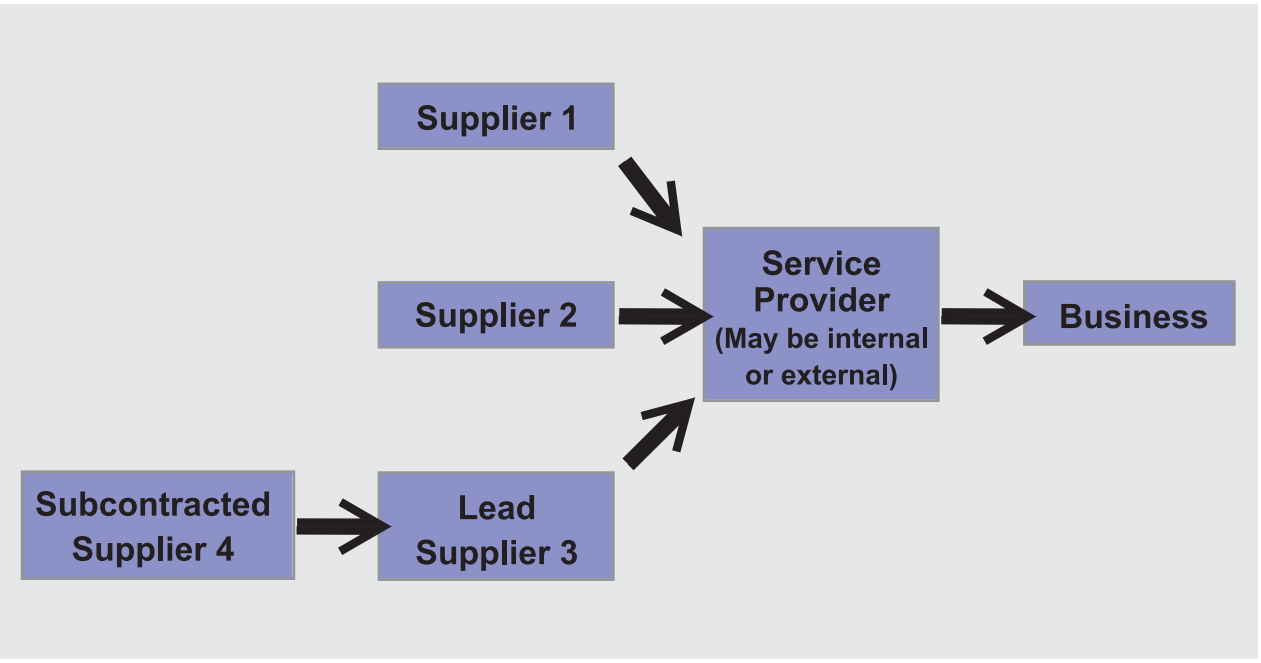
Supplier management

(ISO/IEC 20000–1)

"ข้อกำหนดที่ 7.3 การบริหารจัดการผู้ส่งมอบ (Supplier management)" ตามมาตรฐาน ISO/IEC 20000-1:2005 Information technology – Service management – Part 1: Specification มีวัตถุประสงค์เพื่อบริหารจัดการผู้ส่งมอบ เพื่อให้มั่นใจได้ว่าคุณภาพการให้บริการเป็นไปตามข้อกำหนด

ขอบข่ายของมาตรฐานนี้ ไม่รวมถึงการจัดจ้างของผู้ส่งมอบ

ผู้ให้บริการ (Service providers) อาจมีการมอบหมายการดำเนินการหรือมีการใช้บริการบางส่วนจากผู้ส่งมอบ (Suppliers) แต่ทั้งนี้ ผู้ให้บริการต้องแสดงความสอดคล้องของกระบวนการบริหารจัดการผู้ส่งมอบ



แผนภาพ: ตัวอย่างความสัมพันธ์ระหว่างผู้ให้บริการ (Service providers) และผู้ส่งมอบ (Suppliers)

จากแผนภาพแสดงตัวอย่างความสัมพันธ์ระหว่างผู้ใช้บริการ/ลูกค้า (Business) ผู้ให้บริการ (Service Provider) และผู้ส่งมอบ พบว่า องค์กรที่ให้บริการแห่งหนึ่งมีผู้ส่งมอบที่เกี่ยวข้องกับการบริหารจัดการสารสนเทศจำนวนทั้งสิ้น 3 ราย ประกอบด้วยผู้ส่งมอบที่ 1 ผู้ส่งมอบที่ 2 และผู้ส่งมอบที่ 3 ซึ่งผู้ส่งมอบที่ 3 (Lead Supplier 3) มีการมอบหมายงานบางส่วนให้แก่ผู้รับเหมาช่วงที่ 4 (Subcontracted Supplier 4) ดำเนินการแทน

ประเด็นสำคัญของข้อกำหนดนี้ก็คือ องค์กรผู้ให้บริการ**ต้องจัดทำเอกสารกระบวนการบริหารจัดการผู้ส่งมอบ** (Documented supplier management processes) และสัญญาการบริการ โดยในสัญญาการบริการที่จัดทำขึ้นนี้ ต้องระบุชื่อผู้รับผิดชอบของแต่ละผู้ส่งมอบ ทั้งนี้ เพื่อเป็นข้อตกลงการบริการระหว่างผู้ให้บริการ (Service Provider) และผู้ส่งมอบ (Supplier)

ข้อกำหนด ขอบข่าย ระดับการให้บริการ และกระบวนการสื่อสารที่ผู้ส่งมอบต้องดำเนินการปฏิบัตินั้น **ต้องจัดทำเป็นเอกสารข้อตกลงระดับการให้บริการ** (Service Level Agreements: SLAs ตามข้อกำหนดที่ 6.1 การบริหารจัดการระดับการให้บริการ) หรือเอกสารอื่นๆ และต้องได้รับความเห็นพ้องตรงกันจากผู้เกี่ยวข้อง โดย SLAs ที่องค์กรทำกับผู้ส่งมอบต้องเป็นไปในแนวทางเดียวกัน หรือไม่ขัดแย้งกับ SLAs ที่องค์กรทำกับผู้ใช้บริการ/ลูกค้า นอกจากนี้ ความ

เชื่อมต่อของการปฏิบัติงานระหว่างกระบวนการต่างๆ องค์กรต้องจัดทำเป็นเอกสารและต้องได้รับความเห็นชอบจากผู้มีส่วนเกี่ยวข้องด้วย

บทบาทหน้าที่และความรับผิดชอบระหว่างผู้ส่งมอบ Lead (จากแผนภาพ ได้แก่ Lead Supplier 3) และผู้รับเหมาช่วง (Subcontracted Supplier 4) **ต้องจัดทำเป็นเอกสาร** โดยผู้ส่งมอบ Lead ต้องมีการแสดงกระบวนการปฏิบัติงานที่ชัดเจน เพื่อให้มั่นใจว่าผู้รับเหมาช่วงมีการดำเนินการสอดคล้องและเป็นไปตามที่ระบุไว้ในข้อตกลงระดับการให้บริการ/สัญญา ทั้งนี้ องค์กร**ต้องมีการทบทวนข้อตกลงสัญญาการให้บริการอย่างน้อยปีละ 1 ครั้ง** เพื่อให้มั่นใจว่ายังคงมีความเหมาะสม เพียงพอ และมีประสิทธิผลเป็นไปตามข้อตกลง

การเปลี่ยนแปลงใดๆ ที่เกี่ยวข้องกับสัญญาการให้บริการ และ SLAs ต้องเป็นไปตามผลการทบทวนตามความเหมาะสม หรือตามระยะเวลาที่เหมาะสม **โดยการเปลี่ยนแปลงต้องดำเนินการตามระบบกระบวนการบริหารจัดการความเปลี่ยนแปลง** (Change management process)

ตัวอย่าง: 3 ขั้นตอนของระบบการบริหารจัดการความเปลี่ยนแปลง (Three-step system approach to change management) ประกอบด้วย

ขั้นตอนที่ 1: การชี้บ่งสิ่งที่ต้องการเปลี่ยนแปลง (Identify the task) ประกอบด้วย

- **การกำหนดสิ่งที่ต้องการบริหารจัดการความเปลี่ยนแปลงว่า คืออะไร (Define "What is change management?")** โดยความเปลี่ยนแปลงนั้น อาจเป็นการเปลี่ยนแปลงไป - มาได้ เป็นเพียงการคาดการณ์ทำนาย หรือเป็นการเปลี่ยนแปลงร่วมกับการเปลี่ยนแปลงอื่นๆ ก็ได้

ความเปลี่ยนแปลง มี 2 ประเภทหลักๆ ได้แก่

- **การเปลี่ยนแปลงและการควบคุมภายในโดยองค์กร** เช่น การนำอุปกรณ์เครื่องมือใหม่เข้ามาใช้ในระบบสารสนเทศ การติดตั้งหรือการเปลี่ยนแปลงอาคาร/โครงสร้าง การเปลี่ยนแปลงขั้นตอนการปฏิบัติงาน ระบบการควบคุม เป็นต้น
- **การเปลี่ยนแปลงภายนอกที่อยู่นอกเหนือความควบคุมขององค์กร** เช่น การเปลี่ยนแปลงกฎหมาย การดำเนินการของคู่แข่ง การเปลี่ยนแปลงทางเศรษฐกิจ เป็นต้น (แต่เป็นสิ่งที่องค์กรต้องการที่จะควบคุมให้ได้)

- ผู้ปฏิบัติงานภายใต้การควบคุมขององค์กรต้องมี ความมุ่งมั่น **(Commitment)** ในการดำเนินการเพื่อให้เกิดโอกาสสำหรับการปรับปรุงเปลี่ยนแปลง เนื่องจากช่วงของการเปลี่ยนแปลงใดๆ มักประสบพบเจอกับปัญหาและอุปสรรคมากมาย
- **ผู้นำ (Leadership)** และทีมงานที่ดีในการดำเนินการ แต่ทั้งนี้ผู้บริหารต้องทำการสื่อสารและให้นโยบายถึงความเปลี่ยนแปลงที่องค์กรต้องการ
- **การฝึกอบรม (Training)**
- **การวิเคราะห์ (Analysis)** ความเปลี่ยนแปลงที่มีการดำเนินการ
- **การบริหารจัดการความเปลี่ยนแปลง** (Change management)
- **เครื่องมือสำหรับการเปลี่ยนแปลง** (Tools for change management) โดยอาจจัดทำเป็นรูปแบบง่ายๆ เช่น Checklist สำหรับการควบคุมการดำเนินการ โดยเริ่มจากการชี้บ่งประเภทของความเปลี่ยนแปลง เพื่อกำหนดวิธีการดำเนินการต่อความเปลี่ยนแปลงที่เหมาะสม การกำหนดหน้าที่ความรับผิดชอบ เป้าหมาย และวันที่ครบกำหนดการดำเนินการ เป็นต้น
- **การวางแผนบริการจัดการความเปลี่ยนแปลง** (Change management planning) ทั้งนี้ องค์กรต้องมีการจัดหาทรัพยากร (ทั้งรูปแบบของทรัพยากรภายในและการทำสัญญาจ้าง) ที่เพียงพอต่อการดำเนินการ ผู้ปฏิบัติงาน/ผู้ทำสัญญาจ้าง งบประมาณ และเทคโนโลยีที่จำเป็น

ขั้นตอนที่ 2: ความมั่นใจในปฏิบัติการบริหารจัดการความเปลี่ยนแปลง (Insure the details of change management implementation) ประกอบด้วย

- **การวางแผนและการดำเนินการเปลี่ยนแปลง** (Plans and requirements "identified" in Step One are implemented.)
- **ระบบเอกสารและการควบคุมบันทึก** - ข้อมูล (Documen tation and control of records and data)
- **บทบาทหน้าที่และความรับผิดชอบ** (Roles and responsibilities)
- **ทรัพยากร** (Resources)
- **การสื่อสาร** (Communication)
- **การควบคุมการปฏิบัติ** (Operational control)
- **การเฝ้าระวังและการวัดผลการดำเนินการ** (Monitoring and performance measurement)
- **การปฏิบัติการแก้ไขและป้องกัน** (Corrective and preventive actions)
- **ความรู้ความสามารถ การฝึกอบรม และจิตสำนึก** (Competence, training and awareness)

ขั้นตอนที่ 3: การปรับปรุง (Improvement) โดยกาปรับปรุงขององค์กรนั้น ต้องพิจารณาผลของ:

- **การตรวจติดตามภายใน** (Internal audit)
- **การประชุมทบทวนโดยฝ่ายบริหาร** (Management review)

องค์กรผู้ให้บริการต้องจัดให้มีกระบวนการเพื่อดำเนินการในกรณีที่มีข้อโต้แย้ง และกรณียุติการให้บริการ หรือการโอนย้ายการให้บริการไปยังหน่วยงานอื่นๆ

องค์กรต้องมีการ**เฝ้าระวังและการทบทวนประสิทธิผลการดำเนินการเทียบกับเป้าหมาย** นอกจากนี้ องค์กรต้องดำเนินการและ**บันทึกผลการชี้บ่งการปรับปรุงกระบวนการต่างๆ เพื่อใช้เป็นข้อมูลสำหรับการวางแผนปรับปรุงการให้บริการ**ขององค์กร

อ้างอิง

- ISO/IEC 20000-1:2005 Information technology -- Service management -- Part 1: Specification
- ISO Management Systems: March - April 2007, Vol. 7, No. 2, pp. 15-18

...A refreshing break from the city... ฝ่ายหน่วยตรวจ สรอ. จัดสัมมนาทบทวนความรู้ผู้ตรวจ - เจ้าหน้าที่ และเตรียมความพร้อมรองรับการตรวจ มอก. บรรยากาศริมหาดชะอำ จ.เพชรบุรี

...Promote customer relationship - Seminar in Chiang Mai... สรอ. จัดสัมมนาให้ความรู้แก่ลูกค้าเกี่ยวกับข้อกำหนด ISO/DIS 9001 และ OHSAS 18001 ณ โรงแรมอิมพีเรียล แม่ปิง จ.เชียงใหม่

Management System Certification Institute (Thailand) - MASCI
1025, 11th Floor, Yakult Building, Phaholyothin Road, Samsen-Nai Phyathai, Bangkok 10400, Thailand

Contact: Saowanee (Phai) Tel. 02-617-1727 Fax. 02-617-1708
E-mail: ibd@masci.or.th
Visit our website: www.masci.or.th