การกำหนดมาตรฐานด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล ได้แก่ มาตรฐานข้อมูล มาตรฐานรหัสข้อมูล มาตรฐานการปฏิบัติงาน มาตรฐานความปลอดภัยและความลับของผู้ป่วย มาตรฐานระบบเครือข่ายคอมพิวเตอร์ มาตรฐานทางกายภาพและสภาพแวดล้อม

โรงพยาบาลถลาง อ.ถลาง จ.ภูเก็ต

การกำหนดมาตรฐานด้านเทคโนโลยีสารสนเทศต่างๆ

ความเป็นมา

การพัฒนาคุณภาพโรงพยาบาลในประเทศไทยได้เริ่มดำเนินการมาเป็นเวลานานพอสมควรแล้ว และเทคโนโลยีสารสนเทศโรงพยาบาลเป็นส่วนหนึ่งที่ช่วยให้คุณภาพการดูแลผู้ป่วยมีประสิทธิภาพยิ่งขึ้น อย่างไรก็ดีหากการจัดการระบบเทคโนโลยีสารสนเทศโรงพยาบาลขาดมาตรฐานที่เหมาะสม ย่อมเป็นความเสี่ยงที่จะทำให้ผู้ป่วยได้รับอันตราย

ในมาตรฐานโรงพยาบาล และบริการสุขภาพของสถาบันพัฒนาและรับรองคุณภาพโรงพยาบาล แต่เดิม ได้กล่าวถึงเรื่องมาตรฐานด้านเทคโนโลยีสารสนเทศโรงพยาบาลไว้อย่างกว้างๆ แต่ในปัจจุบัน การใช้เทคโนโลยีสารสนเทศมีความซับซ้อนยิ่งขึ้น ซึ่งทำให้เกิดทั้ง โอกาสใหม่ๆ และเกิดความเสี่ยงใหม่ๆ ด้านเทคโนโลยีสารสนเทศเป็นอย่างมาก ดังนั้น สถาบันพัฒนาและรับรองคุณภาพโรงพยาบาลจึงปรึกษาสมาคมเวชสารสนเทศไทย (TMI) ให้ช่วยพัฒนามาตรฐาน-คุณภาพในด้านเทคโนโลยีสารสนเทศโรงพยาบาลขึ้น เพื่อใช้เป็นแนวทางในการพัฒนา และรับรองคุณภาพโรงพยาบาลต่อไป

TMI ได้ตั้ง คณะทำงานขึ้น ศึกษา และดำเนินการในเรื่องนี้ ตกลงเริ่มจากการพัฒนามาตรฐานเทคโนโลยีเทคโนโลยีสารสนเทศที่เหมาะสมร่วมกันเป็นอันดับแรก โดยกระบวนการดังนี้

คณะทำงานศึกษาเอกสารที่เกี่ยวข้องกับมาตรฐาน Hospital Accreditation (HA) และมาตรฐานการจัดการสากลด้าน IT ก่อนการประชุม ได้แก่

- มาตรฐานโรงพยาบาลและบริการสุขภาพ ฉบับเฉลิมพระเกียรติฉลองสิริราชสมบัติครบ 60 ปี พ.ศ.2549
- SPA (Standards Practice Assessment) สถาบันพัฒนาและรับรองคุณภาพโรงพยาบาล
- มาตรฐาน JCI (Joint Commission International)
- Baldrige National Quality Program 2009 – 2010
- มาตรฐาน CoBIT (Control Objectives for Information and related Technology)
- มาตรฐาน ITIL (Information Technology Infrastructure Library)
- มาตรฐาน ISO/IEC 27002

คณะทำงานเสนอให้ร่าง มาตรฐานเทคโนโลยีสารสนเทศโรงพยาบาล (Hospital Information Technology) เพื่อเป็นแนวทางให้โรงพยาบาลในประเทศไทยพัฒนาเทคโนโลยีสารสนเทศในองค์กรเพื่อสนับสนุนการพัฒนาคุณภาพโรงพยาบาล (HA) เพิ่มเติมจากมาตรฐานโรงพยาบาลและบริการสุขภาพ ของสถาบันพัฒนาและรับรองคุณภาพโรงพยาบาล

เนื่องจาก Information System (IS) กับ Information Technology (IT) มีความสัมพันธ์ใกล้ชิด

กันมากจนบางครั้ง แยกออกจากกันยาก การศึกษาแนวทางการดำเนินงาน (guideline) ของทั้ง สองระบบจึงคาบเกี่ยวกัน อย่างไรก็ตามทั้ง สองระบบก็มีมิติที่มีข้อพิจารณาเฉพาะระบบแยกจากกัน ดังนั่น ในร่างแรกจะเน้นการบริหารจัดการงานบริการเทคโนโลยีสารสนเทศก่อน หลังจากนั่น แล้วจะพัฒนาบูรณาการกับ ระบบข้อมูลสารสนเทศ (Information System) เป็นภาพรวมของระบบสารสนเทศโรงพยาบาล (Hospital Information Systems)

ร่างแนวทาง(Guideline) ที่เสนอใช้กรอบแนวคิด (Framework) ที่บูรณาการ CobIT (Control Objectives for Information and related Technology) , ITIL (Information Technology Infrastructure Library), ISO 27002 (ISO 17799 เดิม)(ISO 27799 for healthcare) ตามการศึกษาของ Angeli Hoekstra & Nicolette Conradie จาก Price Water House Cooper (2002) ร่วมกับแนวทางการเขียนมาตรฐานของ Joint Commission International (JCI)

กรอบแนวคิดนี้ ได้ผ่านการทดสอบและนำไปใช้เบื้องต้นในการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศของโรงพยาบาลนำร่องในโครงการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศของสมาคมเวชสารสนเทศไทย จำนวน 13 โรงพยาบาล ปัจจุบันเป็น version 1.1

คณะทำงานตกลงร่วมกันที่จะใช้ CobIT, ITIL และ ISO 17799 เป็น framework หลักของการพัฒนามาตรฐานเทคโนโลยีสารสนเทศโรงพยาบาล เนื่องจากเป็นมาตรฐานที่เป็นที่ยอมรับ และครอบคลุมการทำงานของโรงพยาบาลได้เป็นอย่างดี คณะทำงานตระหนักดีว่า โรงพยาบาลในประเทศไทยมีความพร้อมในการพัฒนาคุณภาพในด้านนี้ไม่เท่ากัน อันเนื่องมาจากบุคลากร งบประมาณ และการบริหารจัดการอื่นๆ หากนำเอามาตรฐานทั้ง หมดของต่างประเทศมาใช้ทันที จะมีโรงพยาบาลจำนวนมากประสบปัญหา คณะทำงานจึงได้ปรับมาตรฐานให้มีความยืดหยุ่นแต่มีความท้าทาย เพื่อเป็นการกระตุ้นการพัฒนาต่อไปในอนาคต

1. โครงสร้าง และ บทบาท (Structure and Role)

โรงพยาบาลมีการจัดให้มีกำหนดเป้าหมาย นโยบาย แผนงาน และโครงสร้างหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศที่ความชัดเจน รวมทั้ง มีอัตรากำลังบุคลากรที่ทำงานด้านเทคโนโลยีสารสนเทศ เพื่อให้แน่ใจได้ว่า ระบบเทคโนโลยีสารสนเทศโรงพยาบาลจะสามารถตอบสนองการดูแลผู้ป่วยได้อย่างต่อเนื่องปลอดภัย และเกิดประโยชน์สูงสุด โดยควรมีการดำเนินการในสิ่งต่อไปนี้

1.1. จัดให้มีทีมดูแลด้านระบบสารสนเทศของโรงพยาบาล ประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศของโรงพยาบาลและผู้ใช้งานระบบร่วมกำหนดทิศทาง วางแผน จัดการ และติดตาม การดำเนินงานด้านเทคโนโลยีสารสนเทศ ที่ครอบคลุมระบบอภิบาลเทคโนโลยีสารสนเทศ (IT Governance) และระบบบริหารจัดการเทคโนโลยีสารสนเทศ (IT Management)

1.2. จัดให้มีแผนแม่บทเทคโนโลยีสารสนเทศ (IT Master Plan) ของโรงพยาบาล การจัดทำแผนแม่บทหรือแผนยุทธศาสตร์เทคโนโลยีสารสนเทศโรงพยาบาล โดยกำหนด เป้าหมาย และแนวทางการพัฒนาและใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน การจัดทำแผนฯ จัดทำโดยการมีส่วนร่วมของบุคลากรที่เกี่ยวข้องทั้งผู้บริหารและผู้ปฏิบัติซึ่งเป็นผู้ใช้งานระบบเทคโนโลยีสารสนเทศในด้านต่างๆ เพื่อให้แผนแม่บทมีความสอดคล้องกับวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ และเข็มมุ่งของโรงพยาบาล และตอบสนองต่อความต้องการของผู้ปฏิบัติงานในการดูแลผู้ป่วย/บริการสุขภาพให้มีคุณภาพยิ่งขึ้น มีการสื่อสารแผนแม่บทให้ผู้เกี่ยวข้องรับทราบ และดำเนินการในแนวเดียวกัน มีการ ตรวจสอบ การติดตามประเมินผลการดำเนินการตามแผน และนำผลการประเมินมาปรับแผนให้ดีขึ้น

1.3. มีนโยบายและแนวทางปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล มีการกำหนดนโยบาย และแนวทางปฏิบัติด้านเทคโนโลยีสารสนเทศที่ชัดเจน ครอบคลุม นโยบายด้านความครบถ้วนถูกต้องของข้อมูล ความปลอดภัยของระบบ การรักษาความลับของ ผู้ป่วย การเก็บสารสนเทศต่างๆ ระยะเวลาในการเก็บข้อมูลผู้ป่วย ข้อมูลดิบและสารสนเทศ การทำลายข้อมูลดิบและสารสนเทศด้วยความเหมาะสม และนโยบายกำกับดูแล ติดตามการดำเนินงานด้านเทคโนโลยีสารสนเทศ

มีการสื่อสารนโยบายด้านเทคโนโลยีสารสนเทศของโรงพยาบาลให้ผู้เกี่ยวข้องรับทราบและดำเนินการในแนวเดียวกัน

1.4. จัดโครงสร้าง และอัตรากำลังของหน่วยงานเทคโนโลยีสารสนเทศโรงพยาบาลที่เหมาะสม โรงพยาบาลมีการจัดโครงสร้างให้มีหน่วยงานที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ รวมทั้ง กำหนดตำแหน่ง อัตรากำลังและสายการบังคับบัญชา และอำนาจหน้าที่ ที่ชัดเจนและเหมาะสม เพื่อให้สามารถดำเนินการด้านเทคโนโลยีสารสนเทศให้สามารถสนับสนุนงานตาม บริบทของโรงพยาบาลได้อย่างมีประสิทธิภาพ

1.5. มีการกำหนดมาตรฐานด้านเทคโนโลยีสารสนเทศต่างๆที่จำเป็น สอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล ได้แก่ มาตรฐานข้อมูล มาตรฐานรหัสข้อมูล (ซึ่งรวมถึง รหัสโรค รหัสผ่าตัด สัญลักษณ์ ตัวย่อ คำจำกัดความ) มาตรฐานการปฏิบัติงาน มาตรฐานด้านความ ปลอดภัยและความลับผู้ป่วย มาตรฐานระบบเครือข่ายคอมพิวเตอร์ มาตรฐานทางกายภาพและ สภาพแวดล้อม

1.6. มีการตอบสนองความต้องการของผู้ใช้ระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม มีการสำรวจความต้องการสารสนเทศของผู้ปฏิบัติงาน หัวหน้าหน่วยงาน และผู้บริหารโรงพยาบาล และจัดระบบเทคโนโลยีสารสนเทศให้ตอบสนองความต้องการของผู้ใช้ มีการคำนึงถึงบริบทของโรงพยาบาล โดยนำสารสนเทศมาช่วยในการพัฒนาการบริการให้มีความถูกต้อง ปลอดภัย มีประสิทธิภาพ สะดวก รวดเร็ว รวมทั้ง นำสารสนเทศมาช่วยสนับสนุนการ ตัดสินใจของผู้บริหารในการบริหารจัดการ ตลอดจนการศึกษาวิจัย ตอบสนองต่อภารกิจและพันธกิจทุกด้านของโรงพยาบาล

2. เทคโนโลยี (Technology)

การเลือกใช้เทคโนโลยีที่เหมาะสม จัดให้มีการใช้เทคโนโลยีอย่างเป็นระบบ มีความสำคัญยิ่งต่อการพัฒนาเทคโนโลยีสารสนเทศโรงพยาบาล ซึ่งนับว่าเป็นหัวใจของการใช้งานอย่างคุ้มค่า สะดวก ปลอดภัย อย่างไรก็ดีเทคโนโลยีสารสนเทศมาพร้อมกับความเสี่ยง ซึ่งรวมทั้ง การสะดุดหยุดลงของงาน การสูญเสียข้อมูลที่สำคัญทั้งโดยบังเอิญ จากความผิดพลาดของระบบ และการจงใจจากผู้ประสงค์ร้าย รวมทั้งการถูกล้วงความลับข้อมูลของโรงพยาบาลโดยผู้ไม่มีสิทธิ จึงจำเป็นต้องมีการจัดการเทคโนโลยีอย่างเหมาะสม เพื่อลดความเสี่ยงที่ อาจเกิดขึ้น ให้น้อยที่สุด

โรงพยาบาลจำเป็นต้องมีการจัดการด้านเทคโนโลยีดังต่อไปนี้

2.1. จัดให้มี Data center

Data center ของโรงพยาบาล ได้แก่ที่ตั้ง ของ servers และอุปกรณ์ที่เกี่ยวข้อง เช่น ระบบสำรองข้อมูล อุปกรณ์สำรอง redundant system ระบบรักษาความปลอดภัย เป็นต้น data

center นี้ต้องมีการจัดการอย่างเหมาะสม เพื่อให้แน่ใจได้ว่า จะสามารถใช้งานระบบได้อย่าง ปลอดภัย ปราศจากการหยุด หรือสะดุดของระบบ ซึ่ง ต้องคำนึงถึงสิ่งต่อไปนี้

1) ห้อง สถานที่ และสิ่งแวดล้อม ต้องจัดให้มีความปลอดภัย เช่น มีการปรับอากาศที่ดี รักษาความปลอดภัยจากบุคคลภายนอก

2) มีระบบป้องกันการเสียหายของข้อมูลและระบบ (data integrity and fault tolerance) ซึ่งรวมถึง UPS และระบบไฟฟ้าสำรอง, ระบบ RAID, redundant power supply และ redundant servers

3) มีระบบสำรองข้อมูล ทั้งภายใน และภายนอก data center

4) มีการจัดการ network ที่เหมาะสม

2.2. มีการกลั่นกรอง/เลือกใช้ Technology อย่างเหมาะสม

มีการวิเคราะห์ความเหมาะสม คำนึงถึงประโยชน์ มาตรฐาน ความเสี่ยง และความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และการเลือก software ที่เหมาะสม กับเป้าหมาย สอดคล้องกับบริบท และแผนแม่บทเทคโนโลยีสารสนเทศของโรงพยาบาล

มีการทบทวนความก้าวหน้าเทคโนโลยีสารสนเทศทางการแพทย์อย่างสม่ำเสมอเพื่อนำมาพัฒนาและปรับปรุงระบบเทคโนโลยีสารสนเทศให้เกิดประโยชน์สูงสุด

2.3. จัดเทคโนโลยีสำหรับการรักษาความมั่นคงปลอดภัยและคุ้มครองความลับข้อมูลส่วนบุคคล และการเข้าถึงข้อมูลผู้ป่วยความเป็นส่วนตัวของผู้ป่วยเป็นสิ่งสำคัญ ซึ่งเป็นความเสี่ยงอย่างหนึ่งจากการใช้ เทคโนโลยี จำเป็นต้องจัดการให้มีระบบที่ป้องกันผู้ไม่ได้รับอนุญาตเข้าถึงข้อมูลของผู้ป่วย ดังนี้

1) ระบบมีบัญชีรายชื่อผู้ใช้งาน และรหัสผ่าน (username and password) และกลไกการ ยืนยันตัวบุคคล

2) สร้างระบบการเข้าถึงข้อมูลผู้ป่วยให้รัดกุม (ใคร สามารถเข้าถึงข้อมูลส่วนไหน ด้วยวิธีใด เป็นต้น)

3) สามารถระบุตัวบุคคลผู้เข้าถึงข้อมูล ผู้นำข้อมูลผู้รับบริการเข้าสู่ระบบ ผู้ที่แก้ไขข้อมูล และวันเวลาที่เข้าถึงหรือนำข้อมูลผู้รับบริการเข้าสู่ระบบหรือแก้ไขข้อมูลได้ มีเทคโนโลยีด้านความมั่น คงของระบบเช่น firewall ระบบป้องกันไวรัสและโทรจัน การแยกระบบ internet และระบบงานโรงพยาบาล การจัด private network เป็นต้น

3. บุคลากร (People)

มีการจัดการทรัพยากรบุคคลด้านเทคโนโลยีสารสนเทศ ที่เหมาะสม เพื่อให้การพัฒนาและใช้งานเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ

3.1. มีบุคลากรด้านเทคโนโลยีสารสนเทศที่เพียงพอ โดยมีการกำหนดสมรรถนะที่จำเป็นของแต่ละตำแหน่งอย่างเหมาะสม อันได้แก่

1) Chief Information officer (CIO) ได้แก่บุคลากรระดับบริหารของโรงพยาบาลที่ทำหน้าที่เป็นผู้นำในการบริการด้านเทคโนโลยีสารสนเทศ พัฒนาระบบเทคโนโลยีสารสนเทศ
โรงพยาบาล อยู่ในทีมนำของโรงพยาบาล โดยมีหน้าที่หลักดังนี้กำหนดเป้าหมายการดำเนินงานด้านเทคโนโลยีสารสนเทศของโรงพยาบาล ให้ สอดคล้องกับวิสัยทัศน์ พันธกิจ และเข็มมุ่งของโรงพยาบาล รวมทั้งแนวทางในการนำเทคโนโลยีด้านสารสนเทศที่เหมาะสมมาใช้งาน และการพัฒนาคุณภาพ เทคโนโลยีสารสนเทศให้ได้มาตรฐาน โดยผ่านการเห็นชอบจากทีมนำของ โรงพยาบาล และสอดคล้องกับกฎหมายและข้อบังคับต่างๆ จัดให้มียุทธศาสตร์ แผนงาน โครงการเพื่อบรรลุวัตถุประสงค์ดังกล่าว ควบคุม กำกับ และประเมินผล ให้การดำเนินงานด้านเทคโนโลยีสารสนเทศ
เป็นไปอย่างเหมาะสมและราบรื่น
CIO ควรเป็นผู้ที่มีความรู้/ผ่านการอบรม/ หรือมีประสบการณ์ด้านเทคโนโลยี สารสนเทศอย่างเพียงพอ และติดตามความก้าวหน้าดังกล่าวอย่างสม่ำเสมอ เนื่องจาก ความรู้และพัฒนาการ ทั้ง ในด้านอุปกรณ์ ระบบงาน มาตรฐาน กฎระเบียบและกฎหมายรวมถึงภัยคุกคามด้านเทคโนโลยีสารสนเทศเป็นไปอย่างรวดเร็ว

2) หัวหน้าหน่วยงานเทคโนโลยีสารสนเทศ (Head of IT unit) บริหารจัดการและดูแลการบริการด้านเทคโนโลยีสารสนเทศ (IT service management)2 อย่างเป็นระบบ ประเมิน ความเสี่ยง จัดการป้องกัน ดูแล และแก้ปัญหาต่างๆ ที่เกิดขึ้น ในการดำเนินงาน ติดตาม
การทำงานและปัญหาที่เกิดขึ้น ในด้านเทคโนโลยีสารสนเทศและดำเนินการแก้ไข เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลดำเนินการไปได้อย่างราบรื่นต่อเนื่อง รวมทั้ง
การพัฒนาหน่วยงานเทคโนโลยีสารสนเทศให้มีระดับคุณภาพที่สูงขึ้น
3) บุคลากรอื่นๆ หน่วยงานมีการวิเคราะห์ความจำเป็นด้านบุคลากรเทคโนโลยีสารสนเทศตามบริบทของโรงพยาบาล และจัดให้มีบุคลากรด้านนี้อย่างพอเพียงและเหมาะสม
ตัวอย่างบุคลากรที้จำเป็นเช่น

I. IT technician ผู้ดูแลระบบงานทั่ว ไป เช่นแก้ไขเมื่อคอมพิวเตอร์ หรือเครือข่ายมีปัญหา ติดตั้ง โปรแกรม ดูแลเครื่องแม่ข่าย สำรองข้อมูล เป็นต้น

II. IT security personnel ผู้ดูแลความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

III. IT staffs อื่นๆ เช่น นักพัฒนาระบบ(developer) โปรแกรมเมอร์ วิศวกรด้านคอมพิวเตอร์ เจ้าหน้าที่ Service desk ฯลฯ

IV. Health Information Management officer เช่น เจ้าหน้าที่เวชระเบียน ผู้ดูแลเกี่ยวกับข้อมูล สารสนเทศต่างๆ ที่อยู่ในระบบ ให้มีความถูกต้องเที่ยงตรง

V. Clinical Informatician เป็นผู้ที่มีความรู้ความเข้าใจงานทางคลินิก งานด้านสาธารณสุข และงานด้านเทคโนโลยีสารสนเทศในระดับที่สามารถเป็นตัวเชื่อม การทำงานระหว่างบุคคลากรด้าน IT กับบุคคลากรผู้ให้บริการทางการแพทย์และ สาธารณสุขได้อย่างมีประสิทธิภาพ รวมถึงสามารถนำสนเทศโรงพยาบาลมาประมวลผล และใช้งานให้มีประสิทธิภาพ ทั้ง ด้านการดูแลผู้ป่วย และการบริหารจัดการองค์การ

3.2. มีการประเมินสมรรถนะบุคลากรด้านเทคโนโลยีสารสนเทศและนำผลการประเมินมาพัฒนาบุคลากร เพื่อให้บุคลากรมีความรู้ความสามารถที่จำเป็นต่อการปฏิบัติและพัฒนางานอยู่ตลอดเวลา

3.3. มีกระบวนการในการรักษาบุคลากรไว้ในระบบ และป้องกันความเสี่ยงในการสูญเสียบุคลากรด้านเทคโนโลยีสารสนเทศที่จะไม่ก่อให้เกิดปัญหาร้ายแรงต่อการดำเนินการด้านเทคโนโลยี สารสนเทศอย่างต่อเนื่อง

3.4. มีการพัฒนาผู้ใช้งานระบบเทคโนโลยีสารสนเทศ ผู้ใช้งานระบบเทคโนโลยีสารสนเทศสามารถ ใช้งานได้อย่างถูกต้อง และเป็นไปตามบริบทและนโยบายด้านเทคโนโลยีสารสนเทศขององค์กร ทั้ง ด้านความถูกต้องครบถ้วนของข้อมูล การรักษาความลับของผู้ป่วย และความปลอดภัยของระบบเทคโนโลยีสารสนเทศ การพัฒนานี้รวมถึงผู้บริหารระดับสูงและผู้เกี่ยวข้องได้รับการพัฒนาให้เข้าใจเกี่ยวกับหลักการการจัดการสารสนเทศ (Principles of Information Management) ที่จำเป็น โดยมุ่งเน้นให้เกิดวัฒนธรรมการใช้งานสารสนเทศที่ดี อัตรากำลังของหน่วยงานเทคโนโลยีสารสนเทศโรงพยาบาลนัน อาจมีความยืดหยุ่นได้ เช่นงานบางอย่างด้านเทคโนโลยีสารสนเทศอาจจัดจ้างบุคคลภายนอกดูแล แต่ต้องมีการจัดการที่แน่ใจได้ว่าจะสามารถดำเนินการด้านเทคโนโลยีสารสนเทศได้อย่างราบรื่น ปลอดภัย รวมทั้ง จะไม่กระทบต่อภารกิจหลัก ของโรงพยาบาล และไม่กระทบต่อความลับของผู้ป่วย

4. กระบวนการ (Processes)

มีการออกแบบและการจัดการระบบงาน กระบวนการการให้บริการและสนับสนุนงานด้านเทคโนโลยีสารสนเทศที่ตอบสนองต่อบริบทของโรงพยาบาล เพื่อให้แน่ใจว่าการให้บริการด้านสุขภาพเป็นไปอย่างสม่ำเสมอ ต่อเนื่อง เป็นมาตรฐานเดียวกัน และมีการใช้เทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ ได้แก่

4.1. ระบบสนับสนุนการใช้งานด้านเทคโนโลยีสารสนเทศ

ในโรงพยาบาลควรมีระบบสนับสนุนงานด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม โดยมุ่งเน้นที่ผู้ใช้งานด้านเทคโนโลยีสารสนเทศให้ได้รับความสะดวก ลดข้อผิดพลาด และใช้งานได้ราบรื่นต่อเนื่อง รวมทั้ง การรวบรวม แก้ไขอุบัติการณ์ และปัญหาต่างๆ ที่เกิดขึ้น ในส่วนการสนับสนุนงานด้านเทคโนโลยีสารสนเทศ โรงพยาบาลควรมีกระบวนการบริหารจัดการที่สำคัญคือ

1) มีจุดติดต่อ (contact point) กับหน่วยงานเทคโนโลยีสารสนเทศ เช่น ศูนย์ให้บริการด้านเทคโนโลยีสารสนเทศ (IT Service desk) เพื่อผู้ใช้งานสามารถเข้าถึงได้ง่ายเมื่อมี

อุบัติการณ์ หรือปัญหาเกิดขึ้น รวมทั้ง เป็นช่องทางการสื่อสารกับผู้ใช้งาน เพื่อรับฟังปัญหา อุปสรรค และความต้องการของผู้ใช้งานด้วย

2) มีระบบจัดการอุบัติการณ์ และปัญหาด้านเทคโนโลยีสารสนเทศ (incident and problem management) มีการรวบรวมสถิติและวิเคราะห์ ซึ่ง ครอบคลุม แต่ปัญหาง่ายๆ ที่จัดการได้ ณ จุดเกิดอุบัติการณ์ จนถึงปัญหาที่สลับซับซ้อน รวมถึงมีการวิเคราะห์หาสาเหตุราก (root cause) เพื่อการแก้ไขอย่างถาวร ทั้งนี้เพื่อให้การใช้งานเทคโนโลยีสารสนเทศเป็นไปอย่างราบรื่นหรือเกิดผลกระทบต่อการทำงานน้อยที่สุดหากมีการหยุดชะงัก

3) มีระบบบริหารการเปลี่ยนแปลง (Change Management) การเปลี่ยนแปลงในพื้นฐาน หรือสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศเกิดขึ้นได้ตลอดเวลา ซึ่งอาจเกิดจากปัจจัยภายนอก เช่นการเปลี่ยนแปลงของเทคโนโลยี ความต้องการด้านกฎหมาย ด้านการเงิน ระบบประกัน ฯลฯ หรือปัจจัยภายใน เช่น ข้อตกลง ระดับบริการ (service level agreement) การปรับเปลี่ยนหรือพัฒนาระบบให้ดียิ่งขึ้น รวมทั้ง การปรับปรุง software hardware หรือ network ด้วย ฯลฯ จึงต้องมีการบริหาร จัดการเพื่อให้มั่นใจว่า การเปลี่ยนแปลงที่เกิดขึ้น จะไม่ส่งผลกระทบต่อการทำงานและคุณภาพการบริการ หรือเกิดผลกระทบน้อยที่สุด โดยมีคณะกรรมการเฉพาะเพื่อพิจารณา และอนุมัติการเปลี่ยนแปลง

4.2. มีระบบบริหารจัดการด้านการให้บริการเทคโนโลยีสารสนเทศ จัดให้เกิดระบบข้อมูล สำหรับทุกคนที่เข้ามารับบริการ มีการจัดการข้อมูลผู้รับบริการด้วยระบบที่มีประสิทธิภาพ เพื่อให้ ผู้รับบริการได้รับบริการที่ปลอดภัย ถูกต้อง สะดวกรวดเร็ว และต่อเนื่อง โดยมีการประกัน คุณภาพตามข้อตกลงระดับบริการ (Service Level Agreement-SLA) ของโรงพยาบาล

4.3. มีการจัดการและจัดสรรทรัพยากรที่เพียงพอ เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศ เป็นไปอย่างมีประสิทธิภาพ เหมาะสมกับปริมาณงาน (Capacity Management)

4.4. มีการออกแบบระบบคงทนต่อความผิดพลาด (fault tolerance) มีการบำรุงรักษาอย่างสม่ำเสมอ มีการจัดการเพื่อให้ระบบเทคโนโลยีสารสนเทศดำเนินงานได้อย่างต่อเนื่อง (Availability Management) และสามารถกู้คืนระบบได้แม้จะมีเหตุการณ์ไม่คาดฝันเกิดขึ้น (IT Service Continuity Management) โดยมีการวิเคราะห์และจัดทำแผนสำรองฉุกเฉิน (Business Continuity Plan) และแผนกู้คืนระบบ (Disaster Recovery Plan) รวมทั้ง มีการทบทวนและ ซักซ้อมแผนอย่างสม่ำเสมอ

4.5. มีการจัดการข้อมูล ให้แน่ใจว่า ข้อมูลสำคัญได้รับการบันทึก และจัดเก็บในระบบ อย่างถูกต้องและครบถ้วน ประกอบไปด้วย

1) การบันทึก อาการสำคัญ ประวัติ ผลการตรวจร่างกาย และคำวินิจฉัยโรค ในบัตรผู้ป่วย นอกและ/หรือ เวชระเบียนอิเล็กทรอนิกส์ โดยต้องไม่จัดเก็บรหัส ICD แทนคำวินิจฉัยโรค

2) บันทึกประวัติตรวจร่างกายแรกรับ บันทึกความก้าวหน้า และการสรุปเวชระเบียนเมื่อสิ้น สุดการรักษา (Discharge Summary) ในแฟ้มผู้ป่วยใน

3) รายงานการผ่าตัด ในผู้ป่วยทุกรายที่ได้รับการผ่าตัด

4) การให้รหัส ICD ทั้ง รหัสกลุ่มโรค และรหัสการผ่าตัด

5) การบันทึกเวชระเบียนให้สอดคล้องกับมาตรฐานข้อมูลทางการแพทย์อื่นๆ

5. การควบคุม (Control)

การมีระบบการควบคุมการดำเนินงานด้านเทคโนโลยีสารสนเทศ จะทำให้แน่ใจได้ว่าการดำเนินงานจะเป็นไปตามระบบ และแผนงานที่วางไว้ การควบคุมด้านเทคโนโลยีสารสนเทศถือเป็นส่วนหนึ่ง ของการควบคุมภายในของหน่วยงาน ซึ่ง ประกอบด้วยกลไกที่สำคัญดังนี้

5.1. มีระบบควบคุมทั่วไป (General control) เพื่อให้แน่ใจว่า ระบบสารสนเทศจะสามารถใช้งานได้อย่างถูกต้อง ปลอดภัย การควบคุมทั่ว ไปได้แก่ การควบคุมในกรณีต่อไปนี้

1) สร้างวัฒนธรรมการใช้งานเทคโนโลยีสารสนเทศที่ปลอดภัย และสอดคล้องกับทิศทางขององค์การ

2) การจัดสร้าง/ต่อเติม software ให้เป็นไปอย่างมีประสิทธิภาพ รวมทั้ง กำกับดูแล source code/version ของ software

3) ระบบควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Management) มีกระบวนการควบคุมที่ทำให้แน่ใจได้ว่า ระบบและข้อมูลได้รับการ ปกป้องจากการเข้าถึงหรือโจมตีโดยผู้ไม่ประสงค์ดี การใช้งานที่ไม่ถูกต้องหรือไม่ได้รับ อนุญาต ประกอบไปด้วย

3.1) ความปลอดภัยด้านกายภาพ เช่น มาตรการการเข้าออก data center

3.2) ด้าน software และการใช้งาน เช่น การเลือกใช้ database

3.3) การควบคุมการเข้าถึง (Access Control) การจัดการการเข้าถึงของผู้ใช้งาน (User access anagement) รวมถึงการทำบัญชีรายชื่อผู้ใช้งาน การกำหนดสิทธิผู้ใช้งาน การรักษาความลับรหัสผ่านของผู้ใช้แต่ละบุคคล รวมถึงยืนยันตัวบุคคล (Authentication)

3.4) การควบคุมให้เฉพาะผู้ที่เกี่ยวข้องเท่านั้นสามารถเข้าถึงข้อมูล (Business requirements of access control)

3.5) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

3.6) การควบคุมการเข้าถึงระบบ (System and application access control)

3.7) การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

3.8) การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

3.9) ด้านเครือข่าย เช่น การเชื่อมโยง Internet การป้องกันการบุกรุกเครือข่าย

3.10) การบำรุงรักษาระบบโดยบุคคลภายนอก มีมาตรการควบคุม

3.11) การป้องกันไวรัสในระบบคอมพิวเตอร์ และเครื่องมือแพทย์ (Protection from Malware)

3.12) การใช้ Social Media ในการสื่อสารข้อมูลผู้ป่วย

4) ด้าน hardware/software เมื่อมีการเปลี่ยนแปลงระบบงานเกิดขึ้น เช่น การลงระบบงาน การติดตั้ง โปรแกรมครั้ง ใหม่ ตั้งค่า ระบบ(configuration) การเพิ่มหน่วยความจำใน เครื่องคอมพิวเตอร์ เป็นต้น

5.2. มีระบบควบคุมด้วย application (Application control) เพื่อให้แน่ใจว่า ข้อมูลสารสนเทศที่มีอยู่ในระบบเป็นข้อมูลที่ถูกต้อง ครบถ้วน เชื่อถือได้ ทันเวลา โดยมีระบบควบคุมตรวจสอบ ดังนี้

1) การตรวจสอบความครบถ้วน (completeness check) มีระบบที่ทำให้แน่ใจว่ามีการบันทึกข้อมูลผู้รับบริการทุกรายที่เข้ามารับบริการในโรงพยาบาลอย่างครบถ้วน

2) ข้อมูลผู้รับบริการทุกคนที่มารับบริการ ถูกบันทึกข้อมูลไว้ในระบบอย่างเป็นระบบแบบแผน (input control)

3) การตรวจสอบความถูกต้อง (validity check) มีระบบที่ทำให้แน่ใจว่าข้อมูลต่างๆ ที่นำเข้าระบบสารสนเทศ มีความถูกต้อง เที่ยงตรง รวมทั้ง มีระบบการเรียกดูข้อมูลผู้รับบริการ และตรวจสอบความครบถ้วนของข้อมูลผู้รับบริการอย่างสม่ำเสมอ โดยการเรียกดูแบบสุ่มตัวอย่าง ดำเนินการโดยแพทย์ พยาบาลและผู้เกี่ยวข้องที่มีอำนาจหน้าที่ในการนำ ข้อมูลเข้า หรือเรียกดูข้อมูลได้ การเรียกดูข้อมูลผู้รับบริการเน้นไปที่ความตรงต่อเวลา ความครบถ้วนของข้อมูล การเรียกดูข้อมูลครอบคลุมทั้ง ผู้ที่กำลังรับบริการอยู่และที่ กลับไปแล้ว

4) การระบุเจ้าของข้อมูล (identification) มีการควบคุมที่ทำให้แน่ใจว่า มีการระบุบุคคลได้อย่างชัดเจน ไม่มีข้อมูลซ้ำ (ข้อมูลผู้ป่วย 2 ราย ถูกระบุเป็นคนเดียวกันในระบบ) และข้อมูลที่นำเข้าเป็นของผู้ป่วยรายนั่น จริง

5) การระบุตัวผู้เข้าใช้ระบบ และควบคุมให้ผู้มีสิทธิเท่านั่น ที่เข้าใช้งานระบบได้ตามสิทธิ มีการบันทึกข้อมูลการเข้าใช้งาน

5.3. มีระบบบริหารความเสี่ยงเทคโนโลยีสารสนเทศ (IT risk management) ในด้านต่างๆ ดังนี้

1) ความเสี่ยงต่อความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ (hardware software network data)

2) ความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย

3) ความเสี่ยงต่อความเป็นส่วนตัวของข้อมูลผู้ป่วย

4) ความเสี่ยงในการบริหารโครงการเทคโนโลยีสารสนเทศ (IT Project Management

Failure)

5.4. มีระบบควบคุมคุณภาพข้อมูล ให้แน่ใจว่า ข้อมูลสำคัญที่บันทึก และจัดเก็บไว้ในระบบ มีคุณภาพที่ดีขึ้น อย่างต่อเนื่อง โดยมีกระบวนการประเมินระดับคุณภาพข้อมูลที่สำคัญ ดังนี้

1) คุณภาพการบันทึก อาการสำคัญ ประวัติ ผลการตรวจร่างกาย และคำวินิจฉัยโรค ในบัตรผู้ป่วยนอก และ/หรือ เวชระเบียนอิเล็กทรอนิกส์

2) คุณภาพการบันทึกประวัติตรวจร่างกายแรกรับ บันทึกความก้าวหน้า และการสรุปเวชระเบียนเมื่อสิ้น สุดการรักษา (Discharge Summary) ในแฟ้มผู้ป่วยใน

3) คุณภาพการบันทึกรายงานผ่าตัด ในผู้ป่วยทุกรายที่ ได้รับการผ่าตัด

4) ความถูกต้องของการให้รหัส ICD ทั้ง รหัสกลุ่มโรคและรหัสการผ่าตัด และมีการนำผลการประเมินมาวิเคราะห์เพื□อหาแนวทางปรับปรุงระบบให้ดีขึ้น อย่างต่อเนื่อง

6. การวัด (Metrics)

มีการกำหนดตัวชี้วัด และวัดผลที่สามารถใช้ในการติดตามเฝ้าระวังและตรวจสอบการ ดำเนินงานด้านเทคโนโลยีสารสนเทศของโรงพยาบาล ว่าเป็นไปอย่างถูกต้องเหมาะสมและบรรลุ วัตถุประสงค์ การวัดและประเมินผลควรกระทำในทุกๆหมวดของกรอบการพัฒนา เพื่อลดการใช้ความเห็น ของบุคคลในการตัดสินใจ การวัดที่สำคัญ ได้แก่

6.1. วัดและติดตาม กระบวนการทำงานด้านเทคโนโลยีสารสนเทศ เช่น จำนวนครั้ง และระยะเวลาที ต้องหยุดให้บริการ (down time), ระยะเวลาในการแก้ไขอุบัติการณ์ต่างๆ, ค่าใช้จ่ายในการ บำรุงรักษาระบบ

6.2. วัดและติดตามความเสี่ยง การควบคุมภายใน ด้านความมั่นคงและความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

6.3. วัดและติดตามความถูกต้อง ครบถ้วน เชื่อถือได้ ทันเวลาของข้อมูลสารสนเทศ

6.4. ตรวจสอบการปฏิบัติตามนโยบายและระเบียบปฏิบัติ

6.5. ประเมินและวัดผลการดำเนินการตามแผนแม่บทเทคโนโลยีสารสนเทศ การพัฒนาสมรรถนะบุคลากร การพัฒนาความสามารถของระบบ

7. ข้อมูลสารสนเทศ (Data & Information)

วัตถุประสงค์หลักของการมีระบบเทคโนโลยีสารสนเทศในโรงพยาบาลคือ การมีข้อมูล และ สารสนเทศที่จำเป็นสำหรับบุคลากร ผู้บริหาร ผู้ป่วย ผู้รับผลงาน องค์กรภายนอก มีความพร้อมใช้งาน เอื้อต่อการดูแลผู้ป่วย การบริหารจัดการ การตรวจสอบทางคลินิก การพัฒนาคุณภาพ การศึกษา และการวิจัย ความจำเป็นของข้อมูลและสารสนเทศ ขึ้น กับขนาดและความซับซ้อน ตามบริบทของโรงพยาบาล

7.1. มีข้อมูลที่เพียงพอกับการให้บริการผู้ป่วยอย่างมีคุณภาพ ข้อมูลสามารถนำมาใช้ระบุตัวบุคคล สนับสนุนการวินิจฉัยโรค ช่วยพิจารณาการรักษา ช่วยติดตามการรักษา บันทึกผลการรักษา และใช้สนับสนุนการรักษาดูแลอย่างต่อเนื่อง จัดทำเป็นมาตรฐาน อยู่ในเวชระเบียนอิเล็กทรอนิกส์ ปราศจากการซ้ำ ซ้อน หรือขัดแย้งซึ่ง กันและกัน

7.2. ผู้ใช้สามารถเข้าถึงข้อมูลและสารสนเทศได้อย่างสะดวกและเหมาะสมผู้ใช้งานเข้าถึงข้อมูลและสารสนเทศ สำหรับการปฏิบัติงานในความรับผิดชอบได้โดยได้รับข้อมูลและสารสนเทศตามกำหนดเวลา ตรงตามรูปแบบที่ช่วยการใช้งานผู้ป่วยสามารถเข้าถึงข้อมูลของตนเองเพื่อนำไปใช้ในการดูแลรักษาสุขภาพ และหน่วยงานเครือข่ายทีเกี่ยวข้องได้รับข้อมูลเพื่อนำไปใช้พัฒนาบริการสุขภาพ

7.3. สารสนเทศถูกนำมาใช้อย่างเหมาะสม (Appropriate use of information) มีการวิเคราะห์ข้อมูลที่มีอยู่ในระบบ รวมถึงข้อมูลที่จำเป็นต่อการใช้งานแต่ยังไม่มีอยู่ใน ระบบเพื่อจัดการให้มีข้อมูลสารสนเทศที่เหมาะสมเพิ่มขึ้น รวมทั้ง บูรณาการข้อมูลผู้ป่วย และข้อมูลบริหารเข้าหากันเพื□อสนับสนุนการตัดสินใจ และพัฒนาคุณภาพอย่างต่อเนื่อง

7.4. หน่วยงานสามารถใช้ข้อมูลจากแหล่งข้อมูลภายนอกต่างๆ หน่วยงานใช้และบูรณาการข้อมูลจากแหล่งต่างๆ เพื่อ

1) สนับสนุนการตัดสินใจในการดูแลผู้ป่วย

2) สนับสนุน การศึกษา การวิจัย และ

3) สนับสนุนการบริหารจัดการและวางแผนยุทธศาสตร์ มีสารสนเทศทางวิทยาศาสตร์ และด้านอื่นๆ ที่เป็นปัจจุบัน ที่สนองต่อความต้องการของผู้ใช้งาน ภายในเวลาที่เหมาะสม

บทที่ 2

มาตรฐานทางด้านระบบสารสนเทศ (Information System Standard)

การศึกษามาตรฐานสากลด้านสารสนเทศ ข้อกาหนด การประกาศใช้ การบริหารจัดการ การนามาตรฐานต่างๆไปใช้ให้เหมาะสมกับลักษณะงานภายในองค์การต่างๆ ส่งเสริมและยกระดับภูมิปัญญาชาวบ้านด้วยการให้บริการตามมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ มาตรฐานสากลทางด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศที่ผู้บริหารด้านสารสนเทศ (CIO) ควรรู้เพื่อนามาใช้เป็นแนวทางปฏิบัติในองค์กร และ กลยุทธ์ CIO กับการบริหารระบบความปลอดภัยเทคโนโลยีสารสนเทศในองค์กรสมัยใหม่ ในสถานการณ์ปัจจุบันผู้บริหารระบบเทคโนโลยีสารสนเทศระดับสูงหรือ CIO นั้น มีความจาเป็นที่จะต้อง ศึกษามาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัยในระบบ เทคโนโลยีสารสนเทศ เพื่อนามาประยุกต์ใช้ใน องค์กร เหตุผลมีหลายประการ เช่น องค์กรต้อง “Compliance” หรือ จากผู้ตรวจสอบ ”ผ่านการตรวจสอบ“) ระบบสารสนเทศInformation System Internal / External Auditor) เพื่อให้เป็นไปตามกฎหมายของประเทศที่องค์กรนั้นตั้งสานักงานอยู่ เช่น ในประเทศสหรัฐอเมริกา องค์กรที่จดทะเบียนในตลาดหลักทรัพย์ต้องปฏิบัติตาม กฎหมาย Gramm-Leach-Bliley (GLB) กฎหมาย Health Insurance Portability and Accountability Act (HIPAA) และ ล่าสุดกฎหมาย Sarbanes-Oxley (SOX) ซึ่งทาให้อาชีพทางด้านผู้ตรวจสอบระบบสารสนเทศกาลัง เป็นที่ต้องการของหลาย ๆ องค์กรโดยเฉพาะองค์กรที่ต้องเตรียมรับการตรวจสอบ จากองค์กรภายนอก ขณะเดียวกัน ผู้บริหารสารสนเทศขององค์กรต้องมีการเตรียมตัวเพื่อที่จะรับการตรวจสอบจาก ผู้ตรวจสอบ สารสนเทศภายในที่อาจมาจากต่างประเทศในกรณีที่องค์กรเป็นบริษัท ข้ามชาติหรือ มาจากผู้ตรวจสอบสารสนเทศ ภายนอกที่มีความชานาญและมีความเป็นกลางในการตรวจสอบ ดังนั้น ผู้บริหารระบบเทคโนโลยีสารสนเทศ ระดับสูงขององค์กรจึงมีความจาเป็นอย่างยิ่งยวดที่จะต้องเตรียมพร้อมและศึกษาถึงมาตรฐานสากลทางด้านการ รักษาความปลอดภัยระบบสารสนเทศแล้วนามากาหนดเป็น ซึ่งมาตรฐานสากลที่นิยมใช้ ”กรอบแนวทางปฏิบัติ“ กันทั่วโลก

มาตรฐานด้านสารสนเทศในประเทศไทยและสากล

1) ISO/IEC 27001:2005 Information Security Management Systems (ISMS) ระบบมาตรฐานด้านความปลอดภัยของข้อมูล

เป็นมาตรฐานที่มีวัตถุประสงค์เพื่อให้การดาเนินธุรกิจเป็นไปอย่างต่อเนื่อง ซึ่งข้อกาหนดต่างๆ ถูกกาหนดขึ้นโดยองค์กรสากล ISO (International Organization for Standardization) และ IEC (International Electro technical Commission) การประยุกต์ใช้ ISO 27001 จะช่วยให้กิจกรรมทางธุรกิจสามารถดาเนินไปได้อย่าง ต่อเนื่อง ช่วยป้องกันระบบข้อมูลและสารสนเทศขององค์กรจากความเสี่ยงต่อภัยคุกคามต่างๆ สาหรับทุกประเภท Electro technologies ทั้ง ISO และ IEC ได้รับการสนับสนุน โดยองค์กรสมาชิกระดับชาติ ที่มาของความสำคัญสาหรับ ISO 27001 หัวใจสำคัญของระบบบริหารความปลอดภัยสารสนเทศนั้นอยู่ที่ 3 ปัจจัยหลักโดยพื้นฐานดังต่อไปนี้

1. ข้อมูลส่วนตัว ข้อมูลสำคัญขององค์กร

การรักษาความปลอดภัยด้านข้อมูลไม่ให้ถูกขโมย ลักลอบนาไปใช้ ดัดแปลง หรือทาให้เกิดข้อผิดพลาด อื่นใด ซึ่งสาหรับหลายหน่วยงานอาจเป็นอันตรายระดับวิกฤติได้ ซึ่งข้อมูลนี้ไม่เพียงเฉพาะข้อมูลสำคัญขององค์กร แต่ยังรวมถึงข้อมูลส่วนตัว ของลูกค้าหรือบุคคลที่สามที่เกี่ยวข้องอื่นๆ ด้วย

2. การบริหารความเสี่ยงจากเหตุการณ์และปัจจัยต่างๆ

การบริหารความเสี่ยงจากเหตุการณ์และปัจจัยต่างๆ ซึ่งปัจจุบันมีการคานึงถึงการตั้งไซต์สำรอง ในลักษณะของศูนย์สารองข้อมูลและดาเนินการกู้คืนระบบภายหลังภัยพิบัติหรือ Disaster Recovery Center (DRC) ซึ่งมีความสำคัญมากในหลายธุรกิจ เช่น ธุรกิจการเงิน หรือบริการด้านสุขภาพ เพราะข้อมูลเหล่านั้นมีความสาคัญยิ่งยวดต่อความสามารถในการดาเนินธุรกิจให้ ต่อเนื่องต่อไปได้(Business continuity)

3. บริหารระบบเพื่อป้องกันความปลอดภัยของข้อมูล

รายละเอียดการบริหารระบบเพื่อป้องกันความปลอดภัยของข้อมูล ซึ่งหัวข้อนี้นับเป็นหนึ่งในรายละเอียดหลักของเนื้อหาในร่างมาตรฐาน ISO 27000 ทั้งหมดก็ว่าได้ โดยครอบคลุมตั้งแต่นโยบาย แผนกลยุทธ์ การตรวจวัด การบริหาร และการควบคุมการปฏิบัติการ

ปัจจัยในการพิจารณาความปลอดภัยของระบบสารสนเทศ

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

แนวทางในการนามาตรฐาน ISO/IEC 27001 มาใช้ในองค์กรนั้น ควรมีขั้นตอน 7 ขั้นตอน ดังนี้

ขั้นตอนที่ 1

จัดตั้งคณะทางาน IT Security Steering หรือ IT Security Working Group) เฉพาะเรื่องมาตรฐาน ISO/IEC 27001 และ Regulatory Compliance เพื่อทาการศึกษาตัวมาตรฐานโดยละเอียดและหาแนวทางนามาปรับ ประยุกต์ใช้ภายในองค์กร

ขั้นตอนที่ 2

จัดฝึกอบรม ทาความเข้าใจในส่วนของข้อกาหนดทั้ง 11 Domains ของมาตรฐาน ISO/IEC 27001 ซึ่งควรใช้ระยะเวลาประมาณ 3-5 วัน โดยการฝึกอบรมอาจใช้แนวทางในการทา Internal ISO 27001 Workshop หรืออบรมหลักสูตรมาตรฐานของ IRCA ได้แก่ หลักสูตร ISO 27001 (ISMS) Lead Auditor (IRCA2016) ซึ่งจะทาให้ทีมงานได้เข้าใจแนวทางของการตรวจสอบโดยการนามาตรฐาน ISO/IEC 27001 มาใช้อย่างถูกต้องเหมาะสา

หรับองค์กรที่ต้องการได้รับใบรับรองจากผู้ให้บริการออกใบรับรอง หรือ Certification Body เพื่อเป็นการเตรียมตัวในการตรวจสอบเพื่อผ่านการรับรองต่อไป

ขั้นตอนที่ 3

จัดทาการประเมินระบบในภาพรวม)Holistic Approach) โดยนาเทคนิค “Gap Analysis” มาใช้ กล่าวคือ นามาตรฐาน ISO/IEC 27001 ในส่วน Control ที่อยู่ใน Annex A. มาทาเป็นประโยคคาถามในรูปแบบของQuestionnaire มาใช้ในการสัมภาษณ์ผู้ที่เกี่ยวข้องในองค์กรในลักษณะ Workshop ที่ทุกคนสามารถเข้ามามีส่วนร่วมในการตอบคาถามและให้ความเห็น รายงานจากการทา Gap Analysis จะทาให้ผู้บริหารระดับสูงขององค์กรได้ทราบถึงสถานะล่าสุดขององค์กร)“AS IS”) และ ความแตกต่างกับข้อกาหนดในมาตรฐาน)“TO BE”) ว่าระบบในองค์กรยังไม่ได้ปฏิบัติตามข้อกาหนดในมาตรฐานและมีความแตกต่างจาก “สิ่งที่ควรจะเป็น” หรือ “สิ่งที่ควรจะต้องทา” ตามมาตรฐานอย่างไร

ขั้นตอนที่ 4

หลังจากการทา “Gap Analysis Workshop” แล้วควรมีการจัดทารายงานและมีการนาเสนอต่อ Board of Director เพื่อที่จะให้ผู้บริหารระดับสูงเกิดความเข้าใจในปัญหาที่เกิดขึ้น และ สร้าง “Management Buy-In” คือ การทาให้ผู้บริหารระดับสูงตัดสินใจให้การสนับสนุนในการปฏิบัติตามมาตรฐาน ISO/IEC 27001 และดาเนินการแก้ไขข้อบกพร่องจากการที่องค์กรยังไม่ได้ปฏิบัติตามมาตรฐานดังกล่าวอย่างเป็นรูปธรรม (Corrective Action)

ขั้นตอนที่ 5

องค์กรควรลงรายละเอียดหลังจากการนาเสนอ Gap Analysis Report โดยการทากระบวนการบริหารความเสี่ยง (Risk Management) ในสามมุมมอง ได้แก่ มุมมองด้านบุคลากร (People) มุมมองด้านกระบวนการ (Process) และ มุมมองด้านเทคโนโลยี (Technology) เพื่อที่จะได้ประเมินความเสี่ยง (Risk Assessment) ของระบบ และ จัดทาแผนปฏิบัติการเพื่อลดความเสี่ยง (Risk Treatment Plan) เช่น การทา Hardening การจัดฝึกอบรม Security Awareness Training ในองค์กร การจัดทาระบบ Centralized Log Management เพื่อปฏิบัติตามข้อกาหนดของมาตรฐาน ISO/IEC 27001

ขั้นตอนที่ 6

ทาการ Implement ในภาคปฏิบัติตามแผนที่ได้กาหนดไว้จากขั้นตอนที่ 5 เช่น การทา Vulnerability Assessment หรือ Penetration Testing, การปิดช่องโหว่ด้วยการ Hardening หรือ การติดตั้ง Patch ให้กับระบบ การจัดทา Policy, Standard, Guideline ต่างๆ ที่จาเป็น การฝึกอบรม Security Awareness Program ให้กับทุกคนในองค์กร การจัดทา Acceptable Use Policy (AUP), การจัดซื้อจัดจ้างฮาร์ดแวร์และซอฟต์แวร์ในส่วนของเทคโนโลยีที่จาเป็น เช่น Firewall , Anti-Virus Software เป็นต้น

ขั้นตอนที่ 7

หลังจากปฏิบัติตามขั้นตอนที่ 6 แล้ว ควรมีการทบทวน (Review) และ การเฝ้าระวัง (Monitor) เพื่อเปรียบเทียบความเปลี่ยนแปลงระหว่างก่อนการปฏิบัติตามมาตรฐาน และ หลังจากการปฏิบัติตามมาตรฐาน ซึ่งควรจะเห็นผลลัพธ์ในเชิงบวกเป็นรูปธรรมชัดเจน และ ควรทาการเฝ้าระวังระบบด้วยแนวคิด “Continuous Audit” เพื่อที่จะได้แน่ใจว่าระบบสามารถทางานได้ปกติโดยไม่เกิดผลกระทบจากการค้นพบช่องโหว่ใหม่ๆ (New Vulnerability) และ ภัยใหม่ๆ จากแฮกเกอร์ หรือ Malicious Software ต่างๆ (New Threat) ตลอดจนสามารถปรับตัวแก้ไขปัญหาได้อย่างทันท่วงที (Agility)

<u>สาเหตุของปัญหาด้านความปลอดภัยของระบบสารสนเทศ</u>

เทคโนโลยี	กระบวนการ	บุคลากร
ขาดคุณสมบัติด้านความปลอดภัย	ไม่ได้ออกแบบกระบวนการให้รองรับด้านความปลอดภัย	ขาดความรู้ที่เกี่ยวกับเรื่องความปลอดภัย
มี bug , มีช่องโหว่ด้านปลอดภัย และขาด path แก้ไข	ไม่มีบทบาทความรับผิดชอบด้านความปลอดภัยชัดเจน	ขาดความใส่ใจจริงจังในการแก้ปัญหา
ไม่มีมาตรฐาน	ขาดการตรวจประเมินและติดตามตรวจสอบ	ขาดการสื่อสารที่ดีในเรื่องที่เกี่ยวกับความปลอดภัย
ยากที่จะปรับปรุงปัญหาความเสี่ยงด้านความปลอดภัยให้ทันต่อเหตุการณ์	ไม่มีกระบวนการรับรองการปรับความทันสมัยเรื่องความปลอดภัยให้ระบบ	มีข้อผิดพลาดที่เกิดจากการทำงานของบุคลากร

2) มาตรฐาน ISO/IEC17799: 2005 (Second Edition) หรือ BS7799-1

มาตรฐาน ISO/IEC17799: 2005 (Second Edition) ถูกประกาศอย่างเป็นทางการในเดือนมิถุนายน ปี 2005 ได้มีการปรับปรุงแก้ไขมาจากต้นฉบับ ISO/IEC 17799:2000 (First Edition) จากปี 2000 ในประเทศไทยคณะอนุกรรมการความมั่นคงภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ซึ่งจัดตั้งขึ้นตามพระราชบัญญัติการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2546 (http://www.etcommission.go.th) ได้นามาตรฐาน ISO/IEC17799 :2000 (First Edition) หรือ BS7799-1 มาเป็นแนวทางในการกาหนด มาตรฐานการรักษาความปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ ไทยจานวน 144 ข้อ เพื่อให้เป็นแนวทางเสริมสร้างการรักษาความปลอดภัยให้กับองค์กรหรือหน่วยงาน ที่เกี่ยวข้องกับการประกอบธุรกรรมทางอิเล็กทรอนิกส์โดยกาหนดมาตรฐานออกเป็น 3 ระดับ คือ ระดับ 1 ควรปฏิบัติ 31 ข้อ, ระดับ 2 ควรปฏิบัติ 104 ข้อ และ ระดับ 3 ซึ่งเป็นระดับความปลอดภัยสูงสุด ควรปฏิบัติทั้งหมด 144 ข้อ

การนามาตรฐาน ISO/IEC17799 : 2005 มาปฏิบัติในองค์กร สามารถนาองค์กรไปสู่การ “Certified” โดย Certification Body ตามมาตรฐาน BS7799-2:2002 ขณะนี้องค์กรทั่วโลกกาลังให้ความสนใจเรื่องความปลอดภัยระบบเทคโนโลยี สารสนเทศ ตัวอย่างในประเทศญี่ปุ่นนั้นมีองค์กรได้รับการรับรองมาตรฐาน BS7799-2 ไปแล้วกว่าเก้าร้อยองค์กร แสดงให้เห็นถึงมาตรฐานด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศที่พัฒนากว่าประเทศเพื่อนบ้าน ขณะนี้การรับรองมาตรฐาน BS7799-2: 2002 กาลังพัฒนาเปลี่ยนแปลงเป็น ISO/IEC 27001:2005 ที่คาดว่าจะประกาศอย่างเป็นทางการประมาณเดือน พฤศจิกายน คศ. 2005 ซึ่งจะสอดคล้องกับมาตรฐาน ISO/IEC17799:2005(BS7799-1) ที่ถูกประกาศบอกมาแล้วก่อนหน้านี้

3) มาตรฐาน CobiT (Control Objective for Information and Related Technology)

มาตรฐาน CobiT ถูกพัฒนาขึ้นโดย ISACA (http://www.isaca.org) และ IT Governance Institute (http://www.itgi.org) เพื่อ องค์กรที่ต้องการมุ่งสู่การเป็น “ไอทีภิบาล” หรือ “IT Governance” มาตรฐาน CobiT เป็นแนวคิดและแนวทางปฏิบัติของผู้บริหารระบบสารสนเทศ และขณะเดียวกันก็เป็นแนวทางปฏิบัติสาหรับผู้ตรวจสอบระบบสารสนเทศด้วย โครงสร้างของมาตรฐาน CobiT นั้นแบ่งออกเป็น 4 กระบวนการหลัก ซึ่งทั้ง 4 กระบวนการหลักจะประกอบด้วย High Level Control Objective ทั้งหมด 34หัวข้อ และ Detail Control Objective แบ่งแยกย่อยอีกทั้งหมด 318 หัวข้อย่อย

ในปัจจุบันมาตรฐาน CobiT เป็นมาตรฐานเปิดที่สามารถ Download ได้ที่ Web Site ของ ISACA ในประเทศไทย สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ ภาคพื้นกรุงเทพฯ มีโครงการในการแปลมาตรฐาน CobiT ออกมาเป็นภาษาไทย และ ทางสมาคม ISACA สหรัฐอเมริกากาลังจะออก CobiT Version 4 ซึ่งมีการปรับปรุงจาก COBIT Version 3.2 ปัจจุบัน

แนวคิดของมาตรฐาน CobiT กาลังเป็นที่นิยมในกลุ่มธุรกิจด้านการเงินและการธนาคาร ยกตัวอย่าง เช่น ธนาคารแห่งประเทศไทยและ สานักงานคณะกรรมการกากับหลักทรัพย์และตลาดหลักทรัพย์ หรือ กลต. ได้ให้ความสนใจในการนามาตรฐาน CobiT มาเป็นแนวทางในการออกข้อกาหนดและกฎข้อบังคับต่างๆ ที่ธนาคารพาณิชย์และบริษัทหลักทรัพย์ต่างๆ ควรนามาปฏิบัติ ซึ่งขณะนี้ทางธนาคารแห่งประเทศไทย และ กลต. ได้ออกประกาศเรื่องการควบคุมการปฏิบัติงานและแนวทางปฏิบัติในการรักษาความ ปลอดภัยด้านเทคโนโลยีสารสนเทศและการให้บริการการเงินทางอิเล็กทรอนิกส์เพื่อเป็นแนวทางให้กับธนาคารพาณิชย์และบริษัทหลักทรัพย์ต่างๆ ในประเทศไทย

4) มาตรฐาน ITIL (IT Infrastructure Library)/BS15000

มาตรฐาน ITIL นั้นมีต้นตอมาจากประเทศอังกฤษ ซึ่งทางรัฐบาลประเทศอังกฤษ โดย OGC (Office of Government Commerce) พัฒนาร่วมกับ BSI (British Standard Institute) มีวัตถุประสงค์ในการสร้าง Best Practice สาหรับกระบวนการบริหารงานบริการด้านสารสนเทศ (IT Service Management) มาตรฐาน

ITIL กล่าวถึง “Best Practice” ในการบริหารจัดการงานให้บริการด้านระบบสารสนเทศที่ควรจะเป็นและมีประสิทธิภาพและ ประสิทธิผลชัดเจน เช่น มาตรฐานด้าน Service Support และ Service Delivery ตลอดจนการกาหนด SLA (Service Level Agreement) เป็นต้น

มาตรฐาน ITIL ถูกจัดทาเป็นหนังสือหลายเล่าโดยแบ่งออกเป็น 2 ส่วนได้แก่ BS15000-1 Specification for Service management แ ล ะ BS15000-2 Code of practice for service management ปัจจุบันแนวโน้มด้านการ “Outsource” การบริหารจัดการเทคโนโลยีสารสนเทศมีการเพิ่มขึ้นอย่างรวดเร็ว ดังนั้นมาตรฐานในการควบคุมคุณภาพของการให้บริการนั้นจึงถือเป็นเรื่องสาคัญ ที่องค์กรควรจะศึกษาและกาหนดเป็นมาตรฐานขั้นต่าให้กับ Outsourcer Company ที่รับงานบริการด้านสารสนเทศไปจัดการแทนองค์กรเพื่อให้เกิดประสิทธิผลและประสิทธิภาพสูงสุดในการให้บริการ และส่งผลด้านความพึงพอใจของผู้ใช้คอมพิวเตอร์ (Computer Users) ทั่วๆไป และส่งผลต่อภาพลักษณ์ของผู้บริหารเทคโนโลยีสารสนเทศระบบสูงในทางอ้อมด้วย

5) มาตรฐาน SANS TOP20

มาตรฐาน SANS TOP20 เป็น มาตรฐานในการตรวจสอบระบบสารสนเทศสาหรับระบบความปลอดภัยบนระบบปฏิบัติการ Microsoft Windows และ UNIX/Linux ที่ได้รับการยอมรับกันโดยทั่วไป มาตรฐาน SANS Top 20 มีมาตั้งแต่ปี 2000 ขณะนี้ SANS Top 20 ล่าสุดได้มีการปรับปรุงมา 4 ครั้ง และ ปรับปรุงในปี 2004 เรียกว่า SANS Top 20 2004 โดยแบ่งออกเป็นการเตือนช่องโหว่ของระบบปฏิบัติการ Windows 10 ช่องโหว่ และ การเตือนช่องโหว่ระบบปฏิบัติการ UNIX/ Linux อีก 10 ช่องโหว่ รายละเอียดดูที่ http://www.sans.org/top20 ปัจจุบัน SANS ได้ออก SANS Top 20 2005 Quarter 1 and Quarter 2 update มาเพิ่มเติมด้วย

6) มาตรฐาน ISMF 7 (Information Security Management Framework)

มาตรฐาน ISMF ทั้ง 7 ขั้นตอน เป็น มาตรฐานในการตรวจสอบและประเมินความปลอดภัยระบบสารสนเทศที่พัฒนาโดยนัก วิชาการคนไทย จุดประสงค์เพื่อให้เป็นแนวทางในการปริหารจัดการระบบรักษาความปลอดภัยข้อมูล อย่างเป็นระบบและมีประสิทธิภาพให้ทันกับสถานการณ์ปัจจุบันของการโจมตีระบบ โดย Hacker และ MalWare ต่างๆ

7) มาตรฐาน ISO/IEC 27001: 2013

ว่าด้วยเรื่องของข้อกาหนดในการจัดทาระบบบริหารจัดการความมั่นคงปลอดภัยหรือ ISMS ให้กับองค์กร ซึ่งมีหัวข้อที่เกี่ยวข้องคือ

0 Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Context of the organization

5 Leadership

6 Planning

7 Support

8 Operation

9 Performance evaluation

10 Improvement

มาตรฐาน ISO/IEC 27001 นี้ ปัจจุบันได้รับความนิยมอย่างแพร่หลาย เนื่องจากประกอบด้วยวงจร Plan-Do-Check-Act และใช้แนวทางการประเมินความเสี่ยงมาประกอบการพิจารณาหาวิธีการหรือมาตรการ เพื่อป้องกัน ลดความเสี่ยง และรักษาทรัพย์สินสารสนเทศที่มีค่าขององค์กรให้มีความมั่นคงปลอดภัยในระดับที่เหมาะสม

กลยุทธ์ CIO กับการบริหารระบบความปลอดภัยเทคโนโลยีสารสนเทศในองค์กรสมัยใหม่

ตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ CIO (Chief Information Officer) นั้นเป็นตำแหน่งสำคัญที่ทุกองค์กรทั้ง ภาครัฐ และ เอกชนต้องมีบุคลากรที่รับผิดชอบในเรื่องนี้โดยตรง โดยเฉพาะในองค์กรขนาดใหญ่ CIO ควรมีหน้าที่ในการกาหนดยุทธศาสตร์ (Strategy) ทิศทางด้านเทคโนโลยีสารสนเทศขององค์กรตลอดจนมาตรการในการรักษาความปลอดภัยเทคโนโลยีสารสนเทศขององค์กร ในกรณีที่ยังไม่มีตาแหน่ง CSO (Chief Security Office) หรือ CISO (Chief Information Security Officer) มารับผิดชอบด้านความปลอดภัย สารสนเทศ โดยตรง CIO ก็ต้องรับผิดชอบเรื่องความปลอดภัยไปด้วยในตัว ซึ่งนับว่าเป็นภาวะความรับผิดชอบที่ค่อนข้างสูง เพราะเรื่องความปลอดภัยเทคโนโลยีระบบสารสนเทศนั้นมีการเปลี่ยนแปลงอยู่เสมอ CIO ต้องคอยติดตามความเคลื่อนไหวและปรับปรุงความรู้ความสามารถให้สอดคล้องกับสถานการณ์ปัจจุบัน และยังต้องตัดสินใจเรื่องการเลือกใช้เทคโนโลยีด้านความปลอดภัยที่เหมาะสมแก่ องค์กรทั้งในเรื่องของ TCO (Total Cost of Ownership) และ ROI (Return On Investment) จากข้อมูลของ Gartner เรื่อง Hype Cycle for Information Security 2004 ปัญหาด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศยังเป็นประเด็นสาคัญที่ CIO ต้องให้ความ สนใจและจัดการอย่างเป็นระบบ แสดง ให้เห็นถึง Cyber Threat ต่าง ๆ ที่ กาลังเป็นปัญหาอยู่ในปัจจุบัน ปัญหา ใหญ่ของ CIO คือ เรื่อง Spyware, Phishing, SPAM และ Peer-to-Peer Exploit ขณะเดียวกัน CIO ควรนาใช้ในการแก้ปัญหาดังกล่าว บางเทคโนโลยี เช่น IDS นั้น ล้าสมัยไปแล้ว ขณะนี้เทคโนโลยีใหม่เข้ามาแทนที่ เช่น IPS, Vulnerability Management และ Patch Management เป็นต้น การให้บริการเฝ้าระวังระบบรักษาความปลอดภัยจากบริษัทที่รับดูแลด้านความ ปลอดภัยโดยตรงที่เรียกตัวเองว่า MSSP (Managed Security Service Provider) ก็กาลังได้รับความนิยมจาก CIO เพิ่มขึ้นเช่นกัน ดังนั้น CIO ควร

มีกลยุทธ์ในการบริหารจัดการเทคโนโลยีสารสนเทศที่ดีและเตรียมพร้อมกับสถานการณ์ปัจจุบัน และอนาคตโดยสรุปได้ 6 ข้อดังนี้

1. CIO ต้องมีกลยุทธ์ในการรับผิดชอบดูแลเรื่องการประหยัดงบประมาณ การใช้จ่ายทางด้านเทคโนโลยีสารสนเทศ การจัดซื้อจัดจ้างระบบเทคโนโลยีสารสนเทศนั้นจาเป็นต้องใช้งบประมาณค่อนข้างสูง การตัดสินใจเลือกใช้เทคโนโลยีใหม่ๆ จึงเป็นความท้าทายของ CIO เพราะหากตัดสินใจผิดก็อาจส่งผลเสียในระยะยาวให้แก่องค์กรได้ ขณะที่งบประมาณด้านการรักษาความปลอดภัยนั้นมีแนวโน้มที่จะลดลงตามสภาวะเศรษฐกิจโลกที่ถดถอย แต่การโจมตีจากแฮกเกอร์ และไวรัสกลับมีแนวโน้มที่เพิ่มขึ้นอย่างมาก ดังนั้น CIO จึงจาเป็นต้อง “Balance” ปรับสมดุลระหว่างความปลอดภัยขั้นต่าที่องค์กรควรมี และงบประมาณที่จะถูกใช้จ่ายออกไปเพื่อให้ได้มาซึ่งอุปกรณ์ฮาร์ดแวร์และซอฟท์แวร์ ตลอดจนการบริการจาก IT Auditor, IT Consultant, System Integrator และ IT Outsourcer รวมถึง งบประมาณการฝึกอบรม Information Security Awareness Training
และ Information Security Technical Training จาก IT Training Center ต่างๆ อีกด้วย

2. CIO ควรกาหนดแผนยุทธ์ศาสตร์ ด้านความปลอดภัยระบบสารสนเทศ (Information Security Strategic Planning) ให้ชัดเจนและนาไปปฏิบัติจริงได้ แผนยุทธ์ศาสตร์ในระยะยาวควรกาหนดออกมาให้ชัดเจนเพื่อเป็นแนวทางในการดาเนินการด้านสารสนเทศและการรักษาความปลอดภัยข้อมูล สารสนเทศ จากนั้น แผนระยะกลางและแผนระยะสั้น ก็ควรถูกกาหนดออกมาเช่นกัน ยกตัวอย่าง เช่น องค์กรควรมีการจัดทาการประเมินความเสี่ยงระบบสารสนเทศ (IT Risk Assessment) เป็นประจาทุกปี และควรมีการจัดทาแผนฝึกอบรม Information Security Awareness Training ในทุกๆ 3 – 6 เดือน เป็นต้น

3. CIO ควรเพิ่มความรู้และมีความรอบรู้เพียงพอเพื่อใช้ประกอบการตัดสินใจเลือกใช้เทคโนโลยีที่เหมาะสมและไม่ล้าสมัยให้แก่องค์กร ตัวอย่างการเลือกใช้ Platform ว่าจะใช้ Windows Server 2003 Platform หรือ UNIX/LINUX Platform การเลือกใช้เทคโนโลยี J2EE (Jave 2 Enterpirse Edition) หรือเลือกใช้เทคโนโลยี Dot NET ของ Microsoft เป็นต้น

การหมั่นเข้าร่วมฟังงานสัมมนาเทคโนโลยีใหม่ๆ ก็เป็นเรื่องจาเป็นของ CIO เช่นเดียวกัน ซึ่งก็คงต้องปลีกเวลาการทางานบ้างเพื่อเพิ่มพูนความรู้ใหม่ ๆ ที่เป็นประโยชน์ในการตัดสินใจในอนาคต การเดินทางไปชมงาน ICT Expo ในต่างประเทศ ก็ควรอยู่ในโปรแกรมของ CIO ด้วย

4. CIO ควรนาองค์กรเข้าสู่มาตรฐานกาหนดความปลอดภัยสารสนเทศที่สากลให้การยอมรับและเตรียมพร้อมสาหรับในการตรวจสอบจากผู้ตรวจสอบระบบสารสนเทศ

การนำมาตรฐานสากลด้านความปลอดภัยระบบสารสนเทศเช่น ISO/IEC17799 หรือ CobiT มาประยุกต์ใช้บางส่วน ถือเป็นเรื่องจาเป็น CIO ต้องให้ความสำคัญเช่นกัน โดยองค์กรอาจจะไม่จาเป็นต้องได้รับใบรับรองมาตรฐาน BS7799-2 ในกรณีที่องค์กรมองว่าประโยชน์ที่ได้รับจากการได้รับใบรับรองมาตรฐานด้าน

ความปลอดภัยนั้นยังไม่ชัดเจน แต่องค์กรก็ควรนามาตรฐานสากลที่เป็น “Best Practice” ต่าง ๆ มาประยุกต์ใช้เพื่อความปลอดภัยขององค์กรเอง และ เพื่อให้สอดคล้องกับยุคของ IT Governance การตรวจสอบระบบสารสนเทศโดย ผู้ตรวจสอบภายนอกหรือผู้ตรวจสอบภายในเป็นเรื่องจาเป็นที่ต้องทาเป็นประจาทุก ปีเพื่อให้แน่ใจถึงระดับของความเสี่ยงที่ผู้บริหารยอมรับได้ และ ไม่ส่งผลกระทบต่อองค์กร

5. CIO ควรรักษาความสัมพันธ์ที่ดีกับผู้ร่วมงานและพัฒนาการสื่อสารกับผู้ร่วมงานให้มีความชัดเจนและความเข้าใจในทิศทางเดียวกัน

ปัญหาของ CIO ในหลายๆ องค์กร คือ CIO ไม่สามารถอธิบายการทางานด้านสารสนเทศต่าง ๆ ให้แก่ผู้บริหารระดับสูง เช่น CEO หรือ CFO เพื่อให้เกิดความเข้าใจ และ ให้การสนับสนุนได้อย่างมากพอ ทาให้หลายๆ โครงการด้านสารสนเทศ ไม่ประสบความสำเร็จ ดังนั้น CIO ควรต้องมี Communication Skill หรือ ทักษะในการพูดคุย การติดต่อ ตลอดจน การนาเสนอในรูปแบบมืออาชีพ ที่มีความชัดเจน และ ง่ายต่อการเข้าใจของผู้บริหารระดับสูงที่ไม่ใช่ “คนไอที” ตลอดจน CIO ควรรักษาความสัมพันธ์กับ System Integrator, Consultant, Supplier และ Outsourcer เพื่อให้บริษัทเหล่านี้มาช่วยแบ่งเบาภาระของ CIO และ เป็นการ Transfer Risk ไปในตัว ความสัมพันธ์ที่ดีกับหน่วยงานต่าง ๆ ดังกล่าวจะส่งผลช่วย CIO ในทางอ้อมต่อประสิทธิภาพในการปฏิบัติงานและภาพลักษณ์ของตัว CIO เอง

6. CIO ควรเตรียมรับสถานการณ์ฉุกเฉินด้านความปลอดภัยสารสนเทศที่อาจเกิดขึ้นได้

แผน BCP (Business Continuity Planning) และ DRP (Disaster Recovery Planning) ควรถูกจัดทาขึ้นเพื่อให้องค์กรพร้อมกับการเตรียมรับเหตุการณ์ฉุกเฉิน หรือ Incident Response Management ที่อาจเกิดขึ้นและส่งผลกระทบต่อการทางานโดยรวมขององค์กรได้ โดย CIO ต้องช่วยสนับสนุนและเป็นแกนหลักในการจัดทาแผนดังกล่าวด้วยโดยสรุปแล้วตำแหน่ง CIO นั้นเป็นตำแหน่งที่มีความสำคัญต่อองค์กรอย่างสูงในยุคที่เทคโนโลยีระบบสารสนเทศ และ การสื่อสาร เข้ามามีบทบาทสำคัญต่อการดาเนินงานขององค์กรในปัจจุบัน การกำหนดกลยุทธ์ในการบริหารจัดการเทคโนโลยีสารสนเทศและการรักษาความปลอดภัย สารสนเทศเป็นเรื่องสำคัญที่ CIO ทุกท่านต้องจัดทาขึ้น และ CIO จะต้องมีความรับผิดชอบในเรื่องดังกล่าวโดยปริยาย เพราะ ในอนาคตกฎหมายต่าง ๆ ที่กำลังจะถูกประกาศใช้ เช่น กฎหมายการกระทำผิดเกี่ยวกับคอมพิวเตอร์ หรือ ประกาศกฎข้อบังคับต่าง ๆ ขององค์กรที่มีหน้าที่ในการควบคุม เช่น สตง. ธนาคารแห่งประเทศไทย หรือ กลต. มีแนวโน้มที่จะเข้มงวด เรื่องการรักษาความปลอดภัยข้อมูลระบบสารสนเทศมากขึ้น CIO ก็ควรจะปรับตัวให้เข้ากับยุคสมัยทศวรรษแห่งดิจิตอลเพื่อนาองค์กรเข้าสู่ IT Governance หรือ “ไอทีภิบาล” เพื่อจุดมุงหมายปลายทาง คือ Corporate Governance หรือ “บรรษัทภิบาล” ในที่สุด

อ้างอิง

ปริญญา หอมอเนก (2548). มาตรฐานสากลทางด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศที่ CIO ควรรู้เพื่อนามาใช้เป็นแนวทางปฏิบัติในองค์กร และ กลยุทธ์ CIO กับการบริหารระบบความปลอดภัยเทคโนโลยีสารสนเทศในองค์กรสมัยใหม่ [ออนไลน์].

สถาบันรับรองมาตรฐานไอเอสโอ (2556) .มาตรฐาน ISO/IEC 27001: 2013 [ออนไลน์].