วารสารวิชาการสาธารณสุข
ปีที่ 28 ฉบับที่ 1 มกราคม - กุมภาพันธ์ 2562

Journal of Health Science
Vol. 28 No. 1, January - February 2019

นิพนธ์ต้นฉบับ ***Original article***

การพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศภายใต้มาตรฐาน ISO/IEC 27001:2013 ศูนย์ปฏิบัติการ Ministry of Public Health Internet Data Center (MOPH IDC)

สุวันต์นา เสมอเนตร บธ.ม. (การจัดการสาธารณะ)
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข

วันรับ: 19 พ.ย. 2561
วันแก้ไข: 13 ธ.ค. 2561
วันตอบรับ: 20 ธ.ค. 2561

บทคัดย่อ การพัฒนาอย่างรวดเร็วของเทคโนโลยีที่ใช้ง่ายและมีราคาถูกทำให้ประชากรสามารถเข้าถึงสารสนเทศได้อย่างไร้ขีดจำกัด ประเทศใช้เทคโนโลยีขับเคลื่อนระบบเศรษฐกิจและสังคม เพิ่มรายได้และลดความเหลื่อมล้ำของประชาชน อย่างไรก็ตาม ภัยคุกคามไซเบอร์ก็ทวีความรุนแรงไปพร้อมกับการเติบโตของระบบเศรษฐกิจและสังคมดิจิทัล ผู้วิจัยจึงได้ศึกษาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เพื่อประโยชน์ในการป้องกันสินทรัพย์สารสนเทศที่เกี่ยวข้องกับการให้บริการระบบสารสนเทศ ของศูนย์ปฏิบัติการ MOPH IDC (Ministry of Public Health Internet Data Center) จากภัยคุกคามภายในและภายนอกที่อาจเกิดขึ้นทั้งที่โดยเจตนาหรือไม่เจตนาก็ตามเพื่อแสดงถึงคุณภาพในการบริหารความมั่นคงปลอดภัยในการดำเนินงานด้านเทคโนโลยีสารสนเทศโดยนำมาตรฐาน ISO/IEC 27001:2013 มาประยุกต์ใช้ซึ่งมีการดำเนินการแบ่งออกเป็น (1) ศึกษามาตรฐานการจัดการความมั่นคงปลอดภัย (2) วิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร (3) พัฒนาระบบบริหารความมั่นคงปลอดภัย แนวทางปฏิบัติในการรักษาความปลอดภัยทางด้านเทคโนโลยีสารสนเทศตามมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013 และ (4) จัดทำข้อเสนอแนะเพื่อสร้างแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ จากการประเมินผลความพึงพอใจของผู้รับบริการระบบบริหารความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO/IEC 27001:2013 พบว่า กลุ่มที่ 1 ผู้ใช้บริการ VM (virtual machine) และ web hosting มีความพึงพอใจในภาพรวมทุกด้านอยู่ในระดับมาก คะแนนเฉลี่ย 3.99 กลุ่มที่ 2 ผู้ให้บริการ (vendor) มีความพึงพอใจในภาพรวมทุกด้านอยู่ในระดับมาก คะแนนเฉลี่ย 4.17 และกลุ่มที่ 3 ผู้รับบริการทั่วไป มีความพึงพอใจในภาพรวมทุกด้านอยู่ในระดับมาก คะแนนเฉลี่ย 3.98 เช่นกัน การนำมาตรฐาน ISO/IEC 27001:2013 เข้ามาใช้เพื่อเพิ่มความมั่นคงปลอดภัยขององค์กรให้เป็นไปตามมาตรฐานสากล ผลการดำเนินงานประสบผลสำเร็จเป็นอย่างดี

คำสำคัญ: **ความมั่นคงปลอดภัย, ความเสี่ยง, มาตรฐาน ISO/IEC 27001:2013**

บทนำ

กระทรวงสาธารณสุข มีนโยบายการปฏิรูประบบข้อมูลสุขภาพเพื่อรองรับการบริการบัตรเดียวรับบริการได้ทุกที่ภายในจังหวัดเป็นช่วงเดียวกับนโยบายรัฐบาลกำหนดในเรื่อง e-Government ตามแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารแห่งชาติ ฉบับที่ 2 (พ.ศ.

2552-2556)[1] และได้สร้างอาคารศูนย์ข้อมูลข่าวสารและสารสนเทศสุขภาพ (Data Center) พร้อมระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology: ICT) เป็นโครงสร้างพื้นฐานที่สำคัญที่ใช้ในการรองรับกลยุทธ์และกระบวนการดำเนินภาระกิจต่าง ๆ เป็นการนำอุปกรณ์คอมพิวเตอร์เข้ามาช่วยในการปฏิบัติงานการติดต่อสื่อสารการจัดเก็บข้อมูลที่สำคัญของกระทรวง รวมไปถึงการประมวลผลข้อมูลต่าง ๆ เพื่อใช้ในการประกอบการตัดสินใจของผู้บริหารที่ต้องการสารสนเทศที่มีคุณภาพ จัดตั้ง Data Center ของกระทรวงสาธารณสุขตามมาตรฐาน Uptime Teir II และมาตรฐาน ISO/IEC27001:2013 เพื่อให้บริการ MOPH Private Cloud ในรูปแบบ Infrastructure as a Service (IaaS) คือให้บริการในส่วนของ storage, hardware, servers และ Network แก่หน่วยงานในสังกัดกระทรวงสาธารณสุข[2] ต่อมาในช่วงแผนปฏิบัติราชการกระทรวงสาธารณสุข ปีพ.ศ.2556-2559 กระทรวงสาธารณสุขมีนโยบายเรื่องจัดทำระบบฐานข้อมูลกลางที่มีการเชื่อมโยงจากแหล่งข้อมูลที่เกี่ยวข้อง เน้นการพัฒนาข้อมูลข่าวสารสุขภาพให้เป็นระบบเดียวเพื่อลดภาระการจัดเก็บข้อมูลและการจัดทำรายงานของเจ้าหน้าที่ระดับปฏิบัติการ จึงได้ดำเนินการจัดทำคลังข้อมูลสุขภาพในระดับจังหวัด นอกจากนั้นแผนยุทธศาสตร์ชาติด้านสาธารณสุขระยะ 20 ปี (พ.ศ. 2560 - 2579) แผนงานการพัฒนาระบบข้อมูลสารสนเทศสุขภาพ มีมาตรการให้ควบคุมความปลอดภัยของข้อมูลกระบวนการเข้าถึงให้ใช้มาตรการ 1I 3A ได้แก่ identification authentication authorization และ access control เพื่อให้รองรับกับแผนยุทธศาสตร์ชาติ 20 ปี แผนปฏิรูปประเทศด้านสาธารณสุขและแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ได้กำหนดให้จัดระบบมาตรฐานข้อมูลสารสนเทศสุขภาพครบทุกมิติและมีกลไกที่สามารถบูรณาการสารสนเทศสุขภาพทุกระดับเพื่อการนำไปใช้ประโยชน์ได้จริง ที่ประชาชนสามารถเข้าถึงและบริหารจัดการข้อมูลสุขภาพของตนได้

ก้าวแรกที่เป็นกลไกสำคัญในก้าวสู่รัฐบาลดิจิทัลคือการบูรณาการข้อมูลผ่านระบบเชื่อมโยงแลกเปลี่ยนข้อมูลกลางภาครัฐที่มีความปลอดภัย โดยเฉพาะอย่างยิ่งข้อมูลสุขภาพส่วนบุคคล ที่กระทรวงสาธารณสุขได้เริ่มดำเนินการมาตั้งแต่ปี 2556 ถึงปัจจุบันถือได้ว่าเป็น big data ด้านสุขภาพ หรือ Health Data Center (HDC) ซึ่งเป็นข้อมูลที่มีความละเอียดอ่อนซับซ้อน และมีมูลค่าสูงอย่างที่มิอาจประเมินราคาได้ จำเป็นต้องมีการบริหารจัดการความเสี่ยงอย่างเคร่งครัดทั้งความเสี่ยงของข้อมูล ความเสี่ยงของผู้จัดเก็บข้อมูล และความเสี่ยงของผู้ใช้ข้อมูล หากข้อมูลถูกแก้ไขจากผู้ไม่ประสงค์ดี เช่น แก้ไขประวัติการแพ้ยา ซึ่งจากรายงานแนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศปี 2016 โดย Information Security Forum (ISF)[3] ได้ระบุทิศทางเชิงลบด้านความมั่นคงปลอดภัยทางไซเบอร์ (cyber) ยังคงต่อเนื่องใน 3 ประเด็นได้แก่

(1) ไม่มีใครน่าไว้วางใจในไซเบอร์อีกต่อไป

(2) ความเชื่อมั่นในระบบหรือโซลูชั่น (solution) การรักษาความมั่นคงปลอดภัยในแนวทางที่ยอมรับโดยทั่วไปเสื่อมสลายต้องคิดหาแนวทางใหม่

(3) ความล้มเหลวต่อการรักษาระดับการให้บริการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ดังนั้น ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) จึงต้องปรับกระบวนทัศน์ให้มีความสามารถในการปรับตัวเพื่อรองรับการเปลี่ยนแปลงและผลกระทบที่อาจจะเกิดขึ้นจากภัยคุกคามไซเบอร์ในรูปแบบใหม่ ๆ ตลอดเวลา

มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานที่พัฒนาขึ้นโดย ISO (International Organization for Standardization)[4] ได้รับการพัฒนามาจาก Information Security Management Standard BS7799 โดย British Standard Institute (BSI)[5] เป็นข้อกำหนดสำหรับการพัฒนาระบบการจัดการความมั่นคงปลอดภัยของข้อมูล (Information security management system: ISMS) ประกอบด้วยข้อกำหนดที่ครอบคลุมถึงการจัดทำนำไปปฏิบัติ ทบทวนและเฝ้าระวัง รักษาความต่อเนื่อง รวมถึงปรับปรุงระบบให้

สอดคล้องกับสถานการณ์ ผู้ที่ประยุกต์ใช้มาตรฐานนี้ต้องจัดทำเอกสารให้ครอบคลุมข้อกำหนดข้างต้น รวมถึงการดำเนินการที่สอดคล้องตามข้อกำหนดด้านระบบความมั่นคงปลอดภัยทั้งของลูกค้า ข้อกฎหมาย และระเบียบข้อบังคับต่าง ๆ ที่เกี่ยวข้องด้วย นอกจากมาตรฐานและระบบที่จัดทำขึ้นนี้จะต้องเหมาะสมกับความเสี่ยงเชิงธุรกิจขององค์กรเพื่อสร้างความมั่นใจถึงความมีประสิทธิผลและประสิทธิภาพของความมั่นคงปลอดภัยสารสนเทศ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีพันธกิจที่สำคัญในการขับเคลื่อนระบบเทคโนโลยีสารสนเทศด้านสุขภาพตามนโยบายการพัฒนาข้อมูลข่าวสารสุขภาพให้เป็นระบบเดียว เพื่อการบูรณาการข้อมูลผ่านระบบเชื่อมโยงแลกเปลี่ยนข้อมูลกลางภาครัฐที่มีความปลอดภัย โดยเฉพาะอย่างยิ่ง ข้อมูลสุขภาพรายบุคคลสำหรับจัดทำคลังข้อมูลสุขภาพในระดับจังหวัด กระทรวง ตั้งแต่ปี 2556 ถึงปัจจุบัน ถือเป็น big data สุขภาพ จัดที่เก็บไว้บนเซิร์ฟเวอร์จำลองส่วนตัว (virtual private server: VPS) ที่ศูนย์ปฏิบัติการ MOPH IDC นอกจากนั้นยังให้บริการ Co-location สำหรับหน่วยงานในสังกัดกระทรวงสาธารณสุข และบริการ web hosting สำหรับหน่วยงานต่าง ๆ ในสำนักงานปลัดกระทรวงสาธารณสุข ได้กำหนดการใช้งานระบบเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (server virtualization) เป็นเทคโนโลยีเครื่องคอมพิวเตอร์แม่ข่ายเสมือนของทาง VMware และได้กำหนดให้มีความมั่นคงปลอดภัยสารสนเทศโดยใช้การทำ RAID (redundant array of inexpensive disk) และมีระบบสำรองข้อมูลเพื่อป้องกันข้อมูลสูญหาย อีกทั้งด้านความปลอดภัยของระบบเครือข่ายภายในของระบบคอมพิวเตอร์แม่ข่ายเสมือนได้ใช้เทคโนโลยี ป้องกันการบุกรุกเสมือน (virtualization firewall) เพื่อป้องกันการโจมตีภายในระบบเครือข่ายเสมือนของระบบคอมพิวเตอร์แม่ข่ายเสมือน โดยได้แยกเครือข่ายภายใน เครือข่ายภายนอก และเครือข่ายสำหรับบริหารจัดการระบบออกจากกันให้มีประสิทธิภาพ สามารถทำงานได้อย่างต่อเนื่อง โดยใช้เทคโนโลยีเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (server virtualization) เข้ามาช่วยให้สามารถบริหารจัดการทรัพยากรที่มีอยู่ได้อย่างเต็มประสิทธิภาพ และลดเวลา downtimes ของระบบ รวมทั้งได้มีการดำเนินงานศูนย์สำรองฉุกเฉิน ที่ศูนย์โทรคมนาคมศรีราชาจังหวัดชลบุรี

ในขณะเดียวกันคณะรัฐมนตรีมีมติอนุมัติร่างพระราชบัญญัติว่าด้วยรัฐบาลดิจิทัล เมื่อวันที่ 2 ตุลาคม 2561[6] กำหนดให้หน่วยงานของรัฐต้องจัดทำข้อมูลตามภารกิจหลักให้อยู่ในรูปแบบข้อมูลดิจิทัล และต้องปรับปรุงข้อมูลดิจิทัลนั้นให้มีความน่าเชื่อถือได้ มีความสมบูรณ์และสามารถใช้ได้ รวมทั้งมีความถูกต้อง ทันสมัย สามารถเชื่อมโยงกับหน่วยงานของรัฐอื่นผ่านระบบเครือข่ายสารสนเทศและการสื่อสาร และนำไปประมวลผลต่อได้ด้วยนโยบายจากบริการต่าง ๆ ดังกล่าวข้างต้น กระทรวงสาธารณสุขจึงต้องเตรียมความพร้อมในด้านโครงสร้างพื้นฐานด้านเทคโนโลยี ดิจิทัล เพื่ออำนวยความสะดวกให้ประชาชนสามารถเข้าถึงบริการได้อย่างรวดเร็วและมั่นคงปลอดภัยในจุดเดียว

การศึกษานี้มีวัตถุประสงค์เพื่อวิเคราะห์และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของศูนย์ปฏิบัติการ MOPH IDC ภายใต้มาตรฐาน ISO/IEC 27001:2013 เพื่อนำข้อมูลที่ได้มาใช้จัดทำระบบบริหารความมั่นคงปลอดภัย และแนวทางปฏิบัติสำหรับผู้รับบริการของศูนย์ปฏิบัติการ MOPH IDC เพื่อสร้างความมั่นใจจะสามารถป้องกันการโจมตี และเมื่อมีการโจมตีเกิดขึ้นแล้วสามารถตอบสนองได้ทันท่วงที เพื่อให้การปฏิบัติงานได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมทั้งส่งผลให้เจ้าหน้าที่ ผู้รับบริการ และผู้มีส่วนได้ส่วนเสียเกิดการตระหนักถึงผลกระทบที่จะเกิดขึ้นจากความเสี่ยงที่เกิดขึ้น สร้างความมั่นใจถึงความมีประสิทธิผลและประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัย

วิธีการศึกษา

การดำเนินงานแบ่งได้เป็น 4 ขั้นตอน

1. ศึกษามาตรฐานการจัดการความมั่นคงปลอดภัย
2. วิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศของ

องค์กร

3. พัฒนาระบบบริหารความมั่นคงปลอดภัย แนวทางปฏิบัติในการรักษาความปลอดภัยทางด้านเทคโนโลยีสารสนเทศตามมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศISO/IEC27001:2013
4. จัดทำข้อเสนอแนะเพื่อสร้างแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ

ส่วนการประเมินผล ดำเนินการในช่วงเดือนมิถุนายน – กันยายน พ.ศ. 2561 ซึ่งเป็นการประเมินผลความพึงพอใจของผู้รับบริการระบบบริหารความมั่นคงปลอดภัย ภายใต้มาตรฐานISO/IEC 27001:2013 โดยใช้สถิติเชิงพรรณนา ได้แก่ ความถี่ และค่าเฉลี่ย ประชากรที่ใช้ในการประเมิน คือ ผู้ให้บริการรักษาความปลอดภัยภาคเอกชน เจ้าหน้าที่ไอทีของสำนักงานสาธารณสุขจังหวัด และเจ้าหน้าที่ของกรมอื่น ๆ ที่มาใช้บริการ โดยแยกเป็น 3 กลุ่ม จำนวนทั้งสิ้น 294 คน และผู้วิจัยได้จัดทำแบบสอบถาม เพื่อประเมินความพึงพอใจของผู้รับบริการ แบ่งเป็น 2 ส่วน คือ

ส่วนที่ 1 ปัจจัยส่วนบุคคลของผู้ตอบแบบสอบถาม

ส่วนที่ 2 ความพึงพอใจต่อคุณภาพของบริการที่ได้รับ ลักษณะแบบประเมิน มีการจำแนกลักษณะคำตอบเป็นมาตราส่วนประมาณค่า 5 อันดับ โดยเกณฑ์การแปลความหมายข้อมูลโดยการคำนวณค่าเฉลี่ยของข้อมูลแล้วนำค่าเฉลี่ยมาแปลความหมาย แบ่งเกณฑ์ค่าเฉลี่ยออกเป็น 5 ระดับ ดังนี้

- พึงพอใจน้อยที่สุด ค่าเฉลี่ยระหว่าง 1.00 – 1.50
- พึงพอใจน้อย ค่าเฉลี่ยระหว่าง 1.51 – 2.50
- พึงพอใจปานกลาง ค่าเฉลี่ยระหว่าง 2.51 – 3.50
- พึงพอใจมาก ค่าเฉลี่ยระหว่าง 3.51 – 4.50
- พึงพอใจมากที่สุดค่าเฉลี่ยระหว่าง 4.51 – 5.00

ผลการศึกษา

1. ศึกษามาตรฐานการจัดการความมั่นคงปลอดภัย

ผลการศึกษาแนวทางปฏิบัติและมาตรฐานด้านความมั่งคงปลอดภัยที่นิยม เช่น มาตรฐาน COSO ITIL CO-BIT ISMF และ ISO/IEC 27001:2013 พบว่า แผนแม่บท ICT Security แห่งชาติ พ.ศ. 2560-2564 ได้การกำหนดกระบวนงานตามมาตรฐาน ISO 27001 เพื่อเป็นกรอบแนวทางให้องค์กรและหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชน รวมถึงประชาชนผู้ใช้ระบบทั่วไป นำไปบังคับใช้เพื่อให้ข้อมูลและระบบเครือข่ายคอมพิวเตอร์ของประเทศมีความมั่นคงและปลอดภัยโดยรวม

ISO/IEC27001:2013 (Information Security Management System: ISMS) มาตรฐานการจัดการความมั่นคงปลอดภัยของสารสนเทศ ประกอบด้วยข้อกำหนดที่ครอบคลุมถึงการจัดทำ นำปฏิบัติ ทบทวนและเฝ้าระวังรักษาความต่อเนื่อง รวมถึงปรับปรุงระบบให้สอดคล้องกับสถานการณ์ผู้ที่ประยุกต์ใช้มาตรฐานนี้ต้องทำเอกสารให้ครอบคลุมข้อกำหนดและระบบที่จัดทำขึ้นนี้จะต้องเหมาะสมกับความเสี่ยงเชิงกระบวนการขององค์กร มาตรฐาน ISO/IEC 27001:2013 มีการพัฒนากรอบความคิดในแง่ของการบริหารจัดการ เพื่อให้มีการระบุถึงมุมมองของความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูลในแง่มุมของการดำเนินองค์กร ซึ่งได้แก่ การระบุถึงภัยคุกคามต่าง ๆ ที่องค์กรต้องเผชิญ เช่น ภัยคุกคามจากโลกไซเบอร์ การโจรกรรมข้อมูลส่วนบุคคล เป็นต้น ผู้วิจัยจึงได้ดำเนินการประเมิน gap analysis ผลการประเมินการวิธีการดำเนินการและมาตรการควบคุมที่เกี่ยวข้องกับการจัดการความมั่นคงปลอดภัยด้านสารสนเทศของศูนย์ปฏิบัติการ MOPH IDC เทียบกับข้อกำหนดของมาตรฐาน ISO/IEC 27001:2013 (gap analysis) ดังตารางที่ 1 แสดงให้เห็นว่า ณ ขณะที่ทำวิจัย การดำเนินงานยังไม่ค่อยสอดคล้องกับมาตรฐาน ISO/IEC 27001:2013 การจัดการความมั่นคงปลอดภัยด้านสารสนเทศไม่มีประสิทธิภาพการที่จะประยุกต์ใช้มาตรฐาน ISO/IEC 27001:2013 ในส่วนดังกล่าวต้องใช้เวลาและทรัพยากรอีกมาก

การควบคุมความมั่นคงปลอดภัยในภาพรวมจึงยังอยู่ในระดับที่จำเป็นต้องได้รับการปรับปรุงเกือบทุกด้าน โดยต้องกำหนดกระบวนการและกฎระเบียบที่ใช้ในการ

ตารางที่ 1 ระดับความสอดคล้องโดยรวมเทียบกับมาตรฐาน ISO/IEC27001:2013

	ระดับความสอดคล้อง (compliance level)						
ISO/IEC27001:2013	All	F	L	P	N	N/A	Percent
Requirements	22	4	3	7	8	0	37.88
Annex A	35	3	9	15	6	3	39.12
รวม	57	7	12	22	14	3	38.72

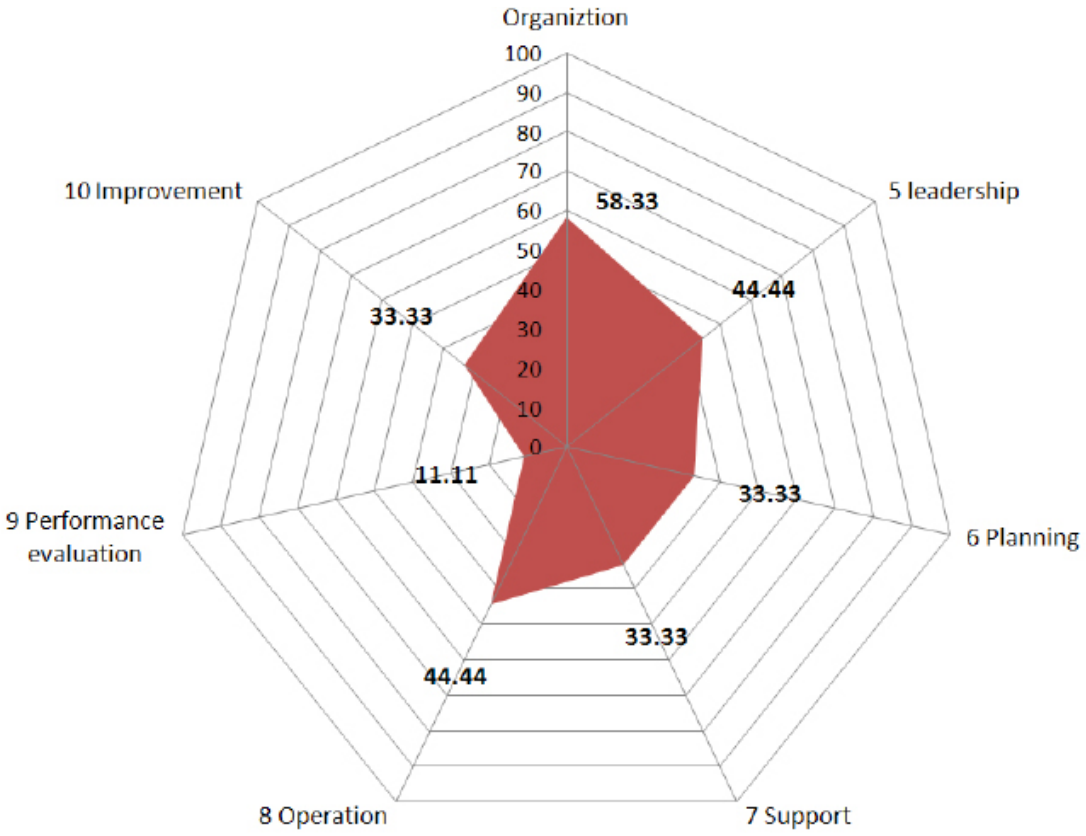
หมายเหตุ: N/A = not applicable; N = not conformed; P = partially conformed; L = largely conformed; F = fully conformed

ควบคุมความมั่นคงปลอดภัยสารสนเทศเพิ่มเติม รวมถึงต้องปรับปรุงการควบคุมทางเทคนิค ให้เป็นมาตรฐานเดียวกัน เพื่อให้ง่ายต่อการบริหารจัดการและการปฏิบัติงานของแต่ละกลุ่มดำเนินการตามระเบียบและคำสั่งทางราชการที่เกี่ยวข้อง ซึ่งส่วนใหญ่ไม่ได้กล่าวถึงการควบคุมความมั่นคงปลอดภัยสารสนเทศ ทำให้ไม่มีระเบียบแบบแผนที่ชัดเจนในการดำเนินการควบคุมความมั่นคงปลอดภัยในส่วนต่าง ๆ

การประเมินระดับความสอดคล้องแยกตามข้อกำหนดหลักของมาตรฐาน ISO/IEC27001:2013 พบว่า ศูนย์ปฏิบัติการ MOPH IDC ยังไม่ค่อยสอดคล้องกับมาตรฐาน ISO/IEC 27001:2013 (ภาพที่ 1) ซึ่งหมายความว่า การจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ยังไม่มีประสิทธิภาพเท่าที่ควร

เปรียบเทียบข้อมูลที่รวบรวมได้กับรายการของมาตรการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศ

ภาพที่ 1 ระดับความสอดคล้องแยกตามข้อกำหนดหลักของมาตรฐาน ISO/IEC27001:2013



หมวด A.5 ถึง A.18 พบว่าศูนย์ปฏิบัติการ MOPH IDC ในปัจจุบันยังไม่ค่อยสอดคล้องกับมาตรฐาน ISO/IEC 27001:2013 (ภาพที่ 2) ส่งผลให้การจัดการความมั่นคงปลอดภัยด้านสารสนเทศสุขภาพไม่มีประสิทธิภาพ โดยเฉพาะการวิเคราะห์และระบุความต้องการในส่วนของความมั่นคงปลอดภัยด้านสารสนเทศสุขภาพ A14 กับ A16 ไม่มีการดำเนินงาน

2. วิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร

การบริหารความเสี่ยง (risk management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลงหรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ซึ่งการจัดการความเสี่ยงอาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลักคือการยอมรับการลด/ควบคุม การยกเลิกและการโอนย้ายหรือแบ่งความเสี่ยง

การจัดระดับความเป็นไปได้ที่จะเกิดภัยคุกคามซึ่งใช้ประโยชน์จากช่องโหว่ที่เอื้อเฉพาะแบ่งตามตารางที่ 2

ในการประเมินความเป็นไปได้ของภัยคุกคามที่ใช้ประโยชน์จากช่องโหว่ จะต้องพิจารณาปัจจัยต่อไปนี้

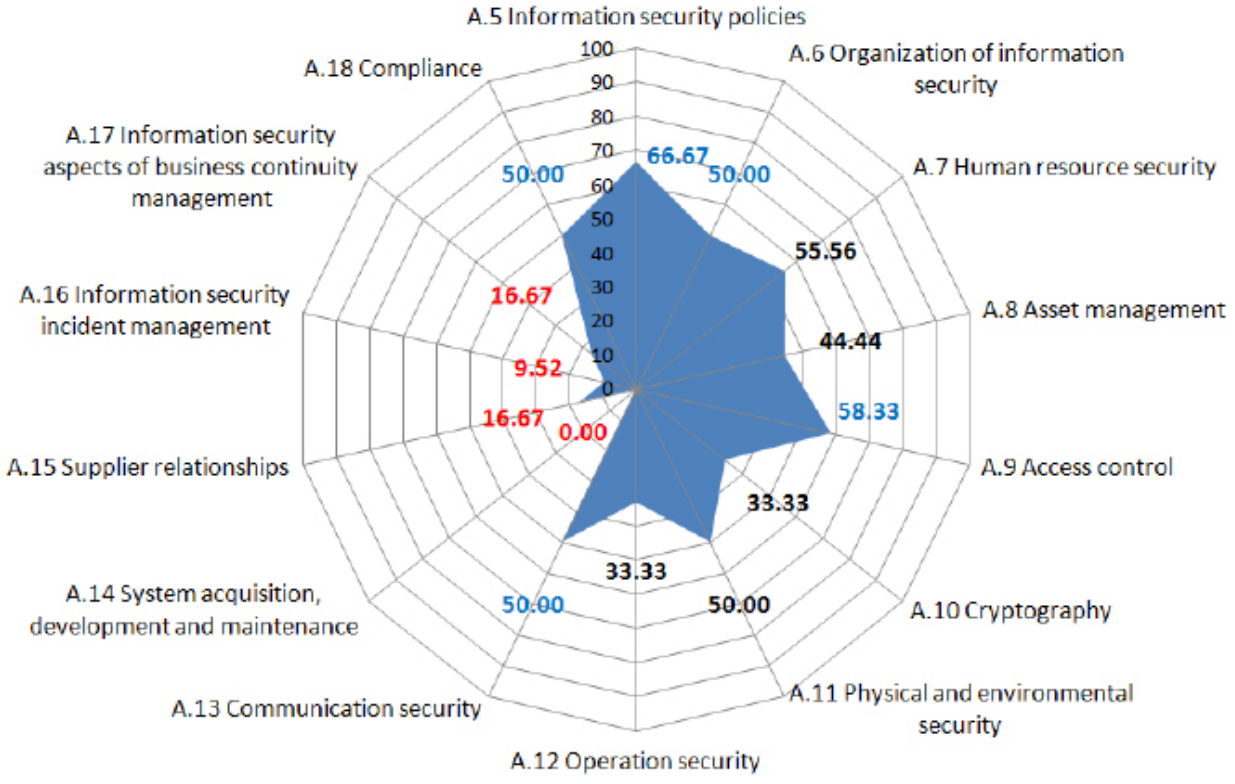
- เหตุการณ์ละเมิดความปลอดภัยในอดีตที่ ศทส. เคยประสบ
- ภัยคุกคามจากสิ่งแวดล้อมในองค์กร ภัยคุกคามที่กระทำโดยเจตนา และภัยคุกคามที่เกิดขึ้นโดยไม่ได้ตั้งใจ
- แรงจูงใจ ประสิทธิภาพที่รับรู้และจำเป็นทรัพยากรที่เอื้อต่อผู้บุกรุกการรับรู้ถึงประโยชน์ที่จะได้รับ เตรียมการป้องกันและมาตรการควบคุมให้พร้อมเพื่อบรรเทาความเป็นไปได้ที่จะเกิดขึ้น

การจัดระดับผลกระทบต่อธุรกิจ (impact)

ในการกำหนดระดับความเสียหายที่มีต่อธุรกิจ ได้พิจารณาการประเมินมาตรการควบคุมที่ใช้งานอยู่ในปัจจุบันก่อน แล้วจึงพิจารณาผลอันอาจจะเกิดมาจากเกิดความไม่ปลอดภัยที่ส่งผลต่อข้อมูล ซึ่งระดับผลกระทบพิจารณาจากผลลัพธ์ของการสูญเสีย ดังนี้

- การสูญเสียความลับ (loss of confidentiality) การ

ภาพที่ 2 แสดงระดับความสอดคล้องแยกตามหมวดของมาตรการควบคุมใน Annex A



ตารางที่ 2 ระดับการประเมินความเป็นไปได้ของภัยคุกคาม-ช่องโหว่

ระดับ	คำอธิบาย
1	ภัยคุกคามซึ่งไม่มีแนวโน้มที่จะใช้ประโยชน์จากช่องโหว่ **มีไม่ถึง 1 ครั้งต่อปี** หรือมีระดับความเป็นไปได้ที่จะก่อให้เกิดความเสียหาย **"ต่ำ"**
2	ภัยคุกคามซึ่งมีแนวโน้มที่จะใช้ประโยชน์จากช่องโหว่ **หนึ่งครั้งต่อปี** หรือมีระดับความเป็นไปได้ที่จะก่อให้เกิดความเสียหาย **"ปานกลาง"**
3	ภัยคุกคามซึ่งมีแนวโน้มที่จะใช้ประโยชน์จากช่องโหว่ **มากกว่าหนึ่งครั้งต่อปี** หรือมีระดับความเป็นไปได้ที่จะก่อให้เกิดความเสียหาย **"สูง"**

เปิดเผยทรัพย์สินประเภทข้อมูลหรือการเข้าถึงระบบโดยไม่ได้รับอนุญาตหรือการแทรกแซงข้อมูล

- การสูญเสียความสมบูรณ์ (loss of integrity) ข้อมูลหรือการทำงานระบบ ไม่ถูกต้องและสมบูรณ์
- การสูญเสียความพร้อมใช้งาน (loss of availability) ผู้ใช้ไม่สามารถใช้ประโยชน์จากข้อมูลหรือระบบที่สำคัญในเวลาที่ต้องการได้

การจัดระดับแยกตามทรัพย์สินหรือชุดของทรัพย์สินและคู่ของภัยคุกคามกับช่องโหว่ ใช้แบบฟอร์มประเมินความเสี่ยงและควบคุมแก้ไขความเสี่ยง (risk assessment & risk treatment form) ซึ่งกำหนดระดับผลกระทบต่อธุรกิจ ดังตารางที่ 3

การประเมินความเสี่ยง

การจัดระดับความเสี่ยงควรแบ่งตามกลุ่มทรัพย์สินที่มีประเภทเดียวกัน และคู่ของภัยคุกคามกับช่องโหว่โดยพิจารณาจากผลกระทบต่อธุรกิจและความเป็นไปได้ที่อาจจะเกิดขึ้นดังแสดงในตารางที่ 4

การจัดการความเสี่ยง

ในการจัดการความเสี่ยงต้องพิจารณาถึงการกำหนดและการคัดเลือกมาตรควบคุมเพื่อใช้ในจัดการทรัพย์สินที่มีค่าความเสี่ยงอยู่ในระดับสูง ซึ่งในการจัดการความเสี่ยงของ ศทส. นั้น พิจารณาระดับความเสี่ยงที่มีค่าระดับดังนี้

ตารางที่ 3 ระดับผลกระทบ (impact)

ระดับ	ระดับผลกระทบ	ผลกระทบ
0	ไม่มีผลกระทบ	ไม่มีผลกระทบ
1	น้อย (L)	ได้รับความเสียหายไม่เกิน 100,000 บาท หรือ ทรัพย์สินประสิทธิภาพการทำงานลดลงหรือหยุดชะงักบางส่วน แต่การให้บริการยังสามารถดำเนินการได้ แก้ไขได้ในช่วงเวลาภายใน 4 ชั่วโมง หรือมีการเผยแพร่ข่าวในวงจำกัดภายในกลุ่ม หรือมีการดำเนินลงโทษทางวินัยระดับกลุ่ม
2	ปานกลาง (M)	ได้รับความเสียหายไม่เกิน 500,000 บาท หรือทรัพย์สินและการให้บริการหยุดชะงัก แก้ไขได้ในช่วงเวลาภายใน 4 ชั่วโมง หรือมีการเผยแพร่ข่าวในวงจำกัดภายในแผนก หรือมีการเผยแพร่ข่าวภายในศูนย์ฯและกระทรวงฯ หรือมีการดำเนินลงโทษทางวินัยระดับศูนย์ฯ และกระทรวงฯ
3	มาก (H)	ได้รับความเสียหายมากกว่า >500,000 บาท หรือทรัพย์สินและการให้บริการหยุดชะงัก ต้องใช้เวลาแก้ไขมากกว่า 4 ชั่วโมงขึ้นไป หรือมีการเผยแพร่ข่าวออกสู่ภายนอก หรือมีการดำเนินคดีทางกฎหมาย อาจมีโทษจำคุกหรือถูกปรับ

ตารางที่ 4 การประเมินความเสี่ยง

ความเป็นไปได้ของภัยคุกคาม-ช่องโหว่	Impact Level			
	N(0)	L (1)	M (2)	H (3)
น้อย (1)	0	1	2	3
ปานกลาง (2)	0	2	4	6
มาก (3)	0	3	6	9

- ระดับ 0-3 สามารถยอมรับได้
- ระดับ 4-5 ควรต้องมีการหามาตรการควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- ระดับ 6-9 เป็นระดับความเสี่ยงที่ไม่สามารถยอมรับได้ ต้องมีการหามาตรการควบคุม เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยเร่งด่วน

ผลการวิเคราะห์ความเสี่ยงแสดงในตารางที่ 5 ความเสี่ยงของรายการประเมินความเสี่ยงที่เกินระดับ

ตารางที่ 5 การวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศของศูนย์ปฏิบัติการ MOPH IDC

รายการ	ภัยคุกคาม	Impact	Likeli-hood	Risk level	Residual risk level	Treatment reference
1. Password admin	เอกสารที่มีชั้นความลับเผยแพร่ไปสู่สาธารณะ อาจะทำให้ถูกโจมตีได้	3	2	6	3	A.12.3.1 การสำรองข้อมูล (Information backup)
2. Configuration file	ข้อมูลเสียหายหรือสูญหาย ไม่พร้อมใช้งาน	3	2	6	2	
3. Form ที่กรอกข้อมูลแล้วอยู่ในระดับ secret	ผู้ไม่มีสิทธิสามารถเข้าถึง แก้ไข หรือเปิดเผยข้อมูล	2	3	6	2	A.8.2 Information classification
4. Access right matrix	ข้อมูลไม่เป็นปัจจุบัน จนเกิดนำไปใช้ปฏิบัติงานผิดพลาด	2	3	6	2	A.12.1.4 Separation of development, testing and operational environments
Operating System	มีการร้องขอการใช้งานเกิน license ที่มี	3	2	6	3	A.12.1.3 การบริหารจัดการขีดความสามารถของระบบ (capacity management)
	ระบบเกิดเหตุขัดข้องทางความมั่นคงปลอดภัยสารสนเทศ	3	2	6	3	A.12.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (management of technical vulnerabilities)
เครื่องกำเนิดไฟฟ้า	เครื่องกำเนิดไฟฟ้าถูกทำลายจากผู้ประสงค์ร้าย	3	2	6	3	A.11.2.1 การจัดวางและการป้องกันอุปกรณ์ (equipment setting and protection)
เครื่องปรับอากาศควบคุมความชื้น	compressor ถูกทำลายจากผู้ประสงค์ร้าย	3	2	6	3	

0-3 (ระดับที่สามารถยอมรับได้) ดำเนินการจัดทำตามระเบียบปฏิบัติ เรื่องการแก้ไขและควบคุมความเสี่ยง (risk treatment procedure) โดยนำมาตรการที่เกี่ยวข้องมาประยุกต์ใช้งานเพื่อการลดโอกาสเกิด และลดผลกระทบจากภัยคุกคามเหล่านั้น มีการติดตามผล ทบทวนแผนจัดการความเสี่ยง และประเมินความเสี่ยงภายหลังการจัดการความเสี่ยง รวมทั้งตรวจสอบและทบทวนความเสี่ยงที่เหลืออยู่ เพื่อนำเสนอในการประชุมของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารพิจารณา รวมทั้งความเสี่ยงที่ไม่สามารถดำเนินการได้จำเป็นต้องยกเลิกการยอมรับ หรือการโอนย้ายความเสี่ยง เช่น การเฝ้าระวังภัยคุกคามไซเบอร์ประสานให้ไทยเซิร์ตเป็นผู้เฝ้าระวังภัยคุกคามไซเบอร์ดำเนินการให้ส่วนหนึ่ง

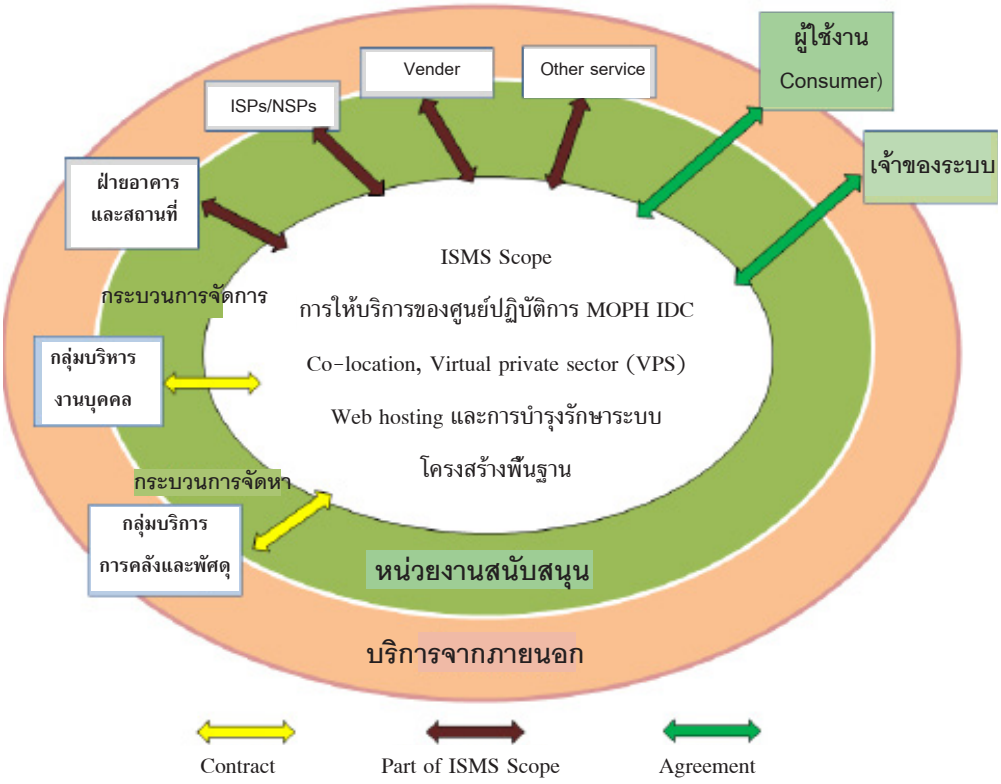
หลังจากการจัดการความเสี่ยงตามแผนการจัดการความเสี่ยง (risk treatment plan) ที่กำหนดแล้วความเสี่ยงที่เหลืออยู่ อยู่ในเกณฑ์ที่ยอมรับได้

3. พัฒนาระบบบริหารความมั่นคงปลอดภัย แนวทางปฏิบัติในการรักษาความปลอดภัยทางด้านเทคโนโลยีสารสนเทศตามมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001

ดำเนินการวิเคราะห์และประเมินเทคโนโลยีที่ใช้ของระบบที่มีความสำคัญต่อภารกิจและการบริการได้แก่ การให้บริการ co-location, virtual private server (VPS) และ web hosting รวมถึงการดำเนินงานและการบำรุงรักษาระบบโครงสร้างพื้นฐานและระบบสนับสนุนที่จำเป็นในการให้บริการ (infrastructure, facilities and supporting systems) รายละเอียดของขอบเขตการรับรองระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Scope) แสดงในภาพที่ 3

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศให้บริการครอบคลุมถึง

ภาพที่ 3 ขอบเขตการขอการรับรอง



1) การให้บริการห้องคอมพิวเตอร์แม่ข่าย (Server) เพื่อเป็น Co-Location

- การบริการเชื่อมโยงเครือข่ายสำหรับเครื่องคอมพิวเตอร์แม่ข่าย
- การบริการเชื่อมโยง Internet สำหรับเครื่องคอมพิวเตอร์แม่ข่าย
- การบริการสิ่งอำนวยความสะดวก (facility management)
- การบริหารความมั่นคงปลอดภัยสารสนเทศ (security management)

2) การให้บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (virtual private server (VPS))

- การบริการพื้นที่จัดทำเครื่องแม่ข่ายเสมือนสำหรับหน่วยงานในกระทรวงสาธารณสุข เพื่อจัดทำระบบข้อมูลสุขภาพระบบทรัพยากรด้านสาธารณสุข เป็นต้น
- การบริการเชื่อมโยง Internet สำหรับเครื่องคอมพิวเตอร์แม่ข่าย
- การบริการสิ่งอำนวยความสะดวก (facility management)
- การบริหารความมั่นคงปลอดภัยสารสนเทศ (security management)

3) การให้บริการ Web hosting

- ให้บริการพื้นที่ในการจัดทำ website ของหน่วยงาน
- การบริการเชื่อมโยง Internet สำหรับเครื่องคอมพิวเตอร์แม่ข่าย
- การบริหารความมั่นคงปลอดภัยสารสนเทศ (Security Management)
- การบริการดูแลช่วยเหลือ (help desk)

4) การบำรุงรักษาระบบโครงสร้างพื้นฐานและสนับสนุนที่จำเป็นในการให้บริการ (Its infrastructure, facilities and supporting systems)

- การบำรุงรักษาระบบโครงสร้างพื้นฐานและสนับสนุนที่จำเป็นในการให้บริการต่าง ๆ
- การบริหารจัดการทรัพยากรบุคคลของหน่วยงานที่ดูแลการให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- การจัดหาระบบ/ฮาร์ดแวร์/ซอฟต์แวร์/บริการ/และอุปกรณ์ประกอบอื่น ๆ เพื่อสนับสนุนการให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่กล่าวมาข้างต้น

นโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (information security management system policy statement) เป้าหมายของนโยบายเพื่อป้องกันสินทรัพย์สารสนเทศ (information assets) ที่เกี่ยวข้องกับการให้บริการระบบสารสนเทศและการสื่อสารของศูนย์ปฏิบัติการ MOPH IDC จากภัยคุกคามภายในและภายนอกที่อาจเกิดขึ้น ทั้งที่โดยเจตนาหรือไม่เจตนาก็ตาม เพื่อแสดงถึงคุณภาพในการบริหารความมั่นคงปลอดภัย จึงได้ประกาศนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS policy) ดังนี้

ข้อ 1 กำหนดนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ((Information Security Management System Policy: ISMS Policy) และให้การสนับสนุนในเรื่องนโยบายงบประมาณทรัพยากรและอื่น ๆ ที่จำเป็น เพื่อให้ระบบบริหารความมั่นคงปลอดภัยสารสนเทศมีการพัฒนาและปรับปรุงอย่างต่อเนื่อง

ข้อ 2 แต่งตั้งผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Representative: ISMR) และคณะทำงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศเพื่อรับผิดชอบในการขับเคลื่อนระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

ข้อ 3 นโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS policy) ผู้บริหารระดับสูงกำหนดนโยบายการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ พร้อมทั้งอนุมัติและประกาศใช้นโยบายดังกล่าวเป็นกลไกให้มั่นใจว่าโครงการนี้ได้รับการสนับสนุนอย่างเป็นรูปธรรมและเป็นสัญญาณว่า ISMS ได้เริ่มอย่างเป็นทางการแล้วได้จัดทำเอกสารต่าง ๆ ตาม ISO/IEC

27001:2013

ข้อ 4 การบริหารความมั่นคงปลอดภัยสารสนเทศต้องดำเนินการประเมินและบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศตามคู่มือการบริหารจัดการความเสี่ยงสารสนเทศที่ได้รับการอนุมัติจาก คณะกรรมการอำนวยการระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศ

4. จัดทำข้อเสนอแนะเพื่อสร้างแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ

จากการดำเนินงานการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศด้วยมาตรฐาน ISO/IEC 27001:2013 ในปี 2560 ถึงปัจจุบันถึงแม้ว่าการจัดทำนโยบายและหลักการปฏิบัติความมั่นคงปลอดภัยระบบสารสนเทศได้ดำเนินการตามขั้นตอนและกระบวนต่าง ๆ ตามมาตรฐาน ISO/IEC 27001:2013 แล้ว เพื่อเป็นการสร้างความมั่นใจต่อการปฏิบัติงานของเจ้าหน้าที่ และความเชื่อมั่นจากผู้รับบริการว่าข้อมูลและสารสนเทศยังถูกเก็บรักษาอย่างปลอดภัยและเข้าถึงได้ตามสิทธิของตน จึงได้ดำเนินการใน 2 เรื่อง ดังนี้

1) ขอการรับรองคุณภาพมาตรฐาน ISO/IEC 27001:2013 โดยผลการตรวจสอบในวันที่ 9-11 สิงหาคม 2560 พบความไม่สอดคล้องกับข้อกำหนดมาตรฐาน ISO/IEC 27001:2013 ในปี 2560 จำนวน 3 เรื่อง

(1) Information security risk assessment was not effective (6.1.2)

(2) NDA has not been signed by some external parties who had accessed data center (A13.2.4)

(3) CCTV record in data center has not been kept for a defined retention time (A11.1.3)

ได้นำขั้นตอนตามระบบ PMQA มาปรับปรุงกระบวนการ เริ่มต้นจากวิเคราะห์ความเสี่ยง ทบทวนปรับปรุงขั้นตอน จัดทำผังการดำเนินงาน พร้อมขอการรับคุณภาพมาตรฐาน ISO/IEC 27001:2013 ในปี 2561 พบความไม่สอดคล้องกับข้อกำหนดฯ จำนวน 1 เรื่อง Clock of CCTV is incorrect (A.12.4.4)

2) นำผลการวิเคราะห์ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เพื่อปรับปรุงแนวทางปฏิบัติในการรักษาความมั่นปลอดภัยสารสนเทศ ภายใต้มาตรฐาน ISO/IEC 27001:2013 ที่เหมาะสมกับศูนย์ปฏิบัติการ MOPH IDC เพื่อให้เกิดประโยชน์และสามารถนำไปใช้ได้จริง ผลการวิเคราะห์ของกลุ่มตัวอย่างใช้สถิติเพื่อหาค่าร้อยละค่าเฉลี่ยสรุปได้ดังนี้

กลุ่มที่ 1 ผู้ใช้บริการ VM (virtual machine) และ web hosting ตอบแบบสอบถามคิดเป็นเพศชาย คิดเป็นร้อยละ 86.1 เพศหญิง ร้อยละ 13.9 อายุ ระหว่าง 31 – 40 และ 41 -50 ปี คิดเป็นร้อยละ 37.6 ปีเท่ากัน รองลงมามีอายุระหว่าง 51 ปีขึ้นไป คิดเป็นร้อยละ 14.9 ปี มีการศึกษาระดับปริญญาตรี ร้อยละ 71.3 รองลงมาเป็นระดับการศึกษาสูงกว่าปริญญาตรีส่วนใหญ่เป็นข้าราชการ คิดเป็นร้อยละ 66.3 และพนักงานราชการของรัฐ (ส่วนใหญ่อยู่ส่วนภูมิภาค) มีประสบ การณ์ในการทำงานตั้งแต่ 5-10 ปี และ 11 – 15 ปี คิดเป็นร้อยละ 22.8 และ 21.8 ตามลำดับ มีการติดต่อประสานงาน โดยเฉลี่ยมากกว่า 10 ครั้ง ตั้งแต่เดือนตุลาคม 2560 จนถึงมิถุนายน 2561

ประเด็นวัดความพึงพอใจ การให้บริการ VM และผู้ใช้บริการ web hosting ภาพรวม พบว่าผู้ใช้บริการจำแนกเพศ ระดับการศึกษา และอาชีพ มีความพึงพอใจให้บริการเหมือนกันทุกกลุ่ม ยกเว้นผู้มีอายุ 51 ปีขึ้นไป มีความพึงพอใจ VM มีคะแนนเฉลี่ย 4.17 ส่วนผู้มีอายุ 20 – 30 ปี ความพึงพอใจ web hosting มีคะแนนเฉลี่ย 4.46

กลุ่มที่ 2 ผู้ให้บริการ (vendors) ตอบแบบสอบถามคิดเป็นเพศชาย คิดเป็นร้อยละ 82.6 เพศหญิง ร้อยละ 17.6 อายุระหว่าง 31 – 40 และ 41 -50 ปีคิดเป็นร้อยละ 41.3 ปี เท่ากัน รองลงมามีอายุระหว่าง 41-50 ร้อยละ 32.6 ปีการศึกษาระดับปริญญาตรี ร้อยละ 80.4 รองลงมาเป็นมีระดับการศึกษาสูงกว่าปริญญาตรีร้อยละ 19.6 ส่วนใหญ่เป็นพนักงานเอกชน คิดเป็นร้อยละ 69.6

และพนักงานของรัฐ ร้อยละ 26.1

ประเด็นวัดความพอใจของผู้ให้บริการพบว่า การให้บริการด้านระบบและอุปกรณ์มีระดับความพึงใจมาก มีคะแนนเฉลี่ย 4.17 ด้านการ support ของเจ้าหน้าที่ สป.มีระดับความพึงใจมาก มีคะแนนเฉลี่ย 4.19 และด้านความสะดวกมีระดับความพึงใจมาก มีคะแนนเฉลี่ย 4.17 ภาพรวมในการทำงานร่วมกันสำนักงานปลัดกระทรวงสาธารณสุขมีระดับความพึงใจมาก มีคะแนนเฉลี่ย 4.15 สรุปได้ว่าผู้ให้บริการมีระดับความพึงใจมาก มีคะแนนเฉลี่ย 4.17

กลุ่มที่ 3 ผู้รับบริการบุคคลทั่วไปตอบแบบสอบถาม คิดเป็นเพศชาย คิดเป็นร้อยละ 63.3 เพศหญิง ร้อยละ 36.7 อายุ ระหว่าง 41 -50 ปี คิดเป็นร้อยละ 37.4 รองลงมา 31 – 40 ปี คิดเป็นร้อยละ 32.0 การศึกษาระดับปริญญาตรี และระดับการศึกษาสูงกว่าปริญญาตรี คิดเป็นร้อยละ ร้อยละ 64.6 และ 32.7 ตามลำดับ ส่วนใหญ่เป็นส่วนราชการคิดเป็นร้อยละ 58.0 รองลงมาเป็นพนักงานของรัฐ ร้อยละ 40.0 ประสบการณ์ในการทำงานตั้งแต่ 15 ขึ้นไป และ 5-10 ปี คิดเป็นร้อยละ 43.5 และ 23.1 ตามลำดับ

ประเด็นวัดความพอใจผู้รับบริการบุคคลทั่วไปพบว่า เพศชาย อายุระหว่าง 41- 50 ปี และระดับการศึกษาปริญญาตรี ระดับความพึงใจมาก ด้านการให้บริการของเจ้าหน้าที่/บุคลากรที่ให้บริการด้านกระบวนการ ขั้นตอนการให้บริการความพึงพอใจของบุคลากรทั่วไป ด้านสิ่งอำนวยความสะดวกด้านผลจากการให้บริการด้านนโยบายความมั่นคงปลอดภัยมีความพึงพอใจ มีคะแนนเฉลี่ย 4.05 มากกว่าเพศหญิง มีคะแนนเฉลี่ย 4.05 ระดับการศึกษาปริญญาตรี มีความพึงพอใจสูงสุด มีคะแนนเฉลี่ย 4.17 รองลงมาเป็นผู้มีการศึกษาระดับสูงกว่าปริญญาตรี และอนุปริญญา มีความพึงใจ มีคะแนนเฉลี่ย 3.55 และ มีคะแนนเฉลี่ย 3.40 ตามลำดับผู้มีอายุระหว่าง 51 ปีขึ้นไป ความพึงพอใจ มีคะแนนเฉลี่ย 4.17 สูงกว่ากลุ่มอายุอื่น ๆ

วิจารณ์

ด้วยเทคโนโลยีที่เปลี่ยนแปลงรวดเร็วไม่ว่าจะเป็น Artificial Intelligence (AI), Internet of Thing (IoT), Machine learning, Blockchain ฯลฯ ทำให้ผู้ใช้เกิดความเชื่อมั่นในการใช้เทคโนโลยีต่าง ๆ และส่งผลให้สามารถนำเทคโนโลยีเหล่านั้นมาสนับสนุนการทำงานได้อย่างมีประสิทธิภาพ แต่ขาดความตระหนักถึงความมั่นคงปลอดภัยและความเป็นส่วนตัว จึงควรวางมาตรการควบคุมและสร้าง digital literacy ในทุกกลุ่มที่เกี่ยวข้องโดยเฉพาะบุคลากรภายใน รวมถึงการนำ AI ซึ่งกระทรวงฯ มีแนวทางการนำมาใช้เพื่อให้ประชาชนสามารถเข้าถึงข้อมูล เนื่องจาก AI มีการเก็บข้อมูลผู้ใช้ตลอดเวลา ทำให้สามารถเรียนรู้และเลือกสรรสิ่งที่เหมาะสมให้แก่ผู้ใช้โดยที่ไม่ต้องทำอะไรมาก ซึ่งอาจกลายเป็นช่องทางใหม่ให้แฮ็คเกอร์ขโมยข้อมูล เนื่องจาก AI มักเก็บข้อมูลส่วนบุคคลเป็นจำนวนมาก ดังนั้น จำเป็นต้องมีมาตรป้องกันระดับประเทศเพื่อจำกัดและควบคุมการเข้าถึงข้อมูลส่วนบุคคลที่มาจากทั่วประเทศ

เอกสารหลักฐาน (documented information) ข้อมูลเอกสารที่จำเป็นสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศมีการควบคุมเพื่อให้มั่นใจว่ามีการป้องกันควบคุมบำรุงรักษาและจัดการเอกสารให้เป็นไปตามคู่มือระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศ พบว่าเมื่อมีการแจกจ่ายไปแล้ว เวลามีการปรับปรุงต้องเก็บเอกสารเก่าด้วยควรมีการทบทวนขั้นตอนเอกสาร

กระบวนการวิเคราะห์สถานภาพและประเมินผลกระทบของภัยคุกคาม ทำให้ทราบถึงปัญหา แนวทางและวิธีปฏิบัติต่าง ๆ ซึ่งในบางข้อการควบคุมที่ศูนย์ปฏิบัติการ MOPH IDC เช่น การให้บริการ VM (virtual machine) ผลการสำรวจอยู่ในระดับความพึงใจมาก แต่มีคะแนนเฉลี่ย 3.89 เท่านั้น ควรนำผลการสำรวจมาจัดทำเป็นแนวทางการปฏิบัติในการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ และตรวจสอบการดำเนินงานอย่างเป็นระบบ มาตรฐาน ISO/IEC 27001:2013 สำหรับการสำรวจความเห็น ต้องพิจารณากลุ่มเป้าหมายเนื่องจาก

ผู้ตอบแบบสอบถามอาจทำหลายหน้าที่และมีความรู้ความเข้าใจแต่ละเรื่องที่แตกต่างกัน ต้องปรับปรุงคำถามให้เหมาะสมเพื่อให้ผลจากการตอบแบบสอบถามเป็นผลที่นำมาวิเคราะห์ได้จริง เพื่อการเตรียมความพร้อมนำมาปรับปรุงมาตรการ และแก้ไขให้ตรงจุดและลดระยะเวลาในการดำเนินการได้อย่างเหมาะสม ตรงกับความเห็นของเอกวิทย์ พิทักษ์คชวงษ์ ซึ่งวิจัยเรื่อง การสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสารสนเทศภายใต้มาตรฐาน ISO/IEC27001:2013 พบว่าการประเมินความเสี่ยงมีความสำคัญเพราะทำให้ได้ทราบถึงความเสี่ยงต่าง ๆ ที่อาจจะเกิดขึ้นกับทรัพย์สินขององค์กรจึงต้องนำความเสี่ยงนั้นไปกำหนดแนวทางนโยบายในการบริหารความเสี่ยงที่เกิดขึ้นได้อย่างถูกต้องได้รับความร่วมมือจากผู้บริหารและคณะทำงานเป็นอย่างดีทำให้การดำเนินโครงการเป็นไปอย่างราบรื่น[7]

นโยบายในการพัฒนาข้อมูลข่าวสารสุขภาพให้เป็นระบบเดียว และทุกหน่วยงานสามารถแลกเปลี่ยนข้อมูลสุขภาพร่วมกันได้ (health information exchange - HIE) ได้ใช้ระบบ Cloud ทำให้มีการค้นหาวิธีในการโจมตีในระดับ hypervisor ของ virtual machine จากการสำรวจทรัพย์สินพบว่าซอฟต์แวร์ที่หมดอายุ หรือไม่มีการ update เสี่ยงต่อการใช้เป็นช่องโหว่ในการเจาะระบบอีกทางหนึ่งได้ ดังนั้นจำเป็นต้องพิจารณาถึงภัยคุกคามไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้วย เพื่อให้การปกป้องรับมือป้องกันและลดความเสี่ยงด้านความมั่นคงปลอดภัยคุกคามด้านความมั่นปลอดภัยไซเบอร์ หรือ cyber security ตลอดจนการละเมิดความปลอดภัยของระบบคอมพิวเตอร์

แม้ว่า ศูนย์ปฏิบัติการ MOPH IDC มีแนวทางปฏิบัติในการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศในระดับเบื้องต้นแล้ว ภัยคุกคามรูปแบบอื่น ๆ มีแนวโน้มเพิ่มขึ้นอย่างรวดเร็วมีความซับซ้อนและมีความรุนแรงมากขึ้นทุกขณะถือเป็นแนวโน้มที่ส่งผลกระทบอย่างยิ่งต่อคุณภาพชีวิตหรือการให้บริการของหน่วยงานและรักษาไว้ซึ่งความสามารถในการดำเนินงานได้อย่างต่อเนื่อง ทั้งนี้ควรพัฒนาและขยายขอบเขตการดำเนินงานให้ครอบคลุมระบบเครือข่ายกลางที่ถือเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศของกระทรวงฯ การพัฒนาศักยภาพด้านการรับมือภัยคุกคามไซเบอร์ การปฏิบัติตามแนวทางการกำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ และแนวปฏิบัติเพื่อรับมือและตอบสนองต่อสถานการณ์ฉุกเฉินทางด้านความมั่นคงปลอดภัยไซเบอร์ แนวทางการพัฒนาบุคลากรที่สภาความมั่นคงแห่งชาติกำหนด ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564[8] ได้กำหนดให้กระทรวงสาธารณสุขรับผิดชอบโครงสร้างพื้นฐานสำคัญทางสารสนเทศของกลุ่มสาธารณสุข บุคลากรอาจเห็นว่า ศทส. ได้การรับรองมาตรฐาน ISO/IEC 27001:2013 จนไม่ดำเนินการตามนโยบายฯ โดยเฉพาะในมาตรการด้านการบริหารจัดการด้านการสื่อสารและการดำเนินการของเครือข่าย จากผลการวิจัยของรัชชา ภรณ์สุภาพ และศักดิ์ชาย ตั้งวรรณวิทย์ เรื่องการจัดทำแนวทางการปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศด้วยมาตรฐาน ISO/IEC 27001 เพื่อลดความเสี่ยงต่าง ๆ ในการดำเนินงานด้านเทคโนโลยีสารสนเทศขององค์กรโดยการนำมาตรฐาน ISO/IEC 27001 มาประยุกต์ใช้นั้น พบว่าควรต้องมีสื่อสารกับเจ้าหน้าที่ทุกระดับ เนื่องจากพบว่าเจ้าหน้าที่ภายในองค์กรส่วนมากยังไม่ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร ISO/ICE 27001 และองค์กรควรมีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและจัดทำนโยบายความมั่นคงปลอดภัย[9] ดังนั้น การที่ ศูนย์ปฏิบัติการ MOPH IDC ได้การรับรองตามมาตรฐาน ISO/IEC 27001:2013 ต้องไม่ลืมการสร้างความตระหนัก และการให้ความรู้ด้านภัยคุกคามและผลกระทบต่อกระทรวงกับบุคลากรภายในองค์กรอีกด้วย และเพื่อให้บรรลุเป้าหมายจำเป็นต้องได้รับการสนับสนุนงบประมาณ กำลังคน และเทคโนโลยีอย่างจริงจัง

ข้อเสนอแนะ

ระบบสารสนเทศได้มีการพัฒนาให้ก้าวหน้าอย่างรวดเร็วอยู่ตลอดเวลา ดังนั้น จึงควรมีการทวนสอบนโยบายตามระยะเวลาที่กำหนด ปรับปรุงนโยบายที่ใช้เพื่อให้นโยบายมีความเหมาะสม กับสถานการณ์ที่เปลี่ยนไป ไม่เกิดช่องโหว่ เหมาะสมกับสภาวะปัจจุบัน และรองรับการเติบโตในอนาคตขององค์กร

ด้านนโยบายและกระบวนการ

1. กำหนดนโยบายและวัตถุประสงค์ด้านคุณภาพขององค์กร เพื่อแสดงทิศทางและความมุ่งมั่นด้านคุณภาพผู้บริหารทุกระดับต้องมีความเชื่อในประโยชน์ของการจัดทำระบบ โดยเห็นว่าการจัดทำระบบเป็นสิ่งจำเป็น และก่อให้เกิดประโยชน์ต่อองค์กร

2. ให้ทุกหน่วยงานดำเนินการประเมินความเสี่ยง เพราะทำให้ได้ทราบถึงความเสี่ยงต่าง ๆ ที่อาจจะเกิดขึ้นกับทรัพย์สินของหน่วยงาน นำความเสี่ยงนั้นไปกำหนดแนวทางนโยบายในการบริหารความเสี่ยงที่เกิดขึ้นได้อย่างถูกต้อง ได้รับความร่วมมือจากผู้บริหารและคณะทำงานเป็นอย่างดีทำให้การดำเนินโครงการเป็นไปอย่างราบรื่น เมื่อศูนย์เทคโนโลยีสารสนเทศและการสื่อสารผ่านการปะเมินตามมาตรฐาน ISO/IEC 27001:2013 ควรดำเนินการขยายผลไปยังหน่วยงานอื่น ๆ โดยใช้เป็นต้นแบบ

3. มีกลไกอภิบาลระบบเทคโนโลยีสารสนเทศระดับชาติ การพัฒนากลไกกระบวนการ และเครื่องมือ เพื่อการสนับสนุน Digital Transformation การรักษาความปลอดภัยและความลับส่วนบุคคลของข้อมูลสุขภาพ โดยพิจารณาประโยชน์ทั้งการป้องกันส่วนบุคคลและการเปิดเผยข้อมูลที่จำเป็น โดยมีมาตรการป้องกันที่เหมาะสมในกรณีที่ต้องละเมิดความเป็นส่วนตัวของบุคคล โดยกฎหมาย และระเบียบที่ปรับปรุงให้เอื้อต่อการพัฒนาระบบเทคโนโลยีสารสนเทศ

4. มีแผนแม่บทการพัฒนาระบบเทคโนโลยีสารสนเทศสุขภาพของประเทศ ซึ่งกลไกบูรณาการสารสนเทศสุขภาพ เช่น ระบบแลกเปลี่ยนประวัติสุขภาพผู้ป่วยอิเล็กทรอนิกส์ (health information exchange) และระบบสารสนเทศกลางด้านบริการ ด้านบุคลากร และด้านการคลังสุขภาพ

ด้านเทคโนโลยีสารสนเทศ

1. การออกแบบความมั่นคงปลอดภัย เพิ่มสำหรับ API ต่าง ๆ เพื่อใช้รับส่งข้อมูลระหว่างระบบ Cloud และอุปกรณ์ IoT การยืนยันตัวตนด้วย จะใช้ certificate หรือ private key ที่ใช้ในการเข้ารหัสเพื่อยืนยันตัวตนของอุปกรณ์ IoT แล้ว ข้อมูลแวดล้อมอย่างเช่น geolocation, device fingerprinting, เวลาที่ใช้ในการยืนยันตัวตนและเชื่อมต่อ รวมถึงข้อมูลแวดล้อมอื่น ๆ ที่จะทำให้เชื่อมั่นได้ว่าอุปกรณ์เหล่านี้เป็นของจริงที่ไม่ได้ถูกแก้ไขหรือปลอมแปลงใด ๆ ก็จะถูกนำมาใช้ในการยืนยันตัวตนด้วย

2. ควรพิจารณาการนำโปรแกรมด้านปัญญาประดิษฐ์ (artificial intelligence – AI) ที่สามารถเข้ามาช่วยในเรื่องการดำเนินการ และลดการใช้ทรัพยากรบุคคล โดยต้องมีการทำความเข้าใจและปรับเปลี่ยนในการนำระบบ AI เข้ามาช่วยเพื่อให้มีความเป็นอัตโนมัติมากขึ้น

3. จัดทำ Disaster Recovery Site หรือ DR site เป็นการสำรองข้อมูลในกรณีที่ระบบหลักเกิดความเสียหาย ไม่ว่าจะเป็นความเสียหายจากภัยพิบัติตามธรรมชาติหรือจากฝีมือของมนุษย์ ก็สามารถใช้ข้อมูลที่สำรองไว้มาทำงานต่อได้ทันทีควรพิจารณา ปัจจุบันสำรองข้อมูลเฉพาะบางระบบงานสำคัญเท่านั้น จึงควรพิจารณาในการดำเนินการให้ควบ

ด้านบุคลากร

1. ต้องมีสื่อสารกับเจ้าหน้าที่ทุกระดับ เนื่องจากพบว่าเจ้าหน้าที่ภายในส่วนมากยังไม่ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร ISO/ICE 27001:2013 กำหนดแนวทางนโยบายในการบริหารความเสี่ยงที่เกิดขึ้นได้อย่างถูกต้องได้รับความร่วมมือจากผู้บริหารและคณะทำงานเป็นอย่างดีทำให้การดำเนินโครงการเป็นไปอย่างราบรื่น ดังนั้นการฝึกอบรมให้เจ้าหน้าที่ตระหนักถึงความสำคัญของงานที่รับผิดชอบเกี่ยวข้องกับความมั่นคงปลอดภัยระบบ

สารสนเทศ หรือการทำบอร์ดประชาสัมพันธ์ ช่วยให้เจ้าหน้าที่รับทราบข่าวสารและร่วมมือปฏิบัติ

2. การพัฒนาทักษะ เมื่อมีการกำหนดมาตรฐาน เกณฑ์ วิธีการ เรียบร้อย เริ่มพิจารณาถึงทักษะที่สำคัญในการทำงานได้อย่างแท้จริง ทักษะที่เจ้าหน้าที่ใช้ในการทำงานเช่นเดียวกับเครื่องมือในการทำงาน ที่เป็นปัจจัยความสำเร็จที่สำคัญของพนักงาน เพื่อทำการพัฒนาและประเมินผลเจ้าหน้าที่ต่อไป

กิตติกรรมประกาศ

ขอขอบคุณ ผศ. (พิเศษ) นพ. พลวรรธน์ วิทูรกลชิต ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทุกท่าน ที่มีส่วนสนับสนุนและดำเนินการในเรื่องนี้ให้สำเร็จเป็นไปด้วยดีและหวังเป็นอย่างยิ่งว่าจะเป็นประโยชน์ต่อผู้ร่วมงาน ผู้เกี่ยวข้อง ผู้สนใจทั่วไป นำไปใช้ประโยชน์ได้

เอกสารอ้างอิง

1. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารแห่งชาติ ฉบับที่ 2 (พ.ศ. 2552-2556). กรุงเทพมหานคร: กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร; 2552.
2. กระทรวงสาธารณสุข. ยุทธศาสตร์เทคโนโลยีสารสนเทศสุขภาพ กระทรวงสาธารณสุข (2560-2569). นนทบุรี: กระทรวงสาธารณสุข; 2560.
3. Sripeamlap T. บทวิเคราะห์แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ปี พ.ศ. 2559 (อินเทอร์เน็ต). [สืบค้นเมื่อ 25 พ.ย. 2561]. แหล่งข้อมูล: https://www.acisonline.net/?p=5040&lang=th
4. International Organization for Standardization. ISO/IEC 27000 family - Information security management systems [Internet]. [cited 2018 Mar 13]. Available from: https://www.iso.org/isoiec-27001-information-security.html
5. Arnason ST, Willett KD. Introduction to ISO Security Standards [Internet]. [cited 2018 Mar 13]. Available from: www.infosectoday.com
6. สำนักงานรัฐบาลอิเล็กทรอนิกส์. แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2560-2564. ฉบับแก้ไข สิงหาคม พ.ศ. 2560. กรุงเทพมหานคร: สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน); 2560.
7. เอกวิทย์ พิทักษ์คชวงษ์. การสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสารสนเทศภายใต้มาตรฐานISO/IEC27001:2013:2013 กรณีศึกษาบริษัทที่วีไดเร็คจำกัดมหาชน. กรุงเทพมหานคร: มหาวิทยาลัยเทคโนโลยีมหานคร; 2557.
8. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). เอกสารประกอบการประชุมแนวนโยบายการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (13 มีนาคม 2561) [อินเทอร์เน็ต]. [สืบค้นเมื่อ 1 พ.ย. 2561]. แหล่งข้อมูล: https://etda.or.th/content/ciip-meeting-at-etda.html
9. รัชชา ภรณ์สุภาพ, ศักดิ์ชาย ตั้งวรรณวิทย์. การจัดทำแนวทางการปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศด้วยมาตรฐาน ISO/IEC 27001 กรณีศึกษา: สำนักงานรัฐบาลอิเล็กทรอนิกส์ (มหาชน). กรุงเทพมหานคร: มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ; 2557.

Abstract: Development of Information Security Management Systems under ISO/IEC 27001:2013 Standard: Case Study of Ministry of Public Health Internet Data Center (MOPH IDC)

Suwanna Smernate, M.B.A. (Public Management)

Information and Communication Technology Center (ICT Center), Office of Permanent Secretary, Ministry of Public Health, Thailand

Journal of Health Science 2019;28:117-32.

The rapid development of convenient and inexpensive technology creates the unlimited access to information technology, resulting rapidly driven economy and society, more revenue and less difference of people. However, cyber threats become more aggressive along with the growth of digital economy and society. In this regards, Information and Communication Technology Center of Ministry of Public Health (MOPH), developed the Information Security Management Systems (ISMS) with the objective to protect information assets related to information technology services of MOPH Internet Data Center from potential internal and external threats, whether intentional or unintentional, in order to proof ISMS quality by applying ISO/IEC 27001:2013 Standard. The procedures consisted of: (1) the study of Information Security Management Systems Standard; (2) the analysis of risks on information technology of organization; (3) the development of ISMS and information technology security process in accordance with ISO/IEC 27001:2013 Standard; and (4) the suggestion on creating information technology security process. The results from the satisfaction evaluation responded by ISMS users under ISO/IEC 27001:2013 Standard indicated that the users in Group 1 (virtual machine and web hosting) had the highest overall satisfaction (average score 3.99), while those in Group 2 (vendors) had high overall satisfaction (average score 4.17) and those in Group 3 (general users) also had high overall satisfaction (average score 3.98). The Information and Communication Technology Center applied ISO/IEC 27001:2013 Standard to increase and standardize the security of the organization with successful results. However, the cyber threats and their impacts on the organization still exist. Therefore, MOPH personnel should knowledgeable on the matter and be able to recognize the threats. Strong manpower, budgetary and technology support is required in order to achieve the goal.

Key words: **ISO/IEC 27001:2013, risk, security**