วารสาร Mahidol R2R e-Journal ปีที่ 7 ฉบับที่ 2 ประจำเดือนกรกฎาคม-ธันวาคม 2563
Received: August 8, 2019, Revised: November 18, 2019, Accepted: December 27, 2019
http://doi.org/..

บริหารการเปลี่ยนแปลงอย่างมีประสิทธิภาพผ่านกระบวนการควบคุมการเปลี่ยนแปลงตามมาตรฐาน ISO27001:2013

Change Management Efficiently Across Change Control Processes According To ISO27001:2013

อิศรา แย้มงามเหลือ[1*] นิธิ ภัทรปิติตานนท์[1]
ISARA YAEMNGAMLUEA[1*], NITHI PATTARAPITITANONT[1]

บทคัดย่อ

ในปัจจุบันองค์กรต่าง ๆ ได้นำเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการบริหารจัดการองค์กร นำมาใช้ในการเก็บข้อมูลเพื่อการขับเคลื่อนให้องค์กรไปสู่เป้าหมายที่ได้กำหนดไว้ ทางคณะแพทยศาสตร์ศิริราชพยาบาลเป็นองค์กรที่มีพันธกิจ ทางด้านการรักษาผู้ป่วย การเรียนการสอนและการวิจัย ทำให้ระบบสารสนเทศต่าง ๆ มีจำนวนมากและถูกเชื่อมโยงเข้าไว้ด้วยกัน ทำให้ในแต่ละส่วนต่างก็มีความสำคัญไม่ยิ่งหย่อนไปกว่ากัน ไม่ว่าจะเป็น ข้อมูลประวัติผู้ป่วย ข้อมูลในการวิจัยทางการแพทย์ต่าง ๆ รวมถึงข้อมูลในการบริหารจัดการองค์กร จะต้องมีความถูกต้องสมบูรณ์ และมีความพร้อมใช้งานตลอดเวลา ฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลได้ตระหนักถึงความสำคัญดังกล่าว และเพื่อสนับสนุนพันธกิจในส่วนของการรักษาพยาบาล ได้นำมาตรฐาน ISO27001:2013 มาใช้ในการดำเนินการด้านสารสนเทศ และมีผลครอบคลุมทั้งหน่วยงาน

มาตรฐาน ISO27001:2013 มีกระบวนการ Change Control Procedure เพื่อตอบสนองในส่วนของการเปลี่ยนแปลงและพัฒนาเทคโนโลยีที่เป็นไปอย่างรวดเร็ว โรงพยาบาลต้องมีการปรับตัวในการนำเทคโนโลยีมาใช้เพื่อให้การบริการที่รวดเร็วยิ่งขึ้น รวมไปถึงการพัฒนาด้านธุรกิจและการบริหารจัดการ กระบวนการควบคุมการเปลี่ยนแปลงช่วยทำให้การบริหารจัดการ และแผนการดำเนินการที่ชัดเจน และมีผลกระทบกับระบบโดยภาพรวมน้อยที่สุด ส่งผลให้คณะแพทยศาสตร์ศิริราชพยาบาลสามารถดำเนินการตามพันธกิจได้อย่างมีประสิทธิภาพ

คำสำคัญ : การควบคุมการเปลี่ยนแปลง;ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ; องค์การระหว่างประเทศว่าด้วยการมาตรฐาน

[1*] ฝ่ายสารสนเทศ สำนักงานคณบดี คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล

[1*] Siriraj Information Technology Department, Faculty of Medicine Siriraj Hospital, Mahidol University

[*] corresponding author : isara.yam@mahidol.edu

วารสาร Mahidol R2R e-Journal ปีที่ 7 ฉบับที่ 2 ประจำเดือนกรกฎาคม-ธันวาคม 2563
Received: August 8, 2019, Revised: November 18, 2019, Accepted: December 27, 2019
http://doi.org/..

Abstract

Currently, the various organizations have applied information technology to manage the organization that use for collect information to drive the organization to reach the goal. The mission of the Faculty of Medicine Siriraj Hospital is patient treatment, teaching, and researching. The various information systems are connected and shared important information such as patient profile, patient medical record. The medical research information including information on organization management services must be accurate, complete and available. The Department of Information Technology, Siriraj Hospital recognized aware of the importance of information security and to support the mission of medical service. Resulting in the establishment of the project of the Information Security Management System (ISO27001:2013) and results covering the entire organization.

The standard of ISO27001: 2013 has the Change Control Procedure process in order to respond in terms of rapid change and development. Siriraj Hospital Information Technology department requires adaptation and using technology to provide patient service, respond immediately including business development and management. The Change Control Process encourages management, clear operation plans and reduces the overall impact on the information system. The systematic operation makes the Faculty of Medicine Siriraj Hospital able to effectively follow the organization's mission.

Keywords: Change Control; Information Security Management System; International Standards Organization

บทนำ

ในปัจจุบันองค์กรต่าง ๆ ได้นำเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการบริหารจัดการองค์กร รวมถึงการนำมาเก็บข้อมูลเพื่อการขับเคลื่อนให้องค์กรไปสู่เป้าหมายที่ได้กำหนดไว้ ความมั่นคงปลอดภัยในด้านของข้อมูลถือเป็นหัวใจหลักในการดำเนินการต่าง ๆ ขององค์กร เพื่อให้มีความน่าเชื่อถือ และมีมาตรฐานที่เป็นที่ยอมรับในระดับสากล โดยระเบียบการจัดการมาตรฐานหลักของระบบบริหารป้องกันความมั่นคงปลอดภัยสารสนเทศหลักๆ คือ มาตรฐาน ISO27001:2013 (ISMS:Information Security Management System) ที่ได้รับการยอมรับเป็นมาตรฐานสากล คณะแพทยศาสตร์ศิริราชพยาบาลได้จัดทำโครงการสร้างความมั่นคงปลอดภัยสารสนเทศ เพื่อให้สอดคล้องตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555 ในข้อ 2 (6) กำหนดให้ ธุรกรรมทางอิเล็กทรอนิกส์ในการให้บริการด้านสาธารณูปโภคและบริการสาธารณะที่ต้องดำเนินการอย่างต่อเนื่องตลอดเวลา ใช้วิธีการแบบปลอดภัยในระดับเคร่งครัด (คณะกรรมการธุรกรรมทาง

Received: August 8, 2019, Revised: November 18, 2019, Accepted: December 27, 2019
http://doi.org/..

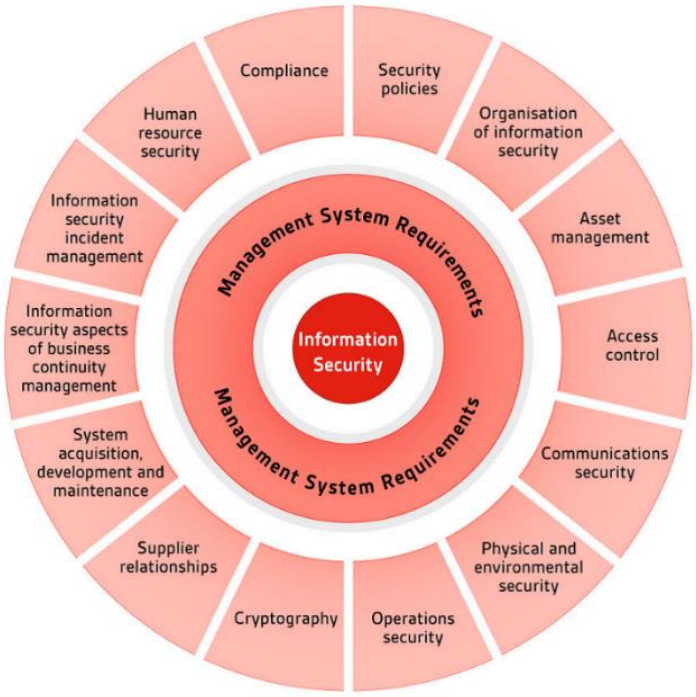
อิเล็กทรอนิกส์, 2562) เพื่อสร้างมาตรฐานความมั่นคงปลอดภัยสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล ตามมาตรฐานสากล ISO 27001 และกฎหมายบังคับใช้ที่เกี่ยวข้อง ก่อให้เกิดความเชื่อมั่น มั่นคงปลอดภัย น่าเชื่อถือในการใช้งานสารสนเทศ การใช้งานสารสนเทศของคณะฯ ดำเนินไปอย่างมีประสิทธิภาพและประสิทธิผล กำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับคณะฯ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานสารสนเทศของคณะฯ ให้ปฏิบัติตามอย่างเคร่งครัด การดำเนินการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) ตามมาตรฐาน ISO/IEC 27001:2013 ครอบคลุมการให้บริการของศูนย์ข้อมูลสารสนเทศ (Data Center) ของคณะแพทยศาสตร์ศิริราชพยาบาล โดยจะต้องครอบคลุมขอบเขตของการให้บริการด้านระบบโครงสร้างสารสนเทศ (Infrastructure) ประกอบด้วย การควบคุมทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Control Service), การให้บริการเครือข่าย(Networking Service), การให้บริการรักษาความปลอดภัยและตรวจสอบความพร้อมใช้ (Security and Monitoring Service) และ การให้บริการโครงสร้างพื้นฐานของเครื่องแม่ข่าย (Server Infrastructure Service)

มาตรฐาน ISO27001:2013 ยังมีกระบวนการที่สำคัญ คือ การควบคุมการเปลี่ยนแปลง (Change Control Procedure) ที่สามารถตอบสนองในส่วนของการเปลี่ยนแปลงและพัฒนาเทคโนโลยีในส่วนต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาลเพื่อปรับปรุงและพัฒนาระบบให้รองรับปริมาณผู้รับบริการที่เพิ่มมากขึ้น ซึ่งกระบวนการควบคุมการเปลี่ยนแปลง ที่จะต้องมีการจัดการให้มีความเป็นระบบ มีแผนการดำเนินการชัดเจน และมีผลกระทบกับระบบโดยภาพรวมน้อยที่สุด ส่งผลให้คณะแพทยศาสตร์ศิริราชพยาบาลสามารถดำเนินการตามพันธกิจได้อย่างมีประสิทธิภาพ ตามวิสัยทัศน์ที่ว่า “คณะแพทยศาสตร์ศิริราชพยาบาลเป็นสถาบันทางการแพทย์ของแผ่นดิน มุ่งสู่ความเป็นเลิศระดับสากล” (คณะแพทยศาสตร์ศิริราชพยาบาล, 2562)

ความเป็นมาของกระบวนการควบคุมการเปลี่ยนแปลง Change Control Procedure

มาตรฐาน ISO 27001:2013 หรือ Information Security Management System (ISMS) เป็นมาตรฐานที่เกี่ยวกับการบริหารจัดการข้อมูลสารสนเทศให้มีความมั่นคงปลอดภัย กำหนดขึ้นโดยองค์กรระหว่างประเทศ International Organization for Standardization (ISO) และInternational Electrotechnical Commission (IEC) เป็นมาตรฐานสากลที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรและใช้เป็นมาตรฐานอ้างอิงเพื่อเป็นแนวทางในการเสริมสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรอย่างแพร่หลาย ซึ่งมาตรฐาน ISO 27001:2013 มีมาตรการจัดการความปลอดภัยของสารสนเทศ เรียกว่า “Annex A (Normative)” ทั้งหมด 14 ข้อ ดังภาพ

วารสาร Mahidol R2R e-Journal ปีที่ 7 ฉบับที่ 2 ประจำเดือนกรกฎาคม-ธันวาคม 2563
Received: August 8, 2019, Revised: November 18, 2019, Accepted: December 27, 2019
http://doi.org/..



ภาพที่ 1 มาตรการจัดการความปลอดภัยสารสนเทศ ISO 27001:2013 (Coders, 2019)

โดยกระบวนการควบคุมการเปลี่ยนแปลง (Change Control Procedure) จะเกี่ยวข้องกับมาตรการจัดการความปลอดภัยจำนวน 2 ข้อ คือ

1. Operations Security ความปลอดภัยสำหรับการดำเนินการ (Annex A.12) โดยมีมาตรการย่อยที่เกี่ยวข้องคือ การเปลี่ยนแปลงใด ๆ ที่เกี่ยวข้องกับองค์กร กระบวนการทางธุรกิจ ระบบประมวลผลสารสนเทศและระบบซึ่งกระทบต่อความมั่นคงปลอดภัยสารสนเทศต้องได้รับการควบคุม (A.12.1.2)

2. System acquisition, development and maintenance การจัดหา การพัฒนา และการบำรุงรักษาระบบ (Annex A.14) โดยมีมาตรการย่อยที่เกี่ยวข้องคือ การเปลี่ยนแปลงต่อระบบภายในวงจรการพัฒนา ต้องได้รับการควบคุมโดยกระบวนการควบคุมการเปลี่ยนแปลงที่ถูกจัดทำขึ้นอย่างเป็นทางการ (A.14.2.2) (International Standard ISO/IEC 27001:2013)

ในการจัดตั้งโครงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) หรือ ISO27001:2013 ของคณะแพทยศาสตร์ศิริราชพยาบาลนั้นได้มีการจัดตั้งกระบวนการควบคุมการเปลี่ยนแปลง (Change Control Procedure) เพื่อควบคุมการเปลี่ยนแปลงใด ๆ ที่ก่อให้เกิดผลกระทบอย่างมีนัยสำคัญต่อระบบ ซึ่งรวมถึงการสร้างเพิ่มเติม แก้ไข หรือยกเลิกโครงสร้างพื้นฐานที่ประกอบกันเพื่อสนับสนุน หรือเป็นส่วนหนึ่งของการให้บริการทางเทคโนโลยีสารสนเทศ รวมถึงการเปลี่ยนแปลงที่กระทบกับหน่วยงานภายนอกให้มีประสิทธิภาพ บรรลุวัตถุประสงค์ที่ต้องการ และมีความปลอดภัยต่อระบบสารสนเทศ โดยแบ่งเป็น 2 ส่วน คือ

1. โครงสร้างพื้นฐาน (Infrastructure) ประกอบด้วยส่วนของศูนย์ข้อมูล (Data Center), เครื่องแม่ข่าย (Server), ความปลอดภัยบนเครือข่าย (Network Security) และสิ่งอำนวยความสะดวกต่าง ๆ (Facilities) การเปลี่ยนแปลงจะส่งผลกระทบต่อระบบสารสนเทศ เช่น การติดตั้ง ใบรับรอง (SSL Certificate) ที่เครื่องคอมพิวเตอร์แม่ข่าย, การดำเนินการติดตั้งระบบเครือข่ายเพื่อรองรับการใช้งานอาคารใหม่, สร้างเครื่องแม่ข่ายเพื่อติดตั้งและทดสอบใช้งานโปรแกรม Management tools เป็นต้น

Received: August 8, 2019, Revised: November 18, 2019, Accepted: December 27, 2019
http://doi.org/..

2. ระบบงาน (Applications) ประกอบด้วยระบบงานต่าง ๆ ที่พัฒนาขึ้นเพื่อตอบสนองความต้องการในการให้บริการผู้ป่วยและใช้สำหรับบริหารจัดการองค์กร เช่น การขอขึ้น Web Portal ในเว็บไซต์คณะแพทยศาสตร์ศิริราชพยาบาลเพื่อแสดงข้อมูลสรุปวันลาของบุคลากร, การขอปรับปรุงรูปแบบใบเสร็จรับเงินให้เป็นรูปแบบใบเสร็จรับเงินอิเล็กทรอนิกส์, การขอนำระบบใบสั่งยา Version 0.0.1.02 ขึ้นใช้งาน, และการขอปรับปรุงข้อมูลบุคลากรในระบบรับเรื่องร้องเรียน เป็นต้น

ความสำคัญของกระบวนการควบคุมการเปลี่ยนแปลง (Change Control Procedure)

กระบวนการควบคุมการเปลี่ยนแปลง (Change Control Procedure) มีความสำคัญต่อการดำเนินงานภายใต้การพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) ตามมาตรฐาน ISO 27001 ดังนี้

1. เพื่อตอบสนองต่อการร้องขอการเปลี่ยนแปลงของธุรกิจและเทคโนโลยีสารสนเทศ

2. เพื่อป้องกันไม่ให้เกิดการเปลี่ยนแปลงที่ไม่ได้รับอนุญาต

3. เพื่อให้มั่นใจว่ามีการบันทึก วิเคราะห์ และทบทวนการเปลี่ยนแปลง ที่บรรลุวัตถุประสงค์ของการเปลี่ยนแปลงนั้น ๆ

4. เพื่อให้มีการควบคุมความเสี่ยง และผลกระทบต่อธุรกิจและเทคโนโลยีสารสนเทศอันเกิดมาจากการเปลี่ยนแปลง (อรวรรณ เพ็ชรวงศ์, 2562)

5. มีคณะกรรมการหลายฝ่ายร่วมพิจารณา ทั้งในส่วนของโครงสร้างพื้นฐาน (Infrastructure) และส่วนของระบบงาน (Application) เพื่อให้มีความครบถ้วนถูกต้องในกระบวนการที่อาจมีผลกระทบต่อการเปลี่ยนแปลงในแต่ละครั้ง รวมไปถึงการสื่อสารไปยังหน่วยงานที่ได้รับผลกระทบในกรณีที่มีผลกระทบต่อระบบเป็นวงกว้าง จะได้ร่วมกันพิจารณาเพื่อหาแผนรองรับต่อไป

6. สามารถนำผลการดำเนินการที่ผ่านมาเป็นบทวิเคราะห์กรณีที่ต้องมีการดำเนินการที่มีความคล้ายคลึงกันเพื่อให้เกิดผลกระทบกับระบบน้อยที่สุด และการเปลี่ยนแปลงนั้น ๆ มีความปลอดภัยมากยิ่งขึ้น

7. ช่วยในการฝึกทักษะของผู้ดูแลระบบและนักพัฒนาระบบให้สามารถวางแผนการทำงานเป็นขั้นตอน การทดสอบระบบ ชี้แจงรายละเอียดผลกระทบที่อาจจะเกิดขึ้น ในกรณีคณะกรรมการมีข้อสงสัยสามารถชี้แจงเพื่อให้เกิดความเข้าใจตรงกัน

การนำกระบวนการควบคุมการเปลี่ยนแปลง (Change Control Procedure) มาใช้ในองค์กร

การดำเนินงานภายใต้การพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) ตามมาตรฐาน ISO 27001:2013 กระบวนการควบคุมการเปลี่ยนแปลงเป็นกระบวนการมาตรฐานที่คณะทำงานจะต้องดำเนินการตามมาตรการจัดการความปลอดภัยสารสนเทศ โดยมีขั้นตอน ดังนี้

1. จัดตั้งคณะทำงานในการบริหารและควบคุมการเปลี่ยนแปลง (Change Advisory Board หรือ CAB) ประกอบไปด้วย หัวหน้างานเทคนิคและปฏิบัติการ หัวหน้างานวิเคราะห์และพัฒนาโปรแกรมและหัวหน้าฝ่ายสารสนเทศ โดยมีรองคณบดีฝ่ายสารสนเทศเป็นประธาน ทำหน้าที่แนะนำในเรื่องการประเมินผลกระทบ จัดลำดับความสำคัญ ตรวจสอบการเปลี่ยนแปลง และพิจารณาอนุมัติคำร้องเพื่อดำเนินการ กำหนดวันเวลา สถานที่ในการประชุม และความถี่ในการประชุม รวมถึงแต่งตั้งผู้ทำหน้าที่เลขาของการประชุม เพื่อทำหน้าที่รวบรวมคำร้องที่ต้องการนำเสนอ จัดทำรายงานการอนุมัติ (แบบบันทึก Change Meeting) ในแต่ละรอบการประชุมและจัดเก็บเอกสารแบบฟอร์มคำร้องซึ่งเป็นเอกสารชั้นความลับภายในองค์กร

2. จัดทำเอกสารที่เกี่ยวข้อง ประกอบด้วย

2.1 แบบฟอร์ม Infrastructure Change Request form สำหรับบันทึกคำร้องขอดำเนินการเปลี่ยนแปลงในส่วนของโครงสร้างพื้นฐาน (Infrastructure)

Received: August 8, 2019, Revised: November 18, 2019, Accepted: December 27, 2019
http://doi.org/..

2.2 แบบฟอร์ม Software Change Request form สำหรับบันทึกคำร้องขอดำเนินการเปลี่ยนแปลงในส่วนระบบงาน (Application)

2.3 แบบบันทึกการดำเนินการเปลี่ยนแปลง Standard Change ประจำเดือน สำหรับบันทึกข้อมูลของการเปลี่ยนแปลงได้รับการอนุมัติไว้ล่วงหน้าเรียบร้อยแล้ว

2.4 แบบบันทึกรายการทรัพย์สิน (CMDB) สำหรับบันทึกการเปลี่ยนแปลงของรายการทรัพย์สินที่เกิดขึ้นและมีผลกระทบต่อระบบ เช่น การเพิ่มเครื่องคอมพิวเตอร์แม่ข่ายเข้ามาในระบบ จะต้องมีการจัดทำรายละเอียดของเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าว เช่น ระบบงาน หมายเลข IP ระบบปฏิบัติการ คุณลักษณะของเครื่อง (Specification) เป็นต้น

2.5 แบบบันทึก Change Meeting บันทึกรายการเปลี่ยนแปลงที่ได้รับการอนุมัติจากที่ประชุม Change Advisory Board (CAB)

3. การกำหนดหน้าที่และความรับผิดชอบ ของแต่ละบุคคลที่เกี่ยวข้องในกระบวนการ เพื่อให้เกิดความเข้าใจและสามารถปฏิบัติงานได้อย่างถูกต้อง

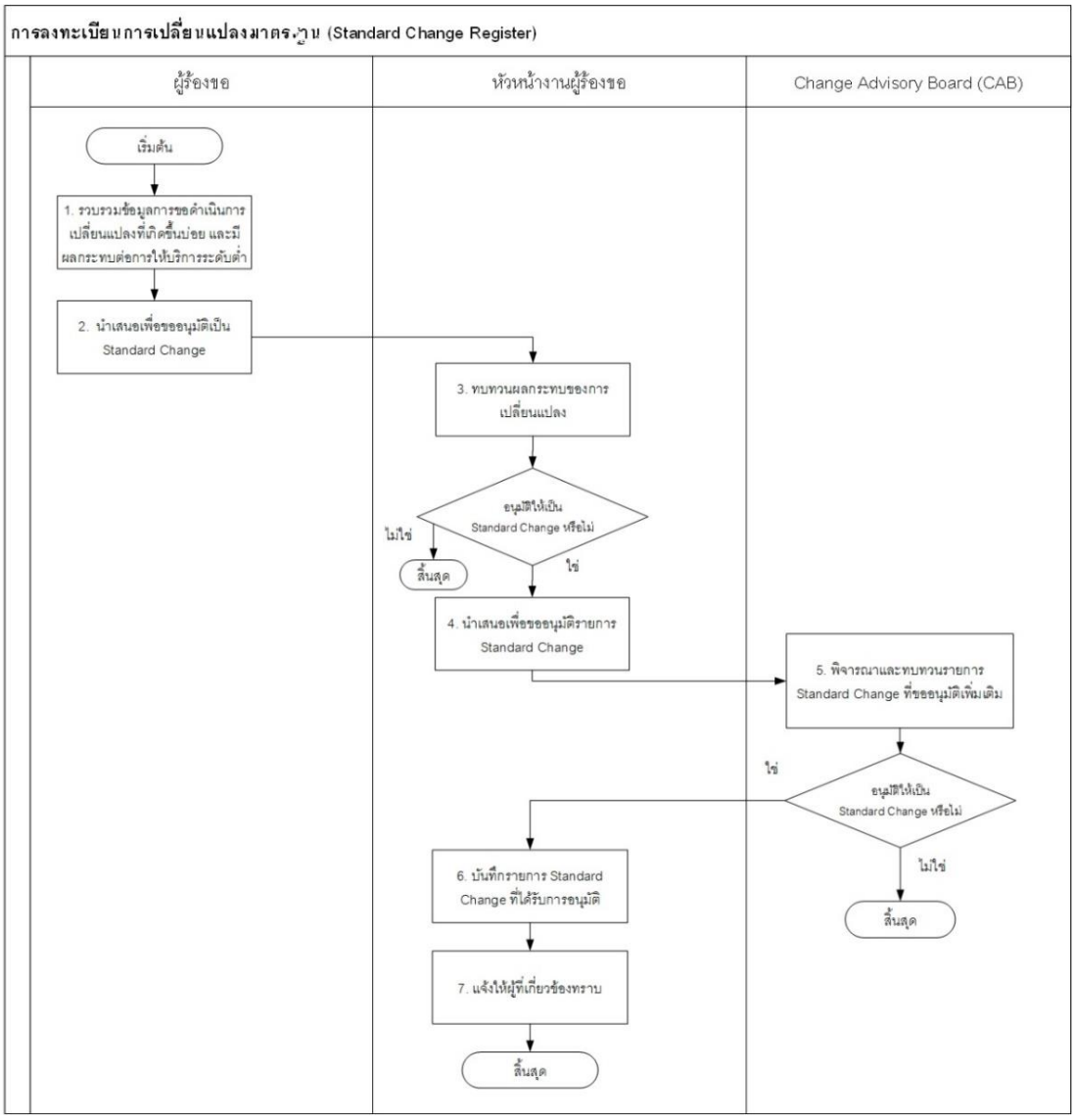
ตารางที่ 1 หน้าที่ความรับผิดชอบที่เกี่ยวข้องในกระบวนการควบคุการเปลี่ยนแปลง

ลำดับ	หน้าที่	ความรับผิดชอบ
1	ผู้ร้องขอ	1. บันทึกคำร้องขอเพื่อดำเนินการเปลี่ยนแปลงในแบบฟอร์ม 2. ทบทวนผลการดำเนินการเปลี่ยนแปลงเพื่อให้แน่ใจว่าตรงตามวัตถุประสงค์ 3. บันทึกปิดคำร้อง
2	หัวหน้างานผู้ร้องขอ	1. ทบทวนคำร้องขอเพื่อดำเนินการเปลี่ยนแปลง ตรวจสอบประเภทของคำร้องขอ และความเหมาะสมต่อการดำเนินการเปลี่ยนแปลง โดยพิจารณาจากผลกระทบ และความเสี่ยงที่อาจเกิดขึ้น 2. พิจารณาอนุมัติคำร้องเพื่อการเปลี่ยนแปลง และนำเสนอเพื่อขออนุมัติจากที่ประชุม Change Advisory Board (CAB)
3	ผู้ดำเนินการเปลี่ยนแปลง	1. ทดสอบการเปลี่ยนแปลง 2. ดำเนินการเปลี่ยนแปลงที่ได้รับอนุมัติ
4	Change Advisory Board (CAB)	1. ทบทวนคำร้องขอเพื่อดำเนินการเปลี่ยนแปลง และความเหมาะสมต่อการดำเนินการเปลี่ยนแปลง โดยพิจารณาจากผลกระทบ และความเสี่ยงที่อาจเกิดขึ้น 2. พิจารณาอนุมัติคำร้องเพื่อการเปลี่ยนแปลง
5	เลขาการประชุม Change Advisory Board (CAB)	รวบรวมคำร้องที่ต้องการนำเสนอ จัดเก็บเอกสารซึ่งเป็นเอกสารชั้นความลับภายในองค์กร จัดทำรายงานการอนุมัติ (แบบบันทึก Change Meeting) ของการประชุมแต่ละครั้ง

4. กำหนดลักษณะการเปลี่ยนแปลง เพื่อดำเนินการตามขั้นตอนการทำงาน โดยแบ่งออกเป็น 3 ระดับ ดังนี้

4.1 การเปลี่ยนแปลงที่มีผลกระทบน้อย (Standard Change) เป็นการเปลี่ยนแปลงที่มีผลกระทบในระดับต่ำ (Low Impact) ไม่ส่งผลกระทบต่อการให้บริการ ซึ่งได้รับการพิจารณาอนุมัติล่วงหน้า (Pre - Approval) จาก Change Advisory Board (CAB) เรียบร้อยแล้ว รายการ Standard Change List เป็นการรวบรวมข้อมูลการขอดำเนินการเปลี่ยนแปลงที่เกิดขึ้นบ่อย และมีผลกระทบต่อการให้บริการระดับต่ำเพื่อลงทะเบียนและสามารถปรับปรุงข้อมูลการขอดำเนินการเปลี่ยนแปลงที่เกิดขึ้นบ่อย และมีผลกระทบต่อการให้บริการในระดับต่ำ ได้ตามความเหมาะสมของการดำเนินงาน โดยมีขั้นตอนการดำเนินการดังภาพ

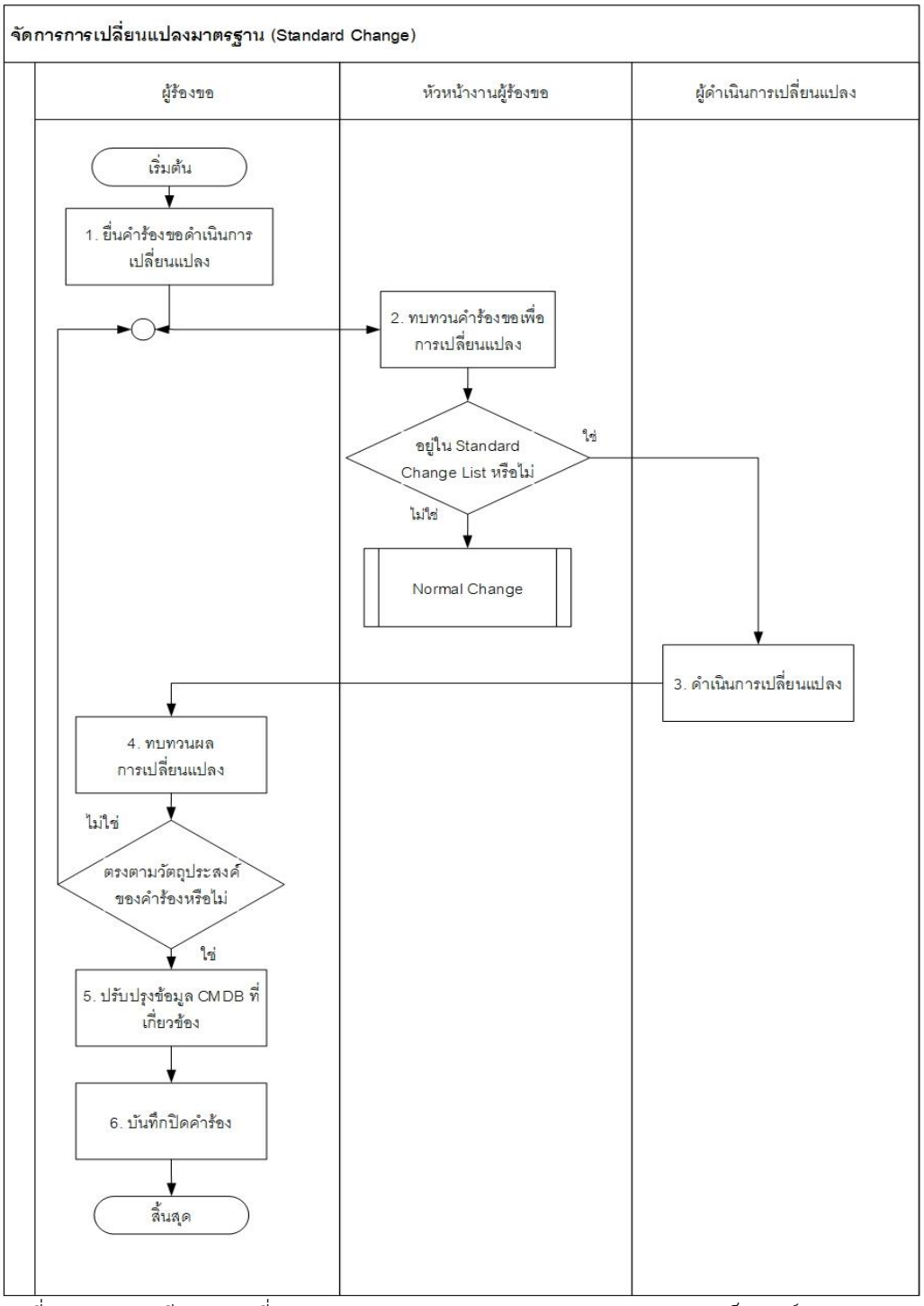
Received: August 8, 2019, Revised: November 18, 2019, Accepted: December 27, 2019
http://doi.org/..



ภาพที่ 2 การลงทะเบียนการเปลี่ยนแปลงมาตรฐาน (Standard Change Register) (อรวรรณ เพ็ชรวงศ์, 2562)

เมื่อลงทะเบียนเสร็จเรียบร้อยแล้วรายการที่ได้รับอนุมัติจะอยู่ในส่วนของ Standard Change List เช่น การตั้งค่า/สร้าง/เปลี่ยนแปลง/ยกเลิกสิทธิ์ของบัญชีรายชื่อผู้ใช้งานระบบ FTP server, การตั้งค่า/สร้าง/เปลี่ยนแปลง/ยกเลิกสิทธิ์ของบัญชีรายชื่อผู้ใช้งานระบบ File server, การกู้คืนข้อมูลจากระบบ เช่น Restore files and databases , การเปลี่ยนอุปกรณ์ (ที่ชำรุด) ของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ ที่ไม่กระทบกับการทำงานของเครื่อง เป็นต้น เมื่อดำเนินการเปลี่ยนแปลงเรียบร้อยแล้วจะต้องบันทึกผลการดำเนินการที่แบบบันทึกการดำเนินการเปลี่ยนแปลง Standard Change ประจำเดือน เพื่อสรุปในที่ประชุม Change Advisory Board (CAB) ในแต่ละเดือน มีกระบวนการดังภาพ

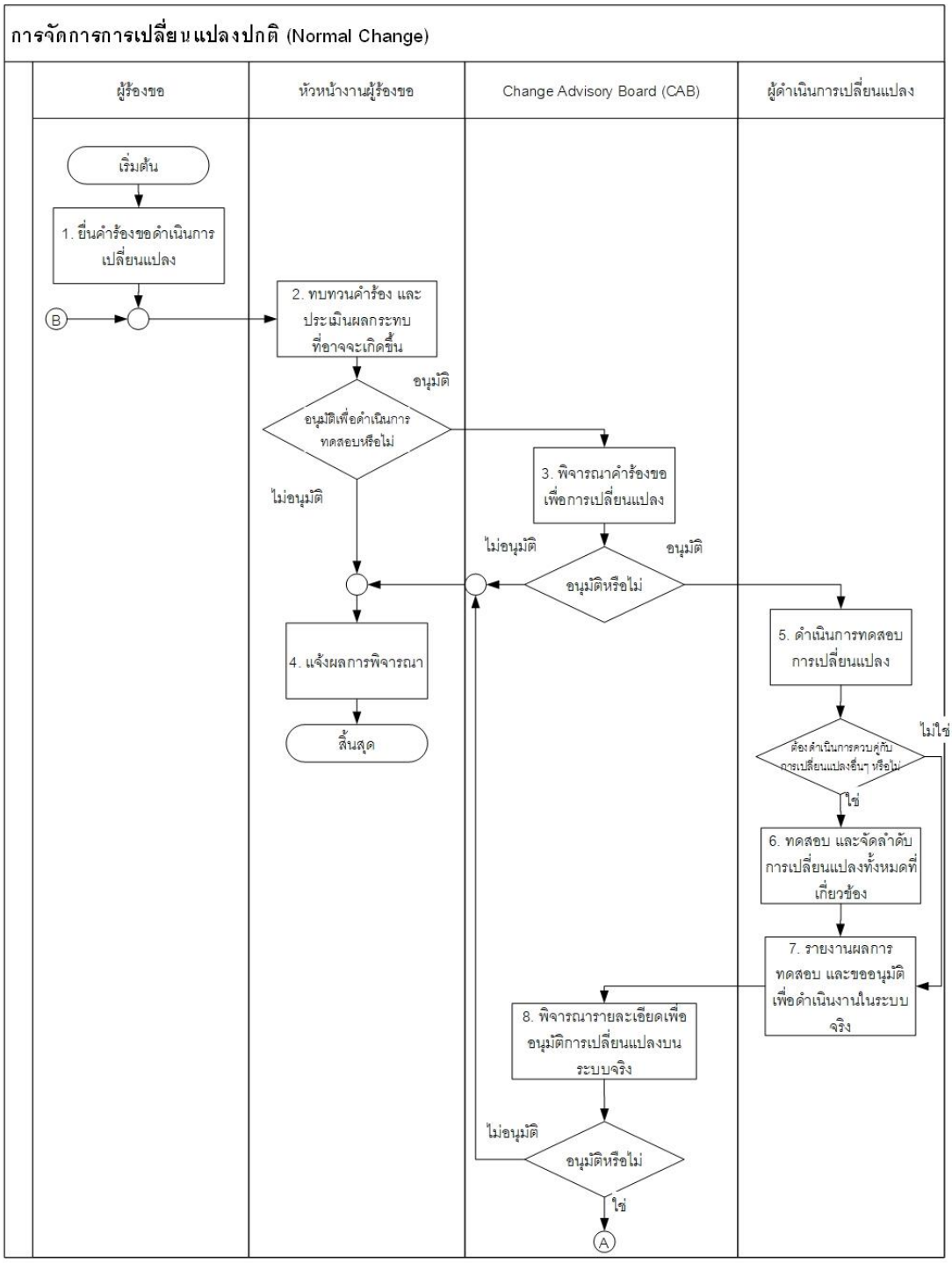
Received: August 8, 2019, Revised: November 18, 2019, Accepted: December 27, 2019
http://doi.org/..



ภาพที่ 3 การลงทะเบียนการเปลี่ยนแปลงมาตรฐาน (Standard Change) (อรวรรณ เพ็ชรวงศ์, 2562)

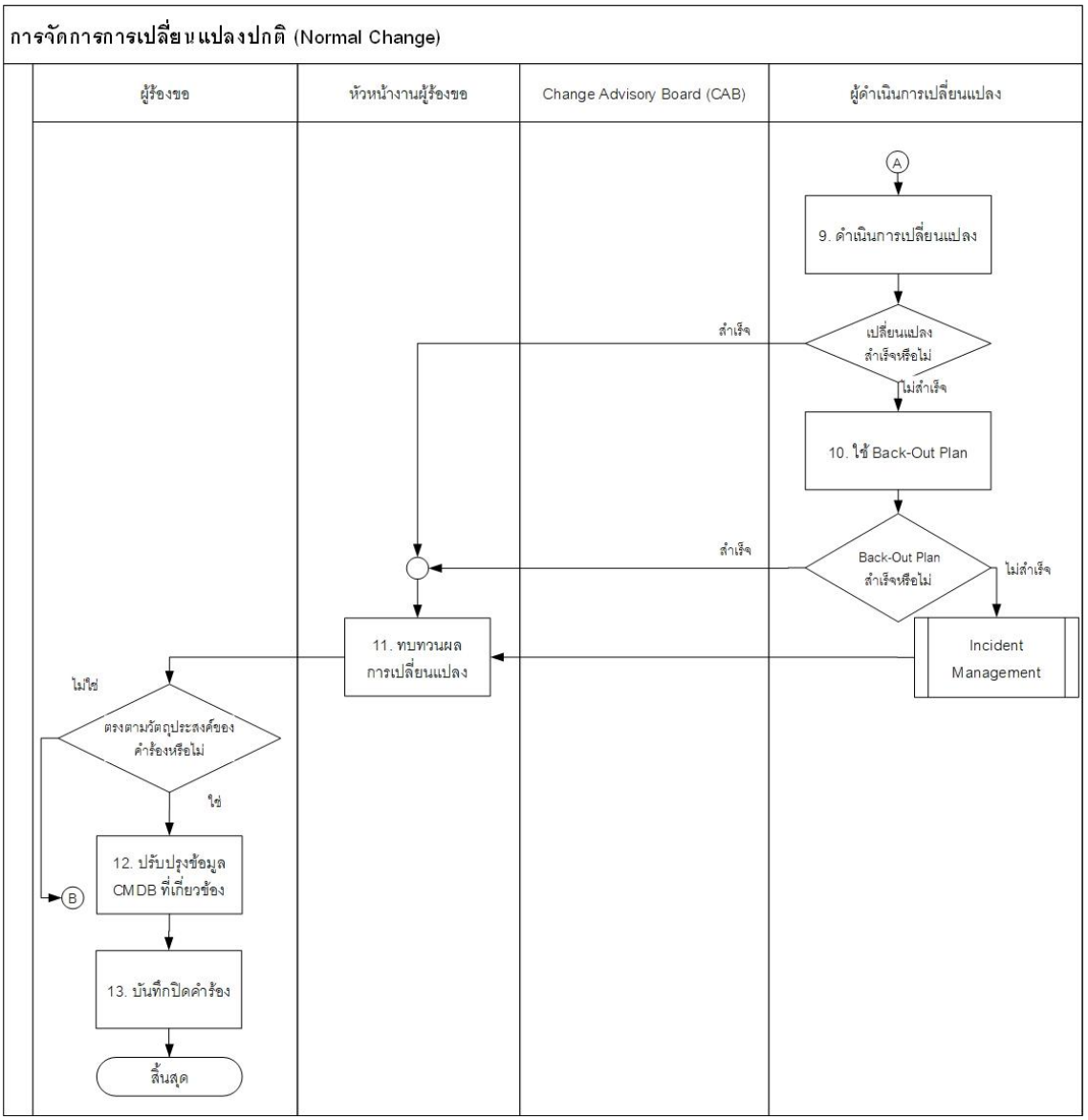
4.2 การเปลี่ยนแปลงที่มีผลกระทบต่อระบบ (Normal Change) การเปลี่ยนแปลงที่มีผลกระทบในระดับสูง แต่ไม่เร่งด่วน เป็นกิจกรรมที่ยังไม่ถูกระบุใน Standard Change โดยต้องบันทึกรายละเอียด และขอการอนุมัติตามขั้นตอนการเปลี่ยนแปลงปกติ (Normal Change Process) จึงจะสามารถดำเนินการเปลี่ยนแปลงนั้นได้ มีกระบวนการ ดังภาพ

Received: August 8, 2019, Revised: November 18, 2019, Accepted: December 27, 2019
http://doi.org/..



ภาพที่ 4 การจัดการการเปลี่ยนแปลงปกติ (Normal Change) (อรวรรณ เพ็ชรวงศ์, 2562)

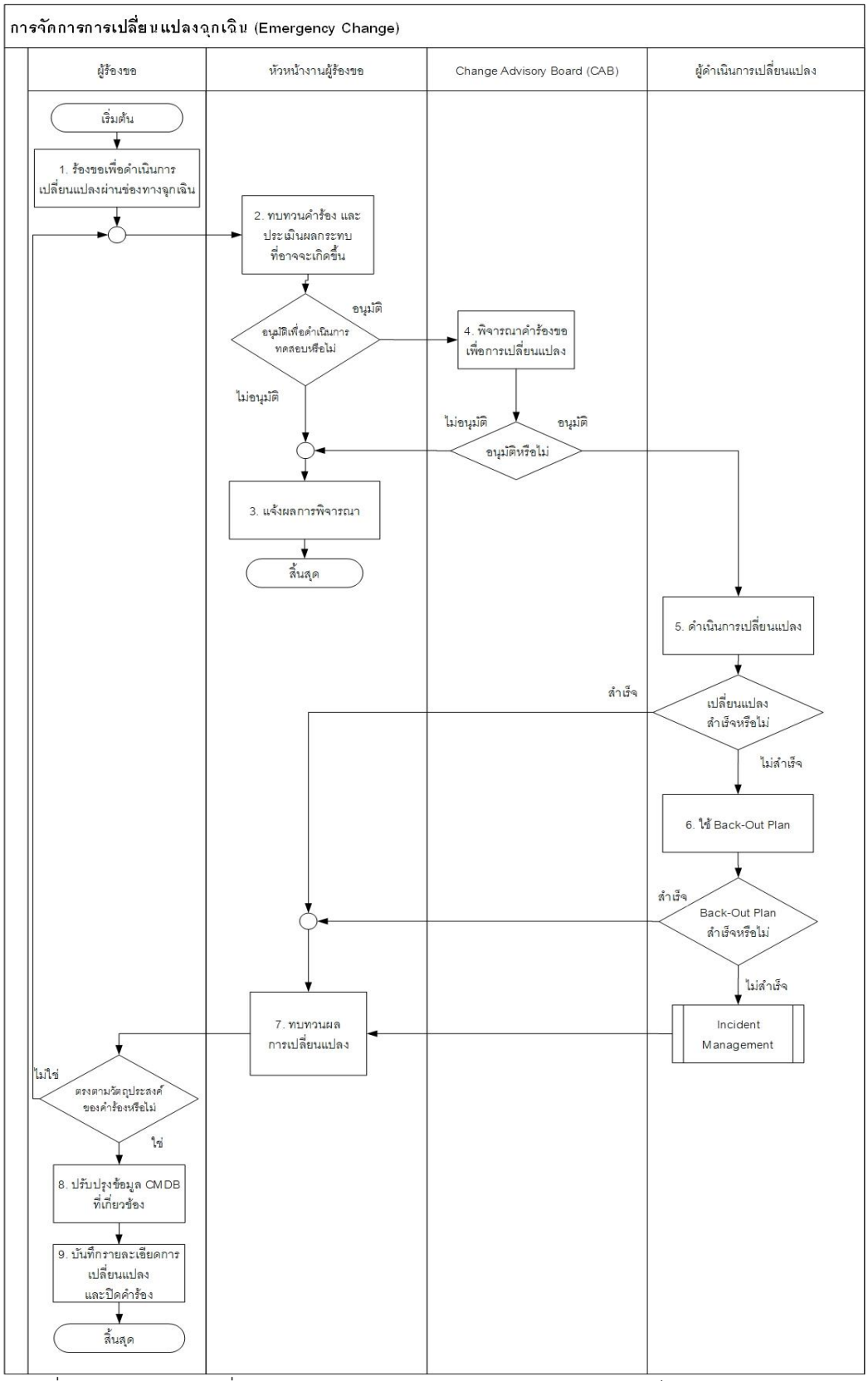
Received: August 8, 2019, Revised: November 18, 2019, Accepted: December 27, 2019
http://doi.org/..



ภาพที่ 5 การจัดการการเปลี่ยนแปลงปกติ (Normal Change) (ต่อ) (อรวรรณ เพ็ชรวงศ์, 2562)

4.3 การเปลี่ยนแปลงที่มีผลกระทบต่อระบบสูง (Emergency Change) เป็นการเปลี่ยนแปลงที่มีผลกระทบระดับสูงในกรณีเร่งด่วน ซึ่งหากไม่รีบดำเนินการอย่างเร่งด่วนหรือทันที จะส่งผลกระทบกับประสิทธิภาพหรือข้อตกลงการให้บริการ สามารถอนุมัติการเปลี่ยนแปลงนั้นทางวาจา จากผู้มีอำนาจอนุมัติ เช่น หัวหน้าฝ่ายสารสนเทศ โดยที่ไม่ต้องรอวาระการประชุม Change Advisory Board (CAB) แต่เมื่อดำเนินงานเสร็จสิ้นต้องบันทึกข้อมูล และขอการอนุมัติตามขั้นตอนปกติภายหลัง มีกระบวนการดังภาพ (UCISA ITIL, 2019)

Received: August 8, 2019, Revised: November 18, 2019, Accepted: December 27, 2019
http://doi.org/..



ภาพที่ 6 การจัดการการเปลี่ยนแปลงฉุกเฉิน (Emergency Change) (อรวรรณ เพ็ชรวงศ์, 2562)

Received: August 8, 2019, Revised: November 18, 2019, Accepted: December 27, 2019
http://doi.org/..

เมื่อจัดตั้งองค์ประกอบในการดำเนินการ Change Control Procedure เรียบร้อยแล้ว ทางผู้บริหารจะกำหนดวันเริ่มนำกระบวนการดังกล่าวมาใช้งาน โดยจะเริ่มในส่วนของการพิจารณารวบรวม การเปลี่ยนแปลงที่มีผลกระทบน้อย (Standard Change) เพื่อขออนุมัติล่วงหน้า (Pre - Approval) ในที่ประชุม Change Advisory Board (CAB) ตามขั้นตอน Standard Change ดังนั้น เมื่อมีคำขอเปลี่ยนอุปกรณ์ (ที่ชำรุด) ของเครื่องคอมพิวเตอร์แม่ข่ายระบบห้องยาที่ไม่กระทบกับการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายที่อยู่ในส่วนของ Standard Change List ก็สามารถดำเนินการได้ทันที เมื่อเสร็จเรียบร้อยจะต้องบันทึกผลการดำเนินการในแบบบันทึกการดำเนินการเปลี่ยนแปลง Standard Change ประจำเดือน เพื่อนำเสนอในที่ประชุม Change Advisory Board (CAB) ในรอบการประชุมสิ้นเดือน ตัวอย่างการเปลี่ยนแปลงอื่น ๆ เช่น

ระบบบริจาคมีการพัฒนาระบบเพื่อเชื่อมโยงกับธนาคาร จึงต้องการขอติดตั้งใบรับรอง (SSL Certificate) ที่เครื่องคอมพิวเตอร์แม่ข่ายของระบบบริจาค เมื่อพิจารณาแล้วเป็นการเปลี่ยนแปลงที่มีผลกระทบในระดับสูง แต่ไม่เร่งด่วน เป็นกิจกรรมที่ยังไม่ถูกระบุใน Standard Change จัดเป็น Normal Change ดังนั้นในกรณีนี้ขอให้ดำเนินการตามขั้นตอนการเปลี่ยนแปลงปกติ (Normal Change)

ระบบการเงินไม่สามารถใช้งานได้ เนื่องจากพื้นที่สำหรับเก็บข้อมูลเต็มจึงต้องเพิ่มพื้นที่สำหรับเก็บข้อมูลให้กับระบบการเงิน จำนวน 100 GB เพื่อรองรับการใช้งานเบื้องต้น เป็นการเปลี่ยนแปลงที่มีผลกระทบระดับสูงในกรณีเร่งด่วน ซึ่งหากไม่รีบดำเนินการอย่างเร่งด่วนหรือทันที จะส่งผลกระทบกับประสิทธิภาพ หรือข้อตกลงการให้บริการ เป็นการเปลี่ยนแปลงที่มีผลกระทบต่อระบบสูง (Emergency Change) โดยจะต้องอนุมัติจากหัวหน้าฝ่ายสารสนเทศก่อนจึงดำเนินการได้ จากนั้นจึงดำเนินการตามขั้นตอนการเปลี่ยนแปลงฉุกเฉิน (Emergency Change)

ในทุกการเปลี่ยนแปลงที่ได้รับการอนุมัติจากที่ประชุม Change Advisory Board (CAB) แต่ละรอบ เลขานุการการประชุมจะบันทึกลงในแบบบันทึก Change Meeting แบบฟอร์มทั้งหมดจะได้รับการอนุมัติจากประธานที่ประชุม เมื่อผู้ปฏิบัติงานดำเนินการเรียบร้อยแล้ว จะทำการบันทึกปิดคำร้อง เลขานุการที่ประชุมจะบันทึกผลการปฏิบัติงานที่แบบบันทึก Change Meeting และรวบรวมแบบฟอร์มจัดเก็บไว้เป็นหลักฐานต่อไป

ปัญหาและอุปสรรคที่พบของกระบวนการ Change Control Procedure

1. กระบวนการควบคุมการเปลี่ยนแปลง (Change Control Procedure) อาจส่งผลให้การดำเนินการล่าช้าและสับสนในระยะแรก เนื่องจากผู้ปฏิบัติงานจะต้องจัดทำแบบฟอร์มเอกสาร บันทึกผลการปฏิบัติงานในการปิดคำร้อง และ แบบบันทึก Standard Change สำหรับการเปลี่ยนแปลงในแต่ละครั้ง ซึ่งผู้ปฏิบัติงานส่วนใหญ่จะไม่มีความชำนาญในการจัดทำเอกสารมากนัก รวมถึงต้องการมีการประชุมพิจารณาอนุมัติในรอบสัปดาห์ จึงจะดำเนินการได้

2. การทำความเข้าใจในขั้นตอนของกระบวนการควบคุมการเปลี่ยนแปลง ผู้ปฏิบัติงานมีความเข้าใจไม่ตรงกันเมื่อมีการนำกระบวนการขึ้นมาใช้ จึงต้องมีการอบรมเพื่อทำความเข้าใจ และจัดทำเป็น “วิธีปฏิบัติงาน เรื่อง: การควบคุมการเปลี่ยนแปลง (Change Control Procedure)” เพื่อเป็นแนวทางให้เกิดความเข้าใจที่ตรงกันและสามารถปฏิบัติได้อย่างถูกต้อง

3. ความซับซ้อนของแบบฟอร์ม การเขียนแบบฟอร์มในแต่ละส่วนงาน จะมีรายละเอียดจำนวนมาก การเขียนให้ครบถ้วนและถูกต้อง ผู้ร้องขอจะต้องมีความเข้าใจในด้านนั้น ๆ ในส่วนของโครงสร้างพื้นฐาน (Infrastructure) จะต้องทราบเกี่ยวกับ Change Category, Change Classification, Environment Affected ดังภาพ

Received: August 8, 2019, Revised: November 18, 2019, Accepted: December 27, 2019
http://doi.org/..

Change Category	☐ Emergency ☐ Normal
Change Classification	☐ Database *(e.g. new or changed, interfaces between Databases)* ☐ Hardware *(e.g., new servers, changes to existing servers, storage devices)* ☐ Network *(e.g., LAN, WAN, inter server changes)* ☐ Operating System *(e.g., Windows, UNIX, Linux)* ☐ Data Center - *environment changes (e.g., cabling, A/C, UPS)* ☐ Back-up *(e.g., scheduling, change files to be backed up)* ☐ Other *(changes that do not fit in the above categories)* .....
Environment Affected	☐ Production ☐ Development ☐ Test / QA ☐ Others .....
Configuration Items	

ภาพที่ 7 ตัวอย่างแบบฟอร์ม Infrastructure Change Request form

รวมถึงการบันทึกแผนกู้คืนระบบสู่สถานะตั้งต้นก่อนการเปลี่ยนแปลง (Back-Out Plan) ให้ถูกต้องครบถ้วน เป็นต้น ในส่วนของระบบงาน (Application) จะต้องทราบรายละเอียดและมีความเข้าใจในกระบวนการ Action plan, Unit Test & UAT Test, Setup & Configuration เป็นต้น

4. คณะกรรมการที่ประชุม Change Advisory Board (CAB) ติดภารกิจ อาจจะมีการเลื่อนการประชุม ส่งผลให้แผนการดำเนินการล่าช้าออกไป หรือ ติดภารกิจไม่สามารถร่วมประชุมได้จะต้องแต่งตั้งผู้ทำหน้าที่ปฏิบัติราชการแทนเพื่อพิจารณาอนุมัติแทนได้

5. รายการที่จะนำเข้าที่ประชุม Change Advisory Board (CAB) ผู้ทำหน้าที่เลขาจะต้องกลั่นกรองรายการเพื่อให้อยู่ในขอบเขตที่จะนำเข้าสู่กระบวนการ ซึ่งกรณีของคณะแพทยศาสตร์ศิริราชพยาบาลนั้นจะมีขอบเขตการดำเนินงานภายใต้การพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) จะครอบคลุมในส่วนของโครงสร้างพื้นฐาน (Infrastructure) และระบบงาน (Application) เท่านั้น

สรุป

การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) หรือ ISO27001:2013 ในส่วนของกระบวนการควบคุมการเปลี่ยนแปลง (Change Control Procedure) เป็นกระบวนการที่ช่วยควบคุมการเปลี่ยนแปลง ในด้านโครงสร้างพื้นฐาน (Infrastructure Change) และระบบงาน (Application) ให้มีประสิทธิภาพ ต้องมีขั้นตอนการดำเนินงานที่มีความชัดเจน ตั้งแต่การจัดตั้งคณะกรรมการที่ประชุม Change Advisory Board (CAB) การกำหนดแบบฟอร์ม กำหนดบทบาทหน้าที่ของแต่ความรับผิดชอบ กำหนดลักษณะการเปลี่ยนแปลงแต่ละรูปแบบ รวมถึงจัดทำคู่มือเพื่อเป็นแนวทางในการปฏิบัติงานให้เป็นไปในแนวทางเดียวกัน และผู้ปฏิบัติงานมีความตระหนักถึงความสำคัญให้ความร่วมมือเป็นอย่างดี ส่งผลให้การดำเนินการเปลี่ยนแปลงสำเร็จตามเป้าหมาย ทั้งยังเป็นกระบวนการที่ใช้พิจารณาเมื่อการตรวจติดตามผล (Surveillance Audit) ซึ่งในแต่ละครั้งจะได้รับคำแนะนำเพื่อนำปรับปรุงทบทวนกระบวนการและปรับปรุงเอกสารแบบฟอร์มให้มีความครอบคลุมมากยิ่งขึ้น

Received: August 8, 2019, Revised: November 18, 2019, Accepted: December 27, 2019
http://doi.org/..

กิตติกรรมประกาศ

บทความทางวิชาการฉบับนี้สำเร็จได้ด้วยการสนับสนุนจากฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล ที่ได้ดำเนินการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) ตามมาตรฐาน ISO/IEC 27001:2013 ผู้เขียนได้มีโอกาสเข้าร่วมเป็นส่วนหนึ่งในการดำเนินการในส่วนของการควบคุมการเปลี่ยนแปลง (Change Control Procedure) ได้ความรู้ ความเข้าใจ และ มีหน้าที่รับผิดชอบในส่วนของ Infrastructure Change Control Procedure ในปัจจุบัน ผู้เขียนขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

เอกสารอ้างอิง

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (2562).กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์. สืบค้นเมื่อ 11 พฤศจิกายน 2562 จาก https://www.etcommission.go.th/files/law/law_type_etransaction_estimate_impact_of_etransaction.pdf

คณะแพทยศาสตร์ศิริราชพยาบาล. (2562). รู้จักองค์กร. สืบค้นเมื่อ 24 กรกฎาคม 2562 จาก https://www.si.mahidol.ac.th/th/history.asp

อรวรรณ เพ็ชรวงศ์. (2562). วิธีปฏิบัติงาน เรื่อง: การควบคุมการเปลี่ยนแปลง (Change Control Procedure). ฝ่ายสารสนเทศ, คณะแพทยศาสตร์ศิริราชพยาบาล, มหาวิทยาลัยมหิดล.

Coders, A. (2019). Changes to ISO 27001: What's new in the 2013 ISO 27001 update?. Retrieved from http://www.aliencoders.org/content/changes-to-iso-27001-whats-new-in-the-2013-iso-27001-update/.

International Standard Organization. (2013). Information technology Security techniques Information security management systems Requirements. (2nd Ed.). Geneva, Switzerland: ISO copyright office.

UCISA ITIL. (2019). A Guide to Change Management. Retrieved from https://www.ucisa.ac.uk/-/media/files/members/activities/itil/servicetransition/chanage_management/itil_a%20guide%20to%20change%20management%20pdf.ashx?la=en.