การพัฒนากรอบความมั่นคงปลอดภัยสำหรับศูนย์ข้อมูล
กรณีศึกษา บริษัท เบทาโกร จำกัด (มหาชน)

The Development of Security Framework for Data Center A Case Study of Betagro Co. Ltd.

นายวรวุฒิ เจ็งสืบสันต์[1] และ ดร.เทพฤทธิ์ บัณฑิตวัฒนาวงศ์[2]
[1,2]หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาระบบสารสนเทศคอมพิวเตอร์
คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม 61 ถ.พหลโยธินจตุจักรกรุงเทพ 10900
E-mail: [1]worawuth.che@hotmail.com, [2]thepparit.ba@spu.ac.th

บทคัดย่อ

สารนิพนธ์ฉบับนี้เป็นการพัฒนากรอบความมั่นคงปลอดภัยสำหรับศูนย์ข้อมูลบริษัท เบทาโกร จำกัด เนื่องจากข้อมูลและสารสนเทศภายในองค์กร ถือเป็นทรัพย์สินที่มีความสำคัญขององค์กร จึงจำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการดำเนินงานทางธุรกิจขององค์กรได้อย่างมีประสิทธิภาพและต่อเนื่อง จึงมีความตระหนักถึงความสำคัญของข้อมูลและสารสนเทศในศูนย์ข้อมูล

อาจมีปัจจัยภายนอกและภายในมากระทบต่อการให้บริการของศูนย์ข้อมูล ซึ่งก่อให้เกิดความเสียหายและความต่อเนื่องในการดำเนินธุรกิจได้ ดังนั้นจึงได้มีการพัฒนากรอบความมั่นคงสำหรับศูนย์ข้อมูลขึ้นจากสถานการณ์ฉุกเฉินและความไม่แน่นอนต่างๆ เพื่อเป็นกรอบแนวทางในการดูแลรักษาและรองรับการให้บริการของศูนย์ข้อมูล ให้สามารถดำเนินธุรกิจต่างๆขององค์กรได้อย่างต่อเนื่อง และมีมาตรฐานที่เป็นสากล

คำสำคัญ—ข้อมูลและสารสนเทศ, ความเสี่ยง, ความมั่นคง, การจัดการความเสี่ยง, ศูนย์ข้อมูล, มาตรฐาน ISO 27001

ABSTRACT

This project is the development of security framework for data center of Betagro Public Company Limited. The data and information within an organization is an important asset of the organization. It needs to be maintained to ensure the safety and security, which can be beneficial to an organization's business operations effectively and continuously. Thus, there is an awareness of the importance of data and information in a data center.

The External and internal factors that may have an impact on services of data center which cause damage and ensure continuity of business operations. Therefore, it has developed a framework on security for data center of emergency and uncertainties to the guidelines on the care and support services for data center to be able to conduct business in the organization’s ongoing and standards are universal.

KEY WORDS: —Data and Information, risk, Security, Risk Management, Data Center, Standard ISO 27001

1. บทนำ

นับตั้งแต่อดีต แต่ละองค์กรได้ให้ความสำคัญต่อข้อมูลทุกประเภทที่มีความเกี่ยวข้องกับการดำเนินธุรกิจขององค์กร เช่น ข้อมูลในการประกอบธุรกิจ ข้อมูลในการดำเนินการซื้อขาย ข้อมูลที่เป็นข้อตกลง หรือสัญญาต่างๆระหว่างองค์กรกับคู่ค้าหรือลูกค้า เป็นต้น ซึ่งข้อมูลเหล่านี้ถือเป็นทรัพยากรอันมีค่าอย่างยิ่ง เพราะหากถูกเปิดเผยหรือเกิดการสูญหายหรือเกิดเหตุการณ์ที่คาดไม่ถึง เช่น ภัยที่เกิดจากบุคคล ได้แก่ การก่อจลาจล ไฟไหม้ หรือภัยที่เกิดจากธรรมชาติ เช่น น้ำท่วม แผ่นดินไหว ตึกถล่ม เป็นต้น อาจทำให้มีผลกระทบต่อความต่อเนื่องในการดำเนินธุรกิจอย่างหลีกเลี่ยงไม่ได้ เช่น ถูกเอารัดเอาเปรียบ ทำให้เสื่อมเสียชื่อเสียง หรือส่งผลกระทบอื่นตามมา

ได้ ดังนั้น แต่ละองค์กรจึงได้มีการคิดค้นวิธีการในการป้องกันข้อมูลสำคัญๆเหล่านั้นโดยการนำระบบสารสนเทศเข้ามาช่วยในการบริหารจัดการข้อมูลเหล่านั้นให้รอดพ้นจากภัยคุกคามและผู้ไม่ประสงค์ดีอย่างต่อเนื่อง

ด้วยความก้าวหน้าด้านวิทยาศาสตร์และเทคโนโลยีสารสนเทศในปัจจุบัน มีเทคโนโลยีต่างๆที่สามารถอำนวยความสะดวกสบายและรวดเร็วในการดำเนินธุรกิจได้มากขึ้น องค์กรสามารถนำเทคโนโลยีเข้ามาช่วยควบคุมคุณภาพการผลิต ควบคุมการดำเนินการ ควบคุมการบริหารจัดการระบบงานต่างๆ เพื่อเพิ่มประสิทธิภาพในการทำงานและช่วยลดต้นทุนในการผลิตได้เป็นอย่างมาก ทำให้การติดต่อสื่อสาร การจัดเก็บข้อมูลและการแลกเปลี่ยนข้อมูลโดยใช้เทคโนโลยีสารสนเทศได้รับความนิยมเป็นอย่างสูง ด้วยสาเหตุนี้เอง องค์กรส่วนใหญ่จึงนิยมจัดเก็บข้อมูลที่มีความสำคัญต่างๆในรูปแบบของข้อมูลสารสนเทศ ภายในศูนย์ข้อมูลขององค์กรนั้นๆ ซึ่งจะง่ายต่อการจัดเก็บ และการบำรุงรักษาและการแลกเปลี่ยนข้อมูล โดยที่ข้อมูลทั้งหมดที่เก็บรวบรวมไว้จะถูกประมวลผลและเลือกสรรเพื่อนำไปใช้ประโยชน์ตาม วัตถุประสงค์และเป้าหมายขององค์กรมากที่สุด และมีการบริหารจัดการที่ให้ความสำคัญต่อความพร้อมใช้ของข้อมูลสารสนเทศเหล่านั้นด้วย ดังนั้น จากที่ได้กล่าวถึงความสำคัญของข้อมูลสารสนเทศข้างต้นแล้ว จะสามารถวิเคราะห์ได้ว่าข้อมูลสารสนเทศที่ดี ควรจะต้องเป็นข้อมูลที่ได้รับการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศเป็นอย่างดี เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึง ใช้งาน เปิดเผย แก้ไขเปลี่ยนแปลง ทำซ้ำ ตรวจจับ หรือขัดขวางการเข้าใช้งานข้อมูลสารสนเทศตามปกติ และระบบสานสนเทศที่ดีควรมีสภาพความพร้อมใช้ที่ดีอยู่เสมอ ทำให้องค์กรที่มีการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจ จำเป็นต้องมีการปรับปรุงและพัฒนานโยบายด้านมาตรฐานความปลอดภัยของข้อมูลสารสนเทศขององค์กรอย่างสม่ำเสมอรวมถึงมีการบริหารความเสี่ยงขององค์กรได้อย่างเหมาะสมและป้องกันไม่ให้เกิดเหตุการณ์ที่ไม่ทราบได้ล่วงหน้า

<u>กรณีศึกษา</u> ด้วยความก้าวหน้าทางเทคโนโลยีและความสำคุญของข้อมูลในยุคปัจจุบัน ทำให้บริษัทฯ ได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยให้กับข้อมูลสารสนเทศเป็นอย่างมาก และเนื่องจากทางบริษัทฯ มีหน่วยงานภายในและมีศูนย์ข้อมูล ที่มีหน้าที่ดูแลเกี่ยวกับการให้บริการระบบสารสนเทศขององค์กร จึงจำเป็นต้องมีมาตรการรักษาความปลอดภัยของข้อมูลสารสนเทศต่างๆภายในองค์กร ให้มีความมั่นคงปลอดภัยสูงสุด เพื่อให้ปราศจากภัยคุกคามต่างๆ รวมถึงมีผลกระทบในการให้บริการ เพื่อความต่อเนื่องในการดำเนินธุรกิจของบริษัทฯต่อไป

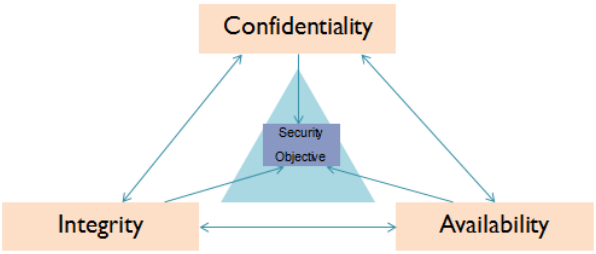
ในด้านมาตรการรักษาความมั่นคงปลอดภัยและแผนความต่อเนื่องทางธุรกิจ บริษัทฯได้วางแผนจัดทำนโยบายด้านมาตรฐานความมั่นคงปลอดภัยสารสนเทศโดยใช้หลักเกณฑ์มาตรฐานISO27001 ซึ่งเป็นมาตรฐานสากลในด้านการบริหารความมั่นคงปลอดภัยและการบริหารความเสี่ยงในการดำเนินธุรกิจขององค์กร เนื่องจากมีแนวทางในการบริหารจัดการที่มีขั้นตอนและวิธีปฏิบัติที่ครอบคลุมในทุกๆด้าน และทางบริษัทฯ มีการสนับสนุนให้มีการนำมาปรับใช้กับองค์กรอย่างจริงจังอยู่แล้ว จึงได้อนุญาตให้ผู้จัดทำใช้องค์กรเป็นกรณีศึกษา เพื่อจะได้มีการตรวจสอบ ปรับปรุง และลดความเสี่ยงด้านความมั่นคงปลอดภัยของศูนย์ข้อมูลขององค์กรให้เป็นไปตามวัตถุประสงค์ที่ตั้งไว้ รวมไปถึง การป้องกันภัยคุกคามต่างๆที่อาจมีผลกระทบกับธุรกิจองค์กรหรือบุคคลภายนอกที่เกี่ยวข้อง เช่น ผู้ใช้บริการภายใน ลูกค้า หรือ คู่ค้า ได้อีกด้วย

2. ทฤษฎี มาตรฐาน และการศึกษาที่เกี่ยวข้อง

2.1 ความมั่นคงปลอดภัยสารสนเทศ (Information Security)

การรักษาความมั่นคงปลอดภัยสารสนเทศมีจุดมุ่งหมายเพื่อปกป้องข้อมูล และระบบสารสนเทศขององค์กรจากผู้ที่ไม่มีสิทธิในการเข้าถึงในการอ่านหรือการใช้งาน การเปิดเผยข้อมูลระบบสารสนเทศ การขัดขวางการใช้งานหรือการให้บริการ รวมไปถึงการแก้ไขเปลี่ยนแปลงข้อมูล และการทำสำเนาข้อมูลอีกด้วย

วิธีการในการรักษาความมั่นคงปลอดภัยของแต่ละองค์กรนั้นล้วนมีวิธีการที่แตกต่างกันออกไป ซึ่งไม่มีผู้ใดสามารถสรุปได้ว่าวิธีการใดที่สามารถแก้ปัญหาที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลได้อย่างครบถ้วนสมบูรณ์ที่สุด แต่การที่จะบอกว่าข้อมูลนั้นมีความมั่นคงปลอดภัยหรือไม่นั้น สามารถวิเคราะห์ได้จากการรักษาคุณสมบัติ 3 ประการของข้อมูลสารสนเทศ ดังรูปที่ 2.1

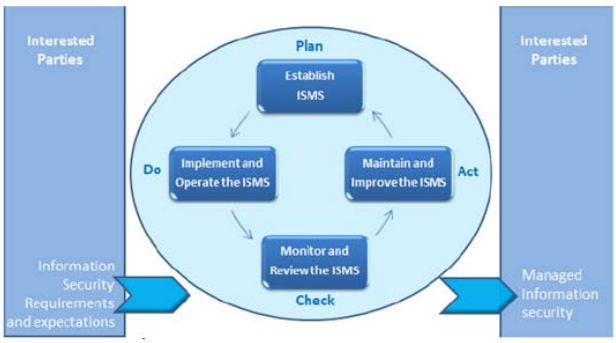


รูปที่ 2.1 แสดงการรักษาคุณสมบัติ 3 ประการของข้อมูลสารสนเทศ

ซึ่งเป็นที่นิยมเรียกกันว่า CIA ซึ่งได้แก่ ความลับของข้อมูล (Confidentiality) ความคงสภาพของข้อมูล (Integrity) และสภาพความพร้อมใช้ของข้อมูล (Available)

2.2 มาตรฐาน ISO/IEC 27001

เป็นขององค์กรที่มีชื่อว่า The International Organization of Standardization (ISO) และ The International Electrotecnical Commission (IEC) เป็นมาตรฐานเกี่ยวกับการบริหารการรักษาความมั่นคงปลอดภัยของข้อมูล ซึ่งใช้เป็นแนวทางในการสร้าง ดูแลรักษา และปรับปรุงระบบบริหารการรักษาความมั่นคงปลอดภัยข้อมูล (Information Security Management System) โดยแนวทางในการบริหารการรักษาความมั่นคงปลอดภัยของข้อมูลนั้นจะมีโครงสร้างที่เรียกว่า Plan-Do-Check-Act ซึ่งประกอบไปด้วยขั้นตอน การวางแผน (Plan) การลงมือทำ (Do) การตรวจสอบ (Check) และการปรับปรุงแก้ไข (Act) ดังรูปที่ 2.2



รูปที่ 2.2 แสดงภาพวงจรการทำงานของมาตรฐาน ISO 27001

นอกจากนั้นในส่วนของ Annex A ของมาตรฐาน ISO/IEC27001 ยังได้กำหนดวัตถุประสงค์และรายการควบคุมต่างๆที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยแบ่งออกเป็นหมวดหมู่ทั้งสิ้นจำนวน 11 หมวด ดังต่อไปนี้

- นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)
- โครงสร้างความมั่นคงปลอดภัยขององค์กร (Organization of Information Security)
- การบริหารจัดการทรัพสินขององค์กร (Asset Management)
- ความมั่นคงปลอดภัยเกี่ยวกับบุคลากรในองค์กร (Human Resources Security)
- ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร (Physical and Environmental Security)
- การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and Operations Management)
- การควบคุมการเข้าถึงระบบสารสนเทศขององค์กร (Access Control)
- การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development and Maintenance)
- การบริหารจัดการเหตุการณ์ที่ข้องกับความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)
- การบริหารความต่อเนื่องในการดำเนินธุรกิจขององค์กร (Business Continuity Management)
- การปฏิบัติที่สอดคล้องตามข้อกำหนดทางด้านกฎหมาย นโยบายความมั่นคงปลอดภัย มาตรฐาน ข้อกำหนดทางเทคนิค และการดำเนินการตรวจประเมินสารสนเทศ (Compliance)

2.3 การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจจะเกิดขึ้นภายใน สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบให้เกิดความเสียหาย หรือโอกาสที่จะทำให้องค์กรประสบความสำเร็จในทุกๆด้าน

ปัจจัยเสี่ยง (Risk Factor) หมายถึง สาเหตุทำให้องค์กรไม่บรรลุเป้าหมายตามที่ องค์กรกำหนดและสาเหตุของความเสี่ยงที่แท้จริง เพื่อจะได้นำมาวิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

ดังนั้นความหมายของการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร คือ การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร คือ กระบวนการการทำงานที่ช่วยให้ ผู้บริการระบบเทคโนโลยีสารสนเทศ สามารถสร้าง มาตรการในการป้องกันเพื่อให้องค์กรประสบผลสำเร็จของในการดำเนินธุรกิจด้วยการปกป้องระบบเทคโนโลยีสารสนเทศและข้อมูลสำคัญ ซึ่งจะช่วยสนับสนุนความสำเร็จขององค์กร

ปัจจัยเสี่ยงจากภายนอก (External Risk Factors) คือ ความเสี่ยงที่องค์กร ควบคุมได้ยากหรือไม่สามารถควบคุมการเกิดได้เลยอันส่งผลกระทบต่อแผนกลยุทธ์เพื่อให้บรรลุเป้าหมายในสถานการณ์ปัจจุบันเช่น การเปลี่ยนแปลงของเศรษฐกิจ สังคม การเมือง เทคโนโลยี สิ่งแวดล้อมสถานการณ์การแข่งขันทางธุรกิจความต้องการของลูกค้ารวมถึงกฎหมายและระเบียบทางราชการ

ปัจจัยเสี่ยงจากภายใน (Internal Risk Factors) คือ ความเสี่ยงที่องค์กรสามารถควบคุมได้ แต่สามารถส่งผลกระทบต่อแผนกลยุทธ์เพื่อให้บรรลุเป้าหมายขององค์กร โดยแต่ละองค์กรย่อมมีปัจจัยเสี่ยงที่แตกต่างกันไปตามลักษณะของการดำเนินธุรกิจในแต่ละองค์กรซึ่งอาจมีได้หลากหลายปัจจัย ที่เข้ามาเกี่ยวข้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความ เสี่ยงการวิเคราะห์ความเสี่ยงและจัดลำดับความเสี่ยงโดยประเมินจากโอกาสที่จะเกิน (Likelihood) และส่งผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น 4 ระดับคือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการ บริหารจัดการเพื่อลดเหตุการณ์ที่เกิดความเสี่ยงลดลง อันส่งผลกระทบให้เกิดความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดย สรุปได้เป็น 4 แบบ คือการยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการขององค์กรบรรลุเป้าหมายแบ่งได้ 4 ประเภท คือ ป้องกัน ตรวจสอบ การชี้แนะ และการแก้ไขหลักการวิเคราะห์ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organization of the Tread way Commission) มีดังนี้

- การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
- การระบุความเสี่ยง (Event Identification)
- การประเมินความเสี่ยง (Risk Assessment)
- กลยุทธ์ที่ใช้ในการจัดการความเสี่ยงแต่ล่อย่าง (Risk Response)
- กิจกรรมการบริหารความเสี่ยง (Control Activities)
- ข้อมูลและการสื่อสารด้านในการบริหารความเสี่ยง (Information and Communication)
- การติดตามผลและเฝ้าระวังความเสี่ยง (Monitoring)

2.4 กระบวนการจัดการความเสี่ยง (Risk Management Process)

หมายถึง กระบวนการดำเนินงานต่างๆ เพื่อลดสาเหตุของแต่ละโอกาสที่จะทำให้เกิดความเสียหาย เพื่อควบคุมระดับของความเสี่ยง และผลกระทบที่จะเกิดขึ้นในอนาคต ให้อยู่ในระดับที่สามารถยอมรับได้ ประเมินได้ควบคุมได้ และตรวจสอบได้อย่างมีระบบ ดังรูปที่ 2.3

รูปที่ 2.3 แสดงขั้นตอนการบริหารความเสี่ยง

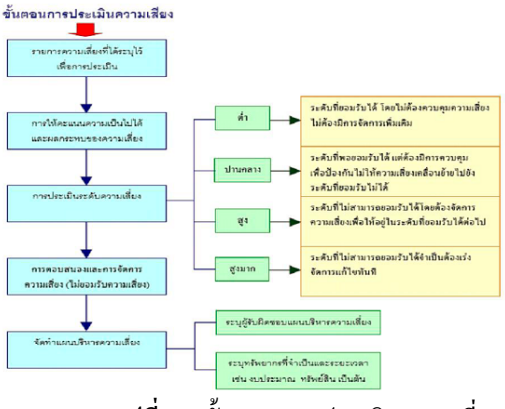
วัตถุประสงค์ของการบริหารจัดการความเสี่ยง

- เพื่อเตรียมพร้อมรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับองค์กรได้ตลอดเวลา
- เพื่อให้มีการวางแผน การควบคุม การป้องกันความเสี่ยง และแนวทางการแก้ปัญหาแต่ละความเสี่ยง
- เป็นการตรวจสอบเกี่ยวกับการบริหารจัดการและบริหารความเสี่ยงภายในองค์กรให้มีประสิทธิภาพ
- เพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงผลกระทบกับการดำเนินงาน วัตถุประสงค์และนโยบาย และหาวิธีจัดการกับความเสี่ยงเหล่านั้น
- เพื่อนำเทคโนโลยีสารสนเทศมาสนับสนุนการทำงานให้เกิดประสิทธิภาพสูงสุด การติดต่อสื่อสารเกิดประสิทธิภาพ และลดโอกาสความเสียหายที่อาจจะเกิดขึ้นทั้งทางตรงและทางอ้อม

ขั้นตอนการจัดการความเสี่ยง

- การบ่งชี้เหตุการณ์ (Identify) คือ เป็นการระบุชี้ว่าองค์กรมีผลกระทบ ลักษณะใดหรือขอบเขตเป็นอย่างไร ซึ่งขั้นตอนนี้ถือเป็นขั้นตอนแรกของการบริหารความเสี่ยง
- การประเมินและการวิเคราะห์ คือ กระบวนการระบุหาความเสี่ยงที่สำคัญขององค์กร ประเมินผลกระทบของความเสี่ยง โดยจะประเมินความเสี่ยงเป็นการวัดค่าระดับความเสี่ยง (Risk Score)

การประเมินความเสี่ยงจะเป็นการประเมินถึงผลกระทบของความเสี่ยงและความเป็นไปได้ที่จะเกิดความเสี่ยง ซึ่งการให้คะแนนในการประเมินความเสี่ยงนี้ขึ้นอยู่กับประสบการณ์ของผู้ประเมิน ดังแสดงในรูปที่ 2.4



รูปที่ 2.4 ขั้นตอนการประเมินความเสี่ยง

3. วิธีการดำเนินงาน

ลำดับขั้นตอนการดำเนินงาน สามารถสรุปได้ดังตารางที่ 3.1

ลำดับ	ขั้นตอนการดำเนินงาน	ผลลัพธ์ที่ได้
1	ศึกษาข้อกำหนดและมาตรฐานที่เกี่ยวข้องกับการดำเนินงาน	มีความรู้ความเข้าใจเกี่ยวกับข้อกำหนดของแต่ละมาตรฐานที่เกี่ยวข้องกับการดำเนินงาน
2	กำหนดขอบเขตการดำเนินงาน	ขอบเขตการดำเนินงาน
3	ระบุขั้นตอนวิธีการการดำเนินงานและเกณฑ์การยอมรับความเสี่ยงรวมถึงกำหนดระดับผลกระทบ (Impact) และโอกาสในการเกิด(Likelihood) ของความเสี่ยงด้านต่างๆ	ทราบขั้นตอนการประเมินความเสี่ยงและเกณฑ์การยอมรับความเสี่ยง
4	ระบุรายชื่อของสินทรัพย์ที่อยู่ภายในขอบเขต	ได้รายชื่อของสินทรัพย์ทั้งหมดภายในศูนย์ข้อมูล
5	ดำเนินการประเมินความเสี่ยงพร้อมกำหนดระดับของความเสี่ยง	ได้ระดับความเสี่ยงในหัวข้อที่เลือกนำมาปรับใช้กับองค์กร
6	เลือกตัวควบคุมที่เกี่ยวข้อง จากมาตรฐาน ISO 27001 : 2005 เพื่อนำมาปรับใช้กับศูนย์ข้อมูล	ได้ตัวควบคุมในการนำมาปรับใช้ในการควบคุมความเสี่ยงของศูนย์ข้อมูล
7	ดำเนินการพัฒนากรอบความมั่นคงทางธุรกิจสำหรับศูนย์ข้อมูล	กรอบความมั่นคงของศูนย์ข้อมูล
8	สรุปผลการดำเนินงาน	ผลการพัฒนากรอบความมั่นคงของทางธุรกิจศูนย์ข้อมูล รวมถึงความเสี่ยงที่ยังคงเหลืออยู่

ตารางที่ 3.1 ขั้นตอนและวิธีการดำเนินงาน

3.1 ศึกษาเอกสารที่เกี่ยวข้องรวมถึงระบุขอบเขตของการดำเนินงาน

1. เอกสารภายใน (Internal Document)

- นโยบายเดิมที่มีอยู่ของศูนย์ข้อมูล
- แผนผังและโครงสร้างของศูนย์ข้อมูล (Organization Chart)
- โครงสร้างของระบบเครือข่ายของศูนย์ข้อมูล (Network & Instruction Layout)
- ขั้นตอนการทำงานต่างๆภายในศูนย์ข้อมูล (Work Instruction)
- แบบฟอร์มและบันทึกการทำงาน (Form and Records)

2. เอกสารภายนอก (External Document)

- มาตรฐาน ISO 27001: 2005
- พ.ร.บ ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
- เอกสารงานวิจัยที่เกี่ยวข้อง
- เอกสารและบทความต่างๆที่มีความน่าเชื่อถือ
- ความรู้และเทคโนโลยีด้านความมั่นคงของระบบคอมพิวเตอร์และเครือข่าย

3. ขอบเขตในการดำเนินงาน

- ศูนย์ข้อมูลบริษัท เบทาโกร จำกัด (มหาชน)

3.2 การศึกษาระบบการทำงานรวมถึงการระบุทรัพย์สินในขอบเขต

1) การสัมภาษณ์ (Interview) เพื่อนำข้อมูลไปวิเคราะห์หาสาเหตุและปัญหา 2) การสังเกต (Observation) พิจารณาจากขั้นตอนการปฏิบัติงานเหตุการณ์ต่างๆที่เกิดขึ้น 3) การระดมสมอง (Brainstorm) เป็นการประชุมร่วมกันจากคณะดำเนินงานที่เกี่ยวข้อง เพื่อให้ได้ข้อสรุปเกี่ยกับระบบงาน การปฏิบัติงานและสินทรัพย์ในขอบเขตงาน

3.3 ขั้นตอนการวิเคราะห์ความเสี่ยงและการประเมินความเสี่ยง

1. วิธีการวิเคราะห์ความเสี่ยง (Risk Analysis)

1.1 การระบุสินทรัพย์ (Indentify Asset) ขั้นตอนการการดำเนินงานของมาตรฐาน ISO 27001/IEC 27001:2005 จำเป็นต้องมีการระบุสินทรัพย์ทั้งหมดที่เกี่ยวข้องภายในศูนย์ข้อมูล ซึ่งข้อมูลสินทรัพย์จะถูกมาประเมินความเสี่ยงและจัดลำดับความเสี่ยง โดยแบ่งแยกประเภทของทรัพย์สินและเลือกมาตรการการควบคุมที่เหมาะสมสำหรับการป้องกันความเสี่ยงที่เกิดขึ้นโดยทางบริษัท เบทาโกร จำกัด (มหาชน) ได้มีการแบ่งประเภทสินทรัพย์ของศูนย์ข้อมูลออกเป็น 4 ประเภท ดังนี้

1) ฮาร์ดแวร์ (Hardware)

ก) สินทรัพย์ภายในศูนย์ขอมูล ได้แก่ คอมพิวเตอร์เครื่องแม่ข่าย, อุปกรณ์ควบคุมการเข้าออก,เครื่องสำรองไฟฟ้า เป็นต้น

ข) สินทรัพย์ของระบบเครือข่าย ได้แก่ Switch Access Point, สายสัญญาณ เป็นต้น

2) ซอฟต์แวร์ (Software)

ก) ซอฟต์แวร์ระบบ ได้แก่ ระบบปฏิบัติการเครื่องแม่ข่าย, ระบบปฏิบัติการเครื่องคอมฯที่ใช้ในการดำเนินงาน เป็นต้น

ข) ซอฟต์แวร์ประยุกต์ ได้แก่ ซอฟต์แวร์ที่ใช้งานเฉพาะบนเครื่องแม่ข่าย,ซอฟต์แวร์ประยุกต์ที่ทำบนเครื่องคอมพิวเตอร์ทั่วไป เป็นต้น

3) สารสนเทศ (Information)

ก) ข้อมูลสารสนเทศ ได้แก่ ข้อมูลยอดขาย,ข้อมูลทางบัญชีการเงิน เป็นต้น

ข) เอกสารคู่มือการใช้งาน ได้แก่ คู่มือปฏิบัติงาน,คู่มือการติดตั้งซอฟต์แวร์ต่างๆ,แผนการดำเนินงานประจำปี เป็นต้น

4) บุคคลากร (Personal)

ก) ผู้ดูแลระบบได้แก่ เจ้าหน้าที่ดูแลระบบ,หัวหน้าแผนก เป็นต้น

1.2 การประเมินค่าสินทรัพย์

ความสำคัญและค่าของสินทรัพย์ นั้นวัดจากค่า CIA ที่สินทรัพย์มีต่อองค์กร โดยการนำข้อมูลสินทรัพย์ทั้งหมดมาระบุนัยสำคัญของสินทรัพย์ (Confidentiality, Integrity, Availability) พร้อมทั้งประเมินค่าสินทรัพย์ (Value) ตามหลักเกณฑ์ ดังตารางที่ 3.2 ดังต่อไปนี้

ประเด็นในการพิจารณา	ระดับคะแนนความสำคัญ		
	น้อย = 1	ปานกลาง = 2	มากที่สุด = 3
การรักษาความลับ/ความน่าเชื่อถือ Confidentiality (C)	เกิดความน่าเชื่อถือ/การรักษาความลับระดับบุคคล	เกิดความน่าเชื่อถือ/การรักษาความลับระดับแผนก	เกิดความน่าเชื่อถือ/การรักษาความลับระดับองค์กรและภายนอกองค์กร
ความถูกต้อง/ความมั่นคง Integrity (I)	เกิดความถูกต้อง/ความมั่นคงระดับบุคคล	เกิดความถูกต้อง/ความมั่นคงระดับแผนก	เกิดความถูกต้อง/ความมั่นคงระดับองค์กรและภายนอกองค์กร
ความพร้อมใช้ Availability (A)	เกิดความพร้อมใช้ระดับบุคคล	เกิดความพร้อมใช้ระดับแผนก	เกิดความพร้อมใช้ระดับองค์กรและภายนอกองค์กร
เชิงปริมาณ (V) หน่วย (บาท)	มูลค่าต่ำกว่า 10000 บาท	มูลค่า 10000 – 100000 บาท	มูลค่ามากกว่า 100000 บาท
เชิงคุณภาพ (Q) ผลคูณ (CIA)	ผลคูณ C.I.A 1 - 3 คะแนน	ผลคูณ C.I.A 4 - 8 คะแนน	ผลคูณ C.I.A มากกว่า 8 คะแนน

ตารางที่ 3.2 เกณฑ์ความสำคัญของสินทรัพย์

ในกรณีที่ไม่สามารถวัดเป็นมูลค่าได้จะคิดเชิงคุณภาพ ซึ่งได้กำหนดเกณฑ์ระดับความสำคัญไว้ 3 ระดับ ดังแสดงในตารางที่ 3.3

ระดับความสำคัญของสินทรัพย์	คะแนน C * I * A * เชิงปริมาณ (V) หรือ เชิงคุณภาพ (Q)
สินทรัพย์สำคัญน้อย	คะแนน 1 - 4
สินทรัพย์สำคัญปานกลาง	คะแนน 5 - 16
สินทรัพย์สำคัญมาก	มากกว่า 16 คะแนน

ตารางที่ 3.3 เกณฑ์ระดับความสำคัญของสินทรัพย์

1.3 ภัยคุกคาม ที่เกิดกับสินทรัพย์นั้นจะมีจุดอ่อนเป็นต้นเหตุเสมอ แต่จุดอ่อนที่เกิดขึ้นถ้าไม่มีภัยคุกคามก็อาจไม่เกิดความเสี่ยงของเหตุการณ์ขึ้นก็ได้ ดังตัวอย่างภายในตารางที่ 3.4 ดังต่อไปนี้

ภัยคุกคาม	ประเภทภัยคุกคาม
1	ภัยคุกคามจากข้อผิดพลาดจากการกระทำของมนุษย์
2	ภัยคกุคามจากการละเมิดทรัพย์สินทางปัญญา
3	ภัยคุกคามจากการบุกรุก
4	ภัยคุกคามจากการโจรกรรมข้อมูลสารสนเทศ
5	ภัยคุกคามจากการก่อวินาศกรรมหรือการทำลาย
6	ภัยคุกคามจากการโจรกรรม
7	ภัยคุกคามจากาการโจมตีซอฟต์แวร์
8	ภัยคุกคามจากธรรมชาติ
9	ภัยคุกคามจากคุณภาพการบริการ
10	ภัยคุกคามจากความล้มเหลวหรือข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์
11	ภัยคุกคามจากความล้มเหลวหรือข้อผิดพลาดทางเทคนิคของซอฟต์แวร์
12	ภัยคุกคามจากเทคโนโลยีล้าสมัย

ตารางที่ 3.4 ประเภทของภัยคุกคาม

การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นการกำหนดเกณฑ์ที่ใช้ในการประเมินความเสี่ยง ได้แก่ ระดับโอกาสในการเกิดความเสี่ยง (Likelihood) สามารถใช้ได้ทั้ง เกณฑ์เชิงปริมาณและเชิงคุณภาพ ดังแสดงในตารางที่ 3.5

ตารางที่ 3.5 เกณฑ์สรุประดับโอกาสที่จะเกิดความเสียหาย

ระดับความรุนแรงของผลกระทบ (Impact) ในเกณฑ์ปริมาณและเชิงคุณภาพ ดังแสดงในตารางที่ 3.6

ตารางที่ 3.6 เกณฑ์สรุประดับความรุนแรงของผลกระทบ

3.4 เกณฑ์การยอมรับความเสี่ยง

ในการยอมรับความเสี่ยงของศูนย์ข้อมูลได้มีการประเมินเพื่อกำหนดเกณฑ์ค่าระดับความเสี่ยงที่สามารถยอมรับได้ และเงื่อนไขที่จำเป็นต้องมีในการยอมรับความเสี่ยง หรือในกรณีที่ไม่สามารถยอมรับความเสี่ยงได้ จะต้องดำเนินการอะไรในการลดความเสี่ยงนั้น ดังแสดงในตารางที่ 3.7

ระดับคะแนน	ระดับความเสี่ยง	การยอมรับ	การดำเนินการเพิ่มเติม
1 - 5	ต่ำ	สามารถยอมรับได้ความเสี่ยง	การควบคุมที่มีอยู่เพียงพอ
6 - 12	ปานกลาง	ยอมรับได้บางส่วน	ต้องมีแผนลดความเสี่ยง
13 - 20	สูง	ไม่สามารถยอมรับได้	ต้องมีแผนลดความเสี่ยง
21 - 25	สูงมาก	ไม่สามารถยอมรับได้อย่างเด็ดขาดต้องดำเนินการลดความเสี่ยงอย่างรวดเร็วที่สุด	ต้องมีแผนลดความเสี่ยงและการควบคุมอย่างใกล้ชิดในการดำเนินการลดความเสี่ยงและมีการประเมินความเสี่ยงซ้ำ หรือต้องมีการถ่ายโอนความเสี่ยง

ตารางที่ 3.7 เกณฑ์ในการยอมรับความเสี่ยง

3.5 การบริหารความเสี่ยง

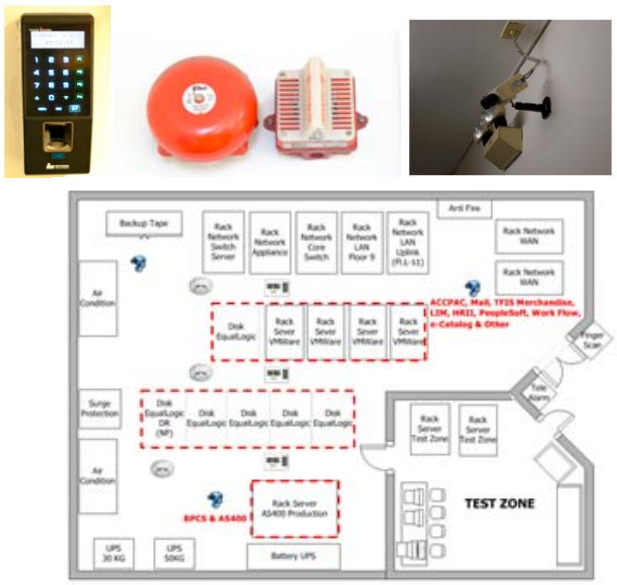
หลังจากการจัดลำดับความเสี่ยงที่มีนัยสำคัญ จะวิเคราะห์หาสาเหตุที่ทำให้เกิดความเสี่ยงและพิจารณาวิธีการควบคุมต่างๆ มีหลายวิธี ดังนี้

การลดความเสี่ยง (Risk Reduction) การยอมรับความเสี่ยง (Risk Acceptance) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) การโอนความเสี่ยง (Risk Transfer)

4. ผลการดำเนินงาน

4.1 สภาพแวดล้อมโดยทั่วไปของศูนย์ข้อมูลก่อนการดำเนินงาน

มีการสำรวจศึกษา แปลน สถานที่ตั้ง ซึ่งมีสภาพแวดล้อมและระบบรักษาความปลอดภัย ทั่วไปที่มีอยู่ในปัจจุบันของศูนย์ข้อมูล ดังรูปที่ 4.1



รูปที่ 4.1 สภาพแวดล้อมโดยทั่วไปของศูนย์ข้อมูล

4.2 ตัวอย่างเหตุการณ์และปัญหาที่เกิดกับศูนย์ข้อมูล

ดังแสดงในตารางที่ 4.1

ลำดับ	เหตุการณ์/ปัญหา	เวลาที่เกิด	หมายเหตุ
1	ไม่สามารถเข้าใช้งาน web mail จาก Internet ภายนอก และ sync main ผ่านมือถือได้	24/2/2014 : 17:25 น.	
2	ไม่สามารถเข้าใช้งาน Accpac โซนภาคใต้ได้	1/3/2014 : 18:35 น.	ไฟล์ License เสีย
3	ไม่สามารถเข้าใช้งาน Accpac โซนภาคกลาง ได้	1/3/2014 : 23:10 น.	ไฟล์ License เสีย
4	Disk EQL Group6 Box8 Slot 11 Failed	3/3/2014 : 13:30 น.	Disk เสีย
5	Disk EQL Group4 Power Supply Failed	8/3/2014 : 17:30 น.	Power Supply เสีย
6	Disk EQL Group6 Box8 Slot 8,13 Failed	10/3/2014 : 11:30 น.	Disk เสีย

ตารางที่ 4.1 ตัวอย่างปัญหาและเหตุการณ์ซึ่งกระทบกับศูนย์ข้อมูล

4.3 ตัวอย่างการวิเคราะห์และระบุภัยคุกคามที่มีต่อทรัพย์สินภายในศูนย์ข้อมูล

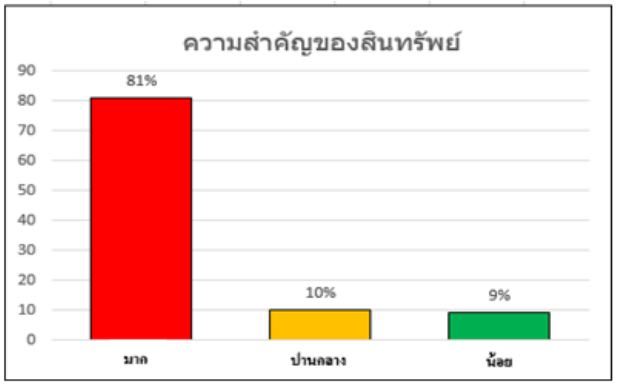
ดังแสดงรายละเอียดภายในตารางที่ 4.2

ตารางที่ 4.2 แสดงการประเมินภัยคุกคามสินทรัพย์ภายในศูนย์ข้อมูล

ลำดับ	Model	Serial Number	ระดับความสำคัญของสินทรัพย์	ชนิดภัยคุกคามที่อาจเกิดขึ้นได้
1	A5820X SERIE	CN18BFQ058	54 (H)	1,3,5,6,8,10,12
2	DELL POWER EDGE R815	4QBP82S	36 (H)	1,2,3,4,5,6,7,8,9,10,11,12
3	DELL POWER EDGE R815	1BFN82S	36 (H)	1,2,3,4,5,6,7,8,9,10,11,12
4	DELL POWER EDGE R815	F9FN82S	36 (H)	1,2,3,4,5,6,7,8,9,10,11,12
5	DELL POWER EDGE R815	52GM82S	36 (H)	1,2,3,4,5,6,7,8,9,10,11,12

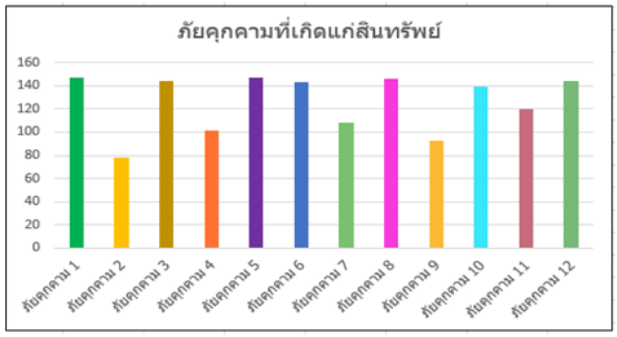
จากการประเมินความสำคัญและภัยคุกคามที่มีผลต่อสินทรัพย์ภายในศูนย์ข้อมูล สามารถจำแนกข้อมูลได้ ดังรูปที่ 4.2 และ 4.3 ดังนี้

ด้านความสำคัญของสินทรัพย์



รูปที่ 4.2 แสดงร้อยละความสำคัญของสินทรัพย์ภายในศูนย์ฯ

ด้านภัยคุกคามที่เกิดแก่สินทรัพย์



รูปที่ 4.3 แสดงระดับภัยคุกคามของสินทรัพย์ภายในศูนย์ข้อมูล

จากกราฟทั้งสองสามารถสรุปได้ว่า สินทรัพย์ทั้งหมดภายในศูนย์ข้อมูลล้วนมีความสำคัญมาก หากได้รับผลกระทบหรือมีความเสียหายเกิดขึ้นกับสินทรัพย์นั้นๆ โดยมีภัยคุกคามหลายๆชนิดที่มีโอกาสเกิดขึ้นกับสินทรัพย์เหล่านั้น

ซึ่งได้แก่ ภัยคุกคามจากข้อผิดพลาดจากการกระทำของมนุษย์ ภัยคุกคามจากการบุกรุก เป็นต้น

4.4 ตัวอย่างการประเมินความเสี่ยงและการวิเคราะห์ความเสี่ยง

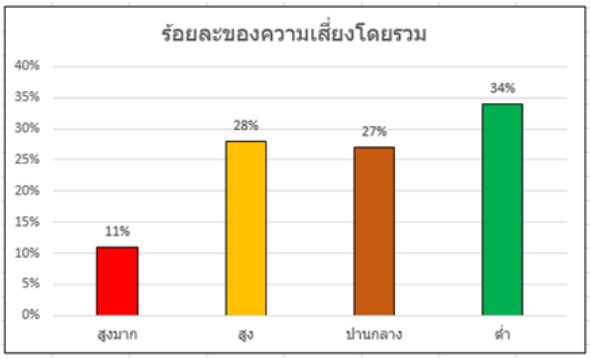
ดังแสดงตัวอย่างในตารางที่ 4.3

ตารางที่ 4.3 การประเมินความเสี่ยงและการวิเคราะห์ความเสี่ยง

เมื่อได้ประเมินความเสี่ยงเสร็จสิ้นแล้ว ได้มีการจัดระดับความเสี่ยงโดยแยกเป็นผลรวมตามระดับความเสี่ยงสูงมาก ระดับความเสี่ยงสูง ระดับความเสี่ยงปานกลาง และระดับความเสี่ยงต่ำ โดยแบ่งเป็นประเภทของสินทรัพย์ภายในศูนย์ข้อมูล ซึ่งจะทำให้เราทราบถึงระดับความเสี่ยง ในแต่ละประเภทของสินทรัพย์ และสามารถจัดระดับความสำคัญ ในการจัดทำกรอบฯ ดังตารางที่ 4.4 และรูปที่ 4.4 ดังนี้

สินทรัพย์	สูงมาก	สูง	ปานกลาง	ต่ำ
สินทรัพย์ประเภทฮาร์ดแวร์	1	10	9	2
สินทรัพย์ประเภทซอฟต์แวร์	0	4	2	4
สินทรัพย์ประเภทสารสนเทศ	2	0	3	7
สินทรัพย์ประเภทบุคคลากร	3	2	1	6
รวม	6	16	15	19

ตารางที่ 4.4 ผลการประเมินความเสี่ยง



รูปที่ 4.4 แสดงร้อยละความเสี่ยงโดยรวม

4.5 การกำหนดแนวทางและแนวปฏิบัติในการจัดการความเสี่ยงจากผลการประเมินความเสี่ยง

โดยพิจาณาตามหลักการควบคุมทางด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001 :2005 โดยเลือกเฉพาะความเสี่ยงที่อยู่ในระดับปานกลาง ระดับสูง และระดับสูงมาก ซึ่งประกอบไปด้วย

- การลดความเสี่ยง
- การถ่ายโอนความเสี่ยง
- การหลีกเลี่ยงความเสี่ยง
- การคงความเสี่ยง

โดยสามารถจัดทำเป็นกรอบการพัฒนาความมั่นคงของศูนย์ข้อมูลภายใต้มาตรฐาน ISO/IEC 27001 :2005 เพื่อประสานงานกับผู้เกี่ยวข้องทำการพัฒนาเป็นนโยบายในโอกาสต่อๆไป ดังตัวอย่างในตารางที่ 4.5

ลำดับ	แนวทางจัดการความเสี่ยง	ระดับความเสี่ยง
1	ความเสี่ยง เครื่องแม่ข่ายไม่สามารถให้บริการได้ ไม่มีข้อกำหนดการบำรุงรักษาเครื่องแม่ข่ายและอุปกรณ์อย่างถูกต้องและสม่ำเสมอ แนวทางจัดการความเสี่ยง ลดความเสี่ยง มีการกำหนดเงื่อนไขในการบำรุงรักษาเครื่องแม่ข่ายอย่างถูกต้องสม่ำเสมออย่างเคร่งครัด โดยมีการกำหนดระยะเวลาเป็นประจำทุก 1 เดือน หลักการควบคุม A.5.2.4) การบำรุงรักษาอุปกรณ์ (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน	ปานกลาง

ตารางที่ 4.5 การกำหนดแนวทางในการจัดการความเสี่ยงสำหรับสินทรัพย์ภายในศูนย์ข้อมูล

5. สรุปผลการดำเนินงานและข้อเสนอแนะ

จากการดำเนินงานตามขั้นตอน ทางเจ้าหน้าที่รวมถึงบุคคลากรภายในศูนย์ข้อมูล ได้ให้ความร่วมมือเป็นอย่างดี โดยในการพัฒนากรอบความมั่นคงปลอดภัยสำหรับศูนย์ข้อมูล บริษัท เบทาโกร จำกัด (มหาชน) ภายใต้ข้อกำหนดตามมาตรฐาน ISO/IEC 27001 : 2005 ทำให้เกิดกรอบแนวทางในการดำเนินงานด้านความมั่นคง ทำให้องค์กรได้รับรู้ถึงความเสี่ยง ปัจจัยเสี่ยงและจุดอ่อนด้านต่างๆของศูนย์ข้อมูลที่มีอยู่ ทำให้องค์กรสามารถหามาตรการป้องกันและลดความเสี่ยงได้อย่างมีประสิทธิภาพ โดยการนำความรู้ที่ได้จากการศึกษามาตรฐาน ISO/IEC 27001 : 2005 นั้นมาประยุกต์ใช้เพื่อเป็นแนวทางในการดำเนินงานเพื่อให้สอดคล้องกับขั้นตอนที่เป็นมาตรฐานสากล

ข้อเสนอแนะ

ในการพัฒนากรอบความมั่นคงปลอดภัยสำหรับศูนย์ข้อมูล บริษัท เบทาโกร จำกัด(มหาชน) เป็นการริเริ่มที่จะนำเอามาตรฐาน ISO/IEC 27001 เข้ามาเป็นแนวทางสำหรับการพัฒนาเป็นนโยบายฯ เพื่อยกระดับความปลอดภัยของศูนย์ข้อมูลและขององค์กรในโอกาสต่อๆไป จึงอาจเกิดปัญหาในด้านต่างๆ เช่น ด้านความรู้ความเข้าใจของผู้จัดทำ ด้านลำดับขั้นตอนการดำเนินงาน รวมถึงความทันสมัยของข้อมูลต่างๆ ซึ่งสิ่งเหล่านี้อาจทำให้กรอบความมั่นคงของศูนย์ข้อมูล ยังไม่ครบถ้วนหรือตรงตามความต้องการขององค์กร ซึ่งปัญหาเหล่านี้จะได้รับการแก้ไขต่อไปในอนาคตจากคณะทำงานขององค์กรซึ่งอาจมีการแก้ไขรวมถึงการทบทวนกรอบความมั่นคงสำหรับศูนย์ข้อมูลให้มีความถูกต้องสมบูรณ์และครบถ้วนมากยิ่งขึ้นในโอกาสต่อไป

บรรณานุกรม

[1] พิรมล เก่งคุมพล, "**การสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO 27001 ขององค์กร กรณีศึกษา บริษัท บิ๊กฟิช เอ็นเตอร์ไพร์ส จำกัด**," 2555

[2] IS0 27001 มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ [Online] Available at : ftp://hrm.moph.go.th/iso27001/iso-27001.pdf, [November 24,2553].

[3] ดวงกมล ทรัพย์พิทยากร, "**มาตรฐาน แนวปฏิบัติ และกรอบวิธีการต่างๆ ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ**," 2550

[4] ณัฐธิดา แซ่คู, "**การนำทฤษฎีการบริหารความเสี่ยงและทฤษฎีสร้างความมั่นคงปลอดภัย ในการใช้งานเทคโนโลยีสารสนเทศขององค์กร โดยใช้มาตรฐาน ISO/IEC 27001 เป็นพื้นฐานดำเนินการ**", วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ บัณฑิตวิทยาลัย, หมาวิทยาลัยศรีปทุม. 2556.

[5] Michael E. Whitman and Herbert J. Mattord, "**Principles of Information Security,**" 2554

[6] บรรจง หะรังษี, "**หัวใจหลักของกระบวนการระบบบริหารจัดการด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001**," 2554

[7] A.Prinya Hom-anek, "**7 ขั้นตอนในนำมาตรฐาน ISO/IEC 27001 และ ISO/IEC 27002 มาประยุกต์ใช้ในองค์กรเพื่อให้ได้ผลในทางปฏิบัติและสอดคล้องกับกฎหมายในปัจจุบัน และอนาคต,**" 2551

[8] บรรจง หะรังษี, "**Do-Plan-Check-Act ตามมาตรฐาน ISO/IEC 27001 กับข้อคำถามสำคัญที่ต้องการคำตอบ**," 2554

[9] ศูนย์เทคโนโลยีอิเลคทรอนิกส์และคอมพิวเตอร์แห่งชาติ, "**มาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2.5)**," 2550

ประวัติผู้วิจัย

นายวรวุฒิ เจ็งสืบสันต์ สำเร็จการศึกษาระดับปริญญาตรี จากคณะวิทยาศาสตร์และเทคโนโลยี สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี เมื่อปี พ.ศ. 2555 E-Mail : worawuth.che@hotmail.com

ดร.เทพฤทธิ์ บัณฑิตวัฒนาวงศ์ ปัจจุบันดำรงตำแหน่งอาจารย์พิเศษ ภาควิชาเทคโนโลยีสารสนเทศและการสื่อสาร คณะเทคโนโลยีสารสนเทศ สำเร็จการศึกษาปริญญาเอก : Doctor of Philosophy – Informatics The Graduate University for Advanced Studies มีความเชี่ยวชาญด้าน ระบบ Cloud Computing IP V6 และ Application Development E-mail : thepparit.ba@spu.ac.th