การประเมินความเสี่ยงระบบสารสนเทศและแนวทางแก้ไข กรณีศึกษา บริษัท อาร์ วี ซี คอนสตั๊คชั่น จำกัด

ณัฐนันท์ พรทวีวัฒน์[1]
ชัยพร เขมะภาตะพันธ์[2]

บทคัดย่อ

การประเมินความเสี่ยงระบบสารสนเทศและแนวทางแก้ไข กรณีศึกษา บริษัท อาร์ วี ซี คอนสตั๊คชั่น จำกัด มีวัตถุประสงค์ในการจัดทำเพื่อการประเมินความเสี่ยงด้านสารสนเทศขององค์กรโดยการประยุกต์ใช้มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013 มาเป็นแนวทางในการประเมินความเสี่ยง และหาแนวทางแก้ไขความเสี่ยงที่มีโดยจัดทำแผนการบริหารจัดการความเสี่ยงอย่างเหมาะสมตามสถานะขององค์กร และเพื่อจัดทำร่างนโยบายความปลอดภัยทางเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการปฏิบัติงาน ซึ่งองค์กรสามารถนำไปพัฒนาต่อยอดเพื่อขอตรวจสอบมาตรฐานหรือพัฒนากระบวนการสร้างความปลอดภัยและบริหารจัดการความเสี่ยงของระบบเทคโนโลยีสารสนเทศได้ในอนาคต

วิธีดำเนินการวิจัย ทำโดยการประเมินความเสี่ยงจากการประยุกต์ใช้มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013 ทั้ง 14 ข้อ ซึ่งแต่ละหัวข้อจะประกอบด้วยวัตถุประสงค์ที่แตกต่างกันจำนวน 35วัตถุประสงค์ และภายใต้วัตถุประสงค์ของแต่ละข้อนั้นจะประกอบไปด้วยมาตรการ ในการรักษาความมั่นคงปลอดภัยที่แตกต่างกันรวม 114มาตรการ และเมื่อดำเนินการประเมินความเสี่ยงก่อนการบริหารจัดการความเสี่ยงเรียบร้อยแล้ว จึงนำผลการดำเนินการดังกล่าวมาประมวลผล สรุปผล และหาแนวทางแก้ไข ซึ่งจะช่วยลดผลกระทบและสามารถบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และจัดทำร่างแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร เพื่อเป็นแนวทางในการปฏิบัติงาน เพื่อการลดผลกระทบที่อาจเกิดขึ้นในอนาคต และยังเป็นการเพิ่มประสิทธิภาพในการทำงานของระบบเทคโนโลยีสารสนเทศภายในองค์กรให้มีมาตรฐานเพิ่มมากขึ้น

Abstract

The dissertation of “Information System Risk Assessment and Solution Guidelines: A Case Study on RVC Construction Co., Ltd.” aimed to assess information

---

[1] นักศึกษาหหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรม มหาวิทยาลัยธุรกิจบัณฑิตย์

[2] อาจารย์ที่ปรึกษาสารนิพนธ์

system risk of the organization. ISO/IEC 27001:2013, a standard of information security management system (ISMS), was applied as a risk assessment guideline in order to find solution guidelines on available risks by providing proper risk management plans based on the organizational status; and to draft information security policies as an implementation guideline. Further development by the organization can be done in order to request for standard inspection, to develop security process, and to conduct IT risk management in the future.

For research implementation, risk assessment was conducted based on the entire 14 domains of ISO/IEC 27001:2013 applied. Each domain basically consists of 35 different objectives, each of which consists of 114 different security measures. After risk assessment before management, the results were processed, concluded, and searched for solution guidelines that could reduce and manage risks to remain at acceptable levels. Information security policies of the organization were drafted as an implementation guideline in order to reduce possible upcoming effects and to enhance the efficiency of internal IT system for better standard.

1. บทนำ

ในโลกยุคปัจจุบันเทคโนโลยีสารสนเทศ เข้ามามีบทบาทสำคัญในหลาย ๆด้าน องค์กรต่าง ๆอาศัยความก้าวหน้าของเทคโนโลยีสารสนเทศ เพื่อช่วยอำนวยความสะดวกให้งานเกิดประสิทธิภาพและความรวดเร็วมากยิ่งขึ้น เทคโนโลยีสารสนเทศอาจอยู่ในหลากหลายรูปแบบ ทั้ง ฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์โทรคมนาคม หรือ อินเทอร์เน็ต ในด้านการสื่อสาร เทคโนโลยีสารสนเทศก็มีส่วนช่วยให้สามารถติดต่อสื่อสารกันได้อย่างง่ายดายและสะดวกรวดเร็วมากขึ้น ซึ่งในการใช้เทคโนโลยีสารสนเทศนี้ มีความเสี่ยงมากมายที่อาจส่งผลกระทบต่อองค์กร อาจเป็นปัจจัยที่เข้ามาก่อให้เกิดความเสียหายต่อข้อมูลและทรัพย์สินขององค์กรได้ ความเสี่ยงที่เป็นภัยคุกคามนี้ อาจแบ่งได้เป็นหลายประเภท ยกตัวอย่าง เช่น 1.ภัยคุกคามจากคน ทั้งภายในและภายนอกองค์กร เช่น การฉ้อโกง, การ Hack, Social Engineering (การหลอกถามข้อมูล), การก่อวินาศกรรม, การโจรกรรม 2.ภัยธรรมชาติ เช่น น้ำท่วม, แผ่นดินไหว 3.ภัยคุกคามจากสภาพแวดล้อมที่ไม่เหมาะสม เช่น ไฟฟ้ารัดวงจร, น้ำรั่ว, ฝุ่นละออง, สารเคมี[1]

บริษัท อาร์ วี ซี คอนสตรั๊คชั่น จำกัด เป็นบริษัทรับออกแบบ ก่อสร้างบ้านพักอาศัยและอาคารสำนักงาน ก่อตั้งมานานกว่า 30 ปี มีการใช้งานเทคโนโลยีสารสนเทศในหลากหลายด้าน เพื่อให้การทำงานมีความสะดวกรวดเร็ว ถูกต้อง และมีประสิทธิภาพ แต่ยังไม่มีการสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศขององค์กร การปฏิบัติเป็นเพียงการใช้งานทั่ว ๆ ไปเท่านั้น

ดังนั้นการพัฒนาให้องค์กรมีมาตรฐานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศตามแนวทางของมาตรฐานสากล ISO/IEC ให้ทัดเทียมกับองค์กรอื่นทั่วไปจึงเป็น 27001:2013 สิ่งจำเป็นที่ต้องเร่งดำเนินการซึ่งการพัฒนานี้ยังส่งผลในเรื่องความมั่นใจต่อการดำเนินธุรกิจให้มีความน่าเชื่อถือ และมีประสิทธิภาพมากยิ่งขึ้น องค์กรจะมีแนวทางการปฏิบัติงานจากการประกาศใช้ร่างแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้บุคลากรทุกระดับเกิดการตระหนักถึงผลกระทบที่จะเกิดขึ้นในอนาคตจากความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎี

การศึกษาและจัดทำสารนิพนธ์ฉบับนี้จำเป็นต้องใช้ทฤษฎีหลากหลายด้านเข้ามาเป็นส่วนช่วยให้สามารถดำเนินการได้ตรงตามวัตถุประสงค์ที่วางไว้ ในส่วนแรกคือ **มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013 (Information Security Management Systems : ISMS)** ซึ่งเป็นมาตรฐานสากลที่เกี่ยวกับการบริหารจัดการข้อมูลสารสนเทศให้มั่นคงปลอดภัย (Information Security Management System : ISMS) และยังมีแนวทางการบริหารความมั่นคงปลอดภัยสารสนเทศที่ขับเคลื่อนผ่านวงจร PDCA (Plan-Do-Check-Act) ซึ่งก็คือกระบวนการวางแผน (Plan) เป็นการกำหนดรายการควบคุม การประเมินความเสี่ยง และกำหนดนโยบายความมั่นคงปลอดภัย กระบวนการนำไปปฏิบัติ (Do) เป็นการลงมือปฏิบัติตามระบบบริหารจัดการความมั่นคงปลอดภัยที่ได้ประเมินไว้เพื่อลดปัญหาที่จะเกิดขึ้น กระบวนการการตรวจสอบ (Check) การประเมินผล ทำการทบทวนสิ่งที่ได้ดำเนินการบริหารจัดการความมั่นคงปลอดภัยไว้รวมถึงการ ทบทวนนโยบายด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้ว่าครบถ้วนครอบคลุมเป็นปัจจุบันหรือไม่ และกระบวนการแก้ไขปรับปรุง (Act) เป็นขั้นตอนของการบริหารความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน คือการนำผลที่ได้จากการตรวจสอบมาปรับปรุงให้ดีขึ้น[1]

[https://sites.google.com/site/yudeemi/3-neuxha]

รูปที่ 1 โครงสร้าง PDCA

การทำ PDCA นั้นเพื่อให้ระบบข้อมูลสารสนเทศขององค์กร มีคุณสมบัติ 3 ด้าน ดังนี้ 1.Confidentiality : ความลับ เป็นการปกป้องสารสนเทศให้เข้าถึงได้เฉพาะผู้มีสิทธิเท่านั้น 2.Integrity : ความถูกต้องสมบูรณ์ของสารสนเทศ โดยต้องไม่ได้ถูกเปลี่ยนแปลงหรือแก้ไขจากผู้ไม่ได้รับอนุญาต 3.Availability : ความพร้อมใช้ เพื่อให้มั่นใจว่าข้อมูลพร้อมที่จะใช้งานอยู่เสมอ

https://op.mahidol.ac.th/ia/wpcontent/uploads/2017/08/07KMISO27001.pdf

รูปที่ 2 หลักการ CIA

โดยมาตรฐาน ISO/IEC 27001:2013 ประกอบไปด้วยมาตรการการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ 14 หมวด ดังนี้ 1) นโยบายความมั่นคงปลอดภัยสารสนเทศ 2) โครงสร้างความมั่นคงปลอดภัยสารสนเทศ 3) ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล 4) การบริหารจัดการทรัพย์สิน 5) การควบคุมการเข้าถึง 6) การเข้ารหัสข้อมูล 7) ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม 8) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน 9) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล 10) การจัดหา พัฒนา และการบำรุงรักษาระบบ 11) ความสัมพันธ์กับผู้ให้บริการภายนอก 12) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ 13) ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ 14) ความสอดคล้อง[2] ทฤษฎีส่วนที่สองคือ

การประเมินความเสี่ยงและการบริหารจัดการความเสี่ยง

ความเสี่ยง (Risk) คือ โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล หรือเหตุการณ์ที่ไม่พึงประสงค์ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน ซึ่งอาจเกิดขึ้นในอนาคต และมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายขององค์กร

การประเมินความเสี่ยง (Risk Assessment)หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง จัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด และผลกระทบ โดยมีระดับของความเสี่ยง 5 ระดับ คือ สูงมาก สูง ปานกลาง น้อย และน้อยมาก

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลง อยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง [3] ทฤษฎีส่วนที่สาม คือ

คู่มือการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจะต้องประกอบไปด้วย 1.หลักการและเหตุผล 2.วัตถุประสงค์ 3.องค์ประกอบของนโยบาย 4.คำนิยาม โดยในองค์ประกอบแต่ละส่วน จะมีการกำหนดวัตถุประสงค์และแนวปฏิบัติของแต่ละส่วนไว้

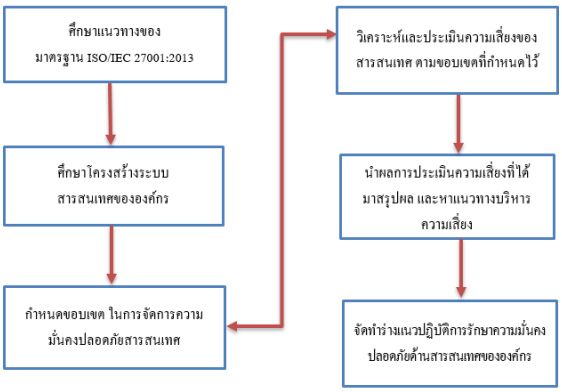
2.2. งานวิจัยที่เกี่ยวข้อง

รัชชาภรณ์ สุภาพ และศักดิ์ชาย ตั้งวรรณวิทย์ ได้ทำการวิจัยเรื่อง การจัดทำแนวทางการปฏิบัติ ในการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศด้วยมาตรฐาน ISO/IEC 27001 กรณีศึกษา : สำนักงานรัฐบาลอิเล็กทรอนิกส์ (มหาชน) (สรอ.) เพื่อกำหนดเป็นแนวทางและวิธิปฏิบัติที่มีมาตรฐานและมีประสิทธิภาพ เมื่อมีการนำแนวทางการทางการปฏิบัติที่จัดทำขึ้นไปปฏิบัติอย่างจริงจัง จะทำให้ องค์กรมีประสิทธิภาพด้านความมั่นคงปลอดภัยสารสนเทศ และเพื่อเป็นการสร้างความตระหนักให้แก่เจ้าหน้าที่ ซึ่งจะนำไปสู่ความมั่นคงปลอดภัยสารสนเทศขององค์กร[4]

วรัญญาภรณ์ สิริพิพัฒนพร และ สมชาย นำประเสริฐชัย ทำการในหัวข้อเรื่องการวิเคราะห์ และแนวทางจัดการความเสี่ยงด้านไอทีของหน่วยงานภาครัฐ โดยทำการศึกษาเชิงคุณภาพ และใช้บทสัมภาษณ์แบบ COBIT 3.0 เข้ามาช่วยในการประเมินหน่วยงานภาครัฐจำนวน 7 แห่ง ซึ่งผลการศึกษาพบว่าความเสี่ยงด้าน ICT ของหน่วยงานของรัฐมีสาเหตุหลักมาจากงบประมาณที่ไม่เพียงพอและการขาดแคลนบุคลากรด้าน ICT รวมไปถึงในส่วนของขั้นตอนการดำเนินการที่ไม่เอื้ออำนวยต่อการตอบสนองด้าน ICT [5]

วรวุฒิ เจ็งสืบสันต์ และ ดร.เทพฤทธิ์ บัณฑิตวัฒนาวงศ์ ทำการวิจัยเรื่องการพัฒนากรอบความมั่นคงปลอดภัยสำหรับศูนย์ข้อมูล กรณีศึกษา บริษัท เบทาโกร จำกัด (มหาชน) เป็นการนำเอามาตรฐาน ISO 27001:2005 มาศึกษาและพัฒนา เพื่อยกระดับความปลอดภัยของศูนย์ข้อมูลและองค์กร ทำให้องค์กรได้รับรู้ถึงความเสี่ยง ปัจจัยเสี่ยงและจุดอ่อนด้านต่าง ๆของศูนย์ข้อมูลที่มีอยู่ ซึ่งผลการศึกษาทำให้องค์กรสามารถหามาตรการป้องกันและลดความเสี่ยงได้อย่างมีประสิทธิภาพ โดยคณะทำงานขององค์กรมีแนวทางในการจัดการปัญหาของศูนย์ข้อมูลให้เกิดเป็นความมั่นคงปลอดภัยของระบบสารสนเทศ [6]

3. วิธีดำเนินการวิจัย



รูปที่ 3 การออกแบบการวิจัย

ในการดำเนินการวิจัย ผู้วิจัยได้กำหนดขั้นตอนการวิจัยดังนี้

1.) ศึกษาแนวทางของมาตรฐาน ISO/IEC 27001:2013เพื่อให้เกิดความรู้ความเข้าใจ และนำความรู้ที่ได้นั้นไปปรับใช้เป็นแนวทางในการดำเนินงาน

2.) ศึกษาโครงสร้างระบบเทคโนโลยีสารสนเทศขององค์กร เป็นการศึกษาข้อมูลด้วยวิธีการสัมภาษณ์ จากผู้ดำเนินงานในแต่ละส่วนงานภายในที่เกี่ยวข้อง

3.) กำหนดขอบเขตในการจัดการความมั่นคงปลอดภัยสารสนเทศ เน้นการทำงานอยู่ในขอบเขตที่เป็นภาพรวมขององค์กร ในส่วนของ ฮาร์ดแวร์ ซอร์ฟแวร์ ข้อมูล บุคลากร และการบริการ รวมถึงระบบสารสนเทศภายในองค์กรที่เกี่ยวข้อง เพื่อให้สามารถจัดการความสำคัญของขอบเขตและมีการจัดการอย่างเหมาะสม

4.) วิเคราะห์และประเมินความเสี่ยงของเทคโนโลยีสารสนเทศ ตามขอบเขตที่กำหนดไว้ โดยการนำแนวทางของข้อกำหนดตามมาตรฐาน ISO/IEC 27001:2013 ทั้ง 14 หมวด (A.5 – A.18) มาประยุกต์เป็นประเด็นความเสี่ยง และทำการประชุม สัมภาษณ์ ผู้บริหาร ตัวแทนบุคลากร และประเมินตามสถานการณ์ที่เป็นอยู่ในปัจจุบันเพื่อให้องค์กรทราบถึงปัญหาและระดับความเสี่ยงที่มีอยู่ เพื่อนำผลที่ได้ไปจัดทำแผนบริหารความเสี่ยงต่อไป

5.) นำผลการประเมินความเสี่ยงที่ได้มาสรุปผล และกำหนดแนวทางบริหารความเสี่ยง เป็นการพิจารณาตามแนวทางของหลักความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 เพื่อลดความเสี่ยงที่มีอยู่ให้น้อยลง อยู่ในสถานะที่องค์กรยอมรับได้

6.) จัดทำร่างนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ภายใต้แนวทางมาตรฐาน ISO/IEC 27001:2013 คือ การนำผลการประเมินความเสี่ยงที่ได้มาประมวลผล วิเคราะห์ และลงความเห็นร่วมกัน กับ ผู้บริหารและบุคลากร ซึ่งการจัดทำแนวทางปฏิบัตินี้ เพื่อให้องค์กรมีไว้ปฏิบัติในการป้องกัน ลดความเสี่ยง และลดความเสียหายที่อาจเกิดขึ้นในอนาคต

การประเมินโอกาส และ ผลกระทบของความเสี่ยง วิเคราะห์ระดับความเสี่ยง คือ เป็นการนำความเสี่ยงและปัจจัยเสี่ยงที่ระบุไว้ มาประเมินโอกาสที่จะเกิดความเสี่ยง และประเมินระดับความรุนแรงของผลกระทบตามเกณฑ์การประเมินความเสี่ยงขององค์กร เพื่อให้เห็นถึงระดับของความเสี่ยงที่แตกต่างกัน ซึ่งได้กำหนดเกณฑ์ระดับความเสี่ยงไว้ 4 ระดับ

ระดับความเสี่ยง (Risk Value)		โอกาสที่จะเกิดความเสี่ยง (Likelihood)				
		ต่ำมาก	ต่ำ	ปานกลาง	สูง	สูงมาก
ผลกระทบของความเสี่ยง (Impact)	ต่ำมาก	1	2	3	4	5
	ต่ำ	2	4	6	8	10
	ปานกลาง	3	6	9	12	15
	สูง	4	8	12	16	20
	สูงมาก	5	10	15	20	25

รูปที่ 4 ตารางประเมินความเสี่ยง

ระดับความเสี่ยงและแนวทางการดำเนินการ			
แถบสี	ระดับความเสี่ยง	การจัดระดับ	การดำเนินการ
เขียว	1 – 3	ต่ำ	ความเสี่ยงอยู่ในระดับต่ำ เป็นระดับที่สามารถยอมรับได้ โดยไม่ต้องมีการควบคุมหรือจัดการความเสี่ยงแต่อาจจะต้องติดตามและเฝ้าระวังความเสี่ยงเป็นระยะๆ
เหลือง	4 – 9	ปานกลาง	ความเสี่ยงอยู่ในระดับปานกลาง (Moderate) เป็นระดับที่พอยอมรับได้ แต่ต้องมีการติดตามเฝ้าระวังอย่างใกล้ชิด เพื่อควบคุมความเสี่ยงไม่ให้เคลื่อนย้ายไปสู่ระดับที่ไม่สามารถยอมรับได้
ส้ม	10 – 16	สูง	ความเสี่ยงอยู่ในระดับสูง (High) เป็นระดับที่ไม่สามารถยอมรับได้ ต้องจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
แดง	17 - 25	สูงมาก	ความเสี่ยงอยู่ในระดับสูงมาก (Extreme) เป็นระดับที่ไม่สามารถยอมรับได้ ต้องมีการจัดการความเสี่ยงโดยด่วนเร่งจัดการความเสี่ยงทันที เพื่อควบคุมความเสี่ยงให้กลับสู่ ระดับที่ยอมรับได้

รูปที่ 5 ตารางระดับความเสี่ยงและแนวทางการดำเนินการ

โดยการดำเนินการในขั้นตอนนี้ ได้มีการจัดทำเอกสาร ISMS จำนวน 3 รายการ ดังนี้

1.Information Security Context Requirements and Scope ข้อกำหนดและขอบเขตบริบทความปลอดภัยของข้อมูล เป็นเอกสารเกี่ยวกับข้อมูทั่วไปขององค์กร การดำเนินกิจกรรมการให้บริการ และปัญหาภายใน – ภายนอก

2.ISMS Roles Responsibilities and Authoritiesบทบาทและหน้าที่ของ ISMS เป็นเอกสารที่เกี่ยวกับ ISMS โครงสร้าง PDCA บทบาท หน้าที่ ของผู้ตรวจสอบภายใน

3.ISMS Manual คู่มือระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เป็นรายละเอียดของขอบเขตของระบบ นโยบาย โครงสร้างคณะทำงาน ความต้องการทั่วไปและข้อกำหนด 7 ข้อ ตามแนวทางของมาตรฐาน ISO/IEC 27001:2013

4. ผลการดำเนินการ

การดำเนินการในขั้นตอนนี้ แบ่งออกเป็น 3 ส่วนคือ

1. การประเมินความเสี่ยงก่อนการบริหารจัดการความเสี่ยง
2. การบริหารจัดการความเสี่ยง

3. การประเมินความเสี่ยงหลังการบริหารจัดการความเสี่ยง

การประเมินความเสี่ยงจากระเด็นความเสี่ยงที่ประยุกต์มาจากแนวทางตามมาตรฐาน ISO/IEC 27001:2013 โดยมีตัวอย่างการประเมินความเสี่ยงก่อนการบริหารจัดการควมเสี่ยง ดังรูปที่ 4

4.3.1 ผลการประเมินความเสี่ยงและการบริหารจัดการความเสี่ยง

ตารางที่ 4.1 การประเมินความเสี่ยงก่อนการบริหารจัดการความเสี่ยง

1.นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

1.1นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

วัตถุประสงค์ เพื่อให้มีการกำหนดทิศทางการบริหารจัดการและสนับสนุนด้านความมั่นคงปลอดภัยสารสนเทศโดยสอดคล้องกับความต้องการทางธุรกิจและกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

ข้อ	ประเด็นความเสี่ยง	ลักษณะความเสี่ยง	ผลกระทบ	โอกาส	ค่าความเสี่ยง	ระดับความเสี่ยง
1.1.1	นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศ	ไม่มีการจัดทำนโยบายความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศแบบบาลยักษ์ยักษ	4	4	16	สูง
1.2.1	การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	ไม่มีการทบทวนนโยบายด้านความมั่นคงปลอดภัย เนื่องจากยังไม่มีประกาศใช้นโยบายความมั่นคงปลอดภัยในองค์กร	4	4	16	สูง

รูปที่ 6 การประเมินความเสี่ยงก่อนการบริหารจัดการความเสี่ยง

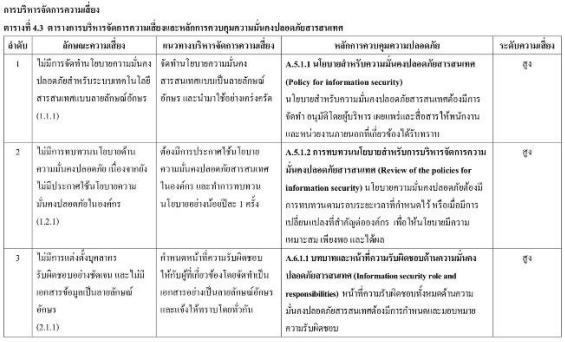
เมื่อทำการประเมินความเสี่ยงต่อข้อมูลและทรัพย์สินขององค์กร โดยการนำมาตรการทั้ง 14 หมวด รวม 114 ข้อ มาประยุกต์เป็นประเด็นความเสี่ยง เพื่อนำผลการประเมินความเสี่ยงที่เกินระดับที่องค์กรสามารถยอมรับได้ ไปดำเนินการควบคุมและแก้ไขความเสี่ยงนั้นในขั้นตอนต่อไป

สรุประดับความเสี่ยง				
	ต่ำ 1 – 3	ปานกลาง 4 - 9	สูง 10 – 16	สูงมาก 17 – 25
จำนวนหัวข้อประเด็นความเสี่ยง	4	24	72	14

รูปที่ 7 ผลการประเมินความเสี่ยงก่อนการบริหารจัดการความเสี่ยง

จากผลการประเมินความเสี่ยงก่อนหน้า พบว่ามีความเสี่ยงเกินกว่าระดับที่องค์กรจะยอมรับได้อยู่หลายข้อ ตามตารางผลการประเมินความเสี่ยงก่อนการบริหารจัดการความเสี่ยงที่ประเมินได้ ผลการประเมินแถบสีเขียวอยู่ในระดับต่ำ ระดับความเสี่ยง 1-3 มีผลการประเมิน 3 ข้อ แถบสีเหลือง ระดับปานกลาง ระดับความเสี่ยง 4-9 มีผลการประเมิน 24 ข้อ แถบสีส้ม ระดับสูง ระดับความเสี่ยง 10-16 มีผลการประเมิน 72 ข้อ แถบสีแดงระดับสูงมาก ระดับความเสี่ยง 17-25 มีผลการประเมิน 14 ข้อ ผู้ประเมินความเสี่ยงต้องนำเสนอแนวทางการจัดการความเสี่ยงต่อคณะกรรมการผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศก่อนดำเนินการ ซึ่งในมาตรฐาน ISO/IEC27001:2013 ไม่ได้มีการระบุถึงวิธีการที่จะต้องใช้ในการจัดการความเสี่ยงไว้ ซึ่งวิธีการของแต่ละองค์กรอสจมีความแตกต่างกันได้หลากหลายวิธี ขึ้นอยู่กับลักษณะใน

การดำเนินธุรกิจ และนโยบายของผู้บริหาร ซึ่งทางองค์กรตัวอย่างได้มีการจัดทำร่างนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศขึ้นมาเพื่อเป็นเครื่องมือในการบริหารจัดการความเสี่ยง



การบริหารจัดการความเสี่ยง

ตารางที่ 4.3 ตารางการบริหารจัดการความเสี่ยงและหลักการควบคุมความมั่นคงปลอดภัยสารสนเทศ

ลำดับ	อักษณะความเสี่ยง	แนวทางบริหารจัดการความเสี่ยง	หลักการควบคุมความปลอดภัย	ระดับความเสี่ยง
1	ไม่มีการจัดทำนโยบายความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศแบบลายลักษณ์อักษร (1.1.1)	จัดทำนโยบายความมั่นคงสารสนเทศแบบเป็นลายลักษณ์อักษร และนำมาใช้อย่างเคร่งครัด	**A.5.1.1 นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศ (Policy for information security)** นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศต้องมีการจัดทำ อนุมัติโดยผู้บริหาร เผยแพร่และสื่อสารให้พนักงานและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบ	สูง
2	ไม่มีการทบทวนนโยบายเดิมความมั่นคงปลอดภัย เนื่องจากยังไม่มีประกาศใช้นโยบายความมั่นคงปลอดภัยในองค์กร (1.2.1)	ต้องมีการประกาศใช้นโยบายความมั่นคงปลอดภัยสารสนเทศในองค์กร และทำการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง	**A.5.1.2 การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Review of the policies for information security)** นโยบายความมั่นคงปลอดภัยต้องมีการทบทวนตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร เพื่อให้นโยบายมีความเหมาะสม เพียงพอ และได้ผล	สูง
3	ไม่มีการแต่งตั้งบุคลากรรับผิดชอบอย่างชัดเจน และไม่มีเอกสารข้อมูลเป็นลายลักษณ์อักษร (2.1.1)	กำหนดหน้าที่ความรับผิดชอบให้กับผู้ที่เกี่ยวข้องโดยจัดทำเป็นเอกสารอ้างเป็นลายลักษณ์อักษร และแจ้งให้ทราบโดยทั่วกัน	**A.6.1.1 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security role and responsibilities)** หน้าที่ความรับผิดชอบทั้งหมดด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการกำหนดและมอบหมายความรับผิดชอบ	สูง

รูปที่ 8 การบริหารจัดการความเสี่ยง

วิธีการบริหารจัดการความเสี่ยงที่องค์กรเลือกใช้ คือ การจัดทำร่างนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งนโยบายที่จัดทำขึ้นมีทั้งหมด 14 ส่วน ดังนี้ 1.นโยบายการรักษาความมั่นคงปลอดภัย ทางด้านกายภาพและสิ่งแวดล้อม 2.นโยบายการรักษาความมั่นคงปลอดภัย ของการควบคุมการเข้าถึงระบบสารสนเทศ 3.นโยบายการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย- 4.นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ 5.นโยบายการควบคุมการเข้าถึงระบบเครือข่าย 6.นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ 7.นโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี 8.นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล 9.นโยบายการใช้งานเครื่องคอมพิวเตอร์พกพา 10.นโยบายการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต 11.นโยบายการป้องกันระบบเครือข่ายและตรวจจับการบุกรุก 12.นโยบายการสำรองและกู้คืนข้อมูล 13.นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์ 14.นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

จากนั้นจึงทำการประเมินความเสี่ยงอีกครั้ง เพื่อวัดผลการบริหารจัดการความเสี่ยง ซึ่งถ้าระดับความเสี่ยงลดลงอยู่ในระดับที่ยอมรับได้ จะถือว่าทรัพย์สินสารสนเทศที่เกี่ยวข้องมีความมั่นคงปลอดภัยเพียงพอ โดยการประเมินความเสี่ยงหลังการบริหารจัดการความเสี่ยงเป็นตามรูปที่ 9

ตารางที่ 4.4 การประเมินความเสี่ยงหลังการบริหารจัดการความเสี่ยง

1.นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

1.1นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

วัตถุประสงค์ เพื่อให้มีการกำหนดทิศทางการบริหารจัดการและสนับสนุนด้านความมั่นคงปลอดภัยสารสนเทศโดยสอดคล้องกับความต้องการทางธุรกิจและกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

ข้อ	ประเด็นความเสี่ยง	สถานะปัจจุบัน	ผลกระทบ	โอกาส	ค่าความเสี่ยง	ระดับความเสี่ยง
1.1.1	นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศ	มีการจัดทำนโยบายความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศแบบลายลักษณ์อักษร	3	1	3	ต่ำ
1.2.1	การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	มีการทบทวนนโยบายด้านความมั่นคงปลอดภัยตามวงรอบ	3	1	3	ต่ำ

2.โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

2.1 โครงสร้างภายในองค์กร (Internal organization)

วัตถุประสงค์ เพื่อให้มีกรอบกำหนดการบริหารจัดการโดยต้องมีการริเริ่มและควบคุมการปฏิบัติและการดำเนินการด้านความมั่นคง ปลอดภัยสารสนเทศภายในองค์กร

ข้อ	ประเด็นความเสี่ยง	สถานะปัจจุบัน	ผลกระทบ	โอกาส	ค่าความเสี่ยง	ระดับความเสี่ยง
2.1.1	บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ	มีการแต่งตั้งบุคลากรรับผิดชอบอย่างชัดเจนเป็นลายลักษณ์อักษร	3	1	3	ต่ำ

รูปที่ 9 การประเมินความเสี่ยงหลังการบริหารจัดการความเสี่ยง

สรุประดับความเสี่ยง				
	ต่ำ 1 – 3	ปานกลาง 4 - 9	สูง 10 – 16	สูงมาก 17 – 25
จำนวนหัวข้อประเด็นความเสี่ยง	102	12	0	0

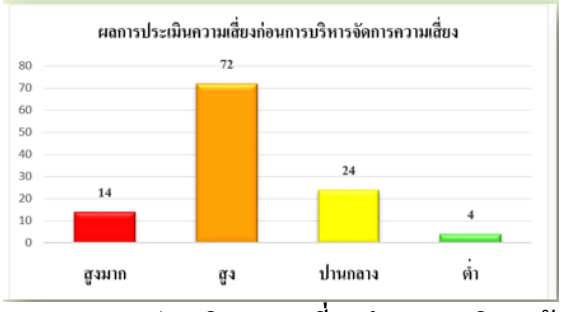
รูปที่ 10 ผลการประเมินความเสี่ยงหลังการบริหารจัดการความเสี่ยง

จากตารางผลการประเมินความเสี่ยงหลังการบริหารจัดการความเสี่ยง ที่ประเมินได้ผลการประเมินแถบสีเขียวอยู่ในระดับต่ำ ระดับความเสี่ยง 1-3 มีผลการประเมิน 102 ข้อ แถบสีเหลือง ระดับปานกลาง ระดับความเสี่ยง 4-9 มีผลการประเมิน 12 ข้อ แถบสีส้ม ระดับสูง ระดับความเสี่ยง 10-16 มีผลการประเมิน 0 ข้อ แถบสีแดงระดับสูงมาก ระดับความเสี่ยง 17-25 มีผลการประเมิน 0 ข้อ

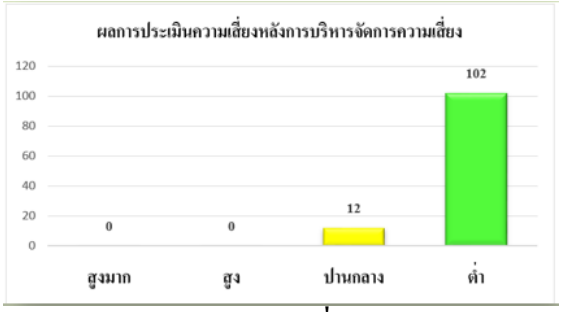
ในขั้นตอนนี้ มีการจัดทำเอกสาร ISMS หนึ่งรายการ คือ Statement of Applicability (SoA) เอกสารระบุการปฏิบัติตามหลักการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ เป็นเอกสารแสดงการประยุกต์ใช้มาตรการในมาตรฐาน ISO/IEC27001:2013 ที่องค์กรได้นำมาใช้งาน

5. สรุปผลการดำเนินการและข้อเสนอแนะ

5.1 สรุปผลการดำเนินการ



รูปที่ 11 กราฟแสดงผลการประเมินความเสี่ยงก่อนการบริหารจัดการความเสี่ยง



รูปที่ 12 กราฟแสดงผลการประเมินความเสี่ยงหลังการบริหารจัดการความเสี่ยง

จากการประเมินความเสี่ยงจำนวน 114 ข้อ ทั้งก่อนและหลังการบริหารจัดการความเสี่ยง จะเห็นว่า รายการความเสี่ยงนั้นลดลงซึ่งเกิดจาก การบริหารจัดการความเสี่ยงที่มีการพิจารณาแนวทางแก้ไข และจัดทำร่างนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร จึงสามารถลดความเสี่ยงลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งบรรลุตามวัตถุประสงค์ที่กำหนดไว้

สรุปผลภาพรวมของการดำเนินงาน โดยแบ่งตามขอบเขตในการดำเนินงานดังนี้

ฮาร์ดแวร์ 1.ผู้ที่จะเข้าในพื้นที่ห้อง Server นอกเหนือ จากผู้ดูแลระบบ ต้องได้รับอนุญาตจากผู้มีอำนาจสั่งการก่อน 2.ในการเข้าพื้นที่แต่ละครั้ง จะมีการลงชื่อ เพื่อควบคุมและเก็บบันทึกการเข้า-ออก ที่เป็นข้อมูลปัจจุบันโดยบันทึกนี้สามารถเรียกดูได้ตลอดเวลา 3.มีการกำหนดระยะเวลาการบำรุงรักษาอุปกรณ์ ทุก ๆ 3-6 เดือน 4.มีการรายงานการตรวจสอบทรัพยากรระบบไปยังผู้บริหารทุก ๆ 6 เดือน เพื่อจัดหาอุปกรณ์ที่มีประสิทธิภาพและเพียงพอต่อการใช้งาน 5.องค์กรมีแผนที่จะทำการจัดซื้อ เครื่อง Server ใหม่จำนวน 2 เครื่อง และ จัดซื้อ UPS เพิ่มเติมในไตรมาสที่ 4 ของปี 2563 เพื่อป้องกันไฟกระชากและเพื่อสำรองไฟฟ้าให้ใช้ได้นาน 30 นาที ในกรณีที่ไฟฟ้าดับเป็นเวลานาน และเพื่อช่วยยืดอายุการใช้งานของอุปกรณ์

ซอฟต์แวร์ 1.มีการกำหนดนโยบายความปลอดภัย ของระบบสารสนเทศภายในองค์กร 2.มีการอัพเดท patch ของระบบ ปฏิบัติการที่มีความสำคัญ 3.มีการทดสอบทุกครั้งที่มีการอัพเดท โดยการอัพเดทจะทำบนเครื่องทดสอบก่อนจะลงเครื่องที่ใช้งานอยู่จริง 4.มีการป้องกันเครื่อง โดยการตั้งการอัพเดท Antivirus อัตโนมัติ 5.มีการดำเนินการปิดพอร์ตที่ไม่จำเป็นและไม่ได้ใช้งานโดย Firewall

ข้อมูล 1.มีการจัดทำร่างนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ เผยแพร่ และจัดอบรมเพื่อให้บุคลากรมีความรู้ และตระหนักถึงความสำคัญของข้อมูลสารสนเทศ 2.มีมาตรการในการตั้งพาสเวิร์ด เพื่อให้เกิดความปลอดภัยมากยิ่งขึ้น 3.มีแนวทางการปฏิบัติให้บุคลากรทุกคนต้องเก็บพาสเวิร์ดเป็นความลับ 4.การจัดการเอกสารบนโต๊ะทำงานมีการดำเนินการให้ถูกเก็บอย่างปลอดภัย

บุคลากร มีแผนจัดการฝึกอบรม ในการส่งผู้ดูแลระบบ เข้ารับการฝึกอบรมในทักษะด้านการจัดการระบบและ การรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อพัฒนาความรู้ ทักษะทางด้านระบบสารสนเทศ รวมถึงการเพิ่มประสิทธิภาพในการทำงาน และเพื่อนำความรู้ที่ได้จากการอบรมมาเผยแพร่ให้กับบุคลากรใน องค์กรได้มีความรู้เช่นกัน

การบริการ 1.กรณีที่ผู้ให้บริการไม่สามารถให้บริการ Internet ได้ ทำให้องค์กรมีการหยุดชะงักของระบบ เกิดการปฏิบัติงานล่าช้า ได้มีการรายงานปัญหาให้กับผู้บริหารทราบถึงการดำเนินการก่อนจะทำการแก้ไขระบบทุกครั้ง 2.มีเอกสารให้ ผู้ให้บริการจากภายนอก ปฏิบัติตามข้อตกลงก่อนการเข้าให้บริการในพื้นที่ขององค์กร

5.2ปัญหาและข้อเสนอแนะ

ปัญหา

1. เนื่องจากมาตรฐาน ISO/IEC 27001:2013 มีหลายมาตรการควบคุม ซึ่งบางมาตรการยากต่อความเข้าใจ จึงต้องใช้เวลานานในการศึกษาทำความเข้าใจ

2. ก่อนการดำเนินงานผู้บริหาร และบุคลากรไม่มีความรู้เกี่ยวกับมาตรฐานนี้ จึงไม่ได้รับความร่วมมือเท่าที่ควร ซึ่งการจะนำแนวทางของมาตรฐาน ISO/IEC 27001:2013 เข้าไปปรับใช้งานให้เหมาะสมกับองค์กร ต้องได้ความร่วมมือจากบุคลากรทุกฝ่าย และผู้บริหารควรมีการสนับสนุนให้ปฏิบัติตามแนวทางมาตรฐาน ISO/IEC 27001:2013 อย่างจริงจังและต่อเนื่อง

ข้อเสนอแนะ

ระบบสารสนเทศได้มีการพัฒนาให้ก้าวหน้าอย่างรวดเร็วอยู่ตลอดเวลา ดังนั้นจึงควรมีการทบทวนนโยบายตามห้วงเวลาที่เหมาะสมอย่างสม่ำเสมอ ปรับปรุงนโยบายที่ใช้ เพื่อให้นโยบายมีความเหมาะสมกับสถานการณ์ปัจจุบัน ป้องกันการเกิดช่องโหว่ และเพื่อให้เกิดความปลอดภัยต่อสารสนเทศขององค์กรทั้งปัจจุบันและในอนาคต

6. เอกสารอ้างอิง

[1] ISO 27001 มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ [Online] ค้นหาเมื่อ ftp://hrm.moph.go.th/iso27001 /iso-27001.pdf, [สิงหาคม 2,2560]

[2] บริษัท ที-เน็ต จำกัด, “มาตรการการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ”,2557

[3] กลุ่มตรวจสอบภายในกระทรวง กระทรวงศึกษาธิการ, “การบริหารความเสี่ยงและ การควบคุมภายใน”,2558

[4] รัชชาภรณ์ สุภาพ และศักดิ์ชาย ตั้งวรรณวิทย์, “การจัดทำแนวทางการปฏิบัติ ในการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศด้วยมาตรฐาน ISO/IEC 27001 กรณีศึกษา : สำนักงานรัฐบาลอิเล็กทรอนิกส์ (มหาชน) (สรอ.)”,2557

[5] วรัญญาภรณ์ สิริพิพัฒนพร และ สมชาย นำประเสริฐชัย, “การวิเคราะห์และแนวทางจัดการความเสี่ยงด้านไอทีของหน่วยงานภาครัฐ”,2556
[6] วรวุฒิ เจ็งสืบสันต์ และ ดร.เทพฤทธิ์ บัณฑิตวัฒนาวงศ์, “การพัฒนากรอบความมั่นคงปลอดภัยสำหรับศูนย์ข้อมูล กรณีศึกษาบริษัท เบทาโกร จำกัด (มหาชน)”,2555