การวิเคราะห์ช่องว่างการดำเนินการด้านไอทีของบริษัทด้านการเงินที่ผ่านการรับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศตามกรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

The Gap Analysis of the IT Processes in Certified ISO/IEC 27001 Financial Organization with COBIT 5 Framework

ธัญญรัตน์ ปิยวัฒน์กานนท์[1*] และ ชุติมา เบี้ยวไข่มุข[2]

Thanyarat Piyawatkanoon[1*] and Chutima Beokhaimook[2]

นักศึกษาปริญญาโท หลักสูตรวิทยาศาสตร์มหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ
วิทยาลัยเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยรังสิต
อาจารย์ประจำ หลักสูตรวิทยาศาสตร์มหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ
วิทยาลัยเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยรังสิต
Graduate student of Master of Science (Information Technology Management),
College of Information and Communication Technology of Rangsit University
Lecturer in Master of Science (Information Technology Management),
College of Information and Communication Technology of Rangsit University
**Corresponding author, E mail: thania.pika@gmail.com*

บทคัดย่อ

งานวิจัยนี้การวิเคราะห์ช่องว่างการดำเนินการด้านไอทีของบริษัทด้านการเงินที่ผ่านการรับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศตามกรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร เมื่อพิจารณาตามกรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร (COBIT 5) ซึ่งประกอบด้วยโดเมน 5 กลุ่ม 37 กระบวนการ ผู้วิจัยได้จัดทำแบบสัมภาษณ์มีคำถามทั้งสิ้น 279 คำถาม นำมาสัมภาษณ์กลุ่มตัวอย่างแบบเจาะจง 2 ท่าน ผลคะแนนที่ได้ใช้เพื่อประเมินช่องว่างโดยใช้ค่าร้อยละ (Percentage) ผลการวิจัยพบว่าภาพรวมการดำเนินงานของบริษัทตาม COBIT 5 อยู่ในระดับปานกลาง พบว่ามีกระบวนการที่ทำคะแนนได้ร้อยละ 100 อยู่ 12 กระบวนการทั้งหมด ซึ่งเป็นกระบวนการที่มีความเกี่ยวข้องกับ ISO/IEC 27001 อีกทั้งพบกระบวนการที่ยังไม่ได้ดำเนินการอยู่ 9 กระบวนการ เช่น EDM02 ความมั่นใจในการส่งมอบผลประโยชน์ EDM05 ความมั่นใจในความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย APO03 บริหารจัดการสถาปัตยกรรมองค์กร ซึ่งบริษัทควรเริ่มดำเนินการตามกระบวนการดังกล่าว รวมทั้งควรมีการปรับปรุงกระบวนการที่มีการดำเนินการแล้วแต่ยังมีคะแนนไม่ถึงร้อยละ 100ให้มีคะแนนเพิ่มมากขึ้น อย่างไรก็ตามบริษัทควรดำเนินการวิเคราะห์ช่องว่างการดำเนินงานตามกรอบ COBIT 5 อย่างสม่ำเสมอเพื่อตรวจสอบระดับช่องว่างและคะแนนของบริษัท เพื่อวิเคราะห์ช่องว่างด้านการกำกับดูแลและการบริหารจัดการด้านเทคโนโลยีสารสนเทศของบริษัทด้านการเงิน ที่ได้รับการรับรอง

มาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001 เวอร์ชัน 2005) เมื่อพิจารณาตามกรอบแนวคิด COBIT 5 ทำให้ทราบถึงจุดบกพร่องของการกำกับดูและและการบริหารจัดการไอทีระดับองค์กร เพื่อใช้ข้อมูลดังกล่าวเป็นแนวทางในการกำหนดแผนปรับปรุงการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

คำสำคัญ: *กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร มาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ กรอบแนวคิด เทคโนโลยีสารสนเทศ มั่นคงปลอดภัยสารสนเทศ*

Abstract

This research performed gap analysis of the certified ISO/IEC 27001 organization by considering a business framework for the governance and the management of the enterprise IT (COBIT 5). COBIT 5 consists of 5 domains with 37 governance and management processes. The 279 questions were created and used to interview 2 IT specialists from the target company resulting in the process assessment scores. The company overall scores showed that the company was in moderate level when considering on COBIT 5 framework. There are 12 processes which are quite similar to those found in ISO/IEC 27001 which received full scores. There are 9 processes that have not been performed yet and the company should embark on them. Moreover, there are several processes that have been done partially and should be improved to get higher scores. However, the company should conduct a gap analysis considering the implementation of the COBIT 5 framework regularly.

Keywords: *COBIT 5, ISO 27001, framework, IT, Security*

1. บทนำ

COBIT คือ กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร จัดทำโดยสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ (ISACA) โดยกรอบแนวคิด COBIT 5 เป็นกรอบแนวคิดสำหรับการบริหารจัดการองค์กร เพื่อให้เกิดการกำกับดูแลด้านเทคโนโลยีสารสนเทศที่ดี บริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ บริหารจัดการด้านการใช้ทรัพยากรให้เกิดประโยชน์สูงสุด อันเป็นผลทำให้ดำเนินการตอบสนองต่อเป้าหมายขององค์กรได้อย่างดีเยี่ยม กรอบแนวคิด COBIT ได้ถูกประกาศใช้ในปี พ.ศ. 2555 โดยปัจจุบันคือเวอร์ชัน 5 (COBIT 5) ทั้งนี้กรอบแนวคิด COBIT 5 ประกอบด้วยโดเมน 5 กลุ่ม ซึ่งมีกระบวนการด้านการกำกับดูแลและการบริหารจัดการ 37 กระบวนการ (ISACA, 2555) กรอบแนวคิด COBIT 5 มีความสัมพันธ์กับมาตรฐานและกรอบการดำเนินงานอื่น ๆ เช่น ITIL ISO/IEC 20000 ISO/IEC 38500 ISO/IEC 27001 (ISACA, 2555) มาตรฐานสากล ISO/IEC 27001 เป็นมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) เพื่อมุ่งมั่นที่จะรักษาความลับ ความถูกต้อง และความพร้อมใช้ของสารสนเทศ ให้ตอบสนองต่อความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสียตามแนวทางการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ผ่านมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ 133 มาตรการควบคุม (ISO, 2005) ทั้งนี้ COBIT 5 มีกระบวนการด้านการกำกับดูและและการบริหารจัดการทั้งหมด 37 กระบวนการ ซึ่งเป็นกระบวนการที่สอดคล้องกับ

มาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ มาตรฐานสากล ISO/IEC 27001 เวอร์ชัน 2005 จำนวน 28 กระบวนการ การวิเคราะห์ช่องว่าง (Gap Analysis) คือ การตรวจประเมินเบื้องต้นเพื่อหาความแตกต่างของระบบที่เป็นอยู่ปัจจุบันขององค์กรกับข้อกำหนดของมาตรฐานที่ต้องการจัดทำ ซึ่งจะทำให้ทราบว่าองค์กรนั้นยังไม่ได้ดำเนินการในเรื่องใด หรือควรดำเนินการเรื่องใดเพิ่มเติมอีกเพื่อให้เป็นไปตามข้อกำหนดของมาตรฐาน (บริษัท ควอลิตี้ พาร์ทเนอร์ จำกัด, 2560) ในงานวิจัยฉบับนี้เป็นการวิเคราะห์ช่องว่างเป็นการประเมินคะแนนเป็นค่าร้อยละของกิจกรรมที่มีในกระบวนการทำงานของบริษัท เมื่อเทียบกับกระบวนการที่ควรมีทั้งหมดตามมาตรฐาน COBIT 5

ที่ผ่านมายังไม่มีงานวิจัยที่ดำเนินการวิจัยเกี่ยวกับการวิเคราะห์ช่องว่างการดำเนินงานด้านเทคโนโลยีสารสนเทศโดยพิจารณาตามกรอบแนวคิด COBIT 5 อีกทั้งกรอบแนวคิด COBIT 5 เป็นกรอบแนวคิดที่มีความสัมพันธ์กับมาตรฐานสากล ISO/IEC 27001 ผู้วิจัยจึงศึกษาช่องว่างการดำเนินงานด้านเทคโนโลยีสารสนเทศกับกรอบแนวคิด COBIT 5 เพื่อการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรของบริษัทที่เคยผ่านการรับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001)

2. วัตถุประสงค์

เพื่อวิเคราะห์ช่องว่างด้านการกำกับดูแลและการบริหารจัดการด้านเทคโนโลยีสารสนเทศของบริษัทที่ได้รับการรับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001) เมื่อพิจารณาตามกรอบแนวคิด COBIT 5 ทำให้ ทราบถึงจุดบกพร่องของการกำกับดูและและการบริหารจัดการไอทีระดับองค์กร ซึ่งใช้เป็นแนวทางในการกำหนดแผนปรับปรุงการกำกับดูและและการบริหารจัดการไอทีระดับองค์กรต่อไป

3. วิธีดำเนินการวิจัย

3.1 กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร (COBIT 5) และมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System)

3.1.1 COBIT คือ กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร ซึ่งจัดทำโดยสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ (ISACA) (ISACA, 2555) โดยกรอบแนวคิด COBIT 5 จะทำให้เกิดการกำกับดูแลด้านเทคโนโลยีสารสนเทศที่ดี บริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ บริหารจัดการด้านการใช้ทรัพยากรให้เกิดประโยชน์สูงสุด อันเป็นผลทำให้ดำเนินการตอบสนองต่อเป้าหมายขององค์กรได้อย่างดีเยี่ยม กรอบแนวคิด COBIT ได้ถูกประกาศใช้ในปี พ.ศ. 2555 ซึ่งเวอร์ชันปัจจุบันคือเวอร์ชัน 5 หรือ COBIT 5 กรอบแนวคิด COBIT 5 ประกอบด้วยโดเมน 5 โดเมน คือ 1) Evaluate, Direct and Monitor (EDM): ประเมิน สั่งการ และเฝ้าติดตาม 2) Align, Plan and Organize (APO): จัดวางแนว จัดทำแผน และจัดระบบ 3) Build, Acquire and Implement (BAI): จัดสร้าง จัดหา และนำไปใช้ 4) Deliver, Service and Support (DSS): ส่งมอบ ให้บริการ และสนับสนุน 5) Monitor, Evaluate and Access (MEA): เฝ้าติดตาม วัดผล และประเมิน ซึ่งทั้ง 5 โดเมนนี้มีกระบวนการด้านการกำกับดูแลและการบริหารจัดการเป็น 37 กระบวนการจำแนกตามแต่ละโดเมน ในปี 2012 สมาคม ISACA (ISACA, 2012) ได้นำเสนอความเชื่อมโยงของกรอบแนวคิด COBIT 5 มีความสัมพันธ์กับมาตรฐานและกรอบการดำเนินงานอื่น ๆ เช่น ITIL, ISO/IEC 20000, ISO/IEC 27001 ซึ่งมาตรฐาน ISO/IEC 27001 มีความสัมพันธ์กับกรอบ

แนวคิด COBIT 5 เป็นจำนวน 4 โดเมน คือ 1) APO: จัดวางแนว จัดทำแผน และจัดระบบ 2) BAI: จัดสร้าง จัดหา และนำไปใช้ 3) DSS: ส่งมอบ ให้บริการ และสนับสนุน 4) MEA: เฝ้าติดตาม วัดผล และประเมิน

3.1.2 ISO/IEC 27001 เป็นมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) (ISO, 2013) โดยมุ่งมั่นที่จะรักษาความลับ ความถูกต้อง และความพร้อมใช้ของสารสนเทศ ดำเนินการโดยการวางแผน ลงมือทำ ตรวจสอบวัดผลการดำเนินงาน และ ปรับปรุงอย่างต่อเนื่อง เพื่อตอบสนองความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย ตามแนวทางการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ด้วยมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ 133 มาตรการควบคุม ในปัจจุบันองค์กรทั่วโลกได้มีความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศมากยิ่งขึ้น จึงได้มีการดำเนินการขอใบรับรองมาตรฐานสากล ISO/IEC 27001 มากยิ่งขึ้น โดยจากปี พ.ศ. 2557 มีองค์กรทั่วโลกได้ผ่านการขอใบรับรอง ISO/IEC 27001 เป็นจำนวนทั้งสิ้น 23,005 องค์กร และต่อมาในปี พ.ศ. 2558 มีองค์กรได้ผ่านการขอใบรับรอง เป็นจำนวนทั้งสิ้น 27,536 องค์กร โดยมีอัตราการผ่านการรับรองเพิ่มขึ้นคิดเป็นร้อยละ 20 (ISO, 2017) ในงานวิจัยนี้จึงเน้นศึกษาองค์กรที่ผ่านการรับรองด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 เวอร์ชัน 2005 ว่าสามารถดำเนินการตามกรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรได้อย่างดีหรือไม่ เมื่อพิจารณาตามกรอบแนวคิด COBIT 5 โดยเลือกบริษัทที่ผ่านรับรับรองมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ISO/ IEC 27001 เวอร์ชัน 2005 จำนวน 1 บริษัท

3.1.3 ความสัมพันธ์ระหว่าง COBIT 5 และ ISO/IEC 27001 เวอร์ชัน 2005 (COBIT5,2012)

COBIT 5 มีกระบวนด้านการกำกับดูและและการบริหารจัดการทั้งหมด 37 กระบวนการ ซึ่งมี 28 กระบวนการที่สอดคล้องกับมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ มาตรฐานสากล ISO/IEC 27001 เวอร์ชัน 2005 ดังแสดงในตาราง

ตารางที่ 1 ตารางแสดงความสัมพันธ์ระหว่าง COBIT 5 และ ISO/IEC 27001 เวอร์ชัน 2005

5 โดเมน ของ COBIT 5	จำนวนกระบวนการ ทั้งหมดใน COBIT 5	จำนวนกระบวนการ ISO/IEC 27001 สอดคล้องกับ COBIT 5
Evaluate, Direct and Monitor (EDM)	5 กระบวนการ	4 กระบวนการ
Align, Plan and Organize (APO)	13 กระบวนการ	7 กระบวนการ
Build, Acquire and Implement (BAI)	10 กระบวนการ	8 กระบวนการ
Deliver, Service and Support (DSS)	6 กระบวนการ	6 กระบวนการ
Monitor, Evaluate and Access (MEA)	3 กระบวนการ	3 กระบวนการ

3.2 การวิเคราะห์ช่องว่างการดำเนินงานด้านเทคโนโลยีสารสนเทศ

เป็นการประเมินการดำเนินงานด้านไอทีของบริษัท ว่ามีระดับการดำเนินงานตามกระบวนการกำกับดูแลและการบริหารจัดการตาม 37 กระบวนการใน 5 โดเมนตามกรอบแนวคิด COBIT 5 ในระดับใด โดยพิจารณาการทำหรือไม่ทำกิจกรรมในแต่ละกระบวนการ ในงานวิจัยนี้ผู้วิจัยเลือกศึกษาบริษัทด้านการเงินหนึ่ง ที่ผ่านรับการรับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 เวอร์ชัน 2005 มาแล้ว การวิเคราะห์ช่องว่างจึง

เป็นวัดค่าร้อยละของกิจกรรมที่ทำในกระบวนการทำงานของบริษัทเมื่อเทียบกับกิจกรรมที่ควรมีทั้งหมดตามมาตรฐาน COBIT5 การวิเคราะห์ช่องว่างมีขั้นตอน 4 ขั้นตอนดังแสดงในรูปที่ 1

รูปที่ 1 กระบวนการในการดำเนินการวิเคราะห์ช่องว่าง

ขั้นตอนแรกคือศึกษากรอบแนวคิด COBIT 5 ผู้วิจัยได้ลงรายละเอียดของกระบวนการด้านการกำกับดูแลและการบริหารจัดการ 37 กระบวนการ ใน 5 โดเมน ซึ่งในแต่ละกระบวนการจะมีรายละเอียดของกิจกรรมอีก รวมกิจกรรมทั้งสิ้น 279 กิจกรรม ขั้นตอนต่อมาผู้วิจัยได้จัดทำแบบสัมภาษณ์ตามกรอบแนวคิด COBIT 5 โดยสร้างคำถาม 1 คำถามต่อ 1 กิจกรรม ทำให้แบบสัมภาษณ์มีข้อคำถามทั้งสิ้น 279 คำถาม รายละเอียดจำนวนคำถามแยกกระบวนการในแต่ละโดเมนมีรายละเอียดดังในตารางที่ 2 ถึงตารางที่ 6 ในขั้นตอนต่อมาแบบสัมภาษณ์นี้จะถูกนำไปใช้สัมภาษณ์เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศที่เกี่ยวข้องของบริษัทจำนวน 2 ท่าน ซึ่งเป็นผู้ที่มีหน้าที่ในการควบคุมดูแลการปฏิบัติงานของระบบเทคโนโลยีสารสนเทศของบริษัท อีกทั้งยังมีประสบการณ์ทำงานในบริษัทเกินกว่า 5 ปี ช่วยกันตอบคำถามทั้ง 279 ข้อ การถามจะมุ่งประเด็นว่าในองค์กรมีการกระทำกิจกรรมต่าง ๆ ทั้ง 279 กิจกรรมหรือไม่ หากใช่ จะได้คะแนน 1 คะแนนต่อ 1 กิจกรรม คะแนนที่ได้จากการสัมภาษณ์จะนำมาใช้วิเคราะห์ข้อมูลเป็นการประเมินร้อยละของกิจกรรมในแต่ละกระบวนการที่องค์กรมีการดำเนินการตามกรอบ COBIT 5 ดังแสดงในสมการ

$$\text{ร้อยละของกิจกรรมที่มีในกระบวนการ} = \frac{\text{จำนวนคะแนนที่ได้ในกระบวนการนั้น}}{\text{จำนวนกิจกรรมทั้งหมดในกระบวนการนั้น}} \times 100 \qquad (1)$$

ร้อยละของกิจกรรมในแต่ละกระบวนการที่องค์กรมีการดำเนินการตามกรอบ COBIT 5 เมื่อนำมาแปลผลจะได้เป็นระดับของกลุ่มคะแนน 3 ระดับ คือ ระดับต่ำ (ร้อยละ 0 – 49) ระดับปานกลาง (ร้อยละ 50 – 79) และระดับสูง (ร้อยละ 80 – 100)

4. ผลการวิจัย

การวิเคราะห์ช่องว่างการดำเนินงานด้านเทคโนโลยีสารสนเทศโดยพิจารณาตามกรอบแนวคิด COBIT 5 กับบริษัทที่ผ่านการรับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ มีผลการวิเคราะห์ข้อมูลแยกตามแต่ละโดเมนดังนี้

4.1 โดเมน Evaluate, Direct and Monitor (EDM): ประเมิน สั่งการ และเฝ้าติดตาม ซึ่งประกอบด้วย 5 กระบวนการที่มี 15 กิจกรรม จากการสัมภาษณ์กลุ่มตัวอย่างจำนวน 15 คำถามได้ผลคะแนนแยกเป็นรายละเอียดตามแต่ละกระบวนการดังแสดงในตารางที่ 1 พบว่าบริษัทมีการดำเนินงานตามกรอบแนวคิด COBIT 5 ในโดเมน EDM มีค่าเฉลี่ยรวมอยู่ที่ร้อยละ 53.33 ของการดำเนินกระบวนการทั้งหมดในโดเมนนั้น แปลว่าบริษัทมีการดำเนินการในโดเมนนี้อยู่ในระดับปานกลาง มี 2 กระบวนการที่บริษัทมีการดำเนินการได้เกินกว่าร้อยละ 80 คือ EDM01 ความมั่นใจในการกำหนดกรอบการดำเนินงานการกำกับดูแลและการบำรุงรักษา และ EDM03 ความมั่นใจในความเสี่ยงที่

เหมาะสม สำหรับกระบวนการที่ควรเร่งดำเนินการเนื่องจากยังไม่พบการดำเนินกระบวนการ 2 กระบวนการ คือ EDM02 ความมั่นใจในการส่งมอบ และ EDM05 ความมั่นใจในความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย

ตารางที่ 2 ตารางผลการประเมินโดเมน Evaluate, Direct and Monitor (EDM): ประเมิน สั่งการ และเฝ้าติดตาม

ลำดับที่		กระบวนการ	จำนวนข้อคำถาม	คะแนนที่ได้	ร้อยละ
1	EDM01*	ความมั่นใจในการกำหนดกรอบการดำเนินงานการกำกับดูแลและการบำรุงรักษา	3	3	100.00
2	EDM02	ความมั่นใจในการส่งมอบผลประโยชน์	3	0	0.00
3	EDM03*	ความมั่นใจในความเสี่ยงที่เหมาะสม	3	3	100.00
4	EDM04*	ความมั่นใจในการใช้ทรัพยากรให้ได้ประโยชน์สูงสุด	3	2	66.67
5	EDM05*	ความมั่นใจในความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย	3	0	0.00
		คะแนนเฉลี่ยรวม	**15**	**8**	**53.33**

หมายเหตุ: * คือกระบวนการที่สอดคล้องกับมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001 เวอร์ชัน 2005)

4.2 โดเมน Align, Plan and Organize (APO): จัดวางแนว จัดทำแผน และจัดระบบ ซึ่งประกอบด้วย 13 กระบวนการ ที่มี 97 กิจกรรม จากการสัมภาษณ์กลุ่มตัวอย่างจำนวน 97 คำถามได้ผลคะแนนแยกเป็นรายละเอียดตามแต่ละกระบวนการดังแสดงในตารางที่ 3พบว่าจากบริษัทมีการดำเนินงานตามกรอบแนวคิด COBIT 5 ในโดเมน APO มีค่าเฉลี่ยรวมอยู่ที่ร้อยละ 53.61 ของการดำเนินกระบวนการทั้งหมดในโดเมนนั้น แปลว่าบริษัทมีการดำเนินการในโดเมนนี้อยู่ในระดับปานกลาง โดยมี 4 กระบวนการที่องค์กรมีการดำเนินการได้เกินกว่าร้อยละ 80 คือ APO01 บริหารจัดการกรอบการดำเนินงานการบริหารงานด้านไอที APO09 บริหารจัดการข้อตกลงการ APO10 บริหารจัดการผู้ขายหรือผู้ให้บริการ และ APO13 บริหารจัดการความมั่นคงปลอดภัย สำหรับกระบวนการที่ควรเร่งดำเนินการเนื่องจากยังไม่พบการดำเนินกระบวนการ 3 กระบวนการ APO03 บริหารจัดการสถาปัตยกรรมองค์กร APO04 บริหารจัดการนวัตกรรม และ APO11 บริหารจัดการคุณภาพ

ตารางที่ 3 ตารางผลการประเมินโดเมน Align, Plan and Organize (APO): จัดวางแนว จัดทำแผน และจัดระบบ

ลำดับที่		กระบวนการ	จำนวนข้อคำถาม	คะแนนที่ได้	ร้อยละ
1	APO01*	บริหารจัดการกรอบการดำเนินงานการบริหารงานด้านไอที	9	8	88.89
2	APO02	บริหารจัดการกลยุทธ์	7	3	42.86
3	APO03	บริหารจัดการสถาปัตยกรรมองค์กร	5	0	0.00
4	APO04	บริหารจัดการนวัตกรรม	13	0	0.00
5	APO05	บริหารจัดการกลุ่มของชุดโครงการ	6	4	66.67
6	APO06	บริหารจัดการงบประมาณและต้นทุน	5	3	60.00
7	APO07*	บริหารจัดการทรัพยากรบุคคล	12	6	50.00
8	APO08*	บริหารจัดการความสัมพันธ์	8	2	25.00
9	APO09*	บริหารจัดการข้อตกลงการให้บริการ	8	8	100.00

ลำดับที่		กระบวนการ	จำนวนข้อคำถาม	คะแนนที่ได้	ร้อยละ
10	APO10*	บริหารจัดการผู้ขายหรือผู้ให้บริการ	6	5	83.33
11	APO11	บริหารจัดการคุณภาพ	7	0	0.00
12	APO12*	บริหารจัดการความเสี่ยง	8	4	50.00
13	APO13*	บริหารจัดการความมั่นคงปลอดภัย	3	3	100.00
		คะแนนเฉลี่ยรวม	**97**	**46**	**51.29**

หมายเหตุ: * คือกระบวนการที่สอดคล้องกับมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001 เวอร์ชัน 2005)

4.3 โดเมน Build, Acquire and Implement (BAI): จัดสร้าง จัดหา และนำไปใช้ ซึ่งประกอบด้วย 10 กระบวนการ ที่มี 96 กิจกรรม จากการสัมภาษณ์กลุ่มตัวอย่างจำนวน 96 คำถามได้ผลคะแนนแยกเป็นรายละเอียดตามแต่ละกระบวนการดังแสดงในตารางที่ 4 พบว่าจากองค์กรมีการดำเนินงานตามกรอบแนวคิด COBIT 5 ในโดเมน BAI มีค่าเฉลี่ยรวมอยู่ที่ร้อยละ 57.29 ของการดำเนินกระบวนการทั้งหมดในโดเมนนั้น แปลว่าองค์กรมีการดำเนินการในโดเมนนี้อยู่ในระดับปานกลาง โดยมี 6 กระบวนการที่องค์กรมีการดำเนินการได้เกินกว่าร้อยละ 80 คือ กระบวนการ คือ BIA01 บริหารจัดการโครงการและดูแลชุดโครงการ BIA02 บริหารจัดการข้อกำหนดความต้องการ BIA04 บริหารจัดการความพร้อมใช้งานและขีดความสามารถ BIA06 บริหารจัดการการเปลี่ยนแปลง BIA07 บริหารจัดการการยอมรับการเปลี่ยนแปลงและการปรับเปลี่ยน และ BIA09 บริหารจัดการสินทรัพย์ สำหรับกระบวนการที่ควรเร่งดำเนินการเนื่องจากยังไม่พบการดำเนินกระบวนการ 2 กระบวนการ คือ BIA03 บริหารจัดการระบุและจัดสร้างกระบวนการแก้ไขปัญหาแบบเบ็ดเสร็จ และ BIA05 บริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล

ตารางที่ 4 ตารางผลการประเมินโดเมน Build, Acquire and Implement (BAI): จัดสร้าง จัดหา และนำไปใช้

ลำดับที่		กระบวนการ	จำนวนข้อคำถาม	คะแนนที่ได้	ร้อยละ
1	BIA01*	บริหารจัดการโครงการและดูแลชุดโครงการ	23	23	100.00
2	BIA02*	บริหารจัดการข้อกำหนดความต้องการ	6	6	100.00
3	BIA03*	บริหารจัดการระบุและจัดสร้างกระบวนการแก้ไขปัญหาแบบเบ็ดเสร็จ	15	0	0.00
4	BIA04*	บริหารจัดการความพร้อมใช้งานและขีดความสามารถ	5	5	100.00
5	BIA05*	บริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล	8	0	0.00
6	BIA06*	บริหารจัดการการเปลี่ยนแปลง	4	4	100.00
7	BIA07*	บริหารจัดการการยอมรับการเปลี่ยนแปลงและการปรับเปลี่ยน	9	8	88.89
8	BIA08*	บริหารจัดการความรู้	6	3	50.00
9	BIA09*	บริหารจัดการสินทรัพย์	6	6	100.00
10	BIA10*	บริหารจัดการองค์ประกอบของระบบ	14	14	100
		คะแนนเฉลี่ยรวม	**96**	**69**	**73.89**

หมายเหตุ: * คือกระบวนการที่สอดคล้องกับมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001 เวอร์ชัน 2005)

4.4 โดเมน Deliver, Service and Support (DSS): ส่งมอบ ให้บริการ และสนับสนุน ซึ่งประกอบด้วย 6 กระบวนการ ที่มี 51 กิจกรรม จากการสัมภาษณ์กลุ่มตัวอย่างจำนวน 51 คำถามได้ผลคะแนนแยกเป็นรายละเอียดตามแต่ละกระบวนการดังแสดงในตารางที่ 5 พบว่าจากองค์กรมีการดำเนินงานตามกรอบแนวคิด COBIT 5 ในโดเมน DSS มีค่าเฉลี่ยรวมอยู่ที่ร้อยละ 72.55 ของการดำเนินกระบวนการทั้งหมดในโดเมนนั้น แปลว่าองค์กรมีการดำเนินการในโดเมนนี้อยู่ในระดับปานกลาง โดยมี 4 กระบวนการที่องค์กรมีการดำเนินการได้เกินกว่าร้อยละ 80 คือ DSS01 บริหารจัดการการปฏิบัติการ DSS02 บริหารจัดการคำร้องขอบริหารและเหตุการณ์ที่เกิดขึ้น DSS04 บริหารจัดการความต่อเนื่อง และ DSS05 บริหารจัดการด้านความมั่นคงปลอดภัย สำหรับกระบวนการที่ควรเร่งดำเนินการเนื่องจากยังไม่พบการดำเนินกระบวนการ 2 กระบวนการ DSS03 บริหารจัดการปัญหา และ DSS06 บริหารจัดการควบคุมกระบวนการทางธุรกิจ

ตารางที่ 5 ตารางผลการประเมินโดเมน Deliver, Service and Support (DSS): ส่งมอบ ให้บริการ และสนับสนุน

ลำดับที่		กระบวนการ	จำนวนข้อคำถาม	คะแนนที่ได้	ร้อยละ
1	DSS01 *	บริหารจัดการการปฏิบัติการ	14	13	92.86
2	DSS02 *	บริหารจัดการคำร้องขอบริหารและเหตุการณ์ที่เกิดขึ้น	7	7	100.00
3	DSS03 *	บริหารจัดการปัญหา	6	0	0.00
4	DSS04 *	บริหารจัดการความต่อเนื่อง	8	8	100.00
5	DSS05 *	บริหารจัดการด้านความมั่นคงปลอดภัย	10	9	90.00
6	DSS06 *	บริหารจัดการควบคุมกระบวนการทางธุรกิจ	6	0	0.00
		คะแนนเฉลี่ยรวม	**51**	**37**	**72.55**

หมายเหตุ: * คือกระบวนการที่สอดคล้องกับมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001 เวอร์ชัน 2005)

4.5 โดเมน Monitor, Evaluate and Access (MEA): เฝ้าติดตาม วัดผล และประเมิน ซึ่งประกอบด้วย 3 กระบวนการที่มี 20 กิจกรรม จากการสัมภาษณ์กลุ่มตัวอย่างจำนวน 20 คำถามได้ผลคะแนนแยกเป็นรายละเอียดตามแต่ละกระบวนการดังแสดงในตารางที่ 6 พบว่าจากองค์กรมีการดำเนินงานตามกรอบแนวคิด COBIT 5 ในโดเมน MEA มีค่าเฉลี่ยรวมอยู่ที่ร้อยละ 100 ของการดำเนินกระบวนการทั้งหมดในโดเมนนั้น แปลว่าองค์กรมีการดำเนินการในโดเมนนี้อยู่ในระดับดีมาก

ตารางที่ 6 ตารางผลการประเมินโดเมน Monitor, Evaluate and Access (MEA): เฝ้าติดตาม วัดผล และประเมิน

ลำดับที่		โดเมน	จำนวนข้อคำถาม	คะแนนที่ได้	ร้อยละ
1	MEA01*	เฝ้าติดตาม วัดผลและประเมินประสิทธิภาพและความสอดคล้องในการดำเนินงาน	5	5	100.00
2	MEA02*	เฝ้าติดตาม วัดผลและประเมินระบบการควบคุมภายใน	11	11	100.00
3	MEA03*	เฝ้าติดตาม วัดผลและประเมินการปฏิบัติตามข้อกำหนดจากหน่วยงานภายนอก	4	4	100.00
		คะแนนเฉลี่ยรวม	**20**	**20**	**100**

หมายเหตุ: * คือกระบวนการที่สอดคล้องกับมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001 เวอร์ชัน 2005)

4.6 สรุปผลการประเมินการดำเนินงานตามกรอบแนวคิด COBIT 5 ทั้ง 5 โดเมนมีค่าเฉลี่ยรวมอยู่ที่ร้อยละ 61.65 โดเมนที่มีการดำเนินการงานตามกรอบแนวคิด COBIT 5 มากที่สุดคือ MEA และโดเมนที่มีการดำเนินงานตามกรอบแนวคิด COBIT 5 น้อยที่สุดคือ EDM ดังแสดงในตารางที่ 7

ตารางที่ 7 ตารางสรุปการประเมินการดำเนินงานทุกโดเมนตามกรอบแนวคิด COBIT 5

ลำดับที่	โดเมน	จำนวนข้อคำถาม	คะแนนที่ได้	ร้อยละ
1	Evaluate, Direct and Monitor (EDM): ประเมิน สั่งการ และเฝ้าติดตาม	15	8	53.33
2	Align, Plan and Organize (APO): จัดวางแนว วัดทำแผน และจัดระบบ	97	46	51.29
3	Build, Acquire and Implement (BAI): จัดสร้าง จัดหา และนำไปใช้	96	69	73.88
4	Deliver, Service and Support (DSS): ส่งมอบ ให้บริการ และสนับสนุน	51	37	72.55
5	Monitor, Evaluate and Access (MEA): เฝ้าติดตาม วัดผล และประเมิน	20	20	100.00
	คะแนนเฉลี่ยรวม	**279**	**180**	**70.21**

5. การอภิปรายผล

การวิเคราะห์ช่องว่างการดำเนินงานด้านเทคโนโลยีสารสนเทศโดยพิจารณาตามกรอบแนวคิด COBIT 5 กับบริษัทที่ได้รับการรับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศพบว่า แม้ว่าบริษัทจะผ่านการรับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 แล้วก็ตาม แต่เมื่อถูกประเมินภาพรวมการดำเนินงานตามกรอบแนวคิด COBIT 5 พบการดำเนินงานด้านเทคโนโลยีสารสนเทศของบริษัทนี้ อยู่ในระดับปานกลาง คิดเป็นร้อยละ 70.21 ของกระบวนการทั้งหมด 37 กระบวนการ มีกระบวนการ 14 กระบวนการที่บริษัทมีการดำเนินงานร้อยละ 100 ซึ่งกระบวนการดังกล่าวส่วนใหญ่ครอบคลุมและเกี่ยวข้องกับมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001) อย่างไรก็ดีผลจากการวิเคราะห์ช่องว่างพบว่าบริษัทยังไม่ได้ดำเนินงานตามกระบวนการในกรอบแนวคิด COBIT 5 และควรเร่งดำเนินการจำนวน 9 กระบวนการ สองสาเหตุที่กระบวนการเหล่านี้ยังไม่ได้ดำเนินการคือ 1) กระบวนการดังกล่าวเป็นกระบวนการที่ไม่ได้เกี่ยวข้องกับ ISO/IEC 27001 เวอร์ชัน 2005 ได้แก่ EDM02 ความมั่นใจในการส่งมอบผลประโยชน์ APO03 บริหารจัดการสถาปัตยกรรมองค์กร APO04 บริหารจัดการนวัตกรรม และ APO11 บริหารจัดการคุณภาพ และสาเหตุที่ 2) เป็นกระบวนการที่ไม่ได้ดำเนินการเป็นประจำ

หรือดำเนินการนานๆ ครั้ง ทำให้บริษัทไม่ได้ตระหนัก หรือละเลยการดำเนินการกิจกรรมดังกล่าว ได้แก่ EDM05 ความมั่นใจในความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย BIA03 บริหารจัดการระบุและจัดสร้างกระบวนการแก้ไขปัญหาแบบเบ็ดเสร็จ BIA05 บริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล DSS03 บริหารจัดการปัญหา และ DSS06 บริหารจัดการควบคุมกระบวนการทางธุรกิจ นอกจากนี้ยังมีกระบวนการที่บริษัทมีการดำเนินการไปบ้างแล้วแต่ยังได้คะแนนไม่ถึงร้อยละ 100 มีจำนวน 14 กระบวนการ ซึ่งควรมีปรับปรุงให้มีการทำกิจกรรมในกระบวนการดังกล่าวเพื่อปรับให้คะแนนของกระบวนการนั้นมีคะแนนเพิ่มขึ้น

๖. บทสรุป

งานวิจัยนี้เป็นการศึกษาการวิเคราะห์ช่องว่างการดำเนินงานด้านเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT 5 ของบริษัทที่ได้รับการรับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001) เพื่อประเมินระดับการดำเนินงานในกระบวนการด้านการกำกับดูแลและการบริหารจัดการ โดยสร้างแบบสัมภาษณ์บริษัทดังกล่าวตามกรอบแนวคิดแนวคิด COBIT 5 เป็นคำถามทั้งสิ้น 279 คำถาม ผลการวิเคราะห์คะแนนสัมภาษณ์พบว่าบริษัทมีการดำเนินงานตามกรอบแนวคิด COBIT 5 อยู่ในระดับปานกลาง คิดเป็นร้อยละ 61.65 ของกระบวนการทั้งหมด 37 กระบวนการ โดยมีกระบวนการที่ทำได้ร้อยละ100 จำนวน 12 กระบวนการซึ่งกระบวนการดังกล่าวส่วนใหญ่เป็นกระบวนการที่มีความเกี่ยวข้องตรงกันกับมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001) ทั้งนี้พบกระบวนการตามกรอบแนวคิด COBIT 5 ที่ยังไม่ได้ดำเนินการจำนวน 9 กระบวนการ โดย 5 กระบวนการแรกที่ควรเร่งดำเนินการก่อน เนื่องจากเป็นกระบวนการที่เคยดำเนินการมาก่อนแล้วขณะที่ได้รับการขอใบรับรองมาตรฐานสากล ISO/IEC 27001 ได้แก่ 1) EDM05 ความมั่นใจในความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย 2) BIA03 บริหารจัดการระบุและจัดสร้างกระบวนการแก้ไขปัญหาแบบเบ็ดเสร็จ 3) BIA05 บริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล 4) DSS03 บริหารจัดการปัญหา 5) DSS06 บริหารจัดการควบคุมกระบวนการทางธุรกิจ แล้วจึงดำเนินการอีก 4 กระบวนการให้เป็นผลสำเร็จ คือ 6) EDM02 ความมั่นใจในการส่งมอบผลประโยชน์ 7) APO03 บริหารจัดการสถาปัตยกรรมองค์กร 8) บริหารจัดการนวัตกรรม 9) APO11 บริหารจัดการคุณภาพ สำหรับกระบวนการที่มีการดำเนินการ แต่ยังมีคะแนนไม่ถึงร้อยละ 100 บริษัทควรพัฒนาปรับปรุงให้มีคะแนนเพิ่มมากขึ้น อย่างไรก็ตามบริษัทควรดำเนินการวิเคราะห์ช่องว่างระหว่างบริษัทกับกรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรอย่างสม่ำเสมอเพื่อตรวจสอบระดับช่องว่างและคะแนนของบริษัท

๗. กิตติกรรมประกาศ

คณะผู้วิจัยขอขอบพระคุณ พนักงานสายงานเทคโนโลยีสารสนเทศ บริษัทด้านการเงิน เป็นอย่างสูง ที่ให้ความร่วมมือ ให้ข้อมูลและคำปรึกษาที่ดีสำหรับการศึกษาวิจัยในครั้งนี้

8. เอกสารอ้างอิง

บริษัท ควอลิตี้ พาร์ทเนอร์ จำกัด. (2560). Gap Analysis & Pre Audit, 1 มกราคม 2560. http://www.qualitypartner.org/service/gap-analysis-pre-audit/.

ISACA. (2555). *กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร*, กรุงเทพฯ. ISACA.

ISACA. (2012). *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT*. Illinois USA. ISACA.

ISACA. (2012). *COBIT 5 for Information Security*. Illinois USA. ISACA.

ISO. (2005). *ISO/IEC 27001 second edition Information Technology – Security techniques – Information security management systems – Requirement*. Switzerland.ISO.

ISO. (2016) . The ISO Survey of Management System Standard Certifications 2015 [Online]. Available : http://www.iso.org/iso/the_iso_survey_of_management_system_standard_certifications_2015.pdf. (Access date: 1 January 2017).