ระบบประเมินตนเองด้านเทคโนโลยีสารสนเทศ ของบริษัทจดทะเบียน ในกลุ่มทรัพยากรตามกรอบโคบิต เพื่อเตรียมความพร้อม ในการเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย

นายสุรชาติ จันทสุวรรณ

วิทยานิพนธ์นี้เป็นส่วนของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
พ.ศ. 2558

Self-Assessment in IT Domain of Listed Companies in the Resources Sector Based on COBIT Framework for Entry Preparation to MAI of the Stock Exchange of Thailand

Mr. Surachat Chantasuwan

A Thesis Submitted in Partial Fulfillment of the Requirements for
the Degree of Master of Science in Information and Communication Technology
School of Science and Technology
Sukhothai Thammathirat Open University
2015

หัวข้อวิทยานิพนธ์ ระบบประเมินตนเองด้านเทคโนโลยีสารสนเทศ ของบริษัทจดทะเบียนในกลุ่มทรัพยากรตามกรอบโคบิต เพื่อเตรียมความพร้อมในการเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย

ชื่อและนามสกุล นายสุรชาติ จันทสุวรรณ

แขนงวิชา เทคโนโลยีสารสนเทศและการสื่อสาร

สาขาวิชา วิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช

อาจารย์ที่ปรึกษา 1. รองศาสตราจารย์ ดร. วิภา เจริญภัณฑารักษ์

2. ผู้ช่วยศาสตราจารย์ ดร. สันติพัฒน์ อรุณธารี

วิทยานิพนธ์นี้ ได้รับความเห็นชอบให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรระดับปริญญาโท เมื่อวันที่ 15 สิงหาคม 2559

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ

(อาจารย์ ดร. ดวงดาว วิชาดากุล)

.....กรรมการ

(รองศาสตราจารย์ ดร. วิภา เจริญภัณฑารักษ์)

.....กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร. สันติพัฒน์ อรุณธารี)

.....ประธานกรรมการบัณฑิตศึกษา

(รองศาสตราจารย์ ดร. สุจินต์ วิศวธีรานนท์)

ชื่อวิทยานิพนธ์ ระบบประเมินตนเองด้านเทคโนโลยีสารสนเทศ ของบริษัทจดทะเบียนในกลุ่มทรัพยากรตามกรอบโคบิต เพื่อเตรียมความพร้อมในการเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย
ผู้วิจัย นายสุรชาติ จันทสุวรรณ **รหัสนักศึกษา** 2549600530 **ปริญญา** วิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศและการสื่อสาร)
อาจารย์ที่ปรึกษา (1) รองศาสตราจารย์ ดร. วิภา เจริญภัณฑารักษ์ (2) ผู้ช่วยศาสตราจารย์ ดร. สันติพัฒน์ อรุณธารี
ปีการศึกษา 2558

บทคัดย่อ

การวิจัยระบบประเมินตนเองด้านเทคโนโลยีสารสนเทศโดยใช้หลักธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ มีวัตถุประสงค์เพื่อ (1) วิเคราะห์และสังเคราะห์องค์ความรู้ของกระบวนการควบคุมภายในด้านเทคโนโลยีสารสนเทศตามมาตรฐานโคบิต 5.0 ที่เหมาะสมสำหรับธุรกิจทรัพยากร เพื่อเตรียมความพร้อมเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย กลุ่มธุรกิจทรัพยากร (2) พัฒนาต้นแบบระบบประเมินตนเองโดยใช้องค์ความรู้ของกระบวนการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ที่สังเคราะห์ขึ้นตามมาตรฐานโคบิต 5.0 ที่เหมาะสมสำหรับธุรกิจทรัพยากร (3) ประเมินความน่าเชื่อถือจากองค์ความรู้ของกระบวนการควบคุมภายในด้านเทคโนโลยีสารสนเทศจากต้นแบบที่สังเคราะห์ขึ้น

การดำเนินการวิจัยมีขั้นตอนประกอบด้วย (1) ศึกษาธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ เกี่ยวกับมาตรฐานโคบิต 5.0 (2) วิเคราะห์กระบวนการการควบคุมภายในด้านเทคโนโลยีสารสนเทศของธุรกิจกลุ่มทรัพยากรจาก 3แหล่งข้อมูลคือ 1) จากกรอบโคบิต 5.0 2) จากประสบการณ์ของผู้วิจัยในด้านเทคโนฯ 3) จากผู้ตรวจสอบบัญชี ในองค์กรที่ได้รับความเห็นชอบ จากสำนักงาน ก.ล.ต.จำนวน 3 องค์กรองค์กรละ 1 ท่าน เพื่อกำหนดกรอบโคบิตที่เกี่ยวข้องและจำเป็นสำหรับกระบวนการการควบคุมภายในงานเทคโนโลยีสารสนเทศของธุรกิจกลุ่มทรัพยากร โดยโคบิตมีโดเมนทั้งหมด 5 โดเมน แต่ผลการวิเคราะห์พบว่ามีเพียง 2 โดเมนที่เกี่ยวข้องและจำเป็น คือ APO,BAI (3) สังเคราะห์องค์ความรู้ตามกรอบโคบิตที่วิเคราะห์ไว้จากโดเมน APOและBAI พบว่ามีกระบวนการและกระบวนการย่อยใน APO ที่จำเป็นคือ APO01 (การบริหารจัดการกรอบการดำเนินงานการบริหารงานด้านไอที) APO07 (การบริหารจัดการทรัพยากรบุคคล) APO10 (บริหารจัดการผู้ขายหรือผู้ให้บริการ) APO12 (การบริหารจัดการความเสี่ยง) APO13 (การบริหารจัดการความมั่นคงปลอดภัย) ส่วน BAI มีกระบวนการและกระบวนการย่อยที่จำเป็นคือ BAI06 (การบริหารจัดการการเปลี่ยนแปลง) และ BAI09 (การบริหารจัดการสินทรัพย์) ซึ่งทั้ง APOและ BAI มีเอกสารที่เกี่ยวข้องในกระบวนการควบคุมภายในงานด้านเทคโนโลยีสารสนเทศที่สำคัญคือ คู่มือปฏิบัติงาน งานประจำ และ เอกสารไอที (4) พัฒนาต้นแบบระบบประเมินตนเองฯ ที่ใช้องค์ความรู้เกี่ยวกับกระบวนการควบคุมภายในฯ ที่วิเคราะห์และสังเคราะห์ขึ้น เครื่องมือที่ใช้ในการพัฒนาต้นแบบ ประกอบด้วย Start UML Version 5.0.2.1570 เพื่อใช้ในการวิเคราะห์ระบบฯ Microsoft Visual Studio Community 2015 เพื่อใช้พัฒนาโปรแกรมต้นแบบ และ SQL Server 2005 เพื่อใช้ในการจัดการฐานข้อมูล (5) ประเมินองค์ความรู้ในต้นแบบฯ ที่ได้พัฒนาขึ้นโดยกลุ่มอุตสาหกรรมทรัพยากร แบ่งเป็น 2 กลุ่มตัวอย่างคือ 1) องค์กรที่ต้องการเตรียมความพร้อมเข้าตลาดฯจำนวน 1 องค์กร 2) องค์กรที่อยู่ในตลาดฯจำนวน 1 องค์กร โดยทดลองใช้งาน ระหว่าง วันที่ 21 มิถุนายน-29 กรกฎาคม 2559 เครื่องมือประเมินผล คือ แบบสอบถามการควบคุมภายในด้านไอทีนำมาจากโดเมน APOและ BAI

ผลการวิจัยพบว่า (1) องค์ความรู้ที่ได้สังเคราะห์จากมาตรฐานโคบิต 5.0 ซึ่งมีทั้งหมด 5 โดเมน พบว่ามีเพียง 2 โดเมนที่เกี่ยวข้องและจำเป็นสำหรับกลุ่มธุรกิจทรัพยากร คือ APO และ BAI เท่านั้น (2) กระบวนการภายใน APO ที่เกี่ยวข้องคือ APO01 (การบริหารจัดการกรอบการดำเนินงานการบริหารงานด้านไอที) APO07 (การบริหารจัดการทรัพยากรบุคคล) APO10 (บริหารจัดการผู้ขายหรือผู้ให้บริการ) APO12 (การบริหารจัดการความเสี่ยง) APO13 (การบริหารจัดการความมั่นคงปลอดภัย) (3) มีกระบวนการภายใน BAI ที่เกี่ยวข้องคือ BAI06 (การบริหารจัดการการเปลี่ยนแปลง) และ BAI09 (การบริหารจัดการสินทรัพย์) (4) ผลการประเมินจากกลุ่มตัวอย่างทั้ง 2 กลุ่ม พบว่า 1) ทั้งองค์กรที่อยู่ในตลาดฯ และอยู่นอกตลาดฯมีกระบวนการควบคุมงานด้านไอทีภายใต้โดเมน APO และ BAI ซึ่งสอดคล้องตามองค์ความรู้ที่งานวิจัยสังเคราะห์ขึ้น แต่ขาดกระบวนการย่อยที่จำเป็นตามองค์ความรู้ที่ได้สังเคราะห์ขึ้นในงานวิจัยนี้ 2) องค์กรที่อยู่ในตลาดฯมีกระบวนการควบคุมงานไอที ใกล้เคียงและสอดคล้องกับองค์ความรู้จากงานวิจัยนี้มากกว่าองค์กรที่นอกตลาดฯ

คำสำคัญ ระบบประเมินตนเองด้านเทคโนโลยีสารสนเทศ

Thesis title: Self-Assessment in IT Domain of Listed Companies in the Resources Sector Based on COBIT Framework for Entry Preparation to MAI of the Stock Exchange of Thailand
Researcher: Mr. Surachat Chantasuwan; **ID:** 2549600530**;**
Degree: Master of Science (Information and Communication Technology);
Thesis advisors: (1) Dr. Vipa Jaroenpuntaruk, Associate Professor ;
(2) Dr. Santipat Arunthari, Assistant Professor; **Academic year:** 2015

Abstract

The research of self-assessment system based on IT governance aimed to (1) analysis and synthesis knowledge assess their own IT departments based on the principles of Public Governance COBIT 5.0 suitable for resources industry to enter MAI (Market for Alternative Investment) Stock Exchange of Thailand (2) develop self-assessment of IT internal process control synthesized from COBIT 5.0 for resources industry (3) evaluate the reliability of the synthesized knowledge of IT internal process control.

The research methodology was as follows; (1) Studied IT governance COBIT 5.0. (2) Analyzed IT internal process control for the resources industry based on 3 data sources: 1) COBIT 5.0; 2) IT Experiences of the researcher; 3) Three accounting auditors approved by the SEC(Securities and Exchange Commission) from three organizations to set and verify a framework of IT internal process control. Since COBIT has 6 domains, but the results showed that only two domains that were relevant and necessary referred to APO,BAI (3) Synthesized knowledge from COBIT. There were mandatory processes and sub-processes in APO such as APO01(Manage the IT management framework), APO07(Manage Human Resources), APO10 (Manage Suppliers), APO12(Manage Risk), APO13(Manage Security) and the mandatory processes and sub process in BAI were as follows; BAI06(Manage Changes), and BAI09(Manage Assets). APO and BAI , which required documents for IT internal control were consisted of work Manual, routine document and IT document. 4) Developed a prototype for IT self-assessment embedded synthesized knowledge extract from the experts and COBIT for the resource industry. The tools used to develop the system were Start UML Version 5.0.2.1570 for system analysis; Microsoft Visual Studio Community 2015 for development of a prototype and SQL Server 2005 for database management. (5) Evaluated of the prototype system were representatives from resource industry divided into two groups. 1) A representative from the organization was not in MAI or Market for Alternative Investment of Thailand. 2) A representative of the organization that was already in MAI Market for Alternative Investment of Thailand. Evaluation period was between 21 June -29 July, 2559. Evaluation tool was the questionnaire based on the context of APO and BAI domains.

Research was shown that (1) From the synthesized knowledge from COBIT 5.0, there were only two domains out of totally six domains relevant and necessary for resources industry which were APO and BAI. (2) There were only some sub APO related such as APO01(Manage the IT management framework), APO07(Manage Human Resources), APO10(Manage Suppliers), APO12(Manage Risk), APO13(Manage Security). (3) The relevant sub BAI required for the resource industry were BAI06(Manage Changes) and BAI09(Manage Assets) (4) an evaluation by the two groups of respondents were validated that 1) both groups had confirmed to the research findings that only two domains, APO and BAI, were necessary processes (2) the organizations that are in MAI have IT process in more systematic manners based on COBOT 5 and the synthesized extract knowledge than the one which was not in MAI explicitly.

Keyword: Self-Assessment in IT

กิตติกรรมประกาศ

การจัดทำวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้เป็นอย่างดีด้วยความกรุณาจากท่านรองศาสตราจารย์ ดร.วิภาเจริญภัณฑารักษ์ สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช และ ผู้ช่วยศาสตราจารย์ ดร.สันติพัฒน์ อรุณธารี ที่ช่วยแนะนำ ปรับปรุง แก้ไข ติดตามอย่างใกล้ชิด ทำให้วิทยานิพนธ์ฉบับนี้ เสร็จสมบูรณ์ ผู้วิจัยรู้สึกซาบซึ้งในความกรุณาของทั้ง 2 ท่านเป็นอย่างมาก

ขอขอบคุณคุณพ่อและคุณแม่ที่ช่วยอบรม สั่งสอนจนประสบความสำเร็จ ขอบใจภรรยาและลูกๆ ที่คอยให้กำลังใจ สนับสนุนการทำวิจัยมาโดยตลอด นอกจากนี้ขอบคุณบริษัท เมืองทองมหาชัย จำกัด ที่ให้ความกรุณาในการเก็บรวบรวม ข้อมูล สำหรับการจัดทำวิทยานิพนธ์ฉบับนี้

สุดท้าย ขอขอบคุณคณาจารย์ แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยสุโขทัยธรรมาธิราช เพื่อนนักศึกษาและผู้ที่มีส่วนเกี่ยวข้องทุกท่าน ที่ช่วยให้การสนับสนุน แก้ไข และให้กำลังใจตลอดมา

สุรชาติ จันทสุวรรณ

สิงหาคม 2558

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

สารบัญตาราง (ต่อ)

หน้า

สารบัญภาพ

หน้า

สารบัญภาพ (ต่อ)

หน้า

บทที่ 1
บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

1.1 ความยุ่งยากในการตรวจสอบภายในด้านไอที

การนำองค์กรเพื่อเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทยของกลุ่มทรัพยากรจำเป็นจะต้องมีหลักการกำกับดูแลกิจการ และการควบคุมภายในตามธรรมาภิบาลของสำนักงานคณะกรรมการกำกับหลักทรัพย์(ก.ล.ต.) กระบวนการการตรวจสอบภายในด้านเทคโนโลยีสารสนเทศตามกรอบธรรมาภิบาลของ ก.ล.ต. มีความยุ่งยากมีความซับซ้อนเพราะต้องมีหน่วยงานในการตรวจสอบจากหน่วยงานภายในองค์กรและหน่วยงานภายนอกองค์กร การตรวจสอบภายในด้านเทคโนโลยีสารสนเทศก็ขึ้นอยู่กับอุตสาหกรรรของแต่ละองค์กร

กระบวนการการตรวจสอบภายในแต่ละองค์กรมีความแตกต่างกันอาจเนื่องมาจากอุตสาหกรรมที่แตกต่าง ประสบการณ์ของหน่วยงานไอทีหรือบุคลากร การไม่มีหน่วยงานการตรวจสอบทางด้านนี้โดยตรงเนื่องจากองค์กรไม่ได้อยู่ในตลาดหลักทรัพย์แห่งประเทศไทยหรือเป็นองค์กรขนาดเล็ก ผู้วิจัยจึงมีเห็นว่าควรมีระบบมาช่วยในการประเมินตนเอง เพื่อให้มีกระบวนการง่ายขึ้น ประหยัดเวลา มีความน่าเชื่อถือต่อการควบคุมภายในด้านไอที

1.2 กรอบการตรวจสอบภายในด้านไอทีเป็นไปตามกรอบ IT General Control ซึ่งไม่มีขั้นตอนที่ลงรายละเอียดชัดเจนตามกลุ่มอุตสาหกรรม จึงต้องใช้ประสบการณ์ของหน่วยงานดังกล่าว

การจัดตั้งหน่วยงานการตรวจสอบภายใน

1.2.1 จากภายนอกองค์กร (Outsourced Internal Auditor)

- ความรู้ความชำนาญงานตรวจหลากหลาย
- การรักษาความลับตามข้อกำหนดสัญญาจ้าง
- ความหลากหลายธุรกิจที่ตรวจสอบทำให้ไม่คุ้นเคย
- มีความยืดหยุ่นในการปรับเปลี่ยนตัวผู้ตรวจสอบ
- ไม่ยืดหยุ่นการตรวจสอบในกรณีเหตุการณ์เร่งด่วน

1.2.2 จากภายในองค์กร (In-house Internal Auditor)

- ความรู้ความชำนาญงานตรวจไม่หลากหลาย

- การรักษาความลับตามข้อกำหนดบริษัท
- ธุรกิจที่ตรวจสอบเป็นองค์กรตนเองทำให้คุ้นเคย
- การปรับเปลี่ยนตัวผู้ตรวจสอบอาจต้องศึกษากระบวนการทำงานขององค์กรเพิ่มเติม
- สามารถการตรวจสอบในกรณีเหตุการเร่งด่วน

1.3 องค์กรส่วนใหญ่ไม่มีหน่วยงานตรวจสอบภายในด้านไอทีการบริหารความเสี่ยงบางกระบวนการอาจเป็นช่องทางของการโจมตีด้านไอที การตรวจสอบภายในของหน่วยงานด้านไอทีนั้นส่วนใหญ่มีกระบวนการดังนี้

- หน่วยงานด้านไอทีใช้ประสบการณ์ด้านไอทีที่ผ่านมาในอดีต
- กรอบการตรวจสอบอาจไม่ได้อ้างอิงกับมาตรฐานใดๆด้านธรรมาภิบาลด้านไอทีทำให้กระบวนการการตรวจสอบอาจไม่ครบถ้วน
- บุคลากรที่จัดทำเอกสารอาจไม่ใช้หน่วยงานที่เกี่ยวข้องทางด้านไอที
- องค์กรนั้นอาจไม่มีหน่วยงานทางด้านไอทีทำให้แนวงานการตรวจสอบดำเนินไปได้อย่างไม่มีทิศทาง
- การบังคับใช้กระบวนการควบคุมภายในอาจไม่มีหน่วยงานดูแลอย่างชัดเจน

1.4 ไม่มีเครื่องมือประเมินกรอบการตรวจสอบภายในด้านไอทีที่ชัดเจน

ยังไม่มีองค์กรหน่วยด้านใดจัดทำเครื่องมือสร้างกรอบของกระบวนการและขั้นตอนการตรวจสอบภายในด้านไอทีโดยแยกกลุ่มอุตสาหกรรมต่างๆ ไว้อย่างชัดเจนเพื่อประเมินตนเอง ปกติต้องใช้หน่วยงานการตรวจสอบภายในขององค์กรหรือหน่วยงานตรวจสอบจากภายนอกองค์กรในการตรวจสอบหน่วยงานไอทีในการดำเนินการ

1.5 กรอบการตรวจสอบภายในด้านไอทีไม่ได้ใช้มาตรฐานทางด้านธรรมมาธิบาลด้านไอทีอ้างอิงชัดเจน

หน่วยงานไอทีถูกประเมินจากหน่วยงานผู้ตรวจ ผู้ตรวจสอบส่วนใหญ่ประเมินและให้ความเชื่อมั่นต่อความเพียงพอและประสิทธิภาพของระบบการควบคุมภายในองค์กร ตามแนวทางของ COSO และแนวทางของ ก.ล.ต.

1.6 เสียเวลา เสียโอกาสที่จะเข้าตลาดหลักทรัพย์และทำให้ค่าใช้จ่ายในการดำเนินการสูงขึ้น

เมื่อหน่วยงานไอทีไม่มีเครื่องมือช่วยสำหรับประเมินตนเอง จึงจำเป็นต้องให้หน่วยงานการตรวจสอบภายในขององค์กรประเมินให้ อาจทำให้เสียเวลาและโอกาสการเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย กลุ่มอุตสาหกรรมทรัพยากร เช่น หน่วยงานด้านไอทีมีความ

พร้อมสามารถดำเนินการตรวจสอบได้รวดเร็วครบถ้วนถูกต้อง ผู้ตรวจสอบก็สามารถมีเวลามากขึ้นในการไปตรวจสอบหน่วยงานอื่นๆ จนกระทั่งครบทั่วทั้งองค์กร

1.7 ประโยชน์ในการเข้าตลาดมีความสำคัญดังนี้

1.7.1 แหล่งระดมเงินทุนระยะยาว บริษัทสามารถระดมทุนจากประชาชนเพื่อนำไปใช้เป็นเงินทุนหมุนเวียนหรือขยายธุรกิจได้โดยง่ายและรวดเร็ว ซึ่งก่อให้เกิดความได้เปรียบในด้านการแข่งขัน รวมทั้งช่วยให้มีโครงสร้างทางการเงินที่เหมาะสมต่อการดำเนินกิจการ นอกจากนี้ยังเป็นการเปิดโอกาสในการเลือกระดมทุนผ่านการออกหลักทรัพย์ประเภทอื่นๆ ได้ง่ายขึ้นภายหลังการเข้าจดทะเบียน เช่น หุ้นกู้ หุ้นกู้แปลงสภาพ เป็นต้น

1.7.2 ภาพลักษณ์ การเข้าเป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์ฯ จะช่วยเสริมสร้างภาพลักษณ์ที่ดีในฐานะที่บริษัทได้ผ่านการพิจารณาจาก สำนักงานคณะกรรมการ ก.ล.ต. และคณะกรรมการตลาดหลักทรัพย์ฯ ซึ่งถือได้ว่าเป็นบริษัทที่มีผลการดำเนินงานที่ดี และมีฐานะมั่นคงในระดับหนึ่ง รวมทั้งมีการเปิดเผยข้อมูลที่โปร่งใส ภาพลักษณ์ที่ดีนี้จะก่อให้เกิดคุณประโยชน์ในด้านต่างๆ ที่เกี่ยวข้องกับการประกอบธุรกิจของบริษัท เช่น ความน่าเชื่อถือ อำนาจในการต่อรอง และสร้างความตระหนักตลอดจนความนิยมในผลิตภัณฑ์/บริการของกิจการโดยทางอ้อม นอกจากนี้การเผยแพร่ข่าวสารและความเคลื่อนไหวของบริษัทผ่านสื่อต่างๆ ของตลาดหลักทรัพย์ฯ ล้วนเป็นสิ่งที่สามารถเกื้อกูลต่อกิจการของบริษัทให้เป็นที่รู้จักและยอมรับของสาธารณชนมากยิ่งขึ้น คุณประโยชน์นี้หากสามารถตีค่าเป็นตัวเงินแล้วย่อมหมายถึงค่าใช้จ่ายมูลค่ามหาศาลสำหรับคู่แข่งที่มิได้อยู่ในตลาดหลักทรัพย์ฯ ที่จะต้องใช้ในการโฆษณาหรือประชาสัมพันธ์ให้เป็นที่รู้จักและยอมรับของสาธารณชน

1.7.3 จุดเริ่มต้นในการเชื่อมโยงหรือขยายธุรกิจกับธุรกิจต่างประเทศ ในยุคโลกาภิวัตน์การประกอบธุรกิจระหว่างประเทศได้ทวีความสำคัญมากขึ้น การมีแนวร่วมโดยเฉพาะแนวร่วมจากกิจการในต่างประเทศที่สามารถเกื้อกูลระหว่างกันทั้งในด้านการตลาด การผลิต เทคโนโลยี การเงิน และบุคลากร ย่อมส่งผลให้เกิดความได้เปรียบในเชิงแข่งขัน การเป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์ฯ ย่อมเป็นจุดเริ่มต้นที่ดี และเป็นแรงจูงใจให้เกิดความสนใจในการเข้าร่วมลงทุนจากธุรกิจต่างชาติซึ่งจะเกื้อหนุนให้เกิดการขยายตัวทางธุรกิจอย่างต่อเนื่องและสามารถเพิ่มความแข็งแกร่งให้แก่บริษัทมากยิ่งขึ้น

1.7.4 การสร้างความรับผิดชอบและการบริหารแบบมืออาชีพ การเข้าจดทะเบียนในตลาดหลักทรัพย์ฯ จะมีส่วนช่วยกระตุ้นให้บริษัทบริหารงานได้อย่างมีประสิทธิภาพ และรัดกุมมากขึ้นเนื่องจากบริษัทจะอยู่ในความสนใจของผู้ลงทุน โดยมีราคาหุ้นของบริษัทเป็นตัวสะท้อนความเชื่อมั่นของสาธารณชนที่มีต่อกิจการในระดับหนึ่ง ในขณะเดียวกันการเข้าจดทะเบียนก็จะเป็น

เครื่องมือ ในการกำกับดูแลการบริหารกิจการให้เป็นไปในทิศทางที่ควรจะเป็น ซึ่งจะช่วยเสริมสร้างประสิทธิภาพตลอดจนเพิ่มพูนประสิทธิผลในการประกอบธุรกิจอันจะเป็นผลประโยชน์แก่ทุกฝ่ายที่มีส่วนเกี่ยวข้องกับบริษัทโดยรวม

1.7.5 ความภาคภูมิใจของบุคลากรของบริษัท คุณประโยชน์ที่สำคัญประการหนึ่งที่มักจะถูกมองข้ามจากการที่บริษัทเข้าจดทะเบียนในตลาดหลักทรัพย์ฯ คือ ความภาคภูมิใจของพนักงานของบริษัท โดยหากบริษัทนั้นมีผลประกอบการและภาพลักษณ์ที่ดีมีชื่อเสียงเป็นที่ยอมรับและรู้จักกันอย่างแพร่หลายย่อมทำให้บุคลากรของบริษัทเกิดความรู้สึกที่ดีต่อบริษัท หากผู้บริหารรู้จักใช้สิ่งนี้ให้เป็นประโยชน์โดยการสร้างความยึดมั่นหรือค่านิยมร่วม (shared value) ให้เกิดขึ้นในลักษณะของการกระตุ้นให้บุคลากรทุกฝ่ายได้ตระหนัก และมีส่วนร่วมต่อการสร้างชื่อเสียงและเกียรติคุณของบริษัท คุณประโยชน์อันมหาศาลย่อมจะเกิดขึ้นกับบริษัทในระยะยาว

1.7.6 สิทธิประโยชน์ทางภาษีเงินปันผล บริษัทจดทะเบียนจะได้รับสิทธิประโยชน์ทางภาษีในกรณีที่บริษัทจดทะเบียนไปถือหุ้นของบริษัทอื่นที่จัดตั้งตามกฎหมายไทยหรือกองทุนรวม เงินปันผลที่ได้รับจากบริษัทอื่นดังกล่าวจะได้รับการยกเว้นภาษีเงินได้ แต่เงินที่ได้รับดังกล่าวต้องเป็นเงินที่ได้รับจากหุ้นหรือหน่วยลงทุนที่ถือไว้ไม่น้อยกว่า 3 เดือนก่อน และหลังวันที่ได้รับเงินได้

2. วัตถุประสงค์การวิจัย

การศึกษานี้มีวัตถุประสงค์เพื่อ

1.1 ศึกษาวิธีการตรวจประเมินตนเองของหน่วยงานไอที โดยการอ้างอิงกระบวนการตามหลักธรรมาธิบาลมาตรฐานโคบิต 5.0 (COBIT 5.0)

1.2 เพื่อพัฒนาระบบสำหรับในการประเมินความพร้อมของหน่วยงานเทคโนโลยีสารสนเทศ เพื่อเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย กลุ่มอุตสาหกรรมทรัพยากร โดยใช้หลักธรรมาภิบาลไอที

3. กรอบแนวคิดการวิจัย

การวิจัยดำเนินการตามลำดับดังต่อไปนี้

3.1 ศึกษามาตรฐานโคบิต 5.0 (COBIT 5.0) เข้ามาช่วยในการพัฒนาระบบการประเมินความพร้อมของหน่วยงานเทคโนโลยีสารสนเทศ เพื่อเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย กลุ่มอุตสาหกรรมทรัพยากร โดยนำในส่วนที่เกี่ยวข้องดังนี้มาใช้เป็นกรอบในการวิจัย

3.2 รวบรวมข้อมูลที่ใช้ในการประเมินผลการการควบคุมภายใน โดยสัมภาษณ์เชิงลึกจากผู้เชี่ยวชาญทางด้านขบวนการตรวจสอบภายในเพื่อพัฒนากรอบกระบวนการการตรวจสอบภายใน

3.2.1 ผู้วิจัยสร้างกรอบกระบวนการการตรวจสอบภายในด้านไอที เพื่อใช้เป็นแนวในการสัมภาษณ์

3.2.2 เมื่อสัมภาษณ์ผู้ตรวจสอบภายในจากกรอบที่เตรียมไว้เพื่อให้ได้กระบวนการณ์ที่ถูกต้องและใช้ในการตรวจสอบจริง

3.2.3 สรุปกระบวนการและขั้นตอนการควบคุมภายในจากการสัมภาษณ์ จนกระทั่งได้และประเมินการตรวจสอบภายในด้านไอที

3.3 ทดสอบการประเมินระบบโดยหน่วยงานไอทีในตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย กลุ่มอุตสาหกรรมทรัพยากรและหน่วยงานไอทีที่ไม่ได้อยู่ตลาดหลักทรัพย์กลุ่มอุตสาหกรรมทรัพยากร โดยระบบขบวนการต่างๆ ดังนี้

3.3.1 กระบวนการสร้างการตรวจสอบภายในของหน่วยงานไอทีที่ใช้ระบบ การความคุมภายในตามข้อมูลปัจจุบัน

3.3.2 รายงานข้อเสนอแนะกระบวนการและแนวการควบคุมที่เหมาะสมจากกรอบการตรวจสอบภายใน

3.3.3 รายงานข้อเสนอแนะความเสี่ยงกระบวนการของแนวปฏิบัติ ที่เหมาะสมจากกรอบการตรวจสอบภายในจากหัวข้อที่ 4.2

3.4 เครื่องมือที่ใช้ในการวิจัยนี้มีดังนี้

3.4.1 Microsoft Visual Studio Community 2015

3.4.2 ภาษา Visual Basic

3.4.3 Microsoft SQL Server

3.4.4 Start UML Version 5.0.2.1570

4. นิยามศัพท์เฉพาะ

4.1 ธรรมาภิบาลไอที (IT Governance) หมายถึง กรอบแนวคิดในการบริหารจัดการงานทางด้านไอที โดยมุ่งหวังให้การทำงานทางด้านไอทีไม่ว่าจะเป็นงานทางด้านโครงการหรืองานบริการ มีการบริหารจัดการที่ดี มีการใช้ทรัพยากรไอที ให้เกิดประโยชน์สูงสุด ส่งมอบงานให้กับผู้ใช้ได้ตามกำหนด โดยเป้าหมายในการบริหารงานทางด้านไอทีจะต้องมีความสอดคล้องกับเป้าหมายขององค์การ

4.2 กรอบโคบิตเวอร์ชั่น 5.0 (Cobit5.0) หมายถึง กรอบวิธีปฏิบัติที่ออกโดยองค์การด้านตรวจสอบระบบสารสนเทศและควบคุม (Information Systems Audit and Control Foundation (ISACF)) ซึ่งมีวัตถุประสงค์เพื่อให้องค์การและหน่วยงานใดๆ สามารถบริหารจัดการระบบสารสนเทศและทรัพยากรไอที ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ บริหารและควบคุมความเสี่ยงให้องค์กร

4.3 ตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย หมายถึง บริษัทที่จะเข้าจดทะเบียนได้ต้องเป็นบริษัทที่มีประวัติการดำเนินงานมาพอสมควร โดยมีผลกำไรที่ผ่านมาชัดเจน พร้อมกระจายการถือหุ้นให้สาธารณชน และที่สำคัญต้องมีบรรษัทภิบาลที่ดี มีความโปร่งใสและมีความน่าเชื่อถือ

4.4 Microsoft Visual Studio Community 2015 หมายถึง ชุดเครื่องมือพัฒนาที่ถูกออกแบบมาเพื่อช่วยเหลือ นักพัฒนาซอฟต์แวร์ (ไม่ว่าพวกเขาจะเป็นนักพัฒนามือใหม่หรือนักพัฒนามืออาชีพก็ตาม) ที่กำลัง เผชิญกับความท้าทายที่ซับซ้อนของการสร้างโซลูชันที่ทันสมัยขึ้นมา บทบาทของ Visual Studio ก็คือการเข้ามาปรับปรุงขั้นตอนการพัฒนาและช่วยให้การแก้ปัญหาที่ซับซ้อนทำได้ง่ายขึ้นและน่าพอใจมากขึ้นกว่าเดิม(ถือเป็นรุ่นแจกฟรีสำหรับนักพัฒนา โดยเน้นไปที่นักพัฒนาที่ไม่ใช่สายองค์กรเป็นหลัก)

4.5 ภาษาVisual Basic หมายถึง โปรแกรมแบบ GUI (ระบบการติดต่อสื่อสารระหว่างผู้ใช้งานกับเครื่องคอมพิวเตอร์โดยผ่านทางภาพหรือแผนภูมิที่เข้าใจได้ง่ายแทนการพิมพ์คำสั่งโดยตรง เพื่อให้คอมพิวเตอร์ทำงานตามที่ต้องการ) พัฒนามาจากภาษา Basic โดยบริษัท Microsoft เป็นเครื่องมือที่ช่วยให้การพัฒนา Application บนระบบปฏิบัติการ Windows ทำได้โดยง่าย ถึงไม่ใช่โปรแกรมเมอร์ก็สามารถสร้างโปรแกรมได้ ภาษานี้เป็นหนึ่งในภาษาโปรแกรมยอดนิยมสำหรับโปรแกรมที่ใช้ในด้านธุรกิจ

4.6 Microsoft SQL Server Management Studio Express หมายถึง ระบบการจัดเก็บกลุ่มของข้อมูล โดยลักษณะการจัดเก็บข้อมูลเหล่านั้นมีการจัดเก็บรูปแบบตารางที่มีความสัมพันธ์กัน การจัดเก็บเป็นแฟ้มเดียวหรือหลายแฟ้มข้อมูลตามขนาดความซับซ้อนแต่ตามปกติระบบงานมักจะประกอบด้วยหลายแฟ้มข้อมูล ซึ่งการออกแบบฐานข้อมูลจัดทำโดยกลุ่มหรือผู้มีความรู้ความเข้าใจในระบบงานนั้นๆ การออกแบบระบบฐานข้อมูลที่ดีควร (1) มีระบบความปลอดภัย (2) เวลาเข้าถึงข้อมูลได้รวดเร็ว (3) โครงสร้างความสัมพันธ์เข้าใจง่ายต่อความเข้าใจ เป็นต้น (เป็นโปรแกรมฟรีจากบริษัทไมโครซอฟต์ ที่มีข้อจำกัดด้านใช้งาน)

4.7 Start UML Version 5.0.2.1570 หมายถึง เครื่องมือสำหรับสร้างภาษา UML (Open Source UML) ภาษายูเอ็มแอล (UML) ย่อมาจาก Unified Modeling Language เป็นภาษาที่ใช้อธิบายแบบจำลองต่างๆ หรือเป็นภาษาสัญลักษณ์รูปภาพมาตรฐาน สำหรับใช้ในการสร้างแบบจำลองเชิงวัตถุ

โดยยูเอ็มแอล เป็นภาษามาตรฐานสำหรับสร้างแบบพิมพ์เขียวให้แก่ระบบงาน เราสามารถใช้ยูเอ็มแอลในการสร้างมุมมอง กำหนดรายละเอียด สร้างระบบงานและจัดทำเอกสารอ้างอิงให้แก่ระบบงานได้

ฐานะทางการเงินและผลการดำเนินงาน

- ทุนชำระแล้วและส่วนของผู้ถือหุ้น (หลังกระจายหุ้นให้กับประชาชนแล้ว) ทุนชำระแล้วและส่วนของผู้ถือหุ้นไม่น้อยกว่า20 ล้านบาท

- ผลการดำเนินงาน (1) มีผลการดำเนินงานต่อเนื่องไม่ต่ำกว่า 2 ปี ภายใต้การจัดการของผู้บริหารส่วนใหญ่กลุ่มเดียวกันอย่างน้อย 1 ปี ก่อนยื่นคำขอ (2) มีกำไรสุทธิในปีล่าสุดก่อนยื่นคำขอ และมีกำไรสุทธิในงวดสะสมของปีที่ยื่นคำขอ (3) กรณีมีผลการดำเนินการเพียง 1 ปี จะต้องมีมูลค่า

การกระจายการถือหุ้น

-ไม่น้อยกว่า 300 ราย

-ไม่น้อยกว่าร้อยละ 20 ของทุนชำระแล้ว

- จำนวนหุ้นที่เสนอขาย ต้องไม่น้อยกว่า 15%ของทุนชำระแล้ว

4.4 กลุ่มทรัพยากร (Resources) หมายถึง ธุรกิจเกี่ยวกับการแสวงหา หรือจัดการทรัพยากรต่างๆ เช่น การผลิตและจัดสรรเชื้อเพลิงพลังงาน และการทำเหมืองแร่มีหมวดธุรกิจดังนี้

- พลังงานและสาธารณูปโภค (Energy & Utilities) ผู้ประกอบธุรกิจเกี่ยวกับ ผลิต สำรวจ ขุดเจาะ กลั่น และตัวแทนจำหน่ายพลังงานธรรมชาติในรูปต่างๆ เช่น น้ำมันและก๊าซธรรมชาติ ผู้ให้บริการสาธารณูปโภค เช่น ไฟฟ้า ประปา และแก๊ส

- เหมืองแร่ (Mining) ผู้สำรวจแร่ ทำเหมืองแร่ ถลุงแร่ ตัวแทนจำหน่ายแร่ โดยแร่เหล่านี้เป็นแร่ธาตุต่างๆ ทั้งที่เป็นโลหะและอโลหะ แต่ไม่รวมแร่ธาตุที่ให้พลังงาน

4.5 ประเมินผล หมายถึง ความพร้อมของหน่วยงานไอที ของบริษัทจดทะเบียนในกลุ่มทรัพยากร ตามกรอบโคบิต เพื่อเตรียมความพร้อมในการเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย

5. ประโยชน์ที่ได้จากการศึกษา

ประโยชน์ที่คาดว่าจะได้รับจากการศึกษามีดังต่อไปนี้

5.1 ทราบถึงวิธีการตรวจประเมินหน่วยงานไอทีโดยใช้กรอบธรรมาภิบาลตามมาตรฐาน COBIT 5.0 โดยใช้กระบวนการได้เป็นกรอบที่อ้างอิงที่มีแนวทางปฏิบัติได้อย่างชัดเจน

5.2 มีระบบประเมินตนเองด้านเทคโนโลยีสารสนเทศ ของบริษัทจดทะเบียนในกลุ่มทรัพยากร ตามกรอบโคบิต เพื่อเตรียมความพร้อมในการเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย

บทที่ 2
วรรณกรรมที่เกี่ยวข้อง

1. หลักการและทฤษฎีที่เกี่ยวข้อง

1.1 ความหมายธรรมาภิบาลด้านไอที ความเสี่ยงทางธุรกิจ

ระบบไอทีมีพัฒนาการอย่างรวดเร็ว ธุรกิจต้องพึ่งพาระบบคอมพิวเตอร์มากยิ่งขึ้น สารสนเทศถูกนำมาใช้เพื่อปรับเปลี่ยนกระบวนการทำงานทำให้สามารถบริหารจัดการต้นทุนได้อย่างมีประสิทธิภาพ แต่การนำไอทีมาใช้ถ้าระบบไอทีไม่มีระบบรักษาความปลอดภัยที่ดี ระบบอาจถูกคุกคามจากผู้ไม่หวังดีได้ ก่อให้เกิดความเสียหายต่อธุรกิจ และอาจทำให้ธุรกิจหยุดชะงักไม่สามารถให้บริการต่อไปได้ ปัญหาต่างๆ เหล่านี้จำเป็นต้องใช้หลักในการจัดการไอทีที่เรียกว่า ธรรมาภิบาลด้านไอที มาช่วยจัดการกระบวนการทางด้านไอทีเพื่อสร้างความมั่นใจว่าทรัพยากรไอทีจะถูกนำไปใช้สร้างคุณค่าให้กับองค์การธุรกิจได้อย่างมีประสิทธิภาพและประสิทธิผล

1.1.1 คำว่า "ธรรมาภิบาลด้านไอที (IT Governance) พบว่าถูกนำมาใช้โดย Loh and Venkatrama ในปี 1992 และ Henderson และ Venkatraman ปี 1993 โดยเป็นการอธิบายกลไกเพื่อให้บรรลุถึงการใช้ไอทีที่เต็มความสามารถแต่ช่วงนั้นคำว่าธรรมาภิบาลด้านไอทียังไม่มีความโดดเด่นในแวดวงวิชาการจนกระทั่งเข้าสู่ตอนปลายของ 1990 โดยในปี 1997 เมื่อ Brow และ Sambamurthy และ Zmud ในปี 1999 เริ่มอ้างถึงคำว่า "IS governance frameworks" และหลังจากนั้นก็ปรับใช้คำว่า "IT Governance frameworksใน บทความวิชาการ[2]

ธรรมาภิบาลด้านไอทีคือหลักในการบริหารจัดการที่ผู้บริหารขององค์การควรผลักดันให้ทุกคนในองค์การยึดถือเป็นแบบอย่างเพื่อปฏิบัติร่วมกัน องค์การธุรกิจจำเป็นต้องมีกรอบในการปฏิบัติงานเพื่อบริหารจัดการกระบวนการทางด้านไอทีและจะต้องมีกระบวนการวัดและประเมินผลการปฏิบัติเพื่อสร้างความมั่นใจให้กับผู้มีส่วนได้ส่วนเสียว่าเงินลงทุนต่างๆ จะไม่สูญเสียไปอย่างไร้ประโยชน์และได้รับความคุ้มค่าจากการลงทุนทางด้านไอทีขององค์การอีกด้วย

ธรรมาภิบาลด้านไอทีมีส่วนสำคัญในการบริหารจัดการองค์กรที่ใช้ไอทีมาเป็นหน่วยงานหนึ่งที่คอยสนับสนุนองค์กร ในอดีตมีงานวิจัยหลายเรื่องที่แสดงให้เห็นถึงความสำคัญของ ธรรมาภิบาลด้านไอที ดังเช่นงานวิจัยในอดีตของ Broadbent ปี 1998 ได้มีการอธิบายว่าธรรมาภิบาลด้านไอทีเป็นส่วนหนึ่งของธรรมาภิบาลขององค์กร[3] (Corporate Governance)

และจากการศึกษา 256 องคก์รทั้งแบบองคก์รที่หวังผลกำไร และ ไม่หวังผลกำไร จาก 23 ประเทศใน อเมริกา ยุโรป และ เอเชียแปซิฟิคของ Peter Weill จากสถาบัน MIT Sloan School of Management พบว่าขีดความสามารถขององค์กร และ ธรรมาภิบาลด้านไอทีพบว่ามีความสัมพันธ์กัน โดยมีการเปรียบเทียบองค์กรที่มีกลยุทธ์เดียวกัน องค์กรที่มีธรรมาภิบาลด้านไอที สามารถสร้างกำไรได้มากกว่า 20% เมื่อเทียบกับองค์กรที่ไม่มีธรรมาภิบาลด้านไอที [2]

1.1.2 ความจำเป็นของธรรมาภิบาลด้านไอที ปัจจุบันระบบไอทีเข้ามามีบทบาทต่อการดำเนินธุรกิจ ช่วยอำนวยความสะดวกให้กับผู้ปฏิบัติงาน ช่วยสร้างความได้เปรียบทางการแข่งขัน องค์การจึงต้องมีการปรับเปลี่ยนกระบวนการทำงานภายในให้เข้ากับสภาพแวดล้อมที่กำลังเปลี่ยนแปลงให้ได้ ทั้งนี้หากองค์การไม่สามารถ ปรับตัวได้ทันกับการเปลี่ยนแปลง อาจส่งผลกระทบต่อธุรกิจดังต่อไปนี้

1) ความเสี่ยงจากการนำไอทีมาใช้อาจก่อให้เกิดความเสียหายกับธุรกิจ องค์กรธุรกิจจัดตั้งบริษัทใช้บริการงานทางด้านไอทีกับบริษัทโดยมุ่งหวังเพื่อต้องการลดค่าใช้จ่ายโดยรวมทางด้านไอที แต่ไม่ได้วางแผนการเชื่อมต่อสถาปัตยกรรมและระบบเครือข่ายเข้าไว้ด้วยเพื่อใช้บริการร่วมกัน (shared service) ขาดการควบคุมภายใน การบริหารความเสี่ยง

2) การนำระบบไอทีมาใช้แต่ไม่มีความสอดคล้องกับวัตถุประสงค์ของธุรกิจ องค์การธุรกิจจัดตั้งบริษัทเพื่อให้บริการงานทางด้านไอทีกับบริษัทในกลุ่มโดยมุ่งหวังลดค่าใช้จ่ายโดยรวมทางด้านไอที แต่ไม่ได้วางแผนการเชื่อมต่อสถาปัตยกรรมและระบบเครือข่ายเข้าไว้ด้วยเพื่อใช้บริการร่วมกัน (shared service)

3) การบริหารการใช้ทรัพยากรไอทีอย่างไม่คุ้มค่า กรณีองค์การลงทุนโครงการพัฒนาระบบวางแผนทรัพยากรขององค์การ

ดังนั้น การจัดการไอทีจำเป็นต้องมีการจัดการอย่างมีประสิทธิภาพ เนื่องจากค่าใช้จ่ายต่างๆ ทางด้านไอทีคือต้นทุนที่มีมูลค่าสูง ถ้ามีการนำมาใช้อย่างไม่เหมาะสม จัดการได้ไม่ดี ไม่ก่อให้เกิดประโยชน์กับองค์การ ก็จะทำให้ต้นทุนในการดำเนินธุรกิจสูงขึ้นตามไปด้วย ดังนั้น การนำระบบไอทีมาใช้ในองค์การ จึงต้องถูกจัดการให้เหมาะสมกับการดำเนินธุรกิจ หลักการจัดการทางด้านไอทีที่นิยมนำมาใช้และได้รับการยอมรับคือ หลักธรรมาภิบาลด้านไอที (IT Governance: ITG)

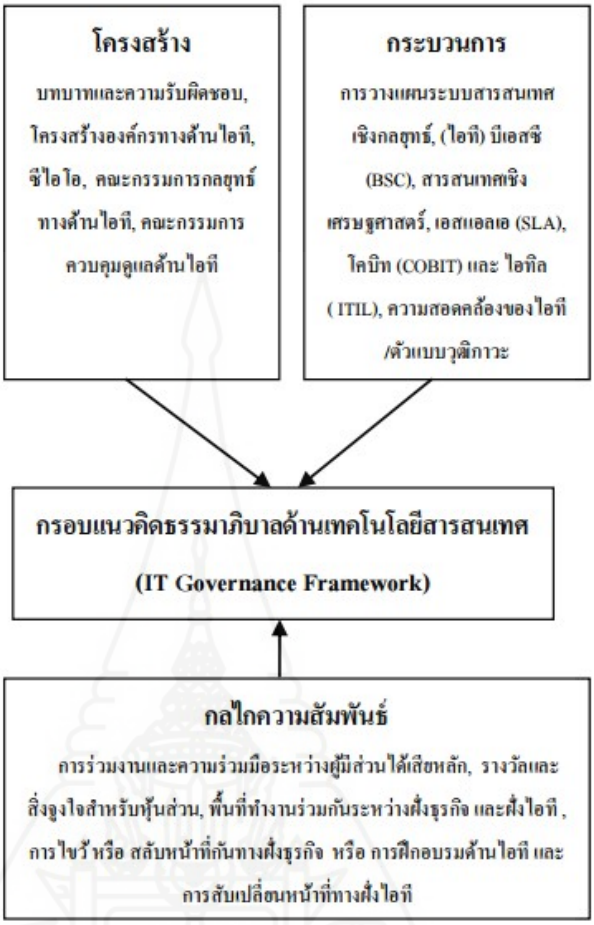
1.2 ความหมายการบริหารความเสี่ยงทางธุรกิจ

ในปัจจุบันการดำเนินธุรกิจอยู่ภายใต้ความเสี่ยงในรูปแบบต่างๆ กัน ผู้บริหารจะประสบผลสำเร็จใน การบริหารงานให้บรรลุตามวัตถุประสงค์หรือไม่ สิ่งหนึ่งที่ผู้บริหารต้องให้ความสำคัญ คือ ความรู้ ความเข้าใจในการบริหารความเสี่ยงรวมถึงการเลือกใช้เครื่องมือเพื่อการบริหารความเสี่ยงให้เกิด ประสิทธิภาพสูงสุด ความเสี่ยงจะมีลักษณะที่แตกต่างกันไปตามประเภท

ของธุรกิจ แต่สิ่งที่เหมือนกัน คือ ความเสี่ยง หมายถึง ความไม่แน่นอนที่เมื่อเกิดขึ้นแล้วจะนำไปสู่ความสูญเสีย ถ้ากิจการไม่ สามารถรับมือหรือบริหารจัดการได้ทัน การบริหารความเสี่ยงจำเป็นต้องทำควบคู่กับการกำกับดูแล และการควบคุมภายในอย่างมีประสิทธิภาพ องค์กรที่มีกระบวนการบริหารความเสี่ยงจะช่วยให้เกิดความมั่นใจระดับหนึ่งว่าการดำเนินงานจะเป็นไปอย่างมีประสิทธิภาพ เพราะการบริหารความเสี่ยง คือการคาดการณ์ความไม่แน่นอนที่อาจเกิดขึ้นอย่างมีหลักการ และกำหนดแนวทางป้องกัน หรือลด ความเสียหายที่อาจเกิดขึ้น และถือเป็นส่วนหนึ่งของการบริหารจัดการที่ทุกส่วนในองค์กรต้องเข้าไป เกี่ยวข้อง เพื่อสร้างระบบบริหารความเสี่ยงที่เหมาะสม องค์กรที่มีระบบการบริหารจัดการที่ดีจะดำเนินการบนพื้นฐานของกิจกรรมหลักๆ ที่สำคัญ 3 ประการ คือ การบริหารความเสี่ยง (Risk Management) การตรวจสอบภายใน (Internal Audit) และการควบคุมภายใน (Internal Control) ภาระหน้าที่ที่สำคัญอย่างหนึ่งของการตรวจสอบภายใน คือ การประเมินและให้ความเชื่อมั่นต่อระบบ การบริหารจัดการขององค์กร เพื่อนำไปสู่การบรรลุตามวัตถุประสงค์ขององค์กร รวมถึงการทำงาน ของผู้ตรวจสอบภายในเอง ต้องมีการกำหนดแผนการตรวจสอบ ซึ่งสอดคล้องกับแนวทางการบริหาร ความเสี่ยง เพื่อตอบสนองการทำงานของผู้บริหาร และเพื่อเตรียมความพร้อมให้องค์กร ในการหาวิธี การจัดการกับความเสี่ยงที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ[5]

1.3 องค์ประกอบที่จำเป็นของกรอบแนวคิดธรรมาภิบาลด้านไอที

Van Grembergen, W. และ De Haes S.2006 ได้นำเสนอองค์ประกอบที่จำเป็นสำหรับกรอบแนวคิด ของธรรมาภิบาลด้านไอที และถูกนำไปปรับใช้อย่างแพร่หลาย ประกอบด้วย โครงสร้าง กระบวนการ และ กลไกความสัมพันธ์ ของผู้มีส่วนได้ส่วนเสียหลัก รวมถึงการทำงานร่วมกันระหว่างฝั่งธุรกิจและฝั่งเทคโนโลยี สารสนเทศดังภาพที่ 2.1



ภาพที่ 2.1 แสดงองค์ประกอบที่จำเป็นของธรรมาภิบาลด้านไอที

องค์ประกอบดังกล่าว เป็นส่วนผลักดันให้องค์กรนั้นๆ มีมุมมองต่อขบวนการทำงานของตนเองในด้านไอทีทั้งทางตรงและทางอ้อม ครบทุกองค์ประกอบหลัก ส่วนการให้น้ำหนักความมากน้อยของแต่ละขบวนการ ขึ้นอยู่กับอุตสาหกรรม วิสัยทัศ พันธกิจ กิจกรรมหลัก มุมมองของฝ่ายบริหารและผู้มีส่วนได้ส่วนเสียขององค์กรนั้นๆเป็นแนวทางใด

1.4 มาตรฐานและเครื่องมือที่เกี่ยวข้องกับธรรมาภิบาลด้านไอที

Michael Holm Larsen และคณะ 2006 ได้ศึกษามาตรฐานหรือเครื่องมือด้านธรรมาภิบาลด้านไอที เพื่อวิเคราะห์และประเมินความสามารถของมาตรฐานและเครื่องมือต่างๆ เหล่านั้น โดยใช้บริษัท Novozymes A/S ซึ่งเป็นองค์กรที่เป็นผู้นำของโลกด้านฐานข้อมูลเทคโนโลยีชีวภาพเป็นกรณีศึกษาได้ทำการศึกษารวบรวมมาตรฐานและเครื่องมือได้จำนวน 17 ตัวแบบ ได้แก่ ITIL, COBIT, ASL, CMM/CMMI, Six Sigma, IT Service CMM, ISO 17799, SOX, SAS70, SysTrust, Prince2, IT Audit, IT Due Diligence, IT Governance Review, IT Governance Assessment, IT

Governance Checklist, IT Governance Assessment Process (ITGAP) Model [10] ต่อมา Mehdi Fasanghari และคณะ 2008 ได้ศึกษา เพื่อเปรียบเทียบมาตรฐานด้านธรรมาภิบาลด้านไอที และสร้างวิธีการแก้ไขปัญหา เพื่อให้องค์กรสามารถ เลือกมาตรฐานที่เหมาะสมที่สุดสำหรับโครงสร้างขององค์กรโดยได้รวบรวมมาตรฐานจากการสำรวจ เอกสารงานวิจัยที่เกี่ยวข้อง ใช้มาตรฐานทั้งสิ้น 13 ตัวแบบในการทำวิจัยซึ่งมีมาตรฐานบางตัวที่เพิ่มเติมและ แตกต่างจากงานวิจัยของ Michael Holm Larsen และคณะ 2006 จำนวน 5 ตัวแบบ ได้แก่ COSO, ISO/IEC 17799:2000, ISO/IEC TR 13335, TickIT, NIST 800-14 [11] และในปัจจุบันมีมาตรฐานเกี่ยวข้องเพิ่มเติม เพื่อใช้เป็นมาตรฐานของธรรมาภิบาลด้านไอที โดยตรงคือ ISO/IEC 38500 [12] โดยสรุปจากการศึกษา เอกสารงานวิจัยที่เกี่ยวข้องในส่วนของมาตรฐานและเครื่องมือด้านธรรมาภิบาลด้านไอที พบว่ามีมาตรฐาน

1.4.1 COBIT (Control Objectives for Information and Relate Technology) ถูกพัฒนาขึ้นตั้งแต่ ปี 1996[12]โดยสถาบัน IT Governance (IT Governance Institute :ITGI)[web] ปัจจุบัน COBIT พัฒนามาถึง รุ่น 5 มีวัตถุประสงค์ เพื่อเป็นกรอบแนวคิดในการบริหารจัดการร่วมกับตัวแบบธรรมาภิบาลด้านไอทีซึ่งสามารถช่วยควบคุมและจัดการสารสนเทศและความสัมพันธ์ของเทคโนโลยี [10] เป็นมาตรฐานหนึ่งที่ได้รับ การยอมรับและใช้กันอย่างแพร่หลาย โดยมาตรฐานนี้ได้รวมถึง (1) การวัดขีดความสามารถของ องค์ประกอบต่างๆ , การวัดผลตอบแทน และขีดความสามารถในการขับเคลื่อนกระบวนการทางไอที (IT Process) (2) รายการปัจจัยความสำเร็จที่สำคัญ (Critical Success Factors: CSF) อย่างกระชับ และตัวแบบ การดำเนินการที่ดีของแต่ละกระบวน (3) ตัวแบบวุฒิภาวะ (Maturity Model) ใช้เป็นต้นแบบเพื่อช่วยเป็นแนวทาง และ การตัดสินใจสำหรับการปรับปรุงความสามารถ

1.4.2 ITIL (Information Technology Infrastructure Library (ITIL) เป็นเครื่องมือหนึ่งที่เน้น ด้านการจัดการบริการ (Service Management) โดยมีลักษณะเด่นคือให้ความสำคัญกับกระบวนการทางธุรกิจ และ คุณภาพของการบริการ ITIL ได้รับการยอมรับอย่างแพร่หลายว่าเป็นรูปแบบการปฏิบัติที่ดีที่สุด (Best Practices) จากนักปฏิบัติหรือผู้ดำเนินงานด้านเทคโนโลยีสารสนเทศทั่วโลกนับพันคน

1.4.3 COSO (Committee of Sponsoring Organizations) เป็นหน่วยงานที่ได้เผยแพร่วิธีการและ กรอบแนวคิดของการควบคุมภายใน (Internal Control Framework) ขององค์กรได้กำหนดการควบคุมภายใน อย่างเป็นระบบ โดยเริ่มพัฒนาตั้งแต่ปี 1992 ซึ่งหมายถึงกระบวนการที่คณะผู้บริหารและบุคลากรในองค์กร กำหนดขึ้น ซึ่งเป็นการออกแบบในระดับที่สมเหตุสมผลเพื่อให้เกิดความเชื่อมั่นในการบรรลุวัตถุประสงค์ ในเรื่องดังต่อไปนี้ (1) ความมีประสิทธิภาพและ

ประสิทธิผลของการดำเนินงาน (2) ความเชื่อถือได้ของ ข้อมูลและรายงานทางการเงิน (3) การปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ[14]

1.4.4 ISO/ IEC 38500 (2008) เป็นมาตรฐานการกำกับดูแลธรรมาภิบาลด้านไอทีขององค์กร (Corporate Governance of Information Technology)โดยตรง มาตรฐานนี้มีวัตถุประสงค์เพื่อเป็นกรอบแนวคิดแนวทางในการประเมิน,ทิศทางและ การตรวจสอบการใช้งานเทคโนโลยีสารสนเทศของแต่ละองค์กรมาตรฐานนี้สอดคล้องกับนิยามของธรรมาภิบาลองค์กร (Corporate Governance) ซึ่งเคยตีพิมพ์ในปี 1992 ขอบเขตของมาตรฐานนี้ประกอบไปด้วยแนวทางรวม 6 หลักการ ได้แก่ (1) บทบาทและหน้าที่ความรับผิดชอบ (Responsibility) (2) กลยุทธ์ (Strategy) (3) การได้มา (Acquisition) (4) ขีดความสามารถ (Performance) (5) ความสอดคล้อง (Conformance) และ 6. พฤติกรรมมนุษย์ (Human behavior) [12]

1.5 ความหมายความเสี่ยงและการควบคุมตามแนวกับธรรมาภิบาลด้านไอที

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานขององค์กร ทั้งในการบริหารจัดการ การจัดเก็บข้อมูล และการประมวลผลระบบงานสำคัญต่างๆ การควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศจึงเป็นเรื่องที่ส่วนองค์กรควรให้ความสำคัญ โดยกำหนดนโยบายที่จะกำกับดูแลและตรวจสอบเกี่ยวกับการบริหารจัดการและการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศของ องค์กรอย่างจริงจัง เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการดำเนินงานขององค์กรให้เกิดประโยชน์สูงสุด และเพื่อลดโอกาสที่จะเกิดความเสียหายที่อาจเกิดขึ้น โดยการบริหารจัดการและการควบคุม ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการดำเนินงาน

โดยทุกองค์กรธุรกิจต้องการให้ตนเองมีความสามารถในการแข่งขันหรือต้องการได้เปรียบต่อการแข่งในกลุ่มอุตสาหกรรมในตลาด จึงควรเตรียมขบวนการทำงานด้านหลักธรรมาภิบาลทางไอทีให้ครบทุกด้านตามลำดับความสำคัญตามมุมมองขององค์กรและการควบคุมผลกระทบทางธุรกิจอันอาจจะเกิดขึ้น รวมทั้งการทบทวนขบวนการการทำงานเป็นระยะตามสภาพในปัจจุบันองค์ประกอบต่างๆ สามารถปรับตัวให้ทันกับความเปลี่ยนแปลงของเทคโนโลยีสารสนเทศในปัจจุบัน ซึ่งจะเป็นผลกระทบต่อองค์กรโดยตรงและผู้มีส่วนได้ส่วนเสีย ในกรณีองค์กรใดๆ ที่เป็นองค์กรที่จดทะเบียนอยู่ในตลาดหลักทรัพย์แห่งประเทศไทย ควรตระหนักให้มากเพราะการบริหารความเสี่ยงขององค์กรมีส่วนการตัดสินใจต่อผู้ลงทุนและความยั่งยืนขององค์กรในอนาคตต่อๆ ไป

สำหรับการประเมินการควบคุมด้านเทคโนโลยีสารสนเทศ ภาพรวมขององค์ประกอบที่สำคัญของการประเมินการควบคุมด้านเทคโนโลยีสารสนเทศ โดยเน้นถึงบทบาทและความรับผิดชอบของบุคลากรหลักขององค์กรที่สามารถผลักดันให้มีการกำกับดูแลทรัพยากรทางด้าน

เทคโนโลยีสารสนเทศ สำหรับเป็นแนวทางการดำเนินงานด้านความเสี่ยงและการควบคุมด้านเทคโนโลยีสารสนเทศ [17]

แม้ว่าเทคโนโลยีจะนำมาซึ่งโอกาสในการเจริญเติบโตและการพัฒนาขององค์กร แต่เทคโนโลยีก็อาจเป็นภัยคุกคาม (threats) ได้ด้วย เช่น การหยุดชะงักของระบบ การหลอกลวง การลักขโมยและการทุจริต เป็นต้น แม้จะมีงานวิจัยแสดงให้เห็นว่า ผู้โจมตีจากภายนอก (outside attackers) มักจะเป็นภัยคุกคามขององค์กร แต่บุคคลภายในองค์กรที่เป็นที่ไว้วางใจก็อาจเป็นภัยคุกคามที่อันตรายยิ่งกว่าได้ อย่างไรก็ตาม เทคโนโลยีสามารถใช้เพื่อป้องกันภัยคุกคามเหล่านี้ได้ ซึ่งผู้อ่านสามารถเรียนรู้ได้จากแนวทางฉบับนี้ ผู้บริหารควรถามคำถามที่ตรงประเด็นและเข้าใจความหมายของคำตอบต่างๆ ด้วย ตัวอย่างเช่น

ทำไมเราจึงควรมีความรู้ความเข้าใจเกี่ยวกับความเสี่ยงและการควบคุมด้านเทคโนโลยีสารสนเทศ

คำตอบคือ “การให้ความเชื่อมั่น” (assurance) และ “ความน่าเชื่อถือ” (reliablility) ผู้บริหารมีบทบาทสำคัญในการทำให้เกิดความเชื่อมั่นต่อความน่าเชื่อถือของข้อมูลสารสนเทศ (information reliability) ความเชื่อมั่นนี้ เริ่มต้นจากการมีกระบวนการควบคุมทางธุรกิจต่างๆ ที่มีผลเชื่อมโยงถึงกัน ประกอบกับหลักฐานที่แสดงให้เห็นว่า การควบคุมนั้นมีความต่อเนื่องและเพียงพอ ซึ่งผู้บริหารต้องพิจารณาให้น้ำหนักหลักฐานที่ได้จากการควบคุมและการตรวจสอบและสรุปว่าหลักฐานนั้นสามารถทำให้เกิดความเชื่อมั่นได้อย่างสมเหตุสมผลหรือไม่

อะไรบ้างที่ควรได้รับการปกป้อง

คำตอบคือ “ความไว้วางใจ” (trust) ทำให้ธุรกิจสามารถดำเนินไปได้และมีประสิทธิภาพ การควบคุมนำมาซึ่งพื้นฐานของความไว้วางใจแม้ว่าเราจะไม่สามารถมองเห็นได้ก็ตาม แต่เทคโนโลยีก็นำมาซึ่งพื้นฐานของการควบคุมทางธุรกิจแทบทุกประเภท ความน่าเชื่อถือของข้อมูลทางการเงินและกระบวนการที่เกี่ยวข้อง (ซึ่งปัจจุบัน หลายๆ องค์กรจัดทำเป็นข้อบังคับ) ทั้งหมดจะขึ้นอยู่กับความไว้วางใจ

ที่ใดบ้างที่สามารถประยุกต์ใช้การควบคุมด้านเทคโนโลยีสารสนเทศได้

คำตอบคือ “ใช้ได้ทุกที่” เทคโนโลยีสารสนเทศประกอบด้วย องค์ประกอบทางด้านเทคโนโลยี กระบวนการ บุคลากร โครงสร้างองค์กร และสถาปัตยกรรม (architecture) รวมทั้งสารสนเทศ การควบคุมด้านโครงสร้างพื้นฐานหลายประเภทเป็นการควบคุมทางเทคนิคและเทคโนโลยีสารสนเทศยังเป็นเครื่องมือที่ใช้ในการควบคุมทางธุรกิจในหลายๆ ด้าน

ใครคือผู้รับผิดชอบ

คำตอบคือ “ทุกคนในองค์กร” แต่ผู้บริหารต้องระบุและประกาศผู้ที่เป็นเจ้าของและมีหน้าที่รับผิดชอบการควบคุมนั้น มิฉะนั้นแล้วจะไม่มีใครรับผิดชอบอะไรเลยและส่งผลที่ค่อนข้างรุนแรง

เมื่อไรที่เราควรจะประเมินความเสี่ยงและการควบคุมด้านเทคโนโลยีสารสนเทศ

คำตอบคือ “ตลอดเวลา” เพราะเทคโนโลยีสารสนเทศเองก็เป็นสภาพแวดล้อมที่มีการเปลี่ยนแปลงอย่างรวดเร็วและเป็นตัวกระตุ้นให้เกิดการเปลี่ยนแปลงทางธุรกิจด้วย นอกจากนี้ยังมีความเสี่ยงใหม่ๆ เกิดขึ้นอย่างรวดเร็วดังนั้น การควบคุมต่างๆ จึงจำเป็นต้องมีหลักฐานที่แสดงให้เห็นถึงประสิทธิผลของการควบคุมที่มีอยู่อย่างต่อเนื่องและหลักฐานดังกล่าวจะต้องได้รับการประเมินและวัดผลอย่างสม่ำเสมอ

การควบคุมควรมีมากน้อยเพียงใดจึงจะเพียงพอ

คำตอบคือ “ฝ่ายบริหารจำเป็นต้องตัดสินใจ” โดยขึ้นอยู่กับความเสี่ยงที่องค์กรยอมรับได้ (risk appetite) ช่วงเบี่ยงเบนของความเสี่ยงที่องค์กรยอมรับได้ (risk tolerance) และกฎระเบียบข้อบังคับต่างๆ เนื่องจากการควบคุมไม่ใช่วัตถุประสงค์ขององค์กร แต่การควบคุมมีไว้เพื่อช่วยให้องค์กรบรรลุวัตถุประสงค์ทางธุรกิจ แม้ว่าการควบคุมจะเป็นต้นทุนในการดำเนินธุรกิจและอาจมีราคาแพง แต่ก็ไม่แพงเท่ากับผลกระทบที่อาจเกิดขึ้นจากการควบคุมที่ไม่เพียงพอ

การควบคุมด้านเทคโนโลยีสารสนเทศ เป็นสิ่งจำเป็นสำหรับการปกป้องสินทรัพย์ ลูกค้า พันธมิตรทางธุรกิจ และข้อมูลสารสนเทศที่อ่อนไหว (sensitive information) แสดงถึงความมั่นคงปลอดภัย ความมีประสิทธิภาพและพฤติกรรมที่มีจริยธรรม ช่วยปกป้องตราผลิตภัณฑ์ชื่อเสียง และความไว้วางใจต่อองค์กร ซึ่งสิ่งเหล่านี้อาจจะสูญเสียไปได้อย่างง่ายดายในตลาดการค้าระดับโลกและในสภาพแวดล้อมที่อยู่ภายใต้กฎข้อบังคับจากหน่วยงานต่างๆ เช่นในปัจจุบันหัวหน้าผู้บริหารงานตรวจสอบภายในสามารถใช้แนวทางฉบับนี้เป็นพื้นฐานในการประเมินกรอบและแนวปฏิบัติของการตรวจสอบภายในด้านความเสี่ยงและการควบคุมด้านเทคโนโลยีสารสนเทศ การปฏิบัติตามกฎระเบียบ และการให้ความเชื่อมั่นขององค์กร แนวทางฉบับนี้ยังสามารถใช้เพื่อตอบสนองต่อความท้าทายที่เกิดจากการเปลี่ยนแปลงอย่างต่อเนื่อง ความซับซ้อนที่เพิ่มขึ้น ภัยคุกคามที่เกิดขึ้นอย่างรวดเร็วและความจำเป็นในการปรับปรุงประสิทธิภาพ

การควบคุมด้านเทคโนโลยีสารสนเทศนำมาซึ่งความเชื่อมั่นในความน่าเชื่อถือของข้อมูลสารสนเทศและการให้บริการข้อมูลสารสนเทศ การควบคุมด้านเทคโนโลยีสารสนเทศสามารถช่วยลดความเสี่ยงที่เกิดจากการที่องค์กรนำเทคโนโลยีมาใช้ โดยเริ่มตั้งแต่การจัดทำนโยบายขององค์กรไปจนถึงการนำไปใช้งานจริง โดยการทำงานที่เขียนไว้ในรหัสคำสั่ง (coded instructions)

ตั้งแต่การป้องกันการเข้าถึงทางกายภาพจนถึงความสามารถในการติดตามการทำรายการและข้อมูลรายการธุรกรรมเพื่อหาผู้รับผิดชอบและการตรวจแก้แบบอัตโนมัติ (automatic edits) จนถึงการวิเคราะห์ความสมเหตุสมผลของข้อมูลขนาดใหญ่ๆ

แนวคิดด้านการควบคุมที่สำคัญ 2 ประการ ได้แก่

ความเชื่อมั่น จะเกิดขึ้นได้จากการมีการควบคุมด้านเทคโนโลยีสารสนเทศที่มีการทำงานอยู่ภายใต้ระบบการควบคุมภายใน ซึ่งความเชื่อมั่นนี้ต้องมีอยู่อย่างต่อเนื่อง และมีร่องรอยของหลักฐานที่เชื่อถือได้และเป็นไปโดยต่อเนื่อง

การให้ความเชื่อมั่นโดยผู้ตรวจสอบภายใน เป็นการประเมินความเชื่อมั่นอย่างเที่ยงธรรมและเป็นอิสระว่า การควบคุมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศปฏิบัติงานตามที่ได้กำหนดไว้ ความเชื่อมั่นนี้มาจากการที่ผู้ตรวจสอบทำความเข้าใจ ตรวจทาน และประเมินการควบคุมหลักที่ใช้จัดการกับความเสี่ยงที่เกี่ยวข้องตลอดจนดำเนินการทดสอบอย่างเพียงพอ เพื่อให้มั่นใจว่าการควบคุมได้รับการออกแบบอย่างเหมาะสม สามารถทำหน้าที่ในการควบคุมได้อย่างมีประสิทธิผลและต่อเนื่อง

กรอบต่างๆ จัดทำขึ้นเพื่อใช้ในการจัดประเภทของการควบคุมด้านเทคโนโลยีสารสนเทศและวัตถุประสงค์ของการควบคุม ซึ่งแนวทางฉบับนี้ได้แนะนำให้แต่ละองค์กรเลือกองค์ประกอบของกรอบที่เหมาะสมไปใช้ เพื่อจัดประเภทและประเมินความเสี่ยงและการควบคุมด้านเทคโนโลยีสารสนเทศ

1.6 กรอบงานโคบิต 5.0 (COBIT5.0 Framework)

สารสนเทศเป็นทรัพยากรหลักสำหรับทุกองค์กร และเทคโนโลยีมีบทบาทอย่างเป็นนัยสำคัญตั้งแต่ได้จัดทำขึ้นจนถึงเวลาที่ทำลายทิ้งเทคโนโลยีสารสนเทศก้าวหน้าขึ้นเรื่อยๆ และใช้กันอย่างแพร่หลายในองค์กรตลอดจนในสภาพแวดล้อมทางสังคม สาธารณะและธุรกิจ

ด้วยเหตุนี้ในปัจจุบันจึงยิ่งทำให้องค์กรและผู้บริหารระดับสูงต่างๆ ต้องเรียกร้องให้มี

- การดูแลรักษาสารสนเทศให้ได้คุณภาพสูงเพื่อใช้สนับสนุนการตัดสินใจ
- สร้างคุณค่าทางธุรกิจจากการลงทุนโดยมีไอทีเป็นปัจจัยเอื้อได้แก่การใช้งานไอทีอย่างประสิทธิผลและสร้างสรรค์
- บรรลุเป้าหมายทางกลยุทธและก่อให้เกิดประโยชน์ทางธุรกิจ
- บรรลุการปฏิบัติงานที่เป็นเลิศผ่านการใช้งานเทคโนโลยีที่เชื่อถือได้และมีประสิทธิผล
- ดูแลความเสี่ยงที่เกี่ยวกับไอทีให้อยู่ในระดับที่ยอมรับได้

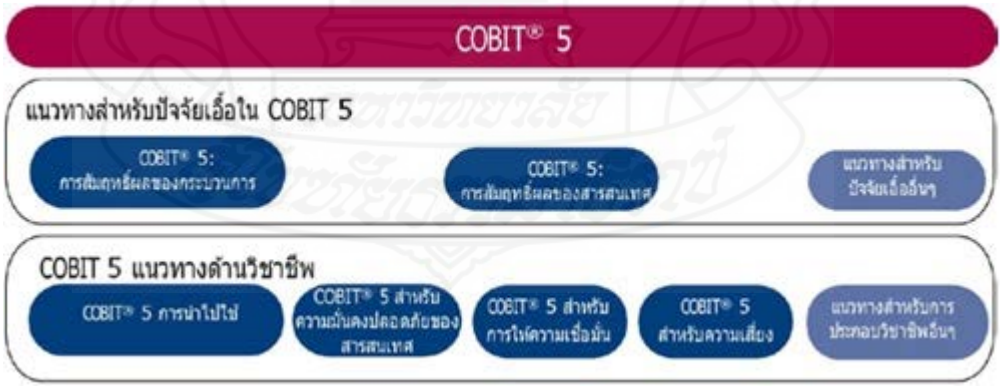
- ดูแลต้นทุนของการให้บริการทางไอทีและต้นทุนทางเทคโนโลยีให้เกิดประโยชน์สูงสุด
- ปฏิบัติตามกฎหมายกฎระเบียบข้อบังคับ ข้อตกลงตามสัญญาและนโยบายที่เกี่ยวข้อง

ในทศวรรษที่ผ่านมา คำว่าการกำกับดูแล (Governance) ได้กลายมาเป็นความคิดของธุรกิจในระดับแนวหน้าที่แสดงให้เห็นถึงความสำคัญของการกำกับดูแลที่ดีและในทางกลับกันก็สะท้อนให้เห็นถึงความล้มเหลวของธุรกิจอันเกิดจากการละเลยการกำกับดูแล

องค์กรที่ประสบความสำเร็จได้ตระหนักดีว่าคณะกรรมการบริหารและผู้บริหารระดับสูงจำเป็นต้องยอมรับการนำไอทีมาใช้เสมือนกับส่วนอื่นๆ ที่มีนัยสำคัญในการดำเนินธุรกิจ ในการดำเนินธุรกิจคณะกรรมการบริหารและผู้บริหาร ทั้งหน้าที่งานทางด้านธุรกิจและไอที จึงต้องร่วมมือ และทำงานร่วมกันเพื่อให้ไอทีได้รวมอยู่ในวิธีปฏิบัติด้านการกำกับดูแลและการบริหารจัดการ นอกจากนี้ ยังมีการออกกฎหมายใหม่ๆ และกฎข้อบังคับที่นำมาใช้เพิ่มขึ้นอย่างต่อเนื่องเพื่อจัดการกับความจำเป็นต่อการกำกับดูแลที่ดี

1.6.1 กรอบการดำเนินงานสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร[15]

เอกสาร COBIT 5 บรรจุเนื้อหาที่เป็นกรอบการดำเนินงานของ COBIT 5 ที่ใช้สำหรับการกับดูแลและการบริหารจัดการไอทีระดับองค์กร เอกสารฉบับนี้เป็นหนึ่งในชุดผลิตภัณฑ์ของ COBIT 5 ดังที่แสดงไว้ในรูปภาพที่ 2.2



ภาพที่ 2.2 สภาพแวดล้อมที่เป็นความร่วมมือกันทางออนไลน์

COBIT 5 ให้กรอบการดำเนินงานที่ครอบคลุมเพื่อช่วยให้องค์กรบรรลุวัตถุประสงค์ในเรื่องการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร กล่าวง่ายๆ ก็คือช่วยองค์กรสร้างคุณค่าที่เกิดประโยชน์สูงสุดจากไอที โดยการรักษาความสมดุลระหว่างประโยชน์ที่จะได้รับกับระดับความเสี่ยงและการใช้ทรัพยากรที่ทำให้เกิดประโยชน์สูงสุด COBIT 5 เอื้อให้ไอทีได้รับการกำกับดูแลและบริหารจัดการในแบบองค์รวมสำหรับทั่วทั้งองค์กร โดยครอบคลุมหน้าที่งานตามความรับผิดชอบทั้งทางด้านธุรกิจและไอทีอย่างครบวงจร พิจารณาถึงผลประโยชน์ที่เกี่ยวข้องกับไอทีของผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก COBIT 5 สามารถใช้ได้ทั่วไปและใช้ประโยชน์ได้สำหรับองค์กรทุกขนาดไม่ว่าจะเป็นองค์กรการค้าองค์กรที่ไม่แสวงหากำไรหรือในภาคเอกชน

ภาพที่ 2.3 หลักการของ COBIT 5

ในการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรตามหลัก COBIT 5

หลักการที่ 1: ตอบสนองความต้องการของผู้มีส่วนได้ส่วนเสียองค์กรตั้งอยู่เพื่อที่สร้างคุณค่าสำหรับผู้มีส่วนได้ส่วนเสียโดยการรักษาความสมดุลระหว่างผลประโยชน์ที่จะได้รับกับความเสี่ยงและการใช้ทรัพยากรที่ทำให้เกิดประโยชน์สูงสุด COBIT 5 ให้กระบวนการที่จำเป็นทั้งหมดและปัจจัยเอื้ออื่นๆ ที่ใช้สนับสนุนการสร้างคุณค่าแก่ธุรกิจจากการใช้ไอที เพราะว่าทุกองค์กรมีวัตถุประสงค์ที่แตกต่างกันองค์กรสามารถปรับแต่ง COBIT 5 ให้เหมาะกับบริบทของตนผ่านทางการส่งทอดเป้าหมาย (goal cascade) การแปลงเป้าหมายองค์กรในภาพรวมไปสู่เป้าหมายใน

ระดับที่สามารถบริหารจัดการได้มีความเฉพาะเจาะจงมีความเกี่ยวข้องกับไอทีและการเชื่อมโยงหรือเทียบเป้าหมายนี้กับกระบวนการ

หลักการที่ 2: ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจรCOBIT 5 บูรณาการการกำกับดูแลไอทีระดับองค์กรเข้าไปในการกำกับดูแลองค์กร

ครอบคลุมทุกหน้าที่งานและกระบวนการภายในองค์กร COBIT 5 ไม่เน้นเพียงแค่หน้าที่งานด้านไอทีเท่านั้นแต่จะถือว่าสารสนเทศและเทคโนโลยีที่เกี่ยวข้องเป็นสินทรัพย์ที่ทุกคนในองค์กรจำเป็นต้องดูแลเช่นเดียวกับสินทรัพย์อื่นๆ

พิจารณาการกำกับดูแลและการบริหารจัดการปัจจัยเอื้อที่เกี่ยวข้องกับไอทีทั้งหมดเพื่อให้ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจรได้แก่การรวมทุกคนและทุกสิ่งทั้งภายในและภายนอกที่เกี่ยวข้องกับการกำกับดูแลและการบริหารจัดการสารสนเทศและไอทีที่เกี่ยวข้อง

หลักการที่ 3: ประยุกต์ใช้กรอบการดำเนินงานที่บูรณาการเป็นหนึ่งเดียวมีมาตรฐานและแนวปฏิบัติที่ดีที่เกี่ยวข้องกับไอทีจำนวนมาก ซึ่งแต่ละอย่างก็ให้แนวทางเกี่ยวกับกิจกรรมของไอทีในด้านใดด้านหนึ่ง COBIT 5 ได้นำมาตรฐานและกรอบการดำเนินงานที่เกี่ยวข้องอื่นๆ มาจัดให้สอดคล้องกันในภาพรวมจึงสามารถใช้เป็นกรอบการดำเนินงานที่ครอบอยู่เหนือกรอบการดำเนินงานอื่นๆ สำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

หลักการที่ 4: เอื้อให้วิธีปฏิบัติแบบองค์รวมสัมฤทธิ์ผล การกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรที่มีประสิทธิภาพและประสิทธิผลต้องใช้วิธีปฏิบัติแบบองค์รวมที่ได้พิจารณาถึงองค์ประกอบหลายๆ อย่างซึ่งมีปฏิสัมพันธ์ต่อกัน COBIT 5 ระบุถึงกลุ่มของปัจจัยเอื้อที่ใช้สนับสนุนการนำระบบการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรไปใช้งานอย่างครอบคลุมปัจจัยเอื้อนิยามได้อย่างกว้างๆ ว่าเป็นสิ่งที่สามารถช่วยในการบรรลุวัตถุประสงค์ขององค์กรกรอบการดำเนินงานของ COBIT 5 ระบุถึงปัจจัยเอื้อ 7 ประเภทดังนี้หลักการนโยบายและกรอบการดำเนินงาน

– กระบวนการ

– โครงสร้างการจัดองค์กร

– วัฒนธรรมจริยธรรม และพฤติกรรม

– สารสนเทศ

– บริการโครงสร้างพื้นฐานและระบบงาน

– บุคลากรทักษะและศักยภาพ

หลักการที่ 5: แบ่งแยกการกำกับดูแลออกจากการบริหารจัดการ กรอบการดำเนินงานของ COBIT 5 ระบุความแตกต่างอย่างชัดเจนระหว่างการกำกับดูแลและการบริหาร

จัดการหลักสองประการนี้ครอบคลุมถึงกิจกรรมที่ต่างกันต้องการโครงสร้างการจัดองค์กรที่แตกต่างกันและใช้เพื่อจุดประสงค์ที่แตกต่างกันในมุมมองของ COBIT 5 ความแตกต่างหลักๆ ที่เห็นเด่นชัดระหว่างการกำกับดูแลและการบริหารจัดการคือ

– การกำกับดูแล (Governance) ในองค์กรส่วนใหญ่คณะกรรมการบริหารเป็นผู้รับผิดชอบการกำกับดูแลโดยรวมภายใต้การชี้นำของประธานกรรมการในองค์กรขนาดใหญ่และมีความซับซ้อน หน้าที่บางประการสำหรับการกำกับดูแลอาจมอบหมายให้กับหน่วยงานที่จัดตั้งขึ้นเป็นพิเศษในระดับที่เหมาะสม

– การบริหารจัดการ (Management) ในองค์กรส่วนใหญ่การบริหารจัดการรับผิดชอบโดยผู้บริหารระดับสูงภายใต้การชี้นำของประธานเจ้าหน้าที่บริหาร (CEO) เมื่อนำหลักการทั้ง 5 ประการนี้มารวมกันจะทำให้องค์กรสามารถสร้างกรอบการดำเนินงานสำหรับการกำกับดูแลและการบริหารจัดการที่มีประสิทธิผลซึ่งส่งผลให้การใช้สารสนเทศและการลงทุนด้านเทคโนโลยีเกิดประโยชน์สูงสุดเพื่อเป็นประโยชน์ให้กับผู้มีส่วนได้ส่วนเสีย

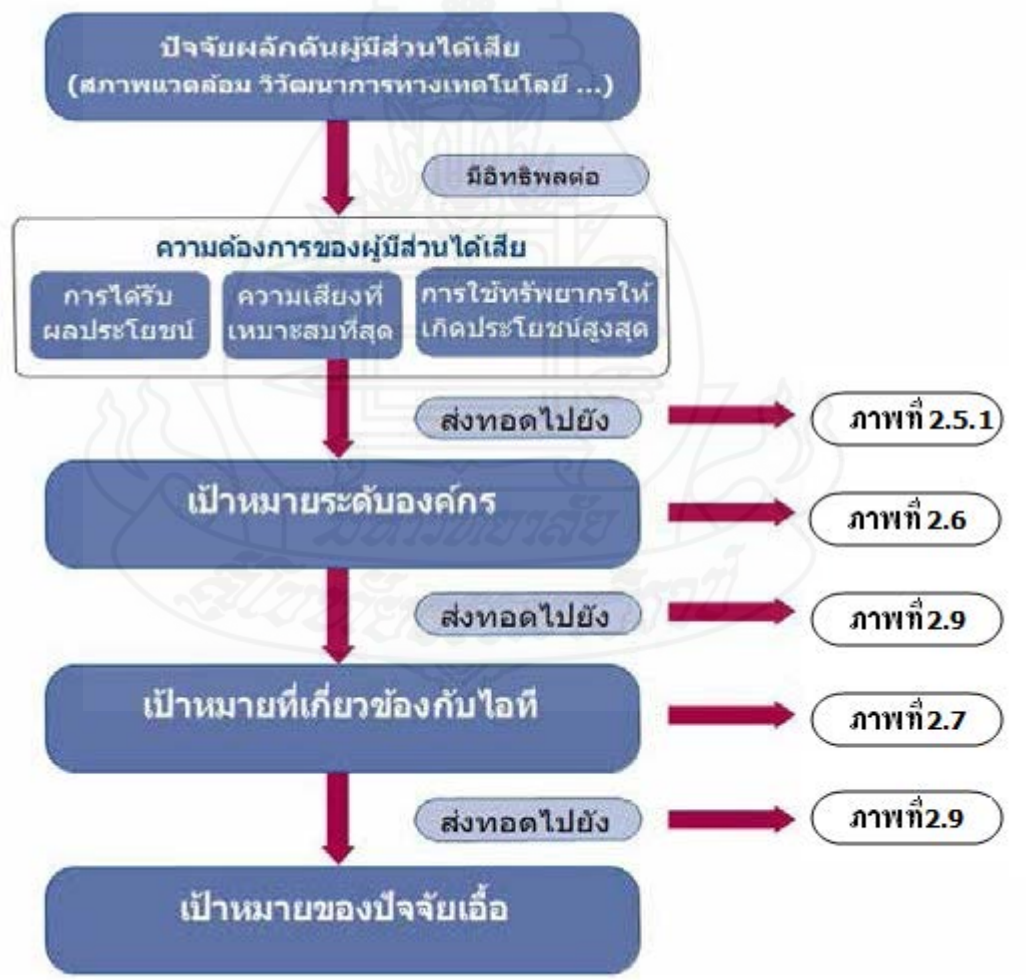
ว่าจะเป็นองค์กรการค้าหรือไม่แสวงหาผลกำไรก็จะต้องมีการสร้างคุณค่าเป็นหนึ่งในวัตถุประสงค์ของการกำกับดูแล การสร้างคุณค่าหมายถึงการได้รับผลประโยชน์ด้วยต้นทุนทรัพยากรที่ให้ประโยชน์สูงสุด และความเสี่ยงที่เหมาะสมที่สุด (ภาพที่ 2.4) ผลประโยชน์สามารถรับรู้ได้หลายรูปแบบยกตัวอย่างเช่นด้านการเงินสำหรับองค์กรที่แสวงหาผลกำไร หรือการบริการสาธารณะสำหรับหน่วยงานภาครัฐ

ภาพที่ 2.4 วัตถุประสงค์ในการกำกับดูและการสร้างคุณค่า

องค์กรมีผู้มีส่วนได้ส่วนเสียหลายคนและคำว่า “สร้างคุณค่า” ก็มีความหมายที่แตกต่างกันไปและบางครั้งก็ขัดแย้งกันการกำกับดูแลจึงเป็นการเจรจาต่อรองและตัดสินใจท่ามกลางความแตกต่างในผลประโยชน์ที่ของผู้มีส่วนได้เสียทั้งหลาย ด้วยเหตุนี้ระบบการกำกับดูแลจึงควรพิจารณาถึงผู้มีส่วนได้เสียทั้งหมดเมื่อจะตัดสินใจในการประเมินผลประโยชน์ความเสี่ยงและทรัพยากร คำถามที่ควรถามในการตัดสินใจแต่ละครั้งคือใครเป็นผู้ได้รับประโยชน์ใครเป็นผู้รับความเสี่ยง และต้องใช้ทรัพยากรอะไรบ้าง

1.6.2 การส่งทอดเป้าหมายและต้นแบบของกระบวนการของ COBIT5

ทุกองค์กรดำเนินงานภายใต้บริบทที่ต่างกันซึ่งบริบทนี้กำหนดโดยทั้งปัจจัยภายนอก (ด้านการตลาด ประเภทธุรกิจภูมิศาสตร์การเมือง และอื่นๆ) และปัจจัยภายใน (วัฒนธรรมการจัดองค์กร การยอมรับความเสี่ยง และอื่นๆ) และจำเป็นต้องมีระบบการกำกับดูแลและการบริหารจัดการที่ปรับแต่งให้เหมาะสมเฉพาะสำหรับองค์กรดังที่แสดงไว้ในรูปภาพที่ 2.5



ภาพที่ 2.5 ภาพรวมของการส่งทอดเป้าหมายใน COBIT 5

1) ปัจจัยผลักดันผู้มีส่วนได้ส่วนเสีย

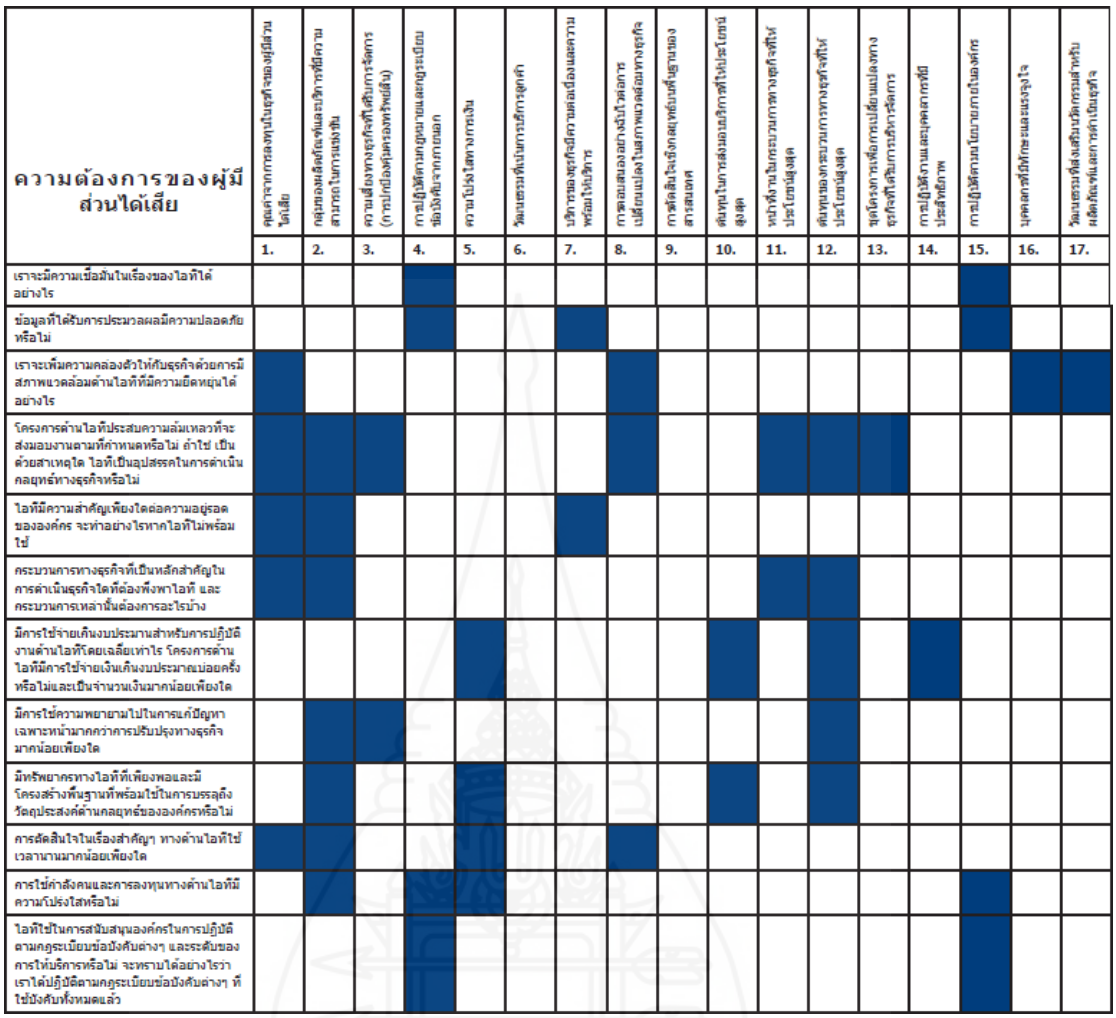
มีอิทธิผลต่อความต้องการของผู้มีส่วนได้ส่วนเสียได้รับอิทธิพลจากปัจจัยผลักดันหลายอย่างยกตัวอย่างเช่นการการเปลี่ยนแปลงกลยุทธ์การเปลี่ยนแปลงสภาพแวดล้อมทางธุรกิจและกฎระเบียบในการควบคุมและเทคโนโลยีใหม่ๆ

2) เป้าหมายระดับองค์กร

ความตอ้งการของผู้มีส่วนได้ส่วนเสียสามารถเชื่อมโยงไปถึงเป้าหมายทั่วไปในระดับองค์กร (Generic enterprise goal) เป้าหมายระดับองค์กรเหล่านี้กำหนดขึ้นโดยใช้มิติต่างๆ ของการวัดผลแบบสมดลุ (BSC)1 และเป็นการแสดงรายการเป้าหมายที่มักใช้กันโดยทั่วไปซึ่งองค์กรสามารถนำมากำหนดใช้เป็นของตนได้ถึงแม้ว่าเป้าหมายต่างๆ ที่มีอยู่ในรายการนี้จะไม่ใช้เป้าหมายทั้งหมดแต่เป้าหมายเฉพาะขององค์กร โดยส่วนใหญ่ก็สามารถเทียบได้ง่ายกับเป้าหมายทั่วไปในระดับองค์กรนี้ตารางแสดงความสัมพันธ์ระหว่างความต้องการของผู้มีส่วนได้ส่วนเสียกับเป้าหมายระดับองค์กรแสดงไว้ในรูปภาพที่ 2.6

ความต้องการของผู้มีส่วนได้เสีย	คุณค่าจากการลงทุนในธุรกิจของผู้มีส่วนได้เสีย	กลุ่มของผลิตภัณฑ์และทักษะที่มีความสามารถในการแข่งขัน	ความสี่ยงทางธุรกิจที่สัมพันธ์กับการจัดการ (การปกป้องทรัพย์สินครอบคลุมทั้งสิ้น)	การปฏิบัติตามกฎระเบียบและกฎหมายภายนอก	ความโปร่งใสทางการเงิน	วัฒนธรรมที่เป็นมืออาชีพและจริยธรรม	บริการของธุรกิจมีความต่อเนื่องและความพร้อมใช้งาน	การตอบสนองอย่างรวดเร็วต่อความเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ	การตัดสินใจเชิงกลยุทธ์บนพื้นฐานของสารสนเทศ	ต้นทุนในการส่งมอบบริการที่ได้ประโยชน์สูงสุด	หน้าที่งานในกระบวนการทางธุรกิจที่ได้ประโยชน์สูงสุด	ต้นทุนของกระบวนการทางธุรกิจที่ได้ประโยชน์สูงสุด	ชุดโครงการเพื่อการเปลี่ยนแปลงทางธุรกิจที่สัมพันธ์กับการบริหารจัดการ	การปฏิบัติงานและบุคลากรที่มีประสิทธิภาพ	การปฏิบัติตามนโยบายภายในองค์กร	บุคลากรที่มีทักษะและแรงจูงใจ	วัฒนธรรมที่สนับสนุนการจัดการความเสี่ยงที่เหมาะสมและการตัดสินใจเชิงธุรกิจ
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
เราจะได้รับคุณค่าจากการใช้ไอทีได้อย่างไร ผู้ใช้งานมีความพอใจกับคุณภาพของบริการด้านไอทีหรือไม่	■	■				■	■						■			■	■
เราจะจัดการกับประสิทธิภาพด้านไอทีได้อย่างไร		■			■				■	■	■	■		■			
เราจะนำเทคโนโลยีใหม่ๆ มาใช้ให้ดีที่สุดเพื่อเปิดช่องทางกลยุทธ์ได้อย่างไร	■	■						■					■			■	■
เราจะจัดตั้งและจัดโครงสร้างหน่วยงานด้านไอทีให้ดีที่สุดได้อย่างไร								■		■	■	■		■	■	■	
เราต้องพึ่งพาผู้ให้บริการภายนอกมากน้อยเพียงใด มีการจัดการกับสัญญาบริการด้านไอทีกับบุคคลภายนอกได้ดีเพียงใด เราจะเชื่อมั่นในผู้ให้บริการภายนอกได้อย่างไร			■	■						■							
มีข้อกำหนด (ด้านการควบคุม) อะไรบ้างเกี่ยวกับสารสนเทศ				■					■						■		
เราได้ระบุถึงความเสี่ยงที่เกี่ยวข้องทั้งหมดแล้ว หรือยัง			■				■		■						■		
เรามีการดำเนินงานด้านไอทีที่มีประสิทธิภาพและด้านทานภัยต่างๆ ได้หรือไม่					■		■										
เราจะควบคุมต้นทุนด้านไอทีได้อย่างไร เราจะใช้ทรัพยากรด้านไอทีให้มีประสิทธิภาพและประสิทธิผลได้อย่างไร ทางเลือกใดที่มีประสิทธิภาพและประสิทธิผลมากที่สุดในการจ้างหน่วยงานภายนอก										■		■		■			
เรามีบุคลากรที่เพียงพอสำหรับงานด้านไอทีหรือไม่ เราจะพัฒนาและรักษาทักษะของบุคลากรได้อย่างไร และจะจัดการประสิทธิภาพในการทำงานได้อย่างไร										■		■		■			

ภาพที่ 2.6 ความสมัพันธ์ระหว่างเป้าหมายระดับองค์กรของ COBIT 5 กับคำถามของผู้บริหาร



ภาพที่ 2.6 ความสมัพันธ์ระหว่างเป้าหมายระดับองค์กรของ COBIT 5 กับคำถามของผู้บริหาร (ต่อ)

ภาพที่ 2.6 นี้สามารถช่วยกำหนดและจัดลำดับความสำคัญให้กับเป้าหมายระดับองค์กรหรือเป้าหมายที่เกี่ยวข้องกับไอทีบนพื้นฐานของความต้องการของผู้มีส่วนได้ส่วนเสียการใช้ตารางนี้มีข้อควรระวังเช่นเดียวกับการใช้ตารางการส่งทอดเป้าหมายอื่นๆ กล่าวคือแต่ละองค์กรมีสภาพแวดล้อมที่แตกต่างกันและตารางนี้ไม่ควรได้รับนำมาใช้แบบตรงๆโดยไม่คำนึงถึงปัจจัยอื่นๆ แต่ควรใช้เป็นเพียงแนวทางที่จะมองหาความสัมพันธ์แบบกว้างๆ เท่านั้นในรูปภาพที่ 2.6 ช่องที่ตัดกันระหว่างความต้องการของผู้มีส่วนได้เสียกับเป้าหมายระดับองค์กรจะมีข้อมูลหากความต้องการเหล่านั้นควรได้รับการพิจารณาสำหรับเป้าหมายข้อนั้นๆ

COBIT 5 กำหนดเป้าหมายทั่วไปไว้ 17 ข้อดังที่แสดงไวในรูปภาพที่ 2.6 ซึ่งประกอบด้วย

• มิติของการวัดผลแบบสมดุล (BSC) ที่เหมาะสมกับเป้าหมายระดับองค์กร

• เป้าหมายระดับองค์กร

• ความสัมพันธ์กับวัตถุประสงค์หลักของการกำกับดูแล 3 ประการคือการได้รับผลประโยชน์ความเสี่ยงในระดับที่เหมาะสมและการใช้ทรัพยากรให้เกิดประโยชน์สูงสุด (P หมายถึง ความสัมพันธ์หลัก และ S หมายถึง ความสัมพันธ์รอง หรือมีความสัมพันธ์กันน้อย)

มิติการวัดผลแบบสมดุล	เป้าหมายระดับองค์กร	ความเชื่อมโยงกับวัตถุประสงค์ในการกำกับดูแล		
		การได้รับผลประโยชน์	ความเสี่ยงที่เหมาะสม	ทรัพยากรที่ให้ประโยชน์สูงสุด
ด้านการเงิน	1. คุณค่าจากการลงทุนในธุรกิจของผู้มีส่วนได้เสีย	P		S
	2. กลุ่ม (Portfolio)ของผลิตภัณฑ์และบริการที่มีความสามารถในการแข่งขัน	P	P	S
	3. ความเสี่ยงทางธุรกิจที่ได้รับการจัดการ (การปกป้องคุ้มครองสินทรัพย์)		P	S
	4. การปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับจากภายนอก		P	
	5. ความโปร่งใสทางการเงิน	P	S	S
ด้านลูกค้า	6. วัฒนธรรมที่เน้นการบริการลูกค้า	P		S
	7. บริการของธุรกิจมีความต่อเนื่องและความพร้อมให้บริการ		P	
	8. การตอบสนองอย่างฉับไวต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ	P		S
	9. การตัดสินใจเชิงกลยุทธ์บนพื้นฐานของสารสนเทศ	P	P	P
	10. ต้นทุนในการส่งมอบบริการที่ให้ประโยชน์สูงสุด	P		P
ด้านกระบวนการภายใน	11. หน้าที่งานในกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	P		P
	12. ต้นทุนของกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	P		P
	13. ชุดโครงการเพื่อการเปลี่ยนแปลงทางธุรกิจที่ได้รับการบริหารจัดการ	P	P	S
	14. การปฏิบัติงานและบุคคลากรที่มีประสิทธิภาพ	P		P
	15. การปฏิบัติตามนโยบายภายในองค์กร		P	
ด้านการเรียนรู้และเติบโต	16. บุคคลากรที่มีทักษะและแรงจูงใจ	S	P	P
	17. วัฒนธรรมที่ส่งเสริมนวัตกรรมสำหรับผลิตภัณฑ์และการดำเนินธุรกิจ	P		

ภาพที่ 2.7 เป้าหมายระดับองค์กรของ COBIT 5

3) เป้าหมายที่เกี่ยวข้องกับไอที

การบรรลุซึ่งเป้าหมายระดับองค์กรจำเป็นต้องมีผลลัพธ์ที่เกี่ยวข้องกับไอทีจำนวนหนึ่งซึ่งได้แก่เป้าหมายที่เกี่ยวข้องกับไอทีนั่นเอง คำว่าเกี่ยวข้องกับไอทีหมายถึงสารสนเทศและเทคโนโลยีที่เกี่ยวข้อง และเป้าหมายที่เกี่ยวข้องกับไอทีนี้ได้กำหนดขึ้นตามมิติของการวัดผลแบบสมดุลด้านไอที (IT BSC) COBIT 5 ได้กำหนดเป้าหมายที่เกี่ยวข้องกับไอทีไว้ 17 ข้อ ตามรูปภาพที่ 2.8

มิติการวัดผลแบบสมดุลด้านไอที	เป้าหมายของสารสนเทศและเทคโนโลยีที่เกี่ยวข้อง	
ด้านการเงิน	01	กลยุทธ์ด้านไอทีสอดคล้องไปในแนวทางเดียวกันกับกลยุทธ์ด้านธุรกิจ
	02	ไอทีเอื้ออำนวยและสนับสนุนให้ธุรกิจสามารถปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับของหน่วยงานภายนอก
	03	ผู้บริหารระดับสูงให้ความมั่นในการตัดสินใจต่างๆ ที่เกี่ยวข้องกับไอที
	04	ความเสี่ยงของธุรกิจที่เกี่ยวข้องกับไอทีสามารถบริหารจัดการได้
	05	ประโยชน์ที่ได้รับจริงจากกลุ่มของการลงทุนและการให้บริการในด้านต่างๆ ที่มีไอทีเป็นปัจจัยเอื้อ
	06	ต้นทุน ประโยชน์ และความเสี่ยงทางด้านไอทีมีความโปร่งใส
ด้านลูกค้า	07	การส่งมอบบริการด้านไอทีเป็นไปตามความต้องการของธุรกิจ
	08	การใช้ระบบงาน สารสนเทศและเทคโนโลยีอย่างเหมาะสม
ด้านกระบวนการภายใน	09	ความคล่องตัวทางด้านไอที
	10	ความมั่นคงปลอดภัยของสารสนเทศ โครงสร้างพื้นฐานในการประมวลผล และระบบงาน
	11	การใช้สินทรัพย์ ทรัพยากร และสมรรถนะทางด้านไอทีให้ได้ประโยชน์สูงสุด
	12	การเอื้ออำนวยและสนับสนุนการทำงานของกระบวนการทางธุรกิจโดยบูรณาการระบบงานและเทคโนโลยีเข้าไปใช้ในกระบวนการทางธุรกิจ
	13	การส่งมอบชุดโครงการต่างๆ ก่อให้เกิดประโยชน์ ตรงเวลา ตามงบประมาณที่ตั้งไว้ และตามความต้องการและมาตรฐานด้านคุณภาพ
	14	ความพร้อมใช้ของสารสนเทศที่เชื่อถือได้ และมีประโยชน์ในการตัดสินใจ
	15	ไอทีที่ปฏิบัติตามนโยบายภายในขององค์กร
ด้านการเรียนรู้และเติบโต	16	บุคลากรทั้งทางด้านไอทีและด้านธุรกิจที่มีความสามารถและมีแรงจูงใจ
	17	ความรู้ ความเชี่ยวชาญ และการริเริ่มดำเนินการเพื่อนวัตกรรมทางธุรกิจ

ภาพที่ 2.8 เป้าหมายเกี่ยวข้องกับไอที COBIT 5

ตารางแสดงความสัมพันธ์ระหว่างเป้าหมายที่เกี่ยวข้องกับไอทีกับเป้าหมายระดับองค์กรได้แสดงไว้ในรูปภาพที่ 2.8 และยังแสดงให้เห็นด้วยว่าเป้าหมายระดับองค์กรแต่ละข้อสนับสนุนด้วยเป้าหมายที่เกี่ยวข้องกับไอทีข้อใดบ้าง

จุดประสงค์ของตารางแสดงความสัมพันธ์ในรูปภาพที่ 2.8 คือการแสดงให้เห็นว่าเป้าหมายระดับองค์กรได้รับการสนับสนุนจาก (หรือการแปลงไปสู่) เป้าหมายที่เกี่ยวข้องกับไอทีได้อย่างไรด้วยเหตุนี้ตารางนี้จึงประกอบด้วยข้อมูลต่อไปนี้

• ในแต่ละสดมภ์ (แนวตั้ง) ระบุถึงเป้าหมายทั่วไปในระดับองค์กรทั้งหมด 17 ข้อใน COBIT 5 และจัดเป็นกลุ่มตามมิติของการวัดผลแบบสมดุล (BSC)

• ในแต่ละแถว (แนวนอน) ระบุถึงเป้าหมายที่เกี่ยวข้องกับไอทีทั้งหมด 17 ข้อและจัดเป็นกลุ่มตามมิติของการการวัดผลแบบสมดุล (BSC) ทางด้านไอที เช่นกัน

• การแสดงความสัมพันธ์ว่าเป้าหมายในระดับองค์กรแต่ละข้อได้รับการสนับสนุนจากเป้าหมายที่เกี่ยวข้องกับไอทีอย่างไร โดยแสดงเป็นระดับของความสัมพันธ์ดังต่อไปนี้

-“P” หมายความว่าเป็นความสัมพันธ์ในระดับหลักใช้เมื่อความสัมพันธ์มีความสำคัญได้แก่เป้าหมายที่เกี่ยวข้องกับไอทีเป็นปัจจัยหลักที่สนับสนุนให้บรรลุเป้าหมายระดับองค์กรในข้อนั้นๆ

- “S” หมายความว่าเป็นความสัมพันธ์ในระดับรอง ใช้เมื่อความสัมพันธ์ชัดเจนแต่มีความสำคัญน้อยกว่าได้แก่เป้าหมายที่เกี่ยวข้องกับไอทีเป็นปัจจัยในระดับรองที่จะสนับสนุนให้บรรลุเป้าหมายระดับองค์กรในข้อนั้นๆ

		เป้าหมายที่เกี่ยวข้องกับไอที	เป้าหมายระดับองค์กร																
			1. คุณค่าจากการลงทุนในธุรกิจของผู้มีส่วนได้เสีย	2. พอร์ตของผลิตภัณฑ์และบริการที่มีความสามารถในการแข่งขัน	3. ความเสี่ยงทางธุรกิจที่เกี่ยวกับการจัดการ (การปกป้องที่อยู่ครอบครองทรัพย์สิน)	4. การปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้องจากภายนอก	5. ความโปร่งใสทางการเงิน	6. วัฒนธรรมที่ม่งการบริการลูกค้า	7. บริการของผู้ให้บริการที่ตอบสนองความพร้อมในทางปฏิบัติ	8. การตอบสนองอย่างรวดเร็วต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ	9. การตัดสินใจเชิงกลยุทธ์บนพื้นฐานของสารสนเทศ	10. ความรับผิดของการดำเนินการที่มีประโยชน์สูงสุด	11. หน้าที่งานในกระบวนการทางธุรกิจที่มีประโยชน์สูงสุด	12. ต้นทุนของกระบวนการทางธุรกิจที่ใช้ประโยชน์สูงสุด	13. โปรแกรมเพื่อการเปลี่ยนแปลงทางธุรกิจที่เหมาะสมการบริหารจัดการ	14. การปฏิบัติงานและบุคลากรที่มีประสิทธิภาพ	15. การปฏิบัติตามกฎหมายในองค์กร	16. บุคลากรที่มีทักษะและแรงจูงใจ	17. วัฒนธรรมองค์กรส่งเสริมนวัตกรรมสำหรับผลิตภัณฑ์และการดำเนินธุรกิจ
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
			ด้านการเงิน					ด้านลูกค้า					ด้านกระบวนการภายใน					ด้านการเรียนรู้และเติบโต	
ด้านการเงิน	01	กลยุทธ์ด้านไอทีสอดคล้องไปในแนวทางเดียวกันกับกลยุทธ์ด้านธุรกิจ	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	ไอทีเอื้ออำนวยและสนับสนุนให้ธุรกิจสามารถปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับของหน่วยงานภายนอก			S	P											P		
	03	ผู้บริหารระดับสูงให้คำมั่นในการตัดสินใจต่างๆ ที่เกี่ยวข้องกับไอที	P	S	S					S	S		S		P			S	S
	04	ความเสี่ยงของธุรกิจที่เกี่ยวข้องกับไอทีสามารถบริหารจัดการได้			P	S			P	S		P			S		S	S	
	05	ประโยชน์ที่ได้รับจริงจากกลุ่มของการลงทุนและการให้บริการในด้านต่างๆ ที่มีไอทีเป็นปัจจัยเอื้อ	P	P				S		S		S	S	P		S			S
	06	ต้นทุน ประโยชน์และความเสี่ยงทางด้านไอทีมีความโปร่งใส	S		S		P				S	P		P					
ด้านลูกค้า	07	การส่งมอบบริการด้านไอทีเป็นไปตามความต้องการของธุรกิจ	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	การใช้ระบบงาน สารสนเทศและเทคโนโลยีอย่างเหมาะสม	S	S	S			S	S		S	S	P	S		P		S	S
ด้านกระบวนการภายใน	09	ความคล่องตัวทางด้านไอที	S	P	S			S		P			P		S	S		S	P
	10	ความมั่นคงปลอดภัยของสารสนเทศ โครงสร้างพื้นฐานในการประมวลผล และระบบงาน			P	P			P								P		
	11	การใช้สินทรัพย์ ทรัพยากร และสมรรถนะทางด้านไอทีให้ได้ประโยชน์สูงสุด	P	S						S		P	S	P	S	S			S
	12	การเอื้ออำนวยและสนับสนุนการทำงานของกระบวนการทางธุรกิจโดยบูรณาการระบบงานและเทคโนโลยีเข้าไปใช้ในกระบวนการทางธุรกิจ	S	P	S			S		S		S	P	S	S	S			S
	13	การส่งมอบชุดโครงการต่างๆ ก่อให้เกิดประโยชน์ ตรงเวลา ตามงบประมาณที่ตั้งไว้ และตามความต้องการและมาตรฐานด้านคุณภาพ	P	S	S			S				S		S	P				
	14	ความพร้อมใช้ของสารสนเทศที่เชื่อถือได้ และมีประโยชน์ในการตัดสินใจ	S	S	S	S			P		P		S						
	15	ไอทีที่ปฏิบัติตามนโยบายภายในขององค์กร			S	S											P		
ด้านการเรียนรู้และเติบโต	16	บุคลากรทั้งทางด้านไอทีและด้านธุรกิจที่มีความสามารถและมีแรงจูงใจ	S	S	P			S		S						P		P	S
	17	ความรู้ ความเชี่ยวชาญ และการริเริ่มดำเนินการเพื่อนวัตกรรมทางธุรกิจ	S	P				S		P	S		S		S			S	P

ภาพที่ 2.9 ความสัมพันธ์ระหว่างเป้าหมายระดับองค์กรใน COBIT 5 กับเป้าหมายที่เกี่ยวข้องกับไอที

4) เป้าหมายของปัจจัยเอื้อ

การบรรลุเป้าหมายเกี่ยวข้องกับไอทีจำเป็นต้องมีระบบงานที่ทำงานได้ดีและใช้ปัจจัยเอื้อจำนวนหนึ่งแนวคิดของปัจจัยเอื้อได้อธิบายรายละเอียดไว้ในบทที่ 5 ปัจจัยเอื้อรวมถึงกระบวนการ โครงสร้างการจัดองค์กรและสารสนเทศและได้มีการกำหนดเป้าหมายสำหรับปัจจัยเอื้อแต่ละประเภทที่จะสนับสนุนเป้าหมายที่เกี่ยวข้องกับไอที

กระบวนการเป็นหนึ่งในปัจจัยเอื้อในรูปภาพที่ 2.9 ได้แสดงความสัมพันธ์ระหว่างเป้าหมายที่เกี่ยวข้องกับไอทีและกับกระบวนการของ COBIT 5 ที่เกี่ยวข้องซึ่งรวมถึงเป้าหมายของกระบวนการเหล่านั้นด้วย

รูปภาพที่ 2.10 ประกอบด้วย

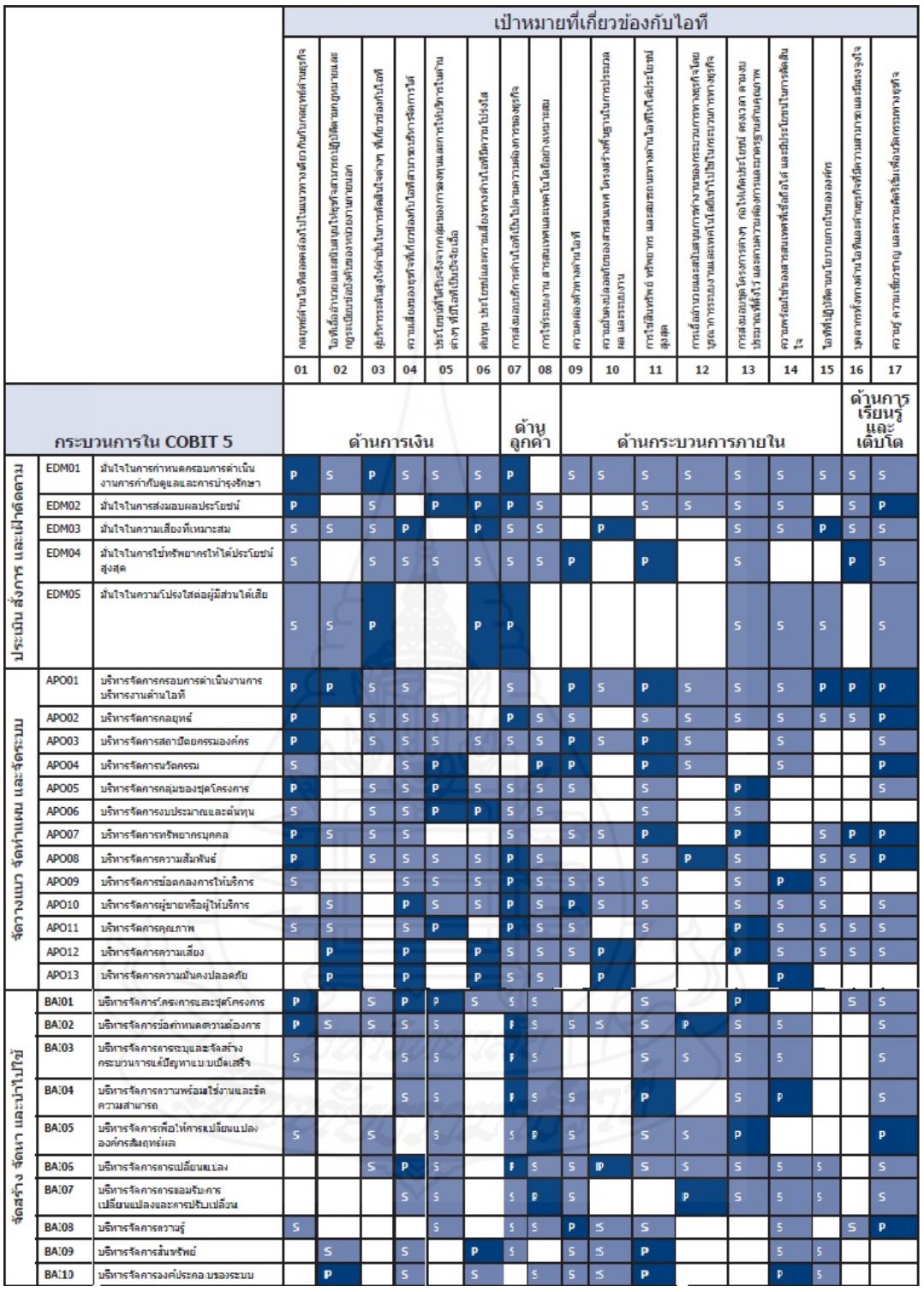
• ในแต่ละสดมภ์ (แนวตั้ง) แสดงถึงเป้าหมายทั่วไปที่เกี่ยวข้องกับไอทีทั้งหมด 17 ข้อตามที่ระบุไว้และจัดเป็นกลุ่มตามมิติของการวัดผลแบบสมดุล (BSC)

• ในแต่ละแถว (แนวนอน) แสดงถึงกระบวนการใน COBIT 5 ทั้งหมด 37 กระบวนการ และจัดเป็นกลุ่มตามโดเมน

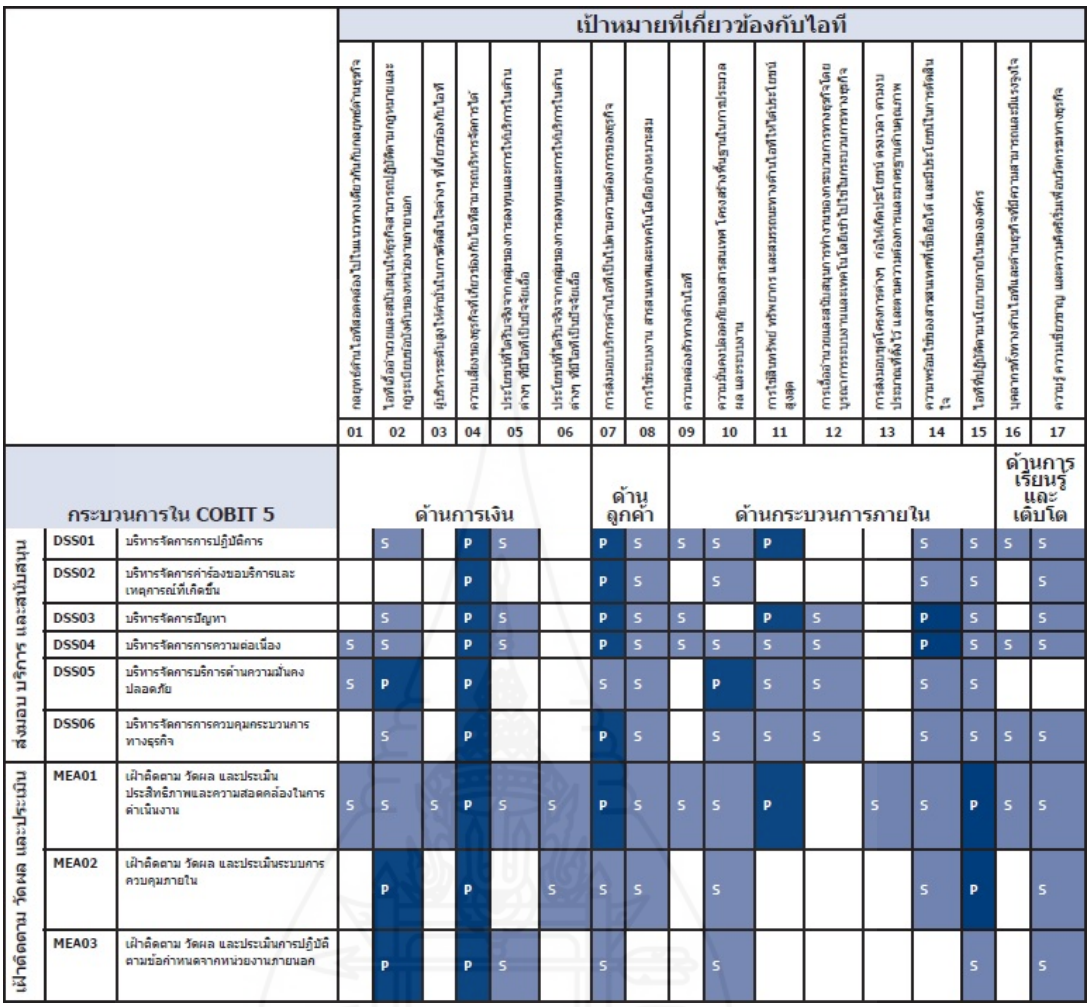
• การแสดงให้เห็นว่าเป้าหมายที่เกี่ยวข้องกับไอทีแต่ละข้อได้รับการสนับสนุนจากกระบวนการที่เกี่ยวข้องกับไอทีของ COBIT 5 อย่างไร โดยแสดงเป็นระดับของความสัมพันธ์ดังต่อไปนี้

- “P” หมายความว่าเป็นความสัมพันธ์ในระดับหลักใช้เมื่อความสัมพันธ์มีความสำคัญได้แก่กระบวนการของ COBIT 5 เป็นปัจจัยสนับสนุนหลักที่จะช่วยให้บรรลุเป้าหมายเกี่ยวข้องกับไอที

- “S” หมายความว่าเป็นความสัมพันธ์ในระดับรอง ใช้เมื่อความสัมพันธ์ชัดเจนแต่มีความสำคัญน้อยกว่าได้แก่กระบวนการของ COBIT 5 เป็นปัจจัยสนับสนุนในระดับรองที่จะช่วยให้บรรลุเป้าหมายเกี่ยวข้องกับไอที



ภาพที่ 2.10 ความสัมพันธ์ระหว่างเป้าหมายที่เกี่ยวข้องกับไอทีกับกระบวนการต่างๆ ใน COBIT 5

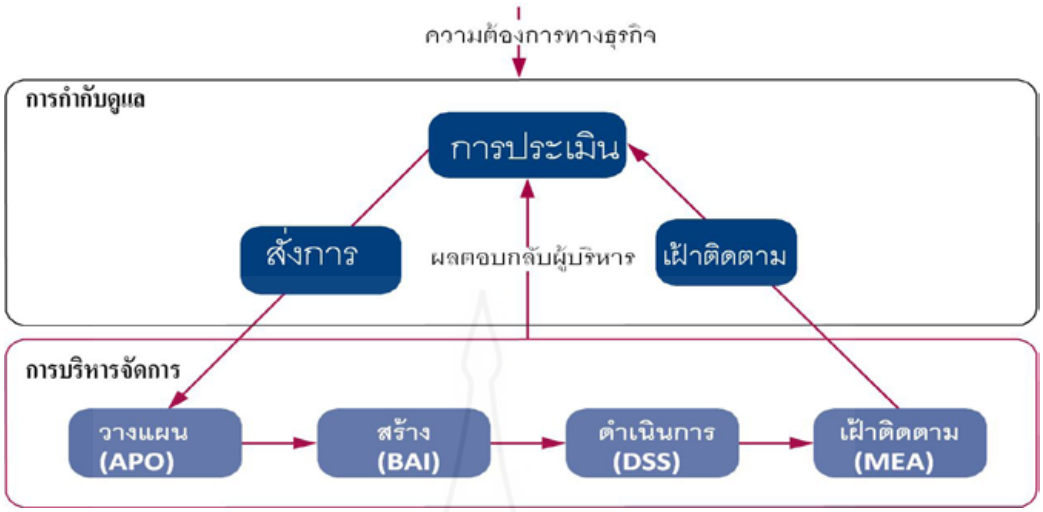


กระบวนการใน COBIT 5			เป้าหมายที่เกี่ยวข้องกับไอที																	
			01 กลยุทธ์ด้านไอทีสอดคล้องไปในแนวทางเดียวกันกับกลยุทธ์ด้านธุรกิจ	02 ไอทีได้ผ่านการและสนับสนุนให้ธุรกิจสามารถปฏิบัติตามกฎหมายและกฎระเบียบต่างๆที่เกี่ยวข้องกับการดำเนินงาน	03 ผู้บริหารระดับสูงได้ร่วมในการตัดสินใจต่างๆ ที่เกี่ยวข้องกับไอที	04 ความเสี่ยงของธุรกิจที่เกี่ยวข้องกับไอทีสามารถบริหารจัดการได้	05 ประโยชน์ที่ได้รับจากการลงทุนและการให้บริการในด้านต่างๆ ที่มีไอทีเป็นตัวขับเคลื่อน	06 ประโยชน์ที่ได้รับจากการลงทุนและการให้บริการในด้านต่างๆ ที่มีไอทีเป็นตัวขับเคลื่อน	07 การส่งมอบบริการด้านไอทีเป็นไปตามความต้องการของธุรกิจ	08 การใช้ระบบงาน สารสนเทศและเทคโนโลยีอย่างเหมาะสม	09 ความน่าเชื่อถือทางด้านไอที	10 ความปลอดภัยของสารสนเทศ โครงสร้างพื้นฐานในการประมวลผล และระบบงาน	11 การให้คำแนะนำ ทรัพยากร และสมรรถนะทางด้านไอทีให้ได้ประโยชน์สูงสุด	12 การเชื่อมโยงและสนับสนุนการทำงานของกระบวนการทางธุรกิจโดยรูปแบบการบวนและเทคโนโลยีสารสนเทศ	13 การส่งมอบโครงการต่างๆ ที่ให้ผลประโยชน์ ตรงเวลา งบประมาณ ประมาณที่ตั้งไว้ และตามความต้องการและข้อกำหนดคุณภาพ	14 ความพร้อมใช้ของสารสนเทศที่เชื่อถือได้ และมีประโยชน์ในการตัดสินใจ	15 ไอทีที่ปฏิบัติตามกฎหมายในขององค์กร	16 บุคลากรทั้งทางด้านไอทีและด้านธุรกิจมีความสามารถและเชี่ยวชาญ	17 ความรู้ ความเข้าใจ และความคิดริเริ่มสร้างสรรค์ของธุรกิจ
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
				ด้านการเงิน					ด้านลูกค้า		ด้านกระบวนการภายใน							ด้านการเรียนรู้และเติบโต	
สั่งมอบ บริการ และสนับสนุน	DSS01	บริหารจัดการการปฏิบัติการ		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	บริหารจัดการคำร้องขอบริการและเหตุการณ์ที่เกิดขึ้น				P			P	S		S				S	S		S
	DSS03	บริหารจัดการปัญหา		S		P	S		P	S	S		P	S		P	S		S
	DSS04	บริหารจัดการการความต่อเนื่อง	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	บริหารจัดการบริการด้านความมั่นคงปลอดภัย	S	P		P			S	S		P	S	S		S	S		
	DSS06	บริหารจัดการการควบคุมกระบวนการทางธุรกิจ		S		P			P	S		S	S	S		S	S	S	S
เฝ้าติดตาม วัดผล และประเมิน	MEA01	เฝ้าติดตาม วัดผล และประเมินประสิทธิภาพและความสอดคล้องในการดำเนินงาน	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	เฝ้าติดตาม วัดผล และประเมินระบบการควบคุมภายใน		P		P		S	S	S		S				S	P		S
	MEA03	เฝ้าติดตาม วัดผล และประเมินการปฏิบัติตามข้อกำหนดจากหน่วยงานภายนอก		P		P	S		S			S					S		S

ภาพที่ 2.10 ความสัมพันธ์ระหว่างเป้าหมายที่เกี่ยวข้องกับไอทีกับกระบวนการต่างๆ ใน COBIT 5 (ต่อ)

1.6.3 ต้นแบบของกระบวนการใน COBIT 5

COBIT 5 ไม่ได้เป็นกฎตายตัวแต่สนับสนุนให้องค์กรนำกระบวนการทางด้านการกำกับดูแลและการบริหารจัดการไปใช้งานให้ครอบคลุมถึงจุดต่างๆ ที่สำคัญตามที่แสดงไว้ในรูปภาพที่ 2.11



ภาพที่ 2.11 จุดสำคัญในการกำกับดูแลและการบริหารจัดการของ COBIT 5

สามารถจัดให้มีกระบวนการต่างๆ ที่เห็นว่าเหมาะสม ตราบใดที่ครอบคลุมถึงวัตถุประสงค์ที่จำเป็นสำหรับการกำกับดูแลและการบริหารจัดการทั้งนี้การบรรลุถึงวัตถุประสงค์เดียวกันองค์กรขนาดเล็กอาจใช้เพียงไม่กี่กระบวนการแต่ในองค์กรขนาดใหญ่และมีความซับซ้อนอาจจำเป็นต้องมีกระบวนการที่มากกว่า

COBIT 5 ประกอบด้วยต้นแบบอ้างอิงของกระบวนการที่ระบุและอธิบายถึงรายละเอียดของกระบวนการสำหรับการกำกับดูแลและการบริหารจัดการโดยแสดงถึงกระบวนการทั้งหมดซึ่งปกติมักจะพบได้ในองค์กรหนึ่งๆ ในส่วนที่เกี่ยวกับกิจกรรมทางไอที และให้ต้นแบบอ้างอิงที่สามารถใช้ร่วมกันได้ในลักษณะที่เข้าใจง่ายสำหรับผู้จัดการทั้งด้านปฏิบัติการไอทีและด้านธุรกิจ ต้นแบบของกระบวนการที่นำเสนอนี้เป็นต้นแบบที่มีความสมบูรณ์และครอบคลุม แต่ก็ไม่ได้เป็นต้นแบบของกระบวนการเพียงอันเดียวที่ใช้ได้ องค์กรแต่ละแห่งจะต้องกำหนดกลุ่มของกระบวนการของตนขึ้นมาใช้ให้เหมาะสมกับในแต่ละสถานการณ์

การผนวกรวมรูปแบบในการดำเนินธุรกิจ (Operational model) และการใช้ภาษาสามัญเข้าไปไว้ในทุกภาคส่วนในองค์กรที่มีส่วนร่วมในกิจกรรมทางด้านไอทีเป็นก้าวสำคัญและจำเป็นที่จะนำไปสู่การกำกับดูแลที่ดีโดยให้กรอบการดำเนินงานสำหรับการวัดผลและการเฝ้าติดตามประสิทธิภาพในการทำงานด้านไอทีการให้ความเชื่อมั่นทางด้านไอที การสื่อสารกับผู้ให้บริการ และการบูรณาการแนวปฏิบัติที่ดีด้านการบริหารจัดการ

ต้นแบบอ้างอิงของกระบวนการใน COBIT 5 แยกการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรออกเป็นสองส่วนที่สำคัญ

• การกำกับดูแลประกอบด้วยกระบวนการกำกับดูแล 5 กระบวนการ ในแต่ละกระบวนการได้มีการระบุแนวปฏิบัติสำหรับประเมิน (Evaluate) การสั่งการ (Direct) และการเฝ้าติดตาม (Monitor) (EDM)5 เอาไว้

• การบริหารจัดการ ประกอบด้วย 4 โดเมนที่สอดคล้องกับความรับผิดชอบในการวางแผน (Plan) สร้าง (Build) ดำเนินการ (Run) และเฝ้าติดตาม (Monitor) (PBRM) และครอบคลุมไอทีอย่างครบวงจร โดเมนเหล่านี้มีวิวัฒนาการมาจากโดเมนและโครงสร้างของกระบวนการใน COBIT 4.1 ชื่อของโดเมนได้ต้องให้สอดคล้องกับงานหลักที่เกี่ยวข้อง

ซึ่งไดมี้การเพิ่มคำกิริยาเข้าไปเป็นคำอธิบายเพิ่มเติมดังนี้

– จัดวางแนว (Align) จัดทำแผน (Plan) และจัดระบบ (Organise) (APO)

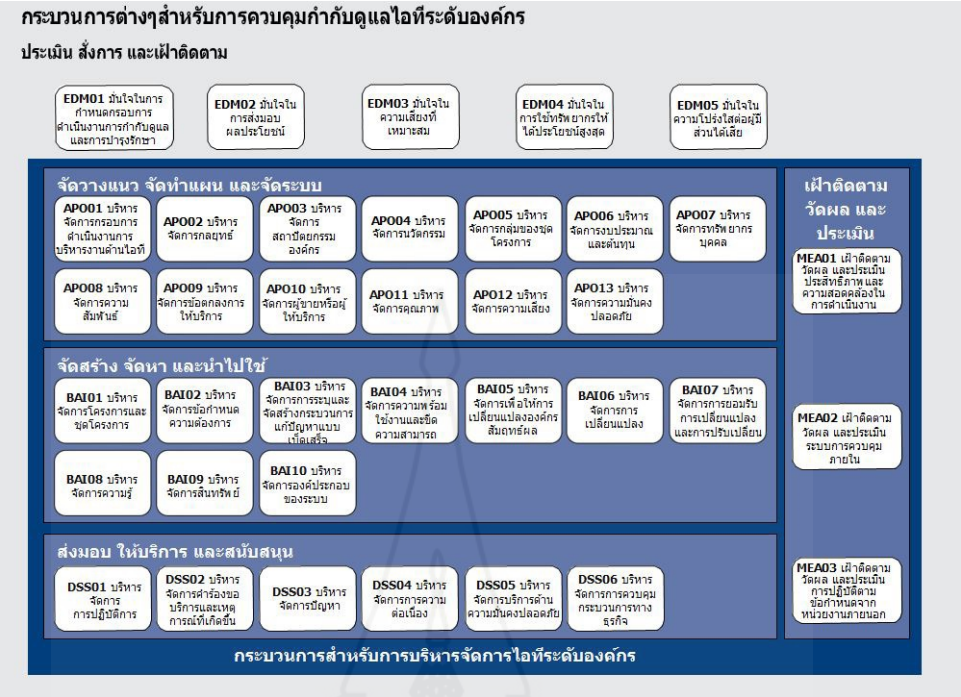
– จัดสร้าง (Build) จัดหา (Acquire) และนำไปใช้ (Implement) (BAI)

– ส่งมอบ (Deliver) ให้บริการ (Service) และสนับสนุน (Support) (DSS))

– เฝ้าติดตาม (Monitor) วัดผล (Evaluate) และประเมิน (Assess) (MEA)

แต่ละโดเมนประกอบด้วยกระบวนการต่างๆ ทั้งนี้ตามที่ได้อธิบายไปแล้วก่อนหน้านี้ แม้ว่ากระบวนการส่วนใหญ่ต่างก็มีกิจกรรมในการ ‘วางแผน’ ‘นำไปใช้’ ‘ปฏิบัติการ’ และ ‘เฝ้าติดตาม’ ภายในกระบวนการนั้นๆ หรือภายใต้ประเด็นปัญหาเฉพาะทางที่ได้รับการหยิบยกขึ้นมา (อาทิเช่นด้านคุณภาพ ด้านความมั่นคงปลอดภัยเป็นต้น) แต่กิจกรรมต่างๆ เหล่านั้นถูกจัดเข้าไปไว้ในแต่ละโดเมนตามความเกี่ยวเนื่องโดยส่วนใหญ่ของกิจกรรมในแต่ละด้าน ตามมุมมองของไอทีในระดับองค์กร

ต้นแบบอ้างอิงของกระบวนการใน COBIT 5 พัฒนาต่อจากต้นแบบของกระบวนการใน COBIT 4.1 และได้บูรณาการเอาต้นแบบกระบวนการใน Risk IT และ Val IT เข้าไปไว้ด้วย



ภาพที่ 2.12 ต้นแบบอ้างอิงของกระบวนการใน COBIT 5

1.7 โดเมนและกระบวนการโคบิต 5.0

1.7.1 ***โดเมน EDM*** (ประเมิน สั่งการ และเฝ้าติดตาม) ใน COBIT 5 โดยมีกระบวนการประกอบด้วย

EDM01 แนวปฏิบัติกระบวนการ การรับข้อมูลการส่งผลลัพธ์และกิจกรรม

EDM02 มั่นใจในการส่งมอบผลประโยชน์

EDM03 มั่นใจในความเสี่ยงที่เหมาะสม

EDM04 มั่นใจในการใช้ทรัพยากรให้ได้ประโยชน์สูงสุด

EDM05 มั่นใจในความโปร่งใสต่อผู้มีส่วนได้เสีย

1.7.2 ***โดเมน APO*** (จัดวางแนว จัดทำแผน และจัดระบบ) ใน COBIT 5 โดยมีกระบวนการประกอบด้วย

APO01 บริหารจัดการกรอบการดำเนินงานการบริหารงานด้านไอที

APO02 บริหารจัดการกลยุทธ์

APO03 บริหารจัดการสถาปัตยกรรมองค์กร

APO04 บริหารจัดการนวัตกรรม

APO05 บริหารจัดการกลุ่มของชุดโครงการ

APO06 บริหารจัดการงบประมาณและต้นทุน

APO07 บริหารจัดการทรัพยากรบุคคล

APO08 บริหารจัดการความสัมพันธ์

APO09 บริหารจัดการข้อตกลงการให้บริการ

APO10 บริหารจัดการผู้ขายหรือผู้ให้บริการ

APO11 บริหารจัดการคุณภาพ

APO12 บริหารจัดการความเสี่ยง

APO13 บริหารจัดการความมั่นคงปลอดภัย

1.7.3 โดเมน BAI (จัดสร้าง จัดหา และนำไปใช้) ใน COBIT 5 โดยมีกระบวนการประกอบด้วย

BAI01 บริหารจัดการ โครงการและชุดโครงการ

BAI02 บริหารจัดการข้อกำหนดความต้องการ

BAI03 บริหารจัดการการระบุและจัดสร้างกระบวนการแก้ปัญหาแบบเบ็ดเสร็จ

BAI04 บริหารจัดการความพร้อมใช้งานและขีดความสามารถ

BAI05 บริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล

BAI06 บริหารจัดการการเปลี่ยนแปลง

BAI07 บริหารจัดการการยอมรับการเปลี่ยนแปลงและการปรับเปลี่ยน

BAI08 บริหารจัดการความรู้

BAI09 บริหารจัดการสินทรัพย์

BAI10 บริหารจัดการองค์ประกอบของระบบ

1.7.4 โดเมน DSS (ส่งมอบ บริการ และสนับสนุน) ใน COBIT 5 โดยมีกระบวนการประกอบด้วย

DSS01 บริหารจัดการการปฏิบัติการ

DSS02 บริหารจัดการคำร้องขอบริการและเหตุการณ์ที่เกิดขึ้น

DSS03 บริหารจัดการปัญหา

DSS04 บริหารจัดการความต่อเนื่อง

DSS05 บริหารจัดการบริการด้านความมั่นคงปลอดภัย

DSS06 บริหารจัดการการควบคุมกระบวนการทางธุรกิจ

1.7.5 โดเมน MEA (เฝ้าติดตาม วัดผล และประเมิน) ใน COBIT 5 โดยมีกระบวนการประกอบด้วย

MEA01 เฝ้าติดตามวัดผลและประเมินประสิทธิภาพและความสอดคล้องในการดำเนินงาน

MEA02 เฝ้าติดตามวัดผล และประเมินระบบการควบคุมภายใน

MEA03 เฝ้าติดตามวัดผลและประเมินการปฏิบัติตามข้อกำหนดจากหน่วยงานภายนอก

1.8 บทบาทหน้าที่ผู้ตรวจสอบตามแนวการวิจัยการเตรียมความพร้อมของบริษัทที่จะเข้าตลาดหลักทรัพย์แห่งประเทศไทย

IPO ย่อมาจากคำว่า Initial Public Offering ซึ่งก็คือการเสนอขายหุ้นใหม่แก่ประชาชนทั่วไปเป็นครั้งแรก การจะมีหุ้นไอพีโอออกเสนอขายหรือไม่นั้นขึ้นอยู่กับว่า บริษัทมองหาแหล่งเงินทุน (ที่นอกเหนือจากเงินกู้) เพื่อขยายกิจการหรือไม่ ถ้าบริษัทต้องการเงินทุนและกระจายการถือครองหุ้นให้ประชาชนทั่วไป ก็สามารถนำหุ้นของตนออกเสนอขายได้ โดยจะต้องทำผ่านบริษัทหลักทรัพย์ที่รับเป็นผู้จัดจำหน่ายหลักทรัพย์ (underwriters) ซึ่งจะต้องได้รับความเห็นชอบจาก ก.ล.ต. และต้องจัดทำหนังสือชี้ชวนตามหลักเกณฑ์ที่ ก.ล.ต. กำหนดไว้

ผู้มีส่วนเกี่ยวข้อง

ภาพที่ 2.13 ผู้มีส่วนเกี่ยวข้อง

ตารางที่ 2.1 ผู้มีส่วนเกี่ยวข้อง

ผู้มีส่วนเกี่ยวข้อง	บทบาทหน้าที่
ก.ล.ต.	กำกับดูแลตลาดทุนในภาพรวม โดยเฉพาะพิจารณาคุณสมบัติบริษัท ที่จะมีการระดมทุนจากประชาชนทั่วไปในครั้งแรก (IPO)
ต.ล.ท.	ตลาดรองสำหรับซื้อขายหลักทรัพย์ให้ประชาชนทั่วไปและดูแลการซื้อขายให้เป็นไปอย่างคล่องตัวและยุติธรรม
ที่ปรึกษาทางการเงิน	เตรียมความพร้อมให้กับบริษัท ที่จะเข้า IPO โดยการศึกษาข้อมูลบริษัทตั้งแต่การดำเนินธุรกิจ โครงสร้างธุรกิจ การจัดโครงสร้างทุน ให้คำแนะนำและปรับปรุงระบบการบริหารจัดการเพื่อให้มีคุณสมบัติพร้อม ก่อนยื่น ก.ล.ต.และ ต.ล.ท.
ที่ปรึกษากฎหมาย	ให้คำแนะนำให้ความเห็นเกี่ยวกับข้อพิพาทต่างๆ ที่มีหรืออาจจะมีขึ้นและมีผลกระทบกับบริษัทการแปรสภาพเป็นบริษัทมหาชนและทำหน้าที่ร่วมกับที่ปรึกษาทางการเงินในการปรับปรุงข้อสัญญากฎและข้อบังคับบริษัทให้เป็นไปตามเกณฑ์ของก.ล.ต.และ ต.ล.ท.
ผู้สอบบัญชี	ตรวจสอบและรับรองงบการเงินให้เป็นไปตามมาตรฐานการบัญชีที่รับรองทั่วไปซึ่งต้องเป็นผู้สอบบัญชีที่ได้รับความเห็นชอบจากก.ล.ต.
กระทรวงพาณิชย์	ดูแลเรื่องการจดแจ้งและการเปลี่ยนแปลงที่สำคัญของนิติบุคคลในกรณีนี้ที่เกี่ยวข้องคือ การแปรสภาพจากบริษทัจำกัดเป็นบริษทัจำกัด (มหาชน)
ผู้จัดจำหน่ายหลักทรัพย์	เป็นผู้กระจายหุ้นบริษัทไปสู่ผู้ลงทุนอย่างกว้างขวาง และให้ความมั่นใจว่าจะสามารถจำหน่ายหุ้นให้แก่ผู้ลงทุนกลุ่มต่างๆ ในจำนวนและราคาที่เหมาะสม

ข้อควรพิจารณา

- มีการบริหารงานที่โปร่งใสไม่มีความขัดแย้งทางผลประโยชน์
- มีการกำหนดข้อบังคับบริษัทในการทำรายการระหว่างกัน
- งบการเงินมีความถูกต้องตามมาตรฐานการบัญชี
- มีระบบการควบคุมภายในที่มีประสิทธิภาพ

การควบคุม (นิยามตามมาตรฐานการปฏิบัติงานตรวจสอบภายใน)หมายถึง การกระทำใดๆ โดยฝ่ายบริหาร คณะกรรมการ และกลุ่มบุคคลอื่นๆ เพื่อบริหารความเสี่ยงและเพิ่มโอกาสให้

องค์กรบรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้โดยฝ่ายบริหารมีการวางแผน จัดองค์กรและอำนวยการดำเนินงานอย่างเพียงพอที่จะเกิดความเชื่อมั่นอย่างสมเหตุสมผลว่าองค์กรจะบรรลุวัตถุประสงค์และเป้าหมาย

กระบวนการควบคุม (นิยามตามมาตรฐานการปฏิบัติงานตรวจสอบภายใน) หมายถึง นโยบายวิธีการปฏิบัติงาน (ทั้งคู่มือการปฏิบัติงานและระบบอัตโนมัติ) และกิจกรรมต่างๆ ขององค์กรซึ่งเป็นส่วนหนึ่งของกรอบโครงสร้างการควบคุมที่ออกแบบมาเพื่อให้เกิดความเชื่อมั่นว่าความเสี่ยงถูกจำกัดให้อยู่ในระดับที่ยอมรับได้

หน่วยงานเทคโนโลยีสารสนเทศเป็นส่วนหนึ่งในหลายๆหน่วยงานที่ผู้สอบบัญชีที่ได้รับความเห็นชอบจากสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์แห่งประเทศไทย เข้าตรวจสอบการควบคุมภายในเพื่อการบริหารความเสี่ยงให้มีผลกระทบน้อยที่สุดหรือไม่มีเลย ในองค์กรที่เข้าตรวจสอบ โดยแต่ละหน่วยงานก็มีการตรวจสอบแตกต่างกันและส่วนของหน่วยงานเทคโนโลยีสารสนเทศ การเตรียมความพร้อมของหน่วยงานตรวจสอบภายใน

สำหรับบริษัทที่จะเข้าจดทะเบียนกับตลาดหลักทรัพยแห่งประเทศไทยมีแนวทางการตรวจสอบ 7 หัวข้อดังนี้

1.8.1 นโยบายและระเบียบการใช้งานคอมพิวเตอร์

1.8.2 การกำหนดสิทธิการเข้าถึงข้อมูลคอมพิวเตอร์

1.8.3 การจัดเก็บข้อมูลสำรองและการทดสอบความสมบูรณ์

1.8.4 สถานที่จัดเก็บคอมพิวเตอร์ Server และอุปกรณ์ป้องกันภัย

1.8.5 การจัดเก็บข้อมูลการใช้งานอินเทอร์เน็ต

1.8.6 ลิขสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์ต่างๆ

1.8.7 แผนรองรับเหตุสุดวิสัย

1.8.8 การใช้งานอีเมล์ และ เว็บไซต์ ของบริษัท

2. วรรณกรรมที่เกี่ยวข้อง

2.1 การนำไอทิลมาประยุกต์ใช้ในการบริหารจัดการระบบสารสนเทศของโรงพยาบาลศิครินทร์

จริยา ไข่มุกด์ (2554) สารนิพนธ์ หลักสูตรวิทยาศาสตร์มหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีมหานคร ได้ทำงานวิจัยเรื่อง การนำไอทิลมา

ประยุกต์ใช้ในการบริหารจัดการระบบสารสนเทศของโรงพยาบาลศิครินทร์ (ITIL Version 2 For Sikarin Hospital)

การวิจัยดังกล่าว มีวัตถุประสงค์ในการนำมาตรฐานไอทิล มาเป็นแนวทางในการบริหารจัดการระบบสารสนเทศของโรงพยาบาลศิครินทร์ เพื่อรองรับการให้บริการทางด้านระบบสารสนเทศให้มีประสิทธิภาพ และจัดการกับปัญหาที่เกิดขึ้นจากการให้บริการ จนนำมาสู่กระบวนการที่ชัดเจน มีบริการอย่างต่อเนื่อง และเกิดปัญหาในการใช้งานน้อยที่สุด โดยนำกระบวนการไอทิล 5 กระบวนการ มาใช้ในการบริหารจัดการระบบสารสนเทศ รวมทั้งพัฒนาโปรแกรมขึ้นมาช่วยในเรื่องการจัดเก็บข้อมูลต่างๆ

ในงานวิจัยนี้ ผู้วิจัยได้ใช้หลักธรรมาภิบาลไอที โดยได้เลือกกรอบมาไอทิลมาใช้เป็นแนวทางในการดำเนินการ ซึ่งตรงกับเป้าหมายขององค์การที่เน้นหลัก ทางด้านการให้บริการเป็นหลัก โดยผู้วิจัยได้ทำการพัฒนาโปรแกรมขึ้นมาโดยอ้างอิงหลักของกระบวนการไอทิล 5 กระบวนการ มาเป็นกรอบในการพัฒนาโปรแกรมซึ่งผลที่ได้ก็ช่วยให้ปรับปรุงการบริการขององค์การให้มีความรวดเร็วมากขึ้น ส่งผลต่อการปฏิบัติงานของแผนกที่เกี่ยวข้องดังนี้

1. มีแนวทางในการให้บริการที่ชัดเจนขึ้น

2. มีการจัดเก็บข้อมูลต่างๆ อยู่ในรูปฐานข้อมูล ซึ่งจากเดิมเป็นการจัดเก็บข้อมูลในรูปไฟล์เอ็กเซล หรือบันทึกในกระดาษ ซึ่งทาให้ลดความซ้ำซ้อนของการบันทึกข้อมูล และยังทำให้นำข้อมูลที่มีมาวิเคราะห์ ตรวจสอบได้

3. มีความสะดวก และรวดเร็ว ในการประเมินต่างๆ เช่นการเปลี่ยนเครื่องพีซียี่ห้อเอเซอร์ สามารถนำข้อมูลที่มีอยู่ มาใช้ เพื่อประเมินการสั่งซื้อเครื่องพีซีได้

นอกจากนี้ข้อมูลที่ได้มีการจัดเก็บไว้สามารถนำมาออกรายงานเพื่อสนับสนุนการทำงานของหน่วยงานต่างๆ ได้เป็นอย่างดีและนอกจากนี้สามารถนำมาวิเคราะห์เพื่อปรับปรุงการบริการให้ดีมากยิ่งขึ้น

แต่ในงานวิจัยนี้ ทางผู้วิจัย มิได้กล่าวถึง การประเมินผลการให้บริการ ว่าอยู่ในระดับไหน เป้าหมายที่ทางองค์การต้องการอยู่ในระดับใด ในงานวิจัยเน้นหลักในเรื่องการพัฒนาโปรแกรมและผลการนำไปใช้งานอย่างเดียว แต่ยังขาดการประเมินผลทางด้านการนำไปใช้งาน

2.2 การประเมินการบริหารโครงการสารสนเทศ โดยใช้หลักธรรมาภิบาลไอที: กรณีของบริษัท เมืองทองมหาชัย จำกัด

นายประสิทธิ์ ธีรวงศธร(2556) วิทยานิพนธ์ หลักสูตรวิทยาศาสตรมหาบัณฑิต แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิทยาศาสตร์และเทคโนโลยี

มหาวิทยาลัยสุโขทัยธรรมาธิราช ได้ทำงานวิจัยเรื่อง การประเมินการบริหารโครงการสารสนเทศโดยใช้หลักธรรมาภิบาลไอที: กรณีของบริษัท เมืองทองมหาชัย จำกัด

การวิจัย การประเมินการบริหารโครงการสารสนเทศโดยใช้หลักธรรมาภิบาลไอที มีวัตถุประสงค์เพื่อ (1) เพื่อนากรอบธรรมาภิบาลด้านไอทีมาใช้ในการบริหารโครงการสารสนเทศ กรณีของบริษัทเมืองทองมหาชัย จากัด (2) กำหนดตัวชี้วัดและประเมินโครงการสารสนเทศตามหลักธรรมาภิบาลไอที กรณีของบริษัทเมืองทองมหาชัยจากัด

การดำเนินการวิจัย ได้มีการศึกษา เกี่ยวกับ ธรรมาภิบาลไอที ขึ้นมาในองค์กร เพื่อสร้างความมั่นใจว่า การดำเนินงานทางด้านโครงการสารสนเทศ จะได้รับผลตอบแทนที่คุ้มค่า ลดความเสี่ยงที่จะเกิดขึ้น และ หลีกเลี่ยงความล้มเหลวของโครงการ โดยผู้วิจัยได้นำกรอบโคบิตเวอร์ชั่น 4.1 (Cobit4.1) ซึ่งเป็นกรอบที่ได้รับการยอมรับในการควบคุมกระบวนการด้านไอทีตามหลักธรรมาภิบาลไอที มาเป็นแนวทางในการบริหารโครงการ โดยงานวิจัยชิ้นนี้ได้ใช้โครงการจัดเก็บข้อมูลและกำหนดสิทธิการใช้งาน ของบริษัท เมืองทองมหาชัย จำกัด ที่เป็นโครงการเกี่ยวกับการแบ่งปันพื้นที่ การเก็บข้อมูลของส่วนกลาง ให้กับหน่วยงานในองค์กร เพื่อไว้สาหรับจัดเก็บข้อมูลที่มีความสำคัญ เครื่องมือที่ใช้ใน การวิจัยประกอบด้วย แบบจำลองวุฒิภาวะ ใช้ในการประเมิน กระบวนการบริหารโครงการ เพื่อให้ทราบว่า อยู่ในสถานะใด โดยในการจัดเก็บข้อมูล ผู้วิจัย ได้ดำเนินการโดยผ่าน ซอฟต์แวร์ Microsoft Project 2007 ที่ใช้ในการวางแผน และ รายงานผลความคืบหน้าของการดำเนินการโครงการ ระยะเวลาการเก็บรวบรมข้อมูลโครงการอยู่ ระหว่างวันที่ 01/09/2555 – 30/11/2555 โครงการวิจัยนี้มีการพัฒนาตัวชี้วัดเพื่อเป็นเครื่องมือในการประเมินโครงการสารสนเทศ โดยอาศัยหลักการและกรอบธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

ผลงานวิจัยพบว่า (1) ประสิทธิภาพของ โครงการจัดเก็บข้อมูลและกำหนดสิทธิการใช้งาน อยู่ในระดับที่ต่ำกว่ามาตรฐานโดยวิเคราะห์จากตัวชี้วัดดัชนีการดำเนินการด้านค่าใช้จ่าย (CPI) และ ดัชนีการดำเนินงานด้านเวลา (SPI)โดยมีสาเหตุมาจาก เจ้าหน้าที่ไอที ยังไม่มีความชำนาญทางด้าน ระบบ Linux Operating System อย่างเพียงพอ ทำให้มีการใช้เวลาในการทำงานมากกว่าแผนที่วางไว้ มาก (2) ประสิทธิผลของโครงการ จัดเก็บข้อมูลและกำหนดสิทธิการใช้งาน พบว่า องค์กรสามารถประหยัดค่าใช้จ่ายทางด้านซอฟต์แวร์มาก เนื่องจากเป็นการใช้ ซอฟต์แวร์ที่ไม่มีค่าลิขสิทธิ์และคุณสมบัติของซอฟต์แวร์สามารถตอบโจทย์การใช้งานในองค์กรได้ตามที่ต้องการ (3) การประเมินวุฒิภาวะของกระบวนการบริหารโครงการ พบว่า อยู่ในระดับ 3 คือ ระดับที่มีการวางแผนการทางาน มีการกำหนดผู้รับผิดชอบ ในแต่ละกระบวนการ แต่ยังไม่ได้ตามเป้าหมายที่องค์กรต้องการ ซึ่งได้กำหนดไว้ที่ระดับ 4 เป็นระดับที่มีการควบคุมและวัดผล ข้อเสนอแนะ คือ ควรเพิ่มทักษะของเจ้าหน้าที่ไอที ให้เพิ่มมากขึ้น และ ติดตาม ปรับปรุง การบริหาร

โครงการผ่านตัวชี้วัดดัชนีการดำเนินการด้านค่าใช้จ่าย (cost performance index:CPI) และ ดัชนีการดำเนินงานด้านเวลา (schedule performance index: SPI) ให้มากขึ้น

2.3 การพัฒนาแนวปฏิบัติและต้นแบบระบบการตรวจสอบการพัฒนาซอฟต์แวร์และควบคุมคุณภาพ ซอฟต์แวร์ตามแนวมาตรฐาน ISO/IEC 29110

นิตยา สิงไทยสงค์ (2557) สารนิพนธ์ หลักสูตรวิทยาศาสตรมหาบัณฑิต แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช ได้ทำงานวิจัยเรื่อง การพัฒนาแนวปฏิบัติและต้นแบบระบบการตรวจสอบการพัฒนาซอฟต์แวร์และควบคุมคุณภาพ ซอฟต์แวร์ตามแนวมาตรฐาน ISO/IEC 29110

ในการพัฒนาซอฟต์แวร์จำเป็นต้องมีกระบวนการติดตามและควบคุมคุณภาพของซอฟต์แวร์ ดังนั้นมาตรฐาน ISO/IEC 29110 จึงเป็นเครื่องมือที่สำคัญในการดำเนินโครงการพัฒนาซอฟต์แวร์เพื่อให้มีคุณภาพ ซึ่งโครงการนี้มีวัตถุประสงค์ดังกล่าว คือ (1) เพื่อพัฒนาแนวปฏิบัติที่ดีด้านการพัฒนาซอฟต์แวร์ในการตรวจสอบและควบคุมคุณภาพตามแนวมาตรฐาน ISO/IEC 29110 ระดับ Basic Profile สำหรับองค์กรพัฒนาซอฟต์แวร์ขนาดกลางและขนาดเล็กไม่เกิน 25 คน (2) เพื่อพัฒนาต้นแบบระบบการตรวจสอบและควบคุมคุณภาพการพัฒนาซอฟต์แวร์ตามแนวมาตรฐาน ISO/IEC 29110 ระดับ Basic Profile2.4

การดำเนินงานประกอบด้วย (1) ทำการศึกษาเกี่ยวกับระบบมาตรฐาน ISO/IEC 29110 สำหรับองค์กรพัฒนาซอฟต์แวร์ขนาดกลางและขนาดเล็กไม่เกิน 25 คน ระดับ Basic Profile (2) รวบรวมข้อมูลจากองค์กรผู้ให้บริการพัฒนาซอฟต์แวร์ที่ผ่านการรับรองมาตรฐาน ISO/IEC 29110 โดยการกำหนดคำถามและออกแบบแบบสอบถามไว้ล่วงหน้าเพื่อให้สามารถรวบรวมข้อมูลได้อย่างครบถ้วน (3) ดำเนินการวิเคราะห์ข้อมูลที่ได้รวบรวมไว้ (4) พัฒนาแนวปฏิบัติที่ดีด้านการตรวจสอบการพัฒนาซอฟต์แวร์และควบคุมคุณภาพซอฟต์แวร์ตามแนวมาตรฐาน ISO/IEC 29110 ระดับ Basic Profile และ (5) พัฒนาต้นแบบระบบการตรวจสอบการพัฒนาซอฟต์แวร์และควบคุมคุณภาพซอฟต์แวร์ตามแนวมาตรฐาน ISO/IEC 29110 ระดับ Basic Profile

ผลที่คาดว่าจะได้รับคือ ข้อมูลสรุปแนวปฏิบัติที่ดีด้านการตรวจสอบการพัฒนาซอฟต์แวร์และควบคุมคุณภาพซอฟต์แวร์ตามมาตรฐาน ISO/IEC 29110 เพื่อเป็นประโยชน์สำหรับองค์กรพัฒนาซอฟต์แวร์ขนาดกลางและขนาดเล็กไม่เกิน 25 คนหรือผู้ที่สนใจจะสามารถใช้เป็นแนวทางในการปรับปรุงกระบวนการดำเนินงานด้านการควบคุมคุณภาพการพัฒนาซอฟต์แวร์ตามมาตรฐาน ISO/IEC 29110 ได้อย่างสะดวก, รวดเร็ว, และมีประสิทธิภาพยิ่งขึ้น พร้อมทั้งสามารถนำข้อมูลต้นแบบระบบการตรวจสอบการพัฒนาซอฟต์แวร์และควบคุมคุณภาพซอฟต์แวร์ตามมาตรฐาน ISO/IEC 29110 ไปใช้ประกอบการพัฒนาเป็นระบบและพัฒนาคุณสมบัติของระบบต่อยอด

เพื่อใช้เป็นเครื่องมือประกอบการควบคุมคุณภาพซอฟต์แวร์ขององค์กรเพิ่มเติมในอนาคตได้ อีกทั้งเพื่อเป็นการตอบสนองนโยบายของทางสภาอุตสาหกรรมแห่งประเทศไทยในการยกระดับคุณภาพซอฟต์แวร์ของไทยสู่ระดับสากลอีกด้วย

บทที่ 3
การดำเนินการวิจัย

1. ขั้นตอนการดำเนินวิจัย

1.1 ศึกษากรอบโคบิต 5.0 ผู้วิจัยศึกษาธรรมาภิบาลตามกรอบโคบิตกรอบการศึกษามีโดเมนดังนี้

1.1.1 ประเมิน สั่งการ และเฝ้าติดตาม (EDM)

1.1.2 จัดวางแนว จัดทำแผน และจัดระบบ (APO)

1.1.3 จัดสร้าง จัดหา และนำไปใช้ (BAI)

1.1.4 ส่งมอบ บริการ และสนับสนุน (DSS)

1.1.5 เฝ้าติดตาม วัดผล และประเมิน (MEA)

1.2 วิเคราะห์กระบวนการการควบคุมภายในด้านเทคโนโลยีสารสนเทศของธุรกิจกลุ่มทรัพยากรจาก 3 แหล่งข้อมูลคือ

1.2.1 จากกรอบโคบิต 5.0

1.2.2 จากประสบการณ์ของผู้วิจัยในด้ายเทคโนโลยีสารสนเทศ

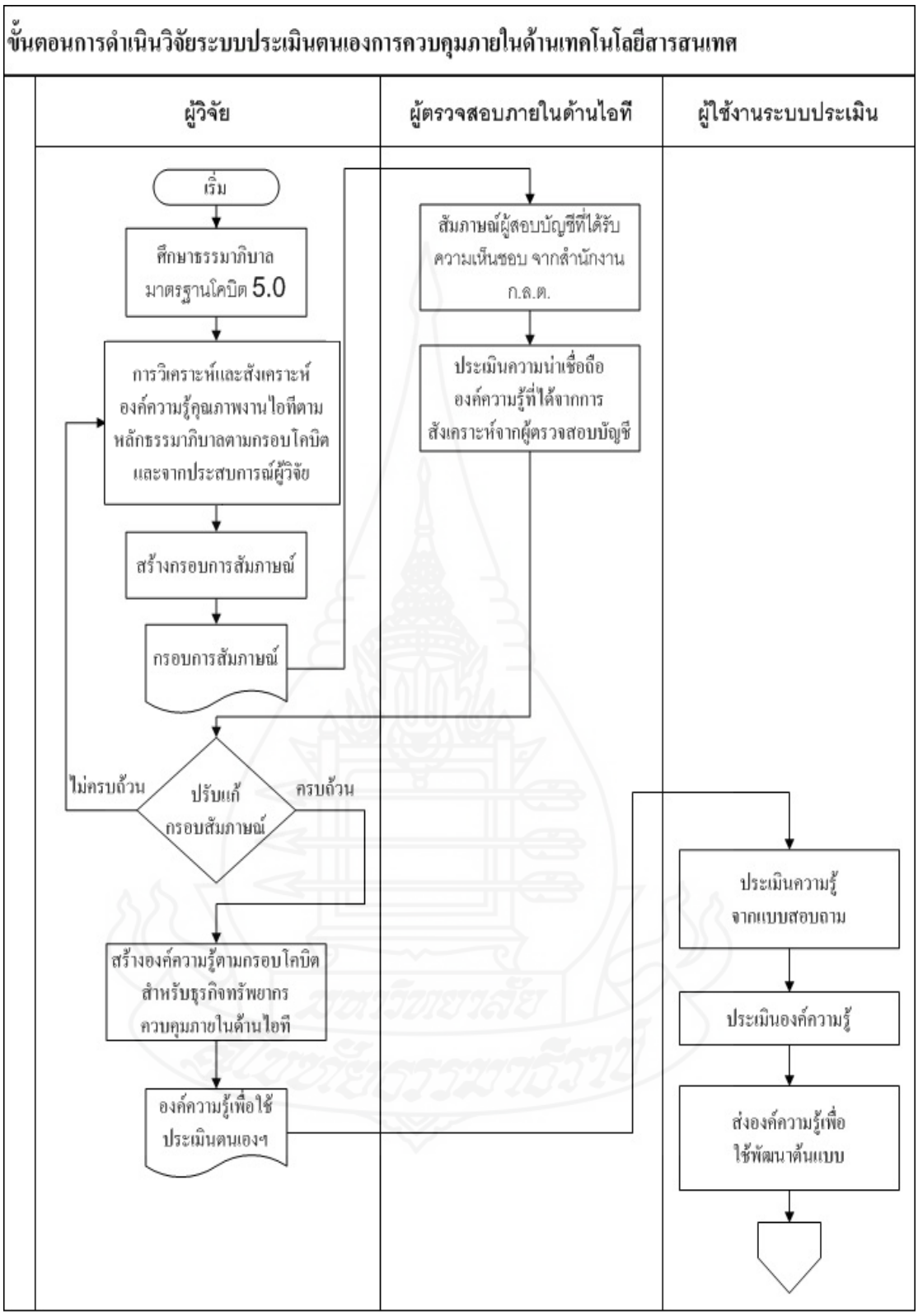
1.2.3 จากผู้ตรวจสอบบัญชี ในองค์กรที่ได้รับความเห็นชอบ จากสำนักงานก.ล.ต. จำนวน 3 องค์กรองค์กรละ 1 ท่าน

1.3 สังเคราะห์องค์ความรู้ตามกรอบโคบิตและจากเอกสารที่เกี่ยวข้องในกระบวนการควบคุมภายในงานด้านเทคโนโลยีสารสนเทศ

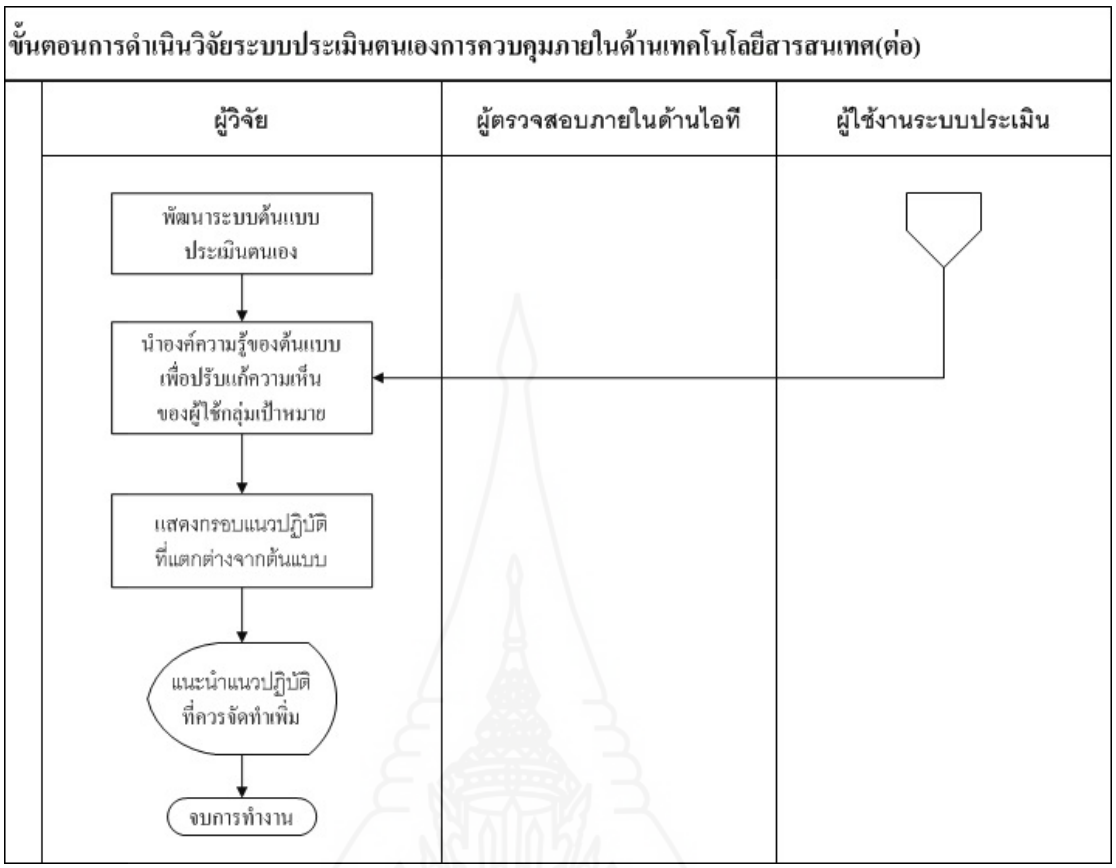
1.4 พัฒนาต้นแบบระบบประเมินตนเองฯ ที่ใช้องค์ความรู้เกี่ยวกับกระบวนการควบคุมภายในฯ ที่วิเคราะห์และสังเคราะห์ขึ้น

1.5 ประเมินองค์ความรู้ในต้นแบบประเมินตนเองด้านเทคโนโลยีสารสนเทศ ของบริษัทจดทะเบียนในกลุ่มทรัพยากรตามกรอบโคบิต เพื่อเตรียมความพร้อมในการเข้าตลาดหลักทรัพย์เอ็ม เอ ไอ แห่งประเทศไทย ที่ได้พัฒนาขึ้นโดยกลุ่มอุตสาหกรรมทรัพยากร

ผังขั้นตอนการดำเนินวิจัยดังภาพที่ 3.1



ภาพที่ 3.1 ขั้นตอนการดำเนินวิจัย



ภาพที่ 3.1 ขั้นตอนการดำเนินวิจัย (ต่อ)

2. วิธีการดำเนินวิจัย

2.1 ศึกษากรอบโคบิต 5.0 ผู้วิจัยศึกษาธรรมาภิบาลตามกรอบโคบิต กรอบการศึกษามีโดเมนที่มีกระบวนการดังนี้

2.1.1 ประเมิน สั่งการ และเฝ้าติดตาม (EDM) โดยมีกระบวนการที่ต้องศึกษาดังนี้

- มั่นใจการกำหนดกรอบการดำเนินงานการกำกับดูแลและการบำรุงรักษา
- มั่นใจในการส่งมอบผลประโยชน์
- มั่นใจในความเสี่ยงที่เหมาะสม
- มั่นใจในการใช้ทรัพยากรให้ได้ประโยชน์สูงสุด
- มั่นใจในความโปร่งใสต่อผู้มีส่วนได้เสีย

2.1.2 จัดวางแนว จัดทำแผน และจัดระบบ (APO) โดยมีกระบวนการต่างๆ ที่ต้องศึกษาดังนี้

- บริหารจัดการกรอบการดำเนินงานการบริหารงานด้านไอที
- บริหารจัดการกลยุทธ์
- บริหารจัดการสถาปัตยกรรมองค์กร
- บริหารจัดการนวัตกรรม
- บริหารจัดการกลุ่มของชุดโครงการ
- บริหารจัดการงบประมาณและต้นทุน
- บริหารจัดการทรัพยากรบุคคล
- บริหารจัดการความสัมพันธ์
- บริหารจัดการข้อตกลงการให้บริการ
- บริหารจัดการผู้ขายหรือผู้ให้บริการ
- บริหารจัดการคุณภาพ
- บริหารจัดการความเสี่ยง
- บริหารจัดการความมั่นคงปลอดภัย

2.1.3 จัดสร้าง จัดหา และนำไปใช้ (BAI) โดยมีกระบวนการต่างๆ ที่ต้องศึกษา ดังนี้

- บริหารจัดการ โครงการและชุดโครงการ
- บริหารจัดการข้อกำหนดความต้องการ
- บริหารจัดการการระบุและจัดสร้างกระบวนการแก้ปัญหาแบบเบ็ดเสร็จ
- บริหารจัดการความพร้อมใช้งานและขีดความสามารถ
- บริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล
- บริหารจัดการการเปลี่ยนแปลง
- บริหารจัดการการยอมรับการเปลี่ยนแปลงและการปรับเปลี่ยน
- บริหารจัดการความรู้
- บริหารจัดการสินทรัพย์
- บริหารจัดการองค์ประกอบของระบบ

2.1.4 ส่งมอบ บริการ และสนับสนุน (DSS) โดยมีกระบวนการต่างๆ ที่ต้องศึกษา ดังนี้

- บริหารจัดการการปฏิบัติการ
- บริหารจัดการคำร้องขอบริการและเหตุการณ์เกิดขึ้น
- บริหารจัดการปัญหา

- บริหารจัดการความต่อเนื่อง
- บริหารจัดการบริการด้านความมั่นคงปลอดภัย
- บริหารจัดการการควบคุมกระบวนการทางธุรกิจ

2.1.5 เฝ้าติดตาม วัดผล และประเมิน (MEA) โดยมีกระบวนการต่างๆ ที่ต้องศึกษา ดังนี้

- เฝ้าติดตาม วัดผล และประเมิน ประสิทธิภาพและความสอดคล้องในการดำเนินงาน
- เฝ้าติดตาม วัดผล และประเมิน ระบบการควบคุมภายใน
- เฝ้าติดตาม วัดผล และประเมินการปฏิบัติตามข้อกำหนดจากหน่วยงานภายนอก

2.2 วิเคราะห์กระบวนการการควบคุมภายในด้านเทคโนโลยีสารสนเทศของธุรกิจกลุ่มทรัพยากรจาก 3 แหล่งข้อมูลคือ

2.2.1 จากกรอบโคบิต 5.0 กำหนดกรอบโคบิตที่เกี่ยวข้องกับการควบคุมภายในงานเทคโนโลยีสารสนเทศของธุรกิจทรัพยากร

2.2.2 จากประสบการณ์ของผู้วิจัยในด้านเทคโนโลยีสารสนเทศ นำกรอบโคบิตที่เกี่ยวข้องและจำเป็นสำหรับกระบวนการการควบคุมภายในงานเทคโนโลยีสารสนเทศของธุรกิจทรัพยากร เพื่อสร้างกรอบการสัมภาษณ์

แต่ละกระบวนการมีขั้นตอนควบคุมประกอบด้วย

1. มีผู้จัดทำเอกสารกระบวนการปฏิบัติงาน
2. มีผู้ตรวจสอบเอกสารครบถ้วนถูกต้องทุกขั้นตอน
3. มีผู้อนุมัติเอกสารโดยผู้บริหารสูงสุดขององค์กรหรือฝ่ายไอที
4. มีประกาศใช้ให้ที่มีการบังคับใช้ทั้งองค์กร
5. มีการทบทวนกระบวนการใช้งานอย่างน้อยปีละหนึ่งครั้ง

แต่ละกระบวนการย่อยมีระดับความเสี่ยง

1 ความเสี่ยงระดับสูง

2 ความเสี่ยงระดับกลาง

3 ความเสี่ยงระดับต่ำ

2.2.3 จากผู้ตรวจสอบบัญชี ในองค์กรที่ได้รับความเห็นชอบ จากสำนักงาน ก.ล.ต. จำนวน 3 องค์กรองค์กรละ 1 ท่าน เพื่อตรวจทานกระบวนการจากกรอบโคบิตที่เกี่ยวข้องและจำเป็นสำหรับกระบวนการการควบคุมภายในงานเทคโนโลยีสารสนเทศของธุรกิจกลุ่มทรัพยากร

2.3 สังเคราะห์องค์ความรู้ตามกรอบโคบิตที่วิเคราะห์ไว้โดยมีเอกสารที่เกี่ยวข้องในกระบวนการควบคุมภายในงานด้านเทคโนโลยีสารสนเทศที่สำคัญคือ

1) คู่มือปฏิบัติงาน หมายถึง กระบวนการการปฏิบัติงานด้านไอทีที่มีการกำหนดวัถุประสงค์ขอบเขต และขั้นตอนการปฏิบัติงานด้านไอที

2) งานประจำ หมายถึง ฟอร์มเอกสารที่มีรายการที่ต้องตรวจสอบ ประจำวัน ประจำเดือน ประจำไตรมาส ประจำปี เป็นต้น

3) เอกสารไอที หมายถึง เอกสารทั่วไปที่ไอทีใช้อธิบาย ผังงาน ผังระบบ ฟอร์มเอกสารและรายการการตรวจสอบความถูกต้อง

2.4 พัฒนาต้นแบบระบบประเมินตนเองฯ ที่ใช้องค์ความรู้เกี่ยวกับกระบวนการควบคุมภายในฯ ที่วิเคราะห์และสังเคราะห์ขึ้น เครื่องมือที่ใช้ในการพัฒนาต้นแบบ ประกอบด้วย

1) Start UML Version 5.0.2.1570 เพื่อใช้ในการวิเคราะห์ระบบเทคโนโลยีสารสนเทศ

2) Microsoft Visual Studio Community 2015 เพื่อใช้พัฒนาโปรแกรมต้นแบบ

3) SQL Server 2005 เพื่อใช้ในการจัดการฐานข้อมูล

2.5 ประเมินองค์ความรู้ในต้นแบบประเมินตนเองด้านเทคโนโลยีสารสนเทศ ของบริษัทจดทะเบียนในกลุ่มทรัพยากรตามกรอบโคบิต เพื่อเตรียมความพร้อมในการเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย ที่ได้พัฒนาขึ้นโดยกลุ่มอุตสาหกรรมทรัพยากร แบ่งเป็น 2 กลุ่มตัวอย่างคือ

1) องค์กรที่ต้องการเตรียมความพร้อมเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย จำนวน 1 องค์กร

2) องค์กรที่อยู่ในตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทยจำนวน 1 องค์กร จากนั้นทดลองการใช้งาน

บทที่ 4
ผลการวิเคราะห์ข้อมูล

1. วิเคราะห์กระบวนการการควบคุมภายในด้านเทคโนโลยีสารสนเทศของธุรกิจกลุ่มทรัพยากรจาก 3 แหล่งข้อมูล

1.1 จากกรอบโคบิต 5.0 จากการศึกษาและวิเคราะห์กระบวนการการควบคุมภายในด้านเทคโนโลยีสารสนเทศจากกรอบโคบิตจากการพบว่าโดเมนที่เกี่ยวข้องมี 2 โดเมนมีกระบวนการและกระบวนการย่อยประกอบด้วย

1.1.1 จัดวางแนว จัดทำแผน และจัดระบบ (APO) มีกระบวนการประกอบด้วย

1) APO01 บริหารจัดการกรอบการดำเนินงานการบริหารงานด้านไอทีมีกระบวนการประกอบย่อยด้วย

APO01.01 กำหนดโครงสร้างองค์กร

APO01.02 กำหนดบทบาทหน้าที่และความรับผิดชอบ

APO01.04 สื่อสารวัตถุประสงค์และทิศทางในการบริหารจัดการสื่อสารให้มีความตระหนักและความเข้าใจในวัตถุประสงค์และทิศทางด้านไอทีให้แก่ผู้มีส่วนได้เสียและผู้ใช้ที่เหมาะสมทั่วทั้งองค์กร

APO01.06 กำหนดความเป็นเจ้าของสารสนเทศและระบบ

APO01.07 บริหารจัดการกระบวนการให้มีการปรับปรุงอย่างต่อเนื่อง

2) APO10 บริหารจัดการผู้ขายหรือผู้ให้บริการมีกระบวนการประกอบย่อยด้วย

APO10.01ระบุและประเมินความสัมพันธ์กับผู้ขายหรือผู้ให้บริการและสัญญาต่างๆ

3) APO12 บริหารจัดการความเสี่ยงมีกระบวนการประกอบย่อยด้วย

APO12.01 รวบรวมข้อมูล

APO12.02 วิเคราะห์ความเสี่ยง

APO12.03 ดูแลรักษาแผนภูมิความเสี่ยง

APO12.04 เชื่อมโยงความเสี่ยง

APO12.05 กำหนดกลุ่มของการดำเนินการบริหารความเสี่ยง

APO12.06 ตอบสนองต่อความเสี่ยง

4) APO13 บริหารจัดการความมั่นคงปลอดภัยมีกระบวนการประกอบย่อยด้วย

APO13.01 จัดทำและดูแลรักษา ISMS (Information Security Management System - ISMS)

APO13.02 กำหนดและบริหารแผนจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

APO13.03 เฝ้าติดตามและสอบทานISMS

1.1.2 จัดสร้าง จัดหา และนำไปใช้ (BAI) มีกระบวนการประกอบด้วย

1) BAI06 บริหารจัดการการเปลี่ยนแปลงมีกระบวนการประกอบย่อยด้วย

BAI06.01 ประเมินจัดลำดับความสำคัญและอนุมัติคำร้องขอให้มีการเปลี่ยนแปลง

BAI06.03 ติดตามและรายงานสถานะของการเปลี่ยนแปลง

BAI06.04 ปิดงานและจัดทำเอกสารเกี่ยวกับการเปลี่ยนแปลง

2) BAI09 บริหารจัดการสินทรัพย์มีกระบวนการประกอบย่อยด้วย

BAI09.01 ระบุและบันทึกสินทรัพย์ในปัจจุบัน

BAI09.03 บริหารจัดการวัฏจักรของสินทรัพย์

BAI09.05 บริหารจัดการใบอนุญาตให้ใช้สิทธิ์

1.2 จากประสบการณ์ของผู้วิจัยในด้ายเทคโนโลยีสารสนเทศ สังเคราะห์องค์ความรู้ตามกรอบโคบิตและจากเอกสารที่เกี่ยวข้องในกระบวนการควบคุมภายในงานด้านเทคโนโลยีสารสนเทศที่สำคัญ

1. คู่มือปฏิบัติงาน หมายถึง กระบวนการการปฏิบัติงานด้านไอทีที่มีการกำหนดวัตถุประสงค์ขอบเขต และขั้นตอนการปฏิบัติงานด้านไอที

2. งานประจำ หมายถึง ฟอร์มเอกสารที่มีรายการการที่ต้องตรวจสอบ ประจำวัน ประจำเดือน ประจำไตรมาส ประจำปี เป็นต้น

3. เอกสารไอที หมายถึง เอกสารทั่วไปที่ไอทีใช้อธิบาย ผังงาน ผังระบบ ฟอร์ม

สังเคราะห์องค์ความรู้ตามกรอบโคบิตเพื่อเป็นกรอบในการสัมภาษณ์เพื่อยืนยันองค์ความรู้ดังภาพที่ 4.1

ลำดับ	รายการแนะนำจากการสัมภาษณ์	ประเภทเอกสาร	โดเมน	กระบวนการ	กระบวนการย่อย
2	แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ	คู่มือปฏิบัติงาน	APO	APO12,APO01	APO12.01, APO12.02, APO12.03, APO12.04,
3	การจัดการและสิทธิของผู้ใช้งานอีเมล์	คู่มือปฏิบัติงาน	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO
4	การจัดเก็บลิขสิทธิ์ซอฟต์แวร์/ทะเบียนคุมลิขสิทธิ์โปรแกรมคอมพิวเตอร์ (Software License List)	คู่มือปฏิบัติงาน	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO01.07
5	สำรองข้อมูล/ฟื้นฟู ฐานข้อมูลของ S/W หลัก เช่น ERP,Accounting,HR Payroll	คู่มือปฏิบัติงาน	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO01.07
6	การสอบทานรหัสและสิทธิของผู้ใช้งานระบบหลัก เช่น ERP,Accounting,HR Payroll	คู่มือปฏิบัติงาน	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO01.07
7	การตรวจสอบและสิทธิของผู้ใช้งานสินทรัพย์ด้านไอที	คู่มือปฏิบัติงาน	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO01.07
8	8 ระดับในการเข้าถึงระบบงานอินเตอร์เน็ต (Authorization)	คู่มือปฏิบัติงาน	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO01.07
9	ทบทวนสัญญาการต่อสัญญาบริการด้านไอที	คู่มือปฏิบัติงาน	APO	APO10,APO01	APO10.01,APO01.06,APO01.04,APO01.07
10	การดำเนินงานโครงงานด้านไอที(ใช้บุคลากรในองค์กร)	คู่มือปฏิบัติงาน	BAI, APO	BAI06,APO01	BAI06.01, BAI06.03,BAI06.04,APO01.06,
11	การบำรุงรักษาเชิงป้องกันสินทรัพย์ไอทีและตรวจสอบโปรแกรมลิขสิทธิ์(Preventive Maintenance)	คู่มือปฏิบัติงาน	BAI, APO	BAI09,APO01	BAI09.01, BAI09.03, BAI09.05,APO01.06,
12	สิทธิ์การใช้ซอฟต์แวร์ตามระดับโครงสร้างบุคลากรและลักษณะงานและฟอร์มขออนุมัติขอใช้สิทธิ์ใช้ซอฟต์แวร์	คู่มือปฏิบัติงาน	BAI, APO	BAI09,APO01	BAI09.05,APO01.06,APO01.04,APO01.07
13	การตรวจสอบห้องเซฟเวอร์	งานประจำ	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO
14	ตรวจอุปกรณ์ไอทีที่ใช้งานส่วนรวมประจำวัน(work dates)	งานประจำ	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO
15	ตรวจสอบการบุกรุกด้านเน็ตเวอร์/เซิฟเวอร์	งานประจำ	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO
16	ตรวจเช็คอุปกรณ์ห้องเซิฟเวอร์(work dates)	งานประจำ	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO
17	ฟอร์มขอใช้งานห้องเซิปเวอร์	งานประจำ	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO01.07

ภาพที่ 4.1 สังเคราะห์องค์ความรู้ตามกรอบโคบิตและจากเอกสาร

ลำดับ	รายการแนะนำจากการสัมภาษณ์	ประเภทเอกสาร	โดเมน	กระบวนการ	กระบวนการย่อย
18	กำหนดผู้รับผิดชอบผู้รับสิทธิสูงสุดของระบบหลัก(High	เอกสารไอที	APO	APO01,APO01	APO01.06,APO01.06,APO01.04,APO
19	ฟอร์มการใช้อินเตอร์เน็ตจากบุคคลภานนอก	เอกสารไอที	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO
20	สัญญาว่าจ้างผู้ให้บริการภายนอก (Outsource Agreement)	เอกสารไอที	APO	APO07,APO01	APO07.06,APO01.06,APO01.04,APO
21	โครงสร้างบุคลากรหน่วยงานคอมพิวเตอร์ (Organization	เอกสารไอที	APO	APO01,APO01	APO01.01,APO01.06,APO01.04,APO
22	ใบบรรยายลักษณะงาน (Job Description)	เอกสารไอที	APO	APO01,APO01	APO01.02,APO01.06,APO01.04,APO
23	แผนผังการวางระบบเครือข่ายคอมพิวเตอร์ (Network	เอกสารไอที	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO
24	แผนผังการวางเครื่องคอมพิวเตอร์ (Computer Layout)	เอกสารไอที	APO	APO13,APO01	APO13.03,APO01.06,APO01.04
25	แผนผังระบบห้อง(Server room layout)	เอกสารไอที	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO
26	ฟอร์มใบเบิกอุปกรณ์ไอที/ใบส่งคืนอุปกรณ์ไอที	เอกสารไอที	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO
27	แผนงานหรือโครงการดำเนินงานทางด้านสารสนเทศ	เอกสารไอที	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO

ภาพที่ 4.1 สังเคราะห์องค์ความรู้ตามกรอบโคบิตและจากเอกสาร (ต่อ)

1.3 จากผู้ตรวจสอบบัญชี ในองค์กรที่ได้รับความเห็นชอบ จากสำนักงาน ก.ล.ต.จำนวน 3 องค์กรองค์กรละ 1 ท่าน เพื่อตรวจทานองค์ความรู้กระบวนการจากกรอบโคบิตที่เกี่ยวข้องและจำเป็นสำหรับกระบวนการการควบคุมภายในงานเทคโนโลยีสารสนเทศของธุรกิจกลุ่มทรัพยากร ประกอบด้วย

1. ท่านแรกตำแหน่ง Manager, Risk Assurance มีประสบการทำงาน 5ปี
2. ท่านที่สาม Assistant Manager, Risk Assurance มีประสบการทำงาน 9ปี
3. ท่านที่สองตำแหน่ง Senior Manager, Assurance มีประสบการทำงาน 14ปี

ระยะเวลาในการสัมภาษณ์ ระหว่าง วันที่ 21 มีนาคม-29 เมษายน 2559

1.3.1 กระบวนการที่จากการตรวจทานจากกรอบโคบิตที่เกี่ยวข้องและจำเป็นสำหรับกระบวนการการควบคุมภายในงานเทคโนโลยีสารสนเทศของธุรกิจกลุ่มทรัพยากร แต่ละกระบวนการมีขั้นตอนควบคุมประกอบด้วย

1. มีผู้จัดทำเอกสารกระบวนการปฏิบัติงาน
2. มีผู้ตรวจสอบเอกสารครบถ้วนถูกต้องทุกขั้นตอน
3. มีผู้อนุมัติเอกสารโดยผู้บริหารสูงสุดขององค์กรหรือฝ่ายไอที
4. มีประกาศใช้ให้ที่มีการบังคับใช้ทั้งองค์กร
5. มีการทบทวนกระบวนการใช้งานอย่างน้อยปีละหนึ่งครั้ง

ดังภาพที่ 4.2

ลำดับ	รายการแนะนำจากการสัมภาษณ์	ประเภทเอกสาร	โดเมน	กระบวนการ	กระบวนการย่อย	ผู้จัดทำ	ผู้ตรวจสอบ	ผู้อนุมัติ	การบังคับใช้	การทบทวน
1	นโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศ	คู่มือปฏิบัติงาน	APO	APO13,APO01	APO13.01, APO13.02,APO01.06,APO01.04,APO	✓	✓	✓	✓	✓
2	แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ	คู่มือปฏิบัติงาน	APO	APO12,APO01	APO12.01, APO12.02, APO12.03, APO12.04,	✓	✓	✓	✓	✓
3	การจัดการและสิทธิของผู้ใช้งานอีเมล์	คู่มือปฏิบัติงาน	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO	✓	✓	✓	✓	✓
4	การจัดเก็บลิขสิทธิ์ซอฟต์แวร์/ทะเบียนคุมลิขสิทธิ์โปรแกรมคอมพิวเตอร์ (Software License List)	คู่มือปฏิบัติงาน	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO 01.07	✓	✓	✓	✓	✓
5	สำรองข้อมูลที่ขึ้นปู ฐานข้อมูลของ S/W หลัก เช่น ERP,Accounting,HR Payroll	คู่มือปฏิบัติงาน	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO 01.07	✓	✓	✓	✓	✓
6	การสอบทานรหัสและสิทธิของผู้ใช้งานระบบหลัก เช่น ERP,Accounting,HR Payroll	คู่มือปฏิบัติงาน	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO 01.07	✓	✓	✓	✓	✓
7	การตรวจสอบและสิทธิของผู้ใช้งานสินทรัพย์ด้านไอที	คู่มือปฏิบัติงาน	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO 01.07	✓	✓	✓	✓	✓
8	8 ระดับในการเข้าถึงระบบงานอินเตอร์เน็ต (Authorization)	คู่มือปฏิบัติงาน	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO 01.07	✓	✓	✓	✓	✓
9	ทบทวนสัญญาการต่อสัญญาบริการด้านไอที	คู่มือปฏิบัติงาน	APO	APO10,APO01	APO10.01,APO01.06,APO01.04,APO 01.07	✓	✓	✓	✓	✓
10	การดำเนินงานโครงงานด้านไอที(ใช้บุคลากรในองค์กร)	คู่มือปฏิบัติงาน	BAI, APO	BAI06,APO01	BAI06.01, BAI06.03,BAI06.04,APO01.06,	✓	✓	✓	✓	✓
11	การบำรุงรักษาเชิงป้องกันสินทรัพย์ไอทีและตรวจสอบโปรแกรมลิขสิทธ์(Preventive Maintenance)	คู่มือปฏิบัติงาน	BAI, APO	BAI09,APO01	BAI09.01, BAI09.03, BAI09.05,APO01.06,	✓	✓	✓	✓	✓
12	สิทธิ์การใช้ซอฟต์แวร์ตามระดับโครงสร้างบุคลากรและลักษณะงานและฟอร์มขออนุมัติขอใช้สิทธิ์ใช้ซอฟต์แวร์	คู่มือปฏิบัติงาน	BAI, APO	BAI09,APO01	BAI09.05,APO01.06,APO01.04,APO 01.07	✓	✓	✓	✓	✓
13	การตรวจสอบห้องเซฟเวอร์	งานประจำ	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO	✓		✓	✓	
14	ตรวจอุปกรณ์ไอทีที่ใช้งานส่วนรวมประจำวัน(work dates)	งานประจำ	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO	✓			✓	
15	ตรวจสอบการบุกรุกด้านเน็ตเวอร์/เซิฟเวอร์	งานประจำ	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO	✓			✓	
16	ตรวจเช็คอุปกรณ์ห้องเซิฟเวอร์(work dates)	งานประจำ	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO	✓			✓	
17	ฟอร์มขอใช้งานห้องเซิปเวอร์	งานประจำ	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO 01.07	✓			✓	
18	กำหนดผู้รับผิดชอบผู้รับสิทธิสูงสุดของระบบหลัก(High	เอกสารไอที	APO	APO01,APO01	APO01.06,APO01.06,APO01.04,APO	✓		✓	✓	✓
19	ฟอร์มการใช้อินเตอร์เน็ตจากบุคคลภายนอก	เอกสารไอที	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO	✓			✓	
20	สัญญาว่าจ้างผู้ให้บริการภายนอก (Outsource Agreement)	เอกสารไอที	APO	APO07,APO01	APO07.06,APO01.06,APO01.04,APO	✓		✓	✓	
21	โครงสร้างบุคลากรหน่วยงานคอมพิวเตอร์ (Organization	เอกสารไอที	APO	APO01,APO01	APO01.01,APO01.06,APO01.04,APO	✓		✓	✓	
22	ใบบรรยายลักษณะงาน (Job Description)	เอกสารไอที	APO	APO01,APO01	APO01.02,APO01.06,APO01.04,APO	✓		✓	✓	
23	แผนผังการวางระบบเครือข่ายคอมพิวเตอร์ (Network	เอกสารไอที	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO	✓			✓	
24	แผนผังการวางเครื่องคอมพิวเตอร์ (Computer Layout)	เอกสารไอที	APO	APO13,APO01	APO13.03,APO01.06,APO01.04	✓			✓	
25	แผนผังระบบห้อง(Server room layout)	เอกสารไอที	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO	✓			✓	
26	ฟอร์มใบเบิกอุปกรณ์ไอที/ใบส่งคืนอุปกรณ์ไอที	เอกสารไอที	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO	✓			✓	
27	แผนงานหรือโครงการดำเนินงานทางด้านสารสนเทศ	เอกสารไอที	APO	APO13,APO01	APO13.03,APO01.06,APO01.04,APO	✓		✓	✓	

ภาพที่ 4.2 การควบคุมกระบวนการจากองค์ความรู้เพื่อประเมินตนเอง

1.3.2 กระบวนการย่อย (จะมีในคู่มือปฏิบัติงานเท่านั้น) ที่จากการตรวจทานจากกรอบโคบิตที่เกี่ยวข้องและจำเป็นสำหรับกระบวนการการควบคุมภายในงานเทคโนโลยีสารสนเทศของธุรกิจกลุ่มทรัพยากร แต่ละกระบวนการย่อยมีระดับความเสี่ยงประกอบด้วย

1. ความเสี่ยงระดับสูง หมายถึง กระบวนการย่อยนี้ควรมีการจัดการโดยเร็วที่สุดตามเงื่อนตามองค์กรที่กำหนดไว้

2. ความเสี่ยงระดับกลาง หมายถึง กระบวนการย่อยนี้ควรมีการจัดการโดยเร็วรองจากระดับความเสี่ยงระดับสูงตามเงื่อนตามองค์กรที่กำหนดไว้

3. ความเสี่ยงระดับต่ำ หมายถึง กระบวนการย่อยนี้ควรมีการจัดการโดยเร็วรองจากระดับความเสี่ยงระดับกลางตามเงื่อนตามองค์กรที่กำหนดไว้

1) นโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยมีระดับความเสี่ยงกระบวนการย่อยประกอบไปด้วยดังตารางที่ 4.1

ตารางที่ 4.1 ระดับความเสี่ยงนโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศ

ระดับความเสี่ยง	**1.นโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศ**
1.1 ข้อกำหนดทั่วไปการกำหนดความปลอดภัยพื้นที่ปฏิบัติการสารสนเทศ	
ต่ำ	1.1.1 ติดป้ายแสดงเขตพื้นที่
ต่ำ	1.1.2 อาหาร/เครื่องดื่ม
กลาง	1.1.3 วัสดุไวไฟ
ต่ำ	1.1.4 สัมภาระที่ไม่เกี่ยวข้องไม่ควรอยู่กับการปฏิบัติงานในพื้นที่ปฏิบัติการสารสนเทศ
ต่ำ	1.1.5 ควบคุม ดูแล รักษาความสะอาด ปลอดภัย และเหมาะสมต่อลักษณะการทำงาน
สูง	1.1.6 การควบคุมการเข้าออกพื้นที่ปฏิบัติการสารสนเทศ
สูง	1.1.7 การควบคุม ดูแล การใช้อุปกรณ์สื่อสัญญาณทุกชนิดอย่างเหมาะสม เพื่อป้องกันการรบกวน หรือทำความสูญเสียหรือเสียหาย
สูง	1.1.8 ผู้ที่ไม่เกี่ยวข้องต้องได้รับอนุญาตจากหัวหน้าส่วนงานเจ้าของพื้นที่ และให้อยู่ในความดูแลโดยใกล้ชิดจากเจ้าหน้าที่ผู้ที่เกี่ยวข้องในพื้นที่ทั้งในและนอกเวลาทำการจนกว่าการปฏิบัติงานจะแล้วเสร็จ
สูง	1.1.9 แผนป้องกันภัยยามฉุกเฉินภายในพื้นที่ปฏิบัติการสารสนเทศ ดำเนินการซักซ้อมอย่างน้อยปีละ 1 ครั้ง
1.2 การรักษาความปลอดภัยด้านเครื่องคอมพิวเตอร์	
กลาง	1.2.1 ผู้ดูแลเครื่องคอมพิวเตอร์ ดูแลคอมพิวเตอร์ให้ใช้งานได้ดีอยู่เสมอ

ตารางที่ 4.1 (ต่อ)

ระดับความเสี่ยง	1.นโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศ
	1.2.2 ดูแลเครื่องคอมพิวเตอร์ ตรวจสอบสภาพแวดล้อมในสถานที่ทำงานให้เหมาะสมกับเครื่องคอมพิวเตอร์
สูง	1.2.2.1 จัดเตรียม UPS ไว้ใช้งาน
สูง	1.2.2.2 หลีกเลี่ยงการติดตั้งคอมพิวเตอร์ ที่มีอุณหภูมิสูง มีฝุ่นละอองมาก มีความชื้นสูง แม่เหล็กรบกวน
สูง	1.2.3 จัดให้มีระบบสำรองข้อมูลลงในสื่อคอมพิวเตอร์ชนิดต่างๆ ตามความจำเป็น เช่น Floppy Disk, CD, Tape Backup, Hard Disk Backup หรืออื่นๆ
สูง	1.2.4 ดูแลเครื่องคอมพิวเตอร์ติดตั้งโปรแกรมหรืออุปกรณ์ป้องกันไวรัส
สูง	1.2.5 ปรับปรุงโปรแกรมหรืออุปกรณ์ป้องกันไวรัสให้เป็นปัจจุบันเสมอ
กลาง	1.2.6 ห้ามการติดตั้งโปรแกรม เพลง ภาพยนต์ ที่ไม่มีลิขสิทธิ์
	1.3 การรักษาความปลอดภัยด้านเครือข่ายคอมพิวเตอร์
สูง	1.3.1 ระบบเครือข่ายไร้สาย (Wireless LAN) ต้องจัดให้มีการควบคุมการเชื่อมต่ออย่างเข้มงวด
สูง	1.3.2 ส่วนงานใดที่มีความต้องการจัดทำระบบงานซึ่งจำเป็นต้องใช้การเชื่อมต่อผ่านเครือข่ายคอมพิวเตอร์ ต้องแจ้งให้ผู้ดูแลเครือข่ายคอมพิวเตอร์ทราบตั้งแต่ขั้นตอนของการวางแผนจัดทำโครงการเพื่อการเตรียมการรองรับการเชื่อมต่อทางด้านเครือข่ายคอมพิวเตอร์ของระบบงานนั้นๆ
สูง	1.3.3 ห้ามผู้ไม่มีหน้าที่เกี่ยวข้องกับการดูแลเครือข่ายคอมพิวเตอร์ใช้โปรแกรมที่สามารถจัดดูข้อมูลภายในเครือข่ายคอมพิวเตอร์ เพื่อดูข้อมูลที่รับ – ส่งผ่านในเครือข่ายคอมพิวเตอร์
	1.4 การรักษาความปลอดภัยด้านข้อมูลสารสนเทศ
สูง	1.4.1 การรับ – ส่ง ข้อมูลสารสนเทศไม่ว่าในสื่อหรือวิธีการใดที่มีความสำคัญ ระหว่างส่วนงานทั้งส่วนงานภายในและภายนอก จะต้องได้รับอนุญาตจากผู้บังคับบัญชาที่ดูแลระบบสารสนเทศนั้นๆ โดยมีการจัดทำทะเบียนควบคุมการรับส่งข้อมูลสารสนเทศนั้นๆ ไว้อย่างชัดเจน
สูง	1.4.2 กรณีที่มีความจำเป็นต้องส่งผ่านข้อมูลสารสนเทศที่มีความสำคัญออกไปในระบบอินเทอร์เน็ตหรืออินทราเน็ต ให้มีการเข้ารหัสของข้อมูลสารสนเทศที่จัดส่งออกไป

ตารางที่ 4.1 (ต่อ)

ระดับความเสี่ยง	1.นโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศ
สูง	1.4.3 การแบ่งปัน (Share) ข้อมูลให้แบ่งปันเฉพาะสิ่งที่ต้องการ และต้องกำหนดรหัสผ่านทุกครั้ง และเมื่อหมดความจำเป็นในการแบ่งปันนั้นให้ยกเลิกการแบ่งปันทันที
	1.5 การรักษาความปลอดภัยด้านซอฟท์แวร์
สูง	1.5.1 ให้ส่วนงานจัดเก็บเอกสารแสดงลิขสิทธิ์และซอฟท์แวร์ต้นฉบับอย่างดีที่สุด เว้นแต่ลิขสิทธิ์รวม ให้อยู่ในความรับผิดชอบของฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ
สูง	1.5.2 ให้ส่วนงานจัดให้มีการบำรุงรักษาซอฟท์แวร์ให้สามารถใช้งานได้อย่างต่อเนื่อง
	1.6 การรักษาความปลอดภัยด้านการสำรองและการกู้คืนสภาพระบบสารสนเทศ
	1.6.1 ส่วนงานที่รับผิดชอบระบบสารสนเทศจะต้องจัดทำแผนการดำเนินการสำรองระบบสารสนเทศ
สูง	1.6.1.1 ลำดับความสำคัญของระบบงานหรือระบบสารสนเทศที่จะทำสำรอง
กลาง	1.6.1.2 เลือกประเภทของสื่อบันทึกข้อมูลที่ใช้ในการสำรองระบบสารสนเทศ
ต่ำ	1.6.1.3 กำหนดตารางเวลาและความถี่ในการสำรองของแต่ละระบบงาน
กลาง	1.6.1.4 สถานที่หลักและสถานที่รอง สำหรับใช้จัดเก็บสื่อบันทึกข้อมูลที่ใช้ในการสำรองระบบสารสนเทศ
สูง	1.6.1.5 จัดทำสมุดบันทึก (Log Book) เพื่อบันทึกการปฏิบัติงานของการสำรองระบบสารสนเทศ โดยมีระยะเวลาการเก็บสมุดบันทึกไม่น้อยกว่า 1 ปี
ต่ำ	1.6.1.6 ให้มีการปรับปรุงเอกสารสำรองระบบสารสนเทศทุกๆ 1 ปี หรือเมื่อมีการเปลี่ยนแปลงของระบบสารสนเทศ
ต่ำ	1.6.1.7 ขั้นตอนการตรวจสอบผลการทำสำรองระบบสารสนเทศ
	1.6.2 แนวทางการกู้คืนสภาพระบบสารสนเทศ (Recovery) ต้องครอบคลุมหัวข้อดังต่อไปนี้เป็นอย่างน้อย
สูง	1.6.2.1 ลำดับความสำคัญของระบบงานและหรือระบบสารสนเทศ ที่จะทำการกู้คืนสภาพ

ตารางที่ 4.1 (ต่อ)

ระดับความเสี่ยง	1.นโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศ
	1.6.2.2 ขั้นตอนการกู้คืนสภาพระบบสารสนเทศ โดยให้มีรายละเอียดอย่างน้อยดังนี้
สูง	1.6.2.3.1 การกู้คืนสภาพระบบคอมพิวเตอร์
สูง	1.6.2.3.2 การกู้คืนสภาพระบบเครือข่าย
สูง	1.6.2.3.3 การกู้คืนสภาพระบบงาน
สูง	1.6.2.3.4 การตรวจสอบการกู้คืนสภาพ
สูง	1.6.2.3 ให้มีการทดสอบการกู้คืนสภาพระบบสารสนเทศในแต่ละระบบงานอย่างน้อยทุกๆ 6 เดือน พร้อมบันทึกผลการดำเนินงาน และรายงานให้หัวหน้าส่วนงานที่รับผิดชอบทราบ
1.7 การรักษาความปลอดภัยด้านเอกสารและอุปกรณ์บันทึกข้อมูลระบบสารสนเทศ	
ต่ำ	1.7.1 เอกสารและอุปกรณ์บันทึกข้อมูลระบบสารสนเทศที่ไม่ได้มีการใช้งานแล้วให้เก็บไว้ช่วงเวลาหนึ่ง
กลาง	1.7.2 การทำลายเอกสารระบบสารสนเทศที่เป็นความลับจะต้องดำเนินการทำลายเอกสารนั้นๆ ด้วยเครื่องทำลายเอกสารเสียก่อนมิให้สามารถใช้งานได้ต่อไป
ต่ำ	1.7.3 การทำลายข้อมูลสารสนเทศที่เก็บอยู่ในสื่อคอมพิวเตอร์ ให้ใช้วิธีการที่มั่นใจได้ว่าข้อมูลได้ถูกลบทิ้งโดยไม่สามารถกู้คืนได้อีก
ต่ำ	1.7.4 มีการกำหนดอายุการใช้งานของสื่อบันทึกข้อมูลสารสนเทศ และให้มีการบันทึกวันเริ่มใช้งานและวันสิ้นสุดการใช้งาน
	1.7.5 มาตรฐานการรักษาความปลอดภัยของห้องเก็บอุปกรณ์บันทึกข้อมูลระบบสารสนเทศ
ต่ำ	1.7.5.1 การเก็บอุปกรณ์บันทึกข้อมูลระบบสารสนเทศ จะต้องจัดทำทะเบียนแสดงรายละเอียดของข้อมูลที่จัดเก็บ
ต่ำ	1.7.5.2 การเก็บอุปกรณ์บันทึกข้อมูลระบบสารสนเทศที่เป็นความลับต้องจัดทำทะเบียนผู้มีสิทธิใช้อุปกรณ์ดังกล่าว
สูง	1.7.5.3 มีการลงทะเบียนทุกครั้งที่มีการยืมหรือคืนอุปกรณ์บันทึกข้อมูลระบบสารสนเทศ
กลาง	1.7.5.4 มีการควบคุม ดูแลทางด้านกายภาพของห้องเก็บอุปกรณ์เก็บข้อมูลระบบสารสนเทศเป็นอย่างดี ให้เหมาะกับการเก็บสื่อคอมพิวเตอร์

ตารางที่ 4.1 (ต่อ)

ระดับความเสี่ยง	1.นโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศ
	1.8 การรักษาความปลอดภัยด้านการใช้รหัสผ่าน
สูง	1.8.1 รหัสผ่าน ให้มีความยาวไม่น้อยกว่า x หลัก และเพื่อให้มีความปลอดภัยมากที่สุด รหัสผ่านควรเป็นทั้งชุดของตัวอักษร สัญลักษณ์พิเศษ ตัวเลขคละรวมกัน
สูง	1.8.2 ผู้ปฏิบัติงานที่รับอนุญาตและได้รับสิทธิในการใช้ระบบสารสนเทศ เมื่อได้รับจัดสรร รหัสผ่าน ให้เปลี่ยนรหัสผ่านเป็นของตัวเองที่เหมาะสมและเป็นความลับเฉพาะตัวชุดทันที
สูง	1.8.3 การขอใหม่ เปลี่ยนแปลง ยกเลิก รหัสผ่าน ให้ทำเป็นลายลักษณ์อักษร และในระบบสารสนเทศที่มีความสำคัญ ต้องผ่านความเห็นชอบจากต้นสังกัดก่อนขออนุมัติจากผู้มีอำนาจก่อนจะดำเนินการใดๆ
สูง	1.8.4 ผู้ปฏิบัติงานควรเปลี่ยนแปลงรหัสผ่านของตัวเองใหม่ทุกๆ 90 วัน หรือตามระยะเวลาที่ระบบสารสนเทศนั้นๆ กำหนด
สูง	1.8.5 การเปลี่ยนแปลงรหัสผ่านชุดใหม่ในแต่ละครั้ง จะต้องไม่นำรหัสผ่านชุดเก่ามาใช้ซ้ำอีก
	1.8.6 เจ้าของรหัสผ่านต้องรับผิดชอบในการปกปิดและรักษารหัสผ่านของตนเองอย่างดีที่สุด
สูง	1.8.6.1 ไม่จดบันทึกรหัสผ่านในที่ที่สามารถพบเห็นได้โดยง่าย
สูง	1.8.6.2 ไม่นำหรือไม่เปิดเผยรหัสผ่านให้บุคคลอื่นรับรู้ หากรหัสผ่านถูกเปิดเผยต้องเปลี่ยนใหม่โดยเร็ว
สูง	1.8.6.3 เมื่อเสร็จสิ้นการใช้งานระบบสารสนเทศแล้ว จะต้องออกจากการใช้ระบบ (Logout) ทุกครั้ง
	1.9 การรักษาความปลอดภัยด้านการป้องกันไวรัสคอมพิวเตอร์
	1.9.1 ผู้ดูแลระบบสารสนเทศ
สูง	1.9.1.1 ดำเนินการจัดหาโปรแกรมป้องกันไวรัสคอมพิวเตอร์ และอบรมการใช้งานให้กับผู้ดูแลเครื่องคอมพิวเตอร์ของส่วนงานต่างๆ
สูง	1.9.1.2 ตรวจสอบความทันสมัยของโปรแกรมป้องกันไวรัสคอมพิวเตอร์

ตารางที่ 4.1 (ต่อ)

ระดับความเสี่ยง	1.นโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศ
สูง	1.9.2.1 ดำเนินการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ให้กับเครื่องคอมพิวเตอร์ทุกเครื่อง โดยประสานงานกับผู้ดูแลระบบสารสนเทศ
สูง	1.9.2.2 ตรวจสอบความทันสมัยของโปรแกรมป้องกันไวรัสคอมพิวเตอร์และปรับปรุงให้กับระบบคอมพิวเตอร์ทุกๆ เครื่องอัตโนมัติ
สูง	1.9.2.3 ต้องป้องกันไม่ให้นำซอฟท์แวร์หรือข้อมูลที่อาจก่อนให้เกิดความเสียหายต่อระบบสารสนเทศของบริษัทมาติดตั้งใช้งาน
สูง	1.9.2.4 ต้องป้องกันผู้ใช้งานยกเลิกการทำงานของโปรแกรมป้องกันไวรัสคอมพิวเตอร์ซึ่งติดตั้งอยู่ในเครื่องคอมพิวเตอร์
	1.10 การบริหารการเปลี่ยนแปลง(Change Management)
สูง	1.10.1 การสร้างเอกสารการเพื่อขอการเปลี่ยนแปลงร้องขอทุกครั้ง ต้องมีหมายเลขประกอบชัดเจนและเลขที่เอกสารต้องไม่ซ้ำกัน
สูง	1.10.2 มีผู้ร้องขอ สร้างงานโครงงานใหม่หรืองานใหม่
สูง	1.10.3 มีผู้อนุมัติ (ต้องหัวหน้าผู้ร้องขอ) ต้องยินยอมโครงงานใหม่ตามผู้ร้องขอ
สูง	1.10.4 พนักงานไอทียืนยันการเริ่มงาน ดำเนินงานตามหัวข้องานและแจ้งผู้เจ้าหน้าที่ไอทีรับผิดชอบงาน
สูง	1.10.5 ผู้ร้องขอทำการทดสอบงานเมื่อใช้งานได้เรียบร้อยและแจ้งพนักงานไอทีทราบ
สูง	1.10.6 พนักงานไอทีผู้รับผิดชอบโครงงานปิดงาน
	1.11 การบริหารบัญชีผู้ใช้ที่มีสิทธิสูง
สูง	1.11.1 ผู้รับผิดชอบทางเทคโนโลยีสารสนเทศรหัสบัญชีสูงสุดควรเป็นผู้จัดการฝ่ายขึ้นไป
	1.12 การบริหารจัดการบัญชีผู้ใช้
สูง	1.12.1 ต้องจัดทำให้มีการทบทวงบัญชีผู้ใช้ประจำเดือน
สูง	1.12.2 แจ้งรายการบัญชีผู้ใช้ให้ต้นสังกัด

2) แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ โดยมีระดับความเสี่ยงกระบวนการย่อยประกอบไปด้วยดังตารางที่ 4.2

ตารางที่ 4.2 ระดับความเสี่ยงแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ

ระดับความเสี่ยง	**2.แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ**
	2.1 ระบุบุคคลที่เกี่ยวข้อง
สูง	2.1.1 ผู้บริหาร
สูง	2.1.2 ผู้ที่เกี่ยวข้อง
	2.2 ระบุการติดต่อกับเหตุการณ์ต่างๆ
สูง	2.2.1 ด้านเน็ตเวอร์
สูง	2.2.2 ด้านHardware
	2.3 ประเภทภัยพิบัติ
กลาง	2.3.1 การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก
สูง	2.3.2 การเตรียมความพร้อมห้องควบคุมระบบเครือข่ายและพร้อมรับสถานการณ์ภัยจากการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ โจมตี ระบบเครือข่าย(Form Audit Failed)
สูง	2.3.3 การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย
สูง	2.3.4 การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุน้ำท่วม
สูง	2.3.5 การเตรียมความพรอมรับสถานการณภัยจากไวรัส
ต่ำ	2.3.6 การเตรียมความพร้อมรับสถานการณภัยจากแผ่นดินไหว
สูง	2.4 เมื่อเกิดเหตุไฟไหม้
สูง	2.5 การกู้ระบบและต้องมีผู้ตรวจสอบว่าระบบใช้ได้จริง
กลาง	2.6 จำเป็นต้องมี DR Site
สูง	2.7 ระยะห่างจากพื้นที่เก็บสำรองระบบสารสนเทศเกิน 3 กม.

3) การจัดการและสิทธิของผู้ใช้งานอีเมล์ โดยมีระดับความเสี่ยงกระบวนการย่อยประกอบไปด้วยดังตารางที่ 4.3

ตารางที่ 4.3 ระดับความเสี่ยงการจัดการและสิทธิของผู้ใช้งานอีเมล์

ระดับความเสี่ยง	**3 การจัดการและสิทธิของผู้ใช้งานอีเมล์**
	1.การเพิ่ม
สูง	1.1 อนุมัติส่งรายชื่อพนักงานใหม่
สูง	1.2 อนุมัติส่งรายกลุ่ม
สูง	1.3 สร้างตามรายการอีเมล์ที่ได้รับการอนุมัติ
	2.การแก้ไข
สูง	2.1 ผู้แจ้งได้รับอนุมัติจากผู้มีอำนาจของฝ่ายนั้นๆ เพื่อแก้ไขชื่ออีเมล์
สูง	2.2 แก้ไขอีเมล์ที่ได้รับการอนุมัติ
	3.การลบ
สูง	3.1 อนุมัติส่งรายชื่อพนักงานลาออก
สูง	3.2 ลบรายการกลุ่มอีเมล์
สูง	3.3 ลบรายการอีเมล์
	4.การทบทวน
สูง	4.1 รายการอีเมล์ให้ผู้มีอำนาจของฝ่ายนั้นๆ ทบทวนและรับทราบ
สูง	4.2 รายการอีเมล์ในกลุ่มต่างๆ ให้ผู้มีอำนาจของฝ่ายนั้นๆ ทบทวนและรับทราบ
สูง	4.3 รายการอีเมล์ฟอร์เวิร์ดให้ผู้มีอำนาจของฝ่ายนั้นๆ ทบทวนและรับทราบ

4) การจัดเก็บลิขสิทธิ์ซอฟต์แวร์/ทะเบียนคุมลิขสิทธิ์โปรแกรมคอมพิวเตอร์ โดยมีระดับความเสี่ยงกระบวนการย่อยประกอบไปด้วยดังตารางที่ 4.4

ตารางที่ 4.4 ระดับความเสี่ยงการจัดเก็บลิขสิทธิ์ซอฟต์แวร์/ทะเบียนคุมลิขสิทธิ์โปรแกรมคอมพิวเตอร์

ระดับความเสี่ยง	**4 การจัดเก็บลิขสิทธิ์ซอฟต์แวร์/ทะเบียนคุมลิขสิทธิ์โปรแกรมคอมพิวเตอร์**
ต่ำ	1 ทำทะเบียนจัดเก็บลิขสิทธิ์ซอฟต์แวร์เหมือนมีการจัดซื้อซอฟต์แวร์ใหม่
ต่ำ	2 ทบทวนต่ออายุลิขสิทธิ์ซอฟต์แวร์และดำเนินการตาม (ข้อที่ 1)
ต่ำ	3 จัดเก็บเอกสารไปยังสถานที่อนุมัติโดยผู้บริหาร

5) สำรองข้อมูล/ฟื้นฟู ฐานข้อมูลของ ซอต์ฟแวร์หลัก โดยมีระดับความเสี่ยงกระบวนการย่อยประกอบไปด้วยดังตารางที่ 4.5

ตารางที่ 4.5 ระดับความเสี่ยงสำรองข้อมูล/ฟื้นฟู ฐานข้อมูลของ ซอต์ฟแวร์หลัก

ระดับความเสี่ยง	5 สำรองข้อมูล/ฟื้นฟู ฐานข้อมูลของ ซอต์ฟแวร์หลัก
	1.สำรองฐานข้อมูล
สูง	5.1.1 กำหนดสำรองไฟล์ข้อมูลประจำวัน
สูง	5.1.2 เข้ารหัสไฟล์ข้อมูล
สูง	5.1.3 ตรวจสอบการสำรองไฟล์ข้อมูลครบถ้วนถูกต้อง
	2.การฟื้นฟูฐานข้อมูล
สูง	5.2.1 ฟื้นฟูฐานข้อมูลอย่างน้อย 2 ครั้ง/ปี
สูง	5.2.2 ตรวจสอบการฟื้นฟูฐานข้อมูลโดยฝ่ายที่รับผิดชอบโดยตรง
	3.สถานที่จัดเก็บ
กลาง	5.3.1 กำหนดสถานที่จัดเก็บไฟล์ข้อมูลควรข้างไกล 3 กม.
สูง	5.3.2 ฟอร์มยืนยันการจัดเก็บระหว่างฝ่ายไอทีและผู้จัดเก็บ
	4.อุปกรณ์จัดเก็บ
กลาง	5.4.1 กำหนดประเภทอุปกรณ์จัดเก็บตามนโยบายด้านไอที
กลาง	5.4.2 กำหนดช่วงเวลาการทำลายอุปกรณ์จัดเก็บตามนโยบายด้านไอที

6) การสอบทานรหัสและสิทธิของผู้ใช้งานระบบหลัก โดยมีระดับความเสี่ยงกระบวนการย่อยประกอบไปด้วยดังตารางที่ 4.6

ตารางที่ 4.6 ระดับความเสี่ยงการสอบทานรหัสและสิทธิของผู้ใช้งานระบบหลัก

ระดับความเสี่ยง	6 การสอบทานรหัสและสิทธิของผู้ใช้งานระบบหลัก
	1 สอบทานสิทธิ
สูง	6.1.1 สอบทานสิทธิการเข้าถึงโมดูลที่เกี่ยวข้องโดยหัวหน้าของฝ่ายนั้นๆ
สูง	6.1.2 สอบทานสิทธิเมื่อพนักงานเริ่มทำงานทันที
สูง	6.1.3 สอบทานสิทธิเมื่อโอนย้ายทันที
สูง	6.1.4 สอบทานสิทธิเมื่อลาออกทันที
สูง	6.1.5 สอบทานสิทธิประจำเดือนเป็นอย่างน้อย
	2 สอบทานรหัส
สูง	6.2.1 กำหนดช่วงเวลาการเปลี่ยนรหัสตามนโยบายด้านไอที
สูง	6.2.2 รูปแบบรหัสเป็นไปตามนโยบายบริษัท

7) การตรวจสอบและสิทธิของผู้ใช้งานสินทรัพย์ด้านไอที โดยมีระดับความเสี่ยงกระบวนการย่อยประกอบไปด้วยดังตารางที่ 4.7

ตารางที่ 4.7 ระดับความเสี่ยงการตรวจสอบและสิทธิของผู้ใช้งานสินทรัพย์ด้านไอที

ระดับความเสี่ยง	7 การตรวจสอบและสิทธิของผู้ใช้งานสินทรัพย์ด้านไอที
	1.สอบทานสิทธิ
สูง	7.1.1 สอบทานสิทธิการเข้าถึงโมดูลที่เกี่ยวข้องโดยหัวหน้าของฝ่ายนั้นๆ
สูง	7.1.2 สอบทานสิทธิเมื่อพนักงานเริ่มทำงานทันที
สูง	7.1.3 สอบทานสิทธิเมื่อโอนย้ายทันที
สูง	7.1.4 สอบทานสิทธิเมื่อลาออกทันที
สูง	7.1.5 สอบทานสิทธิประจำเดือนเป็นอย่างน้อย
	2.สอบทานรหัส
สูง	7.2.1 กำหนดช่วงเวลาการเปลี่ยนรหัสตามนโยบายด้านไอที
สูง	7.2.2 รูปแบบรหัสเป็นไปตามนโยบายบริษัท

8) ระดับในการเข้าถึงระบบงานอินเตอร์เน็ต โดยมีระดับความเสี่ยงกระบวนการย่อยประกอบไปด้วยดังตารางที่ 4.8

ตารางที่ 4.8 ระดับความเสี่ยงของระดับในการเข้าถึงระบบงานอินเตอร์เน็ต

ระดับความเสี่ยง	**8 ระดับในการเข้าถึงระบบงานอินเตอร์เน็ต**
กลาง	1. ระบบที่ใช้แสดงตัวตนในการเข้าใช้อินเทอร์เน็ตตาม พ.ร.บ. ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์พ.ศ.2550
สูง	2. ฟอร์มการลงทะเบียนการใช้อินเทอร์เน็ตจากบุคคลภายนอก
ต่ำ	3. รายการการเข้าถึงเว็บไซต์ประจำเดือน
ต่ำ	4. ทดสอบการเอ็กฟอร์ตรายการเว็บไซต์ที่บุคคลเข้าใช้งานตามช่วงเวลา

9) ทบทวนสัญญาการต่อสัญญาบริการด้านไอที โดยมีระดับความเสี่ยงกระบวนการย่อยประกอบไปด้วยดังตารางที่ 4.9

ตารางที่ 4.9 ระดับความเสี่ยงทบทวนสัญญาการต่อสัญญาบริการด้านไอที

ระดับความเสี่ยง	**9 ทบทวนสัญญาการต่อสัญญาบริการด้านไอที**
ต่ำ	1. แผนการต่อสัญญาผู้ให้บริการที่เกี่ยวข้องกับฝ่ายไอทีทั้งหมด
ต่ำ	2. รายการอุปกรณ์ที่อยู่ในประกันประจำเดือน

10) การดำเนินงานโครงงานด้านไอทีโดยมีระดับความเสี่ยงกระบวนการย่อยประกอบไปด้วยดังตารางที่ 4.10

ตารางที่ 4.10 ระดับความเสี่ยงการดำเนินงานโครงงานด้านไอที

ระดับความเสี่ยง	**10 ทบทวนสัญญาการต่อสัญญาบริการด้านไอที**
	1 ภายในองค์กร
สูง	1.1 ฟอร์มผู้ใช้ระบบงานกรอกรายละเอียดลงในเอกสารการขอแก้ไขระบบงาน
สูง	1.2 มีผู้มีอำนาจ และผู้ดูแลระบบงานตรวจสอบความถูกต้องของเอกสาร พร้อมลงลายมือชื่ออนุมัติและวันที่กำกับ
สูง	1.3 พนักงานแผนก IT ตรวจสอบ และผู้จัดการแผนก IT ลงลายมือชื่ออนุมัติ และวันที่กำกับ ก่อนการดำเนินการแก้ไขระบบงานบนระบบทดสอบ
สูง	1.4 เจ้าหน้าที่ ดำเนินการพัฒนาระบบงานตามรายละเอียดในเอกสาร บนระบบทดสอบ (Test Environment)
สูง	1.5 ผู้มีอำนาจ อนุมัติผลการทดสอบ ลงลายมือชื่อ และวันที่
สูง	1.6 ฝ่าย IT Admin อนุมัติผลการทดสอบระบบงาน อนุมัติการขึ้นระบบงานเพื่อใช้งานจริงผ่านแบบฟอร์ม ขอขึ้นระบบ
สูง	1.7 ฝ่าย IT นำระบบงานที่ได้รับการพัฒนาหรือแก้ไขและผ่านการทดสอบจากผู้ใช้งานขึ้นสู่ระบบใช้งานจริง และลงลายมือชื่อผู้นำขึ้นสู่ระบบใช้งานจริง ในส่วนการนำขึ้นระบบใช้งานจริง
	2. ผู้ให้บริการภายนอก
สูง	2.1ฟอร์มผู้ใช้ระบบงานกรอกรายละเอียดลงในเอกสารการขอแก้ไขระบบงาน
สูง	2.2 มีผู้มีอำนาจ และผู้ดูแลระบบงานตรวจสอบความถูกต้องของเอกสาร พร้อมลงลายมือชื่ออนุมัติและวันที่กำกับ
สูง	2.1 ตัวแทนของบริษัทภายนอกลงลายมือชื่อและวันที่กำกับเพื่อเป็นหลักฐานในการทำงาน รวมทั้งให้กำหนดระยะเวลาในการแก้ไขระบบงาน

11) การบำรุงรักษาเชิงป้องกันสินทรัพย์ไอทีและตรวจสอบโปรแกรมลิขสิทธ์ โดยมีระดับความเสี่ยงกระบวนการย่อยประกอบไปด้วยดังตารางที่ 4.11

ตารางที่ 4.11 ระดับความเสี่ยงการบำรุงรักษาเชิงป้องกันสินทรัพย์ไอทีตรวจสอบโปรแกรมลิขสิทธ์

ระดับความเสี่ยง	**11 การบำรุงรักษาเชิงป้องกันสินทรัพย์ไอทีและตรวจสอบโปรแกรมลิขสิทธ์**
	1 ทะเบียนทรัพย์สิน/โปรแกรมลิขสิทธ์
สูง	1.1 จัดทำแผนประจำปีตรวจสอบทุกสินทรัพย์และโปรแกรมลิขสิทธ์
	2. ทะเบียนทรัพย์สิน
สูง	2.1 ปรับปรุงบุคคลที่รับผิดชอบเมื่อมีการตรวจความถูกต้อง
สูง	2.2 ปรับปรุงผู้รับผิดสินทรัพย์เมื่อเริ่มงานใหม่
สูง	2.3 ปรับปรุงผู้รับผิดสินทรัพย์เมื่อโอนย้าย
สูง	2.4 ปรับปรุงผู้รับผิดสินทรัพย์เมื่อ ลาออก
กลาง	2.5 มีการแจ้งหัวหน้าเป็นประจำเดือน/เริ่มงานใหม่/ลาออก/โอนย้าย
กลาง	2.6 ทุกสินทรัพย์ต้องอ้างอิงรหัสสินทรัพย์ของฝ่ายบัญชี
	3 โปรแกรมลิขสิทธ์
สูง	3.1 ตรวจโปรแกรมตามการอนุมัติโครงสร้างผังพนักงาน
สูง	3.2 ตรวจโปรแกรมผิดลิขสิทธิ์
สูง	3.3 มีการแจ้งหัวหน้าเป็นประจำเดือน/เริ่มงานใหม่/ลาออก/โอนย้าย
สูง	3.4 แจ้งหัวหน้าเมื่อพบโปรแกรมผิดลิขสิทธิ์และทำการลบ
	4 การบำรุงรักษาเชิงป้องกัน
กลาง	4.1 ทำความสะอาดคอมพิวเตอร์และอุปการณ์ต่อพ่วง
กลาง	4.2 ตรวจสอบสภาพทั่วไปและตรวจสอบความชำรุดของอุปกรณ์

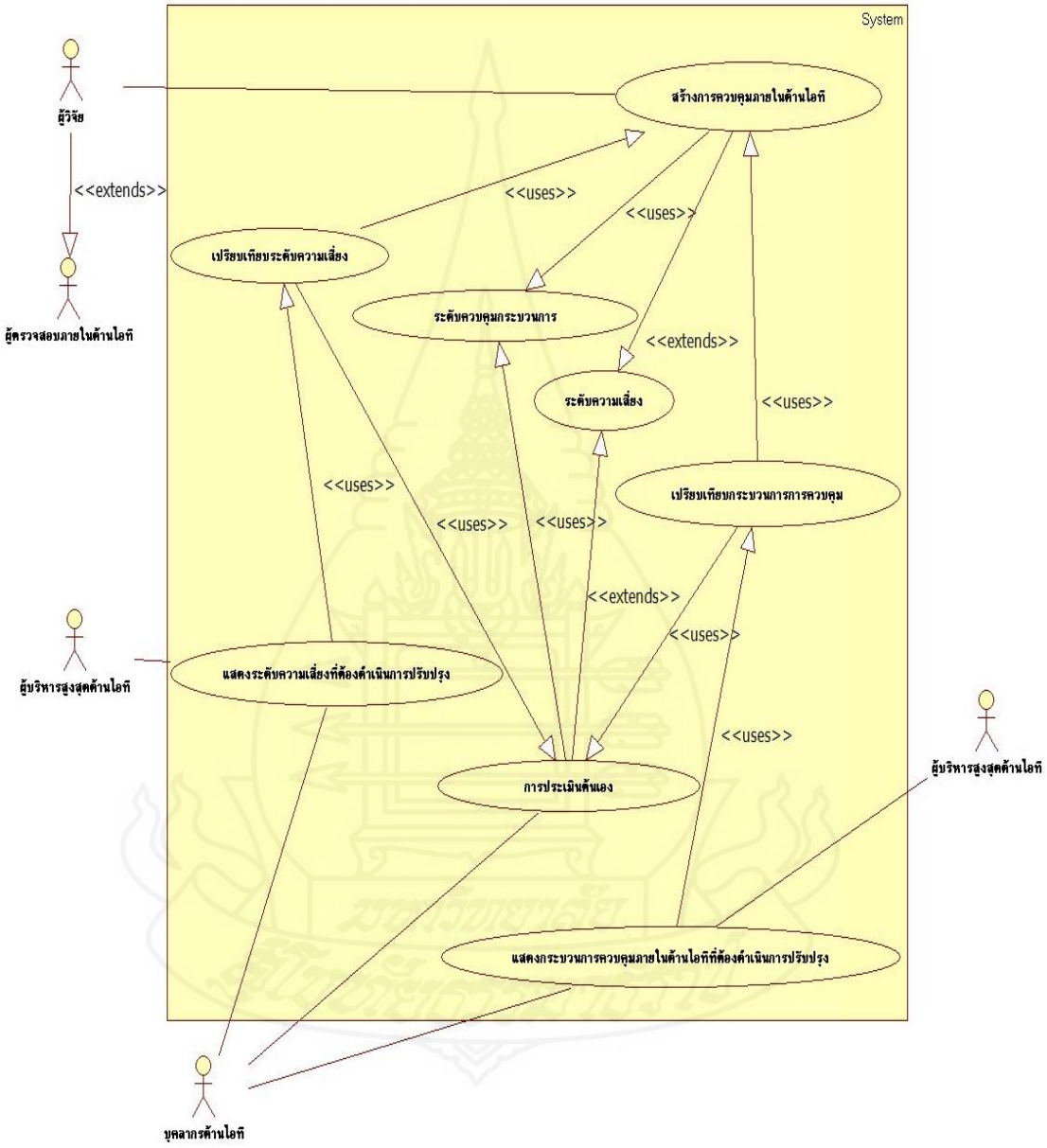
12) สิทธิ์การใช้ซอฟต์แวร์ตามระดับโครงสร้างบุคลากรและลักษณะงานและฟอร์มขออนุมัติขอใช้สิทธิ์ใช้ซอฟต์แวร์เพิ่มเติม โดยมีระดับความเสี่ยงกระบวนการย่อยประกอบไปด้วยดังตารางที่ 4.12

ตารางที่ 4.12 ระดับความเสี่ยงสิทธิ์การใช้ซอฟต์แวร์ตามระดับโครงสร้างบุคลากรและลักษณะงานและฟอร์มขออนุมัติขอใช้สิทธิ์ใช้ซอฟต์แวร์

ระดับความเสี่ยง	**12 สิทธิ์การใช้ซอฟต์แวร์ตามระดับโครงสร้างบุคลากรและลักษณะงานและฟอร์มขออนุมัติขอใช้สิทธิ์ใช้ซอฟต์แวร์เพิ่มเติม**
	1 การติดตั้งโปรแกรม
กลาง	1.1 ฟอร์มโครงสร้างโปรแกรมที่สามารถติดตั้งตามผังพนักงาน
กลาง	1.2 ติดตั้งโปรแกรมตามโครงสร้างโปรแกรมเมื่อเริ่มงานใหม่
กลาง	1.3 ปรับปรุงติดตั้งโปรแกรเมื่อพนักงานถูกโอนย้าย
กลาง	1.4 เมื่อพนักงานลาออก ถอนการติดตั้งตามโครงสร้างโปรแกรม
	2 อนุมัติติดตั้งโปรแกรมเพิ่ม
กลาง	2.1 ฟอร์มอนุมัติติดตั้งโปรแกรมเพิ่มตามการอนุมัติโครงสร้างผังพนักงาน

2. การออกแบบระบบสนับสนุน

2.1 แผนภาพยูสเคส (Use Case Diagram)



ภาพที่ 4.3 แผนภาพยูสเคสขบวนการประเมินการควบคุมภายในด้านไอที

นิยามศัพท์เฉพาะ

Use Case Diagram หมายถึง เป็นแผนภาพที่ใช้ที่แสดงปฏิสัมพันธ์ระหว่างระบบงานและสิ่งที่อยู่นอกระบบงาน แสดงให้เห็นถึงส่วนประกอบทั้งหมด หรือภาพรวมของระบบ

 Actor หมายถึง ผู้เกี่ยวข้องของระบบ

 Use Case หมายถึง หน้าที่หรือขบวนการของกิจกรรมที่ระบบต้องดำเนินการ

System หมายถึง เส้นแบ่งขอบเขตระหว่าง Use Case และ Actor

<< uses>> หมายถึง Use Caseที่ถูกเรียกใช้ กิจกรรมใน Use Case เกิดขึ้นทุกครั้ง

<< extends>> หมายถึง Use Caseที่ถูกเรียกใช้ กิจกรรมใน Use Case เกิดขึ้นเพียงบางครั้ง

“ —— “ หมายถึง เส้นที่ลากเชื่อมต่อระหว่าง Actor กับ Use Case ที่มีปฏิสัมพันธ์กัน ใช้เส้นตรงไม่มีหัวลูกศรเป็นสัญลักษณ์

“ —▷ ” หมายถึง ความสัมพันธ์แบบเรียกใช้เกิดขึ้นในกรณีที่ Use Case หนึ่งไปเรียกหรือดึงกิจกรรมของอีก Use Case หนึ่งมาใช้เพื่อให้กิจกรรมนั้นเกิดขึ้นจริง ลักษณะการทำงานคือลูกศรจะชี้ไป Use Case ที่ถูกเรียกใช้งาน

คำอธิบายแผนภาพ Use Case

อธิบาย Actor

Actor Name: ผู้วิจัย

คำอธิบาย: ผู้ดำเนินการวิจัยผู้สร้างองค์ความรู้และสัมภาษณ์ผู้ตรวจสอบบัญชีเพื่อตรวจทานองค์ความรู้ให้เชื่อถือได้เพื่อใช้เป็นเกณฑ์สำหรับการประเมินฯ

Actor Name: ผู้ตรวจสอบภายในด้านไอที

คำอธิบาย: ผู้ตรวจสอบบัญชี ในองค์กรที่ได้รับความเห็นชอบ จากสำนักงานก.ล.ต. (สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์)

Actor Name: ผู้บริหารสูงสุดด้านไอที

คำอธิบาย: ผู้มีอำนาจสูงสุดด้านไอทีที่ต้องรับทราบปัญหาในกระบวนการการควบคุมภายในเพื่อดำเนินการแก้ไขและประสานงานกับหน่วยงานผู้ตรวจสอบบัญชี

Actor Name: บุคลากรด้านไอที

คำอธิบาย: บุคลากรด้านไอทีที่มีหน้าที่ในส่วนจัดทำเอกสารไดแก่ คู่มือปฏิบัติงาน เอกสารที่เป็นงานประจำ เอกสารไอที

อธิบาย Use Case

ตารางที่ 4.13 ยูสเคสสร้างการควบคุมภายในด้านไอที

Use Case ID:	1
Use Case Title:	สร้างการควบคุมภายในด้านไอที
Primary Actor:	ผู้วิจัย
Stakeholder Actor:	ผู้ตรวจสอบภายในด้านไอที
Main Flow:	องค์ความรู้ของกระบวนการการควบคุมภายในด้านเทคโนโลยีสารสนเทศของธุรกิจกลุ่มทรัพยากรที่ได้ตรวจทานจากผู้ตรวจสอบ

ตารางที่ 4.14 ยูสเคสระดับควบคุมขบวนการ

Use Case ID:	2
Use Case Title:	ระดับควบคุมขบวนการ
Primary Actor:	-
Stakeholder Actor:	-
Main Flow:	การควบคุมกระบวนการของเอกสารประเภท คู่มือปฏิบัติงาน เอกสาร ที่เป็นงานประจำ และเอกสารไอที

ตารางที่ 4.15 ยูสเคสระดับความเสี่ยง

Use Case ID:	3
Use Case Title:	ระดับความเสี่ยง
Primary Actor:	-
Stakeholder Actor:	-
Main Flow:	การควบคุมระดับความเสี่ยงของกระบวนการย่อยภายในเอกสารประเภทคู่มือปฏิบัติงาน

ตารางที่ 4.16 ยูสเคสการประเมินตนเอง

Use Case ID:	4
Use Case Title:	การประเมินตนเอง
Primary Actor:	บุคลากรด้านไอที
Stakeholder Actor:	-
Main Flow:	ฝ่ายไอทีนำข้อมูลของการควบคุมภายในด้านไอทีของตนเองป้อนเข้าสู่ระบบ

ตารางที่ 4.17 ยูสเคสเปรียบเทียบระดับความเสี่ยงของกระบวนการย่อย

Use Case ID:	5
Use Case Title:	เปรียบเทียบระดับความเสี่ยงของกระบวนการย่อย
Primary Actor:	-
Stakeholder Actor:	-
Main Flow:	ขบวนการของระบบประเมินตนเองฯจะนำความเสี่ยงของกระบวนการย่อย หัวข้อใดต้องจัดทำเพิ่มหรือต้องปรับเปลี่ยนให้เหมาะสมตามกรอบองค์ความรู้

ตารางที่ 4.18 ยูสเคสแสดงระดับความเสี่ยงที่ต้องดำเนินการปรับปรุง

Use Case ID:	6
Use Case Title:	แสดงระดับความเสี่ยงที่ต้องดำเนินการปรับปรุง
Primary Actor:	บุคลากรไอที
Stakeholder Actor:	ผู้บริการสูงสุดด้านไอที
Main Flow:	แสดงระดับความเสี่ยงที่ต้องดำเนินการปรับปรุงให้แก่บุคลากรไอทีและผู้บริการสูงสุดด้านไอที

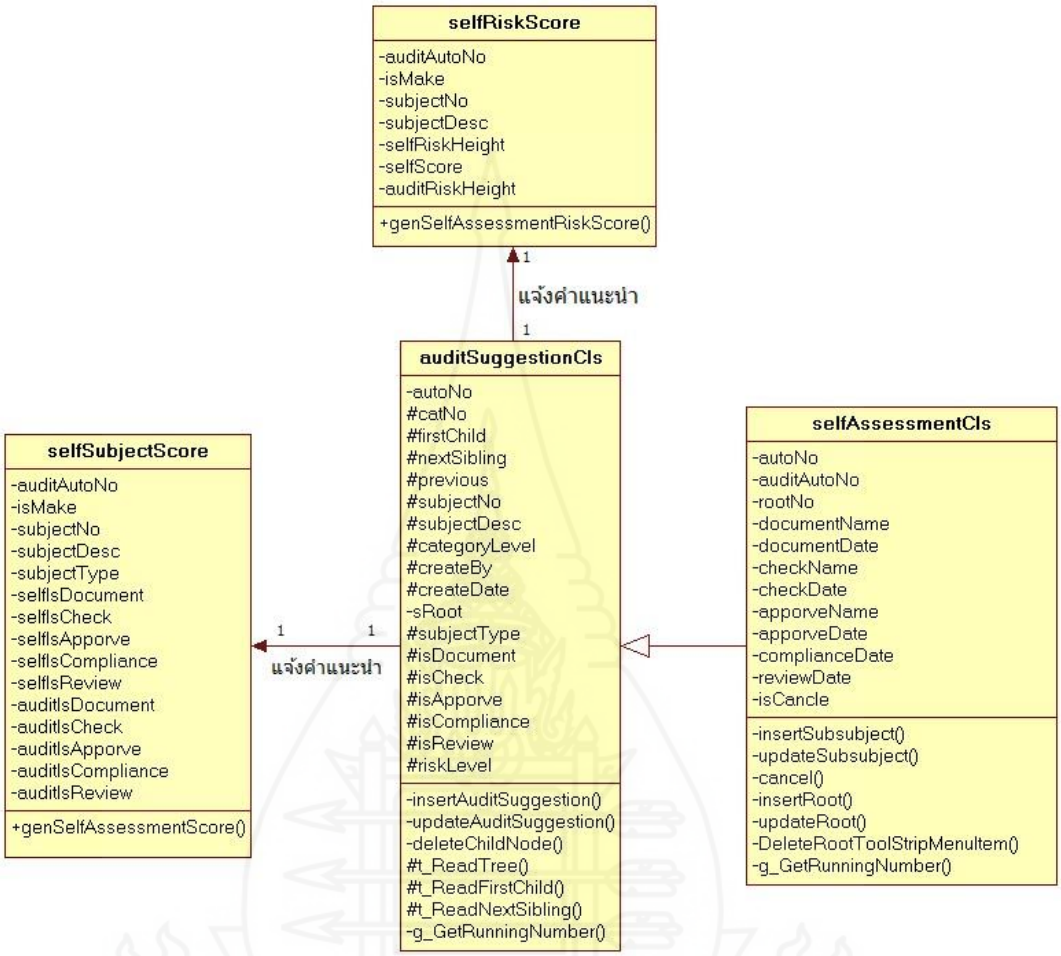
ตารางที่ 4.19 ยูสเคสเปรียบเทียบกระบวนการการควบคุมภายในด้านไอที

Use Case ID:	7
Use Case Title:	เปรียบเทียบกระบวนการการควบคุมภายในด้านไอที
Primary Actor:	-
Stakeholder Actor:	-
Main Flow:	ขบวนการประเมินตนเองฯ จะนำการควบคุม กระบวนการตรวจสอบภายในด้านไอที กระบวนการ หัวข้อใดต้องจัดทำเพิ่มหรือต้องปรับเปลี่ยนให้เหมาะสม
Exceptional Flow:	-

ตารางที่ 4.20 ยูสเคสแสดงกระบวนการควบคุมภายในด้านไอทีที่ต้องดำเนินการปรับปรุง

Use Case ID:	8
Use Case Title:	แสดงกระบวนการควบคุมภายในด้านไอทีที่ต้องดำเนินการปรับปรุง
Primary Actor:	บุคลากรไอที
Stakeholder Actor:	ผู้บริหารสูงสุดด้านไอที
Main Flow:	แสดงองค์ความรู้ตามกรอบโคบิตกระบวนการควบคุมภายในด้านไอที ที่ต้องดำเนินการปรับปรุงให้แก่ บุคลากรด้านไอทีและผู้บริหารสูงสุดด้านไอที
Exceptional Flow:	-

2.2 แผนภาพคลาสไดอะแกรม(Class Diagram)



ภาพที่ 4.4 แผนภาพคลาสไดอะแกรม

นิยามศัพท์เฉพาะ

แผนภาพคลาสไดอะแกรม หมายถึง มุมมองของระบบที่เน้นโครงสร้างของวัตถุ รวมทั้งคลาสของวัตถุ (Class) ความสัมพันธ์ระหว่างคลาส (Relationship) แอททริบิวต์ (Attribute) และโอเปอเรชัน (Operation)

แอททริบิวต์ หมายถึง ข้อมูลที่เป็นคุณสมบัติของคลาส ซึ่งก็คือข้อมูลที่สนใจจะจัดเก็บและนำมาใช้ในระบบ สามารถกำหนดระดับของการเข้าถึงข้อมูลเหล่านี้ได้

โอเปอเรชัน หมายถึง โปรแกรมหรือหน้าที่การทำงานของคลาส

 หมายถึง การเขียนสัญลักษณ์แสดง Association ของคลาสสองคลาสนั้นแสดงด้วยเส้นตรง ลากเชื่อมระหว่างคลาสทั้งสอง โดยเส้นที่ลากเสื่อมนั้นจะต้องมีชื่อของ Association กำกับด้วยเสมอ

 หมายถึง การสืบทอดคุณสมบัติ(Generalization) คลาสหนึ่งสามารถที่จะสืบทอดคุณสมบัติจากอีกคลาสหนึ่งได้ คลาสที่เป็นผู้รับการสืบทอดจะมีคุณสมบัติเหมือนคลาสที่เป็นผู้ให้การสืบทอด โดยลูกศรชี้ไปที่คลาสใดคลาสนั้นคือผู้ให้สืบทอดคุณสมบัติ

การเขียนสัญลักษณ์แทน Class สิ่งที่ต้องคำนึงถึงอีกสิ่งหนึ่งคือระดับการเข้าถึงเรียกสัญลักษณ์ที่ใช้แทนการเข้าถึงนี้ว่า Visibility แบ่งออกได้เป็น 3 ประเภท ประกอบด้วย

Public มีสัญญาลักษณ์คือ“+” แอททริบิวหรือโอเปอเรเตอร์ สามารถเรียกใช้ได้ ทั้งภายในและภายนอกคลาส

Private มีสัญญาลักษณ์คือ “-” แอททริบิวหรือโอเปอเรเตอร์ สามารถเรียกได้เฉพาะในคลาสไม่สามารถเห็นได้เลยจากภายนอก

Protected มีสัญญาลักษณ์คือ“#” แอททริบิวหรือโอเปอเรเตอร์ สามารถเรียกได้เฉพาะในคลาส ไม่สามารถเห็นจากภายนอกแต่เป็นส่วนที่สามารถส่งต่อให้ Inherited Class ได้เท่านั้น

อธิบายคลาส

ตารางที่ 4.21 Class auditSuggestionCls

Class ID:	1
Use Case Title:	auditSuggestionCls
Description:	องค์ความรู้ของกระบวนการการควบคุมภายในด้านเทคโนโลยีสารสนเทศของธุรกิจกลุ่มทรัพยากรที่ได้ตรวจทานจากผู้ตรวจสอบ
Attributes	
autoNo	รหัส
catNo	ตำแหน่งของหัวข้อ
firstChild	AutoNo ของโหนดที่เป็นลูก
nextSibling	AutoNo ของโหนดระดับเดียวกันตำแหน่งถัดไป

ตารางที่ 4.21 (ต่อ)

Class ID:	1
Use Case Title:	auditSuggestionCls
Description:	องค์ความรู้ของกระบวนการการควบคุมภายในด้านเทคโนโลยีสารสนเทศของธุรกิจกลุ่มทรัพยากรที่ได้ตรวจทานจากผู้ตรวจสอบ
previous	AutoNoของโหนดที่เป็นแม่
subjectNo	เลขที่หัวข้อเอกสาร
Attributes	
subjectDesc	ชื่อหัวข้อกระบวนการ
categoryLevel	ตำแหน่งของโหนด
createDate	วันที่สร้าง
sRoot	AutoNoของโหนดระดับสูงสุด
subjectType	ประเภทของเอกสาร
isDocument	การจัดทำเอกสาร
isCheck	การตรวจสอบเอกสาร
isApporve	การอนุมัติเอกสาร
isCompliance	การประกาศเพื่อบังคับใช้เอกสาร
isReview	การทบทวนเอกสาร
riskLevel	ระดับความเสี่ยง
Operation	
insertAuditSuggestion()	โอเปอเรชันการเพิ่มเรคคอร์ดใหม่
updateAuditSuggestion()	โอเปอเรชันการแก้ไขเรคคอร์ด
deleteChildNode()	โอเปอเรชันการเรคคอร์ด
t_ReadTree()	การอ่านข้อมูลเริ่มต้นในการสร้างTree
t_ReadFirstChild()	การอ่านข้อมูลโหนดลูก
t_ReadNextSibling()	การอ่านข้อมูลชั้นเดียวระดับถัดไป
g_GetRunningNumber()	สร้างรหัสใหม่

ตารางที่ 4.22 Class selfAssessmentCls

Class ID:	2
Use Case Title:	selfAssessmentCls
Description:	นำข้อมูลของการควบคุมภายในด้านไอทีของตนเองป้อนเข้าสู่ระบบ
Attributes	
autoNo	รหัส
auditAutoNo	รหัสตาราง AuditSuggestion
Attributes	
isCancle	สร้างเงื่อนไขการยกเลิก
Operation	
insertSubsubject()	โอเปอเรชั่นการเพิ่มเรคคอร์ดใหม่
updateSubsubject()	โอเปอเรชั่นการแก้ไขเรคคอร์ด
DeleteChildNode()	โอเปอเรชั่นการยกเลิกเรคคอร์ด
insertRoot()	โอเปอเรชั่นการเพิ่มชุดเรคคอร์ดของกรอบการควบคุมภายในด้านไอที ธุรกิจทรัพยากร
updateRoot()	โอเปอเรชั่นการเปลี่ยนชื่อ Root
DeleteRootToolStripMenuItem()	โอเปอเรชั่นการลบชุดเรคคอร์ด
g_GetRunningNumber()	สร้างรหัสใหม่

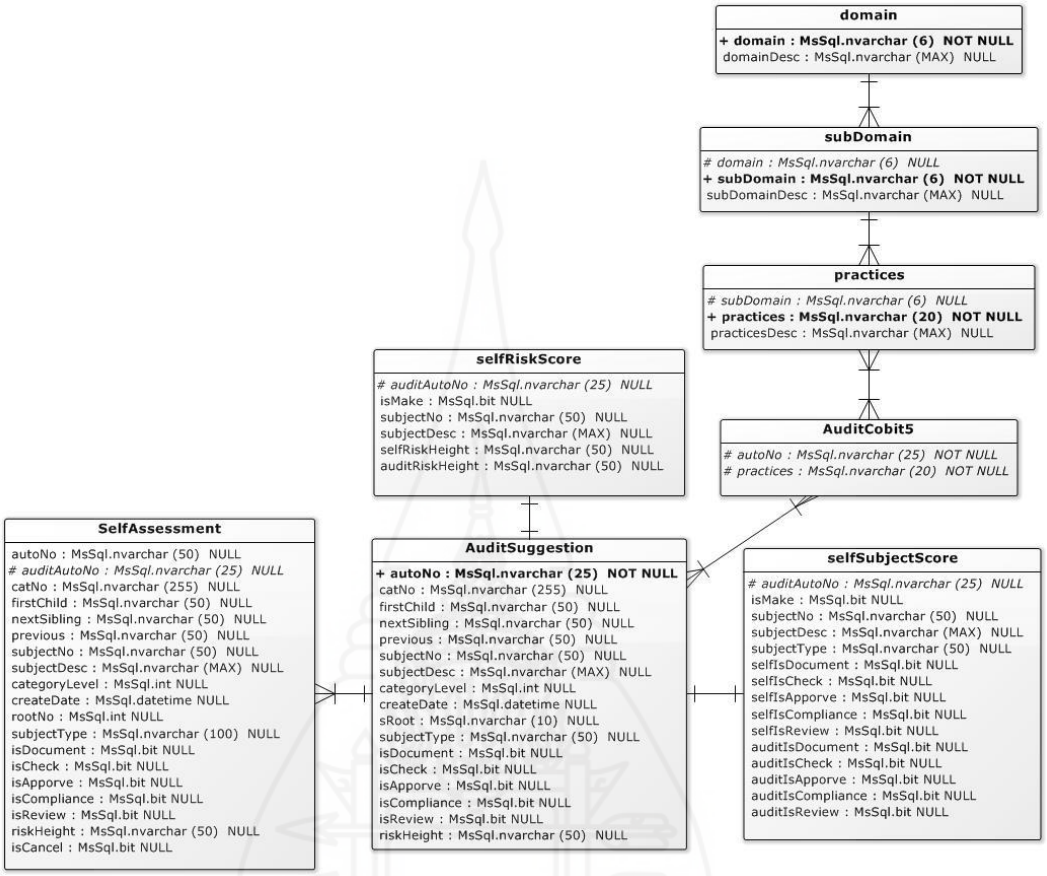
ตารางที่ 4.23 Class selfSubjectScore

Class ID:	3
Use Case Title:	selfSubjectScore
Description:	ขบวนการประเมินต้นเองฯจะนำการควบคุมกระบวนการตรวจสอบภายในด้านไอทีกระบวนการหัวข้อใดต้องจัดทำเพิ่มหรือต้องปรับเปลี่ยนให้เหมาะสม
Attributes	
auditAutoNo	รหัสตาราง AuditSuggestion
isMake	การตรวจสอบกระบวนการใดยังไม่จัดทำ
subjectNo	เลขที่หัวข้อเอกสาร
subjectDesc	ชื่อหัวข้อกระบวนการ
subjectType	ประเภทของเอกสาร
selfIsDocument	การจัดทำเอกสารผู้ใช้งานระบบประเมิน
selfIsCheck	การตรวจสอบเอกสารผู้ใช้งานระบบประเมิน
selfIsApporve	การอนุมัติเอกสารผู้ใช้งานระบบประเมิน
selfIsCompliance	การประกาศเพื่อบังคับใช้เอกสารผู้ใช้งานระบบประเมิน
selfIsReview	การทบทวนเอกสารผู้ใช้งานระบบประเมิน
Attributes	
auditIsDocument	การจัดทำเอกสารที่ได้จากองค์ความรู้
auditIsCheck	การตรวจสอบเอกสารที่ได้จากองค์ความรู้
auditIsApporve	การอนุมัติเอกสารที่ได้จากองค์ความรู้
auditIsCompliance	การประกาศเพื่อบังคับใช้เอกสารที่ได้จากองค์ความรู้
auditIsReview	การทบทวนเอกสารที่ได้จากองค์ความรู้
Operation	
genSelfAssessmentScore()	โอเปอเรชั่นการเปรียบเทียบกระบวนการของผู้ใช้งานระบบประเมินกับกรอบองค์ความรู้

ตารางที่ 4.24 Class selfRiskScore

Class ID:	4
Use Case Title:	selfRiskScore
Description:	ขบวนการของระบบประเมินตนเองฯจะนำความเสี่ยงของกระบวนการย่อย หัวข้อใดต้องจัดทำเพิ่มหรือต้องปรับเปลี่ยนให้เหมาะสมตามกรอบขององค์ความรู้
Attributes	
auditAutoNo	รหัสตาราง AuditSuggestion
isMake	การตรวจสอบความเสี่ยงกระบวนการย่อยใดยังไม่จัดทำ
subjectNo	เลขที่หัวข้อเอกสาร
subjectDesc	ชื่อหัวข้อกระบวนการ
selfRiskHeight	ความเสี่ยงผู้ใช้งานระบบประเมิน
auditRiskHeight	ความเสี่ยงที่ได้จากองค์ความรู้
Operation	
genSelfAssessmentRiskScore()	โอเปอเรชั่นการเปรียบเทียบความเสี่ยงกระบวนการย่อยของผู้ใช้งานระบบประเมินกับกรอบองค์ความรู้

2.3 แผนภาพอีอาร์ (ER-Diagram)



ภาพที่ 4.5 แผนภาพอีอาร์ (ER-Diagram)

2.4 ดาต้าดิกชันนารี่ (Data Dictionary)

ตารางที่ 4.25 ตารางองค์ความรู้กรอบควบคุมภายในด้านไอทีธุรกิจทรัพยากรตามกรอบโคบิต

SelfAssessment ตารางองค์ความรู้กรอบควบคุมภายในด้านไอทีธุรกิจทรัพยากรตามกรอบโคบิต					
Attribute	**Data Type**	**Allow Nulls**	**Description**	**Example**	**Key**
AutoNo	int	Unchecked	รหัส รูปแบบ Cxxxxxxx	C0000194	PK
CatNo	nvarchar(255)	Unchecked	ตำแหน่งของหัวข้อ	1	
FirstChild	nvarchar(50)	Unchecked	AutoNo ของโหนดที่เป็นลูก	C0000594	
NextSibling	nvarchar(50)	Unchecked	AutoNo ของโหนดระดับเดียวกันตำแหน่งถัดไป	C0000195	
Previous	nvarchar(50)	Unchecked	AutoNo ของโหนดที่เป็นแม่	Audit	
subjectNo	nvarchar(50)	Unchecked	เลขที่หัวข้อ	1	
subjectDesc	nvarchar(255)	Unchecked	ชื่อหัวข้อกระบวนการ	นโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศ	
CategoryLevel	int	Unchecked	ตำแหน่งของโหนด		
CreateDate	datetime	Checked	วันที่สร้าง	25/6/2005 10:49	
sRoot	nvarchar(10)	Unchecked	AutoNo ของโหนดระดับสูงสุด	Audit	
subjectType	nvarchar(5)	Unchecked	ประเภทของเอกสาร	คู่มือปฏิบัติงาน	
isDocument	boolean	Checked	True มีการจัดทำ False ไม่มีการจัดทำ	TRUE	
isCheck	boolean	Checked	True ได้รับตรวจสอบ False ไม่ได้รับตรวจสอบ	TRUE	
isApporve	boolean	Checked	True ได้รับการอนุมัติ False ไม่ได้รับการอนุมัติ	TRUE	
isCompliance	boolean	Checked	True มีการบังคับใช้ False ไม่ได้มีการบังคับใช้	TRUE	
isReview	boolean	Checked	True มีการทบทวน False ไม่มีการทบทวน	TRUE	
riskHeight	nvarchar(50)	Checked	ค่าความเสี่ยง ระดับต่ำ ระดับกลาง ระดับสูง	สูง	

ตารางที่ 4.26 ตารางข้อมูลการประเมินตนเอง

SelfAssessment ตารางข้อมูลการประเมินตนเอง					
Attribute	**Data Type**	**Allow Nulls**	**Description**	**Example**	**Key**
AutoNo	int	Unchecked	รหัส รูปแบบ SAyymmxxxx	C0000194	PK
CatNo	nvarchar(255)	Unchecked	ตำแหน่งของหัวข้อ	1	
FirstChild	nvarchar(50)	Unchecked	AutoNo ของโหนดที่เป็นลูก	C0000594	
NextSibling	nvarchar(50)	Unchecked	AutoNo ของโนดระดับเดียวกัน ตำแหน่งถัดไป	C0000195	
Previous	nvarchar(50)	Unchecked	AutoNo ของโหนดที่เป็นแม่	Self1	
subjectNo	nvarchar(50)	Unchecked	เลขที่หัวข้อ	1	
subjectDesc	nvarchar(1000)	Unchecked	ชื่อหัวข้อกระบวนการ	นโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศ	
CategoryLevel	int	Unchecked	ตำแหน่งของโหนด		
CreateDate	datetime	Checked	วันที่สร้าง	25/6/2005 10:49	
EditDate	datetime	Checked	วันที่แก้ไข	25/6/2005 10:49	
sRoot	nvarchar(10)	Unchecked	AutoNo ของโหนดระดับสูงสุด	Self1	
subjectType	nvarchar(5)	Unchecked	ประเภทของเอกสาร	คู่มือปฏิบัติงาน	
isDocument	boolean	Checked	True มีการจัดทำ False ไม่มีการจัดทำ	TRUE	
isCheck	boolean	Checked	True ได้รับตรวจสอบ False ไม่ได้รับตรวจสอบ	TRUE	
isApporve	boolean	Checked	True ได้รับการอนุมัติ False ไม่ได้รับการอนุมัติ	TRUE	
isCompliance	boolean	Checked	True มีการบังคับใช้ False ไม่ได้มีการบังคับใช้	TRUE	
isReview	boolean	Checked	True มีการทบทวน False ไม่มีการทบทวน	TRUE	
riskHeight	nvarchar(50)	Checked	ค่าความเสี่ยง ระดับต่ำ ระดับกลาง ระดับสูง	สูง	
isCancel	boolean	Checked	ยกเลิกกระบวนการ หรือกระบวนการย่อยเรื่องความเสี่ยง	TRUE	

ตารางที่ 4.27 ตารางโดเมนของโคบิต

domain ตารางโดเมนของโคบิต					
Attribute	**Data Type**	**Allow Nulls**	**Description**	**Example**	**Key**
domain	nvarchar(6)	Unchecked	รหัสของโดเมนของโคบิต	APO	PK
domainDesc	nvarchar(255)	Unchecked	อธิบายความหมายของโดเมน	APO หมายถึง จัดวางแนว จัดทำแผน และ จัดระบบ	

ตารางที่ 4.28 ตารางกระบวนการของโคบิต

subdomain ตารางกระบวนการของโคบิต					
Attribute	**Data Type**	**Allow Nulls**	**Description**	**Example**	**Key**
subDomain	nvarchar(6)	Unchecked	รหัสของกระบวนการของโคบิต	APO01	PK
domain	nvarchar(6)	Unchecked	โดเมนของโคบิต	APO	
subDomainDesc	nvarchar(255)	Unchecked	อธิบายความหมายของกระบวนการ	APO01 หมายถึง บริหารจัดการกรอบการดำเนินงานการบริหารงานด้านไอที	

ตารางที่ 4.29 ตารางกระบวนการย่อยหรือแนวปฏิบัติของโคบิต

practices ตารางกระบวนการย่อยหรือแนวปฏิบัติของโคบิต					
Attribute	**Data Type**	**Allow Nulls**	**Description**	**Example**	**Key**
practices	nvarchar(20)	Unchecked	รหัสของกระบวนการย่อยหรือแนวปฏิบัติของโคบิต	APO01.01	PK
subDomain	nvarchar(6)	Unchecked	กระบวนการของโคบิต	APO01	
practicesDesc	nvarchar(255)	Unchecked	อธิบายรายละเอียดกระบวนการย่อยหรือแนวปฏิบัติของโคบิต	APO01.01 หมายถึง กำหนดโครงสร้างองค์กร	

ตารางที่ 4.30 ตารางความสัมพันธ์ระหว่างตาราง AuditSuggestion และตาราง practices

AuditCobit5 ตารางความสัมพันธ์ระหว่างตาราง AuditSuggestion และตาราง practices					
Attribute	**Data Type**	**Allow Nulls**	**Description**	**Example**	**Key**
practices	nvarchar(20)	Unchecked	รหัสของกระบวนการย่อยหรือแนวปฏิบัติของโคบิต	APO01.01	PK
AutoNo	int	Unchecked	รหัส รูปแบบ Cxxxxxxx	C0000194	PK

ตารางที่ 4.31 ตารางเปรียบเทียบกระบวนการการควบคุมภายในด้านไอที

selfSubjectScore ตารางเปรียบเทียบกระบวนการการควบคุมภายในด้านไอที

Attribute	Data Type	Allow Nulls	Descrition	Example	Key
auditAutoNo	nvarchar(25)	Unchecked	รหัส รูปแบบ Cxxxxxxx	C0000194	PK
isMake	boolean	Unchecked	การตรวจสอบกระบวนการใดยังไม่จัดทำ	FALSE	
subjectNo	nvarchar(50)	Unchecked	เลขที่หัวข้อเอกสาร	C0000594	
subjectDesc	nvarchar(50)	Unchecked	ชื่อหัวข้อกระบวนการ	1	
subjectType	nvarchar(50)	Unchecked	ประเภทของเอกสาร	นโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศ	
selfIsDocument	boolean	Unchecked	การจัดทำเอกสารผู้ใช้งานระบบประเมิน	TRUE	
selfIsCheck	boolean	Unchecked	การตรวจสอบเอกสารผู้ใช้งานระบบประเมิน	TRUE	
selfIsApporve	boolean	Unchecked	การอนุมัติเอกสารผู้ใช้งานระบบประเมิน	TRUE	

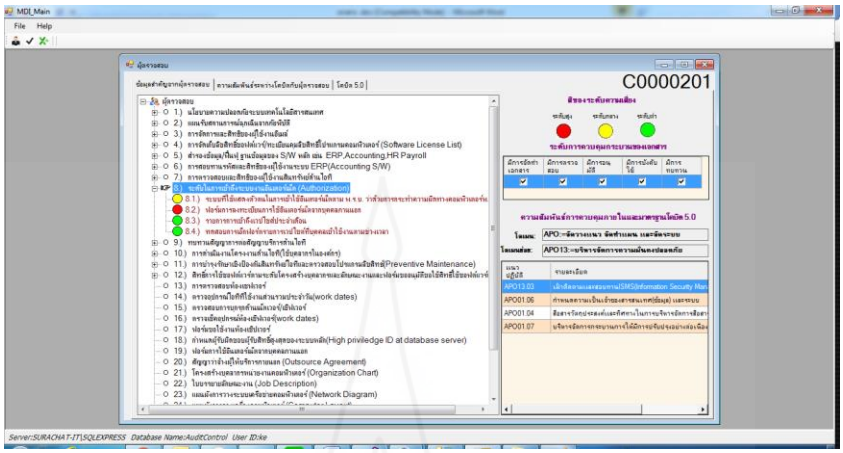
ตารางที่ 4.31 (ต่อ)

selfSubjectScore ตารางเปรียบเทียบกระบวนการการควบคุมภายในด้านไอที					
Attribute	**Data Type**	**Allow Nulls**	**Descrition**	**Example**	**Key**
selfIsCompliance	boolean	Checked	การประกาศเพื่อบังคับใช้เอกสารผู้ใช้งานระบบประเมิน	TRUE	
selfIsReview	boolean	Checked	การทบทวนเอกสารผู้ใช้งานระบบประเมิน	TRUE	
auditIsDocument	boolean	Unchecked	การจัดทำเอกสารที่ได้จากองค์ความรู้	TRUE	
auditIsCheck	boolean	Unchecked	การตรวจสอบเอกสารที่ได้จากองค์ความรู้	TRUE	
auditIsApporve	boolean	Checked	การอนุมัติเอกสารที่ได้จากองค์ความรู้	TRUE	
auditIsCompliance	boolean	Checked	การประกาศเพื่อบังคับใช้เอกสารที่ได้จากองค์ความรู้	TRUE	
auditIsReview	boolean	Checked	การทบทวนเอกสารที่ได้จากองค์ความรู้	TRUE	

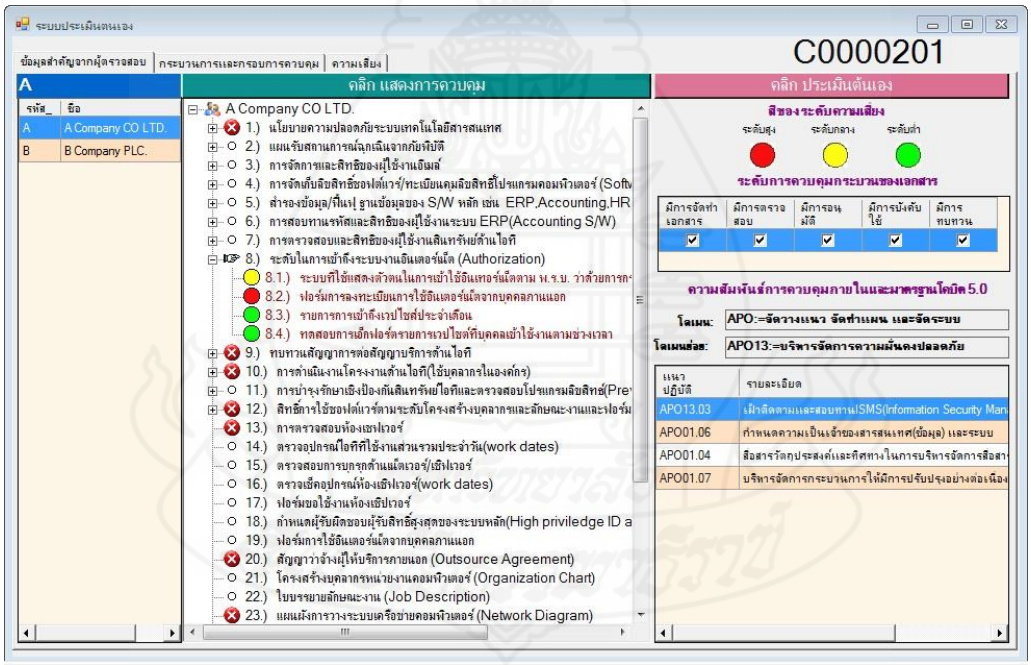
ตารางที่ 4.32 ตารางกรอบเปรียบเทียบระดับความเสี่ยงของกระบวนการย่อย

selfRiskScore ตารางกรอบเปรียบเทียบระดับความเสี่ยงของกระบวนการย่อย					
Attribute	**Data Type**	**Allow Nulls**	**Descrition**	**Example**	**Key**
auditAutoNo	nvarchar(25)	Unchecked	รหัส รูปแบบ Cxxxxxxx	C0000194	PK
isMake	boolean	Unchecked	การตรวจสอบกระบวนการใดยังไม่จัดทำ	FALSE	
subjectNo	nvarchar(50)	Unchecked	เลขที่หัวข้อเอกสาร	C0000594	
subjectDesc	nvarchar(50)	Unchecked	ชื่อหัวข้อกระบวนการ	1	
subjectType	nvarchar(50)	Unchecked	ประเภทของเอกสาร	นโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศ	
selfRiskHeight	boolean	Unchecked	ความเสี่ยงผู้ใช้งานระบบประเมิน	TRUE	
auditRiskHeight	boolean	Unchecked	ความเสี่ยงที่ได้จากองค์ความรู้	TRUE	

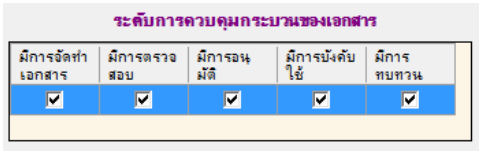
2.5 การใช้งานโปรแกรมประเมิน



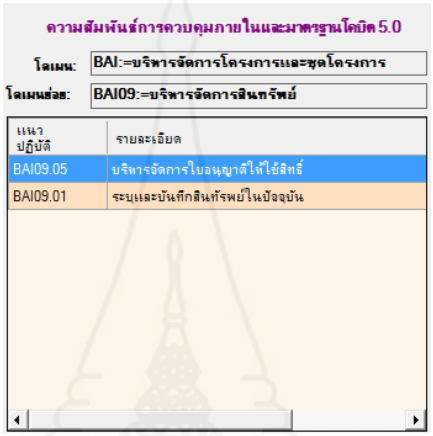
ภาพที่ 4.6 ระบบกรอบการตรวจสอบภายในด้านไอที



ภาพที่ 4.7 ระบบการตรวจสอบภายในด้านไอทีที่สัมพันธ์กับโคบิต 5.0 และกระบวนการการควบคุม

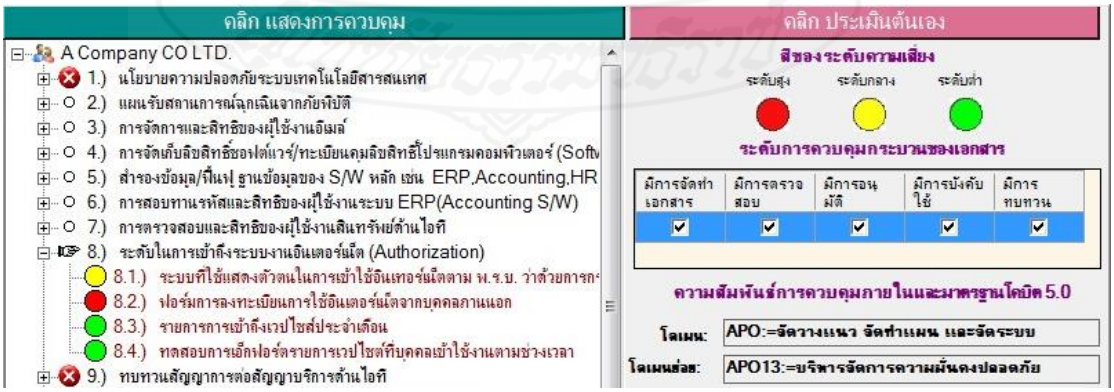


ภาพที่ 4.8 กระบวนการควบคุม

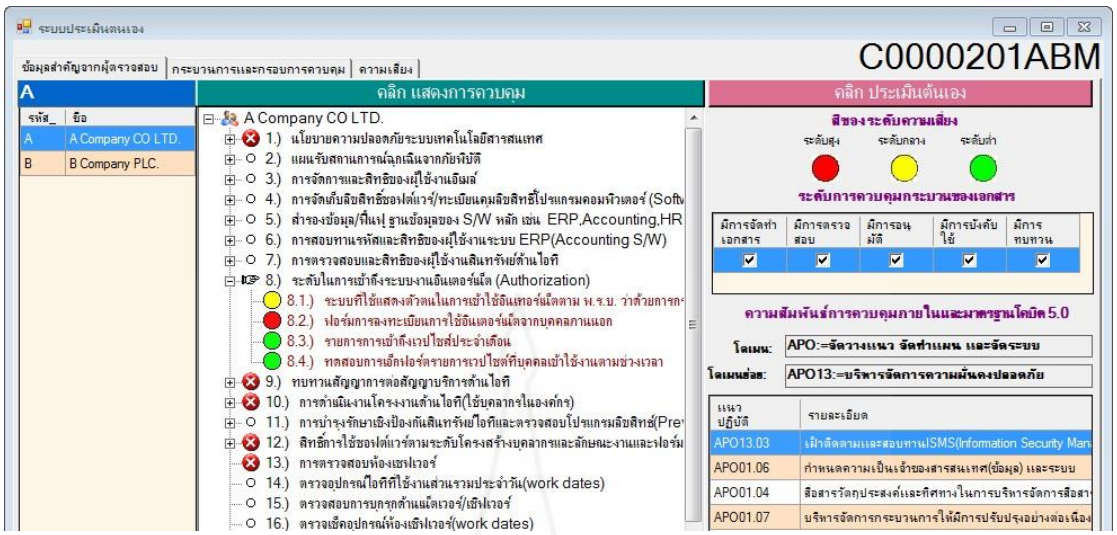


ภาพที่ 4.9 แนวทางปฏิบัติงานกรอบโคบิต 5.0 ที่เกี่ยวข้อง

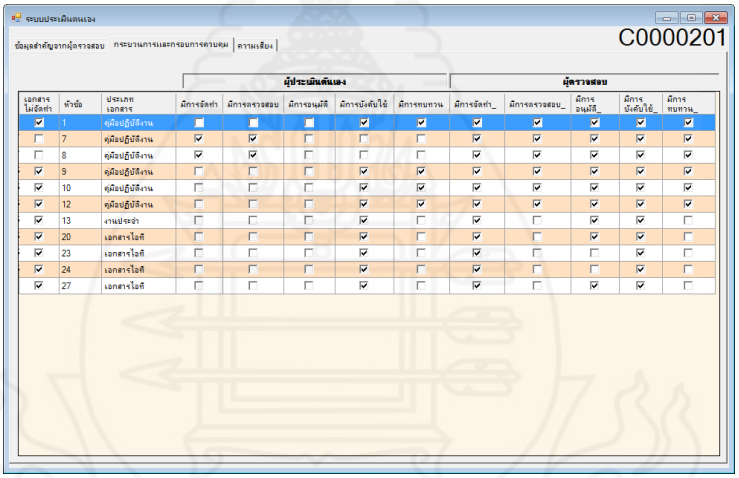
ภาพที่ 4.10 ระดับความเสี่ยงแบ่งตามสี



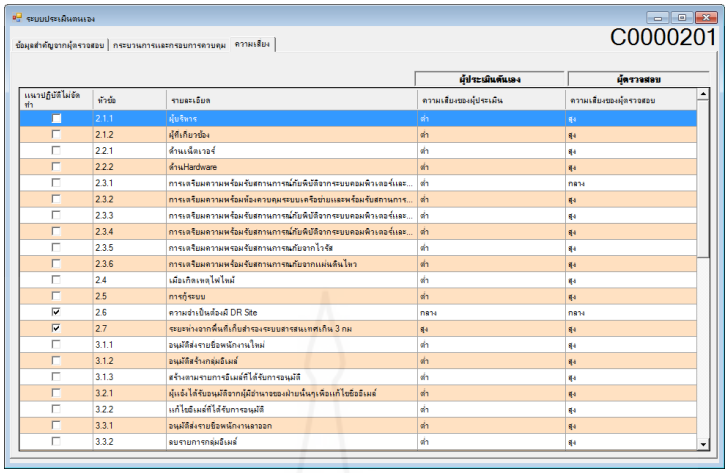
ภาพที่ 4.11 ระดับความเสี่ยงแบ่งตามสีที่แสดงในลิส



ภาพที่ 4.12 ระบบการประเมินตนเอง



ภาพที่ 4.13 แนะนำระบบการประเมินตนเองเรื่องกระบวนการ



ภาพที่ 4.14 แนะนำระบบการประเมินตนเองเรื่องความเสี่ยง

บทที่ 5
สรุปการวิจัย อภิปรายผล และข้อเสนอแนะ

1. สรุปผลการดำเนินงานวิจัย

เรื่องการกำหนดความเสี่ยงขององค์กร

1.1 สรุปการดำเนินงาน

ผู้ถูกประเมินตอบแบบสอบถาม 2 ท่าน 2 องค์กร

1. ท่านแรกอยู่นอกตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย กลุ่มทรัพยากร ท่านแรกตำแหน่ง IT Manager มีประสบการทำงาน 3 ปี 6 เดือน

2. ท่านที่สองอยู่ในตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย กลุ่มทรัพยากร ตำแหน่ง IT Manager มีประสบการทำงาน 4 ปี

ระบบการประเมินตนเองวิเคราะห์ดังนี้

1. การประเมินท่านแรกอยู่บริษัทนอกตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย ระบบประเมินตนเองวิเคราะห์ดังนี้

1.1 กระบวนการปฏิบัติงาน

บริษัทอยู่นอกตลาดหลักทรัพย์													
แนวปฏิบัติ			ผู้ถูกประเมิน					ผู้ตรวจสอบ					
ไม่จัดทำ	หัวข้อ	ประเภท	มีผู้จัดทำ	มีผู้ตรวจสอบ	มีผู้อนุมัติ	ประกาศใช้	การทบทวน	มีผู้จัดทำ	มีผู้ตรวจสอบ	มีผู้อนุมัติ	ประกาศใช้	การทบทวน
✓	1	คู่มือปฏิบัติงาน						✓	✓	✓	✓	✓
✓	9	คู่มือปฏิบัติงาน						✓	✓	✓	✓	✓
	7	คู่มือปฏิบัติงาน	✓	✓				✓	✓	✓	✓	✓
	8	คู่มือปฏิบัติงาน	✓	✓				✓	✓	✓	✓	✓
✓	10	คู่มือปฏิบัติงาน						✓	✓	✓	✓	✓
✓	12	คู่มือปฏิบัติงาน						✓	✓	✓	✓	✓
✓	13	งานประจำ						✓	✓	✓	✓	✓
✓	20	เอกสารไอที						✓		✓	✓	
✓	23	เอกสารไอที						✓			✓	
✓	24	เอกสารไอที						✓			✓	
✓	27	เอกสารไอที						✓		✓	✓	

ภาพที่ 5.1 ระบบประเมินแจ้งกระบวนการควบคุมที่ต้องจัดทำเพิ่ม

1.2 ระดับความเสี่ยง

บริษัทอยู่นอกตลาดหลักทรัพย์									
ลำดับ	แนวปฏิบัติย่อย		ผู้ถูกประเมิน	ผู้ตรวจสอบ	ลำดับ	แนวปฏิบัติย่อย		ผู้ถูกประเมิน	ผู้ตรวจสอบ
	ไม่จัดทำ	หัวข้อ	ระดับความเสี่ยง	ระดับความเสี่ยง		ไม่จัดทำ	หัวข้อ	ระดับความเสี่ยง	ระดับความเสี่ยง
1		2.1.1	ต่ำ	สูง	24	✓	3.4.2		สูง
2		2.1.2	ต่ำ	สูง	25		5.1.1	ต่ำ	สูง
3		2.2.1	ต่ำ	สูง	26		5.1.2	ต่ำ	สูง
4		2.2.2	ต่ำ	สูง	27		5.1.3	ต่ำ	สูง
5		2.3.1	ต่ำ	สูง	28		5.2.1	ต่ำ	สูง
6		2.3.2	ต่ำ	สูง	29		5.2.2	ต่ำ	สูง
7		3.3.3	ต่ำ	สูง	30		5.3.1	ต่ำ	กลาง
8		2.3.4	ต่ำ	สูง	31		5.3.2	ต่ำ	สูง
9		2.3.5	ต่ำ	สูง	32		6.1.1	ต่ำ	สูง
10		2.3.6	ต่ำ	สูง	33		6.1.2	ต่ำ	สูง
11		2.4	ต่ำ	สูง	34		6.1.3	ต่ำ	สูง
12		2.5	ต่ำ	สูง	35		6.1.4	ต่ำ	สูง
13	✓	2.6		สูง	36		6.1.5	ต่ำ	สูง
14	✓	2.7		สูง	37	✓	6.2.1		สูง
15		3.1.1	ต่ำ	สูง	38	✓	6.2.2		สูง
16		3.1.2	ต่ำ	สูง	39		7.1.1	กลาง	สูง
17		3.1.3	ต่ำ	สูง	40		7.1.2	กลาง	สูง
18		3.2.1	ต่ำ	สูง	41		7.1.3	กลาง	สูง
19		3.2.2	ต่ำ	สูง	42		7.1.4	กลาง	สูง
20		3.3.1	ต่ำ	สูง	43		7.1.5	กลาง	สูง
21		3.3.2	ต่ำ	สูง	44		7.2.1	กลาง	สูง
22		3.3.3	ต่ำ	สูง	45		7.2.2	กลาง	สูง
23	✓	3.4.1		สูง					

ภาพที่ 5.2 ระบบประเมินแจ้งระดับความเสี่ยงของแนวปฏิบัติที่ต้องจัดทำเพิ่ม

การประเมินบริษัทนอกตลาดหลักทรัพย์จากองค์ความรู้ในต้นแบบฯ ที่ได้พัฒนาขึ้นโดยกลุ่มอุตสาหกรรมทรัพยากร

กระบวนการควบคุม

1. ต้องจัดทำเพิ่ม 9 กระบวนการควบคุม

2. ต้องปรับระดับกระบวนการปฏิบัติงาน 2 กระบวนการ

แนวปฏิบัติด้านระดับเสี่ยง

1. ต้องจัดทำเพิ่ม 6 หัวข้อแนวปฏิบัติย่อย

2. ต้องปรับระดับเสี่ยง 39 หัวข้อแนวปฏิบัติย่อย

(2) การประเมินท่านที่สองอยู่ในตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย กลุ่มทรัพยากร ระบบประเมินตนเองวิเคราะห์ดังนี้

2.1 กระบวนการปฏิบัติงาน

บริษัทอยู่ในตลาดหลักทรัพย์เอ็ม เอ ไอ แห่งประเทศไทย ในกลุ่มทรัพยากร												
แนวปฏิบัติ			ผู้ถูกประเมิน					ผู้ตรวจสอบ				
ไม่จัดทำ	หัวข้อ	ประเภท	มีผู้จัดทำ	มีผู้ตรวจสอบ	มีผู้อนุมัติ	ประกาศใช้	การทบทวน	มีผู้จัดทำ	มีผู้ตรวจสอบ	มีผู้อนุมัติ	ประกาศใช้	การทบทวน
	2	คู่มือปฏิบัติงาน	✓	✓				✓	✓	✓	✓	✓
	6	คู่มือปฏิบัติงาน	✓		✓	✓		✓	✓	✓	✓	✓
	7	คู่มือปฏิบัติงาน	✓	✓	✓		✓	✓	✓	✓	✓	✓
✓	8	คู่มือปฏิบัติงาน						✓	✓	✓	✓	✓
✓	12	คู่มือปฏิบัติงาน						✓	✓	✓	✓	✓
	13	งานประจำ	✓	✓				✓		✓	✓	
	14	งานประจำ	✓	✓				✓			✓	
✓	15	งานประจำ						✓			✓	
✓	16	งานประจำ						✓			✓	
✓	17	เอกสารไอที						✓			✓	
	20	เอกสารไอที	✓	✓	✓			✓		✓	✓	
	18	เอกสารไอที	✓		✓			✓		✓	✓	✓
✓	25	เอกสารไอที						✓		✓	✓	
	26	เอกสารไอที	✓	✓	✓			✓			✓	
	27	เอกสารไอที	✓	✓				✓		✓	✓	

ภาพที่ 5.3 ระบบประเมินแจ้งกระบวนการควบคุมที่ต้องจัดทำเพิ่ม

2.2 ระดับความเสี่ยง

บริษัทอยู่ในตลาดหลักทรัพย์เอ็ม เอ ไอ แห่งประเทศไทย ในกลุ่มทรัพยากร									
ลำดับ	แนวปฏิบัติย่อย		ผู้ถูกประเมิน	ผู้ตรวจสอบ	ลำดับ	แนวปฏิบัติย่อย		ผู้ถูกประเมิน	ผู้ตรวจสอบ
	ไม่จัดทำ	หัวข้อ	ระดับความเสี่ยง	ระดับความเสี่ยง		ไม่จัดทำ	หัวข้อ	ระดับความเสี่ยง	ระดับความเสี่ยง
1		1.1.3	ต่ำ	กลาง	18		5.2.1	กลาง	สูง
2		1.1.7	กลาง	สูง	19		5.2.2	กลาง	สูง
3		1.2.2.1	กลาง	สูง	20		5.3.2	กลาง	สูง
4		1.2.3	กลาง	สูง	21		6.1.1	กลาง	สูง
5		1.6.2.1	กลาง	สูง	22		6.1.2	กลาง	สูง
6		1.6.2.3.2	กลาง	สูง	23		6.1.3	กลาง	สูง
7		1.6.2.3.3	กลาง	สูง	24		6.1.4	กลาง	สูง
8		1.6.2.3.4	กลาง	สูง	25		6.1.5	กลาง	สูง
9		1.10.2	กลาง	สูง	26		7.1.2	กลาง	สูง
10		1.11.1	กลาง	สูง	27		11.1.1	กลาง	สูง
11		2.1.1	กลาง	สูง	28		11.2.1	กลาง	สูง
12		2.3.3	กลาง	สูง	29		11.2.2	กลาง	สูง
13		2.3.4	กลาง	สูง	30		11.2.3	กลาง	สูง
14		2.5	กลาง	สูง	31		11.3.1	กลาง	สูง
15		2.7	กลาง	สูง	32		11.3.4	กลาง	สูง
16		5.1.2	กลาง	สูง	33		12.1.1	ต่ำ	กลาง
17		5.1.3	กลาง	สูง					

ภาพที่ 5.4 ระบบประเมินแจ้งระดับความเสี่ยงของแนวปฏิบัติที่ต้องจัดทำเพิ่ม

การประเมินบริษัทในตลาดหลักทรัพย์จากองค์ความรู้ในต้นแบบฯ ที่ได้พัฒนาขึ้นโดยกลุ่มอุตสาหกรรมทรัพยากร

กระบวนการควบคุม

1. ต้องจัดทำเพิ่ม 6 กระบวนการควบคุม
2. ต้องปรับระดับกระบวนการปฏิบัติงาน 8 กระบวนการ

แนวปฏิบัติด้านระดับความเสี่ยง

1. ไม่มีรายการใดต้องจัดทำเพิ่ม
2. ต้องปรับระดับเสี่ยง 33 หัวข้อแนวปฏิบัติย่อย

สรุปผลการการประเมิน

1. การประเมินกลุ่มตัวอย่างทั้งกระบวนการและกระบวนการย่อยของการควบคุมภายในด้านไอที มีการทำงาน ที่สอดคล้องกับ ต้นแบบที่สร้างขึ้น โดยมีการทำงานตามอยู่ในกรอบการประเมิน

2. กระบวนการการควบคุมภายในด้านไอทีสามารถใช้หลักธรรมาภิบาลไอทีกรอบโคบิต 5.0 ได้เพราะมีกระบวนการครอบคลุมทุกกระบวนการของงานวิจัยนี้

3. จากการประเมิน 2 กลุ่มตัวอย่างองค์กร องค์กรที่อยู่ในตลาดหลักทรัพย์ เอ็ม เอ ไอ มีการควบคุมภายในด้านไอทีดีกว่า องค์กรนอกตลาดหลักทรัพย์ ทั้งกระบวนการดำเนินงานและความเสี่ยง ของกระบวนการตรวจสอบภายในด้านไอที

ขณะเดียวกันงานวิจัยนี้ได้สรุปตัวชี้วัดต่างๆ ตามหลักธรรมาภิบาลในการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรตามหลัก COBIT 5

(1) หลักการที่ 1: ตอบสนองความต้องการของผู้มีส่วนได้ส่วนเสียองค์กรโดยการรักษาความสมดุลระหว่างผลประโยชน์ที่จะได้รับกับความเสี่ยงและการใช้ทรัพยากรที่ทำให้เกิดประโยชน์สูงสุดคือ

1.1 ฝ่ายไอทีสามารถประเมินตนเองให้ผ่านการควบคุมภายในเพื่อเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย ในกลุ่มทรัพยากรสำเร็จตามเป้าหมายที่กำหนดไว้

1.2 การประเมินตนเองสำหรับการบริหารความเสี่ยงจัดการความเสี่ยง การควบคุม นโยบาย การบริหารสินทรัพย์ด้านไอทีโดยรวม

1.3 การเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทยเป็นการระดมเงินทุนจากผู้ลงทุนสามารถลดอัตราดอกเบี้ยเงินกู้ให้ต่ำลงเพื่อลดต้นทุนทางการเงินและทำให้องค์กรเติบโต ยั่งยืน

(2) หลักการที่ 2: ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจรCOBIT 5 บูรณาการการกำกับดูแลไอทีระดับองค์กรเข้าไปในการกำกับดูแลองค์กรคือ

2.1 การควบคุมภายใน การบริหารความเสี่ยงด้าน การบริหารสินทรัพย์ด้านไอที งานหลักๆ เช่น ERP HR BI มักครอบคลุมงานทั่วทั้งองค์กร

2.2 การบริหารจัดการปัจจัยเอื้อที่เกี่ยวข้องกับไอทีทั้งหมด การทบทวนกระบวนการทำงาน กระบวนการการควบคุมภายในด้านไอทีในองค์กร พ.ร.บ. คอมพิวเตอร์ปี 50 ฟอร์มการใช้อินเตอร์เน็ตจากบุคคลภายนอก ล็อกไฟล์จัดเก็บอย่างน้อย 90 วันและการตรวจสอบลิขสิทธิ์เป็นประจำทุกเครื่องขบวนงานประจำปี ซึ่งมีผลกระทบต่อภาพรวมองค์กร การระดมทุนในตลาดทุน

(3) หลักการที่3: ประยุกต์ใช้กรอบการดำเนินงานที่บูรณาการเป็นหนึ่งเดียว มีมาตรฐานและแนวปฏิบัติที่ดีที่เกี่ยวข้องกับไอทีจำนวนมาก คือ

3.1 การสร้างระบบการประเมินตนเอง เช่น เป็นการบูรณาการกระบวนการเดิมที่ผู้สอบเสนอแนะนำปัญหาและให้ฝ่ายที่เกี่ยวข้องดำเนินการหาวิธีแก้ไขกำหนดช่วงเวลาแล้วเสร็จผู้ดูแลงานหัวข้อนั้นจนกระทั่งจบกระบวนการ ซอฟต์ไฟล์ต่างๆ อาจมีการบันทึกไว้หรืออาจสูญหายเนื่องจาก ไม่มีกระบวนการจัดเก็บ แต่เมื่อมีการใช้ระบบการประเมินตนเองทำให้สามารถจัดเก็บอัตโนมัติเมื่อมีการใช้โปรแกรม

3.2 คู่มือปฏิบัติงานด้านไอทีเป็นกระบวนการที่เกี่ยวข้องกับฝ่ายต่างๆ ในองค์กร เพื่อควบคุมกระบวนการทำงานภายในให้ปลอดภัยมีความเสี่ยงน้อยที่สุด (หรือความเสี่ยงนั้นสามารถยอมรับได้) โดยคู่มือปฏิบัติงานมีกระบวนการย่อยที่ระบุระดับความเสี่ยงเป็นสัญญาณชี้วัดความสำคัญของงานในการแก้ไข เช่น เมื่อพนักงาน เข้าใหม่ โอนย้ายแผนก ลาออก องค์กรมีกระบวนการจัดการ ระบบงานที่เกี่ยวข้องเพื่อความปลอดภัยขององค์กร

(4) หลักการที่ 4: เอื้อให้วิธีปฏิบัติแบบองค์รวมสัมฤทธิ์ผล การกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรที่มีประสิทธิภาพและประสิทธิผลต้องใช้วิธีปฏิบัติแบบองค์รวมที่ได้พิจารณาถึงองค์ประกอบหลายๆ อย่างซึ่งมีปฏิสัมพันธ์ต่อกัน

4.1 ระบบการประเมินตนเอง จัดการเก็บข้อมูลในฐานข้อมูลเมื่อเลือกให้ระบบจัดทำข้อเสนอแนะสามารถดำเนินการได้อย่างรวดเร็วมีประสิทธิภาพ (1) ความเป็นปัจจุบัน (Current) ข้อมูลปรับเปลี่ยนไปเรื่อยๆ มีความทันสมัย (2) ทันเวลา (Timely) มีคุณค่าทางเวลามาเกี่ยวข้อง ถ้าไม่ได้สารสนเทศในเวลาที่ต้องการ อาจจะ เกิดการสูญเสียโอกาสได้ (3) ความเที่ยงตรง (Relevant) ข้อที่ได้ต้องมีความสมบูรณ์ ถูกต้อง (4) ความคงที่ (Consistent) ข้อมูลที่เก็บไว้หลายๆ ที่ อาจไม่ตรงกัน ขัดแย้งกัน สารสนเทศที่ดีต้อง ไม่มีความขัดแย้งกัน หรือขัดแย้งกันน้อยที่สุด (3) นำเสนอรูปแบบที่มีประโยชน์ (Present in usable form) มีรูปแบบในการนำเสนอที่เข้าใจง่าย เหมาะสม

4.2 ระบบการประเมินตนเองมีการแนะนำ (1) กระบวนการ (2) ระดับความเสี่ยงของแนวปฏิบัติการ จากองค์ความรู้ในต้นแบบฯ ที่ได้พัฒนาขึ้นโดยกลุ่มอุตสาหกรรมทรัพยากร โดยมีรูปแบบที่ชัดเจนจึงทำให้ใช้เวลาน้อยลง

(5) หลักการที่ 5: แบ่งแยกการกำกับดูแลออกจากการบริหารจัดการ กรอบการดำเนินงาน

5.1 คู่มือปฏิบัติงานแต่ละหัวข้อแบ่งแยกงานเพื่อให้ประเภทขบวนงานทำงานได้ชัดเจน แต่เมื่อรวบรวมทุกกระบวนการเป็นการตรวจสอบภายใน บริหารความเสี่ยง การบังคับใช้และมีการบททวนกระบวนการต่างๆ ครอบคลุมบริหารจัดการ กรอบการดำเนินงานทั่วทั้งองค์กร

5.2 ระบบการประเมินตนเอง ผู้บริหารสามารถพิจารณาภาพรวมขบวนปฏิบัติงานที่ขาด ที่ต้องดำเนินการเพิ่มเพื่อบริหารจัดการกระบวนการที่ยังพบปัญหาเร่งประสานงานไปหน่วยงานที่เกี่ยวข้องดำเนินการได้รวดเร็วขึ้น เช่น เรื่องกำลังพลขององค์กรซึ่งงานหลักๆ ฝ่ายบุคคลเกี่ยวข้องกับงานนี้โดยตรง แต่ฝ่ายไอทีก็ต้องดำเนินงานบางอย่างได้แก่ สร้างอีเมล์ สร้างแอคเคาท์ระบบงานหลักหรือระบบงานอื่นๆ คู่มือปฏิบัติงานการจัดการและสิทธิของผู้ใช้งานอีเมล์ต้องทำผังงานฝ่ายที่เกี่ยวข้องข้อตกลงดำเนินการในส่วนที่ฝ่ายนั้นๆ เกี่ยวข้องต้องกำหนดขอบเขตให้ชัดเจนในกระบวนการของผังงาน

1.1 ข้อค้นพบจากงานวิจัย

ผลการวิจัย เรื่อง “ระบบประเมินตนเองด้านเทคโนโลยีสารสนเทศ ของบริษัทจดทะเบียนในกลุ่มทรัพยากรตามกรอบโคบิต เพื่อเตรียมความพร้อมในการเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย” มีข้อค้นพบจากการวิจัยและประเด็นต่างๆ ที่ควรนำมาอภิปรายดังนี้

(1) กรอบโคบิต 5.0 มีกระบวนการด้านบริหารจัดการทางด้านไอที 37 กระบวนการ ซึ่งในการใช้งานนั้นผู้วิจัยนำกระบวนการที่เกี่ยวข้องจากการสัมภาษณ์ (อ้างอิงจากตารางที่ 4.2 การสร้างความสัมพันธ์ การควบคุมยืนยันเอกสาร ระดับความเสี่ยง) ที่มีความสัมพันธ์ กับกรอบงานใดที่เหมาะสมมาใช้ได้บ้าง

(2) โดเมน APO,BAI ใช้ในการประเมินตนเองด้านไอที มีกระบวนการต่างๆ โดยการสร้างความสัมพันธ์กับการสัมภาษณ์ผู้ตรวจสอบที่ผู้วิจัยมีความเห็นว่าควรใช้เป็นกรอบมาตรฐานหลักสำหรับองค์กรที่จะจัดทำการประเมินตนเองด้านไอที เพราะมีรายละเอียดที่จำเป็นสำหรับการบริหารโครงการไอทีให้ประสบความสำเร็จ คือ

2.1 APO ,BAI โดยมีรายละเอียดความสัมพันธ์ดังนี้

2.1.1 APO01 โดยมีแนวงานปฏิบัติอ้างถึง APO01.01

2.1.2 APO07 โดยมีแนวงานปฏิบัติอ้างถึง APO07.06

2.1.3 APO10 โดยมีแนวงานปฏิบัติอ้างถึง APO10.01

2.1.4 APO12 โดยมีแนวงานปฏิบัติอ้างถึง APO12.01, APO12.02, APO12.03, APO12.04, APO12.05

2.1.5 APO13 โดยมีแนวงานปฏิบัติอ้างถึง APO13.01, APO13.02, APO13.03

2.1.6 BAI06 โดยมีแนวงานปฏิบัติอ้างถึง BAI06.01, BAI06.03, BAI06.04

2.1.7 BAI09 โดยมีแนวงานปฏิบัติอ้างถึง BAI09.01, BAI09.03, BAI09.05

ประเภทเอกสารที่ใช้ในการประเมินตนเองด้านไอทีได้แก่ คู่มือปฏิบัติงาน งานประจำและเอกสารไอที

2.2 ปัญหาการรอผู้ตรวจสอบแจ้งข้อเสนอแนะล่าช้า เพื่อศึกษาการแก้ไขปัญหาในส่วนนี้

2.3 ทรัพยากรไอที จะเน้นในส่วนของฝ่ายไอที

2.4 ตัวชี้วัดในควบคุมภายใน จะต้องมีความสอดคล้องกับเป้าหมายไอทีที่ได้ตั้งไว้

2.5 บทบาทของผู้ที่เกี่ยวข้องในการควบคุมภายใน ผู้วิจัยมีความเห็นว่าเป็นประเด็นสำคัญที่จะช่วยให้การประเมินประสบความสำเร็จ

2.6 การประเมินสถานะการควบคุม ผู้วิจัยพบว่า การประเมินสถานะการควบคุมภายในจะช่วยให้ผู้บริหารทราบว่า การประเมินควบคุมภายในตนเองเป็นอย่างไร

2.7 ระดับความเสี่ยง

(3) ระบบการประเมินตนเองด้านไอที ที่จะนำเข้าช่วยให้เวลาที่ให้ในการจัดทำการประเมิน การติดตามการประเมินทำได้สะดวก รวดเร็วมากขึ้น

(4) เป้าหมายองค์กรและเป้าหมายไอที ในหลักของธรรมาภิบาล โครงการไอทีที่มีการจัดทำตามกรอบของ APO ,BAI การควบคุมภายในด้านไอที ต้องมีการกำหนดเป้าหมายให้สอดคล้องกับเป้าหมายไอทีและเป้าหมายขององค์กร ดังนั้นถ้าองค์กรไม่ได้มีการกำหนดเป้าหมายที่ชัดเจนจะทำให้การประเมินการควบคุมภายใน บริหารเฉพาะในส่วนงานฝ่ายไอที แต่ไม่สามารถทราบได้ว่าโครงการที่จัดทำบรรลุเป้าหมายขององค์กรได้หรือไม่ ทำให้การควบคุมภายในเป็นไปเฉพาะหน่วยงานของที่เกี่ยวข้องเท่านั้น ไม่สามารถมองเห็นภาพรวมที่สอดคล้องกับเป้าหมายขององค์กรได้

1.2 ประโยชน์ของการประเมินตัวเอง

เป็นกรอบการประเมินตัวเองเพื่อเตรียมพร้อมสำหรับ โดยใช้เครื่องมือทางไอที ที่สามารถชี้แนะแนวทางที่ควรปฏิบัติทั้งประเภทหัวข้อ เช่น คู่มือปฏิบัติงาน งานประจำ เอกสารไอที และคู่มือปฏิบัติงานมีรายละเอียดย่อยที่ต้องปฏิบัติตามที่ได้จากการสัมภาษณ์เชิงลึก

(1) สามารถแสดงสถานะของระบบการประเมินตนเองด้านไอที ได้อย่างถูกต้อง

(2) สามารถกำหนดแนวโน้มของระบบการประเมินตนเองด้านไอทีได้

(3) กำหนดปัญหา ได้อย่างถูกต้อง

(4) มีเหตุผล สำหรับการตัดสินใจ เกี่ยวกับสุขภาพระบบการประเมินตนเองด้านไอที

(5) มีแหล่งข้อมูล สำหรับระบบการประเมินตนเองด้านไอที

จากการทำวิจัย ผู้วิจัยมีความเห็นว่าโคบิตเวอร์ชั่น 5.0 (COBIT 5.0) เหมาะสมอย่างยิ่งสำหรับการนำไปใช้วางกรอบในการควบคุมภายในโดยระบบการประเมินตนเอง โดยโคบิตมีรายละเอียดเกี่ยวกับกรอบกระบวนการทางด้านไอทีต่างๆ ครอบคลุมในแต่ละกระบวนการและมีรายละเอียด กระบวนการการควบคุมภายใน การติดตามอย่างครบสมบูรณ์ ผู้บริหารไอทีสามารถใช้ในการติดตาม ความก้าวหน้าของกระบวนการการควบคุมภายในได้เป็นอย่างดี กรอบโคบิต 5.0 เหมาะสมภาพรวมขององค์กร เพื่อเตรียมความพร้อมในการเข้าตลาดหลักทรัพย์แห่งประเทศไทยไม่จำกัดเรื่องขนาดองค์กร แต่จะต่างกันที่รายละเอียดของการนำไปใช้งานตามอุตสาหกรรมโดยถ้าองค์กรที่มีความพร้อมมาก ก็สามารถลดเวลาในการตรวจสอบทำให้ลดค่าใช้จ่าย อาจจะประยุกต์ใช้กระบวนการหลักในควบคุมกระบวนการตรวจสอบภายในไม่ว่า องค์กรที่มีขนาดเล็กหรือขนาด

ใหญ่ ดังนั้นผู้วิจัยมองว่าโคบิต เหมาะสมกับทุกองค์กร เพียงแต่การนำกระบวนการมาใช้งานขึ้นอยู่ความพร้อมขององค์กรว่าต้องการให้มีการติดตาม ควบคุมมากน้อยเพียงใด

1.3 สรุปกรอบวิธีการการควบคุมภายในโดยระบบการประเมินตนเองที่ได้จากงานวิจัย

การสัมภาษณ์ผู้ตรวจสอบ การนัดสัมภาษณ์ไม่ต้องการให้แสดงชื่อองค์กร ชื่อ-นามสกุล เพราะอาจมีผลกระทบ..

จะเห็นได้ว่า การนำกรอบโคบิตเวอร์ชั่น 5.0 (COBIT 5.0) เข้ามาใช้เพื่อช่วยในการประเมิน โครงการสารสนเทศนั้น อาจจะต้องมีการปรับเปลี่ยนเพื่อให้เหมาะสมกับสภาพแวดล้อมของแต่ละองค์กรซึ่งจะช่วยให้แนวทางปฏิบัตินั้น มีความเหมาะสมกับองค์กรที่จะนำไปใช้ เพื่อให้เกิดประโยชน์สูงสุดกับการบริหารโครงการสารสนเทศ จึงขอเสนอขั้นตอนการนำกรอบโคบิตเวอร์ชั่น5.0 (COBIT) มาประยุกต์ใช้ในองค์กรเพื่อให้ได้ผลในทางปฏิบัติ ซึ่งมีขั้นตอนดังนี้

(1) จัดตั้งคณะทำงานเพื่อศึกษารายละเอียดของกรอบโคบิตเวอร์ชั่น5.0 (COBIT5.0) อย่างละเอียดและหาแนวทางการประยุกต์ใช้กับองค์กร

(2) จัดอบรมเพื่อให้เข้าใจในกรอบรายละเอียดขั้นตอนการบริหารโครงการ APO,BAI ของกรอบโคบิตเวอร์ชั่น5.0 (COBIT 5.0)

(3) กำหนดเป้าหมายขององค์กรและเป้าหมายของไอทีที่สอดคล้องกัน

4) กำหนดบทบาท หน้าที่ความรับชอบแต่ละขั้นตอนการปฏิบัติอย่างชัดเจน

(5) กำหนดเกณฑ์คุณภาพสารสนเทศ ทางด้านประสิทธิภาพและประสิทธิผล เพื่อใช้สำหรับการประเมิน ติดตาม ผลการดำเนินงาน

(6) กำหนดตัวชี้วัดของโครงการ เพื่อใช้ประเมินผลการจัดทำโครงการสารสนเทศ ซึ่งผู้วิจัย มีความเห็นว่า ตัวชี้วัดในกระบวนการบริหารโครงการ APO,BAI ก็น่าจะเพียงพอสำหรับการติดตามโครงการสารสนเทศ

(7) เครื่องมือที่จะนำมาช่วยในการประเมินตนเอง ควรจัดทำเป็นซอฟต์แวร์ที่แสดงผลความคืบหน้าการประเมินตนเอง ดังเช่นในงานวิจัยนี้ ที่ผู้วิจัยได้พัฒนาซอฟต์แวร์สำหรับการประเมินตนเองที่เหมาะสำหรับสถานประกอบการกลุ่มอุตสาหกรรมทรัพยากร ทำให้สะดวกสำหรับการติดตามใช้งาน

(8) การติดตามผลงาน ควรจะนำตัวชี้วัดที่ได้มีการจัดทำมาประชุมติดตามความคืบหน้า เป็นระยะๆ เพื่อช่วยปรับปรุง แก้ไข ก่อนที่การประเมินตนเองจะล่าช้าและเกิดปัญหา

(9) จัดทำการประเมินสถานะกระบวนการ และระดับความเสี่ยง เพื่อประเมินผลหน่วยงานไอทีที่รับผิดชอบเกี่ยวกับการประเมินตนเอง ว่าขาดกระบวนการใดเพื่อเตรียมความพร้อมองค์กรในการเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทยกลุ่มทรัพยากร

2. ปัญหาและอุปสรรค

2.1 กรอบโคบิต โดยกรอบโคบิตให้รายละเอียดเกี่ยวกับกระบวนการต่างๆ ทางด้านไอที แต่ไม่ได้แสดงรายละเอียดเกี่ยวกับการปฏิบัติงาน ว่าจะต้องทำอย่างไรบ้าง ทำให้มีปัญหาในการทำความเข้าใจค่อนข้างมาก ในช่วงแรกของการทำวิจัย

2.2 ระดับความเสี่ยงและระดับสถานการณ์ควบคุมที่ได้รับการแนะนำจาก ผู้ตรวจสอบ ระดับความเสี่ยงมีสามระดับ ระดับสถานะการควบคุมมีห้าระดับ ไม่มีการกำหนดแน่ชัดว่าแต่ละข้อจะต้องมีระยะเวลาให้แล้วเสร็จเป็นเวลาเท่าใด ขึ้นอยู่กับองค์กรนั้นๆ กำหนดขึ้น (หมายถึงระดับความเสี่ยงหรือระดับสถานการณ์ควบคุมอาจมากหรือน้อยกว่าข้อแนะนำจากผู้ตรวจสอบก็ได้) และระดับความเสี่ยงหรือระดับสถานการณ์ควบคุมต้องได้รับอนุมัติโดยผู้บริหาร

2.3 ผู้วิจัยสัมภาษณ์ผู้ตรวจสอบ เรื่องการควบคุมภายในของกลุ่มทรัพยากรบริษัทตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย อาจทำให้การควบคุมภายในด้านไอทีไม่ครบถ้วนสมบูรณ์ครอบคลุมในกลุ่มอุตสาหกรรมอื่น ตลาดหลักทรัพย์แห่งประเทศไทย

2.4 บุคคลากรทางไอทีตามตาราง RACI (Responsible Accountable Consulted and Informed Chart การพูดถึงเรื่องของหน้าที่และความรับผิดชอบของเจ้าของกระบวนการปฏิบัติงานต่างๆ โดยโคบิตเน้นที่การสร้างความเข้าใจในเรื่องของบทบาท หน้าที่ และความรับผิดชอบของกระบวนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ซึ่งถือเป็นประเด็นหลักในการทำให้เกิดธรรมาภิบาลด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ) แบ่งแยกอย่างชัดเจนซึ่งแตกต่างจากในองค์กรในงานวิจัยหนึ่งท่านอาจทำหน้าที่หลายๆ อย่างพร้อมกัน เช่น บางบริษัทผู้ตรวจสอบต้องตรวจสอบทุกๆกระบวนการทั้งองค์กร แต่งานด้านไอทีมีรายละเอียดซับซ้อนผู้ตรวจสอบที่ไม่มีประสบการณ์ด้านไอทีอาจทำให้กระบวนการและความเสี่ยงควบคุมได้ไม่เหมาะสม

3. ข้อเสนอแนะ

ในการดำเนินควบคุมภายในด้านไอทีเพื่อเตรียมตัวของกลุ่มทรัพยากรบริษัทตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย ปัจจุบันได้รับเสนอแนะจากผู้ตรวจสอบภายนอก บริษัทที่ไม่มีประสบการณ์ด้านการควบคุมภายในมาก่อนจะเสียเวลาค่อนข้างมากในการยืนยันข้อเสนอแนะระหว่างกัน ผู้วิจัยจึงจัดทำระบบการประเมินเพื่อแก้ไขปัญหาล่าช้า ถูกต้องและเชื่อถือได้

3.1 ผู้ทำวิจัยมีความเห็นว่าระบบการประเมินตนเองเพื่อเตรียมความพร้อมเพื่อเป็นบริษัทจดทะเบียนในกลุ่มทรัพยากรตามกรอบโคบิต เพื่อเตรียมความพร้อมในการเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย สามารถใช้ได้ทุกอุตสาหกรรม

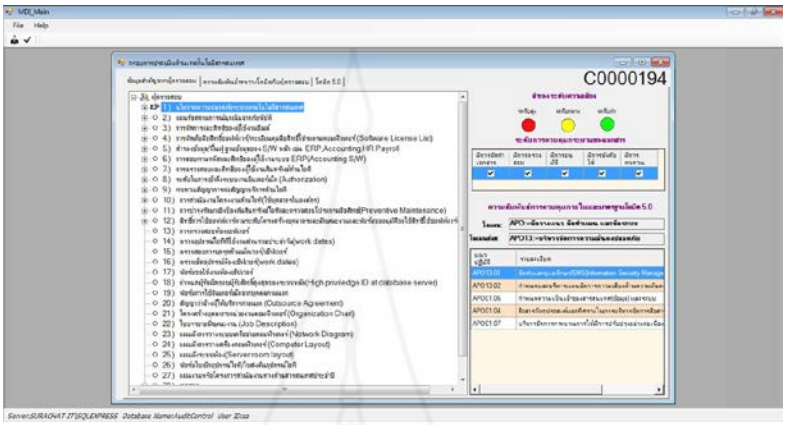
3.2 งานวิจัยนี้ เน้น เฉพาะ การประเมินการควบคุมภายใน APO,BAI บางแนวงานปฏิบัติมาเป็นกรอบหลัก แต่ในกรอบโคบิตนั้นมีกระบวนหลักทั้งหมด 37 กระบวนการ ซึ่งมีความสำคัญมากเช่นกัน ดังนั้นในการดำเนินงานวิจัยในอนาคต อาจจะนำกระบวนการอื่นมาเป็นกระบวนการหลักในการวิจัย

ภาคผนวก

คู่มือการใช้โปรแกรม

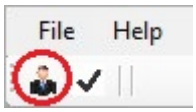
กรอบการประเมินตนเองด้านเทคโนโลยีสารสนเทศ

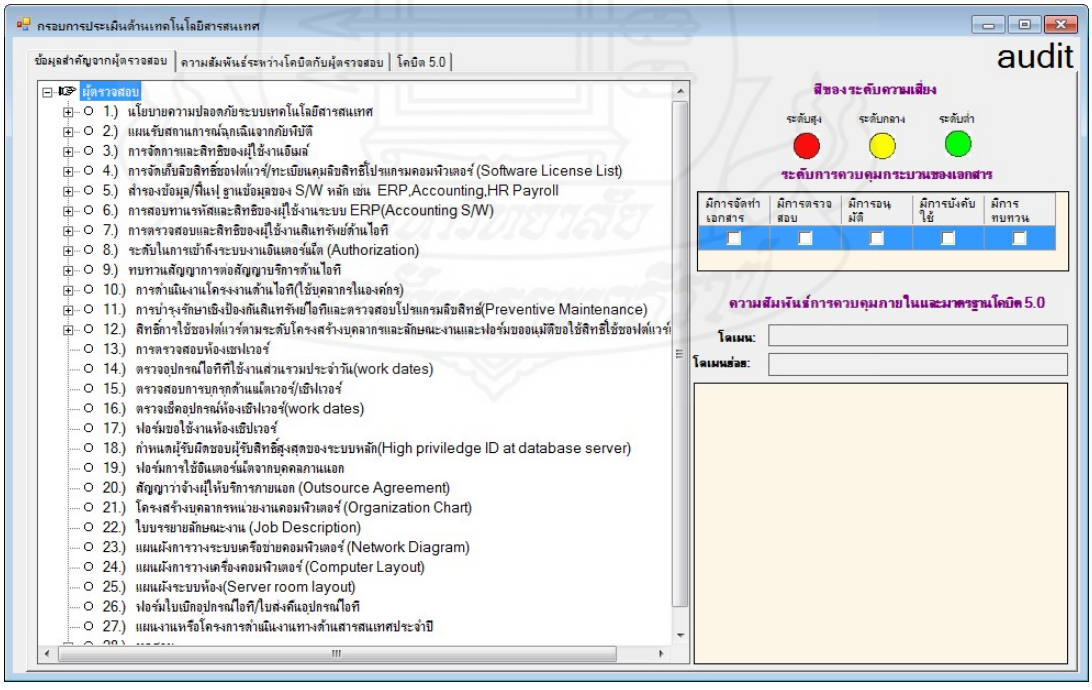
ภาพทั่วไป



การเปิดใช้งานการกรอบประเมินตนเองด้านเทคโนโลยีสารสนเทศ

คลิกหรือเลือกที่ไอคอน"วง"

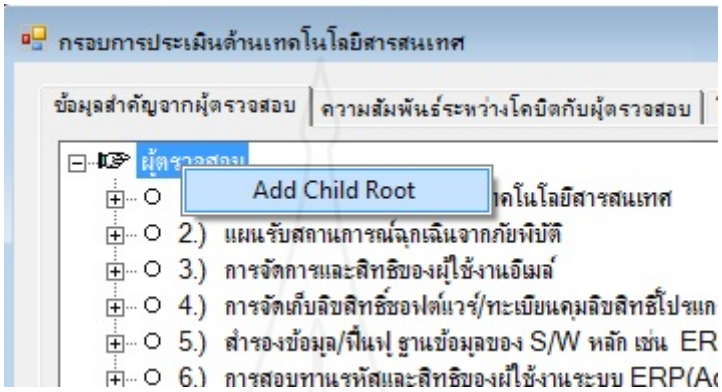




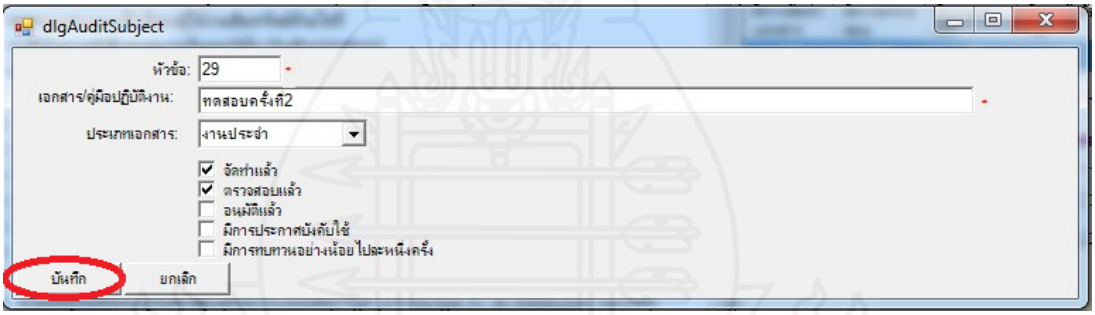
การเพิ่มข้อมูล

การเพิ่มที่รูท

โดยการเลือกข้อมูลที่รูทแล้วคลิกขวาที่เมาส์ เลือก “ Add Child Root”

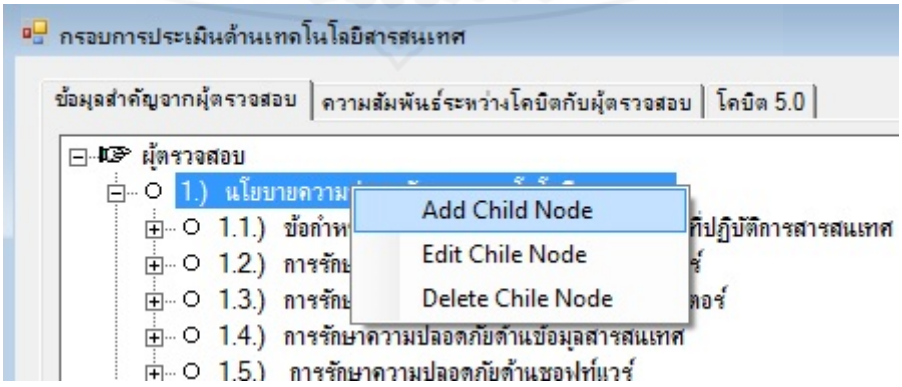


ป้อนข้อมูล แล้วคลิกปุ่ม “บันทึก”

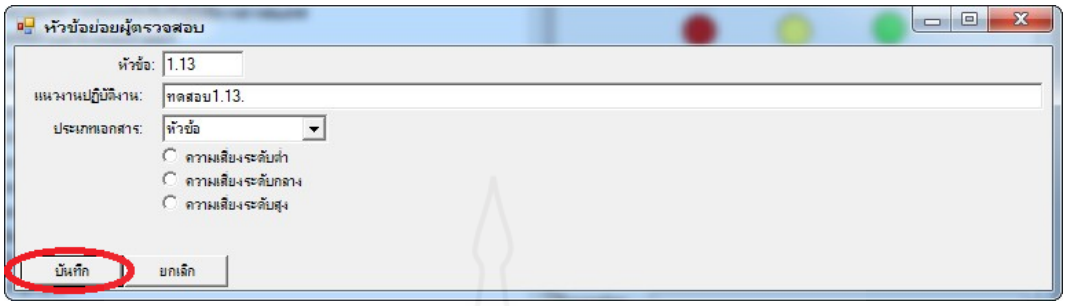


การเพิ่มที่โหนดลูก

โดยการเลือกตำแหน่งโหนดที่ต้องการแล้วคลิกขวาที่เมาส์ เลือก “ Add Child Node”

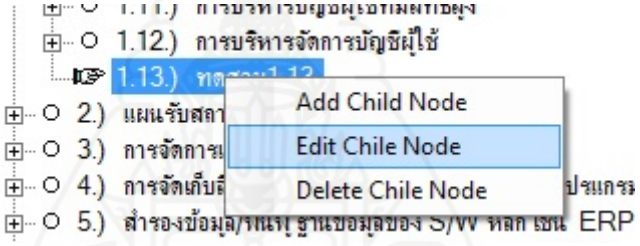


ป้อนข้อมูล แล้วคลิกปุ่ม “บันทึก”

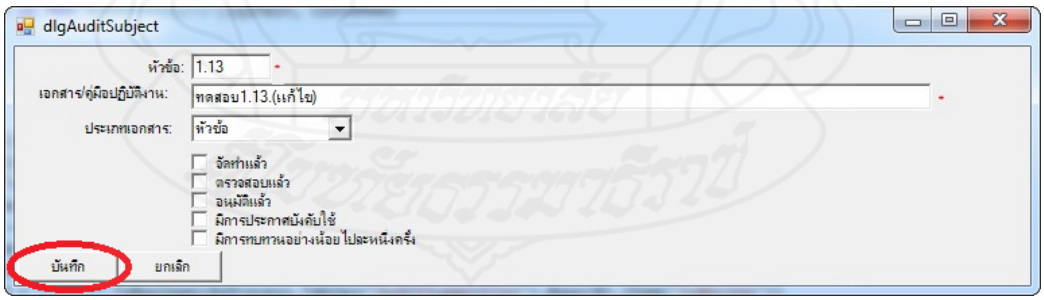


การแก้ไขข้อมูล

โดยการเลือกตำแหน่งโหนดที่ต้องการแล้วคลิกขวาที่เมาส์ เลือก “ Edit Child Node”

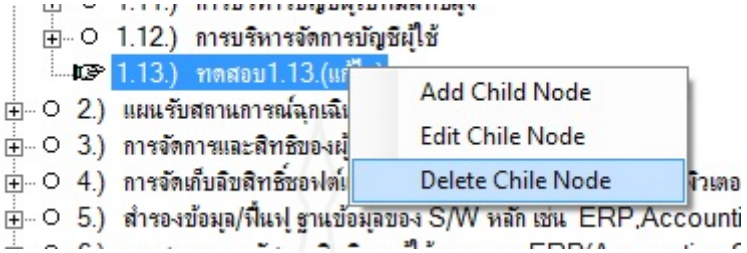


แก้ไขข้อมูล แล้วคลิกปุ่ม “บันทึก”

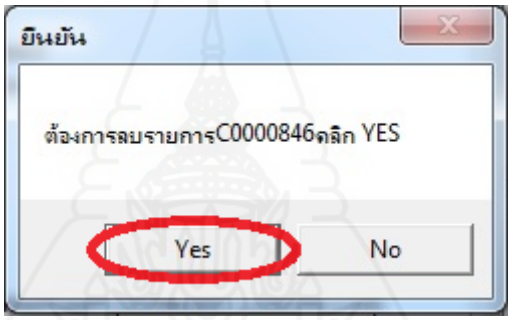


การลบข้อมูล

โดยการเลือกตำแหน่งโหนดที่ต้องการแล้วคลิกขวาที่เมาส์ เลือก “ Delete Child Node”

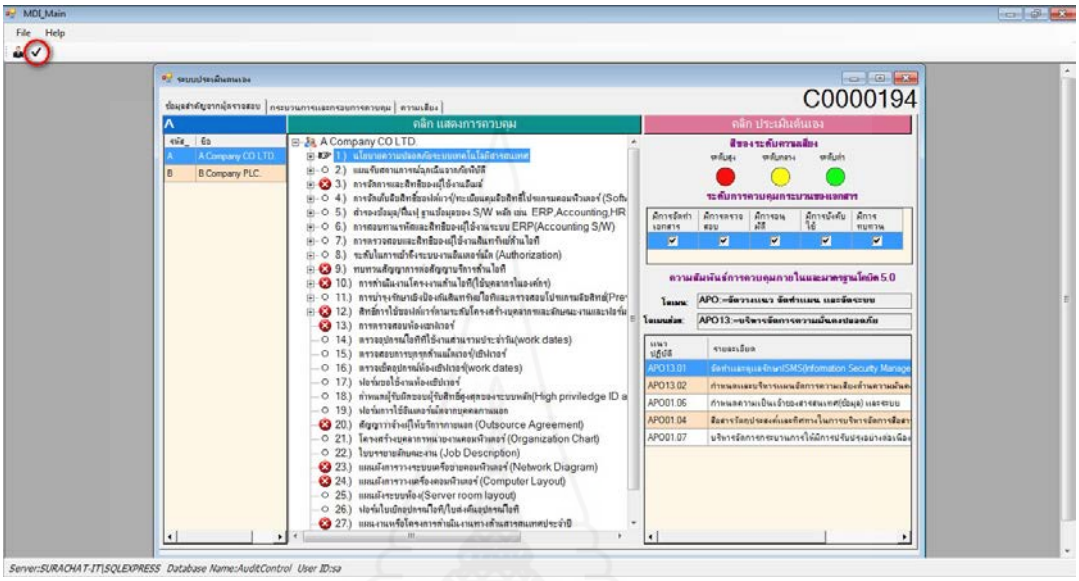


คลิก “Yes” เพื่อยืนยันการลบ



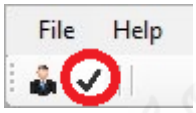
ระบบการประเมินการตรวจสอบภายในด้วยตนเองด้านเทคโนโลยีสารสนเทศ

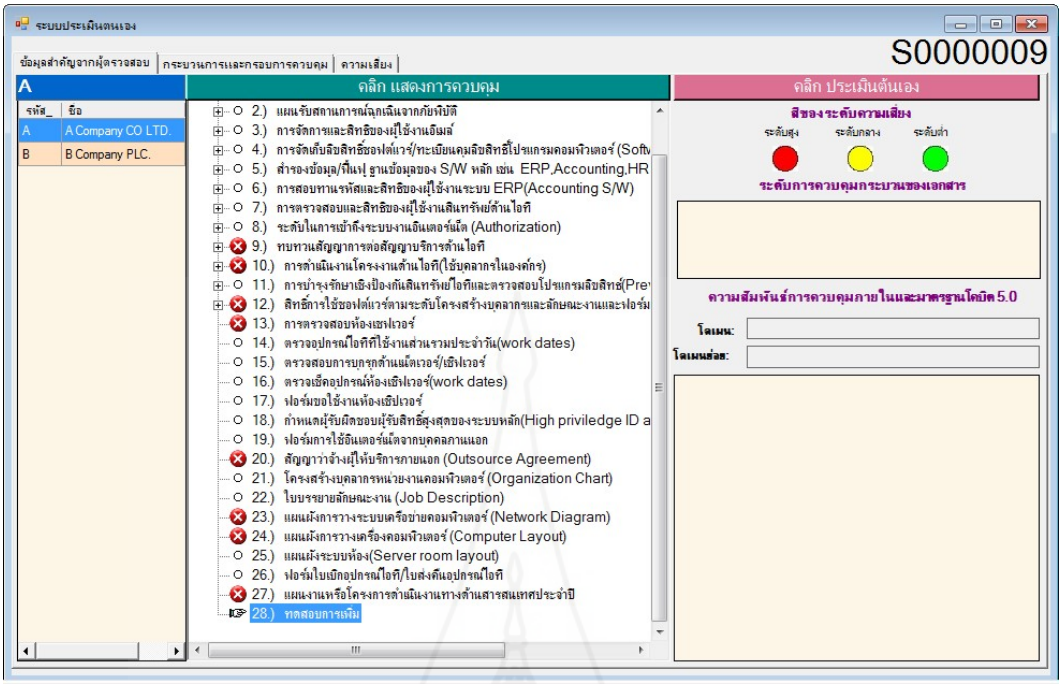
ภาพทั่วไป



การเปิดใช้งานการกรอบประเมินตนเองด้านเทคโนโลยีสารสนเทศ

คลิกหรือเลือกที่ไอคอน"วง"





การเพิ่มข้อมูล

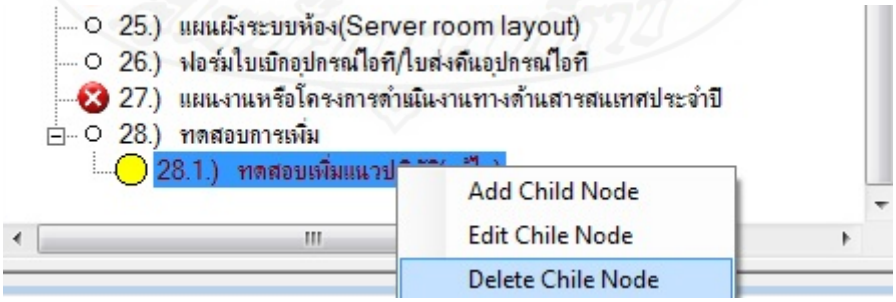
เหมือนการเพิ่มข้อมูลของระบบ”**กรอบการประเมินตนเอง**” ทั้ง (1) รูท (2) โหนดลูก

การแก้ไขข้อมูล

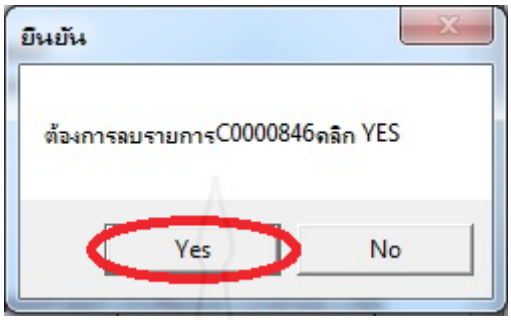
เหมือนการแก้ไขข้อมูลของระบบ”**กรอบการประเมินตนเอง**”

การลบข้อมูล

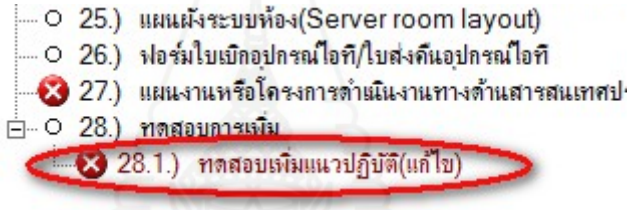
โดยการเลือกตำแหน่งโหนดที่ต้องการแล้วคลิกขวาที่เมาส์ เลือก “ Delete Child Node”



คลิก “Yes” เพื่อยืนยันการลบ

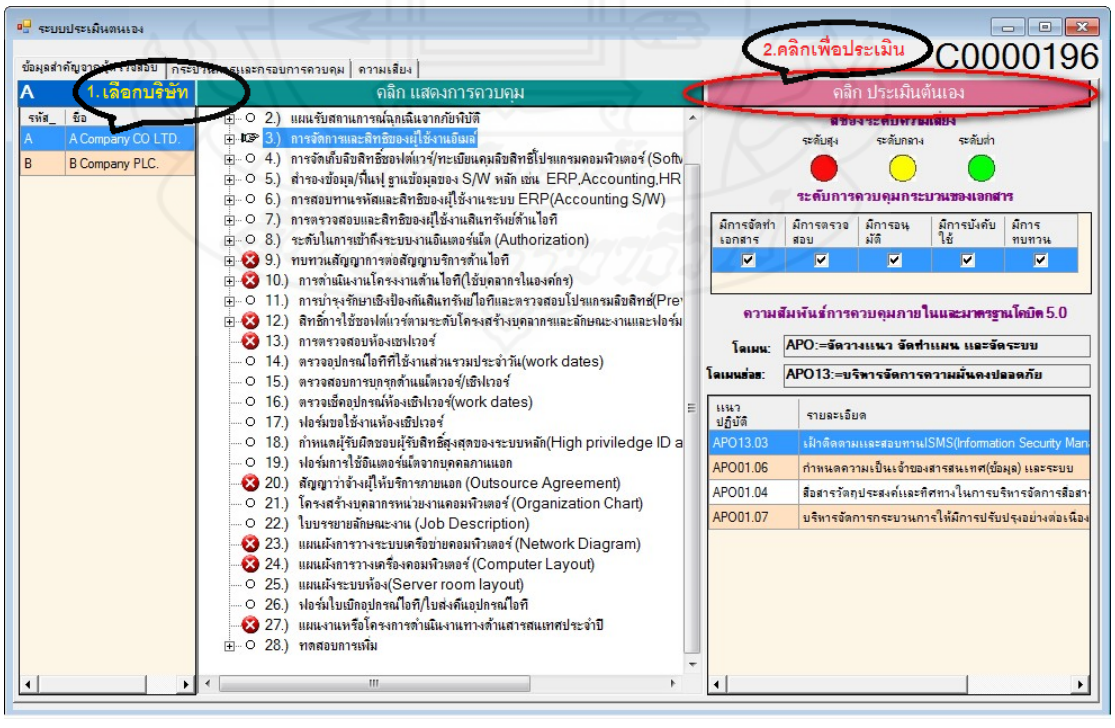


เมื่อรายการใดลบเครื่องหมายจะแสดงดังรูปด้านล่าง

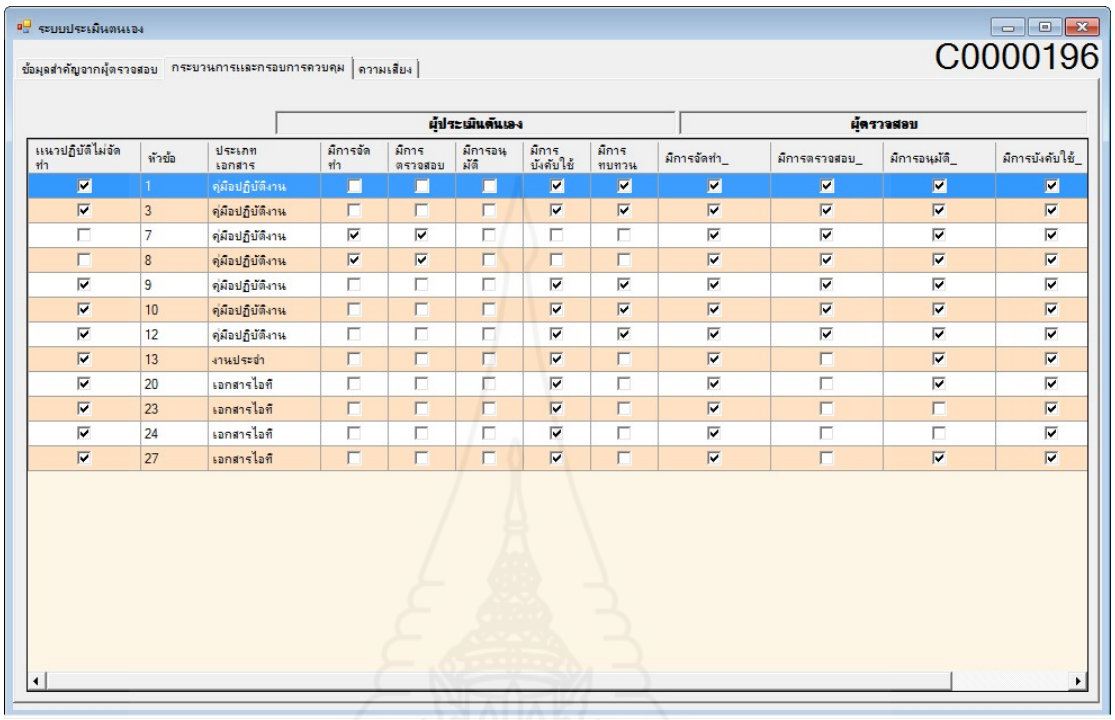


การแนะแนวตรวจสอบภายในให้ผู้ประเมิน

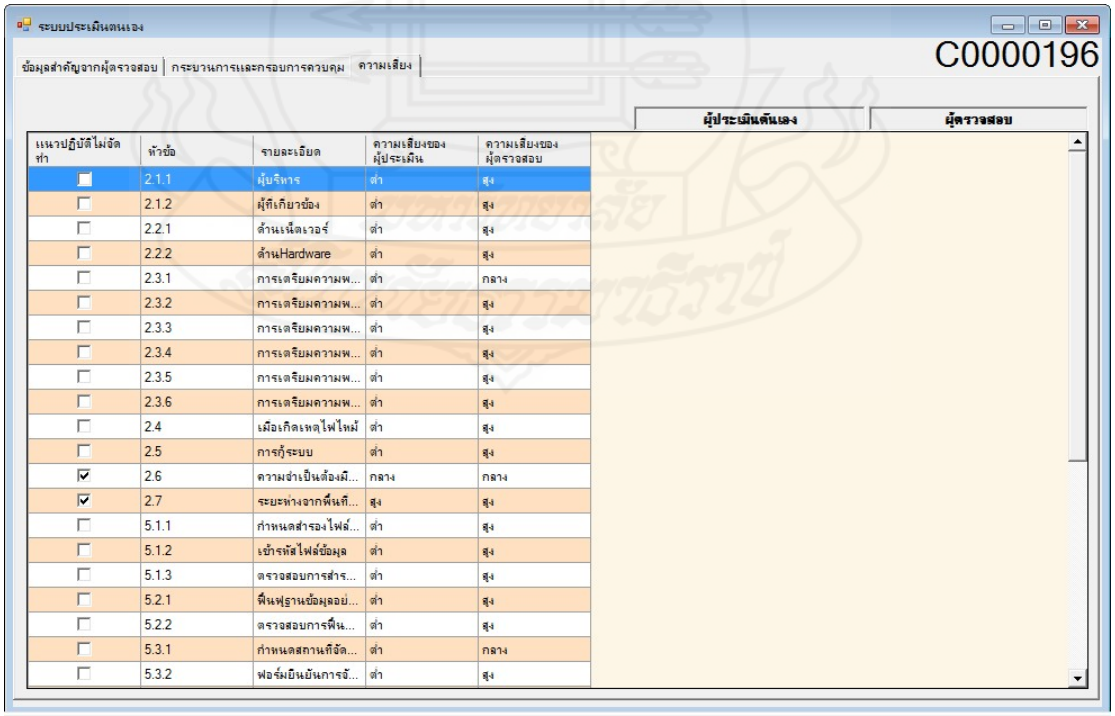
เลือกบริษัทที่ต้องการตรวจสอบ เช่น บริษัท ”A” จากนั้นคลิกที่ปุ่ม “คลิก ประเมินตนเอง”



ระบบประเมินแจ้งกระบวนการควบคุมที่ต้องจัดทำเพิ่ม



ระบบประเมินแจ้งแนวปฏิบัติที่ต้องจัดทำเพิ่ม



ที่ ศธ 0522.25/ 391

สาขาวิชาวิทยาศาสตร์และเทคโนโลยี
มหาวิทยาลัยสุโขทัยธรรมาธิราช
ตำบลบางพูด อำเภอปากเกร็ด
จังหวัดนนทบุรี 11120

21 มีนาคม 2559

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาสัมภาษณ์ เพื่อประกอบการวิจัย

เรียน ผู้บริหารผู้ที่มีรายชื่อผู้สอบบัญชีที่ได้รับความเห็นชอบของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

สิ่งที่ส่งมาด้วย โครงการวิทยานิพนธ์ จำนวน 1 แผ่น

ด้วยนายสุรชาติ จันทสุวรรณ นักศึกษาระดับบัณฑิตศึกษา รหัส 2549600530 แขนงวิชาสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช กำลังทำวิทยานิพนธ์ เรื่อง ระบบสนับสนุนการตรวจสอบการควบคุมภายในโดยกรอบงานโคบิต เพื่อเตรียมความพร้อมของบริษัทจดทะเบียนในกลุ่มอุตสาหกรรมทรัพยากร ในตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย และงานวิจัยดังกล่าวจำเป็นต้องใช้ข้อมูลงานวิจัยให้เกิดความสำเร็จเพื่อเผยแพร่ผลงานวิจัยที่เป็นคุณูปการแก่องค์กรและผู้สนใจต่อไป โดยจะเผยแพร่ข้อมูลที่ไม่ระบุตัวตน เผยแพร่เพียงตำแหน่งงาน ประสบการณ์การทำงาน ที่มาจากกลุ่มรายชื่อของผู้สอบบัญชีที่ได้รับความเห็นชอบของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์เท่านั้น โดยมีรองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์ เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์

ในการนี้ นักศึกษาจำเป็นจะต้องสัมภาษณ์ข้อมูลเพื่อการวิจัย เรื่อง ระบบสนับสนุนการตรวจสอบการควบคุมภายในโดยกรอบงานโคบิต เพื่อเตรียมความพร้อม ของบริษัทจดทะเบียนในกลุ่มอุตสาหกรรมทรัพยากร ในตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย ตั้งแต่วันที่ 21 มีนาคม – 29 เมษายน 2559 จึงขอความอนุเคราะห์จากท่านในการอนุญาตให้ นายสุรชาติ จันทสุวรรณ ได้ดำเนินการสัมภาษณ์ข้อมูลเพื่อการวิจัย ตามวัน เวลา และรายละเอียดที่นักศึกษาเสนอมาพร้อมนี้ หวังเป็นอย่างยิ่งจะได้รับความกรุณาจากท่าน และขอขอบคุณมา ณ โอกาสนี้

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ด้วย จะขอบคุณยิ่ง

ขอแสดงความนับถือ

(รองศาสตราจารย์ณัฏฐพร พิมพายน)
ประธานกรรมการประจำสาขาวิชาวิทยาศาสตร์และเทคโนโลยี

บัณฑิตศึกษา สาขาวิชาวิทยาศาสตร์และเทคโนโลยี
โทร. 02-5048192

ที่ ศธ 0522.25/ ๙๔๒

สาขาวิชาวิทยาศาสตร์และเทคโนโลยี
มหาวิทยาลัยสุโขทัยธรรมาธิราช
ตำบลบางพูด อำเภอปากเกร็ด
จังหวัดนนทบุรี 11120

๒๑ มิถุนายน 2559

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาสัมภาษณ์ เพื่อประกอบการวิจัย

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ

สิ่งที่ส่งมาด้วย โครงการวิทยานิพนธ์ จำนวน 1 แผ่น

ด้วยนายสุรชาติ จันทสุวรรณ นักศึกษาระดับบัณฑิตศึกษา รหัส 2549600530 แขนงวิชาสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช กำลังทำวิทยานิพนธ์ เรื่อง ระบบสนับสนุนการตรวจสอบการควบคุมภายในโดยกรอบงานโคบิต เพื่อเตรียมความพร้อมของบริษัทจดทะเบียนในกลุ่มอุตสาหกรรมทรัพยากร ในตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย และงานวิจัยดังกล่าวจำเป็นต้องใช้ข้อมูลงานวิจัยให้เกิดความสำเร็จเพื่อเผยแพร่ผลงานวิจัยที่เป็นคุณูปการแก่องค์กรและผู้สนใจต่อไป โดยจะเผยแพร่ข้อมูลที่ไม่ระบุตัวตน เผยแพร่เพียงตำแหน่งงาน ประสบการณ์การทำงาน ที่มาจากกลุ่มรายชื่อของผู้สอบบัญชีที่ได้รับความเห็นชอบของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์เท่านั้น โดยมีรองศาสตราจารย์

ในการนี้ นักศึกษาจำเป็นจะต้องสัมภาษณ์ข้อมูลเพื่อการวิจัย เรื่อง ระบบสนับสนุนการตรวจสอบการควบคุมภายในโดยกรอบงานโคบิต เพื่อเตรียมความพร้อม ของบริษัทจดทะเบียนในกลุ่มอุตสาหกรรมทรัพยากร ในตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย ตั้งแต่วันที่ 15 มิถุนายน – 30 กรกฎาคม 2559 จึงขอความอนุเคราะห์จากท่านในการอนุญาตให้ นายสุรชาติ จันทสุวรรณ ได้ดำเนินการสัมภาษณ์ข้อมูลเพื่อการวิจัย ตามวันเวลา และรายละเอียดที่นักศึกษาเสนอมาพร้อมนี้ หวังเป็นอย่างยิ่งจะได้รับความกรุณาจากท่าน และขอขอบคุณมา ณ โอกาสนี้

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ด้วย จะขอบคุณยิ่ง

ขอแสดงความนับถือ

(รองศาสตราจารย์ณัฏฐพร พิมพายน)
ประธานกรรมการประจำสาขาวิชาวิทยาศาสตร์และเทคโนโลยี

บัณฑิตศึกษา สาขาวิชาวิทยาศาสตร์และเทคโนโลยี
โทร. 02-5048192

บรรณานุกรม

บรรณานุกรม

กัลยา ใจรักษ์,ประสงค์ ปราณีตพลกรัง. (2554). *ธรรมาภิบาลด้านไอที*.สืบค้นจาก http://www.spu.ac.th/ graduate/ files /2011/03/IT-Governance-Tutorial_kallaya.pdf

จริยา ไข่มุกด์. (2554). *การนำไอทิลมาประยุกต์ใช้ในการบริหารจัดการระบบสารสนเทศของโรงพยาบาลศิครินทร์ (ITIL Version 2 For Sikarin Hospital).* (วิทยานิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์), มหาวิทยาลัยเทคโนโลยีมหานคร กรุงเทพฯ.

ตลาดหลักทรัพย์แห่งประเทศไทย. (2558). *โครงสร้างการจัดกลุ่มอุตสาหกรรมและหมวดธุรกิจของตลาดหลักทรัพย์ฯ* สืบค้นจาก https://www.set.or.th/th/products/index/files/2015-2-12_SET-Industry-Group-Sector-Classification-Final-version_V1.pdf.

ตลาดหลักทรัพย์แห่งประเทศไทย.การจัดกลุ่มอุตสาหกรรมและหมวดธุรกิจ. สืบค้นจาก http://www .set .or .th /th/regulations/simplified_regulations/industry_sector_p1.html.

ตลาดหลักทรัพย์แห่งประเทศไทย.การจดทะเบียนหลักทรัพย์.สืบค้นจาก http://www.set.or.th/th/faqs/listing_p1.html#1,Going Public Guide.

นิตยา สิงไทยสงค์. (2557). *การพัฒนาแนวปฏิบัติและต้นแบบระบบการตรวจสอบการพัฒนาซอฟต์แวร์และควบคุมคุณภาพ ซอฟต์แวร์ตามแนวมาตรฐาน ISO/IEC 29110.)* (วิทยานิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยสุโขทัยธรรมาธิราช นนทบุรี.

ประสิทธิ์ ธีรวงศธร. (2556). *การประเมินการบริหารโครงการสารสนเทศ โดยใช้หลักธรรมาภิบาลไอที: กรณีของบริษัท เมืองทองมหาชัย จำกัด.* (วิทยานิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์), มหาวิทยาลัยสุโขทัยธรรมาธิราช, นนทบุรี.

ปริญญา อินทร์คง. (2555). บทบาทของผู้บริหารกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ.สืบค้นจาก http://www0.tint.or.th/nkc/nkc55/content55/nstkc55-041.html. .(2008). ISO 38500 (2008). ISO/IEC 38500: 2008 Corporate Governance of Information Technology. ISO/IEC. 2008.สืบค้นจาก www.iso.org.

ผศ.ดร.สันติพัฒน์ อรุณธารี. (2555). *การจัดการเทคโนโลยีสารสนเทศและการสื่อสารเชิงกลยุทธ์.* (พิมพ์ครั้งที่ 1) นนทบุรี มหาวิทยาลัยสุโขทัยธรรมาธิราช.

ระวีวรรณ จันทร์อินทร์,นางธัญญารัตน์ สีโสภาพันธุ์, นางสาวพรรณนิภา อาพันกาญจน์. (2555). จุลสารตรวจสอบภายใน ฉบับที่ 89.ประเทศไทย.กรมบัญชีกลาง

สมาคมผู้ตรวจสอบภายในแห่งประเทศไทยและตลาดหลักทรัพย์แห่งประเทศไทย. (2555). ความ*เสี่ยงและการควบคุมด้านเทคโนโลยีสารสนเทศ.1*.กรุงเทพฯ เมจิกเพรส.

อังสนา ศรีประเสริฐ. (2553). การบริหารความเสี่ยงกับงานตรวจสอบภายใน.*วารสารวิชาการ* มหาวิทยาลัยหอการค้าไทย. 30 (1), 151.

ISACA. (2012). *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT.* United States of America.

ISACA. (2012). *COBIT 5 Enabling Processes.* United States of America.

ประวัติผู้วิจัย

ชื่อ	นายสุรชาติ จันทสุวรรณ
วัน เดือน ปี	3 กรฎาคม 2512
สถานที่เกิด	เขตลุมพินี กรุงเทพมหานคร
สถานที่เกิด	1. วท.บ. สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยรามคำแหง
	2. บริหารธุรกิจมหาบัณฑิต สาขาวิชาวิทยาการจัดการ แขนงวิชา บริหารธุรกิจ มหาวิทยาลัยสุโขทัยธรรมาธิราช
สถานที่ทำงาน	บริษัท เอเชีย กรีน เอนเนอจี จำกัด (หมาชน)
	เขตบางขุนเทียน กรุงเทพมหานคร
ตำแหน่ง	ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ