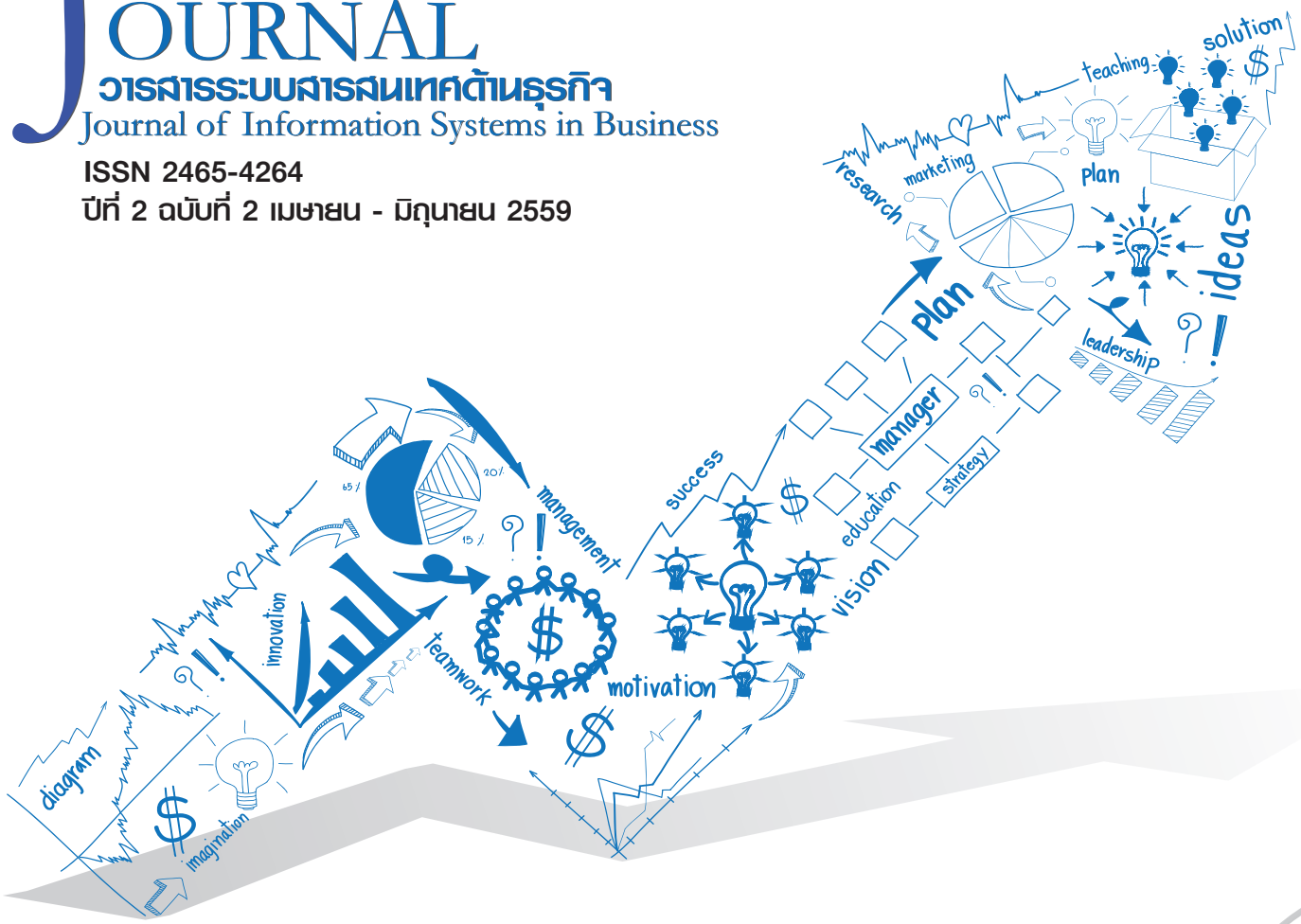
JISB JOURNAL
วารสารระบบสารสนเทศด้านธุรกิจ
Journal of Information Systems in Business
ISSN 2465-4264
ปีที่ 2 ฉบับที่ 2 เมษายน - มิถุนายน 2559



บทความ

พฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว ภายใน Public Cloud

ปัจจัยที่มีผลต่อความสำเร็จในการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืน
กรณีศึกษา : บริษัท โกซอฟท์ (ประเทศไทย) จำกัด

แนวทางในการเสริมสร้างความตระหนักถึงการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล

และอื่นๆ...

MSMIS THAMMASAT BUSINESS SCHOOL

EFMD EQUIS ACCREDITED

www.jisb.tbs.tu.ac.th

SECURITY

บทความวิจัย

บทความการวางแผนด้านเทคโนโลยีสารสนเทศ

บทวิจารณ์หนังสือ

บทบรรณาธิการ

เรียน ผู้อ่านทุกท่าน

การรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เป็นสิ่งที่มีความสำคัญและไม่สามารถมองข้ามได้ จะเห็นได้ว่าภัยคุกคามที่เกิดขึ้นกับเทคโนโลยีสารสนเทศเป็นภัยคุกคามใหม่ๆ ที่เกิดขึ้นตามความก้าวหน้าของเทคโนโลยี แต่ธุรกิจและบุคคลที่ใช้งานเทคโนโลยีอาจละเลยการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศไป วารสารฉบับนี้กล่าวถึงวิจัยที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศในรูปแบบต่างๆ นอกจากนี้ยังกล่าวถึงบทความที่เกี่ยวกับแผนกลยุทธ์ระบบเทคโนโลยีสารสนเทศด้วย

กองบรรณาธิการ

เจ้าของ

โครงการปริญญาโทสาขาวิชาระบบสารสนเทศเพื่อการจัดการ (Master of Science Program in Management Information Systems – MSMIS) คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

บรรณาธิการ

รองศาสตราจารย์ ดร.นิตยา วงศ์ภินันท์วัฒนา	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

กองบรรณาธิการบริหาร

ศาสตราจารย์ ดร.ศิริลักษณ์ โรจนกิจอำนวย	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
รองศาสตราจารย์กิตติ สิริพัลลภ	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
รองศาสตราจารย์ปัญจราศี ปุณณชัยยะ	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ผู้ช่วยศาสตราจารย์ ดร.มฑุปายาส ทองมาก	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ผู้ช่วยศาสตราจารย์ ดร.ปิเตอร์ รักธรรม	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ผู้ช่วยศาสตราจารย์ ดร.ลัดดาวัลย์ แก้วกิติพงษ์	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ผู้ช่วยศาสตราจารย์โอภาศ โสตถิลักษณ์	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ผู้ช่วยศาสตราจารย์วันชัย ขันตี	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

กองบรรณาธิการกลั่นกรองบทความ (ภายใน)

รองศาสตราจารย์ ดร.ศากุน บุญอิต	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
อาจารย์ ดร.พัฒน์ธนะ บุญชู	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
อาจารย์ ดร.ปณิธาน จันทองจีน	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

กองบรรณาธิการกลั่นกรองบทความ (ภายนอก)

ศาสตราจารย์ ดร.อุทัย ตันละมัย	คณะพาณิชยศาสตร์และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย
ศาสตราจารย์ ดร.วิลาศ วูวงศ์	อธิการบดี มหาวิทยาลัยเอเชียน (Asian University)
รองศาสตราจารย์ ดร.ครรชิต มาลัยวงศ์	ราชบัณฑิต สาขาวิชาคอมพิวเตอร์
รองศาสตราจารย์ ดร.ณรงค์ สมพงษ์	คณะศึกษาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์
ผู้ช่วยศาสตราจารย์ ดร.ชัชพงศ์ ตั้งมณี	คณะพาณิชยศาสตร์และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย
ผู้ช่วยศาสตราจารย์ ดร.นิลุบล ศิวบวรวัฒนา	คณะบริหารธุรกิจ มหาวิทยาลัยศรีปทุม
ผู้ช่วยศาสตราจารย์ ดร.ภัทร์ พลอยแหวน	คณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล
ผู้ช่วยศาสตราจารย์ ดร.พิศสมัย อรทัย	คณะแพทยศาสตร์โรงพยาบาลรามาธิบดี มหาวิทยาลัยมหิดล
อาจารย์ ดร.วิเลิศ ภูริวัชร	คณะพาณิชยศาสตร์และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย
อาจารย์ ดร.พิมพ์มณี รัตนวิชา	คณะพาณิชยศาสตร์และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย
ดร.เฉลิมศักดิ์ เลิศวงศ์เสถียร	ศูนย์เทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงการคลัง
ดร.สันติพัฒน์ อรุณธารี	ประธานฝ่ายสารสนเทศ บริษัท พีทีที ไอซีที โซลูชั่นส์ จำกัด

วัตถุประสงค์

วารสาร JISB เป็นวารสารทางวิชารูปแบบวารสารอิเล็กทรอนิกส์ เพื่อเป็นแหล่งเผยแพร่ทางวิชาการและเป็นสื่อกลางแลกเปลี่ยนความคิดเห็นเชิงวิชาการของอาจารย์ นักวิจัย นักวิชาการ และนักศึกษาทั้งภายในและภายนอกคณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์ บทความที่รับพิจารณาเผยแพร่วารสารครอบคลุมสาขาเทคโนโลยีสารสนเทศ ที่เน้นการใช้เทคโนโลยีสารสนเทศเพื่อธุรกิจเป็นหลัก ผลงานที่จะนำมาเผยแพร่ในวารสารนี้ ผ่านกระบวนการ Peer Review เพื่อให้วารสารมีคุณภาพระดับมาตรฐานสากล สามารถนำไปอ้างอิงได้ ประเภทของผลงานที่เผยแพร่ประกอบด้วย

- บทความวิจัย เป็นผลงานทางวิชาการที่ได้รับการศึกษาค้นคว้าตามระเบียบวิธีวิจัยด้านเทคโนโลยีสนเทศที่เน้นทางธุรกิจเป็นหลัก
- บทความการวางแผนด้านเทคโนโลยีสารสนเทศ เป็นผลงานวิชาการที่ได้รับการศึกษาค้นคว้าที่เน้นการนำเทคโนโลยีสารสนเทศมาสร้างกลยุทธ์ให้กับองค์กร
- บทความด้านการพัฒนาระบบสารสนเทศ เป็นผลงานที่แสดงสิ่งประดิษฐ์ ความก้าวหน้าทางวิชาการ หรือเสริมสร้างองค์ความรู้ด้านเทคโนโลยีสารสนเทศที่เน้นทางธุรกิจเป็นหลัก
- บทความวิชาการ เป็นผลงานที่เรียบเรียงจากเอกสารทางวิชาการ ซึ่งเสนอแนวความคิดหรือความรู้ทั่วไปด้านเทคโนโลยีสารสนเทศที่เป็นประโยชน์กับธุรกิจ
- บทวิจารณ์หนังสือ เป็นการนำเสนอและวิจารณ์หนังสือที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่เน้นทางธุรกิจซึ่งแสดงให้เห็นถึงองค์ความรู้ใหม่ที่น่าติดตาม

จึงขอเชิญชวนผู้สนใจจากสถาบันและหน่วยงานต่างๆ ส่งผลงานดังกล่าวข้างต้น มาลงตีพิมพ์ในวารสาร JISB โดยไม่ต้องเสียค่าใช้จ่ายใดๆ ทั้งสิ้น

การเผยแพร่

เป็นวารสารอิเล็กทรอนิกส์กำหนดการเผยแพร่ ปีละ 4 ฉบับ

- ฉบับที่ 1 เดือนมกราคม – มีนาคม
- ฉบับที่ 2 เดือนเมษายน – มิถุนายน
- ฉบับที่ 3 เดือนกรกฎาคม – กันยายน
- ฉบับที่ 4 เดือนตุลาคม – ธันวาคม

โดยเผยแพร่ที่ http://jisb.tbs.tu.ac.th

พฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public Cloud

นิธิป ชวนตันติกมล*

Digital Media Asia Pacific (Toyota Group)

***Correspondence:** z_generation@hotmail.com doi: 10.14456/jisb.2016.7

บทคัดย่อ

งานวิจัยนี้นำเสนอผลการศึกษาเกี่ยวกับพฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public Cloud ซึ่งส่งผลต่อปัจจัยการรับรู้ถึงจุดอ่อน การรับรู้ความรุนแรงของภัยคุกคาม การรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัว การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม การรับรู้ความสามารถของตนเองในการรับมือภัยคุกคาม การรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว แรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว ความตระหนักในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว และพฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว โดยเก็บข้อมูลจากกลุ่มตัวอย่างผู้มีประสบการณ์ในการใช้งาน Public Cloud จำนวน 290 คน ผ่านการแจกแบบสอบถามออนไลน์ ผู้วิจัยได้ตรวจสอบความเที่ยงของเครื่องมือ (Reliability Analysis) ตรวจสอบแบบสอบถามโดยการวิเคราะห์องค์ประกอบ (Factor Analysis) และทดสอบสมมติฐานตามแบบจำลองโดยใช้การวิเคราะห์การถดถอยเชิงพหุคูณ (Multiple Regression Analysis) ระยะเวลาดำเนินงาน เดือนกุมภาพันธ์ – เมษายน 2558 มีผลการวิจัยดังนี้

ปัจจัยที่ส่งผลโดยตรงต่อการรับรู้ถึงภัยคุกคาม (Perceived Threat) ประกอบด้วย ปัจจัยการรับรู้ถึงจุดอ่อน (Perceived Susceptibility) ปัจจัยการรับรู้ความรุนแรง (Perceived Severity) ปัจจัยที่ส่งผลโดยตรงต่อการรับรู้ความสามารถในการหลีกเลี่ยง (Pereived Avoidability) ประกอบด้วย ปัจจัยการรับรู้ประสิทธิผล (Perceived Effectiveness) การรับรู้ค่าใช้จ่าย (Perceived Costs) และปัจจัยการรับรู้ประสิทธิภาพของตนเอง (Self-Efficacy) ปัจจัยที่ส่งผลโดยตรงต่อพฤติกรรมการหลีกเลี่ยง (Avoidance Behavior) ประกอบด้วย ปัจจัยแรงจูงใจในการหลีกเลี่ยง (Avoidance Motivation) และปัจจัยความตระหนักในการหลีกเลี่ยงภัยคุกคาม (Awareness)

จากผลการวิจัยพบว่า ตัวแปรแรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public Cloud ส่งผลต่อพฤติกรรมการหลีกเลี่ยงภัยคุกคามมากที่สุด และเมื่อศึกษาตัวแปรที่มีอิทธิพลต่อแรงจูงใจในการหลีกเลี่ยงภัยคุกคาม พบว่าตัวแปรการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามนั้นมีอิทธิพลมากที่สุด ข้อค้นพบนี้สามารถนำมาใช้พัฒนาการป้องกันภัยคุกคามโดยมุ่งวางกลยุทธ์ให้ผู้ใช้บริการเล็งเห็นประโยชน์ในการหลีกเลี่ยงและหาทางป้องกันภัยที่อาจมาคุกคามข้อมูลส่วนตัว

คำสำคัญ: การหลีกเลี่ยงภัยคุกคาม การรับรู้ภัยคุกคาม แรงจูงใจในการหลีกเลี่ยงภัยคุกคาม พฤติกรรมการหลีกเลี่ยงภัยคุกคาม

Threat Avoidance Behavior of Privacy on Public Cloud

Nithip Chuantantigamol*

Digital Media Asia Pacific (Toyota Group)

***Correspondence:** z_generation@hotmail.com doi: 10.14456/jisb.2016.7

Abstract

The purpose of this research is to identify the effect of Perceived Susceptibility, Perceived Severity, Perceived Threat, Perceived Effectiveness, Perceived Costs, Self-Efficacy, Perceived Avoidability, Avoidance Motivation and Awareness on the Behavior of Threat Avoidance on Public Cloud. Participants in this study were 290 people who have experience in using Public Cloud. The research material is online questionnaire which was shared via online media. The researcher has gone through Reliability Analysis to test the precision of tools, Factor Analysis to test the survey, and Multiple Regression Analysis to test the hypothesis of the model between February – April 2015.

The result shows that Perceived Threat has a direct impact on Perceived Susceptibility and Perceived Severity. Perceived Avoidability has a direct impact on Perceived Effectiveness and Perceived Costs and Self-Efficacy. Avoidance Behavior has a direct impact on Avoidance Motivation and Awareness.

The finding illustrates that “Avoidance Motivation” is the most influential factor effecting to Threat Avoidance Behavior, while the strongest factor effecting Avoidance Motivation is Perceived Avoidability. This insight could be exploited to prevent from Threats by focusing on how to convince people to perceived benefits from Threat Avoidance and find the method to protect personal information.

Keywords: Threat Avoidance, Perceived Threat, Avoidance Motivation, Avoidance Behavior

1. บทนำ

ปัจจุบันเทคโนโลยีด้านข้อมูลเปรียบเสมือนดาบสองคม เมื่อเทคโนโลยีเหล่านี้ได้รับการควบคุมที่ถูกต้องและเหมาะสม จะทำให้มีศักยภาพที่จะพัฒนาคุณภาพของมนุษย์และองค์กรต่างๆ อย่างไรก็ตามหากมีการนำเอาเทคโนโลยีด้านข้อมูลไปใช้ประโยชน์เพื่อวัตถุประสงค์ที่เป็นอันตราย มันจะเป็นภัยคุกคามที่ร้ายแรงต่อบุคคล องค์กรและสังคม ในหลายรูปแบบของการรุกรานด้านข้อมูลสารสนเทศ ดังเช่น ไวรัสคอมพิวเตอร์ หนอนเจาะระบบ อีเมลสแปม สปายแวร์ แอดแวร์และโทรจัน ซึ่งจะมีผลกระทบคอมพิวเตอร์ส่วนบุคคลและแม้แต่โครงสร้างพื้นฐานทางสารสนเทศขององค์กร ส่งผลเสียต่อผลผลิตและสูญเสียทางการเงิน (Bagchi and Udo, 2003; Stafford and Urbaczewski, 2004)

องค์ประกอบของความแตกต่างที่ทำให้เทคโนโลยีสารสนเทศประสบความสำเร็จคือ ความสามารถที่ทำให้ทุกอย่างกลายเป็นจริง มีคุณค่าและมีส่วนช่วยในการสนับสนุนทางเศรษฐกิจแก่โครงสร้างพื้นฐานของโลกแห่งเทคโนโลยี Cloud Computing จึงได้เข้ามาตอบรับโครงสร้างพื้นฐานนี้ และยังสร้างการวิจัยในโลกเสมือนขึ้นมา มีการประมวลผลแบบกระจายหรือที่เรียกว่า “Grid Computing” ใช้ประโยชน์ในการประมวลผล รวมถึงเชื่อมต่อเครือข่าย เว็บไซต์และบริการทางด้านซอฟต์แวร์ เป็นการแสดงถึงสถาปัตยกรรมที่มุ่งเน้นด้านการบริการ ลดข้อมูลทางเทคโนโลยีสำหรับผู้ใช้งานที่ปลายทาง มีความยืดหยุ่นสูงและลดต้นทุนในการให้บริการ (Vouk, 2008)

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

งานวิจัยนี้มีการนำทฤษฎีอ้างอิงมาใช้คือ Technology Threat Avoidance Model (TTAT) เป็น ทฤษฎีแยกแยะผู้ใช้บริการว่ามีความเข้าใจในเทคโนโลยี ซึ่งส่งผลต่อพฤติกรรมการหลีกเลี่ยงความเสี่ยงจากภัยคุกคามโดยจะแบ่งเป็นกรอบการประเมินภัยคุกคาม (Threat Appraisal) ประกอบด้วย การรับรู้ถึงความอ่อนไหวง่าย (Perceived Susceptibility) การรับรู้ถึงความรุนแรง (Perceived Severity) การรับรู้ถึงภัยคุกคาม (Perceived Threat) กรอบการประเมินการรับมือความเสี่ยง (Coping Appraisal) ประกอบด้วย การรับรู้ประสิทธิผล (Perceived Effectiveness) การรับรู้ราคา (Perceived Costs) ประสิทธิภาพของตนเอง (Self-Efficacy) การรับรู้ความสามารถในการหลีกเลี่ยง (Perceived Avoidability) และกรอบการรับมือ (Coping) ประกอบด้วย แรงจูงใจในการหลีกเลี่ยง (Avoidance Motivation) พฤติกรรมการหลีกเลี่ยง (Avoidance Behavior) การรับมือทางอารมณ์ (Emotion-focused) ความเสี่ยงและอิทธิพลทางสังคม (Coping Risk Tolerance and Social Influence) นอกจากนี้งานวิจัยนี้ได้ทำการศึกษาจากงานวิจัยในอดีต โดยมีทั้งหมด 10 ปัจจัยดังต่อไปนี้ :

การรับรู้ถึงจุดอ่อน (Perceived Susceptibility) คือ การที่บุคคลรับรู้ถึงจุดอ่อนแอบนระบบของ Public Cloud ที่อาจถูกโจมตีหรือถูกบุกรุกโดยภัยต่างๆได้โดยง่าย (Liang and Xue, 2009) ซึ่งมาจากความอ่อนแอของระบบที่ไม่อาจป้องกันจากภัยคุกคาม

การรับรู้ความรุนแรงของภัยคุกคาม (Perceived Severity) คือ การที่บุคคลรับรู้ถึงผลกระทบจากภัยคุกคามว่าจะส่งผลด้านลบ มีสาเหตุมาจากความรุนแรงของภัยคุกคาม ซึ่งมีโอกาสส่งผลกระทบต่อระบบสารสนเทศ (Liang and Xue, 2009)

การรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัว (Perceived Threat) คือ การรับรู้ถึงอันตรายจากภัยที่อาจมาคุกคามข้อมูลส่วนตัวภายใน Public Cloud และเกิดผลกระทบต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน (รุจิราธรรมสมบัติ, 2555) ภัยคุกคามยังสามารถเปลี่ยนจากภัยคุกคามธรรมดา ไปสู่ภัยคุกคามที่อาจสร้างความเสียหายให้แก่สารสนเทศขององค์กรได้

การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว (Perceived Effectiveness) คือ การรับรู้ถึงความสามารถในการรักษาข้อมูลส่วนตัวของเครื่องมือป้องกันภัยคุกคาม ว่ามีความปลอดภัยเพียงใด ต่อภัยจากภายนอกหรือภายในที่อาจมาคุกคามข้อมูล (Weinstein, 1993)

การรับรู้ค่าใช้จ่ายของเครื่องมือป้องกันภัยคุกคามข้อมูลส่วนตัว (Perceived Costs) คือ ระดับการรับรู้ถึงค่าใช้จ่ายที่ต้องใช้ รวมถึงประโยชน์ที่จะได้รับ หากใช้เครื่องมือในการป้องกันภัยคุกคามข้อมูลส่วนตัวจาก Public Cloud (Ng et al., 2009; Woon et al., 2005; Workman et al., 2008)

การรับรู้ประสิทธิภาพของตนเองในการรับมือภัยคุกคาม (Self-Efficacy) คือ ระดับของการรับรู้ถึงความสามารถของบุคคลในการใช้เครื่องมือป้องกันเพื่อหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว (Liang and Xue, 2009) และเป็นการที่บุคคลตัดสินความสามารถของตนเองในการที่จะจัดการ โดยดำเนินการแสดงพฤติกรรมให้บรรลุเป้าหมายที่กำหนดไว้

การรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคาม (Perceived Avoiability) คือ การที่บุคคลรับรู้ว่าเครื่องมือป้องกันภัยคุกคามช่วยในการปกป้องข้อมูลและหลีกเลี่ยงจากภัยที่เข้ามาคุกคามข้อมูลส่วนตัวได้มากน้อยเพียงใด (Liang and Xue, 2009)

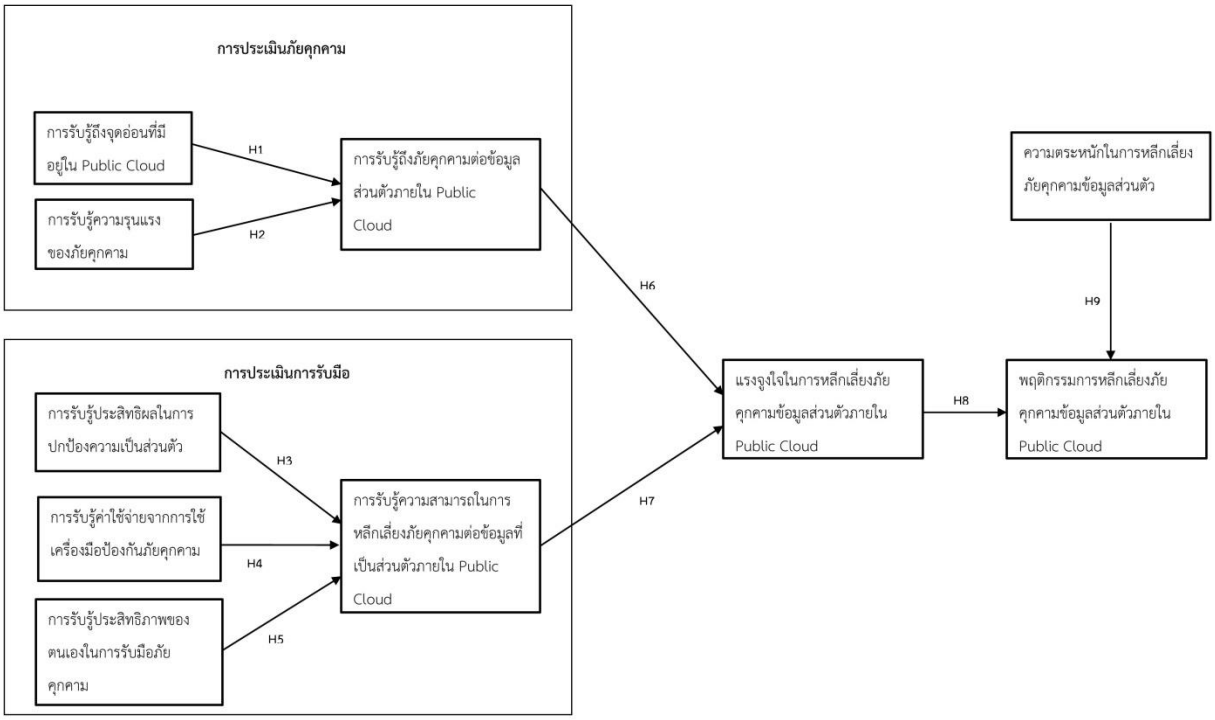
แรงจูงในในการหลีกเลี่ยง (Avoidance Motivation) คือ การที่บุคคลเกิดแรงกระตุ้นจากภัยที่มีความรู้สึกว่าอาจมาคุกคามข้อมูลส่วนตัง จึงหาทางที่จะหลีกเลี่ยงจากภัยเหล่านั้น (ธีรศักดิ์ แสงดิษฐ์, 2553)

ความตระหนัก (Awareness) คือ การรับรู้แบบฉุกคิดขึ้นมากะทันหัน ว่าภัยคุกคามที่พบนั้นอาจจะส่งผลกระทบต่อข้อมูลส่วนตัว ทั้งนี้ความตระหนักจะเกิดขึ้นได้นั้น ต้องอาศัยองค์ประกอบจาก สิ่งแวดล้อมรอบตัว การกระทำในอดีต และสิ่งที่ส่งผลกับอารมณ์และความรู้สึกเป็นต้น (เอกลักษณ์ ธนเจริญพิศาล, 2554)

พฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public Cloud (Avoidance Behavior) คือ การที่บุคคลแสดงอาการที่อาจเป็นการหลีกเลี่ยงออกมาจากสถานการณ์ที่เป็นความเสี่ยงต่อข้อมูลส่วนตัวของผู้ใช้งานบน Public Cloud (Liang and Xue, 2009)

3. กรอบแนวคิดการวิจัยและสมมติฐานการวิจัย

จากการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้องดังที่กล่าวมาข้างต้น ผู้วิจัยจึงได้พัฒนากรอบการวิจัย ดังแสดงในภาพที่ 1



ภาพที่ 1 แสดงกรอบแนวคิดเกี่ยวกับพฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว

ผลการวิจัยของ Liang and Xue (2010) พบว่า การที่บุคคลทราบว่าจุดอ่อนของระบบ Public Cloud ที่เกิดขึ้นนั้นส่งผลทำให้ถูกโจมตีโดยภัยที่เข้ามาคุกคามได้โดยง่าย จึงทำให้เกิดการรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัว นำไปสู่ข้อสมมติฐานดังนี้

H1: การรับรู้ถึงจุดอ่อนส่งผลเชิงบวกต่อการรับรู้ความเสี่ยงของภัยคุกคามข้อมูลส่วนตัวบน Public Cloud

ผลการวิจัยของ Liang and Xue (2009) พบว่า การที่บุคคลรับรู้ถึงผลกระทบจากภัยคุกคามว่าจะส่งผลต่อข้อมูลส่วนตัว โดยมีสาเหตุมาจากความรุนแรงของภัยคุกคาม และมีโอกาสจะส่งผลกระทบต่อระบบสารสนเทศด้วย เช่น เมื่อบุคคลรับรู้ว่าเขารู้สึกถึงภัยคุกคาม โดยภัยนั้นอาจจะมาโจมตีหรือขโมยข้อมูล ทำให้เกิดการรับรู้ถึงภัยที่เข้ามาคุกคามข้อมูลและหาวิธีป้องกัน นำไปสู่ข้อสมมติฐานดังนี้

H2: การรับรู้ความรุนแรงของภัยคุกคามส่งผลเชิงบวกต่อการรับรู้ความเสี่ยงของภัยคุกคามข้อมูลส่วนตัวบน Public Cloud

ผลการวิจัยของ Bandura (1982) ได้กล่าวว่า บุคคลที่มีความเชื่อมั่นในเครื่องมือป้องกันภัยคุกคาม ส่งผลให้รับรู้ถึงประสิทธิภาพในการป้องกันภัยคุกคามของเครื่องมือนั้น นำไปสู่ข้อสมมติฐานดังนี้

H3: การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัวส่งผลเชิงบวกต่อการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคาม

ผลการวิจัยของ Weinstein (1993) ได้ศึกษา พบว่าเป็นการที่ผู้ใช้งานรับรู้ถึงประโยชน์ที่จะได้รับจากการใช้เครื่องมือป้องกันภัยคุกคาม เมื่อเทียบกับค่าใช้จ่ายที่จะต้องเสียไป ดังนั้นเมื่อบุคคลเลือกที่จะใช้เครื่องมือเพื่อปกป้องจากภัยคุกคาม เขาจะไม่ได้คำนึงถึงแค่ความสามารถของเครื่องมือนั้น แต่ยังรวมถึงค่าใช้จ่ายที่ต้องใช้ด้วย นำไปสู่ข้อสมมติฐานดังนี้

H4: การรับรู้ค่าใช้จ่ายจากการป้องกันภัยคุกคาม จะส่งผลเชิงลบต่อการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามของเครื่องมือป้องกันภัยคุกคาม

ผลการวิจัยของ Bandura (1978) พบว่า ผู้ที่รับรู้ความสามารถของตนเองสูงจะส่งผลต่อความสำเร็จของบุคคล โดยที่บุคคลกล้าเผชิญต่อปัญหาต่าง ๆ แม้กระทำความล้มเหลว หรือสิ่งที่ยากและพยายามทำให้สำเร็จ โดยมีความคาดหวังเกี่ยวกับผลที่จะเกิดขึ้นสูง ดังนั้นบุคคลที่รับรู้ความสามารถของตนเองในการหลีกเลี่ยงภัยคุกคามได้สูง ทำให้มีโอกาสที่จะรับรู้ถึงภัยคุกคามและหาทางหลีกเลี่ยง นำไปสู่ข้อสมมติฐานดังนี้

H5: การรับรู้ความสามารถของตนเองในการรับมือภัยคุกคามส่งผลเชิงบวกต่อการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามของเครื่องมือป้องกันภัยคุกคาม

เมื่อบุคคลรับรู้ถึงภัยคุกคามด้านความปลอดภัยและความรุนแรงของภัยคุกคามซึ่งถือเป็นจุดอ่อนของระบบสารสนเทศ เขาก็จะมีแนวโน้มที่จะเกิดแรงจูงใจที่จะปฏิบัติตามนโยบายการรักษาความปลอดภัย เพื่อเลี่ยงภัยนั้น (ประภาดา ตลึงจิตร, 2553) ดังนั้นจึงสามารถตั้งสมมติฐานได้ดังนี้

H6: การรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัวส่งผลเชิงบวกต่อแรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว

การรับรู้ความสามารถในการหลีกเลี่ยงเป็นวิธีการที่จะตัดสินว่า เครื่องมือป้องกันจะมีประสิทธิภาพในการหลีกเลี่ยงภัยคุกคามทางสารสนเทศเพียงไร และจะสร้างความเชื่อมั่นของแต่บุคคลต่อเครื่องมือป้องกันได้อย่างไร ซึ่งบุคคลจะมีแรงจูงใจที่จะนำเครื่องมือป้องกันภัยคุกคามมาใช้ ก็ต่อเมื่อบุคคลนั้นรับรู้ว่าเครื่องมือป้องกันภัยคุกคามสามารถที่จะรับมือกับภัยนั้นได้ และเครื่องมือป้องกันที่มีประสิทธิภาพในการหลีกเลี่ยงภัยมากที่สุดจะถูกนำมาใช้เพื่อเลี่ยงภัยคุกคาม (Compeau and Higgins, 1995) ดังนั้นจึงสามารถตั้งสมมติฐานได้ดังนี้

H7: การรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามของเครื่องมือป้องกันภัยคุกคามส่งผลเชิงบวกต่อแรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว

เมื่อบุคคลที่มีแรงจูงใจในการหลีกเลี่ยงสูงมีแนวโน้มที่จะมีพฤติกรรมหลีกเลี่ยงภัยคุกคามโดยใช้เครื่องมือป้องกันภัยคุกคาม (Liang and Xue, 2010) เพื่อลดอัตราความเสี่ยงที่จะถูกโจมตีข้อมูล จะส่งผลต่อการเปลี่ยนแปลงพฤติกรรม เป็นแรงผลักดันให้บุคคลแสดงพฤติกรรมเพื่อประโยชน์จากเป้าหมายบางประการ

H8: แรงจูงใจในการหลีกเลี่ยงความเสี่ยงจากภัยคุกคามข้อมูลส่วนตัวส่งผลเชิงบวกต่อพฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว

การที่บุคคลมีความตระหนักรู้และเข้าใจในศักยภาพที่สัมพันธ์กับความปลอดภัยของข้อมูลส่วนตัว จะทำให้เกิดพฤติกรรมที่ต้องการหลีกเลี่ยงจากความเสี่ยง ซึ่งความตระหนักรู้ถึงความปลอดภัยในข้อมูลอาจจะสร้างได้จากประสบการณ์ ดังเช่น บุคคลที่ไม่ยึดถือและปฏิบัติตามกฎของการรักษาความปลอดภัย จะมีความเสี่ยงจากการถูกโจมตีโดยไวรัส (Bulgurcu, et al., 2010) ดังนั้นจึงสามารถตั้งสมมติฐานได้ดังนี้

H9: ความตระหนักในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว ส่งผลเชิงบวกต่อพฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว

4. วิธีการวิจัย

งานวิจัยนี้เป็นงานวิจัยเชิงปริมาณ (Quantitative Analysis) โดยใช้แบบสอบถาม เป็นเครื่องมือในการเก็บข้อมูล ซึ่งจะอธิบายถึงรายละเอียดการกำหนดประชากรและกลุ่มตัวอย่าง เครื่องมือที่ใช้ในงานวิจัย วิธีการเก็บรวบรวมข้อมูล และการวิเคราะห์ผลข้อมูล

อนึ่งก่อนการจัดเก็บข้อมูลจากกลุ่มตัวอย่าง งานวิจัยนี้ได้นำแบบสอบถามที่พัฒนามาจากงานวิจัยในอดีต (ประกอบด้วย Johnston and Allen, 2010; Xu et al., 2011; Lankton and Tripp, 2013; Dinev and Hart, 2004; Johnston and Warkentin, 2010; Putri and Hovav, 2014; Liang and Xue, 2010; He and Freeman, 2010; Xu and Chan, 2008; Schmidt et al., 2007) ไปทดสอบกับกลุ่มตัวอย่างจำนวน 30 คน ผลในการทดสอบพบว่าข้อมูลมีการกระจาย ซึ่งผู้วิจัยได้ทำการปรับเปลี่ยนข้อความในคำถามที่กระจายจากกลุ่มให้เหมาะสม ต่อจากนั้นจึงนำแบบสอบถามไปจัดเก็บข้อมูลจากกลุ่มตัวอย่างจริง

หลังจากทำการทดสอบความเหมาะสมเบื้องต้นของเครื่องมือแล้ว จึงเก็บข้อมูลจริงกับกลุ่มตัวอย่างจำนวน 300 คน และเนื่องจากเพื่อความสะดวกรวดเร็วในการกระจายและได้ข้อมูลตอบกลับที่มีคุณภาพ จึงใช้การส่งแบบสอบถามเว็บไซต์ด้านเทคโนโลยีต่างๆ และผ่านทาง Online Media ผลที่ได้จึงได้รับแบบสอบถามตอบกลับมาทั้งหมด 290 ชุด

5. ผลการวิจัย

5.1 การทดสอบข้อตกลงเบื้องต้นทางสถิติ

ข้อมูลที่จัดเก็บจากกลุ่มตัวอย่างถูกนำไปทดสอบข้อมูลขาดหายและข้อมูลสุดโต่ง นอกจากนี้ยังทดสอบว่าข้อมูลมีการกระจายแบบปกติ มีความสัมพันธ์เชิงเส้นตรง มีภาวะร่วมเส้นตรงพหุ และมีภาวะร่วมเส้นตรงหรือไม่ ผลจากการทดสอบพบว่าข้อมูลไม่มีปัญหาด้านข้อมูลขาดหาย ข้อมูลสุดโต่ง และข้อมูลมีการกระจายเป็นแบบปกติ มีความสัมพันธ์เชิงเส้นตรงและไม่มีปัญหาภาวะร่วมเส้นตรงพหุและภาวะร่วมเส้นตรง ดังกล่าว

นอกจากนี้งานวิจัยได้ทดสอบความน่าเชื่อถือของแบบสอบถาม โดยพิจารณาจากค่าสัมประสิทธิ์ ครอนบัคแอลฟาที่สูงที่แต่ไม่น้อยกว่า 0.7 ซึ่งถือเป็นเกณฑ์ที่เหมาะสมสำหรับงานวิจัย Basic Research (Aoki and Downes, 2003) นอกจากนี้ยังได้ทดสอบความตรงของแบบสอบถามด้วยการวิเคราะห์องค์ประกอบโดยใช้เกณฑ์ข้อคำถามจับกลุ่มกันเป็นแต่ละตัวแปรต้องมีค่า น้ำหนักตัวประกอบไม่น้อยกว่า 0.5 (Hair et al., 2006, อ้างถึงใน อรวดี เนื่องฤทธ์, 2556) ผลการวิเคราะห์องค์ประกอบได้จำนวนทั้งหมด 10 องค์ประกอบ ประกอบด้วยการรับรู้ถึงจุดอ่อน การรับรู้ความรุนแรง การรับรู้ถึงภัย

คุกคาม การรับรู้ประสิทธิผล การรับรู้ต้นทุนจากการป้องกันภัยคุกคาม การรับรู้ความสามารถของตนเอง การรับรู้ความสามารถในการหลีกเลี่ยง แรงจูงในในการหลีกเลี่ยง ความตระหนักในการหลีกเลี่ยง และพฤติกรรมการหลีกเลี่ยง (ดังแสดงในตารางที่ 1)

ตารางที่ 1 ปัจจัยที่ได้จากการวิเคราะห์องค์ประกอบ

ปัจจัย	Factor Loading
ปัจจัย 1: การรับรู้ถึงจุดอ่อน (75.678% of variance, α = 0.838)	
ท่านคิดว่ามีความเป็นไปได้สูงที่ระบบ Public Cloud ที่ท่านใช้บริการอยู่ จะมีช่องโหว่ และอาจถูกคุกคาม	0.894
ท่านคิดว่ามีความเป็นไปได้สูงที่ระบบ Public Cloud ที่ท่านใช้บริการอยู่ จะมีสปายแวร์คุกคาม	0.864
ท่านคิดว่าระบบ Public Cloud ที่ท่านใช้บริการอยู่ อาจเก็บรักษาข้อมูลส่วนตัวของท่านได้ไม่เหมาะสม	0.851
ปัจจัย 2: การรับรู้ความรุนแรง (75.415% of variance, α = 0.891)	
ท่านคิดว่าสปายแวร์หรือไวรัสที่ติดมาจาก Public Cloud อาจลอบเก็บข้อมูลในคอมพิวเตอร์ของท่าน	0.846
ท่านคิดว่าสปายแวร์หรือไวรัสที่ติดมาจาก Public Cloud อาจทำให้คอมพิวเตอร์ของท่านทำงานได้ช้าลง	0.890
ท่านคิดว่าสปายแวร์หรือไวรัสที่ติดมาจาก Public Cloud ที่ท่านใช้บริการ อาจทำให้คอมพิวเตอร์ของท่านเสียหาย	0.918
ท่านคิดว่าสปายแวร์หรือไวรัสที่ติดมาจาก Public Cloud อาจจะควบคุมคอมพิวเตอร์ของท่านเพื่อไปขโมยข้อมูลของผู้อื่น	0.816
ปัจจัย 3: การรับรู้ถึงภัยคุกคาม (60.533% of variance, α = 0.795)	
ท่านรู้สึกไม่สบายใจหากข้อมูลส่วนตัวของท่านที่ถูกแชร์บน Public Cloud มีผู้อื่นเข้าถึงได้โดยง่าย	0.882
ท่านรู้สึกไม่สบายใจหาก Public Cloud มีเทคโนโลยีด้านความปลอดภัยที่ยังล้าหลัง จนทำให้ถูกคุกคาม	0.864

ตารางที่ 1 ปัจจัยที่ได้จากการวิเคราะห์องค์ประกอบ (ต่อ)

ปัจจัย	Factor Loading
ปัจจัย 4: การรับรู้ประสิทธิผล (66.940% of variance, α = 0.831)	
ท่านคิดว่านโยบายรักษาความเป็นส่วนตัวของ Public Cloud ที่ท่านใช้บริการ นำเครื่องมือป้องกันภัยคุกคามมาปกป้องข้อมูลได้เหมาะสม	0.818
ท่านคิดว่านโยบายรักษาความเป็นส่วนตัวของ Public Cloud ที่ท่านใช้บริการ จะช่วยกำจัดสปายแวร์ที่อาจมาคุกคามข้อมูลของท่าน	0.722
ท่านมั่นใจในนโยบายรักษาความเป็นส่วนตัวของ Public Cloud ที่ท่านใช้บริการ ว่าข้อมูลส่วนตัวจะถูกเก็บเป็นความลับจากผู้ไม่หวังดี	0.885
ท่านคิดว่านโยบายรักษาความเป็นส่วนตัวของ Public Cloud ที่ท่านใช้บริการอยู่ จะสามารถรักษาข้อมูลได้เป็นอย่างดี	0.840
ปัจจัย 5: การรับรู้ต้นทุนจากการป้องกันภัยคุกคาม (55.375% of variance, α = 0.684)	
ท่านจะเปรียบเทียบผลประโยชน์และค่าใช้จ่ายก่อนที่จะตัดสินใจใช้งานโปรแกรมแอนตีไวรัส	0.797
ท่านรับรู้ถึงประโยชน์ที่จะได้รับ และยอมรับค่าใช้จ่ายที่อาจเกิดขึ้นหากใช้โปรแกรมแอนตีไวรัสในการป้องกันภัยคุกคาม	0.856
ปัจจัย 6: การรับรู้ประสิทธิภาพของตนเอง (74.592% of variance, α = 0.886)	
ท่านคิดว่ามีความสามารถในการแก้ไขปัญหาที่มาจากภัยคุกคามใน Public Cloud ได้ด้วยตัวท่านเอง	0.902
ท่านคิดว่ามีความสามารถในการจัดการกับผู้ที่ต้องการขโมยข้อมูลส่วนตัวของท่านบน Public Cloud ได้	0.865
ท่านคิดว่าจะจัดการกับผู้ที่ต้องการขโมยข้อมูลส่วนตัวของท่านบน Public Cloud ด้วยตัวท่านเองก่อนที่จะปรึกษาผู้อื่น	0.880
ท่านคิดว่ามีความสามารถในการใช้โปรแกรมป้องกันภัยคุกคามใน Public Cloud เพื่อป้องกันสปายแวร์ที่อาจมาคุกคาม	0.849
ปัจจัย 7: การรับรู้ความสามารถในการหลีกเลี่ยง (64.723% of variance, α = 0.726)	
ท่านจะติดตามข่าวสารความเคลื่อนไหวของ Public Cloud ที่ท่านใช้บริการ ในด้านการรักษาความปลอดภัยของข้อมูลเสมอ	0.809
ท่านจะศึกษานโยบายการรักษาความเป็นส่วนตัวของผู้ให้บริการ อย่างระมัดระวัง ก่อนนำข้อมูลส่วนตัวขึ้นสู่ระบบ Public Cloud	0.875
ท่านจะศึกษาการตั้งค่าการเข้าถึงข้อมูลภายใน Public Cloud ก่อนใช้งาน และเปิดเผยข้อมูลส่วนตัวให้น้อยที่สุด	0.722

ตารางที่ 1 ปัจจัยที่ได้จากการวิเคราะห์องค์ประกอบ (ต่อ)

ปัจจัย	Factor Loading
ปัจจัย 8: แรงจูงในในการหลีกเลี่ยง (73.399% of variance, α = 0.814)	
ท่านเข้าใจถึงภัยคุกคามข้อมูลส่วนตัวที่มีมากขึ้น จึงตั้งใจที่จะใช้โปรแกรมป้องกันสปายแวร์ในการป้องกันภัยคุกคาม	0.805
ท่านเข้าใจถึงภัยคุกคามข้อมูลส่วนตัวที่มีมากขึ้น จึงต้องการให้มีการปรับปรุงโปรแกรมป้องกันสปายแวร์อยู่เสมอ	0.909
ท่านเข้าใจถึงภัยคุกคามข้อมูลส่วนตัวที่มีมากขึ้น จึงต้องการใช้บริการ Public Cloud ที่มีโปรแกรมป้องกันสปายแวร์มาตรฐานสูง	0.853
ปัจจัย 9: ความตระหนักในการหลีกเลี่ยง (79.210% of variance, α = 0.869)	
ท่านเข้าใจถึงการปฏิบัติตามระเบียบการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศภายใน Public Cloud	0.897
ท่านเข้าใจถึงอุปสรรคในการปฏิบัติตามระเบียบการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศภายใน Public Cloud	0. 925
ท่านเข้าใจถึงปัจจัยในการเสริมสร้างความปลอดภัยภายใน Public Cloud เพื่อป้องกันภัยจากผู้ที่อาจมาคุกคามข้อมูล	0.847
ปัจจัย 10: พฤติกรรมการหลีกเลี่ยงภัยคุกคาม (62.976% of variance, α = 0.833)	
ถ้าหากท่านใช้งานโปรแกรมแอนตีไวรัส จะใช้เพื่อป้องกันสปายแวร์ที่อาจมาจาก Public Cloud	0.885
ท่านจะปรับปรุงข้อมูลในโปรแกรมแอนตีไวรัส เพื่อป้องกันการถูกขโมยข้อมูลในการ Login เข้าสู่ระบบ Public Cloud	0.891

อนึ่งผลของการวิเคราะห์ข้อมูลทั่วไปเกี่ยวกับผู้ตอบแบบสอบถามของของกลุ่มตัวอย่างพบว่ากลุ่มตัวอย่างส่วนใหญ่ที่ตอบแบบสอบถามเป็นกลุ่มช่วงอายุ 26-30 ปี และส่วนใหญ่มีอาชีพพนักงานบริษัท/ลูกจ้างเอกชน ถึงร้อยละ 45.9 ซึ่งเป็นกลุ่มที่สนใจในเรื่อง Public Cloud มากที่สุด

5.2 การวิเคราะห์ผลการวิจัย

การทดสอบสมมติฐานการวิจัยในครั้งนี้ ผู้วิจัยใช้วิธีวิเคราะห์การถดถอยเชิงเส้นเดียว และการวิเคราะห์ถดถอยพหุคูณ โดยใช้ค่า p-value ที่น้อยกว่าหรือเท่ากับ 0.05 เป็นตัวกำหนดนัยสำคัญทางสถิติโดยแบ่งการวิเคราะห์ออกเป็น 4 ส่วน ดังนี้

ส่วนที่ 1 ผลการวิเคราะห์สมการถดถอยพหุคูณแสดงให้เห็นว่าการรับรู้ความรุนแรงของภัยคุกคาม และการรับรู้ถึงจุดอ่อนกำหนดการรับรู้ถึงภัยคุกคาม ที่ระดับนัยสำคัญ $F(2, 287) = 53.787$ ($p = 0.000$) ซึ่งสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 27.3% ($R^2 = 0.273$) เมื่อวิเคราะห์ในรายละเอียดของตัวแปรอิสระพบว่าการรับรู้ความรุนแรงของภัยคุกคาม และการรับรู้ถึงจุดอ่อน เป็นตัวกำหนดการรับรู้ถึงภัยคุกคามที่ระดับนัยสำคัญที่ $p = 0.005$ และ 0.007 (ดังแสดงในตารางที่ 2-3) ซึ่งสอดคล้องกับงานวิจัยของ Liang and Xue (2009) ที่กล่าวว่าการที่บุคคลรับรู้ถึงช่องโหว่หรือจุดอ่อนแอที่เกิดขึ้น ทำให้บุคคลรับรู้ถึงภัยที่จะมาคุกคามข้อมูลส่วนตัวของตนเองและ การที่บุคคลรับรู้ถึงผลลัพธ์ด้านลบจากภัยคุกคามจะมีสาเหตุมาจากระดับของภัยคุกคามทางสารสนเทศที่มีความรุนแรงต่อข้อมูลส่วนตัว

ตารางที่ 2 ผลการวิเคราะห์การถดถอย (Regression) ของการรับรู้ความรุนแรงของภัยคุกคาม และการรับรู้ถึงจุดอ่อนที่มีอยู่ใน Public Cloud ต่อการรับรู้ถึงภัยคุกคาม

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	54.205	2	27.102	53.787	.000**
Residual	144.615	287	0.504		
Total	198.820	289			

** p<0.05

ตารางที่ 3 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของการรับรู้ความรุนแรงของภัยคุกคาม และการรับรู้ถึงจุดอ่อนที่มีอยู่ใน Public Cloud ต่อการรับรู้ถึงภัยคุกคาม

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.
	B	Beta		
การรับรู้ถึงจุดอ่อนที่มีอยู่ใน Public Cloud (Weak)	0.155	0.172	2.821	0.005**
การรับรู้ความรุนแรงของภัยคุกคาม (Per_serv)	0.305	0.405	6.630	0.000**

** p<0.05

R = 0.522, R^2 = 0.273, SE = 0.70985

ส่วนที่ 2 ผลการวิเคราะห์สมการถดถอยพหุคูณแสดงให้เห็นว่าการรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคามและการรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัวกำหนดการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคาม ที่ระดับนัยสำคัญ F(3, 286) = 39.563 (p = 0.000) ซึ่งสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 29.3% (R^2 = 0.293) เมื่อวิเคราะห์ในรายละเอียดของตัวแปรอิสระพบว่าการรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคามและการรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว เป็นตัวกำหนดการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามที่ระดับนัยสำคัญที่ p = 0.000 (ดังแสดงในตารางที่ 4-5) ซึ่งสอดคล้องกับงานวิจัยของ Bandura (1982) ที่กล่าวว่า การที่บุคคลรับรู้ความสามารถในการหลีกเลี่ยงนั้นจะเป็นผลมาจากการที่บุคคลรู้ถึงประสิทธิภาพในการหลีกเลี่ยงภัยคุกคามของเครื่องมือที่ใช้ในการปกป้องข้อมูลทางสารสนเทศ Weinstein (1993) ที่กล่าวว่า การที่บุคคลจะเลือกใช้เครื่องมือป้องกันภัยคุกคามชนิดใดนั้น บุคคลจะไม่ได้ตัดสินเลือกจากแค่ความสามารถในการหลีกเลี่ยงเท่านั้น แต่ยังรวมถึงค่าใช้จ่ายที่ต้องใช้และ Ng et al. (2009); Woon et al. (2005) และ Workman et al. (2008) ที่กล่าวว่า บุคคลจะแสดงความสามารถหลีกเลี่ยงภัยคุกคาม เมื่อระดับของประสิทธิภาพการหลีกเลี่ยงของตนเองเพิ่มขึ้น

ตารางที่ 4 ผลการวิเคราะห์การถดถอย (Regression) ของการรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม และการรับรู้ความสามารถของตนเองในการรับมือภัยคุกคาม ต่อการรับรู้ความสามารถในการหลีกเลี่ยง

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	63.131	3	21.044	39.563	0.000**
Residual	152.126	286	0.532		
Total	215.257	289			

** p<0.05

ตารางที่ 5 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของการรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม และการรับรู้ความสามารถของตนเองในการรับมือภัยคุกคาม ต่อการรับรู้ความสามารถในการหลีกเลี่ยง

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.
	B	Beta		
การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม (Per_cos)	0.292	0.274	5.325	0.000**
การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว (Per_eff)	0.254	0.202	3.978	0.000**
การรับรู้ความสามารถของตนเองในการรับมือภัยคุกคาม (Self)	0.258	0.313	6.022	0.000**

** P < 0.05

R = 0.542, R^2 = 0.293, SE = 0.72932

ส่วนที่ 3 ผลการวิเคราะห์สมการถดถอยพหุคูณแสดงให้เห็นว่าการรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัวและการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามกำหนดแรงจูงใจในการหลีกเลี่ยงภัยคุกคาม ที่ระดับนัยสำคัญ F(2, 287) = 80.052 (p = 0.000) ซึ่งสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 35.8 % (R^2 = 0.358) เมื่อวิเคราะห์ในรายละเอียดของตัวแปรอิสระพบว่าการรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัวและการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคาม เป็นตัวกำหนดแรงจูงใจในการหลีกเลี่ยงภัยคุกคามที่ระดับนัยสำคัญที่ p = 0.000 ทุกปัจจัย (ดังแสดงในตารางที่ 6-7) ซึ่งสอดคล้องกับงานวิจัยของ (Freud, 1915; James, 1890) ที่ศึกษาในกฎแห่งความชอบว่า บุคคลมีแนวโน้มที่จะหลีกเลี่ยงภัย

ที่อาจมาคุกคามตนเอง หากภัยนั้นทำให้ตนเองเกิดความเสียหายและ Liang and Xue (2010) ที่ศึกษาพบว่า บุคคลจะมีความตั้งใจที่จะนำเครื่องมือป้องกันภัยคุกคามมาใช้ ก็ต่อเมื่อบุคคลนั้นรับรู้ว่าเครื่องมือป้องกันภัยคุกคามสามารถที่จะรับมือกับภัยนั้นได้

ตารางที่ 6 ผลการวิเคราะห์การถดถอย (Regression) ของการรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัวภายใน Public Cloud และการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคาม ต่อแรงจูงใจในการหลีกเลี่ยง

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	74.899	2	37.450	80.052	0.000**
Residual	134.264	287	0.468		
Total	209.163	289			

** p<0.05

ตารางที่ 7 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของการรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัวภายใน Public Cloud และการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคาม ต่อแรงจูงใจในการหลีกเลี่ยง

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.
	B	Beta		
การรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัวภายใน Public Cloud (Per_thr)	0.263	0.257	5.361	0.000**
การรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามต่อข้อมูลที่เป็นส่วนตัว (Avoi)	0.496	0.503	10.507	0.000**

** P < 0.05

R = 0.598, R^2 = 0.358, SE = 0.68397

ส่วนที่ 4 ผลการวิเคราะห์สมการถดถอยพหุคูณแสดงให้เห็นว่าแรงจูงใจในการหลีกเลี่ยงภัยคุกคามและความตระหนักในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวกำหนดพฤติกรรมการหลีกเลี่ยงภัยคุกคาม ที่ระดับนัยสำคัญ F(2, 287) = 71.458 (p = 0.000) ซึ่งสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 33.2% (R^2 = 0.332) เมื่อวิเคราะห์ในรายละเอียดของตัวแปรอิสระพบว่าแรงจูงใจในการหลีกเลี่ยงภัยคุกคามและความตระหนักในการหลีกเลี่ยงภัยคุกคาม เป็นตัวกำหนดพฤติกรรมการหลีกเลี่ยงภัยคุกคาม ที่ระดับนัยสำคัญที่ p = 0.034 และ 0.000 (ดังแสดงในตารางที่ 8-9) ซึ่งสอดคล้องกับงานวิจัยของ ของ Liang and Xue (2010) ที่กล่าวว่า บุคคลที่มีแรงจูงใจในการหลีกเลี่ยงสูงจะมีแนวโน้มที่จะมีพฤติกรรม

หลีกเลี่ยงภัยคุกคามโดยใช้เครื่องมือป้องกันภัยคุกคาม เพื่อลดความเสี่ยงที่จะเกิดขึ้นและ ประภาดา ตลึงจิตร (2553) ที่กล่าวว่าพฤติกรรมทางการหลีกเลี่ยงภัยคุกคามยังถือว่าเป็นการแสดงให้เห็นว่าบุคคลนั้นมีความตระหนักถึงความปลอดภัย

ตารางที่ 8 ผลการวิเคราะห์การถดถอย (Regression) ของแรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว และความตระหนักในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว ต่อพฤติกรรมการหลีกเลี่ยง

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	80.408	2	40.204	71.458	0.000**
Residual	161.472	287	0.563		
Total	241.879	289			

** p<0.05

ตารางที่ 9 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของแรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว และความตระหนักในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว ต่อพฤติกรรมการหลีกเลี่ยง

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.
	B	Beta		
ความตระหนักในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว (Awar)	0.122	0.114	2.127	0.034
แรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว (Motiv)	0.558	0.519	9.718	0.000

** P < 0.05

$R = 0.577$, $R^2 = 0.332$, SE = 0.75008

6. สรุปผลการวิจัย

ผลการวิจัยพบว่า ตัวแปรที่มีอิทธิพลต่อการรับรู้ถึงภัยคุกคามต่อข้อมูลส่วนตัวภายใน Public Cloud มากที่สุด คือ ตัวแปรการรับรู้ความรุนแรงของภัยคุกคาม รองลงมาคือ ตัวแปรการรับรู้ถึงจุดอ่อนที่มีอยู่ใน Public Cloud ส่วนตัวแปรที่มีอิทธิพลต่อการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามต่อข้อมูลที่เป็นส่วนตัวภายใน Public Cloud พบว่า ตัวแปรการรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคามเป็นตัวแปรอิสระที่มีความสัมพันธ์เชิงบวกมากที่สุด รองลงมา คือ ตัวแปรการรับรู้ความสามารถของตนเองในการรับมือภัยคุกคาม และการรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัวเป็นตัวแปรอิสระที่มีความสัมพันธ์น้อยที่สุด ส่วนตัวแปรที่มีอิทธิพลต่อแรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public Cloud มากที่สุด คือ ตัวแปรการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามต่อข้อมูลที่เป็นส่วนตัวภายใน Public Cloud ส่งผลเชิงบวกและมีอิทธิพลมากกว่าตัวแปรการรับรู้ความสามารถในการหลีกเลี่ยงภัยคุกคามต่อข้อมูลที่เป็นส่วนตัวภายใน Public Cloud ส่วนส่วนตัวแปรที่มีอิทธิพลต่อพฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public

Cloud มากที่สุด คือ ตัวแปรแรงจูงใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public Cloud ในขณะที่ตัวแปรความตระหนักในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวนั้นเป็นตัวแปรที่รองลงมา

โดยกลุ่มตัวอย่างของงานวิจัยนี้ ได้แก่ กลุ่มตัวอย่างที่ที่ใช้ในการวิจัยนี้ คือ ผู้ใช้บริการ Public Cloud อันได้แก่ Google Drive และ Dropbox เนื่องจากไม่ทราบจำนวนประชากรทั้งหมดว่ามีจำนวนเท่าไหร่ ในการวิจัยครั้งนี้ จึงใช้วิธีการกำหนดขนาดตัวอย่างจากการประมาณค่าเฉลี่ยประชากร และสร้างแบบสอบถามออนไลน์ในการเก็บข้อมูลเพื่ออำนวยความสะดวกแก่ผู้ตอบแบบสอบถาม โดยการวาง URL ของแบบสอบถามไว้บนเครือข่ายสังคม (Facebook) ของผู้วิจัย กระจายไปยังกลุ่มตัวอย่างทางเว็บไซต์ด้านเทคโนโลยี ซึ่งมีผู้ตอบแบบสอบทั้งสิ้นจำนวน 302 ชุด และได้ตัดข้อมูลที่ไม่ใช่กลุ่มตัวอย่างที่แท้จริงออกเหลือแบบสอบถามทั้งสิ้น 290 ชุด จึงนำข้อมูลดังกล่าวมาวิเคราะห์ทางสถิติ

กลุ่มประชากรที่ตอบแบบสอบถามส่วนใหญ่อยู่ในช่วงอายุ 26-30 ปี และส่วนใหญ่ผู้ตอบแบบสอบถามเป็นพนักงานบริษัท/ลูกจ้างเอกชน หากเป็นช่วงอายุอื่นหรือประกอบอาชีพอื่น อาจได้ผลลัพธ์ที่แตกต่างกัน เนื่องจากผู้ใช้งานมีกระจายกลุ่มมากขึ้น แนวทางในการใช้งานก็จะต่างกันไปด้วย

งานวิจัยนี้ผู้วิจัยได้ศึกษาเฉพาะผู้ที่เคยใช้งานหรือใช้งาน Public Cloud อยู่เท่านั้น ไม่รวมถึง Cloud ประเภทอื่นๆ ซึ่งวิจัยต่อเนื่องอาจจะศึกษาปัจจัยอื่นๆที่อาจส่งผลกระทบต่อพฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวมากกว่านี้ เนื่องจากในผลการวิจัยค่าสถิติของตัวแปรส่วนใหญ่จะอยู่ในช่วง 0.2 ซึ่งถือว่ายังไม่สูงมากนัก อาจมีตัวแปรอื่นๆที่ส่งผลกระทบได้อีก

บรรณานุกรม

กิ่งแก้ว ศรีสาลีกุลรัตน์. (2551). ประสิทธิผล (Effectiveness). ดึงข้อมูลวันที่ 21 มีนาคม 2558, จาก https://www.gotoknow.org/posts/213948.

กองบัญชาการการศึกษา สำนักงานตำรวจแห่งชาติ. (2548). จิตวิทยาเบื้องต้น. ดึงข้อมูลวันที่ 18 เมษายน 2558, จาก http://www.edupol.org/edu_P/systemedu/cschool/data/9.pdf.

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล. (2558). ความหมายของการบริหารความเสี่ยง. ดึงข้อมูลวันที่ 20 มีนาคม 2558, จากhttp://www.eg.mahidol.ac.th/qa/index.php?option=com_content&view=article&id=82&Itemid=113.

ธีรศักดิ์ แสงดิษฐ์ (2553) แรงจูงใจของชุมขนกับการระดมทรัพยากรเพื่อการศึกษาของโรงเรียนสังกัดสำนักงานเขตพื้นที่การศึกษาราชบุรีเขต 1, วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยศิลปากร, คณะศึกษาศาสตร์.

ประภาดา ตลึงจิตร (2555) แนวทางในการเสริมสร้างความตระหนักถึงการปฏิบัติตามระเบียบการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ไทย : Case study research of Thai Cooperative, วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์, คณะพาณิชยศาสตร์และการบัญชี.

วิมลรัศมิ์ พันธุ์จิรภาค (2554) ผลของโปรแกรมออกกำลังกายเพื่อส่งเสริมสุขภาพของผู้สูงอายุหญิง จังหวัดสมุทรปราการ, วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยบูรพา, คณะสาธารณสุขศาสตร์.

Al-Haderi, S.M. (2013). The Effect of Self-Efficacy in the Acceptance of Information Technology in the Public Sector. *International Journal of Business and Social Science*, 4(9), 188-198.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness. *MIS Quarterly*, 34(3), 523-548.

Choi, C. F., and Jiang, Z. (2013). Responses to Social Predicament on Online Social Networks. Proceedings of the Nineteenth Americas Conference on Information Systems.

Dinev, T., and Hart, P. (2004). Internet Privacy, Social Awareness, And Internet Technical Literacy. An Exploratory Investigation BLED 2004 Proceedings, Paper 24.

Hardin, A., Looney, C., and Fuller, M. (2006). Computer based learning systems and the development of computer selfefficacy: Are all sources of efficacy created equal? AMCIS 2006 Proceedings, Paper 273.

He, J., and Freeman, L. A. (2010). Understanding the Formation of General Computer Self-Efficacy. *Communications of the Association for Information Systems*, 26, Article 12.

Hwang, K., Kulkarni, S., and Hu, Y. (2009). Cloud Security with Virtualized Defense and Reputation-based Trust Management. 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 717-722.

Johnston, A. C., and Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34(3), 549-566.

Lankton, N., and Tripp, J. (2013). A Quantitative and Qualitative Study of Facebook Privacy using the Antecedent-Privacy Concern-Outcome Macro. Proceedings of the Nineteenth Americas Conference on Information Systems.

Leberknight, C. S., Widmeyer, G. R., and Recce, M. L. (2008). Decision Support for Perceived Threat in the Context of Intrustion Detection Systems. AMCIS 2008 Proceedings, Paper 317.

Liang, H., and Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly, 33(1), 71-90.

Liang, H., and Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, 11(7), 394-413.

ปัจจัยที่มีผลต่อความสำเร็จในการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืนกรณีศึกษา: บริษัท โกซอฟท์(ประเทศไทย) จำกัด

วลัยพร มณีนิล*

Gosoft (Thailand) Co., Ltd.

***Correspondence:** walaiporn11@gmail.com
doi: 10.14456/jisb.2016.8

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยความสำเร็จของการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืนเพื่อเป็นแนวทางแก่องค์กรที่จะเริ่มนำ ITIL มาใช้หรือนำ ITIL มาใช้แล้วให้สามารถคงไว้ซึ่งกรอบวิธีปฏิบัติ ITIL ได้อย่างยั่งยืนซึ่งมี บริษัท โกซอฟท์(ประเทศไทย) จำกัด เป็นกรณีศึกษาของงานวิจัย

ผลการวิจัยแสดงให้เห็นว่า การสนับสนุนจากผู้บริหารอย่างต่อเนื่อง จะมีส่วนเสริมสร้างให้พนักงานในองค์กรมีความตระหนักในกรอบวิธีปฏิบัติ ITIL ในขณะเดียวกันก็จะทำให้เกิดการจัดตั้งกลุ่ม ITIL Champion ภายในองค์กรขึ้น และผลักดันให้พนักงานในองค์กรมีส่วนร่วมในการปรับปรุงกระบวนการทำงาน ทั้งนี้จะต้องมีการประเมินผลและตรวจติดตามอย่างต่อเนื่อง เพื่อที่จะได้ทราบผลลัพธ์ หรือผลสะท้อนกลับของกระบวนการที่ได้ถูกสร้างขึ้น และนำผลลัพธ์นั้นมามีส่วนทำให้เกิดการปรับปรุงกระบวนการอย่างต่อเนื่อง และทำให้มั่นใจได้ว่ากระบวนการทำงานนั้นๆ สามารถคงไว้ซึ่งความสำเร็จของการนำ ITIL มาในองค์กรอย่างยั่งยืน

คำสำคัญ: การจัดการบริการด้านเทคโนโลยีสารสนเทศ ความสำเร็จ ยั่งยืน

Critical Success Factors for Sustainable Organization's ITIL Implementation Case study: Gosoft (Thailand) Co.,Ltd

Walaiporn Maneeniin*

Gosoft (Thailand) Co., Ltd.

***Correspondence:** walaiporn11@gmail.com

doi: 10.14456/jisb.2016.8

Abstract

The purpose of this research is to study the critical success factors that stimulate the sustainability on organization's ITIL adoption, based on Gosoft (Thailand) Co., Ltd as the case study.

The results prove that continuous support from Management raises employees' standard awareness of the organization. Moreover, setting up groups of ITIL Champion within the organization encourages employees to involve in the streamlining work process. However, evaluation and coherent follow-up are necessary. It is crucial to be aware of and to stay informed on the progress, as well as implementing the necessary improvements. The effective use of ITIL will ensure the long-term maintenance and maximization of organization standards.

Keywords: ITIL, IT Service Management, Success, Sustainable

1. บทนำ

การที่บริษัทนำ ITIL มาประยุกต์ใช้ในการดำเนินการในองค์กรจนประสบความสำเร็จได้รับมาตรฐาน ISO/IEC20000:2011 นั้นเกิดจากปัจจัยแห่งความสำเร็จหลายด้าน ทำให้องค์กรคิดวิธีการให้กระบวนการทางธุรกิจสอดคล้องกับกระบวนการทางด้านเทคโนโลยีสารสนเทศ ซึ่งมีขั้นตอนหรือระบบการประสานงานที่ดี มีวิธีการแก้ปัญหาที่มีคุณภาพ และได้มาตรฐาน สามารถทำให้การจัดการเทคโนโลยีสารสนเทศมีประสิทธิภาพ ลดค่าใช้จ่ายและลดความเสี่ยงในการดำเนินงาน ปรับปรุงคุณภาพการให้บริการกับลูกค้า อย่างไรก็ตามองค์กรยังขาดความรู้ซึ่งปัจจัยที่ส่งผลต่อการคงไว้ซึ่งมาตรฐาน ISO/IEC20000 ทำให้บางครั้งเกิดความผิดพลาด เสียเวลา เสียต้นทุนในการดำเนินงานเกินความจำเป็น และในบางครั้งจากผลการตรวจสอบภายในพบว่า เกิดการปฏิบัติงานที่ไม่สอดคล้องกับสิ่งที่มาตรฐานกำหนด (Non-Compliances) หรือได้รับคำเสนอแนะ (Suggestion) จากทางผู้ตรวจสอบเพื่อเป็นแนวทางในการปรับปรุงการทำงานให้ดียิ่งขึ้น ลดความผิดพลาดในการดำเนินงานและเพิ่มความพึงพอใจให้กับลูกค้า ดังนั้นงานวิจัยนี้จะศึกษาปัญหาดังกล่าวเพื่อให้องค์กรสามารถทราบถึงปัจจัยที่องค์กรจะสามารถคงไว้ซึ่งมาตรฐานอย่างต่อเนื่องและพัฒนาองค์กรให้ดียิ่งขึ้นไป

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดเกี่ยวกับการให้บริการด้านเทคโนโลยีสารสนเทศอย่างยั่งยืน

ความยั่งยืน หรือ Sustainability ในความหมายของ Brundtland Commission of United Nation หมายถึงการรวมกันทางด้านเศรษฐศาสตร์, ด้านสภาพแวดล้อม และ ด้านการพัฒนาสังคม เพื่อความต้องการในปัจจุบัน โดยปราศจากการบรรลุความต้องการจากความสามารถของรุ่นต่อไป และยังคงอยู่ถาวรต่อไปโดยไม่ถูกยกเลิกหรือทำลาย ปัจจุบันอุตสาหกรรมเทคโนโลยีสารสนเทศกำลังเติบโตขึ้นและมีผลกระทบมากขึ้น จึงเป็นเรื่องที่ท้าทายที่จะทำให้เกิดความยั่งยืน ซึ่งการจัดการทางด้านเทคโนโลยีสารสนเทศ คือ ส่วนประกอบหลักในการขับเคลื่อนเศรษฐศาสตร์อย่างยั่งยืน อย่างไรก็ตาม ยังขาดการค้นพบว่า จะต้องทำอย่างไรให้ยั่งยืนในความต้องการที่หลากหลายและซับซ้อนความยั่งยืนนั้นไม่ใช่การจัดการสิ่งแวดล้อมอย่างใกล้ชิด แต่เกี่ยวกับการอยู่ได้ในระยะยาวขององค์กร, ของบุคคล, ของสังคม และรุ่นต่อไปในอนาคต (Korte et al., 2012)

สำหรับความพยายามเกี่ยวกับความยั่งยืนนั้นในการจัดการทางด้านเทคโนโลยีสารสนเทศ จะต้องการการทบทวนปรับปรุงให้เป็นปัจจุบันและผลสะท้อนกลับของการปรับปรุงเปลี่ยนแปลงเพื่อนำไปสู่ความยั่งยืน ซึ่งการปรับปรุงเปลี่ยนแปลงต่างๆนั้น หมายถึงการปรับปรุงเปลี่ยนแปลงนโยบาย รูปแบบการทำงาน ระบบการจัดการ วิธีการปฏิบัติ ซึ่งรวมถึงการเปลี่ยนแปลงของโครงสร้างองค์กรและทักษะการบริหารทรัพยากรมนุษย์ (Korte et al., 2012) ขั้นตอนที่สำคัญที่สุดของการสนับสนุนการพัฒนาอย่างยั่งยืนคือ การสนับสนุนจากผู้บริหารระดับสูง การพัฒนาและจัดการกระบวนการด้านเทคโนโลยีสารสนเทศ (Angheluta et al., 2012)

ความยั่งยืนในการบริการ จะต้องมีกระบวนการที่มีประสิทธิภาพและความน่าเชื่อสำหรับการส่งมอบการให้บริการด้านเทคโนโลยีสารสนเทศ รวมถึงการตรวจติดตามผลการทำงาน (Clifford, 2009) และการพัฒนาความยั่งยืนในการดำเนินงานนั้นจะต้องมีการกำหนดแนวความคิดสร้างเป้าหมายสร้างตัวชี้วัดและรักษาคุณค่าเอาไว้ (Angheluta et al., 2012)

จากแนวคิดข้างต้นจะเห็นได้ว่า การที่จะรักษาวิธีปฏิบัติในรูปแบบ ITIL และมาตรฐาน ISO/IEC20000 ให้สามารถคงอยู่ในองค์กร จะต้องอาศัยการมีส่วนร่วมของผู้ที่เกี่ยวข้องหรือพนักงานในกระบวนการทำงาน และมีกลุ่ม ITIL Champion ภายในองค์กร เพื่อที่จะปรับปรุงและพัฒนากระบวนการทำงานให้ดียิ่งขึ้น ทั้งนี้จะต้องได้รับการสนับสนุนจากทางผู้บริหารระดับสูงเพื่อที่จะให้ ITIL และมาตรฐาน ISO/IEC20000 สามารถขับเคลื่อนภายในองค์กรต่อไปได้ และจะต้องมีการตรวจ

ประเมินผลทำงานอย่างต่อเนื่องตามระยะเวลาที่กำหนด เพื่อผลลัพธ์และสะท้อนกลับผลลัพธ์ เพื่อทำการปรับปรุงกระบวนการทำงานต่อไป ทั้งนี้พนักงานจะต้องมีความรู้และตระหนักในกรอบวิธีปฏิบัติ ITIL ที่ใช้งานอีกด้วย

2.2 การสนับสนุนของผู้บริหารอย่างต่อเนื่อง

การสนับสนุนจากผู้บริหารอย่างต่อเนื่องหมายถึง การให้การสนับสนุนจากผู้บริหารระดับสูง ในด้านการวางแผนการดำเนินการ การจัดสรรทรัพยากรในการทำงาน และให้ความช่วยเหลือในการแก้ไขปัญหาต่างๆที่เกิดขึ้นภายในองค์กร (Marquis, 2006)

ITIL ได้รับการยอมรับอย่างกว้างขว้างว่า การสนับสนุนจากผู้บริหารและความมุ่งมั่นของผู้บริหาร เป็นสิ่งจำเป็นต่อการเริ่มต้นปรับปรุงกระบวนการหลักๆขององค์กร (Cater-Steel et al., 2007) ซึ่งการสนับสนุนเป็นสิ่งจำเป็นในเรื่องของเทคโนโลยีธรรมาภิบาล (IT Governance) โดยหมายรวมถึงการเป็นผู้นำของผู้บริหาร การวางโครงสร้างองค์กรและวางกระบวนการเพื่อให้แน่ใจว่า โครงสร้างของเทคโนโลยีสารสนเทศสอดคล้องกับกลยุทธ์ขององค์กร (Sallé, 2004)

การมีส่วนร่วมของผู้บริหาร จึงเป็นปัจจัยสำคัญในการพัฒนาองค์กรให้ประสบผลสำเร็จ เนื่องจากผู้บริหารจะให้ความช่วยเหลือให้การสนับสนุนและจัดเตรียมทีมงานที่มีความรู้ความสามารถให้เข้ามามีส่วนร่วมและสามารถทำงานได้อย่างมีประสิทธิภาพ (Iden and Eikebrokk, 2011) โดยการสนับสนุนจากผู้บริหารอย่างต่อเนื่องนั้น จะผลักดันให้พนักงานมีความตระหนักในกรอบวิธีปฏิบัติ ITIL มีการจัดหาบุคลากรที่มีความสามารถเข้ามาเป็นส่วนหนึ่งในกลุ่ม ITIL Champion และผลักดันให้พนักงานเข้ามามีส่วนร่วมในการปรับปรุงกระบวนการอย่างต่อเนื่อง

2.3 ความตระหนักในกรอบวิธีปฏิบัติ ITIL

ความตระหนัก หมายถึง ความรู้ในสิ่งๆหนึ่ง ที่ทำให้เกิดการรู้สึกตัว และมีความตั้งใจที่จะสะท้อนถึงการรู้สึกตัวนั้นออกมาให้เห็นในรูปแบบของพฤติกรรม (ประภาดา ตลึงจิตร, 2555)

การสะท้อนถึงการแสดงออกทางพฤติกรรมในการทำงานของแต่ละบุคคลที่แตกต่างกัน ทำให้เกิดรูปแบบการทำงานที่แตกต่างกัน องค์กรจึงต้องมีการสร้างกระบวนการที่เป็นมาตรฐานเพื่อที่จะทำให้แต่ละบุคคลสามารถทำงานร่วมกันได้ ซึ่งการสร้างกระบวนการทำงานนั้นจะต้องมีการพัฒนาและปรับปรุงให้ดีขึ้นเรื่อยๆ จึงต้องเกิดการปรับปรุงกระบวนการสนับสนุนในการทำงานของพนักงาน คือกระบวนการของการทำงานเครื่องมือและการสอนงานเพื่อที่จะให้พนักงานสามารถทำงานได้ตามมาตรฐานเดียวกัน (Pankoff, 2005)

หากพนักงานมีความรู้ในกรอบวิธีปฏิบัติ ITIL และคิดว่ากรอบวิธีปฏิบัติ ITIL นั้น ทำให้เขาสามารถส่งมอบงานอย่างได้อย่างมีคุณภาพ ส่งผลดีต่อประสิทธิภาพการทำงานของตนเองและองค์กร พนักงานก็จะเกิดความตระหนักในกรอบวิธีปฏิบัติ ITIL และเมื่อเกิดความตระหนักในกรอบวิธีปฏิบัติ ITIL แล้ว พนักงานจะเกิดการแสดงพฤติกรรมคือ การปรับปรุงกระบวนการทำงานของตนเองและองค์กร เพื่อให้ได้ซึ่งกระบวนการทำงานและสามารถส่งมอบงานมีประสิทธิภาพอย่างต่อเนื่องและยังคงไว้ซึ่งกรอบวิธีปฏิบัติ ITIL นั้น

2.4 การมีกลุ่ม ITIL Champion ภายในองค์กร

การมีกลุ่ม ITIL Champion ภายในองค์กร หมายถึง การที่องค์กรมีการจัดตั้งกลุ่มคนทำงานทางด้าน ITIL ขึ้น ซึ่งกลุ่มคนเหล่านั้นจะต้องมีความรู้ความสามารถและเข้าใจเกี่ยวกับกระบวนการ ITIL เป็นอย่างดี ทั้งนี้จะต้องเป็นผู้ที่เข้าใจวัฒนธรรมองค์กรและกระบวนการทำงานภายในองค์กรเป็นอย่างดีด้วย (John, 2007)

ผลกระทบที่สำคัญของการทำ ITIL คือระดับการให้บริการทางด้าน IT ด้วยวิธีการใหม่ นโยบายใหม่ ขั้นตอนการทำงานและการประเมินผลการทำงานใหม่ โดยผู้เป็นจ้าของกระบวนการ (Process Owner) จะต้องจัดทำกระบวนการใหม่นี้ร่วมกับกลุ่ม ITIL Champion เพื่อที่จะให้การทำงานบรรลุผลตั้งแต่เริ่มต้นจนจบกระบวนการให้บริการ ซึ่งจะเกี่ยวข้องกับกลุ่มคนทำงานหลายทีม (Cater-Steel et al., 2006) ผู้เป็นจ้าของกระบวนการจะได้รับมอบหมายให้ดูแลแต่ละกระบวนการ

โดยเฉพาะ โดยผู้เป็นจ้าของกระบวนการจะเขียนกระบวนการจากโครงสร้างการทำงานที่ ITIL กำหนด รวมถึงการดูแลและปรับปรุงกระบวนการให้ดีขึ้นต่อไปอย่างต่อเนื่อง (Sharifi et al., 2008)

2.5 การมีส่วนร่วมของพนักงาน

การมีส่วนร่วมของพนักงาน หมายถึง การเปิดโอกาสให้พนักงานมีการร่วมมือกันทำงาน เช่น การสร้างช่องทางในการสื่อสารการทำงานระหว่างกัน และให้พนักงานสามารถออกสิทธิ์ออกเสียง ร่วมกันหารือและตัดสินใจในกระบวนการทำงานได้ (Burge, 2008; Angheluta et al., 2012)

การมีส่วนร่วมของผู้ที่เกี่ยวข้องในการกำหนดกระบวนการให้ตรงความต้องการ จะทำให้มั่นใจได้ว่าการพัฒนาธุรกิจจะมีความยั่งยืน (Angheluta et al., 2012) การมีส่วนร่วมของผู้ที่เกี่ยวข้อง จึงเป็นสิ่งที่จำเป็นสำหรับกลยุทธ์ความยั่งยืนที่มีประสิทธิภาพ ซึ่งการมีส่วนร่วมอย่างต่อเนื่องนั้นจะช่วยให้มีความสัมพันธ์ในระยะยาว เกิดความไว้วางใจซึ่งเป็นสิ่งที่ดีในการพัฒนาคุณภาพของการให้บริการ (Harmon and Moolenkamp, 2012) และการมีส่วนร่วมในการปรับปรุงกระบวนการ โดยการใช้เครื่องมือและการสื่อสารตอบกลับผลการทำงาน (Feedback) จะทำให้ปรับปรุงคุณภาพการทำงานให้ดียิ่งขึ้น (Cătălin et al., 2014)

2.6 การประเมินผลและตรวจติดตามอย่างต่อเนื่อง

การประเมินผลและตรวจติดตามอย่างต่อเนื่อง หมายถึง การวัดผลการทำงานอย่างต่อเนื่อง ซึ่งจะเป็นส่วนหนึ่งของการจัดการด้านผลการทำงาน (Performance Management) ที่ว่าด้วยเรื่องของกระบวนการในการประเมินผลการทำงานของพนักงาน ว่าสามารถทำงานได้ตามงานที่ได้รับมอบหมายหรือไม่ ซึ่งการวัดผลควรจะต้องรวมถึงความสำเร็จในการทำงาน ทัศนคติและวัฒนธรรมในการทำงานความสามารถในการทำงาน และ พฤติกรรมในการทำงาน (Pankoff, 2005)

การวัดผลของการปฏิบัติงานภายใน เช่น นวัตกรรม, การบริการ และประสิทธิภาพการทำงาน สามารถขยายผล จากการวัดผลโดยทั่วไปไปสู่การวัดผลเพื่อความยั่งยืน ซึ่งรวมไปถึงการสร้างและพัฒนานโยบายการทำงานในแบบการบริหารจัดการแบบดั้งเดิมและการบริหารจัดการอย่างยั่งยืน (Huang et al., 2014) โดยการพัฒนาตัวชี้วัดแบบยั่งยืนนั้นทำได้โดยนำตัวชี้วัดจากหลากหลายที่มาทำการทบทวนและวัดผล (Angheluta et al., 2012)

2.7 การปรับปรุงกระบวนการอย่างต่อเนื่อง

การปรับปรุงกระบวนการอย่างต่อเนื่อง หมายถึง การแก้ไขกระบวนการทำงานให้ดียิ่งขึ้นอย่างต่อเนื่อง โดยมีวัตถุประสงค์เพื่อป้องกัน ลดข้อผิดพลาด และเพิ่มคุณค่าให้กับกระบวนการ (Kaziliûnas, 2008) ดังนั้นองค์กรควรจะต้องมีการปรับปรุงกระบวนการทำงานอย่างต่อเนื่องเพื่อให้การทำงานดียิ่งขึ้น

ในกระบวนการของ ITIL มีกระบวนการสำหรับจัดการการเปลี่ยนแปลง (Change Management) ที่จะเกิดขึ้นเพื่อใช้ในการตัดสินใจต่อเหตุการณ์การปรับปรุงเปลี่ยนแปลงต่างๆที่จะเกิดขึ้น เพื่อให้การให้บริการเทคโนโลยีสารสนเทศขององค์กรยั่งยืน (Cherringtonand Greenway, 2008) ซึ่งการเปลี่ยนแปลงในองค์กรเป็นสิ่งที่หลีกเลี่ยงไม่ได้ เนื่องมาจากการเปลี่ยนแปลงของบุคคลหรือเทคโนโลยี การให้บริการด้านเทคโนโลยีสารสนเทศก็ยังต้องดำเนินต่อไปและมีนวัตกรรมใหม่ๆ เกิดขึ้น ดังนั้นองค์กรจึงต้องการระบบจัดการเอกสารที่ดีและการฝึกอบรมเพื่อให้มีความสามารถในการจัดการการเปลี่ยนแปลงที่มากขึ้น (Clifford, 2009) จึงจะทำให้มีการจัดการต่อการปรับปรุงเปลี่ยนแปลงที่เป็นระบบมากขึ้น

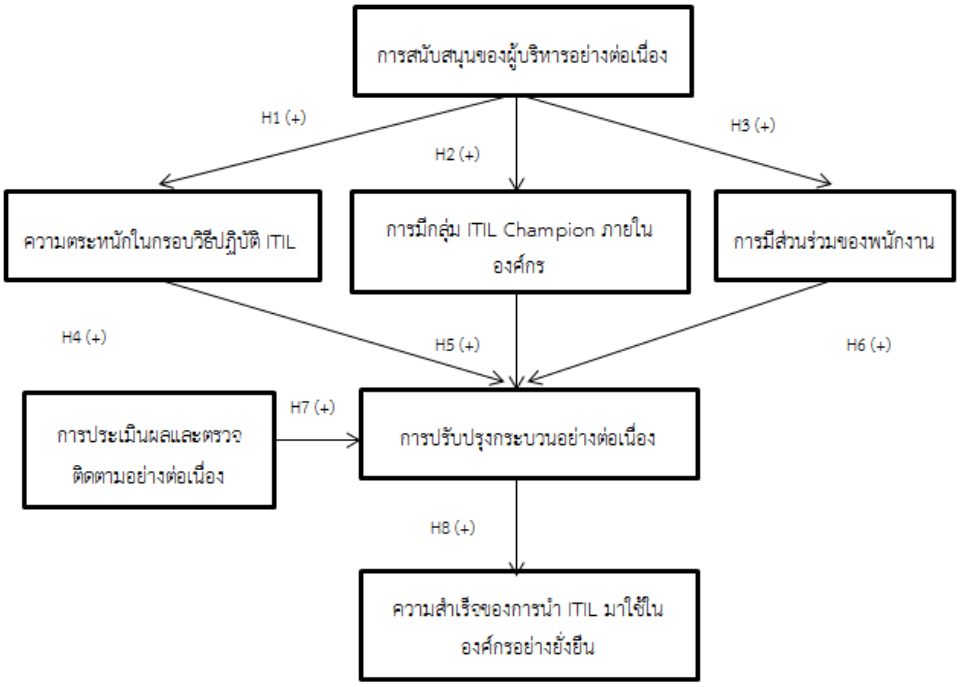
2.8 ความสำเร็จของการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืน

ความสำเร็จในการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืน หมายถึง การวางแผนการให้บริการทางด้าน IT ให้สอดคล้องกับความต้องการทางธุรกิจทั้งในปัจจุบันและอนาคต และปรับปรุงคุณภาพในการให้บริการทางด้าน IT โดยทำให้การให้บริการมีความราบรื่น (Pollard and Cater-Steel, 2009; Harmon and Moolenkamp, 2012)

เป้าหมายหลักของ ITIL คือการขับเคลื่อนหน่วยงานเทคโนโลยีสารสนเทศให้มีคุณค่าเพิ่มมากขึ้น ซึ่งหน่วยงานเทคโนโลยีสารสนเทศ เป็นหน่วยงานที่ทำหน้าที่อย่างมีประสิทธิภาพเพื่อที่จะให้บริการเทคโนโลยีสารสนเทศได้อย่างราบรื่น ดังนั้นปัจจัยแห่งความสำเร็จควรจะถูกกำหนดตัวชี้วัดที่จะนำมาใช้วัดผลเพื่อใช้ตรวจสอบการบรรลุผลของปัจจัยแห่งความสำเร็จ เรียกได้ว่ามีผลลัพธ์สะท้อนกลับให้เห็นถึงการทำงานตามกระบวนการ ซึ่งเป็นผลลัพธ์ที่ทำให้คุณค่าทางธุรกิจเพิ่มมากขึ้น (Neničková, 2011) ดังนั้นจึงกล่าวได้ว่า การวัดความสำเร็จของการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืน จะสามารถวัดได้จาก การที่องค์กรสามารถคงไว้ซึ่งการปฏิบัติตามมาตรฐาน ISO/IEC20000 หรือ วิธีการปฏิบัติ ITIL อย่างต่อเนื่องทำให้องค์กรสามารถเพิ่มคุณค่าทางธุรกิจได้มากขึ้น

3. กรอบแนวคิดการวิจัยและสมมติฐานการวิจัย

จากทฤษฎีแนวคิดที่เกี่ยวข้องการทบทวนวรรณกรรมต่างๆที่ได้ทำการศึกษามาแล้วนั้น พบว่า ปัจจัยที่เพิ่มขึ้นได้แก่ ความตระหนักในกรอบวิธีปฏิบัติ ITIL การจัดตั้งกลุ่ม ITIL ภายในองค์กร และการประเมินผลและตรวจติดตามผลลัพธ์อย่างต่อเนื่อง จะมีผลทำให้เกิดการปรับปรุงกระบวนการทำงานอย่างต่อเนื่องและนำไปสู่การคงไว้ซึ่ง ITIL ภายในองค์กรอย่างยั่งยืน จึงทำให้สามารถกำหนดปัจจัยที่มีผลต่อความสำเร็จของการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืนได้ ดังภาพที่ 1



ภาพที่ 1 แสดงกรอบแนวคิดเกี่ยวกับความสำเร็จของการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืน

การสนับสนุนของผู้บริหาร เป็นปัจจัยสำคัญในการให้ความช่วยเหลือในการแก้ไขปัญหา รวมถึงสนับสนุนและจัดเตรียมทีมงานที่มีความรู้ความสามารถ มีความตระหนักในกรอบวิธีปฏิบัติ ITIL เข้ามาร่วมกันพัฒนาและปรับปรุงกระบวนการ ให้องค์กรมีกระบวนการทำงานที่มีประสิทธิภาพ (Iden and Eikebrokk, 2011) จึงสามารถตั้งสมมติฐานดังนี้

H1: การสนับสนุนจากผู้บริหารอย่างต่อเนื่อง ส่งผลด้านบวกต่อ ความตระหนักในกรอบวิธีปฏิบัติ ITIL
H2: การสนับสนุนจากผู้บริหารอย่างต่อเนื่อง ส่งผลด้านบวกต่อ การมีกลุ่ม ITIL Champion ภายในองค์กร
H3: การสนับสนุนจากผู้บริหารอย่างต่อเนื่อง ส่งผลด้านบวกต่อ การมีส่วนร่วมของพนักงาน

สำหรับแต่ละบุคคลที่รับรู้เกี่ยวกับมาตรฐานและกระบวนการก็จะมีการแสดงพฤติกรรมในการทำงานที่แตกต่างกัน เกิดรูปแบบการทำงานที่แตกต่างกันและเพื่อที่จะทำให้แต่ละบุคคลทำงานร่วมกัน จึงต้องเกิดการปรับปรุงกระบวนการสนับสนุนการทำงานของพนักงาน คือกระบวนการทำงาน เครื่องมือและการสอนงานเพื่อที่จะให้พนักงานสามารถทำงานได้ตามมาตรฐานเดียวกัน (Pankoff, 2005) จึงสามารถตั้งสมมติฐานได้ว่า

H4: ความตระหนักในกรอบวิธีปฏิบัติ ITIL ส่งผลด้านบวกต่อการ ปรับปรุงกระบวนการอย่างต่อเนื่อง

ITIL Champion จะได้รับการฝึกอบรมและมีความรู้เกี่ยวกับ ITIL จะทำให้พนักงานมีทักษะที่จำเป็นในการกำหนดวิเคราะห์และปรับปรุงกระบวนการ โดยใช้วิธีการที่เหมาะสมที่สุดในการพัฒนารูปแบบของกระบวนการและเครื่องมือเพื่อให้องค์กรสามารถนำกระบวนการและเครื่องมือมาใช้ได้อย่างมีประสิทธิภาพและสอดคล้องกับกระบวนการขององค์กร (Iden and Eikebrokk, 2011) จึงสามารถตั้งสมมติฐานได้ว่า

H5: การมีกลุ่ม ITIL Champion ภายในองค์กร ส่งผลด้านบวกต่อ การปรับปรุงกระบวนการอย่างต่อเนื่อง

การมีส่วนร่วมของพนักงานหรือผู้มีส่วนเกี่ยวข้องในการออกความคิดเห็นและปรับปรุงกระบวนการอย่างต่อเนื่องนั้นจะทำให้กระบวนการถูกปรับปรุงให้ดีขึ้นและยังคงไว้ซึ่งกรอบวิธีปฏิบัติ ITIL ทำให้เพิ่มความพึงพอใจให้กับลูกค้าและผลการทำงานขององค์กรด้วยบริการที่มีคุณภาพ โดยผ่านการมีส่วนร่วมของผู้ที่เกี่ยวข้องการปรับปรุงอย่างต่อเนื่องและการทำงานที่มีการใช้เครื่องมือและเทคนิคทางด้านการจัดการคุณภาพ (Mosadeghrad, 2014) จึงสามารถตั้งสมมติฐานได้ว่า

H6: การมีส่วนร่วมของพนักงาน ส่งผลด้านบวกต่อ การปรับปรุงกระบวนการอย่างต่อเนื่อง

การประเมินผลและตรวจติดตามอย่างต่อเนื่อง เพราะทำให้องค์กรสามารถวัดผลระดับของผลลัพธ์จากการปรับปรุงกระบวนการให้มีประสิทธิภาพได้ (Spremić et al., 2008) และทำให้เกิดการปรับปรุงกระบวนการทำงานอย่างต่อเนื่องเพื่อที่จะให้ได้ผลลัพธ์ของการทำงานที่มีประสิทธิภาพและพนักงานเกิดความพึงพอใจ จึงสามารถตั้งสมมติฐานได้ว่า

H7: การประเมินผลและตรวจติดตามอย่างต่อเนื่อง ส่งผลด้านบวกต่อ การปรับปรุงกระบวนการอย่างต่อเนื่อง

ในการ Implement ITIL จะเริ่มตั้งแต่การกำหนดการวิเคราะห์การออกแบบกระบวนการภายในใหม่โดยใช้พื้นฐานจากคำแนะนำของ good practice ซึ่งจะนำไปสู่การจัดการกระบวนการ หากปราศจากการจัดการกระบวนการแล้ว ITIL จะไม่ประสบความสำเร็จตั้งแต่ช่วงเริ่มทำการ Implement การจัดการกระบวนการกล่าวได้ว่าเป็นการบริหารกระบวนการโดยรวมของบริษัท เพื่อทำให้มั่นใจได้ว่ายังคงไว้ซึ่งวัตถุประสงค์ทางธุรกิจคือ ทำให้ลูกค้ามีความสุข (Iden and Eikebrokk, 2011)

H8: การปรับปรุงกระบวนการอย่างต่อเนื่อง ส่งผลด้านบวกต่อ ความสำเร็จในการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืน

4. วิธีการวิจัย

งานวิจัยนี้จัดเก็บข้อมูลจากพนักงานและผู้บริหารในบริษัท โกซอฟท์ (ประเทศไทย) จำกัด ที่เป็นผู้ใช้วิธีปฏิบัติของ ITIL จำนวน 200 คน ผ่านทางแบบสอบถามออนไลน์ อนึ่งก่อนการจัดเก็บข้อมูลจากกลุ่มตัวอย่าง งานวิจัยนี้ได้นำแบบสอบถามที่พัฒนามาจากงานวิจัยในอดีต (ประกอบด้วย Cater-Steel et al., 2006; เบญจพร ฉายาลักษณ์, 2552; กิตติพงษ์ บูรณกูล, 2552; ชมพูนุท สุวารี, 2551; Chow and Cao, 2007; John, 2007; Burge, 2008; Angheluta et al., 2012; Korte et al., 2012; Kaziliûnas, 2008; Pollard and Cater-Steel, 2009; Harmon and Moolenkamp, 2012) นอกนั้นนำแบบสอบถามไปทดสอบกับกลุ่มตัวอย่างจำนวน 20 คน ผลการทดสอบพบว่า แบบสอบถามที่นำไปทดสอบ มีความเหมาะสมที่จะนำไปจัดเก็บข้อมูลจากกลุ่มตัวอย่าง

5. ผลการวิจัย

5.1 การทดสอบข้อตกลงเบื้องต้นทางสถิติ

ข้อมูลที่จัดเก็บจากกลุ่มตัวอย่างถูกนำไปทดสอบข้อมูลขาดหาย (Missing data) และข้อมูลสุดโต่ง (Outliers) นอกจากนี้ยังทดสอบว่า ข้อมูลมีการกระจายแบบปกติ (Normal) มีความสัมพันธ์เชิงเส้นตรง (Linearity) มีภาวะร่วมเส้นตรงพหุ (Multicollinearity) และมีภาวะร่วมเส้นตรง (Singularity) หรือไม่ ผลการทดสอบพบว่าไม่มีข้อมูลขาดหาย ข้อมูลสุดโต่ง และข้อมูลมีการกระจายเป็นแบบปกติ มีความสัมพันธ์เชิงเส้นตรง และไม่มีปัญหาภาวะร่วมเส้นตรงพหุและภาวะร่วมเส้นตรง

นอกจากนี้งานวิจัยได้ทดสอบความเชื่อถือของแบบสอบถาม โดยใช้การวิเคราะห์ค่าสัมประสิทธิ์อัลฟาของครอนบาช พบว่าทุกตัวแปรมีค่ามากกว่า 0.7 จึงถือว่ามีความเชื่อถือได้สำหรับงานวิจัยแบบ Basic research (เพ็ญแข ศิริวรรณ, 2546) นอกจากนี้ยังได้ทดสอบความตรงของแบบสอบถาม ด้วยการวิเคราะห์องค์ประกอบ (Factor analysis) โดยใช้เกณฑ์ที่ข้อคำถามที่จับกลุ่มกันเป็นแต่ละตัวแปรต้องมีค่า Factor loading ไม่น้อยกว่า 0.5 ผลการวิเคราะห์องค์ประกอบได้จำนวนตัวแปรทั้งหมด 7 องค์ประกอบ (ตารางที่ 1 แสดงปัจจัยที่ได้จากการวิเคราะห์องค์ประกอบของงานวิจัยนี้)

ตารางที่ 1 ปัจจัยที่ได้จากการวิเคราะห์องค์ประกอบ

ปัจจัย	Factor loading
ปัจจัย 1: การสนับสนุนจากผู้บริหารอย่างต่อเนื่อง (75.187% of variance, α = 0.944)	
ผู้บริหารระดับสูงมีการติดตามการนำ ITIL มาใช้ในองค์กรอย่างใกล้ชิด	.905
ผู้บริหารระดับสูงมีการกำหนดนโยบาย เพื่อวางแนวทางการนำ ITIL มาใช้ในองค์กร	.893
ผู้บริหารระดับสูงมีความมุ่งมั่นตั้งใจจริงในโครงการนำ ITIL มาประยุกต์ใช้ในองค์กร	.884
ผู้บริหารระดับสูงมีการวางแผนงบประมาณในด้านการจัดหาอุปกรณ์ หรือเครื่องมือเพื่อเตรียมความพร้อมในการนำ ITIL มาใช้ในองค์กร	.859
หน่วยงานของท่านได้รับการจัดสรรจำนวนพนักงานและการกำหนดขอบเขตความรับผิดชอบสำหรับการให้บริการด้าน IT ที่มีประสิทธิภาพอย่างเหมาะสม	.849
ผู้บริหารระดับสูงเข้ามามีส่วนร่วมในการนำ ITIL มาใช้ในองค์กร	.839
ท่านได้รับความช่วยเหลือและคำปรึกษาจากผู้บริหารอย่างเต็มที่ เมื่อพบปัญหาเกี่ยวกับระบบงานหรือการให้บริการ ส่งผลให้การแก้ไขปัญหาประสบผลสำเร็จได้อย่างรวดเร็ว	.837
ปัจจัย 2: ความตระหนักในกรอบวิธีปฏิบัติ ITIL (21.401% of variance, α = 0.869)	
ท่านคิดว่าการนำ ITIL เข้ามาประยุกต์ใช้ในองค์กร ทำให้การดำเนินงานด้านเทคโนโลยีสารสนเทศมีประสิทธิภาพมากขึ้น	.840
ท่านคิดว่าการนำ ITIL เข้ามาประยุกต์ใช้ในหน่วยงานจะช่วยปรับปรุงคุณภาพการให้บริการด้านเทคโนโลยีสารสนเทศให้ดียิ่งขึ้น	.827
ท่านคิดว่าการนำ ITIL เข้ามาประยุกต์ใช้เป็นเรื่องที่เกี่ยวข้องกับภารกิจโดยตรงของบริษัท	.728
ท่านคิดว่าการนำหลัก ITIL มาใช้ในองค์กร ทำให้งานที่ท่านรับผิดชอบมีคุณค่าต่อองค์กรมากขึ้น	.716
ปัจจัย 3: การมีกลุ่ม ITIL Champion ภายในองค์กร (28.593% of variance, α = 0.942)	
บุคลากรในกลุ่ม ITIL Champion มีความเข้าใจกระบวนการในการทำงานด้านต่างๆภายในองค์กร	.863
บุคลากรในกลุ่ม ITIL Champion มีความรู้ความสามารถในเรื่อง ITIL	.858
บุคลากรในกลุ่ม ITIL Champion ที่ทำหน้าที่เป็นที่ปรึกษาจะมีประสบการณ์ในเรื่อง implement ITIL มาก่อน	.826
บุคลากรในกลุ่ม ITIL Champion สามารถนำ ITIL มาประยุกต์ใช้ภายในองค์กรได้อย่างเหมาะสม	.812
บุคลากรในกลุ่ม ITIL Champion มีความเข้าใจวัฒนธรรมในองค์กรเป็นอย่างดี	.798

ตารางที่ 1 ปัจจัยที่ได้จากการวิเคราะห์องค์ประกอบ (ต่อ)

ปัจจัย	Factor loading
ปัจจัย 4: การมีส่วนร่วมของพนักงาน (22.491% of variance, α = 0.844)	
ท่านมีส่วนร่วมตัดสินใจเกี่ยวกับกระบวนการทำงานภายในทีม	.856
ท่านมีส่วนรับผิดชอบในกระบวนการทำงานที่ได้รับมอบหมายจากองค์กร	.804
องค์กรของท่านเปิดโอกาสให้แสดงความเห็นและปรับปรุงกระบวนการทำงานภายในทีมงาน	.702
ในการทำงานท่านมักจะสื่อสารระหว่างหน่วยงาน เพื่อให้แต่ละหน่วยงานที่เกี่ยวข้องเข้าใจตรงกัน	.665
เมื่อพบปัญหาท่านจะได้รับการร่วมมือจากพนักงานในองค์กร	.629
ปัจจัย 5: การประเมินผลและตรวจติดตามอย่างต่อเนื่อง (83.650% of variance, α = 0.901)	
องค์กรมีการนำผลลัพธ์ของการประเมินผลการทำงานมาวิเคราะห์เปรียบเทียบผลลัพธ์	.917
องค์กรมีการประเมินผลลัพธ์ของการทำงานเป็นระยะๆ	.915
องค์กรมีการตรวจสอบประสิทธิภาพในการดำเนินงาน เพื่อติดตามปัญหาที่เกิดขึ้น	.912
ปัจจัย 6: การปรับปรุงกระบวนการอย่างต่อเนื่อง (67.536% of variance, α = 0.755)	
ท่านคิดว่าการปรับปรุงกระบวนการอย่างต่อเนื่องทำให้สามารถสร้างคุณค่าให้กับการทำงานของท่านได้	.853
ท่านคิดว่าการปรับปรุงกระบวนการทำให้ลดการทำงานที่ไม่จำเป็น	.837
ท่านคิดว่าองค์กรมีการปรับปรุงกระบวนการทำงานที่ดีอย่างต่อเนื่อง	.774
ปัจจัย 7: ความสำเร็จในการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืน (99.631% of variance, α = 0.936)	
องค์กรสามารถให้บริการด้านเทคโนโลยีสารสนเทศได้อย่างราบรื่นและสามารถคงไว้ซึ่งการปฏิบัติตาม ITIL	.949
องค์กรได้มีการปรับปรุงคุณภาพในการให้บริการทางด้าน IT ได้อย่างมีประสิทธิภาพ	.943
องค์กรมีการกำหนดวางแนวการให้บริการให้สอดคล้องกับความต้องการทางธุรกิจอย่างต่อเนื่อง	.933

อนึ่งผลการวิเคราะห์ข้อมูลทั่วไปเกี่ยวกับผู้ตอบแบบสอบถามของกลุ่มตัวอย่าง พบว่า ประชากรที่เป็นตัวอย่างส่วนใหญ่เป็นเพศชาย อายุงานภายในบริษัทโกซอฟท์มากกว่า 5 ปี มีระดับการศึกษาปริญญาตรี ซึ่งอยู่สังกัดหน่วยงาน Solution Delivery และอยู่ในตำแหน่งงาน System Analyst หรือ Senior Technical Infrastructure Office

5.2 การวิเคราะห์ผลการวิจัย

งานวิจัยนี้ใช้สถิติวิธีการวิเคราะห์ถดถอยพหุคูณ (Multiple Regression) วิธีการวิเคราะห์ถดถอยเชิงเส้นเดียว (Simple Linear Regression) และวิธีการวิเคราะห์สหสัมพันธ์ส่วนรวม (Canonical Regression) เป็นการวิเคราะห์รูปแบบความสัมพันธ์ระหว่างตัวแปรอิสระและตัวแปรตามในรูปของสมการ เพื่อที่จะนำสมการนั้นไปประมาณค่าหรือพยากรณ์ค่าของตัวแปรตาม โดยงานวิจัยนี้ใช้ค่า p-value ที่น้อยกว่าหรือเท่ากับ 0.05 เป็นตัวกำหนดนัยสำคัญทางสถิติ (Significant

Level) ส่วนค่า p-value ที่อยู่ระหว่าง 0.05 และ 0.10 เป็นตัวกำหนดนัยสำคัญส่วนเพิ่ม (Marginal Significance) ซึ่งการวิเคราะห์การถดถอยจะแบ่งการวิเคราะห์ออกเป็น 3 ส่วนดังนี้

ส่วนที่ 1 ผลการวิเคราะห์สหสัมพันธ์ส่วนร่วม แสดงให้เห็นว่า ตัวแปรอิสระ (การสนับสนุนจากผู้บริหารอย่างต่อเนื่อง) สามารถอธิบายตัวแปรตามทั้งหมด (ความตระหนักในกรอบวิธีปฏิบัติ ITIL การมีกลุ่ม ITIL Champion ภายในองค์กรและการมีส่วนร่วมของพนักงาน) ได้ 55.4%

เมื่อพิจารณาความสัมพันธ์ของตัวแปรตามต่อตัวแปรพหุนามคาโนนิคอลสำหรับกลุ่มตัวแปรตาม พบว่าตัวแปรตามความตระหนักในกรอบวิธีปฏิบัติ ITIL (Canonical loading = 0.746) มีความสัมพันธ์ต่อตัวแปรพหุนามคาโนนิคอลในระดับต่ำการมีกลุ่ม ITIL Championภายในองค์กร (Canonical loading = 0.853) มีความสัมพันธ์ต่อตัวแปรพหุนามคาโนนิคอลในระดับปานกลางส่วนการมีส่วนร่วมของพนักงาน (Canonical loading = 0.886) มีความสัมพันธ์ต่อตัวแปรพหุนามคาโนนิคอลในระดับสูง

อนึ่งเพื่อสามารถตอบสมมุติฐานงานวิจัยนี้โดยใช้เกณฑ์ค่าสหสัมพันธ์คาโนนิคอลพบว่ามีค่าเท่ากับ 0.744 ซึ่งเป็นระดับความสัมพันธ์ปานกลางและได้วิเคราะห์ข้อมูลโดยใช้สถิติ MANOVA ร่วมกับคำสั่ง discriminant เมื่อพิจารณาผลที่ได้จากการวิเคราะห์สถิติพบว่า ตัวแปรต้น (การสนับสนุนจากผู้บริหารอย่างต่อเนื่อง) กำหนดตัวแปรตาม (ความตระหนักในกรอบวิธีปฏิบัติ ITIL การมีกลุ่ม ITIL Champion ภายในองค์กรและการมีส่วนร่วมของพนักงาน) อย่างมีนัยสำคัญทางสถิติ (ดังแสดงในตารางที่ 2-4)

ตารางที่ 2 ระดับสัมประสิทธิ์คาโนนิคอลการสนับสนุนจากผู้บริหารอย่างต่อเนื่องความตระหนักในกรอบวิธีปฏิบัติ ITIL การมีกลุ่ม ITIL Champion ภายในองค์กรและการมีส่วนร่วมของพนักงาน

สัมประสิทธิ์คาโนนิคอล (Cononical function)	สหสัมพันธ์ คาโนนิคอล (Canonical correlation)	Canonical R*2	Willk's Lambda	Chi-Square	DF	Sig.
1	.744	.554	.446	158.671	3.000	0.000

ตารางที่ 3 ความสัมพันธ์ระหว่างกลุ่มตัวแปรการสนับสนุนจากผู้บริหารอย่างต่อเนื่องความตระหนักในกรอบวิธีปฏิบัติ ITIL การมีกลุ่ม ITIL Championภายในองค์กร และการมีส่วนร่วมของพนักงาน

กลุ่มตัวแปร	ตัวแปร	Standardized Canonical Coefficients	Canonical Loadings	Cannonical Cross Loadings
ตัวแปรกลุ่มที่ 1 (กลุ่มตัวแปรอิสระ)	การสนับสนุนจากผู้บริหารอย่างต่อเนื่อง	1.000	0.000	.744
ตัวแปรกลุ่มที่2 (กลุ่มตัวแปรตาม)	ความตระหนักในกรอบวิธีปฏิบัติ ITIL	0.182	0.746	0.555
	การมีกลุ่ม ITIL Champion ภายในองค์กร	0.445	0.853	0.635
	การมีส่วนร่วมของพนักงาน	0.547	0.886	0.659

ตารางที่ 4 ผลการวิเคราะห์การถดถอย ความตระหนักในกรอบวิธีปฏิบัติ ITIL การมีกลุ่ม ITIL Champion ภายในองค์กร และการมีส่วนร่วมของพนักงาน

COVERIATE	B	Beta	Std. Err.	Sig of t
ความตระหนักในกรอบวิธีปฏิบัติ ITIL	0.510	0.555	0.054	0.000
การมีกลุ่ม ITIL Champion ภายใน	0.649	0.635	0.056	0.000
การมีส่วนร่วมของพนักงาน	0.536	0.659	0.043	0.000

ส่วนที่ 2 ผลการวิเคราะห์สมการถดถอยพหุคูณแสดงให้เห็นว่า ความตระหนักในกรอบวิธีปฏิบัติ ITIL การมีกลุ่ม ITIL Champion ภายในองค์กร การมีส่วนร่วมของพนักงานและการประเมินผลและตรวจติดตามอย่างต่อเนื่อง กำหนดการปรับปรุงกระบวนการอย่างต่อเนื่องที่ระดับนัยสำคัญ p = .000 ($F_{(4,195)}$ = 49.533) และการวิเคราะห์แต่ละตัวแปรพบว่า ความตระหนักในกรอบวิธีปฏิบัติ ITIL การมีกลุ่ม ITIL Champion ภายในองค์กร การมีส่วนร่วมของพนักงานและการประเมินผลและตรวจติดตามอย่างต่อเนื่อง เป็นตัวกำหนดการปรับปรุงกระบวนการอย่างต่อเนื่อง ที่ระดับนัยสำคัญ p = 0.042, 0.086, 0.005 และ 0.000 ตามลำดับ อีกทั้งพบว่าสหสัมพันธ์ ความตระหนักในกรอบวิธีปฏิบัติ ITIL การมีกลุ่ม ITIL Champion ภายในองค์กร การมีส่วนร่วมของพนักงานและการประเมินผลและตรวจติดตามอย่างต่อเนื่อง สามารถอธิบายการปรับปรุงกระบวนการอย่างต่อเนื่องได้ 50.4% (ดังแสดงในตารางที่ 5-6)

ตารางที่ 5 ค่าสถิติการวิเคราะห์การถดถอย (Regression) ของการปรับปรุงกระบวนการอย่างต่อเนื่อง

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	43.419	4	10.855	49.533	.000[a]
Residual	42.732	195	.219		
Total	86.151	199			

* p < 0.05

ตารางที่ 6 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของการปรับปรุงกระบวนการอย่างต่อเนื่อง

ตัวแปร	ค่าสัมประสิทธิ์ถดถอย (B)	ค่าสัมประสิทธิ์ถดถอยปรับมาตรฐาน (Beta)	t	Sig.
ค่าคงที่	.069		.239	.812
ความตระหนักในกรอบวิธีปฏิบัติ ITIL	.168	.143	2.046	.042*
การมีกลุ่ม ITIL Champion ภายในองค์กร	.131	.125	1.726	.086**
การมีส่วนร่วมของพนักงาน	.247	.186	2.810	.005*
การประเมินผลและตรวจติดตามอย่างต่อเนื่อง	.430	.379	5.004	.000*

* $p < 0.05$

** $p < 0.10$

$R = .710$, $R^2 = .504$, $SE = .468$

ส่วนที่ 3 ผลการวิเคราะห์สมการถดถอยเชิงเส้นเดียวแสดงให้เห็นว่า การปรับปรุงกระบวนการอย่างต่อเนื่อง กำหนดความสำเร็จในการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืนที่ระดับนัยสำคัญ $p = .000$ ($F_{(1,198)} = 177.290$) และวิเคราะห์ตัวแปรอิสระ จะพบว่า การปรับปรุงกระบวนการอย่างต่อเนื่อง เป็นตัวกำหนด ความสำเร็จในการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืนที่ระดับนัยสำคัญ $p = 0.000$ อีกทั้งพบว่าสหสัมพันธ์การปรับปรุงกระบวนการอย่างต่อเนื่อง สามารถอธิบายความสำเร็จในการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืนได้ 47.2% (ดังแสดงในตารางที่ 7-8)

ตารางที่ 7 ค่าสถิติการวิเคราะห์การถดถอย (Regression) ของความสำเร็จในการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืน

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	40.883	1	40.833	177.290	.000*
Residual	45.659	198	.231		
Total	86.542	199			

* $p < 0.05$

ตารางที่ 8 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของความสำเร็จในการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืน

ตัวแปร	ค่าสัมประสิทธิ์ถดถอย (B)	ค่าสัมประสิทธิ์ถดถอยปรับมาตรฐาน (Beta)	t	Sig.
ค่าคงที่	1.208		5.945	.000
การปรับปรุงกระบวนการอย่างต่อเนื่อง	.689	.687	13.315	.000*

* p <0.05

R = .687, R^2 = 0.472, SE = .470

6. สรุปผลการวิจัย

ผลการวิจัยแสดงให้เห็นว่า การสนับสนุนจากผู้บริหารอย่างต่อเนื่อง จะมีส่วนเสริมสร้างให้พนักงานในองค์กรมีความตระหนักในกรอบวิธีปฏิบัติ ITIL ในขณะเดียวกันก็จะให้การสนับสนุนให้มีการจัดตั้งกลุ่ม ITIL Champion ภายในองค์กรขึ้น และผลักดันให้พนักงานในองค์กรมีส่วนร่วม ในการปรับปรุงกระบวนการทำงานอย่างต่อเนื่อง ทั้งนี้จะต้องมีการประเมินผลและตรวจติดตามอย่างต่อเนื่อง สำหรับการปรับปรุงกระบวนการทำงานต่างๆที่เกิดขึ้นเพื่อที่จะได้ทราบผลลัพธ์ หรือผลสะท้อนกลับของกระบวนการที่ได้ถูกสร้างขึ้น และนำผลลัพธ์นั้นมามีส่วนทำให้เกิดการปรับปรุงกระบวนการอย่างต่อเนื่องและทำให้มั่นใจได้ว่ากระบวนการทำงานนั้นๆ สามารถคงไว้ซึ่งความสำเร็จของการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืน

ประโยชน์ของงานวิจัยนี้ทำให้ทราบว่า ถ้าองค์กรต้องการให้มีการนำ ITIL มาใช้อย่างยั่งยืน ผู้บริหารต้องให้การสนับสนุนอย่างต่อเนื่อง โดยผู้บริหารเป็นปัจจัยที่สำคัญที่สุด เพราะจะเป็นผู้สร้างความตระหนักในกรอบวิธีปฏิบัติ ITILให้เกิดขึ้นได้ภายในองค์กร อีกทั้งยังมีอำนาจในการจัดตั้งกลุ่ม ITIL Champion เพื่อเป็นกลุ่มคนที่ทำงานและผลักดันให้นำ ITIL มาใช้ภายในองค์กรได้อย่างเหมาะสมสอดคล้องกับวัฒนธรรมองค์กร นอกจากนี้ผู้บริหารควรทำให้พนักงานในองค์กรมีส่วนร่วม ในการหารือ วางแผน และปรับปรุงกระบวนการทำงานร่วมกัน และมีการประเมินผลและการตรวจติดตามอย่างต่อเนื่องเป็นตัวสะท้อนกลับผลลัพธ์ของกระบวนการทำงาน และนำไปสู่การปรับปรุงกระบวนการเพื่อให้องค์กรคงไว้ซึ่ง ITIL ภายในองค์กรอย่างยั่งยืน

งานวิจัยได้ศึกษาปัจจัยที่มีผลต่อความสำเร็จในการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืน โดยเป็นการศึกษาเฉพาะภายในบริษัท โกซอฟท์ (ประเทศไทย) จำกัดเท่านั้น ผู้วิจัยเห็นว่า ผู้ตอบแบบสอบถามส่วนใหญ่ทำงานภายในบริษัทมานานมากกว่า 5 ปี จึงค่อนข้างคุ้นชินกับกระบวนการทำงาน และวัฒนธรรมองค์กรเป็นอย่างดี และสามารถทำให้องค์กรคงไว้ซึ่งมาตรฐานไว้มาเป็นเวลานาน ลักษณะในการตอบแบบสอบถามจึงเป็นไปในทิศทางเดียวกัน ดังนั้น การวิจัยในอนาคตควรจะทำการศึกษาปัจจัยที่มีผลต่อความสำเร็จในการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืน จากหลากหลายบริษัท หรือองค์กรที่เพิ่งทำการ Implement ITIL ภายในองค์กร เพื่อหาความแตกต่างที่เกิดจากวัฒนธรรมและสภาพแวดล้อมที่แตกต่างกัน

นอกจากนี้ เนื่องจากปัจจัยที่มีผลต่อความสำเร็จในการนำ ITIL มาใช้ในองค์กรอย่างยั่งยืนที่กล่าวข้างต้น ยังไม่ได้เป็นปัจจัยที่ส่งผลต่อมาตรฐานอื่นๆที่มีสำหรับมาตรฐานของเทคโนโลยีสารสนเทศ เช่น Cobit, IEEE, ISO/IEC27001 เป็นต้น จึงเป็นที่น่าสนใจในการศึกษาเพิ่มเติมเป็นอย่างยิ่งว่า มีปัจจัยอื่นๆที่มีผลต่อความสำเร็จในการนำมาตรฐานอื่นๆ มาใช้ในองค์กรอย่างยั่งยืนหรือไม่

บรรณานุกรม

กิตติพงษ์บูรณกูล. (2552). *ปัจจัยที่มีผลต่อความสำเร็จของการนำ ITIL Best Practice มาประยุกต์ใช้ กรณีศึกษาธนาคารออมสิน*.การค้นคว้าอิสระปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์ วิทยาลัยนวัตกรรม.

ชมพูนุท สุวารี. (2551). *ทัศนคติและความพึงพอใจของพนักงานที่มีต่อการนำ ITIL มาใช้งานในองค์กร กรณีศึกษา: บริษัทรอยเตอร์ ซอฟท์แวร์ ประเทศไทย*.การค้นคว้าอิสระปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์ วิทยาลัยนวัตกรรม.

เพ็ญแข ศิริวรรณ. (2546). สถิติเพื่อการวิจัยโดยใช้คอมพิวเตอร์ (SPSS Version10). กรุงเทพฯ: เท็กซ์แอนด์เจอร์นัลพับลิเคชั่น.

เบญจพร ฉายาลักษณ์. (2552). *ปัจจัยที่มีอิทธิพลต่อความสำเร็จในการนำ ITIL มาใช้ในองค์กร กรณีศึกษา ธนาคารพาณิชย์แห่งหนึ่งการค้นคว้าอิสระปริญญามหาบัณฑิต*.มหาวิทยาลัยธรรมศาสตร์ วิทยาลัยนวัตกรรม.

ประภาดา ตลึงจิตร. (2555). *แนวทางในการเสริมสร้างความตระหนักถึงการปฏิบัติตามระเบียบการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ไทย: Case study research of Thai Cooperative*. การค้นคว้าอิสระปริญญามหาบัญฑิต, มหาวิทยาลัยธรรมศาสตร์.

Angheluta, T., Pirnea, I. C., and Moisa, C.(2012). Quality System Implementation Process for Sustainable Success Developmentin Romanian SMEs.*Economy Transdisciplinarity Cognition*, 15(1), 226-232.

Burge, R. (2008). Ready set Change. ABI/Inform Global, 35.

Cater-Steel, A., Toleman, M., and Tan, W. G. (2006). Transforming IT service management - the ITIL impact.*ACIS 2006: 17th Australasian Conference on Information Systems*, Adelaide, South Australia, Retrieved April 11, 2014 from http://eprints.usq.edu.au/1612/.

Cater-Steel, A., Tan, W. G., and Toleman, M. (2007). *itSMF Australia 2007 Conference: Summary of ITSM Standards and Frameworks Survey Responses*. Unpublished doctoral dissertation, University of Southern Queensland, Toowoomba Australia.

Cătălin, S. H., Bogdan, B., and Dimitrie, G. R. (2014). The Existing Barriers in Implementing Total Quality Management. *Annals of the University of Oradea, Economic Science Series*, 23(1).

Cherrington, C., and Greenway, D. (2008). Green ITIL. *Capgemini, Woking, Surrey*.

Chow, T., and Cao, D. B. (2008). A survey study of critical success factors in agile software projects. *Journal of Systems and Software*, 81(6), 961-971.

Clifford, A. (2009). Sustainable IT.RetrievedNovember 20, 2014 from http://it.toolbox.com/blogs/minimalit/sustainable-it-30157.

Harmon, R.R., and Moolenkamp, N. (2012). Suntainable IT Services: Developing a Strategy Framework.*International Journal of Innovation & Technology Management*, 9(2), 1-23.

Huang, T., Pepper, M., and Bowrey, G. (2014). Implementing a Sustainability Balanced Scorecard to Contribute to the Process of Organisational Legitimacy Assessment. *Australasian Accounting, Business and Finance Journal*, 8(2), 15-34.

Iden, J., and Eikebrokk, T. R. (2011). Understanding the ITIL implementation project. International Organization for Standardization(2004). Retrieved November 19, 2014, from http://www.iso.org/iso/news.htm?refid=Ref930.

John, K. (2007). ITIL and the Corporate Culture: How to Manage the Cultural Change that ITIL Demands. *itSMF Thailand*, Retrieved June 28, 2014 from http://www.itsmf.or.th/index2.php?option=com_docman&task=doc_view&gid=43&Itemid=34.

Kaziliûnas, A. (2008). Problems of auditing using quality management systems for sustainable development of organizations.*Technological and Economic Development of Economy*, 14(1), 64-75.

Korte, M., Lee, K., and Fung, C.C. (2012).Evolving IT management frameworks towards a sustainable future. In: 21st International Conference on Information Systems Development (ISD2012), Prato Italy.

Marquis, H. (2006). ITIL: What it is and what it isn't. *Business Communication Review*. 49-52.

Mosadeghrad, A. (2014). Why TQM programmes fail? A pathology approach. *The TQM Journal*, 26(2), 160-187.

Neničková, H. (2011). Critical Success Factors for ITIL Best Practices Usage.*Economics and Management*. Retrieved June 28, 2014 from http://www.ktu.lt/lt/mokslas/zurnalai/ekovad/16/1822-6515-2011-0839.pdf.

Pankoff, J. A. (2005). Improve and sustain process plant operator performance: A systems approach can enhance workforce execution to achieve operational excellence (OpX). *Hydrocarbon processing*, 84(7), 97-99.

Pollard, C., and Cater-Steel, A. (2009). Justifications, Strategies, and Critical Success Factors in Successful ITIL Implementations in U.S. and Australian Companies: An Exploratory Study. *Information System Management*, 26(2), 164-175.

Sallé, M. (2004). *IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing*. Hewlett-Packard Company.

Sharifi, M., Ayat, M., Rahman, A. A., and Sahibudin, S. (2008). Lessons Learned in ITIL implementation failure. *International Symposium on Information Technology*, Kuala Lumpur, 1-4.

Spremić, M., Zmirak, Z., and Kraljevic, K. (2008). IT and Business Process Performance Management: Case Study of ITIL Implementation in Finance Service Industry. *The ITIL 2008 30th International Conference on Information Technology Interfaces*, Dubrovnik, 243-250.

การสำรวจระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศองค์กร

จรัญยา ธงนิมิตร์*

SC Asset Corporation Public Co., Ltd.

***Correspondence:** Jarunya.msmis@gmail.com doi: 10.14456/jisb.2016.9

บทคัดย่อ

วัตถุประสงค์ของการศึกษานี้ เพื่อสำรวจระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศ ขององค์กรที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย (SET) และตลาดหลักทรัพย์ เอ็ม เอ ไอ (MAI) จำนวน 408 องค์กร ตามกรอบวิธีปฏิบัติ COBIT 5 ในโดเมนการจัดวางแนวทาง การจัดทำแผน และการจัดระบบ (Align, Plan and Organize หรือ APO) ซึ่งประกอบด้วย 13 กระบวนการ ได้แก่ ด้านกรอบการจัดการงานเทคโนโลยีสารสนเทศ ด้านการจัดการกลยุทธ์ ด้านการจัดการสถาปัตยกรรมองค์กร ด้านการจัดการนวัตกรรม ด้านการจัดการผลงาน ด้านการจัดการงบประมาณและค่าใช้จ่าย ด้านการจัดการทรัพยากรมนุษย์ ด้านการจัดการความสัมพันธ์ ด้านการจัดการสัญญาบริการ ด้านการจัดการผู้จัดจำหน่าย ด้านการจัดการคุณภาพ ด้านการจัดการความเสี่ยง และด้านการจัดการความปลอดภัย นอกจากนี้ยังสำรวจแรงผลักดันและอุปสรรคในการกำกับดูแลเทคโนโลยีสารสนเทศองค์กร

ผลการสำรวจ พบว่าระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศตามกรอบวิธีปฏิบัติ COBIT 5 ในโดเมนการจัดวางแนวทาง การจัดทำแผน และการจัดระบบ (Align, Plan and Organize หรือ APO) โดยรวม แยกตามกลุ่มอุตสาหกรรมนั้น กลุ่มอุตสาหกรรมที่มีระดับวุฒิภาวะสูงสุดอยู่ในระดับวุฒิภาวะที่ 3 (หรือมีการกำหนดกระบวนการ) จากระดับวุฒิภาวะที่ 5 ซึ่งเป็นระดับวุฒิภาวะที่สูงที่สุด (หรือมีการปฏิบัติที่ดีที่สุด) ได้แก่ กลุ่มธุรกิจการเงิน กลุ่มสินค้าอุตสาหกรรม กลุ่มเทคโนโลยี กลุ่มทรัพยากร กลุ่มบริการ กลุ่มสินค้าอุปโภคบริโภค และอุตสาหกรรมอื่น ๆที่ไม่จัดอยู่ในกลุ่มอุตสาหกรรมใด และกลุ่มอุตสาหกรรมที่มีระดับวุฒิภาวะต่ำสุดอยู่ในระดับวุฒิภาวะที่ 2 (หรือมีการทำซ้ำ) จากระดับวุฒิภาวะที่ 5 ซึ่งเป็นระดับวุฒิภาวะที่สูงที่สุด (หรือมีการปฏิบัติที่ดีที่สุด) ได้แก่ กลุ่มอสังหาริมทรัพย์และก่อสร้าง และกลุ่มเกษตรและอุตสาหกรรมอาหาร

ส่วนผลของการสำรวจระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศ ตามกระบวนการจำนวน 13 กระบวนการของโดเมนการจัดวางแนวทาง การจัดทำแผน และการจัดระบบ (Align, Plan and Organize หรือ APO) พบว่าระดับวุฒิภาวะสูงสุดอยู่ในระดับวุฒิภาวะที่ 3 (หรือมีการกำหนดกระบวนการ) จากระดับวุฒิภาวะที่ 5 ซึ่งเป็นระดับวุฒิภาวะที่สูงที่สุด (หรือมีการปฏิบัติที่ดีที่สุด) ได้แก่ ด้านการจัดการความปลอดภัย ด้านกรอบการจัดการงานเทคโนโลยีสารสนเทศ ด้านการจัดการงบประมาณและค่าใช้จ่าย ด้านการจัดการความเสี่ยง ด้านการจัดการทรัพยากรมนุษย์ ด้านการจัดการคุณภาพ ด้านการจัดการกลยุทธ์ ด้านการจัดการสัญญาบริการ ด้านการจัดการผู้จัดจำหน่าย ด้านการจัดการความสัมพันธ์ ด้านการจัดการผลงาน ด้านการจัดการนวัตกรรม และที่มีระดับวุฒิภาวะต่ำสุดอยู่ในระดับวุฒิภาวะที่ 2 (หรือมีการทำซ้ำ) จากระดับวุฒิภาวะที่ 5 ซึ่งเป็นระดับวุฒิภาวะที่สูงที่สุด (หรือมีการปฏิบัติที่ดีที่สุด) ได้แก่ ด้านการจัดการสถาปัตยกรรมองค์กร

จากผลการสำรวจแรงผลักดัน พบว่าแรงผลักดันในการกำกับดูแลเทคโนโลยีสารสนเทศองค์กร จากมากไปน้อย ตามลำดับ ได้แก่ เพื่อปรับปรุงประสิทธิภาพการทำงาน เพื่อลดความเสี่ยง เพื่อปฏิบัติตามกฎระเบียบและกฎหมาย เพื่อสร้างชื่อเสียงและความไว้วางใจให้กับองค์กร เพื่อลดค่าใช้จ่าย เพื่อบรรลุพันธกิจและเป้าหมาย และเพื่อเพิ่มสภาพแวดล้อมการแข่งขัน และผลการสำรวจอุปสรรค พบว่าอุปสรรคในการกำกับดูแลเทคโนโลยีสารสนเทศองค์กร จากมากไปน้อย ตามลำดับ ได้แก่ ข้อจำกัดด้านงบประมาณ

การจัดการองค์ความรู้ ความสามารถหรือทักษะของพนักงานไม่เพียงพอ ความยากของวิธีการ ยังไม่ได้จัดอยู่ในลำดับที่ความสำคัญที่จะจัดสรรทรัพยากร ไม่สามารถหาผู้รับผิดชอบในการควบคุม และอุปสรรคอื่นๆ

ประโยชน์จากการสำรวจนี้ ทำให้ทราบระดับวุฒิภาวะขององค์กร และยังเป็นแนวทางในการช่วยวางแผนและกำหนดเป้าหมายที่ควรพัฒนาปรับปรุงเพื่อให้มีระดับวุฒิภาวะระดับที่สูงขึ้น ทั้งนี้ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ หรือผู้ที่เกี่ยวข้องสามารถใช้ผลการสำรวจนี้ในการให้ข้อมูลกับผู้บริหาร นำมาเป็นรายการตรวจสอบ (Check Lists) หรือแผนการตรวจสอบ (Audit Program) เพื่อดำเนินการให้เกิดการกำกับดูแลด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพมากยิ่งขึ้น อันจะสร้างความน่าเชื่อถือและสร้างมูลค่าเพิ่มให้กับองค์กร

นอกจากนี้ผลการสำรวจแรงผลักดันและอุปสรรคในการกำกับดูแลเทคโนโลยีสารสนเทศ ทำให้ทราบถึงเหตุผลส่วนใหญ่ที่เป็นแรงผลักดันให้องค์กรดำเนินการกำกับดูแลเทคโนโลยีสารสนเทศ เช่น ความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ และประโยชน์ของเทคโนโลยีสารสนเทศในการสร้างคุณค่าให้กับองค์กร และ องค์กรควรสนับสนุนด้านงบประมาณในการกำกับดูแลเทคโนโลยีสารสนเทศอย่างเหมาะสม

คำสำคัญ: กรอบวิธีปฏิบัติ COBIT ระดับวุฒิภาวะ การกำกับดูแลด้านเทคโนโลยีสารสนเทศ

Survey of the Maturity Levels of IT Governance

Jarunya Thongnimith*

SC Asset Corporation Public Co., Ltd.

***Correspondence:** Jarunya.msmis@gmail.com doi: 10.14456/jisb.2016.9

Abstract

The objective of this study is to survey the Maturity Levels in IT Governance of listed companies on the Stock Exchange of Thailand (SET) and Market for Alternative Investment (MAI). This research collected data from 408 organizations. The collected data are only APO domain (Align, Plan and Organize domain) in COBIT 5 framework which consists 13 processes: Manage the IT Management Framework, Manage Strategy, Manage Enterprise Architecture, Manage innovation, Manage Portfolio, Manage Budget and Costs, Manage Human Resources, Manage Relationships, Manage Service Agreements, Manage Suppliers, Manage Quality, Manage Risk and Manage Security. Furthermore, this survey also collected data of the driving and inhibiting forces to use IT governance.

From the Maturity Level of overall APO domain in COBIT 5 framework which classified by industry group, the results indicated that the highest Maturity Level is 3 (which is defined processes) out of highest Maturity Level 5 (which is optimized). These industries are Financials, Industrials, Technology, Resources, Services, Consumer Products and Companies Under Rehabilitation. The lowest Maturity Level is 2 (which is repeatable but intuitive) out of highest Maturity Level 5 (which is optimized). These industries are Property & Construction and Agro & Food Industry.

From the Maturity Level of each process in 13 APO processes, the results indicated that the highest Maturity Level is 3 (which is defined processes) out of highest Maturity Level 5 (which is optimized). The processes in this level are Manage Security, Manage the IT Management Framework, Manage Budget and Costs, Manage Risk, Manage Human Resources, Manage Quality, Manage Strategy, Manage Service Agreements, Manage Suppliers, Manage Relationships, Manage Portfolio and Manage innovation. The lowest Maturity Level is 2 (which is repeatable but intuitive) out of highest Maturity Level 5 (which is optimized). The process in this level is Manage Enterprise Architecture.

Furthermore, results from the rank of driving forces of IT Governance from high to low are Performance improvement, Risk reduction, Legal regulatory and contract compliance, Reputation and trust, Cost reduction, Mission and goals and Competitive environment respectively. In addition, results from the rank of inhibiting forces of IT Governance from high to low are Budget limitation, Management awareness, Availability of skilled staff, No easy solution, Resource priorities, Lack of ownership and other Inhibiting.

Benefits of this research are to help organizations know the current Maturity Level, plan and set target to be the higher Maturity Level. Moreover, auditor or related persons can use this survey results as a checklist or audit

program for providing information to the Executive in order to improve IT Governance effectively, build trust and add value to the organization.

The results of survey of driving and inhibiting forces of IT Governance show that the most of reason for driving forces to use IT Governance such as risks associated with the use of information technology and using information technology to benefit the organization and organize should support budget for IT Governance appropriately.

Keywords: COBIT, Maturity Level, IT Governance

1. บทนำ

ในสถานการณ์ปัจจุบันผู้บริหารองค์กร โดยเฉพาะผู้บริหารเทคโนโลยีสารสนเทศมีความจำเป็นที่จะต้องศึกษามาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัยในเทคโนโลยีสารสนเทศ เพื่อนำมาประยุกต์ใช้ในองค์กร เหตุผลมีหลายประการ เช่น องค์กรต้องปฏิบัติตามกฎระเบียบ (Compliance) เพื่อปฏิบัติให้เป็นไปตามกฎหมายของประเทศที่องค์กรนั้นตั้งสำนักงานอยู่ ดังนั้นการกำหนดกลยุทธ์ในการบริหารจัดการเทคโนโลยีสารสนเทศและการรักษาความปลอดภัยสารสนเทศจึงเป็นเรื่องสำคัญที่ผู้บริหารทุกท่านต้องจัดทำขึ้น และผู้บริหารจะต้องมีความรับผิดชอบในเรื่องดังกล่าวโดยปริยาย นอกจากนี้กฎหมายต่าง ๆ ที่กำลังจะถูกประกาศใช้ เช่น กฎหมายการกระทำผิดเกี่ยวกับคอมพิวเตอร์ หรือประกาศกฎข้อบังคับต่างๆ ขององค์กรที่มีหน้าที่ในการควบคุม เช่น สำนักงานตรวจเงินแผ่นดิน (สตง.) ธนาคารแห่งประเทศไทย (ธปท.) หรือสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) เป็นต้น โดยองค์กรดังกล่าวมีแนวโน้มที่จะเข้มงวดเรื่องการรักษาความมั่นคงปลอดภัยของข้อมูลในระบบสารสนเทศมากขึ้น ผู้บริหารที่ต้องการให้องค์กรดำเนินงานอย่างมีประสิทธิภาพ และประสิทธิผล สามารถบรรลุเป้าหมายขององค์กรได้นั้น จำเป็นต้องนำมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัยในเทคโนโลยีสารสนเทศมาประยุกต์ใช้เพื่อความปลอดภัยขององค์กร และเพื่อให้สอดคล้องกับยุคของไอทีภิบาล (IT Governance) และมุ่งสู่การเป็นบรรษัทภิบาลที่ดีในที่สุด (Good Corporate Governance) (นงลักษณ์ กอศรีลบุตร, 2549; ปริญญา หอมเอนก, 2548)

กรอบวิธีปฏิบัติ COBIT (Control Objectives for Information and Related Technology) มีจุดประสงค์ในการสร้างความมั่นใจว่า การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศนั้นสอดคล้องกับวัตถุประสงค์เชิงธุรกิจขององค์กร (Business Objectives) เพื่อให้เกิดความสมดุลระหว่างความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) และผลตอบแทนของการลงทุนในระบบสารสนเทศ (IT Return on Investment) (นงลักษณ์ กอศรีลบุตร, 2549) กรอบวิธีปฏิบัติ COBIT 5 ประกอบด้วยกิจกรรมหลัก 37 หัวข้อ ซึ่งเชื่อมกับกิจกรรมย่อยอีก 210 หัวข้อ โดยสามารถแบ่งได้เป็น 5 โดเมน ดังนี้

การจัดวางแนวทาง การจัดทำแผน และการจัดระบบ (APO: Align, Planning and Organize)

การจัดสร้าง การจัดหา และการนำไปใช้ (BAI: Build, Acquire and Implement)

การส่งมอบ การให้บริการ และการสนับสนุน (DSS: Deliver, Service and Support)

การเฝ้าติดตาม การวัดผล และการประเมิน (MEA: Monitor, Evaluate and Assess)

การประเมิน การสั่งการ และการเฝ้าติดตาม (EDM: Evaluate, Direct and Monitor)

เมื่อพิจารณากรอบวิธีปฏิบัติ และมาตรฐานในการกำกับดูแลเทคโนโลยีสารสนเทศต่างๆ กับสภาวะแวดล้อมและสถานการณ์ปัจจุบันทั้งในประเทศและต่างประเทศแล้ว ทำให้ผู้วิจัยเห็นความสำคัญของการกำกับดูแลเทคโนโลยีสารสนเทศ จึงเห็นว่าควรมีการประเมินขีดความสามารถ โดยวัดระดับวุฒิภาวะของการกำกับดูแลเทคโนโลยีสารสนเทศองค์กร เพื่อให้ทราบระดับวุฒิภาวะปัจจุบัน และสามารถพัฒนาระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศให้สูงขึ้นตามเป้าหมายที่องค์กรได้กำหนดไว้

2. ทบทวนวรรณกรรม

การวิจัยเชิงสำรวจในครั้งนี้ ผู้วิจัยได้ทำการค้นคว้าเอกสารทางวิชาการ เพื่อศึกษาแนวคิดตลอดจนบทความและงานวิจัยที่เกี่ยวข้องกับการกำกับดูแลเทคโนโลยีสารสนเทศในองค์กร ดังนี้

ธรรมาภิบาลเทคโนโลยีสารสนเทศในองค์กร (IT Governance)

ธรรมาภิบาลเทคโนโลยีสารสนเทศในองค์กร หมายถึง หลักการบริหารจัดการเทคโนโลยีสารสนเทศและการสื่อสารในองค์กร ที่จะพิจารณาในเรื่องการสร้างมูลค่าของเทคโนโลยีสารสนเทศ ให้สอดคล้องกับกลยุทธ์ขององค์กร โดย IT governance ประกอบด้วย 5 กิจกรรมหลัก ดังต่อไปนี้

การกำหนดกลยุทธ์ (Strategic alignment) คือ การนำแผนกลยุทธ์ขององค์กรมากำหนดแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ เป็นการทำงานร่วมกันระหว่างผู้บริหารสูงสุดขององค์กร และผู้บริหารสูงสุดด้านเทคโนโลยีสารสนเทศ ร่วมกำหนดกลยุทธ์ทางเทคโนโลยีสารสนเทศ เพื่อที่จะสร้างความมั่นใจในการลงทุนเรื่องทรัพยากรเทคโนโลยีสารสนเทศสามารถสร้างประโยชน์สูงสุดกับองค์กร (กมล สนธนรัชต์, 2553)

การบริหารจัดการทรัพยากร (Resource management) คือ การลงทุน และจัดสรรทรัพยากรเทคโนโลยีสารสนเทศให้กับส่วนต่าง ๆ ในองค์กรตามความต้องการและความเหมาะสม

การสร้างเทคโนโลยีสารสนเทศให้กิจกรรม (Value delivery) คือ การลงทุนพัฒนาเทคโนโลยีสารสนเทศตามความต้องการ เพื่อสร้างผลประโยชน์ให้องค์กร ซึ่งในส่วนกระบวนการพัฒนาระบบยังต้องคำนึงทั้งการพัฒนาเทคโนโลยีสารสนเทศขึ้นเองในองค์กร หรือการใช้บริการภายนอกองค์กร (Outsourcing)

การวัดผลการดำเนินการ (Performance measurement) คือ การวัดผลสำเร็จและการบรรลุวัตถุประสงค์โครงการพัฒนาของเทคโนโลยีสารสนเทศที่ได้สร้างขึ้น ซึ่งแบ่งได้เป็น 2 ส่วนหลักๆ คือ

1. วัดการพัฒนาโครงการด้านเทคโนโลยีสารสนเทศ (Development metrics)
2. วัดการให้บริการ (Services metrics)

การบริหารความเสี่ยง (Risk management) คือ การประมาณความเสี่ยงที่จะเกิดขึ้น และหาแนวทางลดความเสียหายที่อาจจะเกิดขึ้นในการดำเนินกิจกรรมธรรมาภิบาล โดย IT แต่ละหน่วยงานสามารถดำเนินการตามมาตรฐานในการจัดทำไอทีภิบาลของหน่วยงานต่างๆ ได้เพื่อครอบคลุมการดำเนินการ และการวัดผล และเหมาะสมกับหน่วยงานมากที่สุด

COBIT (Control Objectives for Information and Relate Technology)

COBIT เป็นทั้งแนวคิดและแนวทางการปฏิบัติ ถูกพัฒนาขึ้นตั้งแต่ปี 1996 โดยสถาบัน IT Governance (IT Governance Institute : ITGI) ปัจจุบัน COBIT พัฒนามาถึงรุ่น 5 มีวัตถุประสงค์เพื่อเป็นกรอบแนวคิดในการบริหารจัดการร่วมกับตัวแบบธรรมาภิบาลด้านไอที เพื่อการควบคุมภายในที่ดีด้านเทคโนโลยีสำหรับองค์กรต่างๆ ที่จะใช้อ้างอิงถึงแนวทางการปฏิบัติที่ดี (Best Practice) ซึ่งสามารถนำไปปรับใช้ได้ในทุกองค์กรสำหรับกิจกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ใน COBIT 5 นั้นแบ่งกระบวนการ ออกเป็น 37 กระบวนการ จากทั้งหมด 5 โดเมน ดังต่อไปนี้

การจัดวางแนวทาง การจัดทำแผน และการจัดระบบ (APO: Align, Planning and Organize)

การจัดสร้าง การจัดหา และการนำไปใช้ (BAI: Build, Acquire and Implement)

การส่งมอบ การให้บริการ และการสนับสนุน (DSS: Deliver, Service and Support)

การเฝ้าติดตาม การวัดผล และการประเมิน (MEA: Monitor, Evaluate and Assess)

การประเมิน การสั่งการ และการเฝ้าติดตาม (EDM: Evaluate, Direct and Monitor)

COBIT 5 ให้กรอบการดำเนินงานที่ครอบคลุม เพื่อช่วยให้องค์กรบรรลุวัตถุประสงค์ในเรื่องการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร โดยครอบคลุมหน้าที่งานตามความรับผิดชอบทั้งทางด้านธุรกิจและไอทีอย่างครบวงจร พิจารณาถึงผลประโยชน์ที่เกี่ยวข้องกับไอทีของผู้มีส่วนได้เสียทั้งภายในและภายนอก โดยกรอบวิธีปฏิบัติ COBIT 5 มีหลักการที่สำคัญ 5 ประการ ดังต่อไปนี้

หลักการที่ 1 : ตอบสนองความต้องการของผู้มีส่วนได้ส่วนเสีย โดยการรักษาความสมดุลระหว่างผลประโยชน์ที่จะได้รับกับความเสี่ยงและการใช้ทรัพยากรที่ทำให้เกิดประโยชน์สูงสุด

หลักการที่ 2 : ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร โดยการบูรณาการการกำกับดูแลไอทีระดับองค์กรเข้าไปในการกำกับดูแลองค์กร ครอบคลุมทุกหน้าที่งานและกระบวนการภายในองค์กร

หลักการที่ 3 : ประยุกต์ใช้กรอบการดำเนินงานที่บูรณาการเป็นหนึ่งเดียว โดยกรอบวิธีปฏิบัติ COBIT 5 ได้นำกรอบการดำเนินงานที่เกี่ยวข้องอื่นๆ มาจัดให้สอดคล้องกันในภาพรวม จึงสามารถใช้เป็นกรอบการดำเนินงานที่ครอบอยู่เหนือกรอบการดำเนินงานอื่นๆ สำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

หลักการที่ 4 : เอื้อให้วิธีปฏิบัติแบบองค์รวมสัมฤทธิ์ผล กรอบวิธีปฏิบัติ COBIT 5 ระบุถึงกลุ่มของปัจจัยเอื้อที่ใช้สนับสนุนการนำระบบการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรไปใช้งานอย่างครอบคลุม โดยกรอบวิธีปฏิบัติของ COBIT 5 ระบุถึงปัจจัยเอื้อ 7 ประเภท ได้แก่

1. หลักเกณฑ์ นโยบาย แนวทางปฏิบัติ (Principles, Policies and Frameworks) หมายถึง แนวคิดหลัก นโยบาย และแนวทางในการปฏิบัติการดำเนินงาน เพื่อเป็นเครื่องมือที่ถูกนำมาใช้ควบคุมองค์กรในภาพรวม
2. กระบวนการ (Processes) หมายถึง องค์กรต้องมีกระบวนการเพื่อให้งานได้ผลลัพธ์หรือบรรลุเป้าหมายของกระบวนการ ซึ่งจะนำไปสู่การบรรลุซึ่งเป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและเป้าหมายระดับองค์กรได้
3. โครงสร้างบุคลากร (Organizational structures) หมายถึง ส่วนของโครงสร้างขององค์กรในการบริหารจัดการ ที่ผู้บริหารระดับสูง รวมถึง Board of Director ต้องใส่ใจกับเรื่อง IT Governance และ Enterprise Governance
4. วัฒนธรรม จริยธรรม และความประพฤติ (Culture, ethics and behaviour) เน้นไปที่บุคลากร และองค์กรในเรื่องของวัฒนธรรมองค์กร ทัศนคติของพนักงาน และผู้บริหารระดับสูง
5. ข้อมูล (Information) หมายถึง "สารสนเทศ" หรือ "ข้อมูล" ที่เราต้องจัดเก็บดูแลเพื่อนำมาใช้ประโยชน์ในองค์กร
6. โครงสร้างพื้นฐานของการให้บริการสารสนเทศ (Service Infrastructure Applications) หมายถึง โครงสร้างพื้นฐาน (Infrastructure) เทคโนโลยี (Technology) และโปรแกรมประยุกต์ (Applications) ประกอบกันเป็นระบบสารสนเทศ (Information System) ที่ถูกนำมาใช้ในการสนับสนุนการปฏิบัติงานในองค์กรและการประกอบธุรกิจ
7. ทักษะ ความรู้ และความสามารถของบุคลากร (People Skills and competencies) มุ่งเน้นไปที่สมรรถนะของบุคลากรในองค์กร เพื่อช่วยเสริมให้บรรลุเป้าหมายในภาพรวมขององค์กร

หลักการที่ 5 : แบ่งแยกการกำกับดูแลออกจากการบริหารจัดการ เนื่องจากหลักสองประการนี้ครอบคลุมถึงกิจกรรมที่ต่างกัน ต้องการโครงสร้างการจัดองค์กรที่แตกต่างกัน กล่าวคือ

การกำกับดูแล (Governance) ทำให้มั่นใจได้ว่า ความต้องการ เงื่อนไข และทางเลือกของผู้มีส่วนได้เสียได้รับการประเมิน เพื่อกำหนดวัตถุประสงค์ที่องค์กรต้องการให้บรรลุซึ่งมีความสมดุลและเห็นชอบร่วมกัน การกำหนดทิศทางผ่านการจัดลำดับความสำคัญและการตัดสินใจ และการเฝ้าติดตามผลการดำเนินงานและการปฏิบัติตามเทียบกับทิศทางและวัตถุประสงค์ที่ได้ตกลงร่วมกัน

การบริหารจัดการ (Management) ผู้บริหารวางแผน สร้าง ดำเนินงาน และเฝ้าติดตามกิจกรรมต่างๆ ให้สอดคล้องกับทิศทางที่กำหนดโดยหน่วยงานกำกับดูแล (governance body) เพื่อให้บรรลุวัตถุประสงค์ขององค์กร

เมื่อนำหลักการทั้ง 5 ประการนี้มารวมกันจะทำให้องค์กรสามารถสร้างกรอบการดำเนินงานสำหรับการกำกับดูแลและการบริหารจัดการที่มีประสิทธิผล ซึ่งส่งผลให้การใช้สารสนเทศและการลงทุนด้านเทคโนโลยีเกิดประโยชน์สูงสุด เพื่อยังประโยชน์ให้กับผู้มีส่วนได้เสีย (ISACA, 2012)

แบบจำลองวุฒิภาวะ (Maturity Model)

แบบจำลองวุฒิภาวะหมายถึง รูปแบบการประเมินขีดความสามารถขององค์กร โดยมีการวัดระดับของความเข้าใจต่อกระบวนการปฏิบัติงาน โดยมีการจัดลำดับไว้จากน้อยที่สุด ไปมากที่สุด ตั้งแต่ระดับ 0-5 โดยระดับ 0 เป็นระดับไม่มีขีดความสามารถ ไม่ได้มีการ

ดำเนินการบริหาร ควบคุม ตรวจสอบโครงการ ส่วนระดับที่ 5 คือ ระดับสูงสุดที่องค์กรนั้น มีการนำกรอบปฏิบัติที่ดีมาเป็นแนวทางในการบริหารจัดการ สามารถควบคุมบริหารจัดการโครงการได้ตามเป้าหมายที่วางไว้ โดยโมเดลวุฒิภาวะมีสเกลในการวัด ดังนี้

0 – ไม่มี (Nonexistent) ไม่มีผู้บริหารระดับสูงติดตามดูแลกิจการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเพื่อให้มั่นใจว่าเป้าหมายด้านเทคโนโลยีสารสนเทศขององค์กรได้เพิ่มคุณค่าให้กับองค์กรและมั่นใจว่าความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศได้รับการจัดการอย่างเหมาะสม

1 - ริเริ่ม/บางครั้งบางคราว (Initial/Ad hoc) ไม่มีการกำกับดูแลเทคโนโลยีสารสนเทศอย่างเป็นทางการและการติดตามดูแลขึ้นอยู่กับการพิจารณาของผู้บริหารในเรื่องที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ซึ่งจะทำเป็นกรณีๆไป การกำกับดูแลเทคโนโลยีสารสนเทศขึ้นอยู่กับการริเริ่มและประสบการณ์ของทีมบริหารด้านเทคโนโลยีสารสนเทศ โดยมีข้อมูลที่จำกัดจากผู้บริหารด้านอื่นๆในองค์กร นอกจากนี้ผู้บริหารระดับสูงจะเกี่ยวข้องเฉพาะเมื่อมีปัญหาสำคัญๆ หรือเกี่ยวข้องกับความสำเร็จเท่านั้น การวัดผลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศจะถูกจำกัดที่การวัดผลด้านเทคนิคและภายในหน้าที่งานด้านเทคโนโลยีสารสนเทศเท่านั้น

2 - ทำซ้ำแต่เป็นไปโดยสัญชาตญาณ (Repeatable but intuitive) มีความเข้าใจถึงการติดตามเทคโนโลยีสารสนเทศอย่างเป็นทางการมากขึ้นและจำเป็นต้องแบ่งหน้าที่ความรับผิดชอบในการบริหาร ซึ่งต้องการการสนับสนุนจากผู้บริหารระดับสูง มีการปฏิบัติที่แสดงให้เห็นถึงการกำกับดูแลอย่างสม่ำเสมอ เช่น การประชุมเพื่อสอบทาน การจัดทำรายงานผลการปฏิบัติงาน และการสอบทานปัญหาที่เกิดขึ้น แต่การกระทำดังกล่าวจะขึ้นอยู่กับการริเริ่มของทีมงานบริหารด้านเทคโนโลยีสารสนเทศ โดยผู้มีส่วนได้เสียหลักที่ให้ความร่วมมือนั้น จะกระทำโดยสมัครใจและขึ้นอยู่กับโครงการด้านเทคโนโลยีสารสนเทศปัจจุบันและลำดับความสำคัญ การระบุปัญหาจะระบุจากโครงการซึ่งทีมงานเห็นว่าเป็นสิ่งที่จำเป็นในการปรับปรุงเท่านั้น

3 - กำหนดกระบวนการ (Defined process) มีการกำหนดกรอบการประมวลผลเพื่อติดตามดูแลกิจการด้านเทคโนโลยีสารสนเทศและนำมาใช้ในองค์กรซึ่งเป็น พื้นฐานของการกำกับดูแลด้านเทคโนโลยีสารสนเทศ คณะกรรมการบริษัทกำหนดแนวทางเพื่อพัฒนาขั้นตอนการปฏิบัติงานที่ครอบคลุมกิจกรรมการกำกับดูแลหลักๆ ประกอบด้วย การกำหนดเป้าหมายปกติ สอบทานผลการปฏิบัติงาน ประเมินความสามารถกับแผนงานที่จำเป็น และแผนโครงการ และการสนับสนุนเงินทุนเพื่อปรับปรุงเทคโนโลยีสารสนเทศที่จำเป็น การปฏิบัติอย่างไม่เป็นทางการที่ประสบผลสำเร็จได้รับการกำหนดให้ปฏิบัติตามอย่างเป็นทางการและเทคนิคที่ใช้ในการติดตามเป็นเทคนิคที่ง่ายและไม่ซับซ้อน

4 - จัดการและวัดผลได้ (Managed and measurable) มีการกำหนดเป้าหมายที่มีความซับซ้อนพอประมาณที่สัมพันธ์กับเป้าหมายธุรกิจ นอกจากนี้การวัดผลการปรับปรุงกระบวนการด้านเทคโนโลยีสารสนเทศเป็นที่ทราบกันอย่างดี มีการรายงานผลการปฏิบัติงานที่เป็นจริงต่อผู้บริหารในรูปแบบของกระดานสมดุล ทีมงานบริหารขององค์กรทำงานร่วมกันโดยมีเป้าหมายเดียวกัน คือ ส่งมอบเทคโนโลยีที่มีคุณค่ามากที่สุดและบริหารความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ นอกจากนี้ยังมีการประเมินความสามารถด้านเทคโนโลยีสารสนเทศและโครงการที่จัดทำเสร็จสิ้นแล้วว่าสามารถปรับปรุงผลการปฏิบัติงานผ่านทางเทคโนโลยีสารสนเทศอย่างแท้จริงท้ายที่สุด ความสัมพันธ์ระหว่างผู้ใช้งานและผู้ให้บริการภายนอกต่อหน้าที่งานด้านเทคโนโลยีสารสนเทศจะขึ้นกับคำนิยามของบริการและสัญญาการให้บริการตามที่ตกลงกันไว้

5 - มีการปฏิบัติที่ดีที่สุด (Optimized) มีการพัฒนาการกำกับดูแลเทคโนโลยีสารสนเทศด้วยวิธีการที่ซับซ้อน โดยใช้เทคนิคที่มีประสิทธิภาพและประสิทธิผล มีความชัดเจนในกิจกรรมด้านเทคโนโลยีสารสนเทศและคณะกรรมการบริษัทมีการควบคุมกลยุทธ์ด้านเทคโนโลยี

บทความและงานวิจัยที่เกี่ยวข้อง

Ursacescu (2014) กล่าวว่าการกำกับดูแลเทคโนโลยีสารสนเทศตามกรอบวิธีปฏิบัติ COBIT ได้กลายเป็นสิ่งสำคัญสำหรับองค์กร ดังนั้นการดำเนินการกำกับดูแลเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ (ITG) ได้กลายเป็นสิ่งจำเป็น ซึ่งช่วยให้มั่นใจว่าไอทีสนับสนุนเป้าหมายทางธุรกิจ โดยภารกิจหลักของแผนกไอที คือ การสนับสนุนกระบวนการทางธุรกิจขององค์กรและการปรับปรุงประสิทธิภาพและ

การแข่งขันขององค์กร ด้วยเหตุนี้กระบวนการบริหารจัดการไอทีจึงเป็นสิ่งสำคัญสำหรับการบริหารจัดการธุรกิจ ซึ่งมีความสอดคล้องกับหลักการทั่วไปของการกำกับดูแลกิจการ โดยเครื่องมือในการกำกับดูแลเทคโนโลยีสารสนเทศ คือ กรอบวิธีปฏิบัติ COBIT ได้กลายเป็นหนึ่งในแนวทางที่สำคัญที่สุดสำหรับการกำกับดูแลเทคโนโลยีสารสนเทศ ซึ่งเป็นเครื่องมือที่มีประโยชน์ที่จะเริ่มต้นการประเมินระบบสารสนเทศขององค์กร (Abu-Musa, 2010) โดยกรอบวิธีปฏิบัติ COBIT จะช่วยในการเชื่อมโยงระหว่างเป้าหมายธุรกิจกับเทคโนโลยีสารสนเทศ และการวางตำแหน่งของเป้าหมายระบบสารสนเทศ กับ กระบวนการของระบบสารสนเทศ ให้มีความสอดคล้องกัน (Tanuwijaya and Sarno, 2010)

ในขณะที่ Pasquini and Galiè (2013) กล่าวว่าการประเมินระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศเป็นองค์ประกอบหลักของกรอบวิธีปฏิบัติ COBIT โดยการกำหนดขั้นตอนสำหรับกระบวนการที่เกี่ยวข้องกับ IT ช่วยให้องค์กรสามารถกำหนดกระบวนการหลักภายใต้การควบคุมซึ่งเป็นตัวแทนที่มีศักยภาพได้ โดยการประเมินระดับวุฒิภาวะ ช่วยให้องค์กรที่ต้องการประเมินตนเอง สามารถวัดระดับของกระบวนการบริหารจัดการของแต่ละกระบวนการ รู้สถานะการควบคุมด้านเทคโนโลยีสารสนเทศปัจจุบันขององค์กร เพื่อพัฒนากลยุทธ์สำหรับการปรับปรุง และสามารถนำระดับวุฒิภาวะไปเปรียบเทียบกับภาคอุตสาหกรรม และบรรทัดฐานอื่นได้ (Liu and Ridley, 2005) องค์กรที่ต้องการประเมินระดับวุฒิภาวะหรือต้องการบรรลุวัตถุประสงค์ตามที่กำหนด สามารถใช้กรอบวิธีปฏิบัติ COBIT และ BSC ร่วมกัน เพื่อสร้างประสิทธิภาพในการประเมินและพัฒนาคุณภาพของการดำเนินงานด้านสารสนเทศขององค์กรได้ (Frank, 2011) โดยกรอบวิธีปฏิบัติ COBIT ได้ให้แนวทางปฏิบัติที่ดีที่สุดและเป็นตัวชี้วัดในการดำเนินงาน ในขณะที่ BSC ช่วยในเรื่องการวางแผนเชิงกลยุทธ์และการดำเนินการตามกรอบการดำเนินงาน (ISACA, 2012) กรอบวิธีปฏิบัติ COBIT มีปัจจัยความสำเร็จและตัวชี้วัดที่สำคัญ คือ ระดับวุฒิภาวะองค์กร ซึ่งหลักการพื้นฐานของวุฒิภาวะขององค์กร คือองค์กรสามารถย้ายไปอยู่ในระดับวุฒิภาวะที่สูงขึ้นก็ต่อเมื่อเงื่อนไขทั้งหมดที่อธิบายไว้ในระดับที่กำหนดสูงกว่าเป็นจริง โดยการบริหารจัดการสามารถใช้กรอบวิธีปฏิบัติ COBIT ประเมินระดับวุฒิภาวะของตนเอง และสร้างมาตรฐานด้วยการอ้างอิงการควบคุมทางด้านระบบสารสนเทศ อนึ่งการวัดระดับวุฒิภาวะ เริ่มจากระดับ 0 คือ ไม่มีตัวตน เป็นผลให้องค์กรสามารถปรับปรุงระบบการควบคุมภายในขององค์กรให้ไปถึงระดับ 5 คือ ประสิทธิภาพ (Pederiva, 2003) นอกจากนี้ Guldentops, Grembergen and Haes (2002) ได้เก็บรวบรวมและวิเคราะห์ระดับวุฒิภาวะของผู้ประกอบการในการควบคุมกระบวนการด้านเทคโนโลยีสารสนเทศ จากกระบวนการที่สำคัญที่สุด 15 กระบวนการของกรอบวิธีปฏิบัติ COBIT ผลการสำรวจพบว่าโดยเฉลี่ยระดับวุฒิภาวะของกลุ่มอุตสาหกรรมการเงินอยู่ระหว่าง 2.0 และ 2.5 และโดยเฉลี่ยระดับวุฒิภาวะของบริษัทระดับโลก มีระดับวุฒิภาวะอยู่ระหว่าง 2.5 - 3.0 ซึ่งทำให้เห็นว่าความแตกต่างของประเภทอุตสาหกรรม และภูมิศาสตร์ มีผลกับระดับวุฒิภาวะองค์กร

3. วิธีการวิจัย

กลุ่มประชากรของการสำรวจนี้ คือ องค์กรที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย (SET) และตลาดหลักทรัพย์ เอ็ม เอ ไอ (MAI) จำนวน 676 องค์กร ซึ่งจำแนกตาม 9 กลุ่มอุตสาหกรรม ได้แก่ กลุ่มบริการ กลุ่มอสังหาริมทรัพย์และก่อสร้าง กลุ่มสินค้าอุตสาหกรรม กลุ่มธุรกิจการเงิน กลุ่มเกษตรกรและอุตสาหกรรมอาหาร กลุ่มสินค้าอุปโภคบริโภค กลุ่มเทคโนโลยี กลุ่มทรัพยากร และองค์กรที่ไม่ได้จัดอยู่ในกลุ่มอุตสาหกรรมใด การเก็บข้อมูล เลือกใช้วิธีการเก็บข้อมูลด้วยชุดแบบสอบถาม โดยส่งแบบสำรวจความคิดเห็นแก่กลุ่มตัวอย่าง ซึ่งเป็นพนักงานในองค์กรที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย และตลาดหลักทรัพย์ เอ็ม เอ ไอ (MAI) ที่มีบุคลากรทางด้านระบบสารสนเทศปฏิบัติงานอยู่ แบบสอบถามจะถูกส่งไปยังฝ่ายเทคโนโลยีสารสนเทศเพื่อให้ผู้บริหารหรือพนักงานในฝ่ายเทคโนโลยีสารสนเทศตอบคำถามในแบบสอบถาม โดยมีช่องทางส่งแบบสอบถามกลับมายังผู้วิจัยผ่านทางไปรษณีย์ และจดหมายอิเล็กทรอนิกส์ ทั้งนี้แบบสอบถามใดที่ไม่ได้รับตรงตามกำหนดเวลา ผู้วิจัยจะดำเนินการติดตามโดยจดหมายอิเล็กทรอนิกส์หรือทางโทรศัพท์ หลังจากได้รับแบบสอบถามกลับคืนมาแล้ว จะทำการตรวจสอบเพื่อคัดแยกข้อมูลที่ผู้ตอบกรอกข้อมูลไม่ครบตามที่ต้องการออกไป และจะนำข้อมูลที่สามารถนำมาวิเคราะห์โดยใช้เกณฑ์ระดับวุฒิภาวะองค์กร (Maturity Level) ในการวัดระดับ โดยแบ่งการคำนวณ

ตามองค์กรที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย (SET) และตลาดหลักทรัพย์ เอ็ม เอ ไอ (MAI) เพื่อนำข้อมูลมาใช้ในการเปรียบเทียบ ซึ่งมีขั้นตอนการคำนวณดังต่อไปนี้

1. นำคำตอบระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศองค์กรที่แต่ละองค์กรตอบแบบสอบถาม มาแปลงเป็นระดับวุฒิภาวะจาก 0 – 5
2. หาค่าความถี่ของผู้ตอบแบบสอบถาม จากการประเมินระดับวุฒิภาวะในแต่ละกระบวนการ รวมทุกกลุ่มอุตสาหกรรม
3. หาค่าความถี่ของผู้ตอบแบบสอบถาม จากการประเมินระดับวุฒิภาวะในแต่ละกระบวนการ แยกตามกลุ่มอุตสาหกรรม
4. หาค่าเฉลี่ยของระดับวุฒิภาวะในแต่ละกระบวนการ รวมทุกกลุ่มอุตสาหกรรม
5. หาค่าเฉลี่ยของระดับวุฒิภาวะตามกระบวนการด้านการจัดวางแนวทาง การจัดทำแผน และการจัดระบบ (Align, Plan and Organize หรือ APO) แยกตามกลุ่มอุตสาหกรรม
6. นำค่าเฉลี่ยระดับวุฒิภาวะที่ได้ มาจัดระดับวุฒิภาวะตามหลักเกณฑ์ที่กำหนดหลักเกณฑ์ดังนี้ (Krisanthi, Sukarsa and Bayupati, 2014)

   0.00-0.50 ระดับวุฒิภาวะ เท่ากับ 0 คือ ไม่มี

   0.51-1.50 ระดับวุฒิภาวะ เท่ากับ 1 คือ ทำเป็นครั้งคราว

   1.51-2.50 ระดับวุฒิภาวะ เท่ากับ 2 คือ มีการทำซ้ำ

   2.51-3.50 ระดับวุฒิภาวะ เท่ากับ 3 คือ มีการกำหนดกระบวนการ

   3.51-4.50 ระดับวุฒิภาวะ เท่ากับ 4 คือ มีการจัดการและวัดผลได้

   4.51-5.00 ระดับวุฒิภาวะ เท่ากับ 5 คือ มีการปฏิบัติที่ดีที่สุด

4. ผลการศึกษา

ผลการศึกษาพบว่าระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศตามกรอบวิธีปฏิบัติ COBIT ในโดเมนการจัดวางแนวทาง การจัดทำแผน และการจัดระบบ (Align, Plan and Organize หรือ APO) พบว่าระดับวุฒิสูงสุดอยู่ในระดับที่ 3 (หรือมีการกำหนดกระบวนการ) จากระดับวุฒิภาวะที่ 5 ซึ่งเป็นระดับวุฒิภาวะที่สูงที่สุด (หรือมีการปฏิบัติที่ดีที่สุด) ได้แก่ กลุ่มธุรกิจการเงิน กลุ่มสินค้าอุตสาหกรรม กลุ่มเทคโนโลยี กลุ่มทรัพยากร กลุ่มบริการ กลุ่มสินค้าอุปโภคบริโภค และ อุตสาหกรรมอื่นๆที่ไม่จัดอยู่ในกลุ่มอุตสาหกรรมใด และพบว่าระดับวุฒิภาวะต่ำสุดอยู่ในระดับวุฒิภาวะที่ 2 (หรือมีการทำซ้ำ) จากระดับวุฒิภาวะที่ 5 ซึ่งเป็นระดับวุฒิภาวะที่สูงที่สุด (หรือมีการปฏิบัติที่ดีที่สุด) ได้แก่ กลุ่มอสังหาริมทรัพย์และก่อสร้าง และกลุ่มเกษตรและอุตสาหกรรมอาหาร ส่วนผลของการสำรวจระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศ ตามกระบวนการจำนวน 13 กระบวนการของโดเมนการจัดวางแนวทาง การจัดทำแผน และการจัดระบบ (Align, Plan and Organize หรือ APO) พบว่าระดับวุฒิภาวะสูงสุดอยู่ในระดับวุฒิภาวะที่ 3 (หรือมีการกำหนดกระบวนการ) จากระดับวุฒิภาวะที่ 5 ซึ่งเป็นระดับวุฒิภาวะที่สูงที่สุด (หรือมีการปฏิบัติที่ดีที่สุด) ได้แก่ ด้านการจัดการความปลอดภัย ด้านกรอบการจัดการงานเทคโนโลยีสารสนเทศ ด้านการจัดการงบประมาณและค่าใช้จ่าย ด้านการจัดการความเสี่ยง ด้านการจัดการทรัพยากรมนุษย์ ด้านการจัดการคุณภาพ ด้านการจัดการกลยุทธ์ ด้านการจัดการสัญญาบริการ ด้านการจัดการผู้จัดจำหน่าย ด้านการจัดการความสัมพันธ์ ด้านการจัดการผลงาน ด้านการจัดการนวัตกรรม และที่อยู่ในระดับวุฒิภาวะต่ำสุดอยู่ระดับวุฒิภาวะที่ 2 (หรือมีการทำซ้ำ) จากระดับวุฒิภาวะที่ 5 ซึ่งเป็นระดับวุฒิภาวะที่สูงที่สุด (หรือมีการปฏิบัติที่ดีที่สุด) ได้แก่ ด้านการจัดการสถาปัตยกรรมองค์กร

ส่วนผลการสำรวจแรงผลักดัน พบว่าแรงผลักดันในการกำกับดูแลเทคโนโลยีสารสนเทศองค์กร จากมากไปน้อย ตามลำดับ ได้แก่ เพื่อปรับปรุงประสิทธิภาพการทำงาน เพื่อลดความเสี่ยง เพื่อปฏิบัติตามกฎระเบียบและกฎหมาย เพื่อสร้างชื่อเสียงและความไว้วางใจให้กับองค์กร เพื่อลดค่าใช้จ่าย เพื่อบรรลุพันธกิจและเป้าหมาย และเพื่อเพิ่มสภาพแวดล้อมการแข่งขัน และผลการสำรวจอุปสรรค พบว่าอุปสรรคในการกำกับดูแลเทคโนโลยีสารสนเทศองค์กร จากมากไปน้อย ตามลำดับ ได้แก่ ข้อจำกัดด้านงบประมาณ การจัดการองค์ความรู้

ความสามารถหรือทักษะของพนักงานไม่เพียงพอ ความยากของวิธีการ ยังไม่ได้จัดอยู่ในลำดับที่ความสำคัญที่จะจัดสรรทรัพยากร ไม่สามารถหาผู้รับผิดชอบในการควบคุม และอุปสรรคอื่นๆ

5. อภิปรายและสรุปผลการสำรวจ

การสำรวจนี้มีวัตถุประสงค์เพื่อศึกษาระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศขององค์กรภายใต้ตลาดหลักทรัพย์ประเทศไทย รวมถึงศึกษาแรงผลักดัน อุปสรรคในการกำกับดูแลเทคโนโลยีสารสนเทศ จากแนวทางของ ISACA (ISACA, 2012) ซึ่งอธิบายโดเมน APO ใน COBIT 5 ว่าเป็นกระบวนการที่จำเป็นเพื่อการวางแผนและการจัดการอย่างเป็นระบบที่มีประสิทธิผลสำหรับทรัพยากรด้านไอทีทั้งภายใน และภายนอก ซึ่งรวมถึงการวางแผนกลยุทธ์ การวางแผนด้านเทคโนโลยี และสถาปัตยกรรม การวางแผนองค์กร การวางแผนนวัตกรรม การบริหารกลุ่มของชุดโครงการ การบริหารเงินลงทุน การบริหารความเสี่ยง การบริหารความสัมพันธ์ และการบริหารคุณภาพ ซึ่งมีการอธิบายถึงความสอดคล้องกันระหว่างเป้าหมายทางธุรกิจและเป้าหมายด้านไอทีที่แสดงให้เห็นถึงการสนับสนุนวัตถุประสงค์ด้านกลยุทธ์สำหรับกระบวนการที่เกี่ยวข้องกับไอที ซึ่งการกำกับดูแลเทคโนโลยีสารสนเทศองค์กรเป็นสิ่งที่สำคัญยิ่ง ไม่ว่าจะเป็นองค์กรขนาดเล็ก ขนาดกลางหรือขนาดใหญ่ก็ตามต่างก็ให้ความสำคัญ โดยการสำรวจนี้ได้ศึกษาระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศสำหรับองค์กรที่อยู่ภายใต้ตลาดหลักทรัพย์แห่งประเทศไทย โดยใช้วิธีการสำรวจขั้นต้นจากบุคลากรระดับผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศที่ปฏิบัติงานหรือเกี่ยวข้องกับหน่วยงานทางด้านเทคโนโลยีสารสนเทศของแต่ละองค์กร ในการสำรวจนี้ผู้วิจัยได้พัฒนาและจัดส่งแบบสอบถามไปยังองค์กรที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย (SET) และตลาดหลักทรัพย์ เอ็ม เอ ไอ (MAI) จำนวน 676 องค์กร ซึ่งจำแนกตาม 9 กลุ่มอุตสาหกรรม ได้แก่ กลุ่มบริการ จำนวน 125 องค์กร กลุ่มสินค้าอุตสาหกรรม จำนวน 113 องค์กร กลุ่มอสังหาริมทรัพย์และก่อสร้าง จำนวน 161 องค์กร กลุ่มธุรกิจการเงิน จำนวน 65 องค์กร กลุ่มเทคโนโลยี จำนวน 48 องค์กร กลุ่มเกษตรอุตสาหกรรมอาหาร จำนวน 55 องค์กร กลุ่มสินค้าอุปโภคบริโภค จำนวน 49 องค์กร กลุ่มทรัพยากร จำนวน 46 องค์กร และองค์กรที่ไม่จัดอยู่ในกลุ่มอุตสาหกรรมใดๆ จำนวน 14 องค์กร โดยได้รับการตอบกลับจำนวน 408 องค์กร ซึ่งคิดเป็นร้อยละ 60.36

จากผลจากการสำรวจพบว่าระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศขององค์กรภายใต้ตลาดหลักทรัพย์ประเทศไทย (SET) และตลาดหลักทรัพย์ เอ็ม เอ ไอ (MAI) ตามกรอบวิธีปฏิบัติ COBIT 5 ในโดเมนการจัดวางแนวทางการจัดทำแผน และการจัดระบบ (Align, Plan and Organize หรือ APO) และ ผลการสำรวจระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศ ตามกระบวนการจำนวน 13 กระบวนการ พบว่าอยู่ในระดับวุฒิภาวะที่ 3 ความหมายคือ องค์กรมีการกำหนดแนวทางเพื่อพัฒนาเทคโนโลยีสารสนเทศ ขั้นตอนการปฏิบัติงานที่ครอบคลุมกิจการกำกับดูแลหลักๆ ประกอบด้วย การกำหนดเป้าหมายปกติ สอบทานผลการปฏิบัติงาน ประเมินความสามารถกับแผนงาน สนับสนุนเงินทุนเพื่อปรับปรุงเทคโนโลยีสารสนเทศที่จำเป็น และผลจากการสำรวจแรงผลักดันของการกำกับดูแลเทคโนโลยีสารสนเทศ ได้แก่ เพื่อปรับปรุงประสิทธิภาพการทำงาน เพื่อลดความเสี่ยง เพื่อปฏิบัติตามกฎระเบียบและกฎหมาย เพื่อสร้างชื่อเสียงและความไว้วางใจให้กับองค์กร เพื่อลดค่าใช้จ่าย เพื่อบรรลุพันธกิจและเป้าหมาย และเพื่อเพิ่มสภาพแวดล้อมการแข่งขันตามลำดับ และผลจากการสำรวจอุปสรรคของการกำกับดูแลเทคโนโลยีสารสนเทศ ได้แก่ ข้อจำกัดด้านงบประมาณ การจัดการองค์ความรู้ ความสามารถหรือทักษะของพนักงานไม่เพียงพอ ความยากของวิธีการ และเนื่องจากยังไม่ได้จัดอยู่ในลำดับที่ความสำคัญที่จะจัดสรรทรัพยากร รวมถึงไม่สามารถหาผู้รับผิดชอบในการควบคุม และอุปสรรคอื่นๆ ตามลำดับ

เมื่อองค์กรทราบระดับวุฒิภาวะในโดเมนการจัดวางแนวทาง การจัดทำแผน และการจัดระบบ (Align, Plan and Organize หรือ APO) และระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศ ตามกระบวนการจำนวน 13 กระบวนการ

แล้ว ทำให้ทราบว่าปัจจุบันระดับวุฒิภาวะของกลุ่มอุตสาหกรรมนั้นอยู่ในระดับใด และสามารถที่จะวางเป้าหมายได้ว่าต้องการจะพัฒนาปรับปรุงระดับวุฒิภาวะให้ถึงระดับใด ร่วมถึงเมื่อองค์กรทราบถึงแรงผลักดันในการกำกับดูแลเทคโนโลยีสารสนเทศ จะทำให้องค์กรทราบได้ว่าองค์กรอาจยังประสบปัญหาด้านต่างๆ จึงควรนำมาตรฐานและกรอบแนวคิดต่างๆ มาใช้ในการกำกับดูแลเทคโนโลยีสารสนเทศ และเมื่อทราบถึงอุปสรรคของการกำกับดูแลเทคโนโลยีสารสนเทศ ทำให้องค์กรสามารถระบุอุปสรรคและหาทางในการขจัดอุปสรรคให้หมดไป เพื่อให้องค์กรเกิดการกำกับดูแลเทคโนโลยีสารสนเทศที่ดี และประโยชน์ที่ได้จากผลการสำรวจครั้งนี้ทำให้องค์กรสามารถประเมินระดับวุฒิภาวะขององค์กรในปัจจุบัน เพื่อเปรียบเทียบกับระดับวุฒิภาวะของกลุ่มอุตสาหกรรมของตนเอง โดยโมเดลวุฒิภาวะตามกรอบวิธีปฏิบัติ COBIT (COBIT Maturity model) คือ เครื่องมือกำกับดูแลด้านเทคโนโลยีสารสนเทศ (IT Governance)ที่นำมาใช้ในการวัดว่ากระบวนการบริหารจัดการมีการพัฒนาดีอย่างไร เมื่อคำนึงถึงการควบคุมภายในเป็นหลัก โมเดลวุฒิภาวะ (Maturity model) ช่วยให้องค์กรประเมินตนเองจาก ไม่มี (Nonexistent หรือ 0) ไปจนถึง มีการปฏิบัติที่ดีที่สุด (Optimized หรือ 5) ผู้ตรวจสอบหรือผู้ที่เกี่ยวข้องสามารถใช้เครื่องมือนี้ช่วยผู้บริหารในการทำหน้าที่กำกับดูแลด้านเทคโนโลยีสารสนเทศ เช่น ทำให้สามารถบรรลุหน้าที่งานเทคโนโลยีได้อย่างมีประสิทธิผลเหมือนงานอื่นๆของธุรกิจ

การสำรวจครั้งนี้มีข้อจำกัด เนื่องจากงานวิจัยนี้เป็นเพียงการสำรวจเบื้องต้น โดยมุ่งหมายหลักเพื่อศึกษาระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศองค์กรที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย (SET) และตลาดหลักทรัพย์ เอ็ม เอ ไอ (MAI) ซึ่งอาจจะไม่ครอบคลุมทุกองค์กรในประเทศไทย โดยผลที่ได้เป็นเพียงการวัดระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศตามกรอบวิธีปฏิบัติ COBIT 5 ในโดเมนการจัดวางแนวทาง การจัดทำแผน และการจัดระบบ (Align, Plan and Organize หรือ APO) เท่านั้น เพราะในแต่ละโดเมนมีหลายกระบวนการ จึงไม่สามารถทำการสำรวจได้ครอบคลุมทุกโดเมนในกรอบวิธีปฏิบัติ COBIT 5

เนื่องจากการสำรวจระดับวุฒิภาวะในการกำกับดูแลเทคโนโลยีสารสนเทศองค์กรนี้ ใช้เพียง 1 โดเมนของกรอบวิธีปฏิบัติ COBIT 5 เท่านั้น คือ โดเมนด้านการจัดวางแนวทาง การจัดทำแผน และการจัดระบบ (APO: Align, Planning and Organize) ซึ่งตามกรอบวิธีปฏิบัติ COBIT 5 ยังมีอีกหลายโดเมนที่ยังไม่ได้นำมาประเมินระดับวุฒิภาวะ ดังนั้นเพื่อเพิ่มประสิทธิภาพในการกำกับดูแลเทคโนโลยีสารสนเทศ งานวิจัยในอนาคต จึงควรนำโดเมนที่เหลือ เช่น โดเมนการจัดสร้าง การจัดหา และการนำไปใช้ (BAI: Build, Acquire and Implement) โดเมนการส่งมอบ การให้บริการ และการสนับสนุน (DSS: Deliver, Service and Support) โดเมนการเฝ้าติดตาม การวัดผล และการประเมิน (MEA: Monitor, Evaluate and Assess) และโดเมนการประเมิน การสั่งการ และการเฝ้าติดตาม (EDM: Evaluate, Direct and Monitor) มาใช้เป็นแนวทางในการประเมินระดับวุฒิภาวะต่อไป อีกทั้งงานวิจัยในอนาคตอาจศึกษาผลกระทบของการใช้กรอบวิธีปฏิบัติ COBIT 5 หรือวิจัยในเรื่องของตัวแบบการพยากรณ์ธรรมาภิบาลด้านไอที (Prediction) ยกตัวอย่างเช่น การตัดสินใจที่จะนำกรอบแนวคิดหรือมาตรฐานต่างๆ มาใช้สำหรับองค์กรของตนเอง หากสามารถพยากรณ์ล่วงหน้าได้ว่าถ้าปฏิบัติตามแล้ว จะมีขีดความสามารถของธรรมาภิบาลด้านไอที (IT Governance Performance) เพิ่มขึ้นในระดับใด จะทำให้เกิดประโยชน์แก่องค์กรอย่างมาก ทั้งในแง่ของค่าใช้จ่ายในการทดลองปฏิบัติตามกรอบแนวคิดต่างๆ และระยะเวลาในการปฏิบัติ ซึ่งจะต้องใช้เวลากว่าจะเห็นผลที่เกิดขึ้นจริง หากสามารถพยากรณ์ได้ก็จะสามารถช่วยให้ผู้บริหารตัดสินใจได้อย่างมีประสิทธิภาพมากยิ่งขึ้น (กัลยา ใจรักษ์ และ ประสงค์ ปราณีตพลกรัง, 2557)

บรรณานุกรม

กัลยา ใจรักษ์ และ ประสงค์ ประณีตพลกรัง. (2557). IT Governance: A Tutorial ธรรมาภิบาลด้านไอที. ดึงข้อมูลวันที่ 1 มิถุนายน 2558, จาก http://www.spu.ac.th/graduate/ files/2011/03/IT-Governance-Tutorial_kallaya.pdf.

เขมขนิษฐ์ แสนยะนันท์ธนะ. (2555). การใช้กรอบวิธีปฏิบัติ COBIT บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศระดับอุดมศึกษา. *เทคโนโลยีสารสนเทศ* , 1, 69-76.

นงลักษณ์ กอศรีลบุตร. (2549). การนำกรอบวิธีปฏิบัติ COBIT มาประยุกต์ใช้ในองค์กร เพื่อปรับปรุงกระบวนการตรวจสอบระบบสารสนเทศ: กรณีศึกษาผู้ประกอบธุรกิจทางการเงินที่ไม่ใช่สถานบันการเงิน (Non-bank) แห่งหนึ่ง, มหาวิทยาลัยธรรมศาสตร์.

นิตยา วงศ์ภินันท์วัฒนา. (2555). *การควบคุมและตรวจสอบระบบสารสนเทศ.* กทม: บริษัท จามจุรีโปรดักส์ จำกัด.

ปริญญา หอมเอนก. (2553). การกำกับดูแลด้านเทคโนโลยีสารสนเทศเพื่อความเหนือชั้นทางธุรกิจ และแนวทางในการนำกรอบการกำกับดูแลด้านเทคโนโลยีสารสนเทศมาประยุกต์ใช้*สตท*., 58.

วรัญญา สุมทุมทิพย์. (2556). สำรวจปัจจัยที่เกิดความเสี่ยงของภัยคุกคามความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร, มหาวิทยาลัยธรรมศาสตร์.

สันติพัฒน์ อรุณธารี. (2551). การศึกษาการกำกับดูแลกิจการที่ดีทางด้านเทคโนโลยีสารสนเทศ (IT Governance) กับการวางแผนกลยุทธ์, มหาวิทยาลยหอการค้าไทย.

Abu-Musa, A. A. (2010). Exploring COBIT processes for ITG in Saudi organizations: an empirical study. *The International journal of digital accounting research*, *9*, 7.

Omari, L. A., Barnes, P. H., and Pitman, G. (2012). Optimising COBIT 5 for IT governance: examples from the public sector. In *Proceedings of the ATISR 2012: 2nd International Conference on Applied and Theoretical Information.*

COBIT 5 Online Collaborative Environment. (n.d). Retrieved December1, 2014, from https://www.google.co.th/?gws_rd=cr,ssl&ei=XqmfVMXyCo6eugSgw4CQCQ#q=COBIT5_Glenfis-Laminate_ v1.3.

Haes, S. D., and Grembergen, W. V. (2009). An exploratory study into IT governance implementations and its impact on business/IT alignment. *Information Systems Management*, *26*(2), 123-137.

Ferguson, A. (1981). *Statistical Analysis in Psychology and Education*. 5th ed. Tokyam Mc Graw-Hill Book Company.

Frank, S. (2011). IT Organization Assessment—Using COBIT and BSC. Retrieved November 12, 2014, from http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Documents/COBIT-Focus-Vol-1-2011.pdf.

Guldentops, E., Grembergen, W. V., and Haes, S. D. (2002). Control and governance maturity survey: establishing a reference benchmark and a self-assessment tool. *Information Systems Control Journal*, *6*, 12-32.

ISACA, (2007). Framework Control Objectives Management Guidelines Maturity Models. Retrieved March 15, 2015, from www.uninett.no/webfm_send/729.

ISACA, (2012). COBIT 5 กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร. ดึงข้อมูลวันที่ 1 กันยายน 2557, จาก www. http://www.isaca.org/.

Kerr, D. S., and Murthy, U. S. (2007). The Importance of the COBIT Framework IT Processes For Effective Internal Control over the Reliability of Financial Reporting: An International Survey. University of Waterloo.

Krisanth, G., Sukarsa, I., and Bayupati I. (2014). Governance Audit Of Application Procurement Using Cobit Framework. *Journal of Theoretical and Applied Information Technology*, 59(2).

Liu, Q., and Ridley, G. (2005, May). IT Control in the Australian public sector: an international comparison. In *Proceedings of the 13th European Conference of Information Systems*.

Malakooti, M. V., Hashemi, S. M., and Tavakoli, N. (2014). An Effective Solution for the Service Support of Virtual Banking Using the Key Performance Indices Based on COBIT-5 Architecture. In *The International Conference on Computing Technology and Information Management (ICCTIM2014)*, 424-430.

Pasquini, A., and Galiè, E. (2013). COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process : *Proceedings of FIKUSZ '13 Symposium for Young Researchers*, 67-76.

Pederiva, A. (2003). The COBIT® maturity model in a vendor evaluation case. *Information Systems Control Journal*, *3*, 26-29.

Tanuwijaya, H., and Sarno, R. (2010). Comparation of COBIT Maturity Model and Structural Equation Model for Measuring the Alignment between University Academic Regulations and Information Technology Goals. *IJCSNS*, *10*(6), 80.

Tugas, F. C. (2009). Assessing the Level of Information Technolgy (IT) Processes Performance and Capability Maturity in the Philippine Food, Beverage and Tobacco (fbt) Industry Using the COBIT Framework. *Academy of Information and Management Sciences*, *13*(2), 68.

Ursacescu, M. (2014). Assessing The Maturity Level Of Information Technology Management Process In A Romanian Company. *International Journal of Management & Information Systems (IJMIS)*, *18*(3), 201-212.

Volchkov, A. (2013). How to Measure Security from a Governance Perspective. *ISACA JOURNAL.,* 5, 1-8.

อิทธิพลของทัศนคติด้านความเป็นส่วนตัวของประชาชนต่อข้อมูลส่วนบุคคลบนกูเกิลสตรีทวิวที่มีต่อความตั้งใจเชิงพฤติกรรม

ชัยพร ธนันทา*

บริษัท ฟาบริเนท จำกัด

***Correspondence:** tum_ghost@hotmail.com doi: 10.14456/jisb.2016.10

บทคัดย่อ

งานวิจัยฉบับนี้เป็นงานวิจัยที่มีวัตถุประสงค์เพื่อประเมินทัศนคติด้านความกังวลในเรื่องความเป็นส่วนตัวของประชาชนต่อข้อมูลส่วนบุคคลบนกูเกิลสตรีทวิวที่มีต่อความตั้งใจเชิงพฤติกรรม โดยอ้างอิงตามตัววัดทัศนคติด้านความเป็นส่วนตัวของผู้ใช้งานอินเทอร์เน็ต (IUIPC) ซึ่งมุ่งเน้นการวัดความกังวลในความเป็นส่วนตัวต่อข้อมูลส่วนบุคคล 3 ด้าน คือ ความกังวลด้านการจัดเก็บข้อมูล ความกังวลด้านการควบคุมข้อมูล ความกังวลด้านการรับรู้การนำข้อมูลไปใช้ และทฤษฎีความกังวลในนโยบายความปลอดภัยด้านความเป็นส่วนตัวออนไลน์ ที่มีผลต่อความเชื่อในความเสี่ยง และนำไปสู่ความตั้งใจเชิงพฤติกรรม โดยการวิจัยนี้เป็นงานวิจัยเชิงปริมาณที่ใช้แบบสอบถามแบบเอกสารเป็นเครื่องมือในการรวบรวมข้อมูลด้วยการลงพื้นที่สุ่มกลุ่มตัวอย่างที่เคยใช้งานระบบกูเกิลสตรีทวิวบริเวณสถานีรถไฟฟ้ามหานครบางหว้า – สถานีสยาม จำนวน 200 ตัวอย่าง ซึ่งผู้วิจัยได้ตรวจสอบแบบสอบถามโดยการวิเคราะห์องค์ประกอบ (Factor Analysis) และตรวจสอบความเที่ยงของเครื่องมือ (Reliability Analysis) โดยใช้วิธีหาค่าสัมประสิทธิ์แอลฟาครอนบาช (Cronbach's Alpha) และทดสอบสมมติฐานตามแบบจำลองโดยใช้การวิเคราะห์การถดถอยเชิงพหุคูณ (Multiple Regression Analysis)

ผลการวิจัยสรุปได้ว่า ความกังวลต่อการควบคุมข้อมูลมีผลต่อความเชื่อในความเสี่ยงมากที่สุด รองลงมาคือความกังวลต่อการรับรู้การนำข้อมูลไปใช้มีผลต่อความเชื่อในความเสี่ยง ความกังวลด้านนโยบายความปลอดภัยด้านความเป็นส่วนตัวออนไลน์มีผลต่อความเชื่อในความเสี่ยง ความเชื่อในความเสี่ยงมีผลต่อความตั้งใจเชิงพฤติกรรม และความกังวลด้านการจัดเก็บข้อมูลมีผลต่อความเชื่อในความเสี่ยงตามลำดับ เมื่อพิจารณาถึงความตั้งใจเชิงพฤติกรรม พบว่าประชาชนมีความตั้งใจที่จะรายงานปัญหาเกี่ยวกับข้อมูลที่ถูกละเมิดความเป็นส่วนตัวต่อระบบกูเกิลสตรีทวิวมากที่สุด รองลงมาคือรายงานปัญหาเกี่ยวกับข้อมูลที่ละเมิดความเป็นส่วนตัวต่อหน่วยงานภาครัฐ การไม่ใช้บริการกูเกิลสตรีทวิวอีกเมื่อพบการละเมิดความเป็นส่วนตัวบนกูเกิลสตรีทวิว ยินดีที่จะเปลี่ยนไปใช้บริการสตรีทวิวรายอื่นหากมีผู้ให้บริการที่สามารถดูแลข้อมูลส่วนบุคคลได้ดีกว่ากูเกิลสตรีทวิว และการบอกต่อผู้อื่นให้ทราบเรื่องการละเมิดความเป็นส่วนตัวของกูเกิลสตรีทวิว ตามลำดับ ผลของการวิจัยนี้จะเป็นแนวทางในการกำหนดนโยบายควบคุมดูแลข้อมูลส่วนบุคคลให้ทั้งหน่วยงานภาครัฐและเอกชน อีกทั้งยังทำให้ประชาชนเกิดความตระหนักถึงความเป็นส่วนตัวต่อข้อมูลส่วนบุคคลบนระบบสารสนเทศภูมิศาสตร์ รวมไปถึงการนำเรื่องการคุ้มครองสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลไปพิจารณาบรรจุลงในตัวบทบัญญัติแห่งประมวลกฎหมาย

คำสำคัญ: กูเกิลสตรีทวิว ความกังวลด้านความเป็นส่วนตัว ข้อมูลส่วนบุคคล

Impact of People's Privacy Concerns on Behavioral Intention in Google Street View

Chaiyaporn Tananta*

Fabrinet Co., Ltd.

***Correspondence:** tum_ghost@hotmail.com doi: 10.14456/jisb.2016.10

Abstract

This study investigates the impact of popular privacy concerns on the behavioral intention of Google Street View. The survey instruments include the Internet Users' Information Privacy Concerns (IUIPC) theory which focuses on measuring 3 aspects of privacy practices (collection, control, and awareness) and online policy concern theory that influences risk belief and leads to behavioral intention. A questionnaire was used for collecting data from 200 samples in Bangkok Mass Transit System around Bangwa and Siam station areas, with only samples indicating use of Google Street View counted. Using the technique of descriptive statistics, the data collected were analyzed in terms of validity and reliability to confirm components of factor analysis and Cronbach's alpha at upper 0.07. The researcher also used the linear regression and multiple regression analysis for hypothesis testing at the statistically significant level of 0.05.

The results of validity and reliability are acceptable and the independent variable analysis by multiple regressions has shown that the control is the factor most related to risk belief, with awareness of privacy practices the second, policies of online concern the third, and behavioral intention and collection is the fourth. According to the results of this study, citizens show the greatest intention to report violations of privacy to Google Street View report system, secondly to report to a government agency and thirdly to quit the Google Street View service. Finally, they tell others about violations of privacy on Google Street View and switch to another Street View service provider if that provider can safeguard personal information better than Google Street View. For the utilization of this research, first it can be used as a guideline for drafting personal data policy for government agencies and private company. It also provides the public with greater awareness of privacy concerns regarding personal data in Geographic information systems. Finally, this research can be used to adapt or revise the provisions of privacy law.

Keywords: Google Street View, Privacy Concern, Personal Information

1. บทนำ

กูเกิลสตรีทวิวเป็นเทคโนโลยีที่โดดเด่นใน Google Maps และ Google Earth ที่ให้ทัศนียภาพอันงดงามจากตำแหน่งที่กำหนดไปตามถนนหลายแห่งในโลก โดยเปิดตัวครั้งแรกในวันที่ 25 พฤษภาคม 2550 ในประเทศสหรัฐอเมริกาและได้ขยายรวมไปถึงเมืองและชนบททั่วโลก โดยกูเกิลสตรีทวิวคือบริการหนึ่งของ Google ที่นำเสนอภาพตามท้องถนน สถานที่สำคัญต่างๆ ของแต่ละประเทศ ให้ความเสมือนจริงด้วยมุม 360 องศาในแนวนอน และมุม 290 องศาในแนวตั้งสามารถคลิกไปยังพื้นที่ต่างๆ ในรูปภาพที่แสดงเพื่อย้ายมุมมองไปยังจุดดังกล่าวทำให้เหมือนเรากำลังขับรถอยู่บนถนน กูเกิลสตรีทวิวได้เปิดให้ใช้บริการในประเทศไทยอย่างเป็นทางการในวันที่ 23 มีนาคม 2555

กูเกิลสตรีทวิวจึงเป็นนวัตกรรมและเทคโนโลยีที่เพิ่มโอกาสใหม่ๆ มากมายให้แก่มนุษยชาติแต่ในขณะเดียวก็ยังมีแนวโน้มที่จะกลายเป็นปัญหาและภัยคุกคามใหม่ๆ ต่อประชาชนอย่างหลีกเลี่ยงไม่ได้ เนื่องจากกูเกิลสตรีทวิวเป็นระบบข้อมูลเชิงพื้นที่และการบริการที่ได้จัดเก็บข้อมูลไปเป็นจำนวนมหาศาล ทำให้ปัจจุบันไม่ว่าจะเป็นรัฐบาล ธุรกิจเอกชน หรือประชาชนทั่วไปสามารถเข้าถึงเนื้อหามัลติมีเดียบนอินเทอร์เน็ตนี้ได้เพิ่มขึ้นและลึกมากขึ้นกว่าในอดีต และด้วยเหตุนี้ความกังวลในด้านความเป็นส่วนตัวภายในโลกดิจิตอลจึงได้ถูกหยิบยกขึ้นมาเป็นประเด็นสำคัญในระดับเวทีโลก ดังนั้นเพื่อเป็นการขยายความรู้ของงานวิจัยในอดีตให้มีความหลากหลายและครบถ้วนมากยิ่งขึ้น ในงานวิจัยนี้จะมุ่งเน้นศึกษาทัศนคติในความเป็นส่วนตัวของประชาชน ต่อข้อมูลส่วนบุคคลบนกูเกิลสตรีทวิวที่มีต่อความตั้งใจเชิงพฤติกรรม ซึ่งจะใช้วิธีการวัดผลจากความคิดเห็นต่อเรื่องการรักษาความเป็นส่วนตัว

2. ทฤษฎี แนวคิด และงานวิจัยที่เกี่ยวข้อง

งานวิจัยนี้ได้นำทฤษฎีทฤษฎีความกังวลต่อความเป็นส่วนตัวของผู้ใช้งานอินเทอร์เน็ตและ ทฤษฎีความกังวลต่อนโยบายความเป็นส่วนตัวออนไลน์ เมื่อนำมาใช้ในการวิจัยด้านความตั้งใจเชิงพฤติกรรมของประชาชนต่อกูเกิลสตรีทวิว ทำให้ทราบความสัมพันธ์ของตัวแปรด้านความกังวลต่อการจัดเก็บข้อมูล การควบคุมข้อมูล การรับรู้การนำข้อมูลไปใช้ และความกังวลต่อนโยบายความปลอดภัยด้านความเป็นส่วนตัวออนไลน์ ที่ส่งผลต่อความเชื่อในความเสี่ยง โดยผู้วิจัยได้ศึกษาปัจจัยที่มีผลต่อความตั้งใจเชิงพฤติกรรม ดังจะกล่าวต่อไป

ตัววัดทัศนคติด้านความเป็นส่วนตัวของผู้ใช้งานอินเทอร์เน็ต หรือ Internet Users' Information Privacy Concerns (IUPC) เป็นตัววัดที่มุ่งเน้นการวัดความกังวลในความเป็นส่วนตัวต่อข้อมูลส่วนบุคคล โดยมีการแบ่งหัวข้อออกเป็น 3 ด้าน ได้แก่ ความกังวลด้านการจัดเก็บข้อมูล, ความกังวลด้านการควบคุม และความกังวลด้านการรับรู้การนำข้อมูลไปใช้ (Malhotra et al., 2004)

ความกังวลต่อนโยบายความปลอดภัยด้านความเป็นส่วนตัวออนไลน์ หมายถึง ความกังวลในด้านที่ไม่เกี่ยวข้องกับข้อมูลโดยตรง เช่น การเข้าถึงทางกายภาพที่บุคคลอื่นสามารถเข้าถึงข้อมูลส่วนบุคคลของคนนั้นได้ และ การปกป้องขอบเขตการแสดงออกของตนเองผ่านทางคำพูดหรือการทำกิจกรรมที่แสดงออกถึงความเป็นตัวตนโดยไม่ได้รับการรบกวนจากบุคคลใดๆ โดยความกังวลชนิดนี้สะท้อนให้เห็นถึงพฤติกรรมที่มีความกังวลต่อความเป็นส่วนตัว (Buchanan et al., 2007) เช่น การเข้าถึงข้อมูลทางกายภาพความเป็นส่วนตัว ซึ่งเป็นระดับการเข้าถึงข้อมูลที่บุคคลใดๆ สามารถเข้าถึงข้อมูลส่วนบุคคลของใครคนหนึ่งได้ (Bolchini et al., 2004) การรักษาความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นไปตามนโยบายที่เผยแพร่บนเว็บไซต์หรือไม่ และ การควบคุมความเป็นส่วนตัวของข้อมูลส่วนบุคคล (Tsai et al., 2010)

ความเชื่อในความเสี่ยง หมายถึง ความคาดหวังอย่างมั่นใจว่าจะสูญเสียข้อมูลที่เกี่ยวข้องกับการเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลอื่น (Dowling and Staelin, 1994) สำหรับงานวิจัยนี้ความเชื่อในความเสี่ยงคือระดับความเชื่อว่าระบบ Google Street View มีความเสี่ยงจากการจัดเก็บ การควบคุมและ การรับรู้ความเป็นส่วนตัวของข้อมูลส่วนบุคคลของประชาชน

ความตั้งใจเชิงพฤติกรรม หมายถึง ความมุ่งมั่นที่จะกระทำการอันใดก็ทำให้จนสำเร็จตามเป้าหมายที่เกิดขึ้นจริง เป็นเรื่องสมควรที่บุคคลจะโต้แย้งและตั้งใจที่จะเปิดเผยข้อมูลส่วนบุคคลด้วยการกลั่นกรองที่ดี หากเป็นการร้องขอหรือนำข้อมูลไปใช้จากบุคคลอื่น (Fishbein and Ajzen 1975; Ajzen 1991)

งานวิจัยนี้ยังได้ศึกษาวรรณกรรมในอดีตที่เกี่ยวข้อง โดยมีปัจจัยดังนี้

ความกังวลด้านการจัดเก็บข้อมูล คือ ระดับความรู้สึกไม่สบายใจในข้อมูลส่วนบุคคลที่ถูกครอบครองหรือบันทึกด้วยบุคคลอื่น (Malhotra et al., 2004) ความกังวลด้านการจัดเก็บข้อมูล ไม่ว่าจะจัดเก็บอย่างถูกหรือผิดกฎหมายล้วนเป็นจุดเริ่มต้นของความกังวลต่อความเป็นส่วนตัวของข้อมูลต่างๆ เป็นระดับความไม่สบายใจต่อระบบหรือบริการที่อาจเก็บข้อมูลที่เจาะจงตัวบุคคลไปใช้เพื่อหาผลประโยชน์ (Culnan and Bies, 2003)

ความกังวลด้านการควบคุม คือ ระดับความรู้สึกของคนที่ไม่สบายใจในด้านการกำกับดูแลและจัดการกับข้อมูลส่วนบุคคล (Malhotra et al., 2004) ประชาชนมักจะไม่มอบความไว้วางใจให้ระบบหรือบริการมากำกับดูแลและจัดการข้อมูลส่วนบุคคลของตน เพราะมีความเสี่ยงต่อการถูกละเมิดหรือนำไปใช้เพื่อหาประโยชน์ นอกเสียจากระบบหรือบริการนั้นสามารถกำกับดูแลข้อมูลส่วนบุคคลโดยตั้งอยู่บนพื้นฐานของข้อกฎหมาย ศีลธรรม และต้องมีการเสนอทางเลือกที่อิสระว่าจะยอมรับหรือปฏิเสธกระบวนการหรือการตัดสินใจ

ความกังวลด้านการรับรู้การนำข้อมูลไปใช้ คือ ระดับความรู้สึกไม่สบายใจเพราะไม่รู้ว่าข้อมูลที่ถูกจัดเก็บไปนั้นจะถูกนำไปใช้ในด้านใด (Malhotra et al., 2004) การรับรู้การนำข้อมูลไปใช้นั้นเป็นตัวบ่งชี้ถึงระดับความกังวลของประชาชนเกี่ยวกับการรับรู้ถึงความเป็นส่วนตัวของข้อมูลในระบบ

ความกังวลต่อนโยบายความปลอดภัยด้านความเป็นส่วนตัวออนไลน์ Jensen and Potts (2004) กล่าวว่า "นโยบายความเป็นส่วนตัวมีอยู่ทุกที่และมักจะมาจากแหล่งข้อมูลเกี่ยวกับข้อปฏิบัติต่อส่วนที่เป็นส่วนตัวของบริษัท" เพื่อตรวจสอบว่านโยบายสามารถตอบสนองความต้องการของผู้ใช้ นโยบายความเป็นส่วนตัวเผยแพร่มากที่สุดอยู่บนเว็บไซต์เพื่อให้ผู้ใช้งานตามสถานที่ต่างๆ ในโลกที่ให้ความสำคัญต่อนโยบายความเป็นส่วนตัวสามารถเข้าถึงได้ ซึ่งจากงานวิจัยของ Bolchini et al. (2004) พบว่านโยบายความเป็นส่วนตัวออนไลน์จำนวนมากขาดความชัดเจนและต้องใช้ทักษะการอ่านทำความเข้าใจระดับที่สูงเมื่อเปรียบเทียบกับระดับความรู้เฉลี่ยของประชากรบนอินเทอร์เน็ต โดยนโยบายความเป็นส่วนตัวออนไลน์มี 4 ด้านหลักๆ คือ เนื้อหา โครงสร้าง ระบบนำร่องเว็บไซต์ และการเข้าถึง

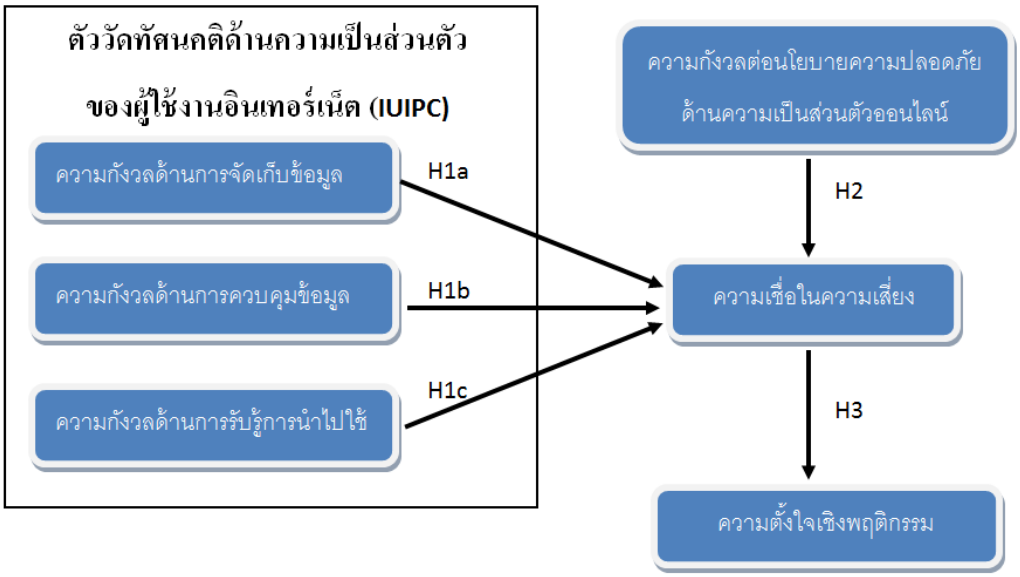
ความเชื่อในความเสี่ยง คือ ระดับที่คนเชื่อมั่นในความเป็นไปได้ในการสูญเสียข้อมูลส่วนบุคคลให้กับบริษัทออนไลน์ (Malhotra et al., 2004) ความเชื่อในความเสี่ยงหมายถึง ความคาดหวังอย่างมั่นใจว่าจะสูญเสียข้อมูลที่เกี่ยวข้องกับการเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลอื่น (Dowling and Staelin, 1994) สำหรับงานวิจัยนี้ความเชื่อในความเสี่ยงคือระดับความเชื่อว่าระบบ Google Street View มีความเสี่ยงจากการจัดเก็บ การควบคุมและ การรับรู้ความเป็นส่วนตัวของข้อมูลส่วนบุคคลของประชาชน

ความตั้งใจเชิงพฤติกรรมเป็นความมุ่งมั่นที่จะกระทำการอันใดก็ทำให้จนสำเร็จตามเป้าหมายที่เกิดขึ้นจริง เป็นเรื่องสมควรที่บุคคลจะโต้แย้งและตั้งใจที่จะเปิดเผยข้อมูลส่วนบุคคลด้วยการกลั่นกรองที่ดี หากเป็นการร้องขอหรือนำข้อมูลไปใช้จากบุคคลอื่น (Fishbein and Ajzen, 1975; Ajzen, 1991) ความตั้งใจเชิงพฤติกรรมด้านความเป็นส่วนตัวจึงเป็นผลมาจากสถานการณ์และบริบทเฉพาะที่ได้วิเคราะห์อย่างถี่ถ้วนแล้วว่าจะตอบสนองให้เกิดประโยชน์ต่อการเผยแพร่ข้อมูลส่วนบุคคลอย่างไร (Xu et al., 2008)

3. กรอบแนวคิดในการวิจัยและสมมติฐานการวิจัย

จากทฤษฎี IUIPC และความกังวลต่อนโยบายความปลอดภัยด้านความเป็นส่วนตัวออนไลน์ แสดงให้เห็นว่า ความกังวลแบ่งออกเป็น 4 ด้าน คือ 1) ความกังวลด้านการจัดเก็บข้อมูล 2) ความกังวลด้านการควบคุมข้อมูล และ 3) ความกังวลด้านการ

รับรู้การนำข้อมูลไปใช้ โดยงานวิจัยนี้ได้เพิ่มปัจจัยที่ 4 คือความกังวลด้านนโยบายความเป็นส่วนตัวออนไลน์ ซึ่งเป็นปัจจัยใหม่ที่ยังไม่เคยนำมากล่าวถึงในทฤษฎีความกังวลต่อความเป็นส่วนตัวของผู้ใช้งานอินเทอร์เน็ตและ ทฤษฎีความกังวลต่อนโยบายความเป็นส่วนตัวที่นำมาเป็นทฤษฎีอ้างอิงในงานวิจัยนี้ ส่งผลต่อความเชื่อในความเสี่ยง ซึ่งส่งผลต่อความตั้งเชิงพฤติกรรมอีกต่อหนึ่ง



ภาพที่ 1 กรอบแนวคิดความตั้งใจเชิงพฤติกรรมต่อความกังวลต่อการให้บริการของกูเกิลสตรีทวิว

ในปัจจุบันความก้าวหน้าในเทคโนโลยีสารสนเทศทางภูมิศาสตร์และวิทยาการคอมพิวเตอร์ ทำให้ปัจจุบันการให้บริการสารสนเทศทางภูมิศาสตร์และการจัดการข้อมูลส่วนบุคคลบนอินเทอร์เน็ตโดยเฉพาะกูเกิลสตรีทวิว สามารถทำได้ง่ายและรวดเร็วมากขึ้นกว่าในอดีต ซึ่งอาจทำให้ประชาชนมีความกังวลเกี่ยวกับการถูกละเมิดความเป็นส่วนตัวได้ เช่น ข้อมูลส่วนบุคคลที่ถูกจัดเก็บและนำไปใช้ทั้งที่รู้ตัวและไม่รู้ตัว และ การนำข้อมูลส่วนบุคคลไปเผยแพร่โดยไม่ได้รับอนุญาต เป็นต้น ซึ่งเป็นปัญหาที่สังคมต้องให้ความสำคัญ (Williams et al., 2009; Xu et al., 2008) จึงอาจมีผลทำให้ประชาชนและผู้ใช้งานระบบกูเกิลสตรีทวิวเกิดความกังวลในด้านการจัดการข้อมูลของผู้ให้บริการได้ ดังนั้นจึงสามารถตั้งสมมติฐานได้ดังนี้

สมมติฐานที่ 1a: การจัดเก็บข้อมูลของกูเกิลสตรีทวิวมีผลกระทบต่อความเชื่อในความเสี่ยง
สมมติฐานที่ 1b: การควบคุมข้อมูลของกูเกิลสตรีทวิวมีผลกระทบต่อความเชื่อในความเสี่ยง
สมมติฐานที่ 1c: การรับรู้เกี่ยวกับการนำข้อมูลส่วนบุคคลไปใช้ของกูเกิลสตรีทวิว มีผลกระทบต่อความเชื่อในความเสี่ยง

นโยบายความปลอดภัยด้านความเป็นส่วนตัวควรประกอบด้วย ข้อมูลที่รวบรวมและเหตุผลที่เก็บรวบรวม วิธีใช้ข้อมูลเหล่านั้น วิธีเข้าถึงและอับเดตข้อมูล ด้วยโครงสร้างและเนื้อหาที่เข้าใจได้ง่าย (Jensen and Potts, 2004) แต่ในปัจจุบันพบว่าบริการออนไลน์จำนวนมากกลับมีโครงสร้าง เนื้อหาของนโยบายความปลอดภัยด้านความเป็นส่วนตัว ที่ไม่เป็นปัจจุบันและขาดความน่าเชื่อถือ ทำให้ประชาชนจึงเกิดความกังวลเกี่ยวกับความเป็นส่วนตัวและระรู้สึกถึงความเสี่ยงของนโยบายความเป็นส่วนตัวว่าผู้ให้บริการได้ละเมิดนำข้อมูลส่วนบุคคลของตนไปเผยแพร่โดยไม่ขออนุญาตหรือไม่ (Tsai et al., 2010; Jensen and Potts, 2004) ดังนั้นจึงสามารถตั้งสมมติฐานได้ดังนี้

สมมติฐานที่ 2: ความกังวลด้านนโยบายความเป็นส่วนตัวออนไลน์ของ Google Street View มีผลกระทบต่อความเชื่อในความเสี่ยง

ปัจจุบันนี้ประชาชนมีการรับรู้ปัญหาการละเมิดความเป็นส่วนตัวด้านข้อมูลส่วนบุคคลมากขึ้น (Fishbein and Ajzen, 1975; Ajzen, 1991) โดยประชาชนที่รับรู้ถึงความเสี่ยงจะปรับเปลี่ยนพฤติกรรมโดยจะไม่ให้ข้อมูลส่วนบุคคลหรือร้องเรียนปัญหากับผู้ให้บริการ เว้นแต่ในบางกรณีที่ประชาชนเต็มใจที่จะเปิดเผยข้อมูลส่วนบุคคลหากได้รับผลประโยชน์หรือการส่งเสริมการสร้างความเชื่อมั่นในการคุ้มครองข้อมูลส่วนบุคคล (Eastlick et al., 2006; Li, Sarathy and Xu, 2010) ดังนั้นจึงสามารถตั้งสมมติฐานได้ดังนี้

สมมติฐานที่ 3: ความเชื่อในความเสี่ยงของ Google Street View มีผลกระทบต่อความตั้งใจของพฤติกรรม

4. วิธีการวิจัย

งานวิจัยนี้จัดเก็บข้อมูลจากประชาชน จำนวน 250 คน โดยใช้แบบสอบถามเป็นเครื่องมือ อนึ่งก่อนการจัดเก็บข้อมูลจากกลุ่มตัวอย่าง งานวิจัยนี้ได้นำแบบสอบถามที่พัฒนามาจากงานวิจัยในอดีต (ประกอบด้วย Grigoroudis, 2009; Malhotra et al., 2004; Oliver, 2010; Smith et al., 1996; Zhang et al., 2012) ไปทดสอบกับกลุ่มตัวอย่างจำนวน 30 คน ผลการทดสอบพบว่าข้อมูลมีการกระจาย ซึ่งผู้วิจัยได้ปรับข้อความในคำถามที่กระจายจากกลุ่มให้เหมาะสม ต่อจากนั้นจึงนำแบบสอบถามที่ปรับแก้ไปจัดเก็บข้อมูลจากกลุ่มตัวอย่างจริง

5. ผลการวิจัย

5.1 การทดสอบข้อตกลงเบื้องต้นทางสถิติ

ข้อมูลที่จัดเก็บจากกลุ่มตัวอย่างถูกนำไปทดสอบข้อมูลขาดหาย (Missing data) และข้อมูลสุดโต่ง (Outliers) นอกจากนี้ยังทดสอบว่าข้อมูลมีการกระจายแบบปกติ (Normal) มีความสัมพันธ์เชิงเส้นตรง (Linearity) มีภาวะร่วมเส้นตรงพหุ (Multicollinearity) และมีภาวะร่วมเส้นตรง (Singularity) หรือไม่ ผลการทดสอบพบว่าข้อมูลไม่มีปัญหาด้านข้อมูลขาดหาย ข้อมูลสุดโต่ง และข้อมูลมีการกระจายเป็นแบบปกติ มีความสัมพันธ์เชิงเส้นตรงและไม่มีปัญหาภาวะร่วมเส้นตรงพหุและภาวะร่วมเส้นตรงดังกล่าว

งานวิจัยนี้ได้ทดสอบความเชื่อถือได้ของแบบสอบถาม โดยใช้การวิเคราะห์ค่าสัมประสิทธิ์อัลฟาของครอนบาชพบว่าทุกตัวแปรมีค่ามากกว่า 0.7 จึงถือว่ามีความเชื่อถือได้สำหรับงานวิจัยแบบ Basic research นอกจากนี้ยังได้ทดสอบความตรงของแบบสอบถาม ด้วยการวิเคราะห์องค์ประกอบ (Factor analysis) โดยใช้เกณฑ์ที่ข้อคำถามที่จับกลุ่มกันเป็นแต่ละตัวแปรต้องมีค่า Factor loading ไม่น้อยกว่า 0.5 ผลการวิเคราะห์องค์ประกอบได้จำนวนตัวแปรทั้งหมด 6 องค์ประกอบ (ตารางที่ 1)

ตารางที่ 1 Factor Analysis ของปัจจัยในงานวิจัย

ปัจจัย	Factor Loading
ปัจจัย 1: ความกังวลเกี่ยวกับความเป็นส่วนตัวด้านการจัดเก็บข้อมูล (48.921% of variance, α = 0.950)	
ท่านรู้สึกกังวลเมื่อกูเกิลสตรีทวิวจัดเก็บข้อมูลส่วนบุคคลของท่านโดยมิได้แจ้งให้ท่านทราบ	0.902
ท่านรู้สึกกังวลเมื่อกูเกิลสตรีทวิวจัดเก็บข้อมูลส่วนบุคคลของท่านมากเกินไป	0.887
ท่านรู้สึกกังวลที่ผู้มีบัญชีกูเกิลสามารถให้ข้อมูลกับกูเกิลสตรีทวิวได้	0.850
ท่านรู้สึกกังวลเมื่อกูเกิลสตรีทวิวจัดเก็บข้อมูลส่วนบุคคลของท่านผ่านระบบเครือข่ายไร้สายที่ไม่ได้เข้ารหัส	0.860
ท่านรู้สึกกังวลเมื่อกูเกิลสตรีทวิวจัดเก็บพิกัดข้อมูลส่วนบุคคลของท่านโดยมิได้แจ้งให้ทราบ	0.851
ปัจจัย 2: ความกังวลเกี่ยวกับความเป็นส่วนตัวด้านการควบคุมข้อมูล (5.851% of variance, α = 0.883)	
ท่านรู้สึกกังวลเมื่อสูญเสียการควบคุมข้อมูลส่วนบุคคลของตนเอง	0.751
ท่านรู้สึกกังวลต่อเทคโนโลยีการเบลอภาพใบหน้าและป้ายทะเบียนของ กูเกิลสตรีทวิวที่ไม่สามารถเบลอภาพที่จัดเก็บได้ทั้งหมด	0.831
ท่านรู้สึกกังวลต่อการรายงานปัญหาจากผู้ใช้บริการกูเกิลสตรีทวิวที่ได้รับการดำเนินการช้าหรือไม่ได้รับการดำเนินการ	0.742
เจ้าของข้อมูลส่วนบุคคลต้องมีสิทธิ์ในการตัดสินใจวิธีที่จะถูกจัดเก็บข้อมูล นำข้อมูลไปใช้ และการนำข้อมูลไปแชร์สู่สาธารณะ	0.711
ท่านรู้สึกว่าการควบคุมข้อมูลส่วนบุคคลของตนเป็นสิ่งสำคัญในการให้บริการข้อมูลของกูเกิลสตรีทวิว	0.510
ปัจจัย 3: ความกังวลเกี่ยวกับความเป็นส่วนตัวด้านการรับรู้เกี่ยวกับการนำข้อมูลไปใช้ (4.248% of variance, α = 0.847)	
ท่านรู้สึกกังวลเมื่อกูเกิลสตรีทวิวไม่แจ้งให้ท่านทราบว่ามีการนำข้อมูลส่วนบุคคลของท่านไปเผยแพร่	0.631
ท่านรู้สึกกังวลเมื่อกูเกิลสตรีทวิวนำข้อมูลส่วนบุคคลของท่านไปเผยแพร่มากเกินไป	0.780
ท่านรู้สึกกังวลว่ากูเกิลสตรีทวิวจะนำข้อมูลส่วนบุคคลของท่านไปใช้เพื่อแสวงหาผลประโยชน์อื่นนอกเหนือจากภาพสตรีทวิว	0.784
กูเกิลสตรีทวิวควรชี้แจงให้ผู้ถูกจัดเก็บข้อมูลส่วนบุคคลทราบว่า จัดเก็บข้อมูลอะไรไปบ้าง ข้อมูลจะถูกประมวลผลและถูกนำไปใช้อย่างไร	0.711
ท่านตระหนักในกระบวนการจัดเก็บข้อมูลและวิธีที่ข้อมูลส่วนบุคคลของท่านถูกนำไปใช้	0.767

ตารางที่ 1 Factor Analysis ของปัจจัยในงานวิจัย (ต่อ)

ปัจจัย	Factor Loading
ปัจจัย 4: ความกังวลต่อนโยบายความปลอดภัยด้านความเป็นส่วนตัวออนไลน์ (11.026% of variance, α = 0.962)	
ท่านรู้สึกกังวลที่กูเกิลสตรีทวิวไม่มีการกำหนดนโยบายการรักษาความปลอดภัยด้านความเป็นส่วนตัว	0.649
กูเกิลสตรีทวิวควรมีนโยบายการรักษาความปลอดภัยด้านความเป็นส่วนตัวที่ใช้ภาษาที่เข้าใจได้ง่าย	0.755
นโยบายการรักษาความปลอดภัยด้านความเป็นส่วนตัวของกูเกิลสตรีทวิวควรคลอบคลุมถึงผู้ที่ไม่ใช่ผู้ใช้งาน	0.859
นโยบายการรักษาความปลอดภัยด้านความเป็นส่วนตัวของกูเกิลสตรีทวิวนั้นควรจะมีการเปิดเผยให้ชัดเจน	0.840
นโยบายการรักษาความปลอดภัยด้านความเป็นส่วนตัวที่ดีนั้นควรแสดงบนหน้าเว็บในจุดที่มองเห็นได้ง่าย	0.859
ปัจจัย 5: ความเชื่อในความเสี่ยง (80.984% of variance, α = 0.941)	
ท่านรู้สึกกังวลว่าข้อมูลส่วนบุคคลของท่านที่เผยแพร่อยู่บนกูเกิลสตรีทวิวจะทำให้ท่านถูกละเมิดความเป็นส่วนตัว	0.931
ท่านรู้สึกกังวลต่อการให้บริการแบบเผยแพร่ข้อมูลส่วนบุคคลของกูเกิลสตรีทวิวบนพื้นที่สาธารณะจะนำมาซึ่งปัญหาที่ไม่คาดคิดมากมาย	0.905
ท่านรู้สึกกังวลว่าข้อมูลส่วนบุคคลของท่านที่เผยแพร่อยู่บนกูเกิลสตรีทวิวจะทำให้ผู้อื่นประเมินท่านในทางไม่ดี	0.854
ท่านรู้สึกกังวลว่าข้อมูลส่วนบุคคลของท่านที่เผยแพร่อยู่บนกูเกิลสตรีทวิวจะละเมิดความเป็นส่วนตัวของคนรอบตัวท่าน	0.909
ท่านรู้สึกกังวลว่าจะมีผู้นำข้อมูลส่วนบุคคลของท่านบนกูเกิลสตรีทวิวไปเผยแพร่ต่อบนเว็บไซต์อื่น	0.899
ปัจจัย 6: ความตั้งใจเชิงพฤติกรรม (8.247% of variance, α = 0.944)	
ท่านจะรายงานปัญหาเกี่ยวกับข้อมูลที่ละเมิดความเป็นส่วนตัวของท่านบนกูเกิลสตรีทวิว	0.694
ท่านจะร้องเรียนข้อมูลที่ละเมิดความเป็นส่วนตัวของท่านบนกูเกิลสตรีทวิวต่อหน่วยงานรัฐ	0.732
ท่านจะไม่ใช้บริการกูเกิลสตรีทวิวอีกเมื่อพบการละเมิดความเป็นส่วนตัวของท่านบนกูเกิลสตรีทวิว	0.729
ท่านจะบอกผู้อื่นให้ทราบเรื่องการละเมิดความเป็นส่วนตัวของท่านบนกูเกิลสตรีทวิว	0.770
ท่านยินดีที่จะเปลี่ยนไปใช้บริการสตรีทวิวรายอื่นหากมีผู้ให้บริการที่สามารถดูแลข้อมูลส่วนบุคคลของท่านได้ดีกว่ากูเกิลสตรีทวิว	0.713

อนึ่งผลการวิเคราะห์ข้อมูลทั่วไปเกี่ยวกับผู้ตอบแบบสอบถามของกลุ่มตัวอย่างคุณลักษณะของกลุ่มผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิง (52.00%) มีอายุระหว่าง 20 - 30 ปี (63.50%) ประกอบอาชีพพนักงานบริษัทเอกชน (43.00%) ระดับการศึกษาอยู่ในระดับปริญญาตรี (57.50%) และมีรายได้เฉลี่ยต่อเดือน 10,000 - 30,000 บาท (57.50%)

5.2 การวิเคราะห์ผลการวิจัย

การทดสอบสมมติฐานการวิจัยในครั้งนี้ ผู้วิจัยใช้วิธีวิเคราะห์การถดถอยเชิงเส้นเดียว (Simple linear regression) และการวิเคราะห์การถดถอยพหุคูณ (Multiple regression) โดยใช้ค่า p-value ที่น้อยกว่าหรือเท่ากับ 0.05 เป็นตัวกำหนดนัยสำคัญทางสถิติ นอกจากนี้ผู้วิจัยยังใช้วิธีวิเคราะห์ระดับความสัมพันธ์ระหว่างปัจจัย (Unstandardized Coefficient) ที่สนับสนุนอิทธิพลของทัศนคติด้านความเป็นส่วนตัวของประชาชนต่อข้อมูลส่วนบุคคลที่มีต่อความตั้งใจเชิงพฤติกรรม และวิธีวิเคราะห์ระดับค่าเฉลี่ยของข้อคำถามปัจจัยด้านความตั้งใจเชิงพฤติกรรม โดยแบ่งการวิเคราะห์ออกเป็น 4 ส่วน ตามกรอบแนวคิดการวิจัยดังนี้

ส่วนที่ 1 ผลการวิเคราะห์การถดถอยเชิงเส้นเดียวแสดงให้เห็นว่าตัวแปรอิสระคือความกังวลด้านการจัดเก็บข้อมูล ความกังวลด้านการควบคุมข้อมูล ความกังวลด้านการรับรู้การนำข้อมูลไปใช้ และความกังวลด้านนโยบายรักษาความปลอดภัยด้านความเป็นส่วนตัวออนไลน์ กำหนดตัวแปรตามคือความเชื่อในความเสี่ยงที่ระดับนัยสำคัญ p = 0.000 ($F_{4,195}$ = 104.109) ซึ่งสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 68.10 (R^2 = 0.681) เมื่อวิเคราะห์ในรายละเอียดของตัวแปรอิสระจะพบว่าความกังวลด้านการจัดเก็บข้อมูล ความกังวลด้านการควบคุมข้อมูล ความกังวลด้านการรับรู้การนำข้อมูลไปใช้และความกังวลด้านนโยบายรักษาความปลอดภัยด้านความเป็นส่วนตัวออนไลน์ เป็นตัวกำหนดความเชื่อในความเสี่ยงระดับนัยสำคัญ p = 0.000 (ตารางที่ 2 และ 3) สอดคล้องกับงานวิจัยของ Xu et al. (2008) ที่กล่าวว่า ปริมาณข้อมูลส่วนบุคคลที่ถูกจัดเก็บ ประมวลผล และนำไปเผยแพร่จาก Applications ผ่าน Social Media ทั้งที่รู้ตัวและไม่รู้ตัวส่งผลที่สูงขึ้นส่งผลให้ความเชื่อในความเสี่ยงเพิ่มสูงขึ้น ซึ่งเป็นไปตามสมมติฐานที่ 1 และงานวิจัยของ Williams et al. (2009) กล่าวว่า ปริมาณข้อมูลส่วนบุคคลที่ถูกจัดเก็บ ประมวลผล และนำไปเผยแพร่จาก Applications ผ่าน Social Media ทั้งที่รู้ตัวและไม่รู้ตัวส่งผลที่ต่ำลงส่งผลให้ความเชื่อในความเสี่ยงลดต่ำลง ซึ่งเป็นไปตามสมมติฐานที่ 1 ความกังวลด้านการจัดเก็บข้อมูล (1a) การควบคุมข้อมูล (1b) และการรับรู้เกี่ยวกับการนำข้อมูลส่วนบุคคลไปใช้ (1c) ส่งผลทางบวกต่อความเชื่อในความเสี่ยง และสอดคล้องกับงานวิจัยของ งานวิจัยของ Tsai et al. (2010) ที่กล่าวว่านโยบายรักษาความปลอดภัยด้านความเป็นส่วนตัวออนไลน์ที่หละหลวม ทำให้ Applications หรือผู้ประกอบการสามารถเข้าถึงข้อมูลส่วนบุคคลของกลุ่มตัวอย่างได้ ส่งผลให้ความเชื่อในความเสี่ยงของกลุ่มตัวอย่างสูงขึ้น ซึ่งเป็นไปตามสมมติฐานที่ 2 และงานวิจัยของ Jensen and Potts (2004) กล่าวว่า การให้ความสำคัญและปรับปรุงนโยบายรักษาความปลอดภัยด้านความเป็นส่วนตัวออนไลน์ให้ครอบคลุม และอัปเดทอย่างสม่ำเสมอส่งผลให้ความเชื่อในความเสี่ยงของกลุ่มตัวอย่างลดลง ซึ่งเป็นไปตามสมมติฐานที่ 2 ความกังวลด้านนโยบายรักษาความปลอดภัยด้านความเป็นส่วนตัวออนไลน์ ส่งผลทางบวกต่อความเชื่อในความเสี่ยง

ตารางที่ 2 ผลการวิเคราะห์การถดถอย (Regression) ของความกังวลด้านการจัดเก็บข้อมูล ความกังวลด้านการควบคุมข้อมูล ความกังวลด้านการรับรู้การนำข้อมูลไปใช้ และความกังวลด้านนโยบายรักษาความปลอดภัยด้านความเป็นส่วนตัวออนไลน์

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	135.535	4	33.884	104.109	0.000*
Residual	63.465	195	0.325		
Total	199.000	199			

* p <0.05

ตารางที่ 3 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของความกังวลด้านการจัดเก็บข้อมูล ความกังวลด้านการควบคุมข้อมูล ความกังวลด้านการรับรู้การนำข้อมูลไปใช้ และความกังวลด้านนโยบายรักษาความปลอดภัยด้านความเป็นส่วนตัวออนไลน์

ตัวแปร	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
ค่าคงที่	-4.096		0.000	1.000	ค่าคงที่
Collect	0.212	0.212	5.235	0.000	Collect
Control	0.522	0.522	12.915	0.000	Control
Awareness	0.428	0.428	10.579	0.000	Awareness
Policy	0.425	0.425	10.504	0.000	Policy

* p <0.05 R = 0.825, R^2 = 0.681, SE = 0.40

ส่วนที่ 2 ผลการวิเคราะห์ระดับความสัมพันธ์ระหว่างปัจจัยที่สนับสนุนอิทธิพลของทัศนคติด้านความเป็นส่วนตัวของประชาชนต่อข้อมูลส่วนบุคคลบนกูเกิลสตรีทวิวที่มีต่อความตั้งใจเชิงพฤติกรรม แสดงให้เห็นว่าความกังวลต่อการควบคุมข้อมูลมีผลต่อความเชื่อในความเสี่ยงอยู่ที่ค่าสัมประสิทธิ์การถดถอยของตัวแปรอิสระในรูปคะแนนดิบหรือค่าจริง (Unstandardized Coefficient) = 0.522 เป็นลำดับที่หนึ่ง ความกังวลต่อการรับรู้การนำข้อมูลไปใช้มีผลต่อความเชื่อในความเสี่ยงอยู่ที่ค่า Unstandardized Coefficient = 0.428 เป็นลำดับที่สอง ความกังวลด้านนโยบายความปลอดภัยด้านความเป็นส่วนตัวออนไลน์มีผลต่อความเชื่อในความเสี่ยงอยู่ที่ค่า Unstandardized Coefficient = 0.425 เป็นลำดับที่สาม ความเชื่อในความเสี่ยงมีผลต่อความตั้งใจเชิงพฤติกรรมอยู่ที่ค่า Unstandardized Coefficient = 0.216 เป็นลำดับที่สี่ และความกังวลด้านการจัดเก็บข้อมูลมีผลต่อความเชื่อในความเสี่ยงอยู่ที่ค่า Unstandardized Coefficient = 0.212 เป็นลำดับที่ห้า (ตารางที่ 4)

ตารางที่ 4 แสดงสรุปผลค่าสัมประสิทธิ์การถดถอย (Unstandardized Coefficient) ของตัวแปรอิสระในรูปคะแนนดิบ

ความสัมพันธ์	คำอธิบายความสัมพันธ์	Unstandardized Coefficient
ความสัมพันธ์ที่ 1	ความกังวลต่อการควบคุมข้อมูลมีผลต่อความเชื่อในความเสี่ยง	0.522
ความสัมพันธ์ที่ 2	ความกังวลต่อการรับรู้การนำข้อมูลไปใช้มีผลต่อความเชื่อในความเสี่ยง	0.428
ความสัมพันธ์ที่ 3	ความกังวลด้านนโยบายความปลอดภัยด้านความเป็นส่วนตัวออนไลน์มีผลต่อความเชื่อในความเสี่ยง	0.425
ความสัมพันธ์ที่ 4	ความเชื่อในความเสี่ยงมีผลต่อความตั้งใจเชิงพฤติกรรม	0.216
ความสัมพันธ์ที่ 5	ความกังวลด้านการจัดเก็บข้อมูลมีผลต่อความเชื่อในความเสี่ยง	0.212

ส่วนที่ 3 ผลการวิเคราะห์ความถดถอยพหุคูณแสดงให้เห็นว่าตัวแปรอิสระคือความเชื่อในความเสี่ยง กำหนดตัวแปรตามคือความตั้งใจเชิงพฤติกรรมที่ระดับนัยสำคัญ p = 0.000 ($F_{1,198}$ = 9.728) ซึ่งสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 4.20 (R^2 = 0.047) เมื่อวิเคราะห์ในรายละเอียดของตัวแปรอิสระจะพบว่าความเชื่อในความเสี่ยง เป็นตัวกำหนดความตั้งใจเชิงพฤติกรรมระดับนัยสำคัญ p = 0.000 (ตารางที่ 5 และ 6) สอดคล้องกับงานวิจัยของ Eastlick et al. (2006) ที่กล่าวว่า กลุ่มตัวอย่างมีพฤติกรรมเรียกร้องเนื่องจากเชื่อว่าถูกละเมิดความเป็นส่วนตัวและตั้งใจหยุดซื้อสินค้าออนไลน์ ซึ่งเป็นไปตามสมมติฐานที่ 3 และงานวิจัยของ Li et al. (2010) ที่กล่าวว่า การให้ผลประโยชน์ที่น่าสนใจเป็นการแลกเปลี่ยนและการส่งเสริมการสร้างความเชื่อมั่นในการคุ้มครองข้อมูลส่วนบุคคล ทำให้กลุ่มตัวอย่างมีความเชื่อในความเสี่ยงต่ำลง และเต็มใจที่จะเปิดเผยข้อมูลส่วนบุคคลมากขึ้น ซึ่งเป็นไปตามสมมติฐานที่ 3 ความเชื่อในความเสี่ยง ส่งผลทางบวกต่อความตั้งใจของพฤติกรรม

ตารางที่ 5 ผลการวิเคราะห์การถดถอย (Regression) ของความเชื่อในความเสี่ยงและความตั้งใจเชิงพฤติกรรม

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	9.319	1	9.319	9.728	0.002*
Residual	189.681	198	0.958		
Total	199.000	199			

* p <0.05

ตารางที่ 6 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของความเชื่อในความเสี่ยงและความตั้งใจเชิงพฤติกรรม

ตัวแปร	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
ค่าคงที่	1.081		0.000	1.000	ค่าคงที่
Riskbelief	0.216	0.216	3.119	0.002	Riskbelief

* p <0.05 R = 0.216, R^2 = 0.047, SE = 0.69

ส่วนที่ 4 ผลการวิเคราะห์ระดับค่าเฉลี่ยของข้อคำถามปัจจัยด้านความตั้งใจเชิงพฤติกรรม พบว่า ข้อคำถามที่ 1 ท่านจะรายงานปัญหาเกี่ยวกับข้อมูลที่ละเมิดความเป็นส่วนตัวของท่านบนกูเกิลสตรีทวิวอยู่ที่ค่าเฉลี่ย = 4.950 เป็นลำดับที่หนึ่ง ข้อคำถามที่ 2 ท่านจะร้องเรียนข้อมูลที่ละเมิดความเป็นส่วนตัวของท่านบนกูเกิลสตรีทวิวต่อหน่วยงานรัฐอยู่ที่ค่าเฉลี่ย = 4.510 เป็นลำดับที่สอง ข้อคำถามที่ 3 ท่านจะไม่ใช้บริการกูเกิลสตรีทวิวอีกเมื่อพบการละเมิดความเป็นส่วนตัวของท่านบนกูเกิลสตรีทวิวอยู่ที่ค่าเฉลี่ย = 4.470 เป็นลำดับที่สาม ข้อคำถามที่ 5 ท่านยินดีที่จะเปลี่ยนไปใช้บริการสตรีทวิวรายอื่นหากมีผู้ให้บริการที่สามารถดูแลข้อมูลส่วนบุคคลของท่านได้ดีกว่ากูเกิลสตรีทวิว มีค่าเฉลี่ย = 4.445 และค่าเบี่ยงเบนมาตรฐาน = 0.88934 เป็นลำดับที่สี่ และข้อคำถามที่ 4 ท่านจะบอกผู้อื่นให้ทราบเรื่องการละเมิดความเป็นส่วนตัวของท่านบนกูเกิลสตรีทวิว มีค่าเฉลี่ย = 4.445 และค่าเบี่ยงเบนมาตรฐาน = 0.87223 (ตารางที่ 7)

ตารางที่ 7 แสดงสรุปผลการวิเคราะห์ระดับค่าเฉลี่ย (Mean) ของข้อคำถามปัจจัยด้านความตั้งใจเชิงพฤติกรรม

ข้อคำถาม	คำอธิบายข้อคำถาม	Mean	Std. Deviation
คำถามที่ 1	ท่านจะรายงานปัญหาเกี่ยวกับข้อมูลที่ละเมิดความเป็นส่วนตัวของท่านบนกูเกิลสตรีทวิว	4.950	0.94042
คำถามที่ 2	ท่านจะร้องเรียนข้อมูลที่ละเมิดความเป็นส่วนตัวของท่านบนกูเกิลสตรีทวิวต่อหน่วยงานรัฐ	4.510	0.97707
คำถามที่ 3	ท่านจะไม่ใช้บริการกูเกิลสตรีทวิวอีกเมื่อพบการละเมิดความเป็นส่วนตัวของท่านบนกูเกิลสตรีทวิว	4.470	0.90731
คำถามที่ 4	ท่านจะบอกผู้อื่นให้ทราบเรื่องการละเมิดความเป็นส่วนตัวของท่านบนกูเกิลสตรีทวิว	4.445	0.87223
คำถามที่ 5	ท่านยินดีที่จะเปลี่ยนไปใช้บริการสตรีทวิวรายอื่นหากมีผู้ให้บริการที่สามารถดูแลข้อมูลส่วนบุคคลของท่านได้ดีกว่ากูเกิลสตรีทวิว	4.445	0.88934

6. อภิปรายและสรุปผลการวิจัย

การวิจัยนี้เกิดจากการที่ผู้วิจัยได้เล็งเห็นถึงปัญหาเรื่องการละเมิดความปลอดภัยด้านความเป็นส่วนตัวของข้อมูลส่วนบุคคล ส่วนหนึ่งได้รับผลมาจากความก้าวหน้าทางเทคโนโลยีสารสนเทศภูมิศาสตร์ โดยเฉพาะระบบกูเกิลสตรีทวิว ที่ได้ทำการจัดเก็บรวบรวมและเผยแพร่ข้อมูลรูปถ่ายสตรีทวิวเข้าสู่อินเทอร์เน็ตโดยไม่ได้ขออนุญาตเจ้าของข้อมูล ส่งผลให้เกิดความเสียหายต่อเจ้าของข้อมูล เช่น ใครซักคนบนโลกนี้ที่เชื่อมต่ออินเทอร์เน็ตกำลังดูภาพบริเวณหน้าบ้านของท่านอยู่โดยที่ท่านไม่รู้ตัว อาชญากรใช้กูเกิลสตรีทวิวในการค้นหาเคหะสถานหรือพื้นที่ซึ่งเอื้อต่อการก่อเหตุอาชญากรรม ผู้ไม่หวังดีแชร์ข้อมูลส่วนบุคคลของท่านหรือคนใกล้ตัวของท่านหรือทรัพย์สินของท่านลงบนเว็บไซต์ใดๆ พร้อมระบุตำแหน่งบนแผนที่ออนไลน์ โดยอาจกระทำเพื่อการแอบอ้าง ประทุษร้าย หรือต้องการให้อับอาย เป็นต้น ซึ่งจากผลการวิจัยพบว่าประชาชนรู้สึกกังวลต่อการให้บริการของกูเกิลสตรีทวิว โดยดู จากความผันแปรของตัวแปรตามคือความเชื่อในความเสี่ยงถึงร้อยละ 68.10 จากตัวแปรต้นความกังวลด้านการจัดเก็บข้อมูล ความกังวลด้านการควบคุมข้อมูล ความกังวลด้านการรับรู้การนำข้อมูลไปใช้และความกังวลด้านนโยบายรักษาความปลอดภัยด้านความเป็นส่วนตัวออนไลน์ และยังพบด้วยว่าประชาชนยังไม่ตื่นตัวจากการให้บริการลักษณะนี้หรือปัญหาที่อาจจะเกิดขึ้นในอนาคต โดยดูจากความผันแปรของตัวแปรตามคือความตั้งใจเชิงพฤติกรรมเพียงร้อยละ 4.20 จากตัวแปรต้นความเชื่อในความเสี่ยง

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาอิทธิพลของทัศนคติด้านความเป็นส่วนตัวของประชาชนต่อข้อมูลส่วนบุคคลบนกูเกิลสตรีทวิวที่มีต่อความตั้งใจเชิงพฤติกรรม ซึ่งมีพื้นฐานการศึกษามาจากทฤษฎีความเป็นส่วนตัว สิทธิส่วนบุคคลในข้อมูลสารสนเทศและความรู้สึกกังวลในเรื่องความเป็นส่วนตัว ตามเกณฑ์วัดทัศนคติด้านความเป็นส่วนตัวของผู้ใช้งานอินเทอร์เน็ต ซึ่งเป็นปัจจัยที่ขับเคลื่อนไปสู่การตั้งใจเชิงพฤติกรรมต่อการละเมิดความเป็นส่วนตัว โดยจากผลการวิเคราะห์ทางสถิติพบว่า ลักษณะทางประชากรศาสตร์จำนวนเพศชายและเพศหญิงใกล้เคียงกัน มีอายุระหว่าง 20-30 ปี ส่วนใหญ่เป็นพนักงานบริษัทเอกชน และมีระดับการศึกษาอยู่ในระดับปริญญาตรี โดยความกังวลต่อการควบคุมข้อมูลมีผลต่อความเชื่อในความเสี่ยงมากที่สุด รองลงมาคือความกังวลต่อการรับรู้การนำข้อมูลไปใช้มีผลต่อความเชื่อในความเสี่ยง ตามด้วยความกังวลด้านนโยบายความปลอดภัยด้านความเป็นส่วนตัวออนไลน์มีผลต่อความเชื่อในความเสี่ยง ต่อไปคือความเชื่อในความเสี่ยงมีผลต่อความตั้งใจเชิงพฤติกรรม และความกังวลด้านการจัดเก็บข้อมูลมีผลต่อความเชื่อในความเสี่ยงเป็นลำดับสุดท้าย เมื่อพิจารณาถึงความตั้งใจเชิงพฤติกรรม พบว่าประชาชนมีความตั้งใจที่จะรายงานปัญหาเกี่ยวกับข้อมูลที่ละเมิดความเป็นส่วนตัวต่อระบบกูเกิลสตรีทวิวเองมากที่สุด รองลงมาคือรายงานปัญหาเกี่ยวกับข้อมูลที่ถูกละเมิดความเป็นส่วนตัวต่อหน่วยงานภาครัฐ ไม่ใช้บริการกูเกิลสตรีทวิวอีกเมื่อพบการละเมิดความเป็นส่วนตัวบนกูเกิลสตรีทวิวเป็นลำดับที่สาม ยินดีที่จะเปลี่ยนไปใช้บริการสตรีทวิวรายอื่นหากมีผู้ให้บริการที่สามารถดูแลข้อมูลส่วนบุคคลได้ดีกว่ากูเกิลสตรีทวิว และ บอกต่อผู้อื่นให้ทราบเรื่องการละเมิดความเป็นส่วนตัวของกูเกิลสตรีทวิว

บรรณานุกรม

Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behavior and Human Decision Processes*, 50, 179-211.

Bolchini, D., He, Q., Antón, A. I., and Stufflebeam, W. (2004). "*I Need It Now": Improving Website Usability by Contextualizing Privacy Policies*. In Web Engineering (pp. 31-44). Springer Berlin Heidelberg.

Buchanan, T., Paine, C.B., Joinson, A. N., and Reips, U-R. (2006). *Development of measures of online privacy concern and protection for use on the Internet*. Retrieved from http://www.prisd.net

Culnan, M. J., and Bies, R. J., (2003). Consumer privacy: Balancing economic and justice consideration. *Journal of Social Issues*, 59(2), 323-342.

Dowling, G. R., and Staelin, R. A. (1994). Model of perceived risk and intended riskhandling activity. *Journal of Consumer Research*, 21, (1),119–134.

Eastlick, M. A., Lotz, S. L., and Warrington, P. (2006). Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment. *Journal of Business Research*, 59(8), 877-886."

Fishbein, M., and Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA : Addison-Wesley.

Grigoroudis, E. (2009). *Customer satisfaction evaluation*. New York: Springer.

Jensen, C., and Potts. P. (2004). Privacy policies as decision-making tools: An evaluation of online privacy notices, *In Proceedings of the SIGCHI conference on Human factors in computing systems*, 6(1), 471- 478

Li, H., Sarathy, R., and Xu, H. (2010). Understanding Situational Online Information Disclosure as a Privacy Calculus, Journal of Computer Information Systems, accepted.

Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model, *Information Systems Research*. 15(4), 336-355.

Oliver, R. L. (2010). *Satisfaction : A Behavioral Perspective on the Consumer*. (2nd ed.). Armonk, NY: Sharpe.

Smith, H. J., Milberg, J. S., and Burke, J.S. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, 20(2), 167-196.

Tsai, J. Y., Kelley, P. G., Cranor, L. F., and Sadeh, N. (2010). *Location-Sharing Technologies: Privacy Risks and Conrols*. Carnegie Mellon University.

Williams, K., Boyd, A., Densten, S., Chin, R., Diamond, D., and Morgenthaler. C. (2009). *Social Networking Privacy Behaviors and Risks*. White Plains, NY : Seidenberg School of CSIS, Pace University

Xu, H., Dinev,T., Smith, J., and Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, 12(12), 798-824.

Zhang, H., Lin, Y. H., Zhang, Z., Zhang, X., Shaw, S. L., Knipping, E. M., and Surratt, J. D. (2012). Secondary organic aerosol formation from methacrolein photooxidation: roles of NOx level, relative humidity and aerosol acidity. Environmental Chemistry, 9(3), 247-262.

ปัจจัยที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร

สุพิชญา อาชวิรดา*

สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ

***Correspondence:** supichaya_a@hotmail.com doi: 10.14456/jisb.2016.11

บทคัดย่อ

ปัจจุบันสารสนเทศเข้ามามีบทบาทต่อการดำเนินธุรกิจเป็นอย่างมาก แต่ความเสี่ยงทางธุรกิจที่พบมากเป็นอันดับต้นๆ คือการรับเอาเทคโนโลยีมาใช้โดยไม่ได้คำนึงถึงการรักษาความมั่นคงปลอดภัยในระดับที่เพียงพอควบคู่กันไปด้วย ดังนั้น การรักษาความมั่นคงปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กรถือเป็นเรื่องสำคัญ องค์กรจำเป็นต้องทบทวนบทบาทและเพิ่มระดับการรักษาความมั่นคงปลอดภัย ให้มากขึ้น นอกจากนี้ ผู้บริหารระดับสูงยังจะต้องเร่งสร้าง การตระหนัก ในเรื่องการรักษาความมั่นคงปลอดภัยของข้อมูลบนระบบสารสนเทศให้เกิดแก่พนักงาน ลูกจ้างและ ผู้ถือหุ้น อื่นๆ รวมทั้งปลูกฝังจริยธรรมในการเผยแพร่ข้อมูลซึ่งถือเป็น สินทรัพย์ ที่สำคัญของบริษัทออกไปภายนอก เนื่องจากการทำให้พนักงานในองค์กรตระหนักถึงการใช้ระบบสารสนเทศในองค์กรจะมีส่วนช่วยให้องค์กรมีระดับการรักษาความมั่นคงปลอดภัยที่สูงขึ้น ผู้วิจัยจึงทำการศึกษาว่ามีปัจจัยใดบ้างที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยในการใช้ระบบสารสนเทศ โดยงานวิจัยนี้เป็นการวิจัยเชิงปริมาณประเภทการวิจัยเชิงสำรวจ โดยรวบรวมข้อมูลจากพนักงานในองค์กรที่มีรายชื่อจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทยจำนวน 240 ชุดและนำข้อมูลที่ได้มาวิเคราะห์สมการถดถอยโดยใช้โปรแกรมสำเร็จรูปทางสถิติ เพื่อศึกษาปัจจัยที่มีผลต่อการตระหนักถึงความปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กร ซึ่งผลของงานวิจัยนี้แสดงให้เห็นว่า การรับรู้ถึงภัยคุกคาม การฝึกอบรมและให้ความรู้ ความรู้ความเข้าใจในระบบสารสนเทศล้วนส่งผลต่อการตระหนักถึงความปลอดภัย และเมื่อพนักงานเกิดความตระหนักแล้วยังส่งผลต่อพฤติกรรมการใช้ระบบสารสนเทศในองค์กรทำให้เกิดความตระหนักในการใช้งานมากขึ้น สุดท้ายก่อให้เกิดระดับการรักษาความมั่นคงปลอดภัยที่สูงขึ้นนั่นเอง ประโยชน์ที่ได้จากการวิจัยนี้ทำให้ทราบถึงระดับการรักษาความมั่นคงปลอดภัยของสารสนเทศในองค์กร อีกทั้งจะช่วยให้ผู้ใช้ตระหนักถึงความปลอดภัยในการใช้สารสนเทศในองค์กร และสามารถนำไปเป็นแนวทางให้องค์กรกำหนดนโยบายการควบคุมดูแลการใช้ระบบสารสนเทศ

คำสำคัญ : ระดับการรักษาความมั่นคงปลอดภัย การตระหนักถึงความปลอดภัย ระบบสารสนเทศ

Factors Affecting the Security Level of Information Systems in Organization

Supichaya Archavajirada*

Computer Center, Srinakharinwirot University

***Correspondence:** supichaya_a@hotmail.com doi: 10.14456/jisb.2016.11

Abstract

Nowadays Information System plays a vital role in running businesses. However, top ranking of their risk is to adopt technology to the organization by not taking the consideration in high level of data security, simultaneously. Technically, data security for organization's information system is very important. Thus, organization would review and raise security's level. Besides, management has to promote not only realization in data security's importance to all staffs, stakeholders, and shareholders but also ethic by not to externally broadcasting organization's data, which is very important organization's asset. This practice tends to help organization to have higher data security's level. Researcher studies factors affecting to level of Information System's data security. This research is a quantitative survey study by collecting data from staffs in the organization, being public company limited total 240 copies. Then, all data is analyzed by regression equation to study factors affecting to realization in data security within the organization. The result of this research represents that risk's awareness, training, and learning in information system altogether impacting to realization in data security. If staffs start realizing in importance of data security, level of its will increase, absolutely. The benefit of research can help to understand level of information system's data security in the organization and can be guideline for organization to set up policy and monitor information system usage.

Keywords: security of information systems, security awareness, information systems

1. บทนำ

เทคโนโลยีสารสนเทศและการสื่อสาร ได้มีอิทธิพลและขยายความสำคัญต่อรูปแบบการดำเนินชีวิตเป็นอย่างมาก โดยเฉพาะด้านเทคโนโลยีสารสนเทศที่มีคุณประโยชน์หลากหลายประการ และเป็นปัจจัยหลักในการพัฒนาประเทศในทุกด้าน ก่อให้เกิดสังคมไร้พรมแดนที่ผู้คนทั่วโลกสามารถสื่อสารได้อย่างสะดวกรวดเร็ว และเป็นสื่อที่ช่วยสนับสนุนให้เกิดการพัฒนาทั้งด้านเศรษฐกิจ สังคมและอุตสาหกรรม การพัฒนาคุณภาพชีวิต การเผยแพร่ข่าวสาร และการประชาสัมพันธ์ การส่งเสริมการท่องเที่ยว ตลอดจนการติดต่อสื่อสารโทรคมนาคม อย่างไรก็ตาม แม้ว่าเทคโนโลยีสารสนเทศจะให้คุณประโยชน์มากมายมหาศาลแก่ผู้ใช้งาน แต่ในขณะเดียวกันเทคโนโลยีสารสนเทศก็สามารถก่อให้เกิดผลกระทบทางลบแก่ผู้ใช้งานได้เช่นกัน เทคโนโลยีเหล่านี้ สามารถเป็นสะพานหรือเป็นช่องทางในการก่ออาชญากรรมในรูปแบบใหม่ เช่น การจารกรรมข้อมูล การสร้างข่าวสารอันเป็นเท็จ การหลอกลวงต่างๆ เป็นต้น สิ่งเหล่านี้ส่งผลเสียต่อผู้ใช้งานได้ หากผู้ใช้งานขาดความรู้ในการป้องกันตนเองอย่างเหมาะสม จึงอาจเป็นเหตุนำมาซึ่งความเสื่อมเสียต่อตัวเอง ข้อมูล และทรัพย์สิน เช่น การถูกหลอกลวงโดยมิจฉาชีพออนไลน์ การขโมยข้อมูลส่วนตัว การขโมยอีเมล์ หรือการหลอกลวงให้ทำการโอนย้ายข้อมูลและทรัพย์สิน เป็นต้น ซึ่งภัยจากเทคโนโลยีสารสนเทศเหล่านี้มีแนวโน้มที่จะเกิดมากขึ้น และมีวิธีการที่หลากหลายอีกด้วย ซึ่งผู้ใช้งานทั่วไปมีความเสี่ยงต่อภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศที่อาจเกิดขึ้น เช่น ไวรัสคอมพิวเตอร์ บัญชีผู้ใช้ถูกแฮก การถูกบุกรุกคอมพิวเตอร์จากระยะไกล เป็นต้น โดยผู้ใช้งานอาจรับทราบถึงภัยคุกคามเหล่านี้ แต่อาจยังไม่ทราบถึงวิธีปฏิบัติหรือป้องกันและแก้ไขเมื่อเกิดภัยจากการใช้เทคโนโลยีสารสนเทศ เช่น เมื่อคอมพิวเตอร์ติดไวรัสควรทำอย่างไร หากเครื่องคอมพิวเตอร์ถูกแฮกควรทำอย่างไร (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2557) ดังนั้นงานวิจัยนี้จึงมีวัตถุประสงค์เพื่อ ศึกษาปัจจัยที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร ได้แก่ พฤติกรรมการใช้ และการตระหนักถึงความปลอดภัย ซึ่งการที่จะทำให้พนักงานเกิดการตระหนักได้นั้น ควรทำให้พนักงานเกิดความรู้ความเข้าใจในการใช้ระบบสารสนเทศอย่างปลอดภัย โดยการฝึกอบรมและให้ความรู้พร้อมทั้งทำให้พนักงานรับรู้ถึงภัยคุกคาม

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ผู้วิจัยได้นำแนวคิดทฤษฎี และงานวิจัยที่เกี่ยวข้องมาเป็นแนวทางในการศึกษาวิจัย ดังต่อไปนี้ (1) แนวคิดพฤติกรรมตามแผน (Theory of planned behavior หรือ TPB) นำเสนอโดย Ajzen เป็นแนวคิดทางจิตวิทยาสังคม (Social psychology) พัฒนามาจากแนวคิด TRA โดย Ajzen ได้เพิ่มปัจจัยการรับรู้ถึงการควบคุมพฤติกรรมของตนเองในการแสดงพฤติกรรมใดๆ (Perceived behavioral control) (สิงหะ ฉวีสุข, 2555) (2) แบบจำลองการสร้างความตระหนักเป็นแบบจำลอง ที่พัฒนาจากการศึกษาปัจจัยที่ส่งผลต่อการตระหนักถึงความเป็นส่วนตัวที่พัฒนาต่อยอดมาจากทฤษฎีพฤติกรรมตามแผนเช่นกัน ซึ่งแสดงให้เห็นว่าหากบุคคลเกิดการรับรู้จะส่งผลต่อความตระหนักและการตั้งใจ จากนั้นจะทำให้เกิดระดับการเปิดเผยข้อมูล (ภัททิยา นภาชัยเทพ, 2555) (3) แบบจำลองในการรักษาความมั่นคงปลอดภัยที่แสดงให้เห็นว่าการฝึกอบรมเป็นส่วนสำคัญในการทำให้พนักงานเกิดความตระหนักและยังส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยที่เพิ่มขึ้นด้วย (Hale, 2012) อนึ่ง งานวิจัยนี้ได้ทำการศึกษาจากงานวิจัยในอดีต โดยมีทั้งหมด 6 ปัจจัย ดังต่อไปนี้

การรับรู้ถึงภัยคุกคาม (perceived threats) หมายถึง การทราบถึงความรุนแรงหรือผลกระทบของอันตรายที่จะเกิดขึ้น ซึ่งแสดงให้เห็นถึงความกลัวต่อความรุนแรง (Gore and Bracken, 2005) ซึ่งการรับรู้ถึงภัยคุกคามจะส่งผลต่อตวามรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Bulgurcu et al., 2010)

ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Insight into the security of information systems) หมายถึง การที่บุคคลมีความทรงจำในเรื่องราว ข้อเท็จจริง รายละเอียดต่างๆ และความสามารถในการนำความรู้ที่เก็บรวบรวมมาใช้ดัดแปลง อธิบาย เปรียบเทียบในเรื่องนั้นๆ ได้อย่างมีเหตุผลในเรื่องของระบบการรักษาความ

มั่นคงปลอดภัยด้านระบบสารสนเทศภายในองค์กร จึงทำให้สามารถก่อให้เกิดเป็นพฤติกรรมในการใช้สารสนเทศอย่างมีความตระหนักถึงความปลอดภัย (จักรกริช ใจดี, 2542) ซึ่งความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศจะส่งผลต่อการตระหนักถึงความปลอดภัย (Son and Jeong, 2013)

การฝึกอบรมและให้ความรู้ (Training and education) หมายถึง รูปแบบของการเรียนรู้ ความรู้ ทักษะ ค่านิยม ความเชื่อ และพฤติกรรมของกลุ่มคนที่ได้รับการถ่ายโอนจากบุคคลหนึ่งไปยังบุคคลอื่น ผ่านการเล่าเรื่อง การสนทนา การเรียนการสอน ด้านการรักษาความมั่นคงปลอดภัย เพื่อพัฒนาความรู้และให้พนักงานทราบถึงวิธีการรักษาความมั่นคงปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กร (Gadzama et al., 2014) ซึ่งการฝึกอบรมและให้ความรู้จะส่งผลต่อความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Maqousi et al., 2014)

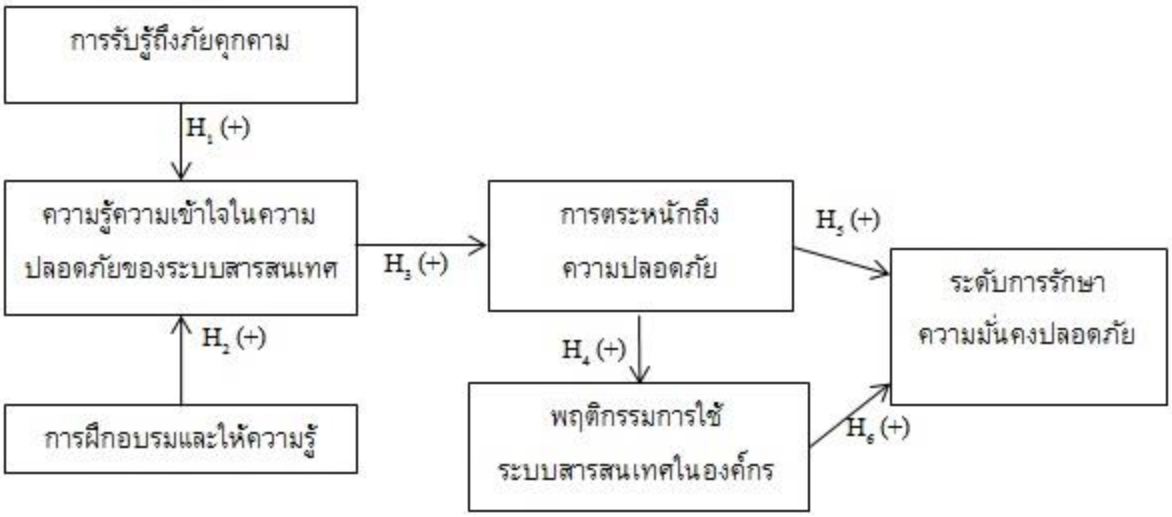
การตระหนักถึงความปลอดภัย (Awareness) หมายถึง ความสามารถในการรับรู้ หรือ รู้สึก หรือ มีสติ ต่อเหตุการณ์ ความรู้สึก หรือรูปแบบการสัมผัส การตระหนักถึงความปลอดภัยเกิดจากทัศนคติที่มีต่อสิ่งเร้าอันได้แก่ บุคคล สถานการณ์ กลุ่มสังคม และสิ่งต่าง ๆ ที่โน้มเอียง หรือตอบสนองในทางบวก หรือทางลบ เป็นสิ่งที่เกิดจากการเรียนรู้และประสบการณ์ (Solic et al., 2012) ซึ่งการตระหนักถึงความปลอดภัยจะส่งผลต่อพฤติกรรมการใช้ระบบสารสนเทศในองค์กร (Liang and Xue, 2009)

พฤติกรรมการใช้ระบบสารสนเทศในองค์กร (Bhavior) หมายถึง ความตั้งใจของพนักงานที่จะปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย จากทัศนคติ กฎเกณฑ์ ความเชื่อและการรับรู้ถึงมาตรการที่ควรปฏิบัติตาม ซึ่งพฤติกรรมดังกล่าวส่งผลกระทบต่อความปลอดภัยของการใช้ระบบสารสนเทศในองค์กร (Rocha et al., 2014) ซึ่งพฤติกรรมการใช้ระบบสารสนเทศในองค์กรจะส่งผลต่อระดับการรักษาความมั่นคงปลอดภัย (Bulgurcu et al., 2010)

ระดับการรักษาความมั่นคงปลอดภัย (Level of security) หมายถึง มาตรฐานที่องค์กรใช้ป้องกันภัยคุกคามที่เกิดขึ้นจากการนำระบบสารสนเทศมาใช้ในองค์กรและสามารถนำมาตรฐานนั้นมาตรวจสอบองค์กรของตนเองเพื่อดูว่าองค์กรของตนเองนั้นมีระดับการรักษาความมั่นคงปลอดภัยมากน้อยเพียงใด (Crossler et al., 2013) ซึ่งการที่องค์กรจะมีระดับการรักษาความมั่นคงปลอดภัยที่สูงขึ้นได้นั้น ขึ้นอยู่กับพฤติกรรมการใช้ระบบสารสนเทศในองค์กร และการตระหนักถึงความปลอดภัย ของพนักงาน

3. กรอบแนวคิดการวิจัยและสมมติฐานการวิจัย

จากทฤษฎี แนวคิดที่เกี่ยวข้อง และการทบทวนวรรณกรรมต่างๆที่ได้ทำการศึกษามาแล้วนั้น ซึ่งกล่าวโดยสรุปได้ว่า การรับรู้ ส่งผลให้เกิดความตระหนัก และแสดงออกเป็นพฤติกรรม จนสามารถกำหนดเป็นระดับต่างๆได้ โดยงานวิจัยนี้ได้เพิ่มปัจจัยด้าน การฝึกอบรมและการให้ความรู้ และความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศเข้าไปในงานวิจัย ทำให้สามารถกำหนดปัจจัยที่มีผลต่อการตระหนักถึงความปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กร ได้ดังภาพที่ 1



ภาพที่ 1 กรอบแนวคิดระดับการรักษาความมั่นคงปลอดภัยต่อระบบสารสนเทศในองค์กร

การรับรู้ความรุนแรงของภัยคุกคามและการรับรู้ถึงสิ่งที่กระทบกระเทือนใจได้ง่ายซึ่งสิ่งกระทบกระเทือนใจได้ง่ายบางครั้งเรียกว่าการรับรู้ช่องโหว่ ที่เป็นตัวกระตุ้นให้เกิดการกระทำในการตอบสนองความกลัว เป็นการรับรู้ความน่าจะเป็นและการมีประสบการณ์กับอันตราย อย่างไรก็ตามการรับรู้ความรุนแรงเป็นระดับที่คนจะเชื่อว่าจะได้รับอันตรายถ้าหากบุคคลนั้นเคยมีประสบการณ์เกี่ยวกับอันตรายเหล่านั้น ดังนั้นเมื่อรับรู้ถึงความรุนแรง บุคคลจะเกิดความกลัวนั่นคือความกลัวไม่ได้ทำหน้าที่โดยตรงในความตั้งใจ แต่เพิ่มระดับความรุนแรงของการรับรู้ ซึ่งเมื่อบุคคลรับรู้ถึงความกลัวแล้วจะส่งผลให้บุคคลนั้นหาความรู้เพิ่มเติมเพื่อให้ตนเองเกิดความรู้ความเข้าใจถึงความปลอดภัย (Bulgurcu et al., 2010) ซึ่งสามารถตั้งสมมติฐานได้ดังนี้

H1 : การรับรู้ถึงถัยคุกคามส่งผลทางบวกต่อความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ

ปัญหาหลักของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่กำลังเติบโต คือความอ่อนแอที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยเนื่องจากผู้ใช้ที่มีความรู้ไม่เพียงพอ เกี่ยวกับการรักษาความมั่นคงปลอดภัย (Son and Jeong, 2013) ดังนั้นเมื่อมีการฝึกอบรมและให้ความรู้ เพื่อให้ผู้ใช้ เกิดความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ เพราะผลของการฝึกอบรมทำให้ผู้ใช้มีความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร ซึ่งสามารถตั้งสมมติฐานได้ดังนี้

H2 : การฝึกอบรมและให้ความรู้ส่งผลทางบวกต่อความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ

หากผู้ใช้เข้าใจถึงการใช้งานสารสนเทศในองค์กร ว่าการใช้งานอย่างไรก่อให้เกิดเป็นอันตรายได้นั้น ผู้ใช้จะตระหนักถึงอันตราย และเกิดการพัฒนาการรับรู้ของตนเอง (Liang and Xue, 2009) หากมีการให้ความรู้เกี่ยวกับรักษาความปลอดภัยที่มีจุดมุ่งหมายเพื่อให้ความรู้กับผู้ใช้ถึงภัยคุกคามทุกด้านที่อาจเกิดขึ้นและกล่าวถึงวิธีการเพื่อป้องกันการคุกคาม จะสามารถกำจัดหรือลดจำนวนของภัยคุกคามที่อาจเกิดขึ้นได้แล้วยังสามารถรักษาผู้ใช้และทรัพย์สินขององค์กรไว้ได้ (Maqousi et al., 2014) ซึ่งสามารถตั้งสมมติฐานได้ดังนี้

H3 : ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศส่งผลทางบวกต่อการตระหนักถึงความปลอดภัย

เมื่อตระหนักได้ว่ากำลังเผชิญอยู่กับภัยคุกคาม บุคคลจะมีส่วนร่วมในการแสดงออกทางพฤติกรรมเพื่อหลีกเลี่ยงภัยคุกคาม นั่นคือ เกิดเป็นพฤติกรรมเพื่อลดการเกิดภัยคุกคามจนกว่าภัยคุกคามที่เกิดขึ้นจะหายไป (Liang and Xue, 2009) โดยผู้ใช้ที่ไม่มีการตระหนักถึงความปลอดภัยของการใช้ระบบสารสนเทศในองค์กรจะกระทำพฤติกรรมที่อาจก่อให้เกิดภัยคุกคามต่อระบบสารสนเทศในองค์กร (Bulgurcu et al., 2010) ซึ่งสามารถตั้งสมมติฐานได้ดังนี้

H4 : การตระหนักถึงความปลอดภัยส่งผลทางบวกต่อพฤติกรรมการใช้ระบบสารสนเทศในองค์กร

เมื่อทุกคนในองค์กรตระหนักถึงความปลอดภัยของระบบสารสนเทศ โดยผู้ใช้ตระหนักถึงสิทธิของแต่ละบุคคลที่ได้รับอนุญาตให้ใช้ระบบ จะส่งผลดีให้แก่องค์กร ทำให้ผู้ใช้มีพฤติกรรมการใช้ระบบสารสนเทศอย่างถูกต้อง จึงทำให้องค์กรมีระดับการรักษาความปลอดภัยที่สูงขึ้น แต่หากผู้ใช้ไม่ตระหนักถึงความผิดพลาดที่อาจเกิดขึ้นได้นั้น จะเป็นอันตรายต่อความปลอดภัยของข้อมูล (Bulgurcu et al., 2010) ซึ่งสามารถตั้งสมมติฐานได้ดังนี้

H5 : การตระหนักถึงความปลอดภัยส่งผลทางบวกต่อระดับการรักษาความมั่นคงปลอดภัย

แม้องค์กรจะมีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยเพื่อรักษาระดับการรักษาความมั่นคงปลอดภัยในองค์กรนั้น แต่ยังมีพนักงานที่ไม่ปฏิบัติตามนโยบายดังกล่าวหรือไม่ตระหนักถึงความปลอดภัย ดังนั้นองค์กรควรมีนโยบายการรักษาความมั่นคงปลอดภัยเพื่อให้แน่ใจว่าระดับการป้องกันและการรักษาความลับของข้อมูลที่สมบูรณ์ ทำให้ข้อมูลองค์กรไม่มีการทำลาย จนเกิดช่องโหว่ในการรักษาความมั่นคงปลอดภัย และความเสี่ยง รวมถึงการจัดการการรักษาความมั่นคงปลอดภัยของข้อมูล ให้ถูกต้องซึ่งการจัดการปัญหาที่เกี่ยวข้องกับข้อมูล จำเป็นต้องมีนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลในองค์กร เพื่อควบคุมพฤติกรรมการใช้ระบบสารสนเทศในองค์กร (Gadzama et al., 2014) ซึ่งสามารถตั้งสมมติฐานได้ดังนี้

H6 : พฤติกรรมการใช้ระบบสารสนเทศในองค์กรส่งผลทางบวกต่อระดับการรักษาความมั่นคงปลอดภัย

4. วิธีการวิจัย

งานวิจัยนี้จัดเก็บข้อมูลจากกลุ่มตัวอย่างที่เป็นพนักงานในองค์กรที่มีรายชื่อจดทะเบียนในตลาดหลักทรัพย์จำนวน 240 คน ผ่านทางการเก็บแบบสอบถามออนไลน์ อนึ่งก่อนการจัดเก็บข้อมูลจากกลุ่มตัวอย่าง งานวิจัยนี้ได้นำแบบสอบถามที่พัฒนามาจากงานวิจัยในอดีต (ประกอบด้วย Bulgurcu et al., 2010; Crossler et al., 2013; Kruger et al., 2011; Puhakainen and Siponen, 2010; Rocha et al., 2014) ไปทดสอบกับกลุ่มตัวอย่างจำนวน 240 คน ผลการทดสอบพบว่าข้อมูลไม่มีปัญหาด้านข้อมูลสุดโต่ง และพบว่ามีตัวแปรบางตัวที่ไม่ได้มีการกระจายแบบปกติ แต่ต่างจากเกณฑ์มาตรฐานไม่มากนัก ต่อจากนั้นจึงนำแบบสอบถามที่ปรับแก้ไปจัดเก็บข้อมูลจากกลุ่มตัวอย่างจริง

5. ผลการวิจัย

5.1 การทดสอบข้อตกลงเบื้องต้นทางสถิติ

ข้อมูลที่จัดเก็บจากกลุ่มตัวอย่างถูกนำไปทดสอบข้อมูลขาดหาย (Missing data) และข้อมูลสุดโต่ง (Outliers) นอกจากนี้ยังทดสอบว่าข้อมูล มีการกระจายแบบปกติ (Normal) มีความสัมพันธ์เชิงเส้นตรง (Linearity) มีภาวะร่วมเส้นตรงพหุ (Multicollinearity) และมีภาวะร่วมเส้นตรง (Singularity) หรือไม่ ผลการทดสอบพบว่า ข้อมูลไม่มีปัญหาด้านข้อมูลขาดหาย ข้อมูลสุดโต่ง และข้อมูลมีการกระจายเป็นแบบปกติ มีความสัมพันธ์เชิงเส้นตรง และไม่มีปัญหาภาวะร่วมเส้นตรงพหุและภาวะร่วมเส้นตรง

นอกจากนี้งานวิจัยได้ทดสอบความเชื่อถือของแบบสอบถาม โดยใช้การวิเคราะห์ค่าสัมประสิทธิ์อัลฟาของครอนบาช พบว่าทุกตัวแปรมีค่ามากกว่า 0.7 จึงถือว่ามีความเชื่อถือได้สำหรับงานวิจัยแบบ Basic research (กัลยา วานิชย์บัญชา, 2552) นอกจากนี้ยังได้ทดสอบความตรงของแบบสอบถาม ด้วยการวิเคราะห์องค์ประกอบ (Factor analysis) โดยใช้เกณฑ์ที่ข้อคำถามที่จับกลุ่มกันเป็นแต่ละตัวแปรต้องมีค่า Factor loading ไม่น้อยกว่า 0.5 ผลการวิเคราะห์องค์ประกอบได้จำนวนตัวแปรทั้งหมด 23 องค์ประกอบ (ตารางที่ 1 แสดงปัจจัยที่ได้จากการวิเคราะห์องค์ประกอบของงานวิจัยนี้) อนึ่งผลการวิเคราะห์ข้อมูลทั่วไปเกี่ยวกับผู้ตอบแบบสอบถามของกลุ่มตัวอย่าง พบว่าลักษณะประชากรส่วนใหญ่ เป็นเพศหญิง (64%) ช่วงอายุ 41-50 ปี (28%) ทำงานในกลุ่มอุสาหกรรมด้านการบริการ (34%) มีอายุการทำงานในองค์กรมากกว่า 10 ปีขึ้นไป (50%) ระดับการศึกษาอยู่ในระดับปริญญาตรี (54%) มีรายได้มากกว่า 55,000 บาท (51%) และเป็นพนักงานในระดับปฏิบัติการ (39%) ซึ่งกลุ่มตัวอย่างทั้งหมด 240 คน ปฏิบัติงานอยู่ในองค์กรที่มีรายชื่อจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย

ตารางที่ 1 Factor analysis ของตัวแปรในงานวิจัย

ปัจจัย	น้ำหนักตัวประกอบ (Factor Loading)
ปัจจัย 1: การรับรู้ถึงภัยคุกคาม (Variance = 15.539, α = 0.746) ท่านรู้สึกไม่สบายใจเมื่อมีบุคคลอื่นมาขอใช้เครื่องคอมพิวเตอร์ของท่าน	0.715
ท่านมีความกังวลหากมีบุคคลอื่นมาใช้เครื่องคอมพิวเตอร์ของท่านโดยไม่ได้รับอนุญาต	0.826
ท่านรู้สึกกังวลว่าหากไม่มีการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ระบบสารสนเทศนั้นอาจเกิดอันตรายได้	0.696
ท่านรู้ว่าหากใช้ระบบสารสนเทศโดยไม่คำนึงถึงความปลอดภัย อาจก่อให้เกิดอันตรายต่อระบบสารสนเทศได้ เช่น โดนคุกคามจากไวรัส เป็นต้น	0.636
ปัจจัย 2: ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Variance = 13.249, α = 0.796) ท่านสามารถระบุได้ว่าโปรแกรมใดที่อาจเป็น spyware หรือ adware ที่รบกวนการทำงานของท่าน	0.819
ท่านมีความเข้าใจถึงวิธีการรักษาความมั่นคงปลอดภัย Information Security ในองค์กร	0.816
ท่านทราบถึงวิธีการป้องกัน ไม่ให้เครื่องคอมพิวเตอร์ของท่าน ถูกคุกคามจากโปรแกรมที่อาจเป็นไวรัสต่างๆ	0.826

ตารางที่ 1 Factor analysis ของตัวแปรในงานวิจัย (ต่อ)

ปัจจัย	น้ำหนักตัวประกอบ (Factor Loading)
ปัจจัย 3: การฝึกอบรมและให้ความรู้ (Variance = 12.442, α = 0.826) ท่านคิดว่าหากมีการให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร จะช่วยให้ “ท่าน” เข้าใจวิธีการรักษาความมั่นคงปลอดภัยต่อระบบสารสนเทศมากขึ้น	0.818
ท่านคิดว่าหากมีการให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร จะช่วยให้ “พนักงานในองค์กร” เข้าใจวิธีการรักษาความมั่นคงปลอดภัยต่อระบบสารสนเทศมากขึ้น	0.838
หากท่านได้รับการฝึกอบรมจะทำให้ท่านตระหนักถึงความปลอดภัยของข้อมูลในเครื่องคอมพิวเตอร์	0.748
สาเหตุที่พนักงานในองค์กรไม่คำนึงถึงความปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กร ส่วนหนึ่งมาจากพนักงานไม่ได้รับการฝึกอบรมหรือให้ความรู้ที่เพียงพอ	0.647
ปัจจัย 4: การตระหนักถึงความปลอดภัย (Variance = 12.277, α = 0.613) ท่านมักจะมีการสำรองข้อมูลที่สำคัญ ไว้หลายๆ แห่งเสมอ เพื่อป้องกันการสูญหาย	0.729
เมื่อท่านได้รับ E-mail ที่กล่าวว่าส่งจากองค์กรที่น่าเชื่อถือ ให้ไปที่ link ตามที่แนบมากับ mail เพื่อยืนยันข้อมูลส่วนบุคคลของท่าน ท่านจะไม่ไปที่ link ดังกล่าวโดยทันที	0.824
หากท่านกำหนดรหัสผ่านในเครื่องคอมพิวเตอร์ส่วนบุคคลของท่าน ท่านจะคิดว่ารหัสผ่านดังกล่าวควรมีระดับความปลอดภัยมากน้อยแค่ไหน	0.568
ปัจจัย 5: พฤติกรรมการใช้ระบบสารสนเทศในองค์กร (Variance = 9.935, α = 0.613) ท่านให้ความสำคัญกับการจัดเก็บข้อมูลที่เป็นความลับขององค์กร	0.64
ท่านปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยในองค์กร	0.743
เมื่อปรากฏ pop up หรือหน้าต่างแจ้งเตือน ปรากฏขึ้นมาระหว่างการใช้เครื่องคอมพิวเตอร์ ท่านจะอ่านข้อความเหล่านั้นให้เข้าใจก่อนทำการ click ตัวเลือกใดๆ ก่อนเสมอ	0.692
หากท่านติดตั้งโปรแกรมสแกนไวรัสไว้ที่เครื่องคอมพิวเตอร์ส่วนบุคคลของท่าน ท่านจะทำการสแกนไวรัสเครื่องคอมพิวเตอร์ส่วนบุคคลทุกครั้งที่ท่านใช้งานเครื่องคอมพิวเตอร์	0.703

ตารางที่ 1 Factor analysis ของตัวแปรในงานวิจัย (ต่อ)

ปัจจัย	น้ำหนักตัวประกอบ (Factor Loading)
ปัจจัย 6: ระดับการรักษาความมั่นคง (Variance = 10.333, α = 0.727) ระบบสารสนเทศในองค์กรของท่าน มีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลที่แตกต่างกัน เช่น ระดับผู้บริหาร และระดับปฏิบัติการ เป็นต้น	.520
องค์กรของท่านมีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นลายลักษณ์อักษร	.765
องค์กรของท่านมีการประกาศหรือแจ้งนโยบายดังกล่าวให้บุคลากรรับทราบ	.784
ผู้บริหารมีการสนับสนุนการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภับของระบบสารสนเทศ หรือไม่ (เช่น งบประมาณ บุคลากร อุปกรณ์ เป็นต้น)	.630
องค์กรของท่านมีการดูแลด้านความมั่นคงปลอดภัย เมื่อมีการว่าจ้างหน่วยงานภายนอก (Outsource) เพื่อปรับปรุงระบบสารสนเทศขององค์กร	.598

5.2 การวิเคราะห์ผลการวิจัย

การทดสอบสมมติฐานการวิจัยในครั้งนี้ ผู้วิจัยใช้วิธีวิเคราะห์การถดถอยเชิงเส้นเดียว (Simple linear regression) และการวิเคราะห์การถดถอยพหุคูณ (Multiple regression) โดยใช้ค่า p-value ที่น้อยกว่าหรือเท่ากับ 0.05 เป็นตัวกำหนดนัยสำคัญทางสถิติ โดยแบ่งการวิเคราะห์ออกเป็น 4 ส่วน ตามกรอบแนวคิดการวิจัยดังนี้

ส่วนที่ 1 การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปร การรับรู้ถึงภัยคุกคาม และ การฝึกอบรมและให้ความรู้ กับ ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ พบว่ามีความสัมพันธ์โดยตรงกับตัวแปรตาม คือ ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ โดยค่า R = 0.258 และสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 6.7 (R^2 = 0.067) นอกจากนี้ผลการวิเคราะห์ความถดถอยยังแสดงให้เห็นว่าตัวแปรอิสระกำหนดตัวแปรตาม คือ ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ที่ระดับนัยสำคัญ p = 0.000 ($F_{(1.237)}$ = 8.479) (ดังแสดงในตารางที่ 2-3) ซึ่งสอดคล้องกับงานวิจัยของ Bulgurcu et al. (2010) ที่กล่าวว่าเมื่อบุคคลรับรู้ถึงความกลัวแล้วจะส่งผลให้บุคคลนั้นหาความรู้เพิ่มเติมเพื่อให้ตนเองเกิดความรู้ความเข้าใจ และ Son and Jeong (2013) ได้กล่าวว่าการฝึกอบรมทำให้ผู้ใช้มีความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร

ตารางที่ 2 ค่าสถิติการวิเคราะห์การถดถอย (Regression model) ของความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	**5.028**	**2**	**2.514**	**8.479**	**0.000***
Residual	70.268	237	.296		
Total	75.296	239			

* p < 0.05

ตารางที่ 3 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ

ตัวแปร	ค่าสัมประสิทธิ์ถดถอย (b)	ค่าสัมประสิทธิ์ถดถอยปรับมาตรฐาน (beta)	T	Sig.
ค่าคงที่	**2.320**		**7.082**	**0.000**
การรับรู้ถึงภัยคุกคาม	.131	.127	1.977	0.049
การฝึกอบรมและให้ความรู้	.253	.247	3.585	0.000

หมายเหตุ * $p < 0.05$

$R = .258$, $R^2 = .067$, $SE = .544$

ส่วนที่ 2 การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปร ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ และการตระหนักถึงความปลอดภัย พบว่ามีความสัมพันธ์โดยตรงกับตัวแปรตาม คือ การตระหนักถึงความปลอดภัย โดยค่า $R = 0.237$และสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 5.6 ($R^2 = 0.056$) นอกจากนี้ผลการวิเคราะห์ความถดถอยยังแสดงให้เห็นว่าตัวแปรอิสระกำหนดตัวแปรตาม คือ ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ที่ระดับนัยสำคัญ $p = 0.000$ ($F_{(1.238)} = 14.145$) (ดังแสดงในตารางที่ 4-5) ซึ่งสอดคล้องกับงานวิจัยของ Liang and Xue (2009) ได้กล่าวว่าหากผู้ใช้มีความรู้และเข้าใจถึงการใช้งานสารสนเทศในองค์กร ว่าการใช้งานอย่างไรก่อให้เกิดเป็นอันตรายได้นั้น ผู้ใช้จะตระหนักถึงอันตราย

ตารางที่ 4 ค่าสถิติการวิเคราะห์การถดถอย (Regression model) ของ การตระหนักถึงความปลอดภัย

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	**3.407**	**1**	**3.407**	**14.145**	**0.000***
Residual	57.326	238	.241		
Total	60.733	239			

* $p < 0.05$

ตารางที่ 5 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของการตระหนักถึงความปลอดภัย

ตัวแปร	ค่าสัมประสิทธิ์ถดถอย (b)	ค่าสัมประสิทธิ์ถดถอยปรับมาตรฐาน (beta)	T	Sig.
ค่าคงที่	**3.041**		**15.224**	**0.000**
ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ	.213	.237	3.761	0.000

หมายเหตุ * $p < 0.05$

$R = .237$, $R^2 = .056$, $SE = .490$

ส่วนที่ 3 การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปร การตระหนักถึงความปลอดภัย และ พฤติกรรมการใช้ระบบสารสนเทศในองค์กร พบว่ามีความสัมพันธ์โดยตรงกับตัวแปรตาม คือ พฤติกรรมการใช้ระบบสารสนเทศในองค์กร โดยค่า $R = 0.325$และสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 10.6 ($R^2 = 0.106$) นอกจากนี้ผลการวิเคราะห์ความถดถอยยังแสดงให้เห็นว่าตัวแปรอิสระกำหนดตัวแปรตาม คือ พฤติกรรมการใช้ระบบสารสนเทศในองค์กร ที่ระดับนัยสำคัญ $p = 0.000$ ($F_{(1.238)} = 28.080$) (ดังแสดงในตารางที่ 6-7) ซึ่งสอดคล้องกับงานวิจัยของ Liang and Xue (2009) ได้กล่าวว่า เมื่อบุคคลตระหนักได้ว่ากำลังเผชิญอยู่กับภัยคุกคาม บุคคลจะมีส่วนร่วมในการหลีกเลี่ยงภัยคุกคาม นั่นคือ เกิดเป็นพฤติกรรมเพื่อลดการเกิดภัยคุกคามจนกว่าภัยคุกคามที่เกิดขึ้นจะหายไป

ตารางที่ 6 ค่าสถิติการวิเคราะห์การถดถอย (Regression model) ของ พฤติกรรมการใช้ระบบสารสนเทศในองค์กร

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	**6.371**	**1**	**6.371**	**28.080**	**0.000***
Residual	54.001	238	.227		
Total	60.373	239			

* $p < 0.05$

ตารางที่ 7 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของ พฤติกรรมการใช้ระบบสารสนเทศในองค์กร

ตัวแปร	ค่าสัมประสิทธิ์ถดถอย (b)	ค่าสัมประสิทธิ์ถดถอยปรับมาตรฐาน (beta)	T	Sig.
ค่าคงที่	**2.896**		**12.416**	**0.000**
การตระหนักถึงความปลอดภัย	.324	.325	5.299	0.000

หมายเหตุ * $p < 0.05$

$R = .325$, $R^2 = .106$, $SE = .476$

ส่วนที่ 4 การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปร การตระหนักถึงความปลอดภัย และ พฤติกรรมการใช้ระบบสารสนเทศในองค์กร กับ ระดับการรักษาความมั่นคงปลอดภัย พบว่ามีความสัมพันธ์โดยตรงกับตัวแปรตาม คือ ระดับการรักษาความมั่นคงปลอดภัย โดยค่า R = 0.510 และสามารถอธิบายความผันแปรของตัวแปรตามได้ร้อยละ 26.1 (R^2 = 0.261) นอกจากนี้ผลการวิเคราะห์ความถดถอยยังแสดงให้เห็นว่าตัวแปรอิสระกำหนดตัวแปรตาม คือ ระดับการรักษาความมั่นคงปลอดภัย ที่ระดับนัยสำคัญ p = 0.000 ($F_{(1.237)}$ = 41.751) (ดังแสดงในตารางที่ 8-9) ซึ่งสอดคล้องกับงานวิจัยของ Bulgurcu et al. (2010) ได้กล่าวว่า เมื่อทุกคนในองค์กรตระหนักถึงความมั่นคงปลอดภัยของระบบสารสนเทศ จะส่งผลให้องค์กรมีระดับ การรักษาความมั่นคงปลอดภัยที่สูงขึ้น และ Gadzama et al. (2014) ได้กล่าวว่าพฤติกรรมการใช้ระบบสารสนเทศส่งผลต่อความมั่นคงปลอดภัยขององค์กร

ตารางที่ 8 ค่าสถิติการวิเคราะห์การถดถอย (Regression model) ของ ระดับการรักษาความมั่นคงปลอดภัย

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	**25.735**	**2**	**12.868**	**41.751**	**0.000***
Residual	73.044	237	.308		
Total	98.780	239			

* p < 0.05

ตารางที่ 9 ผลการวิเคราะห์การถดถอยแบบปกติ (Coefficients) ของ ระดับการรักษาความมั่นคงปลอดภัย

ตัวแปร	ค่าสัมประสิทธิ์ถดถอย (b)	ค่าสัมประสิทธิ์ถดถอยปรับมาตรฐาน (beta)	T	Sig.
ค่าคงที่	**1.050**		**3.009**	**0.000**
การตระหนักถึงความปลอดภัย	.311	.244	3.884	0.003
พฤติกรรมการใช้ระบบสารสนเทศในองค์กร	.606	.474	8.025	0.000

หมายเหตุ * p < 0.05

R = .510, R^2 =.261, SE = .555

6. สรุปผลการวิจัย

งานวิจัยนี้จัดเก็บข้อมูลจากแบบสอบถามในรูปแบบออนไลน์ และนำข้อมูลที่เก็บรวบรวมมาวิเคราะห์ผลทางสถิติ ซึ่งจากการวิจัยพบว่าหากทำให้พนักงานรับรู้ถึงอันตรายที่อาจเกิดขึ้นพร้อมทั้งมีการฝึกอบรมให้แก่พนักงานแล้วนั้นจะส่งผลต่อความเข้าใจของพนักงาน และเมื่อพนักงานเกิดความเข้าใจถึงวิธีการรักษาความมั่นคงปลอดภัยจากการใช้ระบบสารสนเทศจะทำให้พนักงานเกิดการตระหนักถึงการใช้ระบบสารสนเทศดังกล่าว และนำไปสู่พฤติกรรมการใช้งานที่คำนึงถึงความปลอดภัย สุดท้ายส่งผลให้องค์กรมีระดับการรักษาความมั่นคงปลอดภัยที่สูงขึ้นตามไปด้วย

เนื่องจากปัจจุบัน สารสนเทศเข้ามามีบทบาทสำคัญยิ่งต่อองค์กรหลายแห่ง บางองค์ใช้ระบบสารสนเทศเป็นหลักในการขับเคลื่อนธุรกิจให้มีการเจริญเติบโต และใช้ระบบสารสนเทศเก็บข้อมูลต่างๆ ขององค์กร ดังนั้นองค์กรจึงต้องเห็น

ความสำคัญในการรักษาความมั่นคงปลอดภัย ของการใช้ระบบสารสนเทศเพื่อปกป้องข้อมูลให้มีความปลอดภัยอยู่เสมอ ซึ่งสามารถสรุปประโยชน์ที่ได้รับจากงานวิจัยได้ ดังนี้

(1) ผลของงานวิจัยแสดงให้เห็นว่าระดับการรักษาความมั่นคงปลอดภัยนอกจากจะขึ้นอยู่กับ การรับรู้ถึงภัยคุกคาม และ พฤติกรรมการใช้ระบบสารสนเทศในองค์กร ตามทฤษฎีพฤติกรรมตามแผน ยังขึ้นอยู่กับปัจจัยด้าน ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ การฝึกอบรมและให้ความรู้ และ การตระหนักถึงความปลอดภัย ซึ่งเป็นปัจจัยที่ได้จากการทบทวนวรรณกรรม เพื่อเสริมเข้าไปในทฤษฎีพฤติกรรมตามแผน

(2) งานวิจัยนี้สามารถประยุกต์ใช้ในแง่ของธุรกิจต่อองค์กรอื่นๆที่มีรายชื่อจดทะเบียนในตลาดหลักทรัพย์ได้ ซึ่งผลของการวิจัยทำให้ทราบว่าหากพนักงานในองค์กรมีความตระหนักถึงความปลอดภัยแล้วจะส่งผลให้องค์กรมีระดับการรักษาความมั่นคงปลอดภัยที่เพิ่มขึ้นดังนั้นองค์กรจึงต้องเพิ่มปัจจัยต่างๆที่จะทำให้พนักงานเกิดความตระหนักมากขึ้น ได้แก่การทำให้พนักงานรับรู้ถึงภัยคุกคามและมีความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยโดยการจัดการฝึกอบรมและให้ความรู้แก่พนักงาน หรือมีการประชาสัมพันธ์ให้พนักงานทุกคนในองค์กรทราบถึงวิธีการรักษาความมั่นคงปลอดภัยเบื้องต้น และส่วนที่สำคัญก็คือ การที่ผู้บริหารเห็นความสำคัญในการรักษาความมั่นคงปลอดภัยต่อระบบสารสนเทศในองค์กร

งานวิจัยนี้ศึกษาอิทธิพลที่มีต่อระดับการรักษาความมั่นคงปลอดภัยของการใช้ระบบสารสนเทศในองค์กร ซึ่งศึกษาเฉพาะกลุ่มพนักงานที่ทำงานในองค์กรที่มีการจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทยเท่านั้น ดังนั้นงานวิจัยในอนาคตควรศึกษาเพิ่มเติม ในกลุ่มองค์กรอื่นๆ เช่น หน่วยงานรัฐบาล หน่วยงานรัฐวิสาหกิจ หรือ บริษัทข้ามชาติ เป็นต้น นอกจากนี้ ระเบียบวิธีวิจัยจากงานวิจัยนี้เป็นรูปแบบงานวิจัยเชิงปริมาณที่เก็บรวบรวมข้อมูลโดยการสำรวจ จากการทำแบบสอบถามและนำข้อมูลที่ได้มาวิเคราะห์ผลทางสถิติ จึงควรศึกษาในรูปแบบงานวิจัยเชิงคุณภาพเพิ่มเติม ซึ่งเป็นการวิจัยที่ไม่เน้นข้อมูลตัวเลข แต่เน้นการหารายละเอียดต่างๆ ของกลุ่มประชากรที่ทำการศึกษาจึงก่อให้เกิดความรู้ความเข้าใจอย่างลึกซึ้งในเรื่องนั้นๆ เพื่อค้นหาปัจจัยที่ส่งผลให้พนักงานเกิดความตระหนักและส่งผลให้มีระดับการรักษาความมั่นคงปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กรเพิ่ม มากขึ้น

จากผลการวิจัยทำให้พบว่าปัจจัยที่ได้กล่าวมาทั้งหมด อาจจะยังไม่ใช่ปัจจัยทั้งหมดที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัย จากค่าทางสถิติที่สามารถอธิบายความผันแปรของตัวแปรตามไม่มากนัก จึงแสดงให้เห็นว่าปัจจัยในกรอบการวิจัยนี้ยังไม่ครอบคลุมถึงปัจจัยที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยทั้งหมด ผู้สนใจสามารถทำการศึกษาเพิ่มเติมว่ามีปัจจัยอื่นใด ที่จะส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยอีกหรือไม่

บรรณานุกรม

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2557). วิธีปฏิบัติตนเมื่อเกิดภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศ. ดึงข้อมูลวันที่ 20 มิถุนายน 2557, จาก http://www.ictkm.info/content /detail/112.html.

กัลยา วานิชย์บัญชา. (2552). สถิติสำหรับงานวิจัย (พิมพ์ครั้งที่ 4). กรุงเทพฯ: โรงพิมพ์แห่งจุฬาลงกรณ์ มหาวิทยาลัย.

จักรกริช ใจดี. (2542). *ความเข้าใจเกี่ยวกับประชาธิปไตย ของนิสิตมหาวิทยาลัยเกษตร*. กรุงเทพมหานคร: วิทยานิพนธ์ปริญญาโท, มหาวิทยาลัยเกษตรศาสตร์.

ภัททิยา นภาชัยเทพ. (2555). *การตระหนักถึงความเป็นส่วนตัวในการใช้เฟซบุ๊ก.* วิทยานิพนธ์ที่ยังไม่ได้ตีพิมพ์, มหาวิทยาลัยธรรมศาสตร์.

สิงหะ ฉวีสุข และ สุนันทา วงศ์จตุรภัทร. (2555). *ทฤษฎีการยอมรับการใช้เทคโนโลยีสารสนเทศ*. วิทยานิพนธ์ที่ ยังไม่ได้ตีพิมพ์, สถาบันพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: Anempirical Study Of Rationality-Based Beliefsand Information Security Awareness. *MIS Quarterly*, 34(3), 523-548.

Crossler, E. R., Johnston, C. A., Lowry, B. P., Hu, Q., Warkentin, M., and Baskerville, R. (2013). Future directions for behavioral information security research. *ELSEVIER*, 32, 90-101.

Gadzama, W. A., Katuka, J. I., Gambo, Y., Abali, A. M., and Usman, M. J. (2014). Evaluation of employees awareness and usage of information security policy in organizations of developing countries: a study of federal inland revenue service. Journal of Theoretical and Applied Information Technology, 67(2), 443-460.

Gore, T. D., and Bracken, C. C. (2005). Testing the theoretical design of a health risk message: Reexamining the major tenets of the extended parallel process model. *Health Education and Behavior*, 32(1), 27-41.

Hale, Gr. (2012). SCADA Security is a Mindset. Retrieved April 20, 2015 from https://www.tofinosecurity.com/blog/scada-security-mindset-isssource-explains-why-belden-design-seminar.

Kruger, H., Flowerday, S., Drevin, L., and Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness. *IEEE*, 978-984.

Liang, H., and Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, 33(1), 71-90.

Maqousi, A., Balikhina, T., Meridji, K., and Al-Sarayreh, Kh. T. (2014). A reference model of security requirements for early identification and measurement of security awareness program. *Journal of Theoretical and Applied Information Technology*, 63(1), 74-84.

Puhakainen, P., and Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 34(4), 757-778.

Rocha Flores, W., Antonsen, E., and Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security, 43, 90–110.

Solic, K., Tovjanin, B., and Ilakovac, V. (2012). Assessment Methodology for the Categorization of ICT System Users Security Awareness. *MIPRO*, 1560-1564.

Son, H. J., and Jeong, S. (2013). A Research on Security Awareness and Countermeasures for the Single Server. *International Journal of Security and Its Applications*, 7(6), 31-42.

แนวทางในการเสริมสร้างความตระหนักถึงการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล

สลิสา เอียดสุย*
ธนาคารกสิกรไทย จำกัด (มหาชน)
ศากุน บุญอิต
สาขาวิชาบริหารการปฏิบัติการ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

***Correspondence:** pickzpickz@gmail.com
doi: 10.14456/jisb.2016.12

บทคัดย่อ

ในปัจจุบันหลายองค์กรได้มีแนวความคิดที่อนุญาตให้พนักงานสามารถนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนบุคคลมาใช้ในการทำงานขององค์กรมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง ในขณะเดียวกันหลายองค์กรต่างตระหนักดีว่าพนักงานเป็นจุดอ่อนที่สำคัญที่ทำให้เกิดการรั่วไหลของสารสนเทศหรือแม้กระทั่งขาดความตระหนักในความเสี่ยงที่เกี่ยวข้องกับการใช้สื่อสังคมออนไลน์ผ่านอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนบุคคล อาจทำให้บุคลากรตกเป็นเหยื่อของการขโมยสารสนเทศ ซึ่งความเสี่ยงเหล่านี้สามารถทำให้เกิดความเสียหายอย่างมีนัยสำคัญต่อชื่อเสียง ความน่าเชื่อถือขององค์กรหรือแม้กระทั่งข้อได้เปรียบทางการแข่งขัน องค์กรจะต้องมุ่งเน้นการรักษาความปลอดภัยข้อมูลโดยสร้างนโยบายการรักษาความปลอดภัยข้อมูลเพื่อเป็นแนวทางสำหรับพนักงานในการปฏิบัติงาน ดังนั้นองค์กรจึงจำเป็นจะต้องทำความเข้าใจถึงปัจจัยที่กระตุ้นให้พนักงานปฏิบัติตามกฎระเบียบการรักษาความปลอดภัยข้อมูลขององค์กร เพื่อสนับสนุนการตระหนักถึงการรักษาความปลอดภัยข้อมูลขององค์กรให้สอดคล้องกับแนวทางการประกอบธุรกิจขององค์กร

การวิจัยนี้ใช้การสำรวจโดยใช้แบบสอบถามเป็นเครื่องมือในการรวบรวมข้อมูล ซึ่งจากกลุ่มตัวอย่างจำนวน 447 ราย จากประชากรไทยที่ทำงานทั้งในองค์กรทั้งภาครัฐและภาคเอกชนและสามารถนำอุปกรณ์สมาร์ทโฟนส่วนบุคคลไปใช้ในที่ทำงานได้ พบว่าทัศนคติที่มีต่อการปฏิบัติตามนโยบายของพนักงาน ความเชื่อเกี่ยวกับกลุ่มอ้างอิงของพนักงาน การรับรู้ความสามารถในการควบคุมพฤติกรรมของพนักงาน ความตระหนักต่อการรักษาความปลอดภัยข้อมูลของพนักงานมีความสัมพันธ์เชิงบวกต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล

ผลจากการวิจัยนี้ นอกจากจะทำให้ทราบว่าความตระหนักต่อการรักษาความปลอดภัยข้อมูลของพนักงานนำมาซึ่งการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคลแล้ว ยังทำให้เห็นว่าทัศนคติมีบทบาทในการทำหน้าที่เป็นสื่อตัวกลางเพียงบางส่วน (Partial mediator) ในการอธิบายความสัมพันธ์ระหว่างความตระหนักถึงความปลอดภัยข้อมูลและความตั้งใจต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กร

คำสำคัญ: การปฏิบัติตามระเบียบ การรักษาความปลอดภัย อุปกรณ์สมาร์ทโฟน

Information Security Policy Compliance: an Empirical Study of Information Security Awareness on Smartphone Devices

Salisa Adsuy*

Kasikornbank Public Company Limited

Sakun Boon-It

Operations Management Program, Thammasat Business School, Thammasat University

***Correspondence:** pickzpickz@gmail.com

doi: 10.14456/jisb.2016.12

Abstract

An increasingly trend of many organizations nowadays is allowing employees to bring personal mobile devices into organizational workspaces, meanwhile those organizations have realized that, the employees are also a weakest link of information security. The employees often lack the information security awareness, especially when surfing social medias thru their smartphones. Consequencely, the organizational information, including sensitive data or even employee's profiles, can be disclosure by unintention. The cost can be effect to a privacy of individuals, the reliability and reputation of organizations, and eventually lossing of competitive opportunity. Therefore, the organizations would realize factors to encourage their employees to comply with the information security policy rigorously.

This work studies the factors by questionaires in order to collect employee's opinion, and then process the collected data by SPSS program. The poll is collected from 447 Thai participants, who work for various organizations including both government and private sectors. According to the results, we found the factors - attitude towards behaviour, social influence, self-efficacy, and information security awareness - have positive significants to the intention to comply with organizational information security policy, when employees surf social medias thru personal smartphones in organizational workspaces.

By the results, despite the information security awareness positively related to intention to comply with the information security policy, we found that, the employee's attitude is a partial mediator for explaining the relation between the information security awareness and the intention to comply with information security policy.

Keywords: Compliance, Security, Smartphone Devices

1. บทนำ

ในปัจจุบันหลายองค์กรได้มีแนวความคิดที่อนุญาตให้พนักงานสามารถนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนบุคคล เช่น โน๊ตบุ๊ก สมาร์ทโฟน และ แท็บเล็ต มาใช้ในการทำงานขององค์กร มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง (ประภาดา ตลึงจิตร, 2555) ดังจะเห็นได้จากงานวิจัยของ Cisco IBSG ที่ระบุว่าการเติบโตของแนวคิดการนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนบุคคลมาใช้ในการทำงาน (Bring Your Own Device หรือ BYOD) ของประเทศชั้นนำระดับโลก มีอัตราเติบโตสูงขึ้นร้อยละ 105 ระหว่างปี ค.ศ. 2013-2016 และผลสำรวจจากผู้บริหารระดับสูง CIO (Chief Information Officer) ทั่วโลกต่างระบุตรงกันว่าบุคลากรนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนบุคคลมาใช้ในที่ทำงาน ซึ่งเกี่ยวข้องกับงานทั้งสิ้น คิดเป็น ร้อยละ 28 (ธนาคารแห่งประเทศไทย, 2556) ส่วนในประเทศไทยก็มีองค์กรจำนวนไม่น้อยที่พนักงานนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการทำงาน ซึ่งมีทั้งที่ผู้บริหารขององค์กรรับทราบพร้อมทั้งอนุญาตให้นำมาใช้งานอย่างเป็นทางการ และไม่รับทราบต่อการนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการทำงาน (ประจิต หาวัตร, 2556; อัครา วัฒนโยธิน, 2553) ผู้บริหารขององค์กรจึงควรทำความเข้าใจถึงแนวคิดการนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการทำงาน ทั้งในด้านคุณประโยชน์ และด้านความเสี่ยงต่อการรั่วไหลของข้อมูลสารสนเทศองค์กร (Allam et al., 2014) โดยข้อมูลสารสนเทศเป็นสิ่งสำคัญที่องค์กรจะนำมาใช้ในการบริหารจัดการ พัฒนากระบวนการทำงาน และสร้าง ความได้เปรียบทางการแข่งขันขององค์กร หากบุคลากรสามารถเข้าถึงข้อมูลสารสนเทศขององค์กรได้ทุกที่ทุกเวลาก็จะช่วยเพิ่มประสิทธิภาพในการทำงานให้แก่องค์กรมากยิ่งขึ้น (Allam et al., 2014) ในขณะเดียวกันหลายองค์กรต่างตระหนักดีว่าบุคลากรเป็นจุดอ่อนที่สำคัญที่ทำให้เกิดการรั่วไหลของข้อมูลสารสนเทศ (Haeussinger and Kranz, 2013; Ifinedo, 2012; Toshihiko Takemura, 2013) หรือแม้กระทั่งขาดความตระหนักในความเสี่ยงที่เกี่ยวข้องกับการใช้สื่อสังคมออนไลน์ผ่านอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนบุคคล (Fagnot and Paquette, 2012) ได้ในหลายกรณี เช่น อุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนบุคคลสูญหาย (ประภาดา ตลึงจิตร, 2555) หรือบุคลากรขาดความตระหนักในการดูแลอุปกรณ์หรือติดตั้งซอฟแวร์ที่สำคัญ (Ifinedo, 2012) อาจทำให้บุคลากรตกเป็นเหยื่อของการขโมยข้อมูลสารสนเทศหรืออาจจะเผยแพร่ข้อมูลสารสนเทศขององค์กรโดยตั้งใจหรือไม่ได้ตั้งใจ (อัครา วัฒนโยธิน, 2553) หากอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวไม่มีการป้องกันไว้อย่างดีก็อาจเป็นช่องโหว่ที่ทำให้ระบบเครือข่ายหรือข้อมูลสารสนเทศขององค์กรโดนโจมตีได้ง่ายยิ่งขึ้น (Bertot et al., 2012; อัครา วัฒนโยธิน, 2553) หรือบุคลากรละเมิดกฎระเบียบและข้อบังคับขององค์กรเกี่ยวกับการรักษาความปลอดภัยข้อมูล (Information Security Policy หรือ ISP) (BRohme, 2013; Cheng et al., 2013; Lebek et al., 2013) เป็นต้น ซึ่งความเสี่ยงเหล่านี้จะสามารถทำให้เกิดความเสียหายอย่างมีนัยสำคัญต่อชื่อเสียงขององค์กร ความน่าเชื่อถือขององค์กร ความเสียหายที่เป็นตัวเงิน หรือแม้กระทั่งข้อได้เปรียบทางการแข่งขัน (Webb et al., 2014)

องค์กรจึงพยายามที่จะลดความเสี่ยงที่เกี่ยวข้องกับการรักษาความปลอดภัยข้อมูล (Lebek et al., 2013) หลายองค์กรมักจะพึ่งพาเทคโนโลยีเข้ามาช่วยบรรเทาความเสี่ยง มีการลงทุนกับ Firewall , VPN , Anti-Virus Solution และอื่นๆ อีกเป็นจำนวนเงินมหาศาล (อัครา วัฒนโยธิน, 2553) ถึงแม้ว่าการแก้ไขปัญหาเหล่านั้นจะช่วยปรับปรุงการรักษาความปลอดภัยข้อมูลขององค์กร แต่ผลลัพธ์ที่ได้ไม่เป็นไปตามที่คิดไว้ ซึ่งปัญหาส่วนใหญ่มาจากการขาดความร่วมมือของพนักงานที่อาจจะไม่เข้าใจในเรื่องของการรักษาความปลอดภัยข้อมูลที่ดี (ประภาดา ตลึงจิตร, 2555; อัครา วัฒนโยธิน, 2553) องค์กรจะต้องมุ่งเน้นการรักษาความปลอดภัยข้อมูลโดยสร้างนโยบายการรักษาความปลอดภัยข้อมูลเพื่อเป็นแนวทางสำหรับพนักงานในการปฏิบัติงาน (Al-Omari et al., 2013) อย่างไรก็ตามในขณะที่การสร้างนโยบายการรักษาความปลอดภัยข้อมูลและแนวทางสำหรับการปฏิบัติงานที่จำเป็น อาจจะยังไม่เพียงพอที่จะทำให้แน่ใจว่าพนักงานขององค์กรจะปฏิบัติตามนโยบายหรือปฏิบัติตามกฎระเบียบ (Gritzalis et al., 2014)

ดังนั้นองค์กรจึงจำเป็นจะต้องทำความเข้าใจถึงปัจจัยที่กระตุ้นให้พนักงานปฏิบัติตามกฎระเบียบการรักษาความปลอดภัยข้อมูลขององค์กร (Bulgurcu et al., 2010) เพื่อสนับสนุนการตระหนักถึงการรักษาความปลอดภัยข้อมูลขององค์กร (Information security awareness หรือ ISA) ให้สอดคล้องกับแนวทางการประกอบธุรกิจขององค์กรและอ้างอิงตามนโยบายการรักษาความปลอดภัยขององค์กร (Anderson and Agarwal, 2010; Mani et al., 2014) ถึงแม้ว่าบทบาทความสำคัญของการตระหนักถึงการรักษาความปลอดภัยข้อมูล(Information security awareness) จะได้รับการยอมรับอย่างแพร่หลายแต่ความเข้าใจต่อปัจจัยที่มีอิทธิพลต่อการตระหนักถึงการรักษาความปลอดภัยข้อมูล (Information security awareness) ยังขาดแคลน (Bulgurcu et al., 2010)

การวิจัยฉบับนี้จัดทำขึ้นเพื่อศึกษาปัจจัยเกี่ยวกับ นโยบายการรักษาความปลอดภัยข้อมูล (Information Security Policy) องค์ความรู้ (Knowledge) จะอ้างถึงสิ่งที่พนักงานรู้ ทัศนคติ (Attitude) จะมุ่งเน้นในสิ่งที่พนักงานคิด และพฤติกรรม (Behavior) จะเกี่ยวกับสิ่งที่พนักงานทำ โดยยึดทฤษฎีพฤติกรรมตามแบบแผน (Theory of Planned Behavior) เป็นพื้นฐาน และเพื่อศึกษาความสัมพันธ์ระหว่างการตระหนักถึงการรักษาความปลอดภัยข้อมูลส่วนบุคคล (Information security awareness's antecedents) และความตั้งใจที่จะปฏิบัติตามกฎระเบียบและข้อบังคับขององค์กร (Intention to Comply with the security policies) เพื่อเป็นแนวทางในการเสริมสร้างนโยบายการรักษาความปลอดภัยข้อมูลสำหรับองค์กรและให้พนักงานเกิดการตระหนักในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรและนำไปสู่ความตั้งใจที่จะปฏิบัติตาม

2. ทบทวนวรรณกรรม

จากการศึกษางานวิจัยในอดีตที่เกี่ยวข้อง เนื่องจากนโยบาย กฎระเบียบและข้อบังคับขององค์กรเป็นสิ่งที่กำหนดขึ้นมาเพื่อเป็นแนวทางสำหรับการแสดงพฤติกรรมของพนักงานขององค์กร ดังนั้นวิธีการนำนโยบายมาบังคับใช้จะมีความสำคัญอย่างมากต่อการยอมรับนโยบายนั้นในองค์กร เพื่อให้เข้าใจพฤติกรรมของมนุษย์และวิธีการสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรและนำไปสู่ความตั้งใจที่จะปฏิบัติตาม จึงได้ศึกษาทฤษฎีเชิงพฤติกรรม (Behavior Research)

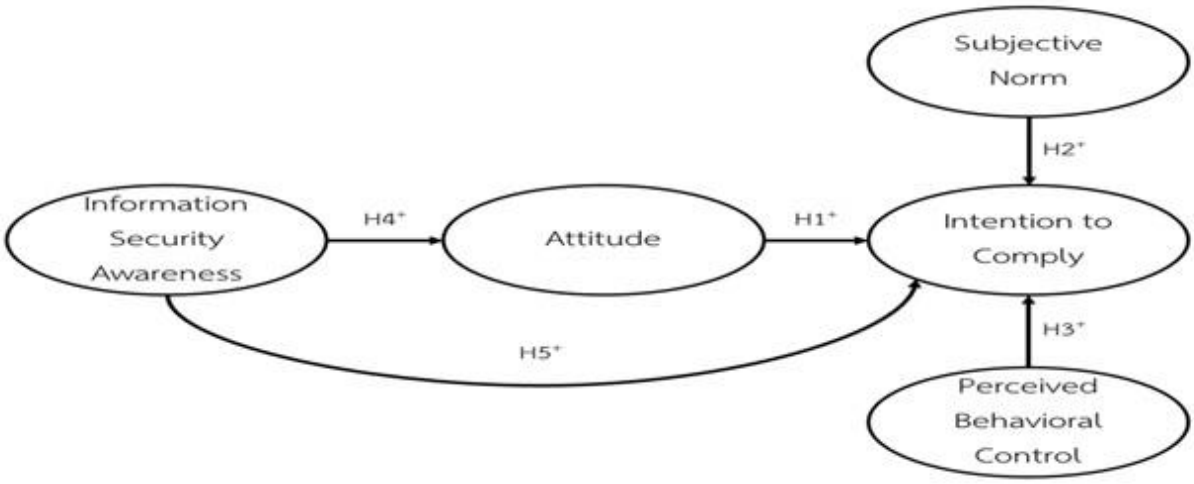
ทฤษฎีพฤติกรรมตามแผน (Theory of Planned Behavior หรือ TPB) นำเสนอโดย (Ajzen, 1991) จัดอยู่ในกลุ่มของทฤษฎีเชิงพฤติกรรม (Bulgurcu et al., 2010; Lebek et al., 2013) พัฒนามาจากทฤษฎีการกระทำตามหลักเหตุและผล (The Theory of Reasoned Action หรือ TRA) นำเสนอโดย (Ajzen and Fishbein, 1980) ซึ่งทฤษฎีดังกล่าวถูกนำมาใช้เป็นพื้นฐานสำหรับการศึกษาพฤติกรรมของมนุษย์มากที่สุด (Lebek et al., 2013; Toshihiko Takemura, 2013; สิงหะ ฉวีสุข และสุนันทา วงศ์จตุรภัทร, 2555)

หลักการของทฤษฎีพฤติกรรมตามแผนเป็นการรับรู้ของแต่ละบุคคลเพื่อที่จะแสดงพฤติกรรมที่ได้รับแรงขับเคลื่อนจากความตั้งใจ (Bulgurcu et al., 2010; Lebek et al., 2013) เพื่อแสดงพฤติกรรมใดๆของบุคคลสามารถคาดการณ์ได้จากทัศนคติต่อพฤติกรรม (Attitude toward behavior) ความเชื่อเกี่ยวกับกลุ่มอ้างอิง (Subjective Norm) และการรับรู้ความสามารถในการควบคุมพฤติกรรม (Perceived Behavioral Control) (Lebek et al., 2013; ประภาดา ตลึงจิตร, 2555; สิงหะ ฉวีสุข และสุนันทา วงศ์จตุรภัทร, 2555) พบว่าความตั้งใจจะได้รับอิทธิพลจากทัศนคติที่มีต่อพฤติกรรม (Attitude toward behavior) ความเชื่อเกี่ยวกับกลุ่มอ้างอิง (Subjective Norm) และการรับรู้ความสามารถในการควบคุมพฤติกรรม (Perceived Behavioral Control) และความตั้งใจมีอิทธิพลโดยตรงกับพฤติกรรม

จากทฤษฎีพฤติกรรมตามแผน แนวทางในการเสริมสร้างความตระหนักถึงการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล จะเกิดขึ้นได้ ปัจจัยแรกคือ พนักงาน

จะต้องมีความเชื่อว่าความตระหนักถึงกฎระเบียบและข้อบังคับขององค์กรเกี่ยวกับการรักษาความปลอดภัยข้อมูล (Information Security Policy) จะก่อให้เกิดประโยชน์ต่อตนเองและองค์กร เมื่อพนักงานมีทัศนคติที่ดีต่อกฎระเบียบและข้อบังคับขององค์กรแล้ว พนักงานก็จะมีความตั้งใจที่จะปฏิบัติตามกฎระเบียบ ปัจจัยที่สองคือ พนักงานเห็นว่าเพื่อนร่วมงานได้กระทำตามกฎระเบียบและข้อบังคับขององค์กรเกี่ยวกับการรักษาความปลอดภัยข้อมูล พนักงานก็จะแนวโน้มที่จะแสดงพฤติกรรมเหล่านั้นด้วย ปัจจัยที่สามคือ พนักงานสามารถรับรู้ความสามารถในการควบคุมพฤติกรรมถึงการปฏิบัติตามกฎระเบียบและข้อบังคับขององค์กร รวมถึงผลให้เป็นไปตามที่ต้องการ พนักงานก็จะมีความตั้งใจที่จะปฏิบัติตามกฎระเบียบและข้อบังคับขององค์กร

การทบทวนแนวคิดและทฤษฎีที่เกี่ยวข้องทำให้สามารถนำมาพัฒนากรอบแนวคิดของปัจจัยทางด้านความตระหนักถึงการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล ซึ่งเป็นการบูรณาการกรอบแนวคิดมาจากงานวิจัยในอดีต ประกอบด้วย ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย ความเชื่อเกี่ยวกับกลุ่มอ้างอิง การรับรู้ความสามารถในการควบคุมพฤติกรรม ความตั้งใจที่จะปฏิบัติตาม และความตระหนักถึงความปลอดภัยข้อมูล



ภาพที่ 1 กรอบแนวคิดของงานวิจัย (Conceptual model)

3. วิธีการวิจัย

งานวิจัยชิ้นนี้เป็นงานวิจัยเชิงปริมาณ (Quantitative Research) มีจุดมุ่งหมายเพื่อพิสูจน์สมมติฐานงานวิจัยที่กำหนดขึ้น เป็นการศึกษาในลักษณะของการวิจัยเชิงสำรวจ (Survey Research) ด้วยวิธีการทบทวนวรรณกรรมที่เกี่ยวข้อง ซึ่งใช้วิธีการเก็บรวบรวมข้อมูลด้วยแบบสอบถาม (Questionnaire) แบบสอบถามจะพัฒนาเป็นแบบสอบถามอิเล็กทรอนิกส์และแบบสอบถามแบบกระดาษ เพื่อนำมาวิเคราะห์ทางสถิติ

ผู้วิจัยได้ทำออกแบบและทดสอบแบบสอบถาม ซึ่งจะใช้เป็นเครื่องมือในการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง จำนวน 447 ตัวอย่าง จากประชากรไทยที่ทำงานทั้งในองค์กรทั้งภาครัฐและภาคเอกชนและสามารถนำอุปกรณ์สมาร์ทโฟนส่วนบุคคลไปใช้ในที่ทำงานได้ ในเขตกรุงเทพมหานครและปริมณฑล การสร้างและพัฒนาข้อคำถามของงานวิจัยทางผู้วิจัยเป็นการรวบรวมข้อคำถามที่เกี่ยวข้องจากงานวิจัยในอดีต ซึ่งแบบสอบถามที่ใช้ได้จากการปรับประยุกต์จากการศึกษางานวิจัยในอดีตที่เกี่ยวข้อง บทความ เพื่อนำมากำหนดขอบเขตและเนื้อหาของแบบสอบถามที่จะนำไปใช้ศึกษากับกลุ่มตัวอย่างและผู้วิจัยมีการพัฒนาข้อคำถามที่เกี่ยวข้องจากการรวบรวมงานวิจัยในอดีต โดยข้อคำถามทางด้านระเบียบการรักษาความ

มั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร จากงานวิจัยของ (Anderson and Agarwal, 2010; Bulgurcu et al., 2010; Fagnot and Paquette, 2012)

การวิจัยครั้งนี้ผู้วิจัยดำเนินการควบคุมของเครื่องมือที่ใช้ในการวิจัย 2 ส่วน ดังนี้ (1) การตรวจสอบความเที่ยงตรงเชิงเนื้อหา (Content Validity) ให้อาจารย์ที่ปรึกษาผู้ทรงคุณวุฒิ ซึ่งมีความชำนาญในการทำงานวิจัย พิจารณาและตรวจสอบความเที่ยงตรงของเนื้อหา แล้วทำการปรับปรุงแก้ไขตามข้อเสนอแนะ เพื่อความชัดเจนและครบถ้วนตามจุดประสงค์ของงานวิจัย (2) การทดสอบความเชื่อมั่นของชุดคำถามที่ใช้วัดตัวแปร โดยการนำแบบสอบถามที่ได้รับการปรับปรุงแก้ไขแล้วเพื่อทดสอบแบบสอบถามของงานวิจัยกับกลุ่มตัวอย่าง จำนวน 20 คน (Pre-Test) โดยใช้แบบสอบถามแบบกระดาษ เพื่อประเมินถึงความเหมาะสมและความชัดเจนของแบบสอบถามก่อนการเก็บข้อมูลจริง โดยใช้สูตรของ Cornbach เพื่อคำนวณหาค่าสัมประสิทธิ์แอลฟา (Cronbach, 1951) แล้วทำการปรับปรุงแก้ไขแบบสอบถาม หลังจากได้แบบสอบถามที่มีความเหมาะสมเรียบร้อยแล้ว ผู้วิจัยจึงนำแบบสอบถามไปใช้ในการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง โดยใช้แบบสอบถามอิเล็กทรอนิกส์

4. ผลการศึกษา

ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ผลการวิเคราะห์ในส่วนนี้เป็นการแจกแจงข้อมูลทั่วไปของผู้ตอบแบบสอบถาม จำนวนกลุ่มตัวอย่างที่ใช้ในการวิจัยครั้งนี้มีทั้งหมด 447 คน และเมื่อแยกตามข้อมูลส่วนบุคคลของกลุ่มตัวอย่าง พบว่าช่วงอายุของกลุ่มตัวอย่าง 26-30 ปี สูงถึงร้อยละ 61.74 และระดับการศึกษาของกลุ่มตัวอย่างพบว่า ปริญญาตรี ร้อยละ 70.02 ในขณะที่ทำการจำแนกตามระดับตำแหน่งงานระดับปฏิบัติการ ร้อยละ 82.77 แจกแจงตามกลุ่มสายงานที่เกี่ยวข้องพบว่ากลุ่มสายงาน Financial Services มีมากที่สุดถึงร้อยละ 58.61 สุดท้ายการจำแนกกลุ่มตัวอย่างตามลักษณะการใช้งานอุปกรณ์สมาร์ทโฟนส่วนบุคคลของกลุ่มตัวอย่าง โดยแบ่งตามระดับความรู้เกี่ยวกับคอมพิวเตอร์และเทคโนโลยี ไม่ดีเลย ร้อยละ 0.45 ค่อนข้างไม่ดี ร้อยละ 4.03 ปานกลาง ร้อยละ 46.31 ค่อนข้างดี ร้อยละ 40.27 และ ดีมาก ร้อยละ 8.95

ผลการวิเคราะห์องค์ประกอบร่วม (Factor Analysis) เป็นการนำเสนอผลของการจับกลุ่มปัจจัยที่ส่งผลถึงการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัย ทั้ง 5 ตัวแปร ประกอบด้วย ความตระหนักถึงความปลอดภัยข้อมูล ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย ความเชื่อเกี่ยวกับกลุ่มอ้างอิง การรับรู้ความสามารถในการควบคุมพฤติกรรม และความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งวิธีการสกัดปัจจัยจะเลือกเฉพาะปัจจัยที่มีค่า Eigenvalue มากกว่า 1 เท่านั้น เมื่อพิจารณาค่าสถิติพบว่าค่าดัชนี KMO มีค่ามากกว่า 0.80 ทุกตัวแปรแสดงว่า ข้อมูลที่มีอยู่มีความเหมาะสมที่จะใช้ Factor Analysis ในการวิเคราะห์องค์ประกอบร่วมมาก

ความเชื่อมั่นของเครื่องมือ ได้ทำการตรวจสอบความเชื่อมั่น (Reliability) ของเครื่องมือ โดยใช้สูตรสัมประสิทธิ์แอลฟ่า (Alpha Coefficient) ของ Cronbach ซึ่งผลการวิเคราะห์ปรากฏว่าจำนวนกลุ่มตัวอย่างที่เก็บรวบรวม ให้ค่าความเชื่อมั่นของทั้ง 5 ตัวแปร อยู่ในเกณฑ์ที่ยอมรับได้ คือมากกว่า 0.7 ซึ่งแสดงให้เห็นว่ามีความเชื่อมั่นในระดับที่สูงมาก

5. สรุปผลการวิจัย

งานวิจัยนี้มีการศึกษาเอกสารงานวิจัยในอดีตที่เกี่ยวข้อง เพื่อเป็นแนวทางในการสร้างและสรุปกรอบแนวคิดในการวิจัยเพื่อทดสอบสมมติฐานที่ว่าทัศนคติของพนักงานที่มีต่อการปฏิบัติตามนโยบายรักษาความปลอดภัยข้อมูลขององค์กร ความเชื่อเกี่ยวกับกลุ่มอ้างอิงของพนักงานเกี่ยวกับการปฏิบัติตามนโยบายรักษาความปลอดภัยข้อมูลขององค์กร การรับรู้ความสามารถในการควบคุมพฤติกรรมของพนักงานเกี่ยวกับการปฏิบัติตามนโยบายรักษาความปลอดภัยข้อมูลขององค์กร และความตระหนักถึงความปลอดภัยข้อมูลของพนักงานเป็นปัจจัยที่ส่งผลเชิงบวกต่อความตั้งใจที่จะปฏิบัติตาม ข้อกำหนด

ของนโยบายการรักษาความปลอดภัยข้อมูลขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล รวมถึงความตระหนักถึงความปลอดภัยข้อมูลของพนักงานเป็นปัจจัยที่ส่งผลเชิงบวกต่อทัศนคติที่มีต่อการปฏิบัติตามข้อกำหนดของนโยบายการรักษาความปลอดภัยข้อมูลขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล

การวิจัยนี้มีกลุ่มตัวอย่างเป็นพนักงานขององค์กรทั้งภาครัฐและภาคเอกชนในประเทศไทย โดยสามารถนำอุปกรณ์สมาร์ทโฟนส่วนบุคคลไปใช้ในที่ทำงานได้ จำนวน 447 ราย ซึ่งการเลือกกลุ่มตัวอย่างนั้นใช้วิธีการสุ่มแบบเฉพาะเจาะจง และใช้แบบสอบถามเป็นเครื่องมือในการรวบรวมข้อมูล

สถิติที่ใช้ในการวิเคราะห์ข้อมูลสำหรับการวิจัยในครั้งนี้ ได้แก่ สถิติบรรยายเพื่อวิเคราะห์การแจกแจงความถี่ของข้อมูลส่วนตัวของผู้ตอบแบบสอบถาม การวิเคราะห์องค์ประกอบร่วม (Factor analysis) เพื่อจับกลุ่มปัจจัย และการวิเคราะห์ Regression เพื่อหาความสัมพันธ์ระหว่างกลุ่มปัจจัยทัศนคติของพนักงานที่มีต่อการปฏิบัติตามนโยบายรักษาความปลอดภัยข้อมูลขององค์กร ความเชื่อเกี่ยวกับกลุ่มอ้างอิงของพนักงาน การรับรู้ความสามารถในการควบคุมพฤติกรรมของพนักงานและความตระหนักถึงความปลอดภัยข้อมูลของพนักงานกับความตั้งใจที่จะปฏิบัติตามข้อกำหนดของนโยบายการรักษาความปลอดภัยข้อมูลขององค์กร สรุปผลการทดสอบสมมติฐานแสดงในตารางที่ 1

ตารางที่ 1 สรุปผลการทดสอบสมมติฐาน

สมมติฐาน	**ความสัมพันธ์**			**ผลทดสอบการสนับสนุนสมมติฐานที่ระดับนัยสำคัญ(P<0.01)**
H1	ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย	→	ความตั้งใจที่จะปฏิบัติตามนโยบาย	สนับสนุน
H2	ความเชื่อเกี่ยวกับกลุ่มอ้างอิง	→	ความตั้งใจที่จะปฏิบัติตามนโยบาย	สนับสนุน
H3	การรับรู้ความสามารถในการควบคุมพฤติกรรม	→	ความตั้งใจที่จะปฏิบัติตามนโยบาย	สนับสนุน
H4	ความตระหนักถึงความปลอดภัยข้อมูล	→	ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย	สนับสนุน
H5	ความตระหนักถึงความปลอดภัยข้อมูล	→	ความตั้งใจที่จะปฏิบัติตามนโยบาย	สนับสนุน

5.1 ประโยชน์ที่จะได้รับ

เชิงทฤษฎี งานวิจัยฉบับนี้สามารถทำให้ทราบถึงองค์ความรู้ที่สำคัญ ซึ่งเกี่ยวข้องกับปัญหาเชิงพฤติกรรมของพนักงานต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรและปัจจัยของการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร จากการทบทวนวรรณกรรมที่เกี่ยวข้องและตรวจสอบบทบาทของปัจจัยอิทธิพลจากทัศนคติที่มีต่อพฤติกรรม (Attitude toward behavior) ในการทำหน้าที่เป็นสื่อตัวกลางที่สำคัญ (มีการใช้กันอย่างกว้างขวางจากหลายทฤษฎี เช่น TAM) (Bulgurcu et al., 2010; Kaur and Mustafa, 2013) จากผลการวิจัยครั้งนี้ได้ทำการตรวจสอบในบริบทของทัศนคติของพนักงานที่มีต่อความตั้งใจในการปฏิบัติตามนโยบายองค์กร งานวิจัยฉบับนี้ได้ชี้แนวทางให้เห็นว่าทัศนคติมีบทบาทในการทำหน้าที่เป็นสื่อตัวกลางเพียงบางส่วน (Partial mediator) ในการอธิบายความสัมพันธ์ระหว่างความตระหนัก

ถึงความปลอดภัยข้อมูล (Information Security Awareness) และความตั้งใจต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กร (Intention to Comply) นอกจากนี้งานวิจัยยังสามารถแสดงให้เห็นว่าปัจจัยความตระหนักต่อการรักษาความปลอดภัยข้อมูลของพนักงานมีอิทธิพลทางตรงต่อปัจจัยการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล ดังนั้นวิจัยฉบับนี้ได้ชี้แนวทางให้เห็นว่าความตระหนักถึงความปลอดภัยข้อมูล (Information Security Awareness) มีอิทธิพลทั้งทางตรงต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรได้และทางอ้อมโดยผ่านปัจจัยทัศนคติที่มีต่อการปฏิบัติตามนโยบายของพนักงานกับพฤติกรรมของพนักงานต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรได้

เชิงปฏิบัติ งานวิจัยฉบับนี้สามารถนำไปกำหนดแนวทางเพื่อส่งเสริมความตระหนักของพนักงานต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยทางด้านสารสนเทศขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคล องค์กรต่างๆ สามารถใช้มาตรการตอบโต้ทั้ง 3 รูปแบบเพื่อที่จะสามารถลดการกระทำผิดของพนักงานต่อการปฏิบัติตามระเบียบการรักษาความปลอดภัยทางด้านสารสนเทศขององค์กร ซึ่งมาตรการตอบโต้ ทั้งสามรูปแบบได้แก่ ความตระหนักต่อนโยบายความปลอดภัยของผู้ใช้งาน การศึกษาและฝึกอบรมเกี่ยวกับทางด้านความมั่นคงปลอดภัย และการตรวจสอบคอมพิวเตอร์และอุปกรณ์สมาร์ทโฟนส่วนบุคคล โดยองค์กรสามารถนำไปประยุกต์ใช้ในทางปฏิบัติได้ ดังนี้ ผู้บริหารขององค์กร หรือผู้บริหารสารสนเทศระดับสูงควรให้ความสำคัญในการบริหารจัดการ โดยผู้บริหารจะต้องแสดงถึงการให้ความสำคัญต่อการกำหนดการลงมือปฏิบัติการ ดำเนินการ เฝ้าระวัง การทบทวน การบำรุงรักษาและการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย ผู้บริหารควรมอบหมายให้หน่วยงานภายในองค์กรที่เกี่ยวข้อง เช่น ฝ่ายสารสนเทศ ฝ่ายทรัพยากรบุคคลในการบริหารจัดการทรัพยากรที่จำเป็น เช่น การอบรม การประชาสัมพันธ์เผยแพร่ข้อมูลข่าวสาร การสร้างความรู้ความเข้าใจเกี่ยวกับการควบคุมภายในและนโยบายความมั่นคงปลอดภัยข้อมูลองค์กร การสร้างความตระหนักถึงความปลอดภัยข้อมูลและการเพิ่มขีดความสามารถเพื่อให้พนักงานทั้งหมดที่ได้รับมอบหมายหน้าที่สามารถปฏิบัติงานได้ตามที่กำหนดไว้ในนโยบายความมั่นคงปลอดภัย เพื่อสร้างความมั่นใจว่าพนักงานทุกคนในองค์กรมีความตระหนักในบทบาทของพวกเขาและความรับผิดชอบที่มีต่อการรักษาความปลอดภัยข้อมูลขององค์กร นอกจากนี้ผู้บริหารควรให้ความสำคัญในการลงทุนด้านความมั่นคงปลอดภัยข้อมูลองค์กรซึ่งต้องพัฒนาความความรู้ด้านความปลอดภัยทางเทคโนโลยีอย่างต่อเนื่องและเปิดโอกาสให้พนักงานได้เข้าอบรม ศึกษาดูงานเพื่อเพิ่มพูนความรู้ตามความเหมาะสม ดังนั้นงานวิจัยชิ้นนี้สามารถกระตุ้นให้องค์กรเห็นความสำคัญของการเสริมสร้างความตระหนักถึงการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรในการใช้อุปกรณ์สมาร์ทโฟนส่วนบุคคลของพนักงาน เพื่อเป็นแนวทางในการเสริมสร้างนโยบายการรักษาความปลอดภัยข้อมูลสำหรับองค์กรและให้พนักงานเกิดการตระหนักในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรและนำไปสู่ความตั้งใจที่จะปฏิบัติตาม

5.2 ข้อจำกัดในงานวิจัย

แม้ว่างานวิจัยฉบับนี้จะมีการค้นพบที่เป็นประโยชน์และน่าสนใจ แต่ก็ยังมีข้อจำกัดบางประการ ได้แก่ งานวิจัยในครั้งนี้เลือกกลุ่มตัวอย่างทั้งหมดจากองค์กรทั้งภาครัฐและภาคเอกชนโดยสามารถนำอุปกรณ์สมาร์ทโฟนส่วนบุคคลไปใช้ในที่ทำงาน วิธีการเลือกกลุ่มประชากรที่ใช้เป็นกลุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) ถึงแม้ว่ากลุ่มตัวอย่างจำนวน 447 รายจะสามารถเป็นตัวแทนของประชากรทั้งหมด แต่วิธีการเลือกกลุ่มตัวอย่างแบบเจาะจงเป็นการเลือกกลุ่มตัวอย่างโดยใช้ดุลพินิจและการตัดสินใจของผู้วิจัยหลักในการพิจารณาเลือกกลุ่มตัวอย่างว่ามีลักษณะสอดคล้องหรือเป็นตัวแทนที่จะศึกษาได้หรือเป็นไปตามวัตถุประสงค์ของการงานวิจัยหรือไม่ ซึ่งการตัดสินใจของผู้วิจัยอาจจะส่งผลต่อความน่าเชื่อถือของผลที่ได้จากการวิจัย จาการคัดเลือกกลุ่มตัวอย่างผู้วิจัยได้คัดเลือกเฉพาะกลุ่มตัวอย่างที่ทำงานเป็นพนักงานประจำ

(Permanent Employee) เท่านั้น อาจจะทำให้เกิดอคติหรือขาดข้อมูลในการตอบแบบสอบถามในส่วนของพนักงานชั่วคราว (Temporary Employee)

5.3 ข้อเสนอแนะ

สืบเนื่องจากข้อจำกัดที่ได้กล่าวข้างต้น เพื่อให้งานวิจัยในอนาคต มีความสมบูรณ์และน่าสนใจยิ่งขึ้น จึงใคร่ขอเสนอข้อเสนอแนะสำหรับการทำงานวิจัยครั้งต่อไป ใน 2 ประเด็น ดังนี้ ประเด็นที่แรก งานวิจัยในครั้งนี้มุ่งศึกษาปัจจัยที่จะนำไปสู่การปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กร โดยเลือกปัจจัยจากกลุ่มของทฤษฎีเชิงพฤติกรรม (Behavioral Theories) เป็นหลัก งานวิจัยครั้งต่อไปควรมีการศึกษาปัจจัยทางด้านแรงจูงใจเพื่อศึกษาปัจจัยใดบ้างที่ช่วยเสริมสร้างแรงจูงใจในการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร เช่น การให้รางวัลหากพนักงานปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กร หรือ การลงโทษหากพนักงานไม่ตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กร ประเด็นที่สอง เนื่องจากงานวิจัยชิ้นนี้ได้ระบุขอบเขตการวิจัยเฉพาะพนักงานประจำเนื่องจากพนักงานประจำได้ผ่านกระบวนการอบรมหรือได้รับความรู้ถึงกฎระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรเป็นอย่างดี และมีสิทธิ์หรือสามารถเข้าถึงข้อมูลขององค์กรได้ แต่อย่างไรก็ตามบางองค์กรให้สิทธิ์พนักงานชั่วคราวสามารถเข้าถึงข้อมูลขององค์กรได้เช่นกันและหลายองค์กรไม่ได้ให้ความสำคัญหรือเน้นย้ำต่อการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรสำหรับพนักงานชั่วคราว เนื่องจากมองว่าพนักงานเหล่านั้นใช้เวลาทำงานตามสัญญาจ้าง ซึ่งจากจุดนี้อาจจะทำให้เกิดช่องโหว่หรือเกิดความเสี่ยงที่จะทำให้ข้อมูลขององค์กรรั่วไหล ดังนั้นสำหรับงานวิจัยในอนาคต อาจจะทำการศึกษาเกี่ยวกับปัจจัยที่เสริมสร้างความตระหนักให้พนักงานชั่วคราวในการปฏิบัติตามระเบียบการรักษาความปลอดภัยข้อมูลขององค์กรทั้งในขณะที่ปฏิบัติงานในองค์กรและหมดสัญญาจ้าง

บรรณานุกรม

ธนาคารแห่งประเทศไทย. (2556). BYOD@BOT เปิดโลกการทำงานยุคใหม่แบบไร้ขีดจำกัด.

ประจิต หาวัตร. (2556). กลยุทธ์การจัดการความเสี่ยงจากการใช้ BYOD. บทความวิชาการ, 25, 91-95.

ประภาดา ตลึงจิตร. (2555). แนวทางในการเสริมสร้างความตระหนักถึงการปฏิบัติตามระเบียบการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ไทย: case study research of Thai cooperative. [กรุงเทพฯ]: คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์.

สิงหะ ฉวีสุข และสุนันทา วงศ์จตุรภัทร. (2555). ทฤษฎีการยอมรับการใช้เทคโนโลยีสารสนเทศ. KMITL Information Technology, jan-jun.2012.

อัครา วัฒนโยธิน. (2553). ความตระหนักของพนักงานต่อการป้องกันรักษาทรัพย์สินทางด้านสารสนเทศ: กรณีศึกษา : การไฟฟ้าส่วนภูมิภาค สำนักงานกลาง. [กรุงเทพฯ]: วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์.

Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.

Ajzen, I., and Fishbein, M. (1980). Understanding attitudes and predicting social. Behaviour. Englewood Cliffs, NJ: Prentice-Hall.

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., and Aleassa, H. (2013). Information Security Policy Compliance: An Empirical Study of Ethical Ideology. Paper presented at the System Sciences (HICSS), 2013 46th Hawaii International Conference on.

Allam, S., Flowerday, S. V., and Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. Computers & Security, 42(0), 56-65.

Anderson, C. L., and Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS quarterly, 34(3), 613-643.

Bertot, J. C., Jaeger, P. T., and Hansen, D. (2012). The impact of polices on government social media usage: Issues, challenges, and recommendations. Government Information Quarterly, 29(1), 30-40.

BRohme, R. (2013). The Economics of Information Security and Privacy. Book. doi: 10.1007/978-3-642-39498-0.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), 523-548.

Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security, 39, Part B(0), 447-459.

Fagnot, I., and Paquette, S. (2012). Organizational Information Security: The Impact of Employee Attitudes and Social Media Use.

Gritzalis, D., Kandias, M., Stavrou, V., and Mitrou, L. (2014). History of Information: The case of Privacy and Security in Social Media. Paper presented at the Proc. of the History of Information Conference.

Haeussinger, F., and Kranz, J. (2013). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., and Hohler, B. (2013). Employees' Information Security Awareness and Behavior: A Literature Review. Paper presented at the System Sciences (HICSS), 2013 46th Hawaii International Conference on.

Mani, D., Mubarak, S., and Choo, K.-K. R. (2014). Understanding the Information Security Awareness Process in Real Estate Organizations Using the Seci Model. Paper presented at the 20th Americas Conference on Information Systems (AMCIS 2014).

Toshihiko Takemura, A. K. (2013). An Empirical Study on Information Security Behaviors and Awareness. Book, 95-114.

Webb, J., Ahmad, A., Maynard, S. B., and Shanks, G. (2014). A situation awareness model for information security risk management. Computers & Security, 44(0), 1-15.

แผนระบบสารสนเทศเชิงกลยุทธ์: กรณีศึกษา โรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิต

พิชชารีย์ พรรธนะจรัส*
โรงเรียนเอ็นคอนเส็ปท์ อี แอคเคเดมี่
สุรัตน์ โคอินทรางกูร
ภาควิชาระบบสารสนเทศเพื่อการจัดการ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

***Correspondence:** pp_oamsin@hotmail.com
doi: 10.14456/jisb.2016.14

บทคัดย่อ

โรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิต มีหลักสูตรการเรียนที่ครอบคลุมตั้งแต่นักเรียนในระดับชั้นประถมศึกษาตอนปลาย ระดับมัธยมศึกษาตอนต้น ระดับมัธยมศึกษาตอนปลาย ไปจนถึงบุคคลทั่วไปที่ต้องการใช้ภาษาอังกฤษเพื่อสอบแข่งขัน ปัจจุบัน มีทั้งหมด 29 สาขาทั่วประเทศ และมีช่องทางการเรียนที่หลากหลายเพื่อตอบโจทย์กับความต้องการของนักเรียน

จากการวิเคราะห์สภาพแวดล้อมขององค์กร และปัจจัยภายใน ภายนอก ทำให้สามารถกำหนดกลยุทธ์ทางธุรกิจเพื่อให้โรงเรียนสามารถสร้างผลกำไรในอนาคตได้ คือ กลยุทธ์การสร้างนวัตกรรมสินค้าและบริการใหม่ และกลยุทธ์การสร้างความพึงพอใจให้กับลูกค้าด้านสินค้าและบริการ

เพื่อให้การจัดทำแผนระบบสารสนเทศสอดคล้องกับกลยุทธ์ของโรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิต จึงได้นำเสนอระบบสารสนเทศทั้ง 6 ระบบ ได้แก่ ระบบ S.E.L.F. ระบบจัดเก็บข้อมูลและฝึกอบรมพนักงาน ระบบคลังข้อสอบ ระบบข้อสอบเสมือนจริง Simulation Exam ระบบการจัดการและบริหารองค์ความรู้ และระบบบริหารลูกค้าสัมพันธ์ โดยระบบทั้ง 6 ระบบนั้นจะสนับสนุนกระบวนการทำงานในแต่ละกลยุทธ์ทางธุรกิจของโรงเรียนได้

ผลสรุปในเรื่องการลงทุนในระบบสารสนเทศที่องค์กรต้องดำเนินการจัดหาภายในระยะเวลา 3 ปี แบ่งออกเป็น 2 ระยะ โดยระยะแรกจะเป็นระบบ S.E.L.F. ระบบห้องสอบเสมือนจริง Simulation Exam และระบบบริหารลูกค้าสัมพันธ์ เนื่องจากเป็นระบบที่เกี่ยวข้องกับนักเรียนโดยตรง และสามารถดำเนินการจัดทำได้ทันที เพราะองค์กรมีทรัพยากรที่พร้อมอยู่แล้ว สำหรับในระยะที่ 2 คือ ระบบจัดเก็บข้อมูลและการฝึกอบรมพนักงาน ระบบคลังข้อสอบ ระบบการจัดการและบริหารองค์ความรู้ เป็นระบบที่องค์กรต้องศึกษาและเรียนรู้เพิ่มเติมก่อนดำเนินการจัดทำ ในเรื่องของค่าใช้จ่ายในการจัดทำระบบองค์กรมีทรัพยากรที่พร้อมใช้งานได้อยู่แล้ว ในขณะที่การได้มาของระบบสารสนเทศทั้ง 6 ระบบนั้น จะดำเนินการพัฒนาโดยทีมงานระบบสารสนเทศของบริษัทในเครือ และการซื้อโปรแกรมสำเร็จรูป และจากการคำนวณระยะเวลาคืนทุนของระบบที่พัฒนาทั้งหมด มีการจัดสรรการใช้ทรัพยากรร่วมกันของทุกระบบจึงสามารถคืนทุนได้ไม่ภายในไม่เกิน 3 ปี มีเพียงระบบเดียวคือ ระบบคลังข้อสอบที่ต้องอาศัยระยะเวลาในการคืนทุนมากกว่า 3 ปีขึ้นไป

คำสำคัญ: แผนระบบสารสนเทศ กลยุทธ์ โรงเรียนกวดวิชา กลยุทธ์การสร้างนวัตกรรม กลยุทธ์การสร้างความพึงพอใจให้กับลูกค้า

Strategic Information Systems Planning in Case Study of Triam Bundit English Language and Tutoring School

Pitcharee Phanthanajarus*

Encocept E-Academy

Surat Kointarangkul

Department of Management Information Systems, Thammasat Business School, Thammasat University

***Correspondence:** pp_oamsin@hotmail.com

doi: 10.14456/jisb.2016.14

Abstract

TRIAM BUNDIT English Language and Tutoring School develop the distinct effective English courses for primary student, secondary student, high school student and adult which provide 29 branches all over the country and have various learning channel that suitable for the student.

From the external environment and the internal environment analysis that can provide strategy for school are as follows: Innovation strategy and Customer Orientation strategy that suitable with 6 systems are S.E.L.F. System, Training and collecting data System, E-Exam System, Simulation Exam System, Knowledge Management System, and Customer Relationship Management System.

The school should provide all information systems within 3 years and split in 2 phases. First phase are as follows: S.E.L.F. System, Simulation Exam System and Customer Relationship Management System that can management as soon with the school's resource. Last phase are as follows: Training and collecting data System, E-Exam System and Knowledge Management System that developer should learning before develop the system. All System can develop by developer staff in school and buy instant program. And it will return the profit within 3 Years. Only E-Exam System that take more than 3 Years to return the profit.

Keywords: Strategic information system planning, Strategy, Tutoring school, Innovation strategy, Customer orientation strategy

1. บทนำ

ธุรกิจกวดวิชาโดยรวมในประเทศไทย ปี พ.ศ. 2557 มีมูลค่า 7,600 ล้านบาท มีโรงเรียนกวดวิชาประมาณ 2,005 แห่ง อยู่ในเขตกรุงเทพฯ 460 แห่ง และภูมิภาค 1,545 แห่ง และมีแนวโน้มเพิ่มขึ้นเรื่อยๆ โดยธุรกิจกวดวิชาได้แบ่งการกวดวิชาออกเป็นรายวิชา ในส่วนของโรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิต เป็นโรงเรียนกวดวิชา และสอนภาษาอังกฤษ ที่มีคู่แข่งจำนวนมากในตลาด ปัจจุบันธุรกิจกวดวิชาภาษาอังกฤษมีแนวโน้มการขยายตัวอย่างต่อเนื่อง เนื่องจากนักเรียน หรือผู้ปกครองมีค่านิยมว่า การเรียนกวดวิชาจะช่วยในการสอบเข้าศึกษาต่อในสถาบันที่มีชื่อเสียงได้ นอกจากนี้ยังมีเรื่องที่ประเทศไทยกำลังจะก้าวเข้าสู่ประชาคมเศรษฐกิจอาเซียน หรือ AEC ทำให้เกิดกระแสตื่นตัวในการพัฒนาทักษะภาษาอังกฤษมากยิ่งขึ้น ดังนั้นจึงมีการแข่งขันสูงในตลาดกวดวิชาภาษาอังกฤษ สถาบันกวดวิชาหลายแห่งจำเป็นต้องสร้างความแตกต่าง เพื่อใช้ดึงดูดกลุ่มนักเรียน รวมถึงผู้ปกครอง

โรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิต เป็นโรงเรียนกวดวิชาและสอนภาษาอังกฤษ โดยมีความมุ่งมั่นที่จะสร้างสรรค์การเรียนรู้รูปแบบใหม่ เพื่อให้เกิดแนวความคิดและความเข้าใจต่อสิ่งที่เรียนรู้มากกว่าเพียงแค่การท่องจำ ปัจจุบันมีคอร์สเรียนที่รองรับกลุ่มนักเรียนตั้งแต่ระดับชั้นประถมศึกษาตอนปลาย ระดับมัธยมศึกษาตอนต้น ระดับมัธยมศึกษาตอนปลาย ไปจนถึงบุคคลทั่วไปที่ต้องการพัฒนาทักษะภาษาอังกฤษ เพื่อนำไปใช้สอบวัดระดับต่างๆ ปัจจุบันมี 29 สาขาทั่วประเทศ มีรูปแบบการเรียนที่หลากหลาย แบ่งออกเป็น 4 รูปแบบ คือ

(1) การเรียนในรอบสอนสด เป็นการเรียนที่มีครูผู้สอนดำเนินการสอนในห้องเรียน

(2) การเรียนผ่านระบบ S.E.L.F. เป็นการเรียนเนื้อหาผ่านเครื่องคอมพิวเตอร์ส่วนตัวที่สาขา โดยไฟล์วิดีโอที่นักเรียนเรียนเป็นไฟล์ที่มีการบันทึกจากการเรียนในรอบสอนสด

(3)การเรียนผ่านระบบ S.E.L.F.@HOME 100% เป็นการเรียนเนื้อหาทั้งคอร์สเรียนจากที่บ้าน โดยเป็นไฟล์วิดีโอที่มีการบันทึกจากการเรียนในรอบสอนสด และแปลงในระบบ เพื่อให้นักเรียนดาวน์โหลดเนื้อหาเรียนได้จากที่บ้าน

(4) การเรียนผ่านระบบ S.E.L.F.@Tablet เป็นการเรียนเนื้อหาทั้งคอร์สเรียนผ่านอุปกรณ์ Tablet โดยเป็นไฟล์วิดีโอที่มีการบันทึกจากการเรียนในรอบสอนสด และแปลงในระบบ เพื่อให้นักเรียนเรียนได้ผ่านอุปกรณ์ Tablet เท่านั้น

นอกจากนี้ยังมีการเรียนในรูปแบบอื่นๆ ซึ่งทางโรงเรียนได้มีการพัฒนาหลักสูตรการเรียนโดยนำไปประยุกต์ใช้กับอุปกรณ์การสื่อสาร SmartPhone ให้นักเรียนสามารถเรียนรู้วิชาภาษาอังกฤษเพิ่มเติมได้ผ่าน Applications ที่ทางโรงเรียนได้พัฒนาขึ้น

2. ผลการวิเคราะห์โดยใช้เครื่องมือในการทำแผนกลยุทธ์

2.1 ผลการวิเคราะห์โดยใช้ PEST

จากการวิเคราะห์สภาวะแวดล้อมทั่วไป โดยใช้เครื่องมือ PEST Analysis พบว่ายังคงมีโอกาสในการเติบโตของธุรกิจกวดวิชาภาษาอังกฤษ เนื่องจากนักเรียนยังคงมีค่านิยม และความเชื่อมั่นต่อการเรียนกวดวิชา ว่าจะสามารถทำให้สอบได้คะแนนดี หรือมีความรู้เพิ่มขึ้นจริง และมีส่วนช่วยในการสอบเข้าโรงเรียน หรือมหาวิทยาลัยที่มีชื่อเสียง และเลือกเรียนกวดวิชาภาษาอังกฤษเป็นลำดับต้นๆ เพราะใช้ในทุกสนามสอบ จากการที่นักเรียนส่วนใหญ่มองว่าการเรียนกวดวิชาเป็นสิ่งจำเป็น ทำให้ยังคงเกิดพฤติกรรมการเรียนพิเศษอยู่ในปัจจุบัน หากโรงเรียนมีการปรับตัวให้สอดคล้องกับสภาวะทางการเมือง หรือสภาวะทางเศรษฐกิจของประเทศ จะไม่ก่อให้เกิดผลกระทบมากนัก ในส่วนของความก้าวหน้าทางเทคโนโลยี การใช้งานอินเทอร์เน็ตเพื่อตอบสนองความต้องการจะช่วยอำนวยความสะดวกต่อผู้ใช้งานมากยิ่งขึ้น โดยเฉพาะปัจจุบันนี้คนส่วนใหญ่พกพาอุปกรณ์การสื่อสาร เช่น SmartPhone หรือ Tablet ติดตัวไปด้วยทุกที่ การใช้งานอินเทอร์เน็ตผ่านอุปกรณ์การ

สื่อสารนี้จึงมีแนวโน้มเพิ่มขึ้นเรื่อยๆ ดังนั้นการเติบโตของเทคโนโลยีจะช่วยสร้างนวัตกรรมใหม่ๆ เกี่ยวกับการเรียน สร้างความสะดวกกับผู้เรียน ในขณะที่โรงเรียนสามารถปรับใช้และสร้างยอดขายจากส่วนนี้ได้

การวิเคราะห์ปัจจัยที่มีผลต่อการแข่งขันของธุรกิจโดยใช้เครื่องมือ Five Forces พบว่า มีการแข่งขันที่รุนแรงในธุรกิจกวดวิชาภาษาอังกฤษ ทั้งคู่แข่งรายเก่า และรายใหม่ ทั้งนี้มีสาเหตุมาจากการใช้วิชาภาษาอังกฤษเป็นวิชาหลักในการสอบเข้าศึกษาต่อทุกสนามสอบ รวมถึงความต้องการพัฒนาทักษะภาษาอังกฤษ ทำให้นักเรียนมีความสนใจลือกเรียนวิชาภาษาอังกฤษเป็นลำดับต้นๆ ของการกวดวิชา โดยคู่แข่งหลักในปัจจุบันมีศักยภาพที่ใกล้เคียง ทั้งในเรื่องของคอร์สเรียนที่เปิดสอน จำนวนสาขา และรูปแบบกิจกรรมทางการตลาด ในขณะที่คู่แข่งรายใหม่ได้พยายามสร้างจุดขายในเรื่องของวิธีการสอน รวมถึงสร้างพันธมิตรที่แข็งแกร่ง เพื่อเป็นกลยุทธ์ในการสร้างความได้เปรียบเหนือโรงเรียนอื่นๆ

การแข่งขันที่รุนแรง ทำให้แต่ละโรงเรียนต่างก็นำเสนอทางเลือกที่ตรงกับความต้องการของนักเรียน และผู้ปกครองมากที่สุด ทั้งการนำเสนอคอร์สเรียน รวมถึงกิจกรรมทางการตลาด การจัดโปรโมชั่นต่างๆ เพื่อดึงดูดใจ ทำให้นักเรียน และผู้ปกครองมีทางเลือกในการสมัครเรียนมากขึ้น ส่งผลให้อำนาจต่อรองของผู้ซื้อมีมากขึ้น

ในขณะที่อำนาจต่อรองของผู้ขายปัจจัยการผลิต จากการวิเคราะห์ยอดขายพบว่า คอร์สที่สอนโดยติวเตอร์หลักจะสร้างรายได้มากกว่าคอร์สอื่นๆ ในขณะที่บุคลากรทางวิชาการ ที่ถือเป็น Supplier สำคัญรองลงมา เนื่องจากเป็นผู้จัดทำหลักสูตรเบื้องหลังติวเตอร์ มีอัตราการลาออกค่อนข้างสูงในแต่ละปี และการรับคนเข้ามาใหม่ใช้เวลานาน เพราะมีกระบวนการคัดกรองเป็นพิเศษ ดังนั้นหากมีการลาออกในทีม จะส่งผลกระทบต่อแผนงานวิชาการที่ได้วางแผนไว้ก่อนหน้านี้ จึงส่งผลให้อำนาจต่อรองในส่วนนี้อยู่ในระดับที่สูง

ภัยคุกคามของสินค้าหรือบริการทดแทน เช่น การค้นหาเนื้อหาที่ตรงกับความต้องการผ่านอินเทอร์เน็ต หรือการใช้งานผ่านอุปกรณ์การสื่อสาร เช่น SmartPhone หรือ Tablet ปัจจัยเหล่านี้ได้ก่อให้เกิดความสะดวกกับผู้เรียนมากที่สุด อีกทั้งไม่มีค่าใช้จ่ายเพิ่มเติมเหมือนเรียนกวดวิชา ซึ่งถือเป็นช่องทางการเรียนรู้รูปแบบใหม่และมีโอกาสเป็นสินค้าหรือบริการทดแทนในอนาคตได้

2.2 ผลการวิเคราะห์โดยใช้ SWOT Analysis

จากการวิเคราะห์สภาพแวดล้อมขององค์กรในปัจจุบัน เพื่อค้นหาจุดแข็ง จุดอ่อน โอกาส และอุปสรรค มีประเด็นสำคัญดังนี้

ด้านสภาพแวดล้อมภายใน

(1) โรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิตเป็นโรงเรียนที่เป็นที่รู้จักของการติวกวดวิชาภาษาอังกฤษเพื่อสอบเข้าโรงเรียน หรือมหาวิทยาลัย โดยมีติวเตอร์ผู้สอนที่เป็นที่รู้จักในหมู่นักเรียน หรือผู้ปกครอง “ครูเอ็ม” และเป็นที่รู้จักในสื่อมวลชนที่เกี่ยวข้องกับการศึกษา

(2) ระบบ S.E.L.F. ซึ่งเป็นระบบหลักในการเรียนเกิดปัญหาบ่อยครั้ง และไม่มีกระบวนการในการตรวจสอบไฟล์วิดีโอการเรียน รวมถึงไม่มีการจัดการข้อมูลข่าวสารจากส่วนกลางอย่างเป็นระบบ

ด้านสภาพแวดล้อมภายนอก

(1) มาตรฐานการสอนของแต่ละโรงเรียนต่างกัน ทำให้นักเรียนเกิดความไม่เชื่อมั่น จึงต้องหาความรู้จากแหล่งอื่น เช่น การกวดวิชาเพื่อเตรียมตัวสอบแข่งขัน

(2) วิชาภาษาอังกฤษ เป็นวิชาที่นำมาใช้ในการคำนวณคะแนนทุกสนามสอบ ทำให้นักเรียนมองเห็นความสำคัญเป็นลำดับต้นๆ ในการเลือกเรียนกวดวิชา

(3) อุปกรณ์การสื่อสารทั้ง SmartPhone และ Tablet เป็นอุปกรณ์ที่ทุกคนมีพกติดตัว และใช้งานได้ตลอดเวลา การพัฒนาเนื้อหาบทเรียนให้สามารถเรียนได้จากทุกที่ ทุกเวลา หรือการพัฒนาทางเทคโนโลยีอื่นๆ จะช่วยเพิ่มความสะดวกในการเรียนมากยิ่งขึ้น

(4) เมื่อพิจารณาเรื่องคู่แข่งพบว่า ในปัจจุบันมีคู่แข่งในธุรกิจกวดวิชาภาษาอังกฤษเป็นจำนวนมาก ซึ่งมีทั้งคู่แข่งหลักรายเดิม และคู่แข่งรายใหม่ โดยแต่ละโรงเรียนต่างก็มีการนำเสนอกลยุทธ์ต่างๆ เพื่อสร้างจุดขายให้กับโรงเรียน และตอบสนองความต้องการของนักเรียน และผู้ปกครองให้มากที่สุด

(5) ในขณะที่การเข้าถึงข้อมูลต่างๆ ทำได้ง่ายขึ้น เพราะมีการพัฒนาอินเทอร์เน็ต โดยเฉพาะการเข้าถึงเนื้อหาผ่านช่องทางเว็บไซต์ YouTube ซึ่งเป็นแหล่งรวบรวมคลิปวิดีโอต่างๆ รวมถึงคลิปบทเรียนวิชาภาษาอังกฤษด้วย ส่วนนี้จะทำให้นักเรียนสามารถเรียนเนื้อหาได้สะดวก และมีข้อดีคือ ไม่มีค่าใช้จ่ายในการเรียน

3. กลยุทธ์องค์กรที่ได้จากการวิเคราะห์ และระบบที่นำเสนอ

กลยุทธ์ในการสร้างความได้เปรียบในการแข่งขันที่ได้ทำการศึกษามา ประกอบไปด้วย 12 กลยุทธ์ ดังต่อไปนี้

- Cost leadership strategy กลยุทธ์การเป็นผู้นำต้นทุนต่ำ
- Differentiation strategy กลยุทธ์การสร้างความแตกต่างของสินค้าและบริการ
- Niche strategy กลยุทธ์การเจาะตลาด
- Growth strategy กลยุทธ์การเติบโต ขยายตลาด
- Alliance strategy กลยุทธ์พันธมิตรร่วมค้า
- Innovation strategy กลยุทธ์นวัตกรรม คิดค้นประดิษฐ์สินค้าและบริการใหม่ๆ
- Entry-barrier strategy กลยุทธ์การสร้างอุปสรรคสำหรับผู้เข้ามาใหม่
- Customer orientation กลยุทธ์การให้ความสำคัญกับความพึงพอใจของลูกค้า
- Time กลยุทธ์เรื่องเวลา
- Operational effectiveness กลยุทธ์การดำเนินการอย่างมีประสิทธิผลกว่าคู่แข่ง
- Lock in customers or suppliers กลยุทธ์การให้คงอยู่กับบริษัทตลอดไป
- Increase switching costs กลยุทธ์ไม่ให้เปลี่ยนไปใช้บริษัทอื่นเพราะอาจแพงกว่า

จากการวิเคราะห์ในประเด็นสำคัญข้างต้นจึงได้แนวทางในการพัฒนาเป็นกลยุทธ์ขององค์กรได้ดังนี้

3.1 กลยุทธ์การสร้างนวัตกรรมสินค้าและบริการใหม่ (Innovation Strategy)

หมายถึง การใช้ไอทีในการสร้างสินค้าหรือบริการใหม่ๆ เข้าสู่ตลาด ทำให้สินค้าแตกต่างจากที่มีอยู่ในปัจจุบัน สร้างความได้เปรียบเหนือคู่แข่ง จากการวิเคราะห์ที่พบว่า มีแนวโน้มการเติบโตของการใช้อินเทอร์เน็ต และมีการใช้อุปกรณ์สื่อสาร เช่น SmartPhone หรือ Tablet ในสัดส่วนที่สูงขึ้นเรื่อยๆ จึงสามารถสร้างความได้เปรียบในการแข่งขันโดยใช้กลยุทธ์นี้มาพัฒนา และปรับใช้เป็นอีกหนึ่งช่องทางการเรียน ในขณะที่โรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิตเองก็มีกลยุทธ์การจัดทำ และพัฒนาระบบการเรียนให้ครบสมบูรณ์ โดยมีแผนที่จะพัฒนาเกี่ยวกับระบบการเรียน อย่างไรก็ตามในส่วนของความเข้มข้นทางเนื้อหาวิชาการ ทางโรงเรียนสามารถนำมาประยุกต์สร้างให้เกิดนวัตกรรมได้เช่นกัน จึงสรุปแผนการปฏิบัติงานดังนี้

แผนงานระยะยาว เพื่อสร้างความยั่งยืนให้กับองค์กรโดยส่งผลระยะยาว องค์กรจำเป็นต้องให้ความสำคัญกับการวางแผนงานอย่างเป็นระบบ โดยดำเนินการดังนี้

(1) **จัดตั้งคณะกรรมการ ทีมวิจัย ด้านนวัตกรรมการเรียน**

เนื่องจากการพัฒนานวัตกรรมการเรียน จะต้องดำเนินการสร้างสรรค์สิ่งใหม่ๆ ขึ้นมาเพื่อให้ตรงกับความต้องการของนักเรียน และสามารถเกิดเป็นยอดขายในอนาคตได้ จึงเป็นเรื่องใหม่ที่องค์กรควรให้ความสำคัญ โดยมีการวางแผนการทำงานตั้งแต่การจัดตั้งคณะกรรมการที่เกี่ยวข้องกับการพัฒนานวัตกรรมการเรียน รวมถึงทีมงานวิจัยในการค้นหาข้อมูล เพื่อนำเสนอในที่ประชุมต่อไป

(2) **พัฒนาศักยภาพทีมงาน**

ระบบที่ดีจะเกิดจากการสร้างระบบโดยทีมงานที่มีศักยภาพ รวมถึงผู้ให้คำแนะนำที่ให้ข้อมูลที่เป็นประโยชน์ การพัฒนาทีมงานสามารถดำเนินงานได้ด้วยการฝึกอบรม เริ่มตั้งแต่ทีมงานผู้พัฒนาระบบที่ต้องมีความรู้ความสามารถตลอดจนความเชี่ยวชาญในการพัฒนาระบบ เพื่อให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพ เกิดปัญหาน้อยและลดข้อร้องเรียนน้อยที่สุด ในขณะที่ผู้ใช้งานระบบ รวมถึงผู้ที่ให้คำแนะนำระบบกับนักเรียนควรพัฒนาความรู้และฝึกทักษะเพิ่มเติมเพื่อให้สามารถให้คำแนะนำได้อย่างมีประสิทธิภาพสูงสุด

แผนงานระยะสั้น สามารถดำเนินการได้ทันที เพื่อสร้างยอดขายให้เกิดขึ้นทันกับสถานการณ์ในปัจจุบัน

(3) **เพิ่มช่องทางการเรียนที่สะดวกให้กับนักเรียนผ่านอุปกรณ์การสื่อสาร**

จากการวิเคราะห์ที่พบว่า ในปัจจุบันการใช้งานอินเทอร์เน็ตผ่าน SmartPhone มีสัดส่วนที่สูงขึ้นเรื่อยๆ นั่นหมายความว่าความต้องการในเรื่องการเข้าถึงข้อมูลผ่านช่องทางที่สะดวกกำลังเป็นที่ต้องการในปัจจุบัน จึงควรพัฒนาช่องทางการเข้าถึงข้อมูล หรือช่องทางการเรียนที่สะดวก โดยพัฒนาระบบการเรียนให้สามารถเรียนได้ผ่านอุปกรณ์ SmartPhone หรือ Tablet และปรับปรุงการใช้งานผ่าน Applications

(4) **จัดทำคลังข้อสอบ**

จากการวิเคราะห์ที่พบว่า โรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิต มีศักยภาพในเรื่องการพัฒนาเนื้อหาวิชาภาษาอังกฤษ โดยเฉพาะการนำโจทย์ หรือแบบฝึกหัดมาใช้ประกอบการสอน ซึ่งทำให้นักเรียนสามารถนำไปใช้ในการเตรียมตัวก่อนสอบแข่งขันได้ จึงควรพัฒนางานในส่วนคลังข้อสอบ เพื่อส่งมอบไปถึงนักเรียน โดยสามารถนำมาประยุกต์ให้เข้ากับอุปกรณ์การสื่อสาร เช่น Smart Phone หรือ Tablet ที่ทำให้เข้าถึงได้สะดวก

(5) **ศูนย์ทดสอบวิชาภาษาอังกฤษออนไลน์**

จากความแข็งแกร่งทางด้านวิชาการภาษาอังกฤษของโรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิต ซึ่งสร้างความเชื่อมั่นให้กับนักเรียนที่มาสมัครเรียนเพื่อเตรียมตัวสอบแข่งขัน ทำให้เกิดโอกาสในการพัฒนาเรื่องการเตรียมความพร้อมก่อนเข้าสอบจริง โรงเรียนสามารถจัดทำศูนย์ทดสอบ โดยพัฒนาโจทย์ หรือแบบฝึกหัดที่มีเนื้อหาใกล้เคียงกับข้อสอบภาษาอังกฤษจริงในแต่ละสนามสอบ และสามารถประเมินผลในหลากหลายมิติ รวมถึงให้คำแนะนำกับนักเรียนเป็นรายบุคคลเพื่อสร้างความเชื่อมั่นให้กับนักเรียนก่อนเข้าสอบจริงได้

3.2 กลยุทธ์สร้างความพึงพอใจให้กับลูกค้าด้านสินค้าและบริการ (Customer Orientation)

หมายถึง กลยุทธ์การให้ความสำคัญกับลูกค้า เพื่อให้ได้รับความพึงพอใจสูงสุด เนื่องจากในปัจจุบันมีการแข่งขันกันอย่างหนักในธุรกิจกวดวิชา นักเรียน หรือผู้ปกครองมีทางเลือกในการสมัครเรียนมากขึ้น โรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิตจึงจำเป็นต้องดำเนิน กลยุทธ์เพื่อตอบสนองความต้องการอย่างตรงจุด โดยเริ่มจากการค้นหาความต้องการของลูกค้า ศึกษาพฤติกรรมของลูกค้า จากนั้นจึงนำเสนอสินค้าหรือบริการที่ตรงตามความต้องการของลูกค้ามากที่สุด เป็นการสร้างความสัมพันธ์ที่ดีกับลูกค้า ส่งผลถึงการเป็นลูกค้าประจำในอนาคตได้

(1) การทำวิจัยตลาด

เพราะการแข่งขันที่รุนแรงในตลาดกวดวิชา การตอบสนองความต้องการของนักเรียนหรือผู้ปกครองให้โดนใจ เป็นสิ่งที่โรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิตควรให้ความสำคัญมากที่สุด เพราะตัวเลือกการเรียนที่หลากหลายจากทั้งคู่แข่งเก่าและใหม่ จะทำให้ลูกค้าเกิดทางเลือกในการตัดสินใจสมัครเรียน ทางโรงเรียนจึงควรค้นหาความต้องการที่นักเรียนต้องการสูงสุด โดยดำเนินการในเรื่องของการจัดทำกระบวนการวิจัยทางการตลาด เพื่อค้นหาความต้องการของนักเรียน และผู้ปกครอง ทั้งในเรื่องการตอบสนองความต้องการในเรื่องบทเรียน หรือสิทธิพิเศษที่ต้องการได้รับระหว่างการเรียน เพื่อสร้างแรงจูงใจ อย่างไรก็ตามผลจากงานวิจัยก็ควรจัดทำเป็นระบบ เพื่อให้ทีมงานนำไปใช้ในงานอื่นๆ ได้

(2) บริหารความสัมพันธ์ลูกค้า

เนื่องจากนักเรียนแต่ละกลุ่มมีพฤติกรรมการเรียนที่แตกต่างกัน การวิเคราะห์ข้อมูลลูกค้าจึงเป็นสิ่งสำคัญ เพราะจะทำให้โรงเรียนสามารถจัดประเภทกลุ่มลูกค้าได้ และนำเสนอสิ่งที่สามารถตอบสนองความต้องการของลูกค้าได้สูงสุด ตรงกลุ่มเป้าหมาย โดยจัดทำระบบบริหารความสัมพันธ์ลูกค้า Customer Relationship Management ซึ่งพิจารณาจากพฤติกรรมของลูกค้า และหาความเชื่อมโยงกับคอร์สเรียน หรือบริการที่เหมาะสม รวมถึงกลยุทธ์ทางการตลาดของโรงเรียน ข้อมูลของลูกค้าที่สำคัญ เช่น ข้อมูลเรื่องการสมัครเรียน ข้อมูลสถานะการเรียนปัจจุบัน คะแนนสอบ เป็นต้น หลังจากการวิเคราะห์พฤติกรรม และแบ่งกลุ่มประเภทลูกค้าแล้ว ก็จะต้องมีการติดต่อสื่อสาร หรือจัดกิจกรรมกับกลุ่มเป้าหมายต่อไป เพื่อสร้างความสัมพันธ์ที่ดี

อย่างไรก็ตามการนำเสนอข้อมูลที่ถูกต้อง และครบถ้วนให้กับลูกค้าก็เป็นสิ่งสำคัญ จึงควรพัฒนาระบบศูนย์รวมข้อมูลคอร์สเรียน และโปรโมชั่น เพื่อให้เจ้าหน้าที่เข้าถึงข้อมูลได้ง่าย และให้คำแนะนำกับนักเรียนได้อย่างถูกต้อง รวมถึงการพัฒนาศักยภาพของเจ้าหน้าที่ที่ปฏิบัติงานใกล้ชิดลูกค้าให้สามารถทำงาน และให้ข้อมูลได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

จากการวิเคราะห์ข้อมูล และสรุปเป็นกลยุทธ์ข้างต้น จึงสามารถนำเสนอระบบสนเทศที่สามารถตอบสนองกลยุทธ์องค์กร และช่วยให้องค์กรบรรลุเป้าหมายได้อย่างมีประสิทธิภาพ ได้ทั้งหมด 6 ระบบ ดังนี้

- **ระบบ S.E.L.F.**

เนื่องจากระบบหลักที่ใช้ในการเรียนที่โรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิต คือ ระบบ S.E.L.F. ซึ่งมีช่องทางการเรียนที่รองรับในปัจจุบันทั้งการเรียนแบบ S.E.L.F. 100% S.E.L.F.@HOME 100% S.E.L.F.@Tablet ตอบสนองความต้องการในเรื่องการจัดตารางเรียนได้เองผ่านเครื่องคอมพิวเตอร์ส่วนตัวที่สาขา รวมถึงการเรียนที่บ้าน หรืออุปกรณ์การสื่อสาร Tablet อย่างไรก็ตามการวิเคราะห์ พบว่า ปัจจุบันนี้อุปกรณ์การสื่อสาร เช่น SmartPhone หรือ Tablet ส่งผลกับการดำเนินชีวิตประจำวัน ทุกคนมีในครอบครอง และใช้เป็นสื่อในการเข้าถึงเนื้อหาผ่านอินเทอร์เน็ต จึงส่งผลให้เกิดโอกาสการขยายช่องทางการเรียนมาสู่อุปกรณ์การสื่อสารนี้ รวมถึงการใช้งาน Applications บน SmartPhone หรือ Tablet

- **ระบบจัดเก็บข้อมูลและการฝึกอบรมพนักงาน**

เนื่องจากการปฏิบัติงานในแต่ละส่วนให้มีประสิทธิภาพได้นั้น พนักงานผู้ปฏิบัติงานควรมีความรู้ความสามารถในการจัดทำผลงานจนประสบผลสำเร็จ และได้ผลงานที่มีประสิทธิภาพ การฝึกอบรมเป็นเครื่องมืออย่างหนึ่งในการเสริมสร้างศักยภาพของพนักงาน ปัจจุบันโรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิตมีการฝึกอบรมพนักงานในแต่ละแผนก อย่างไรก็ตามเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพยิ่งขึ้น ระบบควรมีการปรับปรุงในบางส่วน

- **ระบบคลังข้อสอบ**

จากการวิเคราะห์ที่พบว่า โรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิตมีศักยภาพในเรื่องการพัฒนาเนื้อหาวิชาภาษาอังกฤษ โดยเฉพาะการนำโจทย์ หรือแบบฝึกหัดมาใช้ประกอบการสอน ซึ่งทำให้นักเรียนสามารถนำไปใช้

ในการเตรียมตัวก่อนสอบแข่งขันได้ จึงมีโอกาสในเรื่องการพัฒนาในส่วนคลังข้อสอบ เพื่อส่งมอบไปถึงนักเรียน โดยสามารถนำมาประยุกต์ให้เข้ากับอุปกรณ์การสื่อสาร เช่น Smart Phone หรือ Tablet ที่ทำให้เข้าถึงได้สะดวก

- **ระบบห้องสอบเสมือนจริง Simulation Exam**

จากความแข็งแกร่งทางด้านวิชาการภาษาอังกฤษของโรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิต ซึ่งสร้างความเชื่อมั่นให้กับนักเรียนที่มาสมัครเรียน เพื่อเตรียมตัวสอบแข่งขัน ทำให้เกิดโอกาสในการพัฒนาเรื่องการเตรียมความพร้อมก่อนเข้าสอบจริง โรงเรียน สามารถจัดทำศูนย์ทดสอบ โดยพัฒนาโจทย์ หรือแบบฝึกหัดที่มีเนื้อหาใกล้เคียงกับข้อสอบภาษาอังกฤษจริงในแต่ละสนามสอบ และสามารถประเมินผลในหลากหลายมิติ รวมถึงให้คำแนะนำกับนักเรียนเป็นรายบุคคลเพื่อสร้างความเชื่อมั่นให้กับนักเรียนก่อนเข้าสอบจริงได้

- **ระบบการจัดการและบริหารองค์ความรู้**

เนื่องจากข้อมูลในการปฏิบัติงานต่างๆ ของโรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิตมีเป็นจำนวนมาก เช่น ข้อมูลคอร์สเรียน ข้อมูลกิจกรรมทางการตลาด โปรโมชั่นต่างๆ หรือข้อมูลความรู้อื่นๆ การกระจายข้อมูลเพื่อให้แต่ละฝ่ายสามารถใช้งานได้อย่างทั่วถึง และมีประสิทธิภาพ เป็นสิ่งที่โรงเรียนควรให้ความสำคัญ โดยเฉพาะอย่างยิ่งเจ้าหน้าที่งานขายที่ต้องรับข้อมูลทั้งหมดเพื่อให้การบริการแก่นักเรียน หรือผู้ปกครอง การให้ข้อมูลที่ครบถ้วนและถูกต้องจะช่วยสร้างความสัมพันธ์ที่ดีกับกลุ่มลูกค้าได้ การจัดเก็บข้อมูลที่หลากหลายและมีความซับซ้อนนั้นเป็นปัญหาที่โรงเรียนต้องพยายามแก้ไขปัญหา โดยการนำเทคโนโลยีสารสนเทศเข้ามาปรับใช้จะช่วยสร้างประสิทธิภาพการดำเนินงานได้ดียิ่งขึ้น

- **ระบบบริหารความสัมพันธ์ลูกค้า**

คือ การบริหารสร้างความผูกพันกับลูกค้า ให้ลูกค้ามีความรู้สึกผูกพันกับสินค้า บริการ หรือโรงเรียน เมื่อลูกค้ามีความผูกพันในทางที่ดี ก็จะไม่คิดเปลี่ยนใจ ทำให้เรามีฐานลูกค้าที่มั่นคง และนำมาซึ่งความมั่นคงของบริษัท โดยข้อมูลที่โรงเรียนจำเป็นต้องทราบเพื่อนำมาใช้ในการวิเคราะห์ เช่น พฤติกรรมของลูกค้า และนำระบบเทคโนโลยีเข้ามาปรับใช้เพื่อช่วยในการวิเคราะห์หาความเกี่ยวข้องระหว่าง พฤติกรรมของลูกค้ากับกลยุทธ์ทางการตลาด

3.3 ความคุ้มค่าของระบบสารสนเทศที่นำเสนอใหม่

การวางแผนระบบสารสนเทศของโรงเรียนกวดวิชาและสอนภาษาอังกฤษเตรียมบัณฑิต เป็นการวางแผนสารสนเทศเชิงกลยุทธ์เป็นระยะเวลา 3 ปี (พ.ศ.2559-2561) เพื่อแก้ปัญหา และตอบสนองต่อกลยุทธ์ของโรงเรียนได้อย่างมีประสิทธิภาพ รวมถึงการสร้างผลกำไร และความยั่งยืนให้กับโรงเรียน

การนำเทคโนโลยีสารสนเทศเข้ามาใช้ในโรงเรียน มีต้นทุนค่าใช้จ่ายในการจัดซื้อทรัพยากร รวมถึงค่าใช้จ่ายทางด้านบุคลากรผู้พัฒนาระบบ จึงต้องมีการประเมินความคุ้มค่าก่อนการลงทุน เพื่อให้การลงทุนมีความเสี่ยงน้อย และคุ้มค่ามากที่สุด จากระบบที่ได้นำเสนอทั้ง 6 ระบบนั้น จะต้องนำมาประเมินเพื่อวิเคราะห์ความสำคัญของแต่ละระบบ และจัดลำดับความสำคัญ โดยรายละเอียดวิธีการที่จะใช้ประเมินโครงการมีดังนี้

- **การประเมินความคุ้มค่าของระบบสารสนเทศ**

ในการประเมินความคุ้มค่าของระบบสารสนเทศจะต้องวิเคราะห์จากประโยชน์ที่คาดว่าจะได้รับจากการลงทุน โดยผลตอบแทนของโครงการสามารถจำแนกได้ 2 ลักษณะ ดังนี้

(1) ประโยชน์ที่ไม่เป็นตัวเงิน (Intangible Benefits) เป็นผลตอบแทนที่ไม่ใช่ตัวเงิน ไม่สามารถวัดค่าได้ หรือยากแก่การประเมินค่า เช่น ความพึงพอใจของลูกค้า ภาพลักษณ์ที่ดีขององค์กร การสร้างขวัญและกำลังใจแก่พนักงาน เป็นต้น

(2) ประโยชน์ที่เป็นตัวเงิน (Tangible Benefits) เป็นผลตอบแทนที่สามารถประเมินค่าเป็นตัวเงินได้ เช่น การลดค่าใช้จ่าย เพิ่มยอดขาย เป็นต้น

- **การวิเคราะห์ Cost/Benefit Analysis ของแต่ละระบบ**

การวิเคราะห์โครงการด้วยเครื่องมือทางการเงินในครั้งนี้ ได้ใช้เครื่องมือทางการเงินทั้งสิ้น 2 ประเภท คือ

(1) มูลค่าปัจจุบันสุทธิ (Net Present Value: NPV) คือ ผลต่างระหว่างมูลค่าปัจจุบันของกระแสเงินสดรับสุทธิตลอดอายุของโครงการกับเงินลงทุนเริ่มแรก ณ อัตราผลตอบแทนที่ต้องการหรือต้นทุนของเงินทุนของโครงการ ซึ่งการวิเคราะห์ด้วยการใช้เครื่องมือนี้ ทำให้ทราบถึงมูลค่าปัจจุบันของโครงการ ณ วันสิ้นปี

(2) ระยะเวลาคืนทุน คือ จำนวนปีที่กิจการจะได้รับเงินที่จ่ายลงทุนในโครงการลงทุนกลับมา ซึ่งการวิเคราะห์ด้วยการใช้เครื่องมือนี้ทำให้ทราบถึงระยะเวลาในการคืนทุนของโครงการ

จากการประเมินผลการวิเคราะห์ทำให้สามารถสรุปลำดับการพัฒนาระบบสารสนเทศเพื่อตอบสนองกลยุทธ์ขององค์กรได้ดังนี้

ระยะที่ 1 : เป็นระบบที่ควรพัฒนาทันที เนื่องจากเกี่ยวข้องกับลูกค้าโดยตรง เพื่อเพิ่มรายได้ให้กับองค์กร

ระบบ S.E.L.F. เนื่องจากเป็นระบบหลักของการเรียนในโรงเรียนอยู่แล้ว จึงสามารถนำมาพัฒนาต่อยอดให้สามารถเรียนได้ผ่าน SmartPhone หรือ Tablet หรือการใช้งานผ่าน Applications โดยเป็นระบบที่เกี่ยวข้องกับกลุ่มนักเรียนมากที่สุด และมีโอกาสในการพัฒนาต่อยอดมากที่สุด

ระบบบริหารลูกค้าสัมพันธ์ ระบบนี้จะช่วยเพิ่มรายได้ให้กับโรงเรียนมากยิ่งขึ้น เนื่องจากมีการศึกษาข้อมูลของลูกค้า และนำเสนอข้อมูลการเรียน หรือสิทธิพิเศษได้อย่างตรงตามความต้องการของลูกค้ามากที่สุด โดยสามารถพัฒนาได้ทันที เพราะเป็นการต่อยอดจากระบบ XS และระบบ S.E.L.F. ซึ่งเป็นระบบหลักขององค์กรอยู่แล้ว

ระบบห้องสอบเสมือนจริง Simulation Exam ระบบนี้เป็นรูปแบบการทดสอบ ทำโจทย์ออนไลน์เป็นอีก 1 ช่องทางเลือกสำหรับนักเรียน สามารถพัฒนาได้ทันที โดยต่อยอดจากระบบเรียน S.E.L.F. และ Applications และพัฒนาเพิ่มในส่วนของช่องทางการชำระเงิน

ระยะที่ 2 : เป็นระบบที่สำคัญ เสริมสร้างการวางแผนงานกลยุทธ์ในระยะยาว

ระบบคลังข้อสอบ ระบบนี้เป็นการพัฒนาระบบจากระบบ S.E.L.F. โดยนำเนื้อหาการทำข้อสอบไปอยู่ใน Applications เชื่อมโยงกับสื่อประกอบการเรียนซึ่งระบบนี้ยังไม่เคยเกิดขึ้นมาก่อน แต่ในทางปฏิบัติสามารถทำได้ เพื่อเป็นอีกนวัตกรรมหนึ่งของการเรียน

ระบบการจัดการและบริหารองค์ความรู้ ระบบนี้จะช่วยเสริมสร้างแผนกลยุทธ์ของโรงเรียนในระยะยาวในการรวบรวมข้อมูลที่สำคัญจากทุกแผนก และนำมาแบ่งปันในแต่ละแผนกเพื่อนำไปใช้งานได้อย่างมีประสิทธิภาพได้ในอนาคต

ระบบจัดเก็บข้อมูลและฝึกอบรมพนักงาน ระบบนี้เป็นระบบรองรับการพัฒนาศักยภาพของพนักงานในแต่ละแผนกเพื่อให้มีความรู้ความชำนาญ และสามารถสร้างประโยชน์ให้เกิดกับองค์กรได้

การได้มาของระบบสารสนเทศทั้ง 6 ระบบนั้น จะดำเนินการพัฒนาโดยทีมงานระบบสารสนเทศของโรงเรียน และการซื้อโปรแกรมสำเร็จรูป และจากการคำนวณระยะเวลาคืนทุนของระบบที่พัฒนาทั้งหมด โดยที่มีการจัดสรรการใช้ทรัพยากรร่วมกันของทุกระบบจะสามารถคืนทุนได้ภายในไม่เกิน 3 ปี มีเพียงระบบเดียวคือ ระบบคลังข้อสอบที่ต้องอาศัยระยะเวลาในการคืนทุนมากกว่า 3 ปีขึ้นไป

การพิจารณาจัดสรรงบประมาณเพื่อพัฒนาระบบสารสนเทศตามนี้ จะนำไปสู่การพัฒนาโรงเรียนอย่างยั่งยืน มีการเจริญเติบโต และสามารถพัฒนาศักยภาพของบุคลากรในโรงเรียนให้สามารถทำงานได้อย่างมีประสิทธิภาพ รวมถึง การนำเทคโนโลยีมาช่วยในการปฏิบัติงานเพื่อลดต้นทุนของโรงเรียนได้

4. สรุปผลแผนด้านเทคโนโลยีสารสนเทศ

จากการวิเคราะห์สภาพแวดล้อมขององค์กรในปัจจุบัน โรงเรียนมีติวเตอร์ผู้สอนที่เป็นที่รู้จักในหมู่นักเรียน หรือผู้ปกครอง แต่โรงเรียนมีปัญหาที่ระบบ S.E.L.F. ซึ่งเป็นระบบหลักในการเรียนมักเกิดปัญหาบ่อยครั้ง และไม่มีกระบวนการในการตรวจสอบไฟล์วิดีโอการเรียน รวมถึงไม่มีการจัดการข้อมูลข่าวสารจากส่วนกลางอย่างเป็นระบบ ดังนั้นเพื่อเป็นการเสริมสร้างจุดแข็งและปรับจุดอ่อนของโรงเรียนด้วยการนำเทคโนโลยีสารสนเทศมาใช้ โรงเรียนควรนำตอบสนองการดำเนินแผนกลยุทธ์ด้วยการนำระบบ 6 ระบบมาใช้ คือ ระบบ S.E.L.F., ระบบจัดเก็บข้อมูลและฝึกอบรมพนักงาน, ระบบคลังข้อสอบ, ระบบข้อสอบเสมือนจริง Simulation Exam, ระบบการจัดการและบริหารองค์ความรู้, และระบบบริหารลูกค้าสัมพันธ์

บรรณานุกรม

เกื้อกูล จิตร์พล. (2554). *การศึกษาและพัฒนากลยุทธ์ในการหารายได้และบริการเพื่อเพิ่มความสามารถในการแข่งขันของสถาบันสอนภาษาศรีกลัย์วิทยา จังหวัดระยอง*. กรุงเทพฯ: มหาวิทยาลัยหอการค้าไทย.

ไทยรัฐออนไลน์. (2557). ธุรกิจกวดวิชามีมูลค่า 7.6 พันล้าน คาดปี 58 พุ่งอีก 5.4%. ดึงข้อมูลวันที่ 20 พฤศจิกายน 2557, จาก http://www.thairath.co.th/content/444743.

สมนึก ชูสุวรรณ. (2557). ภาษาอังกฤษของคนไทยกับความพร้อมสู่ประชาคมเศรษฐกิจอาเซียน. ดึงข้อมูลวันที่ 20 ตุลาคม 2557, จาก http://www.sjworldedu.com/blog/english-for-thai-citizen-to-aec.

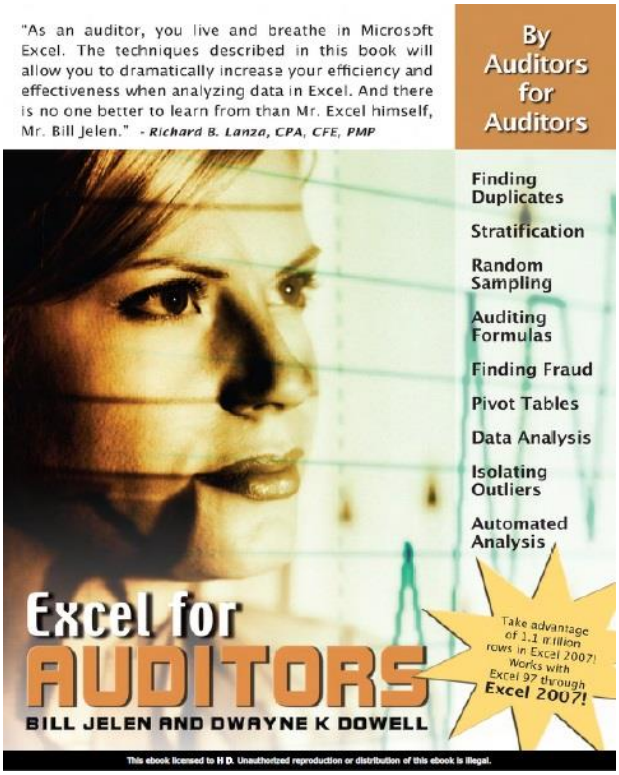
สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. (2557). ภาวะเศรษฐกิจไทยไตรมาสที่สี่ ทั้งปี 2557 และแนวโน้มปี 2558. ดึงข้อมูลวันที่ 17 กุมภาพันธ์ 2558, จาก http://www.nesdb.go.th/Portals/0/eco_datas/economic/eco_state/4_57/PressThaiQ4-2014.pdf.

ASTV ผู้จัดการออนไลน์. (2558). พ่อแม่หนุนเก็บภาษีโรงเรียนกวดวิชา ไม่หวั่นขึ้นค่าเรียน ห่วงครูกั๊กวิชาในชั้น. ดึงข้อมูลวันที่ 1 กุมภาพันธ์ 2558, จาก http://www.manager.co.th/QOL/ViewNews.aspx?NewsID=9580000011973.

Hemmatfar, M., and Bayat M. (2010). *Competitive Advantage and Strategic Information Systems*. Iran: Islamic Azad University.

บทวิจารณ์หนังสือ

นิตยา วงศ์ภินันท์วัฒนา
ภาควิชาระบบสารสนเทศเพื่อการจัดการ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
doi: 10.14456/jisb.2016.15



Title: Excel for Auditors

Author: Bill Jelen and Dwayne K Dowell

Edition: 1st Edition, 2007

Publisher: Holy Macro Books

Number of pages: 212

หนังสือ Excel for Auditors เป็นหนังสือที่กล่าวถึงการใช้คำสั่ง Excel เพื่อวิเคราะห์ข้อมูลให้ผู้ตรวจสอบทราบถึงสิ่งผิดปกติที่แสดงให้เห็นจากข้อมูล คำสั่งสำหรับการวิเคราะห์ข้อมูลด้วย Excel ประกอบด้วย

- การวิเคราะห์ในแนวนอน (Horizontal analysis)
- การวิเคราะห์ในแนวตั้ง (Vertical analysis)
- อัตราส่วน (Ratios)
- การวิเคราะห์แนวโน้ม (Trend analysis)
- สถิติ (Statistics)
- การจัดชั้น (Stratifications)
- การวิเคราะห์อายุหนี้ (Aging)

นอกเหนือจากการวิเคราะห์อายุลูกหนี้ดังกล่าวข้างต้นแล้วยังกล่าวถึงการวิเคราะห์ Pivot table เพื่อจัดสร้างรายงานในรูปแบบต่างๆ โดยไม่ต้องมีการเขียนโปรแกรม การตรวจสอบข้อมูลซ้ำ (Duplicate) การตรวจสอบข้อมูลกระโดด (Gap) โดยหนังสือเล่มนี้นอกจากจะกล่าวถึงการใช้คำสั่งของ Excel เพื่อช่วยในการตรวจสอบ ซึ่งเป็นคำสั่งของโปรแกรม ACL (Audit Control Language) ซึ่งเป็นโปรแกรมสำเร็จรูปเพื่อการตรวจสอบแล้ว ยังกล่าวถึงคำสั่งสำคัญอื่นๆ ของ Excel ที่ผู้ตรวจสอบสามารถนำมาช่วยวิเคราะห์ข้อมูลด้วยเช่นกัน

คำแนะนำในการส่งผลงานเผยแพร่

หลักเกณฑ์โดยทั่วไป

1. เป็นบทความวิจัย บทความการวางแผนด้านเทคโนโลยีสารสนเทศ บทความด้านการพัฒนาระบบสารสนเทศ บทความวิชาการหรือบทวิจารณ์หนังสือ ที่เน้นการใช้เทคโนโลยีสารสนเทศเพื่อธุรกิจเป็นหลัก
2. เป็นบทความวิจัย บทความการวางแผนด้านเทคโนโลยีสารสนเทศ บทความด้านการพัฒนาระบบสารสนเทศ บทความวิชาการหรือบทวิจารณ์หนังสือ **ที่ไม่เคยตีพิมพ์เผยแพร่ที่ใดมาก่อนและไม่อยู่ระหว่างการพิจารณาของวารสารอื่น หากตรวจพบว่ามีการตีพิมพ์ซ้ำซ้อน ถือเป็นความรับผิดชอบของผู้เขียนแต่เพียงผู้เดียว**
3. ไม่มีค่าใช้จ่ายใดๆ สำหรับผู้ส่งบทความวิจัย บทความการวางแผนด้านเทคโนโลยีสารสนเทศ บทความด้านการพัฒนาระบบสารสนเทศ บทความวิชาการหรือบทวิจารณ์หนังสือ
4. เป็นบทความวิจัย บทความการวางแผนด้านเทคโนโลยีสารสนเทศ บทความด้านการพัฒนาระบบสารสนเทศ บทความวิชาการหรือบทวิจารณ์หนังสือจะได้รับการเผยแพร่ในวารสาร JISB ต่อเมื่อได้ผ่านกระบวนการประเมินโดยผู้ทรงคุณวุฒิที่แต่งตั้งขึ้น

หลักเกณฑ์การประเมินบทความเพื่อการตอบรับตีพิมพ์

1. ผู้สนใจเสนอบทความสามารถจัดส่งบทความผ่านทางเว็บไซต์วารสาร http://jisb.tbs.tu.ac.th
2. กองบรรณาธิการจะพิจารณาบทความเบื้องต้นถึงความสอดคล้องของบทความที่จัดส่งมาว่าตรงกับวัตถุประสงค์ของวารสารหรือไม่ ถ้าไม่ตรงจะแจ้งกลับการพิจารณา
3. ถ้าบทความมีเนื้อหาสอดคล้องกับวารสาร กองบรรณาธิการจะพิจารณาความถูกต้องของรูปแบบการเตรียมข้อมูลต้นฉบับว่าตรงตามรูปแบบที่กำหนดในวารสาหรือไม่ ถ้าไม่ตรงจะแจ้งกลับการพิจารณา
4. ส่งบทความให้ผู้ทรงคุณวุฒิเพื่อประเมินบทความ เมื่อผลการประเมินผ่านหรือไม่ผ่านหรือมีการแก้ไขจะแจ้งให้ผู้เขียนทราบ เมื่อบทความได้รับการตีพิมพ์ ผู้เขียนจะได้รับการแจ้งกลับรับรองการตีพิมพ์ พร้อมทั้งแจ้งวันที่จะสามารถ download วารสารที่ได้ตีพิมพ์บนเว็บไซต์ต่อไป

การส่งบทความ

ผู้ที่ประสงคจะส่งบทความกับวารสารระบบสารสนเทศด้านธุรกิจ กรุณาส่งไฟล์ต้นฉบับบทความที่ http://jisb.tbs.tu.ac.th

คำแนะนำในการเตรียมต้นฉบับภาษาไทย/ภาษาอังกฤษ

เพื่อให้การตีพิมพ์ผลงานเป็นไปอย่างถูกต้องและรวดเร็วให้ผู้เขียนปฏิบัติตามรายละเอียดดังนี้

1. ต้นฉบับควรพิมพ์ด้วยกระดาษ A4 พิมพ์หน้าเดียว และพิมพ์ด้วย Microsoft Word เนื้อหาจัดพิมพ์เป็นแบบธรรมดา
2. รูปแบบ ขนาดและชนิดของตัวอักษร
   - บทความภาษาไทยใช้ BrowalliaUPC ส่วนบทความภาษาอังกฤษใช้ Time news roman
   - การตั้งหน้ากระดาษ บน ล่าง ซ้าย และขวา อย่างละ 1 นิ้ว ช่องห่างก่อนและหลังบรรทัด 0 pt และระหว่างบรรทัดเป็น At least และ page size เป็น letter (8.5” x 11”)
3. ตารางต้องมีชื่อตารางกำกับบนตาราง และภาพต้องมีชื่อภาพกำกับใต้ภาพ พร้อมทั้งให้หมายเลขเรียงลำดับสำหรับตารางและภาพ และให้อยู่ในเนื้อหา (ภาพให้จัดทำเป็น .jpeg แล้วนำมา insert ในบทความ)

รูปแบบการพิมพ์บทความ

1. ต้นฉับบภาษาไทย ใช้แบบอักษร BrowalliaUPC เนื้อหาขนาด 14 ตลอดทั้งบทความ ส่วนต้นฉบับภาษาอังกฤษ ใช้แบบอักษร Time news roman เนื้อหาขนาด 12 ตลอดทั้งบทความ ต้นฉบับควรพิมพ์ด้วยกระดาษ A4 พิมพ์หน้าเดียว และพิมพ์ด้วย Microsoft Word เนื้อหาจัดพิมพ์เป็นแบบธรรมดา พิมพ์ให้ห่างจากขอบทุกด้าน 1 นิ้วและใส่เลขกำกับทุกหน้าที่มุมขวาบนของกระดาษทุกหน้า
2. ประเภทข้อความ ขนาดและชนิดของตัวอักษร

ประเภทข้อความ	**ขนาด**	**ชนิด**
ชื่อเรื่อง (ภาษาไทย)	18 (จัดกึ่งกลางหน้ากระดาษ)	ตัวหนา
ชื่อผู้เขียน (ภาษาไทย) (กรณีมีผู้เขียนมากกว่าหนึ่งคนให้เรียงชื่อในบรรทัดถัดไป)	16 (จัดกึ่งกลางหน้ากระดาษ)	ตัวหนา
หน่วยงานที่สังกัดของผู้เขียน (ภาษาไทย)	14 (จัดกึ่งกลางหน้ากระดาษ)	ตัวธรรมดา
* Correspondence:	14 (ชิดซ้าย)	ตัวหนา
email ของนักวิจัยหลัก (จัดวางต่อท้าย correspondence:)	14 (ชิดซ้าย)	ตัวธรรมดา
เนื้อหากิตติกรรมประกาศ (ภาษาไทย) (ถ้ามี)	14 (ชิดซ้าย)	ตัวธรรมดา
บทคัดย่อ	16 (จัดชิดซ้ายหน้ากระดาษ)	ตัวหนา
เนื้อหาบทคัดย่อ (ภาษาไทย)	14 (จัดชิดซ้ายและชิดขวาหน้ากระดาษ)	ตัวธรรมดา
คำสำคัญ: (ภาษาไทย) (ไม่เกิน 5 คำ)	14 (ชิดซ้าย)	ตัวธรรมดา
ชื่อเรื่อง (ภาษาอังกฤษ)	18 (จัดกึ่งกลางหน้ากระดาษ)	ตัวหนา

ประเภทข้อความ	**ขนาด**	**ชนิด**
ชื่อผู้เขียน (ภาษาอังกฤษ) (กรณีมีผู้เขียนมากกว่าหนึ่งคนให้เรียงชื่อในบรรทัดถัดไป)	16 (จัดกึ่งกลางหน้ากระดาษ)	ตัวหนา
หน่วยงานที่สังกัดของผู้เขียน (ภาษาอังกฤษ)	14 (จัดกึ่งกลางหน้ากระดาษ)	ตัวธรรมดา
* Correspondence:	14 (ชิดซ้าย)	ตัวหนา
email ของนักวิจัยหลัก (จัดวางต่อท้าย correspondence:)	14 (ชิดซ้าย)	ตัวธรรมดา
Acknowledgement: (ถ้ามี)	14 (ชิดซ้าย)	ตัวธรรมดา
Abstract	16 (จัดชิดซ้ายหน้ากระดาษ)	ตัวหนา
เนื้อหาบทคัดย่อ (ภาษาอังกฤษ)	14 (จัดชิดซ้ายและชิดขวาหน้ากระดาษ)	ตัวธรรมดา
Keywords: (ภาษาอังกฤษ) (ไม่เกิน 5 คำ)	14 (ชิดซ้าย)	ตัวธรรมดา
หัวข้อใหญ่ (ใส่หมายเลขเรียงลำดับ)	16 (ชิดซ้าย)	ตัวหนา
หัวข้อย่อย (ใส่หมายเลขย่อยเรียงลำดับตามหัวข้อใหญ่)	14 (ชิดซ้าย)	ตัวหนา
เนื้อหาภายใต้หัวข้อ	14 (จัดชิดซ้ายและชิดขวาหน้ากระดาษ)	ตัวธรรมดา

3. องค์ประกอบของเนื้อหาในบทความวิจัย ความยาวต้นฉบับ 10-15 หน้า ลำดับหัวข้อบทความมีดังนี้
   - ชื่อบทความวิจัย ไม่ยาวเกินไปแต่ครอบคลุมสาระทั้งเรื่อง มีทั้งภาษาไทยและภาษาอังกฤษ
   - ชื่อผู้เขียน ภาษาไทยและภาษาอังกฤษ
   - หน่วยงานที่สังกัดของผู้เขียน ภาษาไทยและภาษาอังกฤษ
   - บทคัดย่อ และ Abstract
   - เนื้อหาบทคัดย่อ ภาษาไทยและภาษาอังกฤษ เป็นการสรุปสาระสำคัญของเรื่องความยาวประมาณ 150-200 คำ มีทั้งภาษาไทยและภาษาอังกฤษ ท้ายภาษาอังกฤษให้ใส่ e-mail ของ corresponding author กรณีมีชื่อผู้เขียนหลายคน
   - คำสำคัญ (ไม่เกิน 5 คำ) ภาษาไทยและภาษาอังกฤษ ให้ใส่ใต้เนื้อหาบทคัดย่อ และ Abstract
   - เนื้อหาของบทความวิจัย
     - 1. บทนำ กล่าวถึงเหตุผล ความจำเป็นที่จัดทำวิจัย วัตถุประสงค์ของการวิจัยและคำถามการวิจัย
     - 2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง
     - 3. กรอบแนวคิการวิจัยและสมมติฐานการวิจัย (กรณีงานวิจัยเชิงคุณภาพสามารถปรับเปลี่ยนให้เหมาะสมกับงานวิจัยที่จัดทำ)
     - 4. วิธีการวิจัย

- 5. ผลการวิจัย
- 6. สรุปผลการวิจัย กล่าวถึงบทสรุปการวิจัย การประยุกต์ใช้งานวิจัยในเชิงธุรกิจ ข้อจำกัดและวิจัยในอนาคต
- บรรณานุกรม (ตามรูปแบบการอ้างอิงข้างล่าง)
- ภาคผนวก (ถ้ามี)

กรณีที่บทความมีหัวข้อย่อย ให้ใส่หมายเลข X.X เรียงลำดับกันไป ไม่ควรมีหัวข้อย่อยเกิน 3 ลำดับย่อย เช่น X.X.X เป็นต้น

4. องค์ประกอบของเนื้อหาในบทความการวางแผนด้านเทคโนโลยีสารสนเทศ ความยาวต้นฉบับ 10-15 หน้า ลำดับหัวข้อบทความมีดังนี้
   - ชื่อบทความ ไม่ยาวเกินไปแต่ครอบคลุมสาระทั้งเรื่อง มีทั้งภาษาไทยและภาษาอังกฤษ
   - ชื่อผู้เขียน ภาษาไทยและภาษาอังกฤษ
   - หน่วยงานที่สังกัดของผู้เขียน ภาษาไทยและภาษาอังกฤษ
   - บทคัดย่อ และ Abstract
   - เนื้อหาบทคัดย่อ ภาษาไทยและภาษาอังกฤษ เป็นการสรุปสาระสำคัญของเรื่องความยาวประมาณ 150-200 คำ มีทั้งภาษาไทยและภาษาอังกฤษ ท้ายภาษาอังกฤษให้ใส่ e-mail ของ corresponding author กรณีมีชื่อผู้เขียนหลายคน
   - คำสำคัญ (ไม่เกิน 5 คำ) ภาษาไทยและภาษาอังกฤษ ให้ใส่ใต้เนื้อหาบทคัดย่อ และ Abstract
   - เนื้อหาของบทความ
     - 1. บทนำ กล่าวถึงเหตุผลและความจำเป็นที่จัดทำแผนด้านเทคโนโลยีสารสนเทศ
     - 2. ภาพรวมองค์กร
     - 3. การวิเคราะห์องค์กร
     - 4. แผนกลยุทธ์ที่เสนอแนะ
     - 5. สรุปผลแผนด้านเทคโนโลยีสารสนเทศ
     - บรรณานุกรม (ตามรูปแบบการอ้างอิงข้างล่าง)
     - ภาคผนวก (ถ้ามี)

   กรณีที่บทความมีหัวข้อย่อย ให้ใส่หมายเลข X.X เรียงลำดับกันไป ไม่ควรมีหัวข้อย่อยเกิน 3 ลำดับย่อย เช่น X.X.X เป็นต้น
5. องค์ประกอบของเนื้อหาในบทความการพัฒนาระบบสารสนเทศ ความยาวต้นฉบับ 10-15 หน้า ลำดับหัวข้อบทความมีดังนี้
   - ชื่อบทความ ไม่ยาวเกินไปแต่ครอบคลุมสาระทั้งเรื่อง มีทั้งภาษาไทยและภาษาอังกฤษ
   - ชื่อผู้เขียน ภาษาไทยและภาษาอังกฤษ
   - หน่วยงานที่สังกัดของผู้เขียน ภาษาไทยและภาษาอังกฤษ
   - บทคัดย่อ และ Abstract
   - เนื้อหาบทคัดย่อ ภาษาไทยและภาษาอังกฤษ เป็นการสรุปสาระสำคัญของเรื่องความยาวประมาณ 150-200 คำ มีทั้งภาษาไทยและภาษาอังกฤษ ท้ายภาษาอังกฤษให้ใส่ e-mail ของ corresponding author กรณีมีชื่อผู้เขียนหลายคน
   - คำสำคัญ (ไม่เกิน 5 คำ) ภาษาไทยและภาษาอังกฤษ ให้ใส่ใต้เนื้อหาบทคัดย่อ และ Abstract
   - เนื้อหาของบทความ

- 1. บทนำ กล่าวถึงเหตุผลและความจำเป็นในการพัฒนาระบบสารสเทศ
- 2. ขอบเขตการทำงานของระบบสารสนเทศ
- 3. สถาปัตยกรรมของระบบที่พัฒนา
- 4. สรุปผลระบบสารสนเทศ กล่าวถึงประโยชน์ของระบบที่พัฒนา
- บรรณานุกรม (ตามรูปแบบการอ้างอิงข้างล่าง)
- ภาคผนวก (ถ้ามี)

กรณีที่บทความมีหัวข้อย่อย ให้ใส่หมายเลข X.X เรียงลำดับกันไป ไม่ควรมีหัวข้อย่อยเกิน 3 ลำดับย่อย เช่น X.X.X เป็นต้น

6. องค์ประกอบของเนื้อหาในบทความวิชาการและบทความเกี่ยวกับงานสร้างสรรค์ ความยาวต้นฉบับ 10-15 หน้า ลำดับหัวข้อบทความมีดังนี้
   - ชื่อเรื่องไม่ยาวเกินไปแต่ครอบคลุมสาระทั้งเรื่อง มีทั้งภาษาไทยและภาษาอังกฤษ
   - ชื่อผู้เขียนและชื่อหน่วยงานหรือสถาบันที่สังกัดเป็นภาษาไทยและภาษาอังกฤษ ชื่อผู้เขียนไม่ต้องใส่ตำแหน่งวิชาการ
   - บทคัดย่อ และ Abstract
   - บทคัดย่อ เป็นการสรุปสาระสำคัญของเรื่องความยาวประมาณ 150-200 คำ มีทั้งภาษาไทยและภาษาอังกฤษ ท้ายภาษาอังกฤษให้ใส่ e-mail ของ corresponding author กรณีมีชื่อผู้เขียนหลายคน
   - เนื้อหาของบทความ (บทความที่เป็นงานแปลหรือเรียบเรียงต้องบอกแหล่งที่มาอย่างละเอียด)
   - การอ้างอิงในเนื้อเรื่องใช้ตามรูปแบบข้างล่าง (ถ้ามี)
7. องค์ประกอบของเนื้อหาในบทวิจารณ์หนังสือ ความยาวต้นฉบับ 2-4 หน้า ลำดับหัวข้อบทความมีดังนี้
   - ชื่อหนังสือที่วิจารณ์
   - ชื่อผู้เขียนหนังสือที่วิจารณ์และสำนักพิมพ์
   - ชื่อผู้วิจารณ์และชื่อหน่วยงานหรือสถาบันที่สังกัดเป็นภาษาไทย
   - เนื้อหาบทวิจารณ์หนังสือ (กระชับและได้ใจความ)

รูปแบบการอ้างอิง

1. การอ้างอิงแบบแทรกในเนื้อหา

เป็นการระบุแหล่งอ้างอิงแบบย่อซึ่งการอ้างอิงจะแยกพิจารณาเป็น 2 กรณี ดังนี้

กรณีที่ 1 ข้อความที่ผู้เขียนคัดลอกมาจากข้อเขียนหรือคำพูดของผู้อื่น เพื่อใช้ประกอบเนื้อเรื่องในวิจัย ต้องใส่เครื่องหมายอัญประกาศ (Quotations) คู่ไว้ด้วย เช่น "....." พร้อมกับอ้างอิงแหล่งที่มาของข้อความ ซึ่งมีรูปแบบ ดังนี้

- **ผู้แต่งคนเดียว** ให้ระบุชื่อต่อด้วยชื่อสกุลของผู้แต่ง ต่อด้วยเครื่องหมายจุลภาค ปีที่พิมพ์ เครื่องหมายจุลภาค เลขที่หน้าอ้างอิง สำหรับเอกสารภาษาไทย ให้ระบุชื่อและนามสกุลของผู้แต่ง สำหรับเอกสารภาษาอังกฤษ ให้ระบุนามสกุลของผู้แต่ง เช่น (นงลักษณ์ วิรัชชัย, 2542, น. 3) หรือ (Weber, 1999, p. 234)

- **ผู้แต่งสองคน** ให้ระบุชื่อและชื่อสกุลของผู้แต่งทั้ง 2 คน ทุกครั้งที่มีการอ้างโดยใช้คำว่า “และ” สำหรับเอกสารภาษาไทย หรือ “and” เชื่อมชื่อสกุลของผู้แต่งสำหรับเอกสารภาษา ต่างประเทศ เช่น (ผ่องพรรณ ตรัยมงคลกูล และสุภาพ ฉัตราภรณ์, 2545, น. 4-8) หรือ (Franz and Robey, 1984, p. 250)

- **ผู้แต่งสามคนขึ้นไป** การอ้างถึงทุกๆ ครั้งให้ระบุชื่อและชื่อสกุลของผู้แต่งคนแรก แล้วตามด้วย “และคณะ” สำหรับเอกสารภาษาไทย และระบุเฉพาะชื่อสกุลของผู้แต่งคนแรก แล้วตามด้วย “et al.” สำหรับเอกสารภาษาอังกฤษ เช่น (สุรพงษ์ โสธนะเสถียร และคณะ, 2545, น. 9-14) หรือ (Alexander et al., 2003, p. 154)

- **ผู้แต่งที่เป็นสถาบัน** ชื่อสถาบันที่อ้าง ระบุชื่อเต็มทุกครั้ง เช่น (มหาวิทยาลัยธรรมศาสตร์, คณะพาณิชยศาสตร์และการบัญชี, 2535, น. 12-23)

- **ผู้แต่งคนเดียวเขียนเอกสารหลายเล่ม แต่ละเล่มพิมพ์ต่างปีกัน และต้องการอ้างถึง พร้อมกัน** ให้เรียงลำดับเอกสารหลายเรื่องนั้นไว้ตามลำดับของปีที่พิมพ์ โดยใช้เครื่องหมาย ; คั่น เช่น (สุวิมล ว่องวาณิช, 2553, น. 22; 2554, น. 90) หรือ (Benbasat, 1998, p. 283; 1999, p. 78)

- **ผู้แต่งคนเดียวเขียนเอกสารหลายเล่ม พิมพ์ปีซ้ำกัน** ให้ใช้อักษรตัวแรกของชื่อเรื่อง เช่น ก ข ค ง เป็นต้น ตามหลังปีสำหรับเอกสารภาษาไทยและใช้ตัวอักษรตัวแรกของชื่อเรื่อง เช่น a b c d เป็นต้น ตามหลังปีสำหรับ เอกสารภาษาต่างประเทศ เช่น (ศุภกิจ วงศ์วิวัฒน์นนุกิจ, 2550ก, น. 22), (ศุภกิจ วงศ์วิวัฒน์นนุกิจ, 2550ข, น. 22), (Yin, 1998a, p. 5-9) หรือ (Yin, 1998b, p. 31-40)

- **ผู้แต่งหลายคน เอกสารหลายเรื่อง และต้องการอ้างอิงถึงพร้อม ๆ กัน** ให้ระบุชื่อผู้แต่งเรียง ตามลำดับอักษร คั่นด้วยเครื่องหมาย ; สำหรับเอกสารภาษาไทยและ ให้ระบุชื่อสกุลของผู้แต่งเรียงตามลำดับ อักษรคั่นด้วยเครื่องหมาย ; สำหรับเอกสารภาษาอังกฤษ เช่น (ผ่องพรรณ ตรัยมงคลกูล และสุภาพ ฉัตราภรณ์, 2545, น. 10; สุวิมล ว่องวาณิช, 2553, น. 45-50) หรือ (Weber et al., 1999, p. 180; Benbasat, 1998, p. 120)

กรณีที่ 2 ข้อความที่ผู้เขียนประมวลมาจากข้อเขียนหรือคำพูดของผู้อื่นเพื่อใช้ประกอบเนื้อเรื่องในงานวิจัย ให้อ้างอิงแหล่งที่มาของข้อมูลที่ประมวลมาโดย**ไม่**ต้องใส่เครื่องหมายอัญประกาศคู่ ระหว่างข้อความ แต่ให้อ้างอิงแหล่งที่มาของข้อความซึ่งมีรูปแบบเช่นเดียวกับกรณีที่ 1 โดย**ไม่**ต้องใส่เลขหน้าที่อ้างอิง

กรณีอื่น ๆ กรณีที่ไม่ได้อ่านบทความที่อ้างอิงในบทความที่อ่าน ให้ระบุชื่อผู้แต่งแล้วตามด้วย อ้างถึงใน กรณีเป็น) บทความภาษาไทย) สุชาติ ประสิทธิ์รัฐสินธุ์ (2554 อ้างถึงใน สุรพงษ์ โสธนะเสถียร, 2554) หรือ as cited in เช่น (Yin, 1998, as cited in Benbasat, 2002).

2. การอ้างอิงในบรรณานุกรม

กรณีหนังสือ มีรูปแบบ ดังนี้

ชื่อ ชื่อสกุลผู้แต่ง (กรณีหนังสือภาษาไทย). (ปีที่พิมพ์). *ชื่อหนังสือและลำดับที่ (ตัวเอียง).* สถานที่พิมพ์: สำนักพิมพ์หรือโรงพิมพ์,.

ชื่อสกุล, ชื่อ (อักษรตัวแรกของชื่อตามด้วยจุด) ผู้แต่ง (กรณีหนังสือภาษาอังกฤษ). (ปีที่พิมพ์). *ชื่อหนังสือและลำดับที่ (ตัวเอียง).* สถานที่พิมพ์: สำนักพิมพ์หรือโรงพิมพ์,.

ตัวอย่าง

สุชาติ ประสิทธิ์รัฐสินธุ์. (2544). *ระเบียบวิธีการวิจัยทางสังคมศาสตร์.* กรุงเทพฯ: บริษัทเฟื่องฟ้า พริ้นติ้ง จำกัด.

Weber, R. (1999). *Information Systems Control and Audit.* New Jersy: Prentice Hall.

กรณีบทความในวารสาร มีรูปแบบ ดังนี้

ชื่อ ชื่อสกุลผู้แต่ง (กรณีวารสารภาษาไทย). (ปีที่พิมพ์). ชื่อบทความ. *ชื่อวารสาร (ตัวเอียง),* ฉบับที่ (เล่มที่), หน้า.

ชื่อสกุล, ชื่อ (อักษรตัวแรกของชื่อตามด้วยจุด) ผู้แต่ง (กรณีวารสารภาษาอังกฤษ). (ปีที่พิมพ์). ชื่อบทความ. *ชื่อวารสาร (ตัวเอียง),* ฉบับที่ (เล่มที่), หน้า.

ตัวอย่าง

วัจนา รัตนวร. (2548). ความล้มเหลวของสถาบันการเงิน. *บริหารธุรกิจ*, 12 (1), 50-55.

Benbasat, I., Goldstein, D. K. and Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, 37(10), 369-386.

กรณีข้อมูลจาก Internet มีรูปแบบ ดังนี้

ชื่อ ชื่อสกุลผู้แต่ง (กรณีบทความภาษาไทย). (ปีที่พิมพ์). ชื่อบทความ. วันเดือนปีที่ดึงข้อมูล, ชื่อ Web address.

ชื่อสกุล, ชื่อ (อักษรตัวแรกของชื่อตามด้วยจุด) ผู้แต่ง (กรณีบทความภาษาอังกฤษ). (ปีที่พิมพ์). ชื่อบทความ. Retrieved month date, year, from http://Web address.

ตัวอย่าง

วัจนา รัตนวร. (2548). ความล้มเหลวของสถาบันการเงิน. ดึงข้อมูลวันที่ 17 มีนาคม 2550, จาก www.bus.tu.ac.th.

Grace Fleming. (2007). Choosing a Strong Research Topic. Retrieved January 12, 2009, from http://homeworktips.about.com/od/researchandreference/a/topic.htm.

ในกรณีที่ไม่มีชื่อผู้เขียนบทความ และไม่มีปีให้อ้างอิงดังตัวอย่างข้างล่าง

GVU's 8th WWW user survey. (n.d.). Retrieved September 19, 2001, from http://www.cc.gatech.edu/gvu/user_surveys/survey-1997-10/.

กรณีข้อมูลจากสัมมนาทางวิชาการ มีรูปแบบ ดังนี้

ชื่อ ชื่อสกุลผู้แต่ง (กรณีบทความภาษาไทย). (ปีที่พิมพ์). ชื่อบทความ. *ชื่อสัมมนาทางวิชาการ (ตัวเอียง),* สถานที่, หน้า.

ชื่อสกุล, ชื่อ (อักษรตัวแรกของชื่อตามด้วยจุด) ผู้แต่ง (กรณีบทความภาษาอังกฤษ). (ปีที่พิมพ์). ชื่อบทความ. *ชื่อสัมมนาทางวิชาการ (ตัวเอียง),* สถานที่, หน้า.

ตัวอย่าง

Bonoma, T. V. (1983). A Case Study in Case Research: Marketing Implementation. *Proceedings of the National Academy of Sciences,* USA, 89-102.

กรณีข้อมูลจากวิทยานิพนธ์ มีรูปแบบ ดังนี้

ชื่อ ชื่อสกุลผู้แต่ง (กรณีบทความภาษาไทย). (ปีที่พิมพ์). *ชื่อเรื่องวิทยานิพนธ์ (ตัวเอียง).* วิทยานิพนธ์ที่ยังไม่ได้ตีพิมพ์, ชื่อมหาวิทยาลัย.

ชื่อสกุล, ชื่อ (อักษรตัวแรกของชื่อตามด้วยจุด) ผู้แต่ง (กรณีบทความภาษาอังกฤษ). (ปีที่พิมพ์). *ชื่อเรื่องวิทยานิพนธ์ (ตัวเอียง).* Unpublished doctoral dissertation, ชื่อมหาวิทยาลัย.

ตัวอย่าง

Ross, D. F. (1990). *Unconscious transference and mistaken identity: When a witness misidentifies a familiar but innocent person from a lineup*. Unpublished doctoral dissertation, Cornell University, NY.

กรณีข้อมูลจากหนังสือรวมบทความ มีรูปแบบ ดังนี้

ชื่อ ชื่อสกุลผู้แต่ง (กรณีบทความภาษาไทย). (ปีที่พิมพ์). ชื่อบทความ. ใน ชื่อ ชื่อสกุลของบรรณาธิการ (บรรณาธิการ), ชื่อหนังสือรวมบทความ (หน้า). สำนักพิมพ์.

ชื่อสกุล, ชื่อ (อักษรตัวแรกของชื่อตามด้วยจุด) ผู้แต่ง (กรณีบทความภาษาอังกฤษ). (ปีที่พิมพ์). In ชื่อ (อักษรตัวแรกของชื่อตามด้วยจุด) ชื่อสกุล (Ed.), ชื่อหนังสือรวมบทความ (หน้า). สำนักพิมพ์.

ตัวอย่าง

Benbasat, I. (1984). An Analysis of Research Methodologies. In F. Warren McFarlan (Ed.), The Information Systems Research Challenge (pp. 47-85). Boston: Harvard Business School Press.

กรณีข้อมูลจากสัมมนา มีรูปแบบ ดังนี้

ชื่อ ชื่อสกุลผู้แต่ง (กรณีบทความภาษาไทย). (ปีที่พิมพ์). *ชื่อบทความ. ชื่อสัมมนา, สถานที่, ครั้งที่ (ตัวเอียง),* หน้า.

ชื่อสกุล, ชื่อ (อักษรตัวแรกของชื่อตามด้วยจุด) ผู้แต่ง (กรณีบทความภาษาอังกฤษ). (ปีที่พิมพ์). ชื่อบทความ. *ชื่อสัมมนา, สถานที่, ครั้งที่ (ตัวเอียง),* หน้า.

ตัวอย่าง

Franz, C. R. and Robey, D. (1984). An Investigation of User-Led System Design: Rational and Political Perspectives. *Proceedings of the National Academy of Sciences, USA, 89,* 1372-1375.

กรณีข้อมูลจากงานแปล มีรูปแบบ ดังนี้

ชื่อ ชื่อสกุลผู้แต่ง (กรณีบทความภาษาไทย). (ปีที่พิมพ์). *ชื่อบทความ (ตัวเอียง)* (ชื่อ ชื่อสกุลผู้แปล, ผู้แปล). สำนักพิมพ์. (ต้นฉบับตีพิมพ์ในปี ปีที่ตีพิมพ์.)

ชื่อสกุล, ชื่อ (อักษรตัวแรกของชื่อตามด้วยจุด) ผู้แต่ง (กรณีบทความภาษาอังกฤษ). (ปีที่พิมพ์). *ชื่อบทความ (ตัวเอียง)* (ชื่อ (อักษรตัวแรกของชื่อตามด้วยจุด) ชื่อสกุล, Trans.). สำนักพิมพ์. (Original work published ปีที่ตีพิมพ์.)

ตัวอย่าง

Freud, S. (1970). *An outline of psychoanalysis* (J. Strachey, Trans.). New York: Norton. (Original work published 1940.)

กรณีข้อมูลจากบทสัมภาษณ์ มีรูปแบบ ดังนี้

ชื่อ ชื่อสกุลผู้แต่ง (กรณีบทความภาษาไทย). (ปีที่พิมพ์). [สัมภาษณ์ ชื่อ-ชื่อสกุลผู้สัมภาษณ์, ตำแหน่ง]. *ชื่อบทความ (ตัวเอียง),* ฉบับที่, หน้า.

ชื่อสกุล, ชื่อ (อักษรตัวแรกของชื่อตามด้วยจุด) ผู้แต่ง (กรณีบทความภาษาอังกฤษ). (ปีที่พิมพ์). [Interview with ชื่อ-ชื่อสกุลผู้สัมภาษณ์, ตำแหน่ง]. *ชื่อบทความ (ตัวเอียง),* ฉบับที่, หน้า.

ตัวอย่าง

Weber, R. (2003). [Interview with Robert Yin, author of Case study research]. *MIS Quarterly,* 21(10)*,* 211-216.