JISB JOURNAL
วารสารระบบสารสนเทศด้านธุรกิจ
Journal of Information Systems in Business
ISSN 2465-4264
ปีที่ 4 ฉบับที่ 3 กรกฎาคม - กันยายน 2561

IT Audit

www.jisb.tbs.tu.ac.th

บทความ

บทวิจารณ์หนังสือ

บทบรรณาธิการ

เรียน ผู้อ่านทุกท่าน

วารสารฉบับนี้มีบทความส่วนใหญ่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศ ไม่ว่าจะเป็นคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT ประสิทธิภาพของงานตรวจสอบภายใน: มุมมองของผู้ตรวจสอบภายใน การส่งเสริมให้พนักงานในองค์กรแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ และรูปแบบการฝึกอบรมที่เหมาะสมกับทักษะในงานทางด้านเทคโนโลยีสารสนเทศ นอกจากนี้ยังกล่าวเกี่ยวกับการสร้างแรงจูงใจในการสร้างองค์ความรู้ใหม่ในระบบการจัดการความรู้ขององค์การ หวังว่าผู้อ่านทุกท่านจะได้รับสาระและสามารถนำผลการวิจัยนี้ไปปรับใช้ให้เกิดประโยชน์ ตามความเหมาะสมต่อไป

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
รองศาสตราจารย์ ดร.ปิเตอร์ รักธรรม	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ผู้ช่วยศาสตราจารย์ ดร.มฑุปายาส ทองมาก	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ผู้ช่วยศาสตราจารย์ ดร.ลัดดาวัลย์ แก้วกิติพงษ์	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ผู้ช่วยศาสตราจารย์โอภาศ โสตถิลักษณ์	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ผู้ช่วยศาสตราจารย์วันชัย ขันตี	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

กองบรรณาธิการกลั่นกรองบทความ (ภายใน)

รองศาสตราจารย์ ดร.ศากุน บุญอิต	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ผู้ช่วยศาสตราจารย์ ดร.พัฒน์ธนะ บุญชู	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ผู้ช่วยศาสตราจารย์ 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
รองศาสตราจารย์ ดร.พิศสมัย อรทัย	คณะแพทยศาสตร์โรงพยาบาลรามาธิบดี มหาวิทยาลัยมหิดล
ผู้ช่วยศาสตราจารย์ ดร.ชัชพงศ์ ตั้งมณี	คณะพาณิชยศาสตร์และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย
ผู้ช่วยศาสตราจารย์ ดร.นิลุบล ศิวบวรวัฒนา	คณะบริหารธุรกิจ มหาวิทยาลัยศรีปทุม
ผู้ช่วยศาสตราจารย์ ดร.ภัทร์ พลอยแหวน	คณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล
ผู้ช่วยศาสตราจารย์ ดร.วิเลิศ ภูริวัชร	คณะพาณิชยศาสตร์และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย
ผู้ช่วยศาสตราจารย์ 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

ปัจจัยที่มีผลต่อคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT

ชัชพงศ์ อธิปัญญาวงศ์*

บริษัท อีซี่ บาย จำกัด (มหาชน)

***Correspondence:** chatpong.ath@gmail.com

doi: 10.14456/jisb.2018.12

วันที่รับบทความ: 1 ส.ค. 2560 วันแก้ไขบทความ: 3 ก.ย. 2560 วันตอบรับบทความ: 17 ก.ย. 2560

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ส่งผลต่อคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT ซึ่งเป็นงานวิจัยเชิงปริมาณและผู้วิจัยพัฒนากรอบแนวคิดคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT จากโมเดลปัจจัยที่ส่งผลต่อคุณภาพการตรวจสอบเทคโนโลยีสารสนเทศ และกรอบแนวคิด COBIT ที่พัฒนาโดย ISACA การวิจัยนี้มีปัจจัยเพิ่มจากการศึกษาในอดีตที่ผ่านมาได้แก่ วุฒิภาวะการประยุกต์ใช้กระบวนการของกรอบแนวคิด COBIT ในการตรวจสอบ และระดับความสำคัญของกลุ่มกระบวนการตามกรอบแนวคิด COBIT ที่มีต่อองค์กร รวมถึงปัจจัยคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศ โดยทำการศึกษากลุ่มประชากรในองค์กรธุรกิจที่เป็นบริษัทที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย โดยไม่รวมบริษัทที่อยู่ในระหว่างการฟื้นฟูกิจการ และบริษัทจดทะเบียนในตลาดหลักทรัพย์เอ็มเอไอ และไม่รวมบริษัทที่ว่าจ้างหรือแต่งตั้งบริษัทภายนอก (Outsource) ให้ดำเนินงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ โดยแบบสอบถามที่สมบูรณ์และนำมาใช้ประกอบงานวิจัยครั้งนี้ มีจำนวนทั้งสิ้น 118 ชุด จากนั้นผู้วิจัยได้นำแบบสอบถามที่สมบูรณ์มาประมวลผลด้วยโปรแกรมสำเร็จรูปทางสถิติ และโปรแกรมการวิเคราะห์สมการเชิงโครงสร้าง ผลการวิจัยพบว่า คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ มีอิทธิพลต่อ คุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT โดยมีองค์ประกอบที่สำคัญ เรียงตามลำดับค่าสัมประสิทธิ์อิทธิพลที่มากที่สุด ดังนี้ (1) ระดับความสำคัญของกลุ่มกระบวนการตามกรอบแนวคิด COBIT ที่มีต่อองค์กร (2) การวิเคราะห์ความเสี่ยง (3) วุฒิภาวะการประยุกต์ใช้กระบวนการของกรอบแนวคิด COBIT ในการตรวจสอบ ตามลำดับ

คำสำคัญ: การตรวจสอบเทคโนโลยีสารสนเทศ กรอบแนวคิด COBIT การสร้างคุณค่า

Factors affecting the Value Creation to organization in Information Technology Audit from COBIT framework

Chatpong Athipanyawong*

Easy Buy Public Company Limited

***Correspondence:** chatpong.ath@gmail.com
doi: 10.14456/jisb.2018.12

Received: 1 Aug 2017 Revised: 3 Sep 2017 Accepted: 17 Sep 2017

Abstract

The objective of this study is to examine the factors influencing the value creation to organization in Information Technology (IT) Audit from COBIT framework. This research is quantitative research, and refined by the theoretical framework for the internal IT audit process, and COBIT 5 framework that was released by ISACA. The study was extended to prior research by identification of a set of factors from COBIT framework comprises COBIT capability, and Importance of COBIT process domain to organization, and include factors affecting the value creation to organization in Information Technology Audit. The sample of this study is based on a survey of 118 IT audit related officers as subjects: Audit Executive, Head of Internal Audit Officer, or Head of IT Audit Officer, and Internal Auditor, or IT auditor that operates to IT audit of Thai listed companies (not including the companies listed in MAI, and those under rehabilitation, and outsourcing audit) additionally, researcher selected the completed surveys to analyze the study by statistical package software and Structural Equation Modeling (SEM) analysis software. The research result showed that IT audit quality factor affects the value creation to organization in Information Technology Audit, and the factor affecting IT audit quality include (1) Importance of COBIT process domain to organization has the most significant effect, and (2) Risk Analysis, and (3) COBIT capability has significant effect on IT audit Quality as well.

Keywords: IT audit, COBIT framework, Value creation

1. บทนำ

1.1 ความสำคัญและที่มาของปัญหา

สารสนเทศถือได้ว่าเป็นทรัพยากรสำคัญสำหรับทุกองค์กรธุรกิจ และ เทคโนโลยีก็เข้ามามีบทบาทอย่างมีนัยสำคัญ (ISACA, 2012) ด้วยความก้าวหน้าด้านเทคโนโลยีสารสนเทศ ทำให้องค์กรธุรกิจเลือกใช้เทคโนโลยีสารสนเทศเป็นกลยุทธ์เพื่อสร้างการเติบโตและความสำเร็จให้แก่องค์กรในการเพิ่มผลผลิต ลดต้นทุน และเพิ่มประสิทธิภาพในการดำเนินงาน (สมาคมผู้ตรวจสอบภายในแห่งประเทศไทยและตลาดหลักทรัพย์แห่งประเทศไทย, 2555) ในขณะเดียวกันการใช้เทคโนโลยีสารสนเทศก็มีความเสี่ยงหลายประการที่ควรคำนึงถึง ถ้าหากองค์กรธุรกิจไม่มีการบริหารจัดการและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่รัดกุมเพียงพอ ก็อาจส่งผลกระทบต่อองค์กรธุรกิจได้ ดังนั้นการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศจึงเป็นเรื่องที่องค์กรธุรกิจต้องให้ความสำคัญ เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการประกอบธุรกิจนั้นเกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น (สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2545) การตรวจสอบเทคโนโลยีสารสนเทศ จึงเป็นตัววัดที่ใช้พิจารณาประเมินว่าองค์กรธุรกิจได้จัดการความเสี่ยงด้านระบบสารสนเทศเพื่อให้องค์กรธุรกิจบรรลุวัตถุประสงค์ขององค์กรได้มากน้อยเพียงใด หากยังพบว่ามีความเสี่ยงสูงก็จะมีผลกระทบต่อการจัดการความเสี่ยงโดยรวมขององค์กร (ครรชิต มาลัยวงศ์, 2553)

กรอบแนวคิด COBIT เมื่อครั้งแรกเริ่มได้พัฒนามาจากมุมมองการตรวจสอบระบบสารสนเทศ ในปี ค.ศ. 1996 โดยกรอบแนวคิด COBIT ในแต่ละรุ่นได้พัฒนาให้ตอบสนองต่อความต้องการทางธุรกิจขององค์กร เพื่อบริหารจัดการสารสนเทศและเทคโนโลยีที่สนับสนุนสารสนเทศทางธุรกิจยิ่งขึ้นโดยกรอบแนวคิด COBIT รุ่นล่าสุด หรือ COBIT 5 ได้ปรับปรุงให้ครอบคลุมการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศภายในองค์กรอย่างครบวงจร ทั้งยังสอดคล้องและสนับสนุนกับกรอบแนวคิดและมาตรฐานอื่นๆ ทางด้านสารสนเทศ รวมทั้งสามารถนำไปปรับใช้ภายในองค์กรได้โดยเทียบเคียงกับกรอบแนวคิด และกระบวนการภายในองค์กร เพื่อให้เห็นถึงจุดอ่อนและสิ่งที่ถูกละเลยจากการดำเนินงานด้านเทคโนโลยีสารสนเทศภายในองค์กร (Oliver & Lainhart, 2012; Tuttle & Vandervelde, 2007) นำไปสู่การตอบสนองกระบวนการทางธุรกิจขององค์กร และการคำนึงถึงประโยชน์จากเทคโนโลยีสารสนเทศภายในองค์กรที่จะส่งมอบให้แก่ผู้มีส่วนได้ส่วนเสียขององค์กรทั้งภายในและภายนอก กรอบแนวคิด COBIT จึงช่วยส่งเสริมให้ผู้ตรวจสอบเทคโนโลยีสารสนเทศ บรรลุวัตถุประสงค์ในการปฏิบัติงานตรวจสอบ อันนำไปสู่ประสิทธิผลของการปฏิบัติงานตรวจสอบเทคโนโลยีสารสนเทศ (Zororo, 2014)

ด้วยเหตุนี้ ผู้วิจัยจึงสนใจที่จะศึกษาปัจจัยที่มีผลต่อคุณค่าที่องค์กรได้รับจากการตรวจสอบภายในด้านเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT เนื่องจากในปัจจุบัน การศึกษาวิจัยถึงการนำกรอบแนวคิด COBIT มาใช้ยังมีอยู่อย่างจำกัด (Zhang, 2013) ดังที่ Haes et al. (2013) ได้กล่าวไว้ว่า กรอบแนวคิด COBIT เป็นแนวคิดแบบกว้าง มีหลายแง่มุมและซับซ้อนต่อการนำไปประยุกต์ใช้ในทางปฏิบัติ อีกทั้งยังสอดคล้องตามที่ Simonsson et al. (2007) ได้ชี้ให้เห็นว่า กรอบแนวคิด COBIT ยังต้องการการศึกษาวิจัยองค์ความรู้เพื่อทำความเข้าใจในการนำมาประยุกต์ใช้เพื่อเป็นเครื่องมือสนับสนุนการสร้างคุณค่าด้วยแนวคิดในการกำกับดูแลและการบริหารจัดการ ตลอดจนการดำเนินงานต่างๆ ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศทั่วทั้งองค์กรให้เป็นไปในแนวทางเดียวกับกลยุทธ์ทางธุรกิจขององค์กร อันเป็นจุดแข็งในการช่วยในเรื่องของการควบคุมภายในและกระบวนการตรวจสอบ (Simonsson et al., 2007 อ้างถึงใน Zhang, 2013) นอกจากนี้ การศึกษาวิจัยก่อนหน้า (Havelka & Merhout, 2013) ที่ผู้วิจัยได้นำมาศึกษาเรื่องแนวคิดปัจจัยที่มีอิทธิพลต่อคุณภาพการตรวจสอบเทคโนโลยีสารสนเทศนั้น ยังไม่ได้มุ่งเน้นปัจจัยที่ทำให้เกิดความแตกต่างระหว่างการตรวจสอบด้านเทคโนโลยีสารสนเทศ และการตรวจสอบทั่วไปเท่าใดนักผู้วิจัยจึงนำกรอบแนวคิด COBIT ที่เป็นกรอบแนวคิดการควบคุมภายในด้านเทคโนโลยีสารสนเทศอย่างครอบคลุมวงจรของการลงทุนด้านเทคโนโลยีสารสนเทศขององค์กรทั้งระบบ ทั้งในมุมมองการกำกับดูแลและมุมมองการบริหารจัดการ นอกจากนี้ประโยชน์สำคัญ

กรอบแนวคิด COBIT ยังช่วยสนับสนุนการสร้างคุณค่าจากสารสนเทศและเทคโนโลยีได้ทั่วทั้งองค์กร ผู้วิจัยจึงสนใจศึกษากรอบแนวคิดคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT

1.2 วัตถุประสงค์ของการวิจัย

เพื่อศึกษาปัจจัยต่างๆ ที่มีผลต่อคุณค่าที่องค์กรจะได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT ผ่านปัจจัยคุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ ประกอบด้วย ความเป็นอิสระอย่างเที่ยงธรรมของผู้ตรวจสอบ การวิเคราะห์ความเสี่ยง ความเข้าใจในความรับผิดชอบและบทบาทของผู้ตรวจสอบ ความรู้ด้านเทคโนโลยีสารสนเทศและกระบวนการทางธุรกิจของผู้ตรวจสอบ วุฒิภาวะการประยุกต์ใช้กระบวนการของกรอบแนวคิด COBIT ในการตรวจสอบ และระดับความสำคัญของกลุ่มกระบวนการตามกรอบแนวคิด COBIT ที่มีต่อองค์กร

2. งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยในอดีตสามารถสรุปปัจจัยที่เกี่ยวข้องกับการศึกษาได้ดังนี้

ความเป็นอิสระอย่างเที่ยงธรรมของผู้ตรวจสอบ (Transparency and independent auditor หรือ IND) หมายถึง สภาวะที่ผู้ตรวจสอบเทคโนโลยีสารสนเทศ สามารถดำเนินกิจกรรมเพื่อทำให้การตรวจสอบเทคโนโลยีสารสนเทศ บรรลุผลโดยปราศจากอคติและความเอนเอียง อันเป็นการเอื้อให้ผู้ตรวจสอบสามารถปฏิบัติงานตามภารกิจด้วยความเชื่อมั่นในงาน และไม่มีการลดหย่อนในคุณภาพของงาน ตามหลักการของกรอบแนวคิด COBIT 5 ที่ได้ระบุความแตกต่างระหว่างการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศ

การวิเคราะห์ความเสี่ยง (Risk analysis หรือ RSK) หมายถึง การพิจารณาผลกระทบของความไม่แน่นอนของเหตุการณ์ หรือปัจจัยที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศระดับองค์กรโดยภาพรวม เช่น ความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่าที่อาจเกิดขึ้นโดยเกี่ยวข้องกับระบบสารสนเทศและเทคโนโลยีต่อวัตถุประสงค์ขององค์กรธุรกิจ (สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย และตลาดหลักทรัพย์แห่งประเทศไทย, 2555)

ความเข้าใจในความรับผิดชอบและบทบาทของผู้ตรวจสอบ (Responsibilities and roles of auditor หรือ ROL) หมายถึง การรู้หน้าที่และขอบเขตการปฏิบัติงานของผู้ตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ (ISACA, 2013) ตามแนวทางสำหรับการให้ความเชื่อมั่นภายใต้กรอบแนวคิด COBIT 5

ความรู้ด้านเทคโนโลยีสารสนเทศและกระบวนการทางธุรกิจของผู้ตรวจสอบ (IT and business process knowledge for auditor หรือ KNW) หมายถึง ความเข้าใจหรือสิ่งที่สั่งสมทางสติปัญญาเฉพาะบุคคลที่ได้มาจากการศึกษา หรือ มาจากประสบการณ์ที่เกี่ยวข้องในด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถเข้าใจและนำมาประยุกต์ใช้ให้เข้ากับลักษณะเฉพาะขององค์กร ตามประเภทและลักษณะของธุรกิจ รวมทั้งวัตถุประสงค์ขององค์กร เช่น ระดับความชำนาญด้านเทคโนโลยีสารสนเทศโดยทั่วไป ความเข้าใจในโปรแกรมประยุกต์สำหรับกระบวนการและการปฏิบัติงาน ความเข้าใจในโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการปฏิบัติงาน เป็นต้น (Havelka & Merhout, 2013)

วุฒิภาวะการประยุกต์ใช้กระบวนการของกรอบแนวคิด COBIT ในการตรวจสอบ (COBIT capability หรือ CCB) หมายถึง เกณฑ์ความสามารถในการนำกระบวนการตามกรอบแนวคิด COBIT (COBIT capability model) มาปรับใช้ในการตรวจสอบเทคโนโลยีสารสนเทศขององค์กรซึ่งปรับมาจากวุฒิภาวะการประยุกต์ใช้กระบวนการของ COBIT ตามกรอบแนวคิด COBIT 5 (ISACA, 2012)

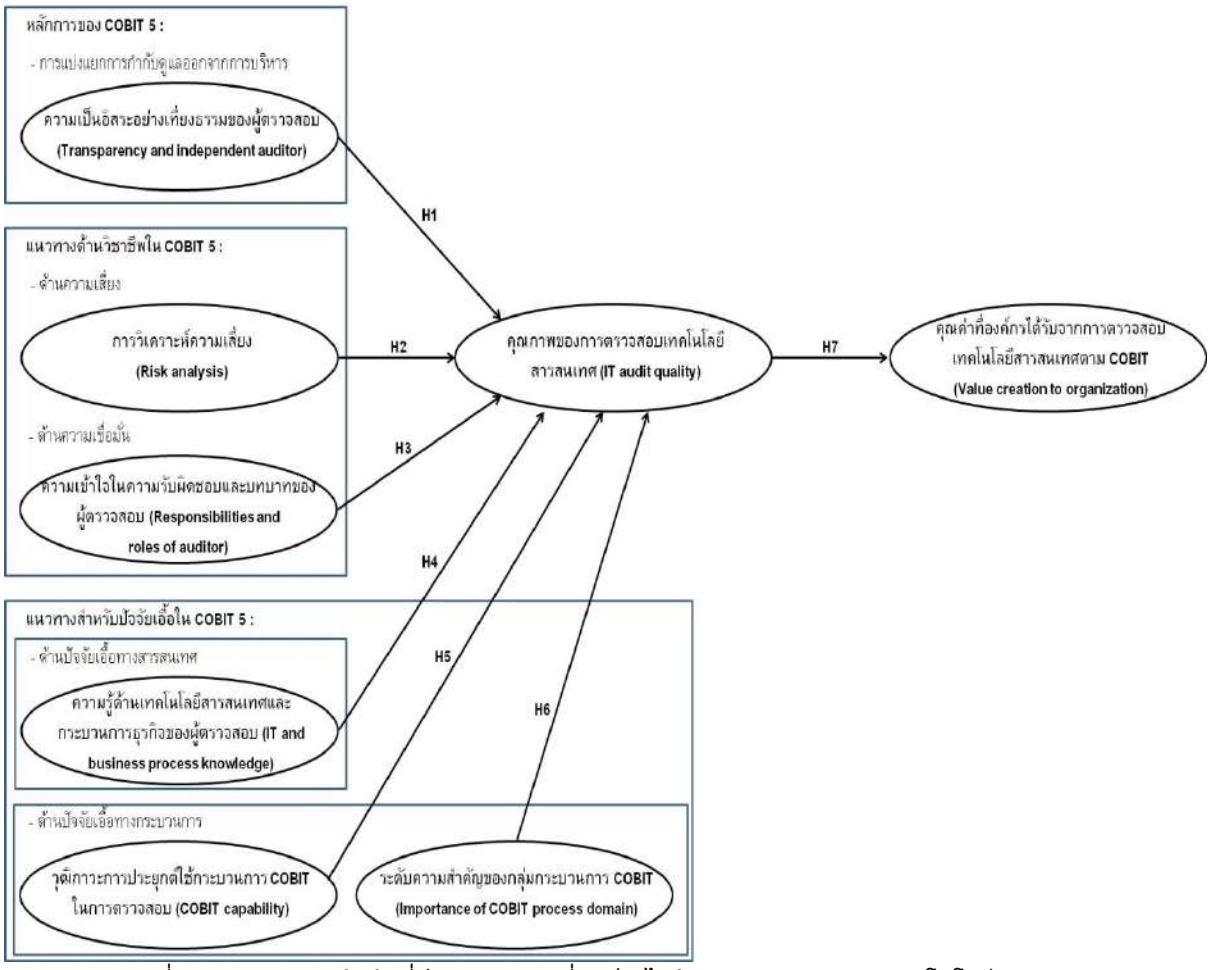
ระดับความสำคัญของกลุ่มกระบวนการตามกรอบแนวคิด COBIT (Importance of COBIT process domain to organization หรือ ICB) หมายถึง การประเมินค่ากลุ่มกระบวนการตามกรอบแนวคิด COBIT เพื่อเลือกปรับใช้กับองค์กรธุรกิจ ตามความสำคัญที่จะทำให้บรรลุวัตถุประสงค์ด้านเทคโนโลยีสารสนเทศขององค์กร (ISACA, 2012)

คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ (IT audit quality หรือ ITAQ) หมายถึง ความมีประสิทธิผลและมีประสิทธิภาพของกิจกรรมการวางแผน และการปฏิบัติงานตรวจสอบเทคโนโลยีสารสนเทศ รวมถึง เครื่องมือ เทคนิค และวิธีการที่นำกรอบแนวคิดมาประยุกต์ใช้ในระหว่างการปฏิบัติงานตรวจสอบเทคโนโลยีสารสนเทศ (Havelka & Merhout, 2013)

คุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศ (Value creation to organization หรือ VALU) หมายถึง ประโยชน์ที่องค์กรธุรกิจจะได้รับจากการประยุกต์ใช้กรอบแนวคิด COBIT เพื่อการตรวจสอบเทคโนโลยีสารสนเทศ (ISACA, 2012)

3. กรอบแนวคิดการวิจัยและสมมติฐานการวิจัย

ผู้วิจัยได้นำปัจจัยต่าง ๆ ที่อยู่ในชุดของแนวทางของกรอบแนวคิด COBIT มาประกอบกับกรอบแนวคิดเรื่องคุณภาพการตรวจสอบเทคโนโลยีสารสนเทศของ Havelka and Merhout (2013) ร่วมกับ ตัวแบบการสร้างคุณค่าแก่องค์กรจากกรอบแนวคิด COBIT 5 เป็นแนวคิดคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศ เพื่อกำหนดเป็นกรอบแนวคิดปัจจัยที่มีผลต่อคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT ดังภาพที่ 1



ภาพที่ 1 กรอบแนวคิดปัจจัยที่มีผลต่อคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT

D'Onza et al. (2015) ระบุว่า ผู้ตรวจสอบเทคโนโลยีสารสนเทศ จะต้องปฏิบัติงานต่อหน่วยงานรับการตรวจด้วยการให้ความเชื่อมั่นอย่างเป็นอิสระ (Chou, 2015) หากผู้ตรวจสอบขาดความเป็นอิสระอย่างเที่ยงธรรม ผู้ตรวจสอบอาจไม่สามารถปฏิบัติงาน หรือไม่สามารถชี้ให้เห็นถึงประเด็นเพื่อลดปัญหาที่เป็นความเสี่ยง (Al-Ajmi, 2009) ผู้ที่มีบทบาทในงานตรวจสอบจึงจำเป็นต้องเป็นอิสระจากกลุ่มผู้รับการตรวจ ทั้งในเรื่องโครงสร้างการบริหารหน่วยงานตรวจสอบและความสามารถในการเข้าถึงข้อมูล ซึ่งจำเป็นต้องใช้ในการตรวจสอบ (Havelka & Merhout, 2013) ตลอดจนขอบเขตของการปฏิบัติงานตรวจสอบ และการสื่อสารผลการปฏิบัติงาน (Vaicekauskas & Mackevič̆ius, 2014) ตามที่ ISACA (2012) ระบุว่า หลักการกำกับดูแลและการบริหารจัดการ ประกอบด้วยประเภทของกิจกรรมที่แตกต่างกันมีหน้าที่รับผิดชอบที่ต่างกัน ฉะนั้นหลักการของกรอบแนวคิด COBIT 5 จึงได้แบ่งแยกกระบวนการการกำกับดูแลและการบริหารจัดการ สอดคล้องตามที่ Kerr and Murthy (2013) กล่าวว่า หน่วยงานตรวจสอบซึ่งมีความเป็นอิสระสามารถใช้กรอบแนวคิด COBIT เพื่อสร้างความเชื่อมั่นในงานตรวจสอบ ซึ่งปรากฏในงานวิจัยที่เกี่ยวข้องกับแนวคิดเรื่องคุณภาพการตรวจสอบเทคโนโลยีสารสนเทศ ทั้งในมุมมองโครงสร้างการดำเนินงาน และในมุมมองการปฏิบัติงาน (Havelka & Merhout, 2013; Stoel et al., 2012) จึงสามารถตั้งสมมติฐานได้ว่า

H1: ความเป็นอิสระอย่างเที่ยงธรรมของผู้ตรวจสอบ ส่งผลทางบวกต่อคุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ

Cangemi (2014) ระบุว่า จากความเปลี่ยนแปลงในแนวคิดของมุมมองการตรวจสอบองค์กร ที่แต่เดิมนั้นการตรวจสอบมุ่งเน้นไปที่การเฝ้าสังเกตและการปฏิบัติตามข้อบังคับ มาสู่มุมมองการตรวจสอบแนวใหม่ ซึ่งมีความเกี่ยวข้องกับการบริหารความเสี่ยงมากขึ้น เพื่อช่วยให้ผู้บริหารเข้าใจถึงแนวทางที่จะป้องกันความเสี่ยงที่อาจกระทบต่อเป้าหมายทางธุรกิจขององค์กรได้ และในมุมมองผู้ตรวจสอบนั้น Elliott et al. (2007) ระบุว่า ขอบเขตการตรวจสอบขึ้นอยู่กับความเสี่ยงขององค์กร และพิจารณากำหนดเป็นแผนการตรวจสอบจากการวิเคราะห์ความเสี่ยงและตรวจสอบสถานะความเสี่ยงที่เป็นอยู่ว่ามีความเสี่ยงใดบ้าง จากนั้นจึงกำหนดเป็นระดับความเสี่ยงที่ชัดเจนในขอบเขตเรื่องที่นำมาพิจารณา รวมถึงโอกาสที่อาจจะเกิดขึ้น ความรุนแรง และมูลค่าความเสียหาย (เมธา สุวรรณสาร, 2558) การพิจารณาประเมินระดับความเสี่ยง นอกจากจะมีผลกระทบต่อการวางแผนการตรวจสอบ (El-Masry & Hansen, 2007) แล้ว ยังส่งผลต่อความมีประสิทธิผลของรายงานประเด็นที่พบจากการตรวจสอบ อันเป็นคุณลักษณะหนึ่งของคุณภาพการตรวจสอบ (Vaicekauskas & Mackevič̆ius, 2014) ทั้งยังช่วยสร้างคุณค่าให้แก่องค์กร (Alhosban, 2014) จึงสามารถตั้งสมมติฐานได้ว่า

H2: การวิเคราะห์ความเสี่ยง ส่งผลทางบวกต่อคุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ

ผู้ตรวจสอบจำเป็นต้องเข้าใจในบทบาทและความรับผิดชอบ เพื่อให้ความเชื่อมั่นในการใช้เทคโนโลยีสารสนเทศภายในองค์กร โดยแนวคิดกระบวนการให้ความเชื่อมั่นปรากฏใน COBIT 5 for assurance โดยเริ่มตั้งแต่การกำหนดเป้าหมายและขอบเขตการปฏิบัติงาน เพื่อให้บรรลุวัตถุประสงค์การตรวจสอบ อีกทั้งยังต้องเข้าใจในปัจจัยต่างๆ ที่เป็นอยู่ภายในองค์กร เพื่อกำหนดหลักเกณฑ์ที่เหมาะสม (Suitable criteria) มาใช้ประเมินสำหรับการปฏิบัติงานตรวจสอบตามที่ Bamber and Lyer (2007) ได้ศึกษาพบว่าความคุ้นเคยต่อผู้รับการตรวจของผู้ตรวจสอบ (The auditors' familiarity with the client) มีผลต่อการพิจารณาประเมินประเด็นที่พบจากผู้รับการตรวจ แม้ว่าในมุมมองหนึ่งอาจเป็นภัยคุกคามต่อความเที่ยงธรรมของผู้ตรวจสอบ แต่ในอีกมุมมองหนึ่งความคุ้นเคยต่อผู้รับการตรวจก็ยังจำเป็นต่อผู้ตรวจสอบ เพื่อที่จะเข้าใจผู้รับการตรวจอย่างเพียงพอที่จะวางแผน และปฏิบัติงานตรวจสอบได้อย่างมีประสิทธิภาพและมีประสิทธิผล นอกจากนี้ผู้ตรวจสอบยังต้องสามารถสื่อสารผลการปฏิบัติงาน และข้อจำกัด รวมทั้ง

ประเด็นที่พบจากการปฏิบัติงานตรวจสอบ ตามที่ El-Masry and Hansen (2007) กล่าวว่า การตรวจสอบที่มีประสิทธิผล ขึ้นอยู่กับการลงความเห็นที่มีน้ำหนักอย่างเพียงพอของผู้ตรวจสอบ โดยทั้งหมดนี้ สอดคล้องกับการศึกษาของ Havelka and Merhout (2013) ที่ได้ระบุว่า บทบาทของผู้ตรวจสอบและหน่วยงานตรวจสอบที่มีต่อองค์กร มีความสำคัญต่อคุณภาพการตรวจสอบเทคโนโลยีสารสนเทศ จึงสามารถตั้งสมมติฐานได้ว่า

H3: ความเข้าใจในความรับผิดชอบและบทบาทของผู้ตรวจสอบ ส่งผลทางบวกต่อคุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ

IAASB (2014) ระบุว่า องค์ประกอบสำคัญประการหนึ่งที่ก่อให้เกิดคุณภาพของการตรวจสอบ เกิดขึ้นจากความรู้ของผู้ตรวจสอบในเรื่องที่เกี่ยวข้องกับการตรวจสอบอย่างเพียงพอต่อการปฏิบัติงาน เพื่อที่จะสามารถตัดสินประเด็นที่พบจากการตรวจสอบได้อย่างสมเหตุสมผล ถึงแม้ว่า กรอบแนวคิด COBIT จะเป็นอิสระจากรูปแบบของเทคโนโลยีที่ใช้ภายในองค์กร (Moreira & Silva, 2013) และไม่ได้ครอบคลุมประเด็นในเชิงเทคนิค เนื่องจากแต่ละองค์กร หรือแต่ละประเภทธุรกิจมีลักษณะจำเพาะ จึงไม่สามารถระบุเป็นแนวทางในเชิงเทคนิค หรือ แนวทางการปฏิบัติงานเฉพาะทาง เช่น แนวทางที่จะจัดสร้างรายการข้อมูล รายการสารสนเทศ ฐานข้อมูล หรือ การปฏิบัติการต่อระบบจัดเก็บข้อมูล ซึ่งสิ่งต่างๆ เหล่านี้ขึ้นอยู่กับนโยบาย มาตรฐานต่างๆ รวมถึงซอฟต์แวร์ที่ใช้เฉพาะแต่ละองค์กร (ISACA, 2013) จึงสามารถตั้งสมมติฐานได้ว่า

H4: ความรู้ด้านเทคโนโลยีสารสนเทศและกระบวนการทางธุรกิจของผู้ตรวจสอบ ส่งผลทางบวกต่อคุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ

Cater-Steel and Lepmets (2014) ระบุว่า วุฒิภาวะของกระบวนการ สามารถเป็นตัวชี้วัดสมรรถนะการบริหารจัดการบริการด้านเทคโนโลยีสารสนเทศภายในองค์กรได้เป็นอย่างดีที่สุด โดยระดับของความสอดคล้องทางธุรกิจและเทคโนโลยีสารสนเทศจะยิ่งมีมากขึ้น เมื่อองค์กรธุรกิจได้ประยุกต์ใช้แนวปฏิบัติในการกำกับดูแลเทคโนโลยีสารสนเทศ (Buchwald et al., 2014) กรอบแนวคิด COBIT เป็นกรอบแนวคิดการกำกับดูแลเทคโนโลยีสารสนเทศที่ได้บ่งชี้ถึงวุฒิภาวการณ์ประยุกต์ใช้กระบวนการ ซึ่งเป็นตัวชี้วัดถึงเกณฑ์การควบคุมเพื่อสนับสนุนให้องค์กรธุรกิจสามารถมั่นใจในการใช้เทคโนโลยีสารสนเทศภายในองค์กรที่สอดคล้องกับเป้าหมายทางธุรกิจ รวมถึงข้อบังคับต่างๆ ที่เกี่ยวข้องกับการบริหารจัดการเทคโนโลยีสารสนเทศ เช่น การบริหารจัดการบริการด้านเทคโนโลยีสารสนเทศ (ได้แก่ ITIL V3 2011 และ ISO/IEC 20000) สถาปัตยกรรมองค์กรที่ผนวกกับโครงสร้างและการจัดการเทคโนโลยีสารสนเทศ (TOGAF) การบริหารจัดการความมั่นคงสารสนเทศ (ได้แก่ ISO/IEC 27001) เป็นต้น กระบวนการด้านเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT แต่ละกระบวนการสามารถนำมาใช้เพื่อวางแผนและควบคุมการตรวจสอบทั่วทั้งองค์กรได้อย่างเป็นอิสระ (Kerr & Murthy, 2013) เพื่อให้องค์กรมั่นใจได้ว่า กระบวนการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่ใช้ภายในองค์กรได้บรรลุเป้าหมายและวัตถุประสงค์ขององค์กร (Chou, 2015) จึงสามารถตั้งสมมติฐานได้ว่า

H5: วุฒิภาวะการประยุกต์ใช้กระบวนการของกรอบแนวคิด COBIT ในการตรวจสอบ ส่งผลทางบวกต่อคุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ

Karkoskova and Feuerlicht (2015) กล่าวว่า องค์กรสามารถนำกระบวนการตามกรอบแนวคิด COBIT มาประยุกต์ใช้เท่าที่จำเป็นเพื่อให้องค์กรประสบความสำเร็จในการประกอบธุรกิจ (Buchwald et al., 2014) และจากการศึกษาของ Abu-Musa (2009) พบว่า ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ ผู้ตรวจสอบภายในและผู้จัดการระดับ

บริหารองค์กรต่างๆ ได้ตระหนัก และให้ความสำคัญต่อกรอบแนวคิด COBIT และการนำมาปรับใช้ในองค์กร โดยเฉพาะอย่างยิ่งในกลุ่มธุรกิจธนาคาร สถาบันการเงิน กลุ่มธุรกิจดูแลสุขภาพ และกลุ่มธุรกิจด้านบริการ และจากการศึกษาของ Fedorowicz and Gelinas (1999) พบว่า องค์กรที่ได้ประยุกต์ใช้กรอบแนวคิด COBIT ในการตรวจสอบด้านเทคโนโลยีสารสนเทศ เชื่อมั่นว่าผลที่ได้จากรายงานตรวจสอบจะเกิดประโยชน์ ทันกาล แม่นยำ และมีความสมบูรณ์มากขึ้น อันจะช่วยให้บรรลุวัตถุประสงค์ทางธุรกิจขององค์กรได้มากกว่าองค์กรที่ไม่ได้ประยุกต์ใช้ (Non-users) จึงสามารถตั้งสมมติฐานได้ว่า

H6: ระดับความสำคัญของกลุ่มกระบวนการตามกรอบแนวคิด COBIT ที่มีต่อองค์กร ส่งผลทางบวกต่อคุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ

เมธา สุวรรณสาร (2558) กล่าวว่า คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศจำเป็นต้องอาศัยกระบวนการ รวมถึงเครื่องมือ เทคนิค และวิธีการปฏิบัติงานตรวจสอบเทคโนโลยีสารสนเทศที่มีคุณภาพ (Havelka & Merhout, 2013) ร่วมกับหลักการบริหารจัดการโครงการ เพื่อนำไปสู่การสร้างคุณค่าในการตรวจสอบเทคโนโลยีสารสนเทศให้แก่องค์กรได้มากขึ้น (Merhout & Havelka, 2008) ตามแนวคิดการตรวจสอบเทคโนโลยีสารสนเทศสมัยใหม่ ที่ไม่เพียงแต่เป็นกิจกรรมที่มุ่งสอบทานประสิทธิภาพและประสิทธิผลของระบบสารสนเทศให้แก่องค์กรเท่านั้น หากแต่ยังต้องมุ่งเน้นการสร้างคุณค่าให้แก่องค์กรอีกด้วย (Vaicekauskas & Mackevičius, 2014) จึงสามารถตั้งสมมติฐานได้ว่า

H7: คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ ส่งผลทางบวกต่อคุณค่าที่องค์กรได้จากการตรวจสอบเทคโนโลยีสารสนเทศ ตามกรอบแนวคิด COBIT

4. วิธีการวิจัย

งานวิจัยนี้จัดเก็บข้อมูลจากกลุ่มตัวอย่างที่มีส่วนเกี่ยวข้องกับการดำเนินงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ ได้แก่ ผู้บริหารงานตรวจสอบภายใน หัวหน้างานตรวจสอบภายใน หรือ หัวหน้างานตรวจสอบเทคโนโลยีสารสนเทศ และผู้ตรวจสอบภายในที่ปฏิบัติงานตรวจสอบเทคโนโลยีสารสนเทศ หรือผู้ตรวจสอบเทคโนโลยีสารสนเทศของบริษัทที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย โดยไม่รวมบริษัทที่อยู่ในระหว่างการฟื้นฟูกิจการและบริษัทที่จดทะเบียนในตลาดหลักทรัพย์เอ็มเอไอ และไม่รวมบริษัทที่ว่าจ้างหรือแต่งตั้งบริษัทภายนอก (Outsource) ให้ดำเนินงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ จำนวน 118 กลุ่มตัวอย่าง โดยใช้แบบสอบถามเป็นเครื่องมือ ซึ่งงานวิจัยนี้พัฒนากรอบแนวคิดคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT จากโมเดลปัจจัยที่ส่งผลต่อคุณภาพการตรวจสอบเทคโนโลยีสารสนเทศ ของ Havelka and Merhout (2013) รวมทั้งกรอบแนวคิด COBIT ที่พัฒนาโดย ISACA และออกเผยแพร่ในปี ค.ศ. 2012

5. ผลการวิจัย

5.1 การทดสอบข้อตกลงเบื้องต้นทางสถิติ

ข้อมูลที่จัดเก็บจากกลุ่มตัวอย่างได้นำมาทดสอบความครบถ้วนของข้อมูล (Valid data) และทดสอบการแจกแจงปกติ (Normality) รวมถึงค่าความเบ้ (Skewness) และค่าความโด่ง (Kurtosis) จากผลการวิเคราะห์ พบว่าตัวแปรสังเกตทุกตัวแปรมีการแจกแจงปกติตามเกณฑ์ที่กำหนด ทางผู้วิจัยจึงใช้ข้อมูลที่จัดเก็บนำมาวิเคราะห์ข้อมูลทางสถิติต่อไป

งานวิจัยนี้ได้ทดสอบความน่าเชื่อถือของแบบสอบถาม โดยการวิเคราะห์ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรสังเกต เพื่อตรวจสอบว่าตัวแปรมีความสัมพันธ์กันในภาพรวมหรือไม่ ด้วยตารางแสดงความสัมพันธ์ (Sample

correlation) พบว่า ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรสังเกตทุกคู่ส่วนใหญ่มีค่าไม่เกิน 0.85 (Kline, 2005) เมื่อพิจารณาความเหมาะสมของข้อมูลที่จะทำการวิเคราะห์องค์ประกอบ โดยพิจารณาจากสถิติทดสอบ 2 ค่า คือ ค่า Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO) และค่า Bartlett Test of Sphericity พบว่าค่า KMO มีค่าเท่ากับ 0.848 ซึ่งมากกว่า 0.50 และค่า Bartlett Test of Sphericity พบว่า มีความสัมพันธ์อย่างมีนัยสำคัญทางสถิติเท่ากับ 0.688 สรุปได้ว่าข้อมูลที่มีอยู่เหมาะสมที่จะใช้เทคนิคการวิเคราะห์องค์ประกอบเชิงยืนยัน

5.2 ลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่าง

ผู้ตอบแบบสอบถามซึ่งเป็นกลุ่มตัวอย่างส่วนมากเป็นกลุ่มอุตสาหกรรมธุรกิจการเงิน ร้อยละ 24.58 ตำแหน่งงานเป็นหัวหน้างานตรวจสอบเทคโนโลยีสารสนเทศ ร้อยละ 44.07 ระดับการศึกษาสูงสุด คือ ปริญญาโท ร้อยละ 77.12 และสาขาวิชาที่จบการศึกษา คือ ด้านเทคโนโลยีสารสนเทศ ร้อยละ 41.11 ดังตารางที่ 1

ตารางที่ 1 จำนวนร้อยละของข้อมูลทั่วไปของกลุ่มตัวอย่าง

ลักษณะส่วนบุคคล		จำนวน	ร้อยละ
กลุ่มอุตสาหกรรม	เกษตรและอุตสาหกรรมอาหาร	15	12.71
	ทรัพยากร	12	10.17
	เทคโนโลยี	11	9.32
	ธุรกิจการเงิน	29	24.57
	บริการ	21	17.80
	สินค้าอุตสาหกรรม	13	11.02
	สินค้าอุปโภคบริโภค	5	4.24
	อสังหาริมทรัพย์และก่อสร้าง	12	10.17
	รวม	118	100.00
ตำแหน่งงาน	ผู้บริหารงานตรวจสอบ	14	11.87
	หัวหน้างานตรวจสอบภายใน	30	25.42
	หัวหน้างานตรวจสอบเทคโนโลยีสารสนเทศ	52	44.07
	ผู้ตรวจสอบภายใน	4	3.39
	ผู้ตรวจสอบเทคโนโลยีสารสนเทศ	8	6.78
	อื่น ๆ	10	8.47
	รวม	118	100.00
ระดับการศึกษาสูงสุด	ต่ำกว่าปริญญาตรี	-	-
	ปริญญาตรี	27	22.88
	ปริญญาโท	91	77.12
	สูงกว่าปริญญาโท	-	-
	รวม	118	100.00

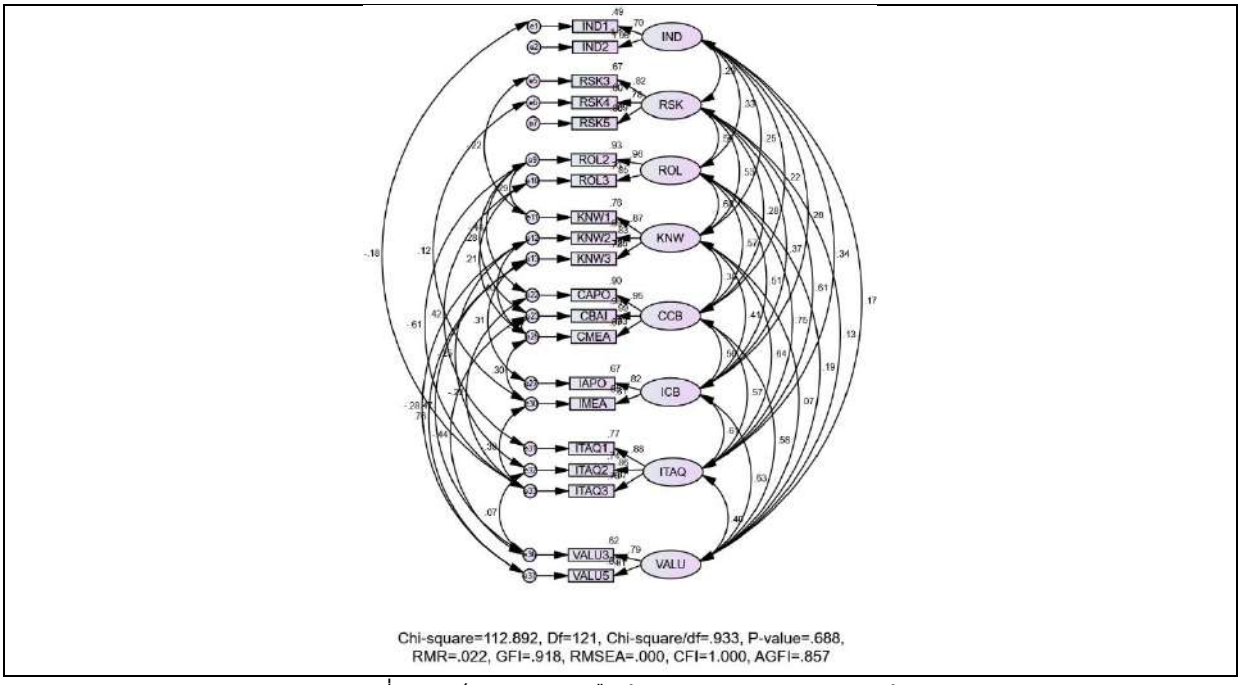
ตารางที่ 1 จำนวนร้อยละของข้อมูลทั่วไปของกลุ่มตัวอย่าง (ต่อ)

ลักษณะส่วนบุคคล		จำนวน	ร้อยละ
สาขาวิชาที่จบการศึกษา[a]	ด้านบัญชี	44	26.99
	ด้านการบริหาร	38	23.31
	ด้านเทคโนโลยีสารสนเทศ	67	41.11
	ด้านอื่น ๆ	14	8.59
	รวม	163	100.00

หมายเหตุ: ผู้ตอบแบบสอบถามสามารถเลือกตอบได้มากกว่า 1 ข้อ เนื่องจากอาจศึกษาจบการศึกษาปริญญาตรี และปริญญาโทต่างสาขาวิชา

5.3 การวิเคราะห์องค์ประกอบเชิงยืนยัน

ในการวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory factor analysis หรือ CFA) ผู้วิจัยเริ่มจากการตรวจสอบการจับกลุ่มของข้อมูลโดยใช้องค์ประกอบการวิเคราะห์เชิงสำรวจ (Exploratory factor analysis หรือ EFA) ผลปรากฏว่ามีตัวแปรสังเกตที่เหลือทั้งสิ้น 20 ตัวแปรที่จะนำมาใช้ในการวิเคราะห์ ต่อจากนั้นใช้เกณฑ์ค่าไคสแควร์สัมพันธ์น้อยกว่า 3 ($X^2/df < 3$) ค่าระดับนัยสำคัญทางสถิติมากกว่า 0.05 ($p > 0.05$) ค่าดัชนีวัดระดับความสอดคล้องกลมกลืนมากกว่า 0.90 (GFI > 0.90) ค่าดัชนีวัดระดับความสอดคล้องกลมกลืนที่ปรับแก้แล้วมากกว่า 0.80 (AGFI> 0.80) ดัชนีความสอดคล้องกลมกลืนเชิงสัมพันธ์มากกว่า 0.90 (CFI > 0.90) ค่าดัชนีรากของค่าเฉลี่ยกำลังสองของการประมาณค่าความคลาดเคลื่อนโดยประมาณน้อยกว่า 0.08 (RMSEA< 0.08) เพื่อพิจารณาว่าตัวแบบการวัด (Measurement model) มีความสอดคล้องกลมกลืน (Fit) (Hair et al., 1998; Tabachnik and Fidell, 2013) ผลการวิเคราะห์องค์ CFA แสดงให้เห็นว่าตัวแปรที่เหลือทั้งหมดมีความเหมาะสมดังแสดงในภาพที่ 2



ภาพที่ 2 องค์ประกอบเชิงยืนยันของกรอบแนวคิดการวิจัย

นอกจากนี้ตัวแปรในตัวแบบการวัดนั้นมีความตรง (Reliability) ซึ่งพิจารณาจากค่าความเชื่อมั่นโดยรวม (Composite reliability หรือ CR) ที่มีค่าตั้งแต่ 0.70 ขึ้นไป และความเที่ยง ประกอบด้วย (1) ความเที่ยงตรงเชิงเหมือน (Convergent validity) พิจารณาจากค่า Factor loading ของตัวแปรสังเกต ที่ต้องมีค่าไม่ต่ำกว่า 0.70 และมีนัยสำคัญทางสถิติที่ระดับ 0.736 และ ค่า Average variance extract (AVE) ที่มีค่าตั้งแต่ 0.50 ขึ้นไปและ (2) ความเที่ยงตรงเชิงแตกต่าง (Discriminate validity) โดยพิจารณาจากค่า MSV (Maximum shared variance) น้อยกว่า AVE และ ASV (Average shared variance) น้อยกว่า AVE แสดงให้เห็นว่าตัวแบบของการวัดในงานวิจัยนี้มีความเที่ยงและความตรงตามเกณฑ์ที่กำหนด ดังตารางที่ 2

ตารางที่ 2 ความตรงและความเที่ยงของการวัด

Constructs	Factor loading	α	CR	AVE	MSV	ASV
ความเป็นอิสระอย่างเที่ยงธรรมของผู้ตรวจสอบ						
องค์กรของท่านแบ่งโครงสร้างคณะกรรมการตรวจสอบออกจากคณะกรรมการบริหาร (IND1)	0.927	0.859	0.893	0.814	0.117	0.063
โครงสร้างการบริหารหน่วยงานตรวจสอบ IT ภายในองค์กรของท่านไม่ได้ขึ้นตรงต่อหน่วยงานใดๆ ซึ่งเป็นผู้รับการตรวจ (IND2)	0.888					
การวิเคราะห์ความเสี่ยง						
ผู้ตรวจสอบ IT องค์กรของท่านสามารถประเมินและระบุความเสี่ยงในเรื่องที่ตรวจสอบได้อย่างชัดเจน (RSK3)	0.850	0.870	0.870	0.691	0.366	0.170
ผู้ตรวจสอบ IT องค์กรของท่าน เฝ้าติดตามจุดบกพร่องของระบบการควบคุมภายใน เพื่อวิเคราะห์ความเสี่ยงในเรื่องที่ตรวจสอบ (RSK4)	0.853					
ผู้ตรวจสอบ IT องค์กรของท่าน สามารถเสนอแนะแนวทาง เพื่อจัดการกับความเสี่ยงสำคัญที่เกี่ยวข้องกับ IT ได้อย่างมีประสิทธิภาพและประสิทธิผล (RSK5)	0.793					

ตารางที่ 2 ความตรงและความเที่ยงของการวัด (ต่อ)

Constructs	Factor loading	α	CR	AVE	MSV	ASV
ความเข้าใจในความรับผิดชอบและบทบาทของผู้ตรวจสอบ						
ผู้ตรวจสอบ IT องค์กรของท่าน สามารถระบุได้ว่าใครเป็นผู้รับผิดชอบในส่วนที่เกี่ยวข้องกับการดำเนินงานภายในองค์กร ตามขอบเขตการตรวจสอบ (ROL2)	0.696	0.901	0.906	0.828	0.555	0.294
ผู้ตรวจสอบ IT องค์กรของท่านเข้าใจถึงสภาพแวดล้อมการควบคุม (Control environment) และปัจจัยต่างๆ ที่เป็นอยู่ภายในองค์กร (ROL3)	0.538					
ความรู้ด้านเทคโนโลยีสารสนเทศและกระบวนการทางธุรกิจของผู้ตรวจสอบ						
ผู้ตรวจสอบ IT องค์กรของท่าน มีความเข้าใจในอุปกรณ์ฮาร์ดแวร์ โครงสร้างระบบเครือข่าย ฐานข้อมูล และเทคโนโลยีพื้นฐานต่างๆ (General IT knowledge) (KNW1)	0.793	0.888	0.887	0.724	0.465	0.217
ผู้ตรวจสอบ IT องค์กรของท่าน มีความเข้าใจเกี่ยวกับซอฟท์แวร์ โปรแกรมประยุกต์ และระบบปฏิบัติการเฉพาะด้านทางคอมพิวเตอร์ที่องค์กรนำมาใช้ เช่น SAP และ Oracle เป็นต้น (KNW2)	0.816					
ผู้ตรวจสอบ IT องค์กรของท่าน มีความเข้าใจในความมั่นคงเครือข่ายและเทคโนโลยีสารสนเทศ (IT security/ cybersecurity) และการคุ้มครองข้อมูลส่วนบุคคล (Data privacy) (KNW3)	0.868					

ตารางที่ 2 ความตรงและความเที่ยงของการวัด (ต่อ)

Constructs	Factor loading	α	CR	AVE	MSV	ASV
วุฒิภาวะการประยุกต์ใช้กระบวนการของกรอบแนวคิด COBIT ในการตรวจสอบ						
องค์กรของท่าน มีการนำกลุ่มกระบวนการ**จัดวางแนวทางจัดทำแผน และจัดระบบ** ที่อยู่ในกรอบแนวคิดCOBIT มาประยุกต์ใช้ เพื่อการตรวจสอบ (CAPO)	0.862	0.968	0.961	0.925	0.341	0.222
องค์กรของท่าน มีการนำกลุ่มกระบวนการ**การจัดสร้าง จัดหา และนำไปใช้** ที่อยู่ในกรอบแนวคิด COBIT มาประยุกต์ใช้ เพื่อการตรวจสอบ (CBAI)	0.881	0.968	0.961	0.925	0.341	0.222
องค์กรของท่าน มีการนำกลุ่มกระบวนการ **การเฝ้าติดตาม วัดผล และประเมิน** ที่อยู่ในกรอบแนวคิด COBIT มาประยุกต์ใช้ เพื่อการตรวจสอบ (CMEA)	0.873					
ระดับความสำคัญของกลุ่มกระบวนการตามกรอบแนวคิด COBIT ที่มีต่อองค์กร						
องค์กรของท่าน ให้ความสำคัญต่อการจัดวางแนวทาง แผนงาน และการจัดระบบ IT ขององค์กร (IAPO)	0.704	0.802	0.795	0.660	0.391	0.245
องค์กรของท่าน ให้ความสำคัญต่อผลลัพธ์ของระบบ IT กับ ความสอดคล้องของการดำเนินงานระบบการควบคุมภายใน และข้อกำหนดจากภายนอก (IMEA)	0.725					

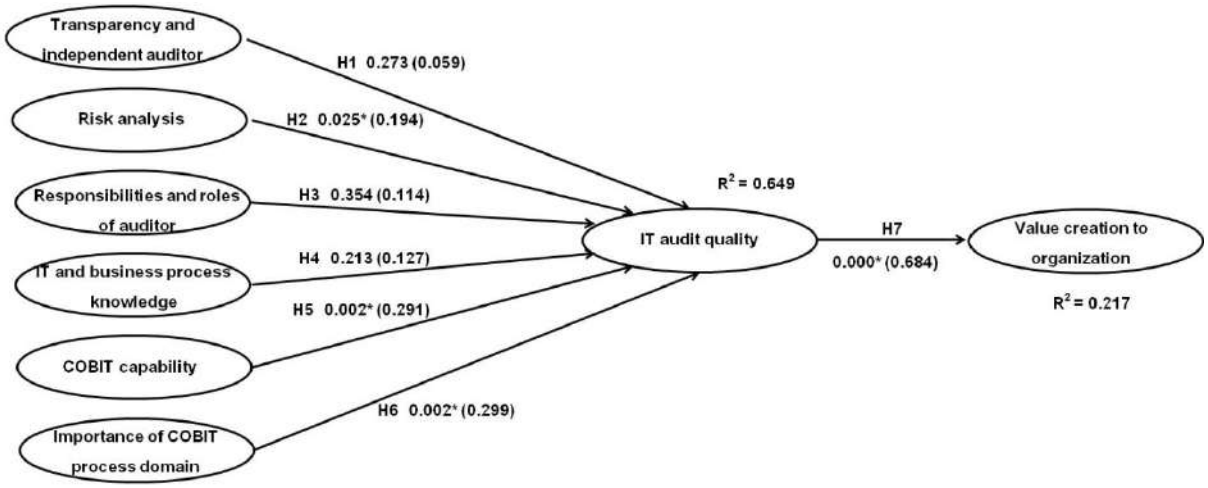
ตารางที่ 2 ความตรงและความเที่ยงของการวัด (ต่อ)

Constructs	Factor Loading	α	CR	AVE	MSV	ASV
คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ						
ผู้ตรวจสอบ IT องค์กรของท่าน มีความเข้าใจต่อสภาพแวดล้อมของผู้รับการตรวจที่เป็นอยู่อย่างเพียงพอที่จะวางแผน และปฏิบัติงานตรวจสอบ (ITAQ1)	0.810	0.906	0.904	0.758	0.555	0.328
ผู้ตรวจสอบ IT องค์กรของท่าน มีความสามารถในการวางแผน และปฏิบัติงานตามมาตรฐานหรือเกณฑ์ที่ใช้ประเมินในการตรวจสอบ (ITAQ 2)	0.754					
ผู้ตรวจสอบ IT องค์กรของท่าน สามารถเก็บรวบรวมหลักฐานที่เกี่ยวข้องกับการตรวจสอบอย่างเพียงพอที่จะประเมิน และพิจารณาการตรวจสอบ (ITAQ 3)	0.808					
คุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศ ตามกรอบแนวคิด COBIT						
การลงทุนด้าน IT ภายในองค์กรของท่าน เกิดประโยชน์จริง (VALU3)	0.748	0.826	0.841	0.727	0.391	0.140
การส่งมอบบริการด้าน IT ภายในองค์กรของท่าน เป็นไปตามความต้องการทางธุรกิจ (VALU5)	0.839					

หมายเหตุ: **α** = ค่าประสิทธิ์แอลฟาของครอนบาซ (Cronbach's alpha) ที่มีค่ามากกว่า 0.70 ซึ่งถือว่ามีความเชื่อถือได้สำหรับงานวิจัยแบบ Basic research (สุพิชญา อาชวจิรดา, 2557)

5.4 การวิเคราะห์สมการเชิงโครงสร้าง

จากการวิเคราะห์สมการเชิงโครงสร้าง (Structural equation model) ด้วยโปรแกรมสำเร็จรูปทางสถิติ และโปรแกรมวิเคราะห์สมการเชิงโครงสร้าง เพื่อตรวจสอบความสอดคล้องกลมกลืนของโมเดลแต่ละองค์ประกอบในโมเดลสมการโครงสร้าง โดยผลการวิเคราะห์สมการโครงสร้างแสดงให้เห็นว่า กรอบแนวคิดปัจจัยที่มีผลต่อคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ตามเงื่อนไขในระดับการยอมรับทางสถิติ โดยมีค่า ไคสแคว์ (X^2) = 148.000 ค่าระดับความอิสระ (df) = 125 ค่าระดับนัยสำคัญทางสถิติ (p-value) = 0.078 ค่าความคาดเคลื่อนมาตรฐาน (RMSEA) = 0.040 ค่า GFI = 0.898 และค่า AGFI = 0.828 ซึ่งถือเป็นค่ามาตรฐาน และแสดงว่ารูปแบบการวัดองค์ประกอบเชิงยืนยันของตัวแปรที่เกี่ยวข้องกับกรอบแนวคิด COBIT เพื่อคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศ มีความกลมกลืนกับข้อมูลเชิงประจักษ์ ดังภาพที่ 3



หมายเหตุ * p < 0.05

ภาพที่ 3 ผลการวิเคราะห์กรอบแนวคิดปัจจัยที่มีผลต่อคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT หลังจากวิเคราะห์ปัจจัย

ตารางที่ 3 ค่าสัมประสิทธิ์อิทธิพลทางตรงและทางอ้อมของตัวแปร ปัจจัยที่มีผลต่อคุณค่าจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT

Dependent variables	**R^2**	**Relation**	**Independent variables**						
			IND	**RSK**	**ROL**	**KNW**	**CCB**	**ICB**	**ITAQ**
IT audit quality	0.649	Direct effect	0.064	0.238*	0.125	0.149	0.106*	0.254*	_
		Indirect effect	_	_	_	_	_	_	_
		Total effect	0.064	0.238*	0.125	0.149	0.106*	0.254*	_
Value creation to organization	0.217	Direct effect	_	_	_	_	_	_	0.824*
		Indirect effect	0.052	0.196	0.103	0.123	0.088	0.209	_
		Total effect	0.052	0.196	0.103	0.123	0.088	0.209	0.824*

* p < 0.05

จากผลทางสถิติของปัจจัยการวิเคราะห์ความเสี่ยง วุฒิภาวะการประยุกต์ใช้กระบวนการของ COBIT ในการตรวจสอบ และระดับความสำคัญของกลุ่มกระบวนการตามกรอบแนวคิด COBIT ที่มีต่อองค์กร ส่งอิทธิพลต่อคุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ ที่ระดับนัยสำคัญที่ 0.05 โดยมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 64.9 (R^2 = 0.649) และคุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ ส่งอิทธิพลต่อคุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ โดยมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 21.7 (R^2 = 0.217) อีกทั้งผลทางสถิติตามตารางที่ 3 แสดงค่าอิทธิพลทางตรงและทางอ้อมซึ่งสนับสนุนสมมติฐานที่ 2, 5, 6 และ 7 และไม่สนับสนุนสมมติฐาน

การวิจัยที่ 1 ซึ่งอาจมีสาเหตุจากความเป็นอิสระอย่างเที่ยงธรรมของผู้ตรวจสอบ นอกจากจะขึ้นอยู่กับผู้ตรวจสอบแล้ว อาจปรับเปลี่ยนไปตามจำนวนบุคลากรหรือขนาดขององค์กร โดยรูปแบบและเนื้อหาของนโยบายและขั้นตอนการปฏิบัติงาน จะขึ้นอยู่กับขนาดและโครงสร้างของกิจกรรมและความซับซ้อนของงาน (IIA, 2013) และไม่สนับสนุนสมมติฐานการวิจัยที่ 3 ซึ่งอาจมีสาเหตุจากการกำหนดเป้าหมายและขอบเขตการปฏิบัติงานเพื่อให้บรรลุวัตถุประสงค์การตรวจสอบ รวมถึงความเข้าใจในปัจจัยต่าง ๆ ที่เป็นอยู่ภายในองค์กร (Bamber & Iyer, 2007) เพื่อกำหนดหลักเกณฑ์ที่เหมาะสม (Suitable criteria) สำหรับกลุ่มธุรกิจที่หลากหลายแตกต่างกันของกลุ่มตัวอย่าง นอกจากนี้ยังไม่สนับสนุนสมมติฐานการวิจัยที่ 4 ซึ่งอาจมาจากการที่แม้ว่าผู้ตรวจสอบจะมีความรู้เฉพาะทางซึ่งเกี่ยวข้องกับธุรกิจขององค์กร แต่ความรู้เฉพาะทางที่ผู้ตรวจสอบมีอยู่ ก็ไม่อาจทำให้เกิดคุณภาพของการตรวจสอบได้เสมอไป ผู้ตรวจสอบอาจจำเป็นต้องใช้ความรู้เฉพาะทางที่มีร่วมกับการสั่งสมประสบการณ์ (Audit time) และวิจารณญาณในการสังเกตและสงสัยเยี่ยงผู้ประกอบวิชาชีพของผู้ตรวจสอบ (Professional skepticism) อีกด้วย (Hu, 2015) สรุปผลการวิจัยแสดงในตารางที่ 4

ตารางที่ 4 สรุปผลการวิจัย

สมมติฐาน	สมมติฐานงานวิจัย	ผลการทดสอบ
H1	ความเป็นอิสระอย่างเที่ยงธรรมของผู้ตรวจสอบ ส่งผลทางบวกต่อ คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ	ไม่สนับสนุน
H2	การวิเคราะห์ความเสี่ยง ส่งผลทางบวกต่อ คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ	สนับสนุน
H3	ความเข้าใจในความรับผิดชอบและบทบาทของผู้ตรวจสอบ ส่งผลทางบวกต่อ คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ	ไม่สนับสนุน
H4	ความรู้ด้านเทคโนโลยีสารสนเทศและกระบวนการทางธุรกิจของผู้ตรวจสอบ ส่งผลทางบวกต่อ คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ	ไม่สนับสนุน
H5	วุฒิภาวะการประยุกต์ใช้กระบวนการของกรอบแนวคิด COBIT ในการตรวจสอบ ส่งผลทางบวกต่อ คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ	สนับสนุน
H6	ระดับความสำคัญของกลุ่มกระบวนการตามกรอบแนวคิด COBIT ที่มีต่อองค์กร ส่งผลทางบวกต่อ คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ	สนับสนุน
H7	คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ ส่งผลทางบวกต่อ คุณค่าที่องค์กรได้จากการตรวจสอบเทคโนโลยีสารสนเทศ ตามกรอบแนวคิด COBIT	สนับสนุน

6. สรุปผลการวิจัย

6.1 อภิปรายผลการวิจัย

จากผลการวิเคราะห์ทางสถิติพบว่ากลุ่มตัวอย่างที่ตอบแบบสอบถามส่วนมาก ปฏิบัติงานในธุรกิจการเงิน (ร้อยละ 24.58) เป็นหัวหน้างานตรวจสอบเทคโนโลยีสารสนเทศ (ร้อยละ 44.07) ระดับการศึกษาปริญญาโท (ร้อยละ 77.12) สาขาวิชาที่จบการศึกษาด้านเทคโนโลยีสารสนเทศ (ร้อยละ 41.11) มีประสบการณ์การทำงานตรวจสอบภายใน เฉลี่ย 9.76 ปี และ มีประสบการณ์การทำงานตรวจสอบเทคโนโลยีสารสนเทศ เฉลี่ย 7.34 ปี ซึ่งไม่มีประกาศนียบัตรทางด้านวิชาชีพ (ร้อยละ 51.94) และ มีความเข้าใจ หรือมีประสบการณ์ต่อกรอบแนวคิด COBIT ในระดับปานกลาง (ร้อยละ 61.90) และผลการวิจัยพบว่า คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ มีอิทธิพลต่อ คุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT โดยมีองค์ประกอบที่สำคัญ โดยเรียงตามลำดับค่าสัมประสิทธิ์อิทธิพลที่มากที่สุด ดังนี้ (1) ระดับความสำคัญของกลุ่มกระบวนการตามกรอบแนวคิด COBIT ที่มีต่อ

องค์กร (2) การวิเคราะห์ความเสี่ยง (3) วุฒิภาวะการประยุกต์ใช้กระบวนการของกรอบแนวคิด COBIT ในการตรวจสอบ ตามลำดับ

งานวิจัยนี้พัฒนากรอบแนวคิดปัจจัยที่มีผลต่อคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT จากโมเดลปัจจัยที่ส่งผลต่อคุณภาพการตรวจสอบเทคโนโลยีสารสนเทศ ตามกรอบแนวคิด ของ Havelka and Merhout (2013) และกรอบแนวคิด COBIT ที่พัฒนาโดย ISACA และออกเผยแพร่ในปี ค.ศ. 2012 โดยมีปัจจัยเพิ่มจากการศึกษาในอดีตที่ผ่านมา ได้แก่ วุฒิภาวะการประยุกต์ใช้กระบวนการของกรอบแนวคิด COBIT ในการตรวจสอบ และระดับความสำคัญของกลุ่มกระบวนการตามกรอบแนวคิด COBIT ที่มีต่อองค์กรรวมถึง ปัจจัยคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศ และจากการศึกษาวิจัยพบว่า นอกจากการวิเคราะห์ความเสี่ยงซึ่งส่งผลต่อคุณภาพการตรวจสอบเทคโนโลยีสารสนเทศแล้ว การตรวจสอบเทคโนโลยีสารสนเทศยังจำเป็นต้องพิจารณาถึง ระดับความสำคัญของกลุ่มกระบวนการตามกรอบแนวคิด COBIT ที่มีต่อองค์กร โดยที่องค์กรธุรกิจสามารถจัดให้มีกระบวนการต่าง ๆ ตามกรอบแนวคิด COBIT 5 ที่องค์กรเห็นว่าเหมาะสมตราบเท่าที่ยังครอบคลุมถึงวัตถุประสงค์ที่จำเป็นสำหรับการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศภายในองค์กร (ISACA, 2012; Karkoskova & Feuerlicht, 2015) และนำไปสู่คุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ เพื่อคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศ จากผลการวิจัย พบว่า ผู้ที่มีส่วนเกี่ยวข้องกับการดำเนินงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ ได้แก่ ผู้บริหารงานตรวจสอบภายใน หัวหน้างานตรวจสอบภายใน หรือหัวหน้างานตรวจสอบเทคโนโลยีสารสนเทศ และผู้ตรวจสอบภายในที่ปฏิบัติงานตรวจสอบเทคโนโลยีสารสนเทศ หรือผู้ตรวจสอบเทคโนโลยีสารสนเทศ ระบุว่า ผู้ที่มีส่วนเกี่ยวข้องกับการดำเนินงานตรวจสอบเทคโนโลยีสารสนเทศ ควรพิจารณาถึงการวิเคราะห์ความเสี่ยงในการตรวจสอบเทคโนโลยีสารสนเทศ โดยประเมินและระบุความเสี่ยงในเรื่องที่ตรวจสอบ และเฝ้าติดตามจุดบกพร่องของระบบการควบคุมภายในเพื่อวิเคราะห์ความเสี่ยงในเรื่องที่ตรวจสอบ รวมถึงเสนอแนะแนวทางสำหรับจัดการกับความเสี่ยงที่สำคัญซึ่งเกี่ยวข้องกับสารสนเทศและเทคโนโลยีได้อย่างมีประสิทธิภาพและประสิทธิผล เพื่อที่จะนำมาประเมินระดับความสำคัญของกลุ่มกระบวนการตามกรอบแนวคิด COBIT ที่มีต่อองค์กร โดยเฉพาะอย่างยิ่งในกลุ่มกระบวนการจัดวางแนวทางแผนงาน และการจัดระบบเทคโนโลยีสารสนเทศภายในองค์กร (Align, Plan and Organize หรือ APO) และกลุ่มกระบวนการเฝ้าติดตาม วัดผล และประเมิน (Monitor, Evaluate and Assess หรือ MEA) ซึ่งจะใช้กำหนดเป็นวุฒิภาวะการประยุกต์ใช้กระบวนการของกรอบแนวคิด COBIT สำหรับการตรวจสอบเทคโนโลยีสารสนเทศ (COBIT capability) ที่เหมาะสมต่อองค์กร อันเป็นเครื่องมือสนับสนุนการปฏิบัติงานตรวจสอบ เพื่อให้เกิดคุณภาพการตรวจสอบเทคโนโลยีสารสนเทศ และส่งผลต่อคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศ

6.2 ข้อเสนอแนะในเชิงปฏิบัติ

หัวหน้างานหรือผู้จัดการส่วนงานตรวจสอบเทคโนโลยีสารสนเทศสามารถนำผลการวิจัยไปบริหารจัดการ หรือควบคุมกระบวนการตรวจสอบเทคโนโลยีสารสนเทศ ดังนี้

(1) หัวหน้างานหรือผู้จัดการส่วนงานตรวจสอบเทคโนโลยีสารสนเทศควรคำนึงถึงปัจจัยที่มีอิทธิพลต่อคุณค่าที่องค์กรจะได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT ให้ดียิ่งขึ้น

(2) คณะกรรมการตรวจสอบหรือหน่วยงานที่มีส่วนเกี่ยวข้องกับความเสี่ยงด้านเทคโนโลยีสารสนเทศภายในองค์กร ควรสนับสนุนส่วนงานตรวจสอบเทคโนโลยีสารสนเทศในกระบวนการวิเคราะห์และประเมินความเสี่ยงที่สำคัญตามแนวทางการตรวจสอบเทคโนโลยีสารสนเทศเพื่อให้เกิดคุณค่าที่องค์กรจะได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศตามกรอบแนวคิด COBIT

6.3 ข้อเสนอแนะสำหรับงานวิจัยต่อเนื่อง

จากการวิเคราะห์ข้อมูลความเข้าใจหรือประสบการณ์ต่อกรอบแนวคิด COBIT ของกลุ่มตัวอย่าง เป็นการประเมินโดยมุมมองของผู้ที่เกี่ยวข้องกับการตรวจสอบเทคโนโลยีสารสนเทศ ซึ่งผู้วิจัยมิได้กำหนดแบบทดสอบความเข้าใจและ

ประสบการณ์ต่อกรอบแนวคิด COBIT ของผู้ตอบแบบสอบถาม เนื่องจากผู้วิจัยต้องการให้แบบสอบถามมีความกระชับ เพื่อให้เกิดความร่วมมือในการตอบแบบสอบถามของกลุ่มตัวอย่างที่มากขึ้น อีกทั้งผลการวิจัย พบว่า ความเป็นอิสระอย่างเที่ยงธรรมของผู้ตรวจสอบ และความเข้าใจในความรับผิดชอบและบทบาทของผู้ตรวจสอบ ไม่ส่งอิทธิพลต่อคุณภาพการตรวจสอบเทคโนโลยีสารสนเทศ อาจมีสาเหตุจากการกำหนดเป้าหมายและขอบเขตการปฏิบัติงานเพื่อให้บรรลุวัตถุประสงค์การตรวจสอบของกลุ่มอุตสาหกรรมขององค์กรที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย มีความแตกต่างหลากหลาย โดยปัจจัยความเป็นอิสระของผู้ตรวจสอบอาจปรับเปลี่ยนไปตามจำนวนบุคลากรหรือขนาดขององค์กร รวมทั้งรูปแบบและเนื้อหาของนโยบายและขั้นตอนการปฏิบัติงาน ซึ่งจะขึ้นอยู่กับขนาดและโครงสร้างของกิจกรรมและความซับซ้อนของงาน (IIA, 2013)

นอกจากนี้ กรอบแนวคิด COBIT จะเป็นกรอบแนวคิดที่เป็นอิสระจากรูปแบบของเทคโนโลยีที่ใช้ภายในองค์กร (Moreira & Silva, 2013) ผู้วิจัยจึงพัฒนาปัจจัยความรู้ด้านเทคโนโลยีสารสนเทศและกระบวนการทางธุรกิจของผู้ตรวจสอบจากผลการสำรวจโดยสำนักงานสอบบัญชีขนาดใหญ่ ในประเด็นเกี่ยวกับทักษะที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่จำเป็นต่องานตรวจสอบภายใน ซึ่งกลุ่มอุตสาหกรรมธุรกิจการเงินที่เป็นกลุ่มตัวอย่างส่วนใหญ่ อาจมีความต้องการผู้ตรวจสอบเทคโนโลยีสารสนเทศที่มีความรู้ความเชี่ยวชาญเฉพาะทางมากกว่ากลุ่มอุตสาหกรรมอื่นๆ เช่น การใช้โปรแกรมประยุกต์ที่เป็นเครื่องมือสนับสนุนงานตรวจสอบโดยเฉพาะ

จากผลการวิจัย พบว่า R square ที่บ่งบอกนัยแห่งความสัมพันธ์ของคุณค่าที่องค์กรได้รับจากการตรวจสอบเทคโนโลยีสารสนเทศยังไม่สูงมากนัก อาจเป็นเพราะกลุ่มตัวอย่างที่เป็นองค์กรที่มีการตรวจสอบเทคโนโลยีสารสนเทศซึ่งจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย ยังมีจำนวนไม่มากนัก อีกทั้งผลการวิเคราะห์สถิติแสดงให้เห็นว่าความรู้ด้านเทคโนโลยีสารสนเทศและกระบวนการทางธุรกิจของผู้ตรวจสอบ ไม่มีผลกระทบอย่างมีนัยสำคัญกับคุณภาพของการตรวจสอบเทคโนโลยีสารสนเทศ ดังนั้นควรนำประเด็นในเรื่องการสั่งสมประสบการณ์ (Audit time) และวิจารณญาณในการสังเกตและสงสัยเยี่ยงผู้ประกอบวิชาชีพของผู้ตรวจสอบ (Professional skepticism) มาพิจารณาร่วมกับปัจจัยความรู้ด้านเทคโนโลยีสารสนเทศและกระบวนการทางธุรกิจของผู้ตรวจสอบเพื่อให้เกิดคุณภาพการตรวจสอบเทคโนโลยีสารสนเทศในงานวิจัยต่อไป

บรรณานุกรม

ครรชิต มาลัยวงศ์. (2553). *การตรวจสอบไอที (IT Audit) ใน สำนักงาน ก.พ.ร. การประชุมสัมมนาเชิงปฏิบัติการเกี่ยวกับ การควบคุมภายในและการบริหารความเสี่ยงระดับจังหวัด ครั้งที่ 1 ระหว่างวันที่ 16 – 27 เมษายน 2553, จ. สุรินทร์.* ดึงข้อมูลวันที่ 16 กรกฎาคม 2560, จาก http://www.opdc.go.th/uploads/files/audit/ IT_Audit.ppt.

เมธา สุวรรณสาร. (2558). *การบริหารความเสี่ยงด้านไอซีที (ICT Risk Management) ใน หลักสูตรผู้บริหารเทคโนโลยีสารสนเทศระดับสูง รุ่นที่ 26.* ดึงข้อมูลวันที่ 16 กรกฎาคม 2560, จาก http://old.ega.or.th/Files/20150331014615.pdf.

สุพิชญา อาชวจิรดา. (2557). *ปัจจัยที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร.* การค้นคว้าอิสระที่ยังไม่ได้ตีพิมพ์, คณะพาณิชยศาสตร์และการบัญชี, มหาวิทยาลัยธรรมศาสตร์.

สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย และ ตลาดหลักทรัพย์แห่งประเทศไทย. (2555). *ความเสี่ยงและการควบคุมด้านเทคโนโลยีสารสนเทศ.* กรุงเทพ: ตลาดหลักทรัพย์แห่งประเทศไทย.

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2545). *แนวทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศ.* กรุงเทพ: สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์.

Abu-Musa, A. (2009). Exploring the importance and implementation of COBIT processes in Saudi organizations. *Information Management & Computer Security*, 17(2), 73 – 95.

Alhosban, A. (2014). Role for internal auditor to cope with IT risks and IT infrastructure in Jordan Commercial Banks. *Global Journal of Management & Business Research*, 14 (11A), 13-21.

Al-Ajmi, J. (2009). Audit firm, corporate governance, and audit quality: Evidence from Bahrain. *Advances in Accounting, incorporating Advances in International Accounting*, 25, 64–74.

Bamber, E., & Iyer, V. (2007). Auditors' identification with their clients: Effects on audit quality. *Auditing: a journal of practice & theory*, 26(2), 1-24.

Buchwald, A., Urbach, N., & Ahlemann, F. (2014). Business value through controlled IT: toward an integrated model of IT governance success and its impact. *Journal of Information Technology*, 29(2), 128-147.

Cangemi, M. (2014). Performing a strategic risk-based assessment: integrating data analytics into the audit universe. *EDPACS: the EDP Audit, Control & Security Newsletter*, 49(5), 1-6.

Cater-Steel, A., & Lepmets, M. (2014). Measuring IT service quality: evaluation of IT service quality measurement framework in industry. *Journal of Service Science Research*, 6(1), 125-147.

Chou, D. (2015). Cloud computing risk and audit issues. *Computer Standards and Interfaces*, 42, 137–142.

D'Onza, G., Lamboglia, R., & Verona, R. (2015). Do IT audits satisfy senior manager expectations?. *Managerial Auditing Journal*, 30(4), 413 – 434.

El-Masry, E., & Hansen, K. (2007). Factors affecting auditors' utilization of evidential cues. *Managerial Auditing Journal*, 23(1), 26-50.

Elliott, M., Dawson, R., & Edwards, J. (2007). An improved process model for internal auditing. *Managerial Auditing Journal*, 22(6), 552-565.

Fedorowicz, J., & Gelinas, U. (1999). Adoption and Usage Patterns of an IT Audit and Control Framework. *Proceedings of the Americas Conference on Information Systems association for information systems: Association for Information Systems*, 729-731.

Haes, S., Grembergen, W., & Debreceny, R. (2013). COBIT 5 and Enterprise Governance of information technology: building blocks and research opportunities. *Journal of Information Systems*, 27(1), 307-324.

Havelka, D., & Merhout, J. (2013). Internal Information Technology Audit Process Quality: Theory development using structured group processes. *International Journal of Accounting Information Systems*, 14, 165–192.

Hair, J. F., Anderson, R. E., Tatham, R.L., & Black, W. C. (1998). *Multivariate Data Analysis, 5th ed*. Englewood Cliffs, NJ: Prentice-Hall.

Hu, D. (2015). Audit quality and measurement: towards a comprehensive understanding. *Academy of Accounting and Financial Studies Journal*, 19(1), 209-222.

IAASB. (2014). *Audit quality: an IAASB perspective*. New York: International Federation of Accountants.

IIA. (2013). *International Professional Practices Framework (IPPF)*, 2013 Edition. Altamonte Springs, FL: IIA Research Foundation.

ISACA. (2012). *COBIT 5: a business framework for the governance and management of enterprise IT.* Rolling Meadows, IL: ISACA.

ISACA. (2012). *COBIT 5: enabling processes.* Rolling Meadows, IL: ISACA.

ISACA. (2013). *COBIT 5: for risk.* Rolling Meadows, IL: ISACA.

ISACA. (2013). *COBIT Process Assessment Model (PAM): Using COBIT 5.* Rolling Meadows, IL: ISACA.

Karkoskova, S., & Feuerlicht, G. (2015). Extending MBI Model using ITIL and COBIT Processes. *Journal of Systems Integration*, 6(4), 29-44.

Kerr, D., & Murthy, U. (2013). The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations: An international survey. *Information and Management*, 50, 590-597.

Merhout, J., & Havelka, D. (2008). Information Technology Auditing: A Value Added IT Governance Partnership between IT Management and Audit. *Communications of the Association for information systems*, 23, 463-482.

Moreira, J., & Silva, P. (2013). IT Management model for financial report issuance and regulatory and legal compliance. *Journal of Information Systems and Technology Management*, 10(3), 597-620.

Oliver, D., & Lainhart, J. (2012). COBIT 5: Adding Value through Effective GEIT. *EDPACS: The EDP Audit, Control, and Security Newsletter*, 46(3), 1-12.

Simonsson, M., Johnson, P., & Wijkström, H. (2007). Model Based IT Governance Maturity Assessments With COBIT. *Proceedings of the 15th European Conference on Information Systems*, Switzerland, 77.

Stoel, D., Havelka, D., & Merhout, J. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. *International Journal of Accounting Information Systems*, 13, 60-79.

Tabachnick, B., & Fidell, L. S. (2013). *Using Multivariate Statistics (Sixth Edition)*. Boston: Pearson Education, Inc.

Tuttle, B., & Vandervelde, S. (2007). An empirical examination of CobiT as an internal controlframework for information technology. *International Journal of Accounting Information Systems*, 8, 240-263.

Vaicekauskas, D., & MackeviČius, J. (2014). Developing a framework for audit quality management in audit firms. *Zeszyty Teoretyczne Rachunkowosci*, 75(131), 171-193.

Zororo, T. (2014). IT Governance Assurance and Consulting: a compelling need for today's IT Auditors. *EDPACS: The EDP Audit, Control, and Security Newsletter*, 49(6), 1-9.

Zhang, S. (2013). *An Exploratory Examination of the Practicability of COBIT framework*. Unpublished Master of ICT in Business Thesis, Leiden Institute of Advanced Computer Science, Leiden University, Leiden.

ปัจจัยที่ส่งผลกระทบต่อประสิทธิภาพของงานตรวจสอบภายใน: มุมมองของผู้ตรวจสอบภายใน

อรพรรณ แสงศิวะเวทย์*

บริษัท บุญรอดบริวเวอรี่ จำกัด

***Correspondence:** oraphan.sangsivavait@gmail.com doi: 10.14456/jisb.2018.14

วันที่รับบทความ: 30 พ.ค. 2560 วันแก้ไขบทความ: 29 มิ.ย. 2560 วันตอบรับบทความ: 12 ก.ค. 2560

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ส่งผลกระทบต่อประสิทธิภาพของงานตรวจสอบภายใน ซึ่งเป็นงานวิจัยเชิงปริมาณ โดยทำการศึกษากลุ่มประชากรในกลุ่มผู้ประกอบอาชีพผู้ตรวจสอบภายในที่มีประสบการณ์ตั้งแต่ 3 เดือนขึ้นไป จำนวน 200 กลุ่มตัวอย่าง ด้วยวิธีการแจกแบบสอบถามรูปแบบออนไลน์ ผลการวิจัยแสดงให้เห็นว่า การสนับสนุนจากผู้บริหารและการติดตามและประเมินผลนั้นส่งผลต่อประสิทธิภาพของงานตรวจสอบภายใน ซึ่งการสนับสนุนจากผู้บริหารขึ้นอยู่กับการรับรู้ถึงความสำคัญของหน่วยงานตรวจสอบภายในผ่านคุณภาพของงานตรวจสอบภายใน รวมทั้งพบว่าทักษะของผู้ตรวจสอบภายในจะส่งผลต่อประสิทธิภาพของงานตรวจสอบภายในและขึ้นอยู่กับลักษณะของงานตรวจสอบภายในที่แตกต่างกันไปในแต่ละองค์กร และความเป็นอิสระของผู้ตรวจสอบภายในยังขึ้นอยู่กับขนาดและรูปแบบการบริหารจัดการขององค์กร

คำสำคัญ: ประสิทธิภาพ งานตรวจสอบภายใน ผู้ตรวจสอบภายใน

Factors affecting the effectiveness of Internal Audit: View of Internal Auditor

Oraphan Sangsivavait*

Boonrawd Brewery Co., Ltd.

***Correspondence:** oraphan.sangsivavait@gmail.com doi: 10.14456/jisb.2018.14

Received: 30 May 2017 Revised: 29 Jun 2017 Accepted: 12 Jul 2017

Abstract

The objective of this study is to examine the factors influencing the effectiveness of internal audit. This is quantitative research. The study was conducted on a sample of 200 sample groups with more than 3 months of experience by online questionnaire. The results show that management support and monitoring affect the effectiveness of internal auditing. Management support is based on the perception of the importance of internal auditing through the quality of internal auditing. In addition, the skills of internal auditors would affect the effectiveness of internal auditing, depending on the nature of the internal auditing process. The independence of internal auditors also depends on the size and style of the organization's management.

Keywords: Effectiveness, Internal audit, Internal auditor

1. บทนำ

1.1 ความสำคัญและที่มาของปัญหา

ปัจจุบันการดำเนินงานขององค์กรต้องพบกับการเปลี่ยนแปลงของปัจจัยในแต่ละด้านอย่างรวดเร็ว ทั้งจากสภาพแวดล้อมภายในและสภาพแวดล้อมภายนอก อาทิ สภาพแวดล้อมทางด้านเศรษฐกิจ การเมือง เทคโนโลยี สังคม และวัฒนธรรม ส่งผลให้องค์กรต้องเผชิญกับความเสี่ยงในการบริหารจัดการ การเตรียมพร้อมในการปรับตัวให้ทันต่อสภาพแวดล้อมภายนอกที่เปลี่ยนแปลงไปรวมถึงการพัฒนาศักยภาพขององค์กร

กรมบัญชีกลางได้กล่าวถึง การปรับตัวรับการเปลี่ยนแปลงในอนาคตของบริษัท การดำเนินการต่างๆ จะเปลี่ยนไป ไม่ว่าจะเข้าลักษณะจำเป็นต้องมีการเปลี่ยนแปลงหรือต้องมีการปรับตัวของการดำเนินการของตลาดเงิน ตลาดทุน ธุรกิจบริการ ตลาดการค้า และตลาดแรงงาน ทั้งนี้ การเปลี่ยนแปลงที่เกิดขึ้นอาจมีผลกระทบต่องค์กรในด้านต่างๆ ซึ่งผู้ตรวจสอบภายในอาจต้องนำมาเป็นข้อมูลในการเตรียมความพร้อม ผลกระทบต่อหน่วยงานอาจทำให้วิธีการหรือขั้นตอนการดำเนินการมีการเปลี่ยนแปลงไปด้วย นอกจากนี้ ผู้ตรวจสอบภายในจะต้องรอบรู้ข่าวสารและทันโลก ทำความเข้าใจปัจจัยหรือสภาพแวดล้อมที่มีการเปลี่ยนแปลงอย่างต่อเนื่องและรวดเร็วทั้งจากภายในและภายนอก เพื่อสามารถตรวจสอบให้ตรงประเด็น สามารถเป็นหน่วยงานสนับสนุนที่มีประสิทธิภาพ ทำให้องค์กรดำเนินงานไปได้อย่างมีประสิทธิภาพและเพิ่มคุณค่า รวมทั้งสามารถให้ข้อเสนอแนะแก่ผู้บริหารในบทบาทด้านงานให้คำปรึกษา (Consultant) ได้อย่างมีประสิทธิภาพ

ดังนั้น ผู้ตรวจสอบภายในซึ่งทำหน้าที่เป็นเครื่องมือของฝ่ายบริหาร ไม่ว่าจะเป็นการให้ข้อมูลและการเสนอแนะมาตรการแก้ไขที่เป็นประโยชน์ให้กับองค์กร จำเป็นต้องอาศัยความรู้ความสามารถ ความเชี่ยวชาญในวิชาชีพ รวมทั้งการพัฒนาความรู้ในงานตรวจสอบ ความรอบรู้ในวิชาชีพความรู้อื่นๆ ตลอดจนจัดเตรียมความพร้อมเพื่อรับมือกับการเปลี่ยนแปลงจากปัจจัยภายนอก ก็เป็นส่วนสำคัญที่จะช่วยให้การปฏิบัติงานตรวจสอบมีประสิทธิภาพเพิ่มมากขึ้นและเป็นที่น่าเชื่อถือให้กับผู้บริหารและหน่วยงานรับตรวจ

ผู้วิจัยในฐานะที่เป็นผู้ปฏิบัติงานด้านการตรวจสอบภายใน จึงต้องการศึกษาปัจจัยที่ส่งผลต่อประสิทธิภาพของงานตรวจสอบภายในตามมุมมองของผู้ตรวจสอบภายใน เพื่อใช้เป็นแนวทางในการแก้ไขและวางแผนเพื่อส่งเสริมรวมทั้งพัฒนาผู้ปฏิบัติงานตรวจสอบในแต่ละด้านต่อไป

1.2 วัตถุประสงค์ของการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาอิทธิพลของปัจจัยต่างๆ ประกอบด้วยคุณภาพของงานตรวจสอบภายใน การสนับสนุนจากผู้บริหาร การฝึกอบรมและพัฒนา ทักษะของผู้ตรวจสอบภายใน การติดตามและประเมินผล และความเป็นอิสระของผู้ตรวจสอบภายในที่ส่งผลต่อประสิทธิภาพของงานตรวจสอบภายในตามมุมมองของผู้ตรวจสอบภายใน

2. งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยในอดีตสามารถสรุปปัจจัยที่เกี่ยวข้องกับการศึกษาได้ดังนี้

คุณภาพของงานตรวจสอบภายใน (Internal audit quality) หมายถึง ความเป็นไปได้ในการตรวจพบความผิดพลาด และค้นพบเพื่อควบคุมไม่ให้เกิดช่องโหว่ในการบริหารงาน (Heras et al., 2012) ซึ่งเป็นหน้าที่ของผู้ตรวจสอบภายในที่จะตรวจพบข้อมูลซึ่งขัดแย้งกับข้อเท็จจริงด้วยความสามารถทางเทคนิคและรายงานข้อผิดพลาดที่เกิดขึ้นอย่างเป็นอิสระ (Chadegani, 2011)

การสนับสนุนจากผู้บริหาร (Management support) หมายถึง ปัจจัยสำคัญที่มีความจำเป็นอย่างมากในการช่วยส่งเสริมการพัฒนาองค์ความรู้ภายในองค์กร การจัดหาเงินทุนเพื่อโครงสร้างพื้นฐานด้านความรู้และการเพิ่มขีดความสามารถของพนักงานในการสร้างสรรค์ แบ่งปัน จัดเก็บ และเผยแพร่ความรู้ (Haque & Anwar, 2012) ซึ่งถือเป็นปัจจัยหนึ่งที่ส่งผลต่อคุณลักษณะของผู้ตรวจสอบภายใน หากผู้บริหารสามารถปฏิบัติตามผลการตรวจสอบและ

คำแนะนำที่ได้รับจากหน่วยงานตรวจสอบภายในจะทำให้สามารถระบุประสิทธิภาพของผลงานได้ (Mihret & Yismaw, 2007)

การฝึกอบรมและการพัฒนา (Training and development) หมายถึง กระบวนการเรียนรู้ที่เกี่ยวข้องกับการได้มาซึ่งความรู้ ทักษะ แนวคิด หลักเกณฑ์ หรือการเปลี่ยนทัศนคติและพฤติกรรม เพื่อเพิ่มประสิทธิภาพการทำงานให้กับบุคลากร ซึ่งเป็นกระบวนการที่ต้องปฏิบัติอย่างต่อเนื่อง โดยบุคลากรจะได้รับความรู้อย่างแท้จริงและทราบถึงแนวทางในการปฏิบัติงานในองค์กรได้ดีขึ้น (Ameeq & Hanif, 2013)

ทักษะของผู้ตรวจสอบภายใน (Skills of internal audit) หมายถึง ความรู้และความสามารถในการตรวจสอบข้อมูลหลักฐานทางการบัญชีและข้อมูลอื่น ๆ ตามมาตรฐานที่ได้รับการยอมรับโดยทั่วไปในการปฏิบัติงานภาคสนามและช่วยให้บรรลุกิจกรรมและหน้าที่ที่รับผิดชอบ (Usman, 2016)

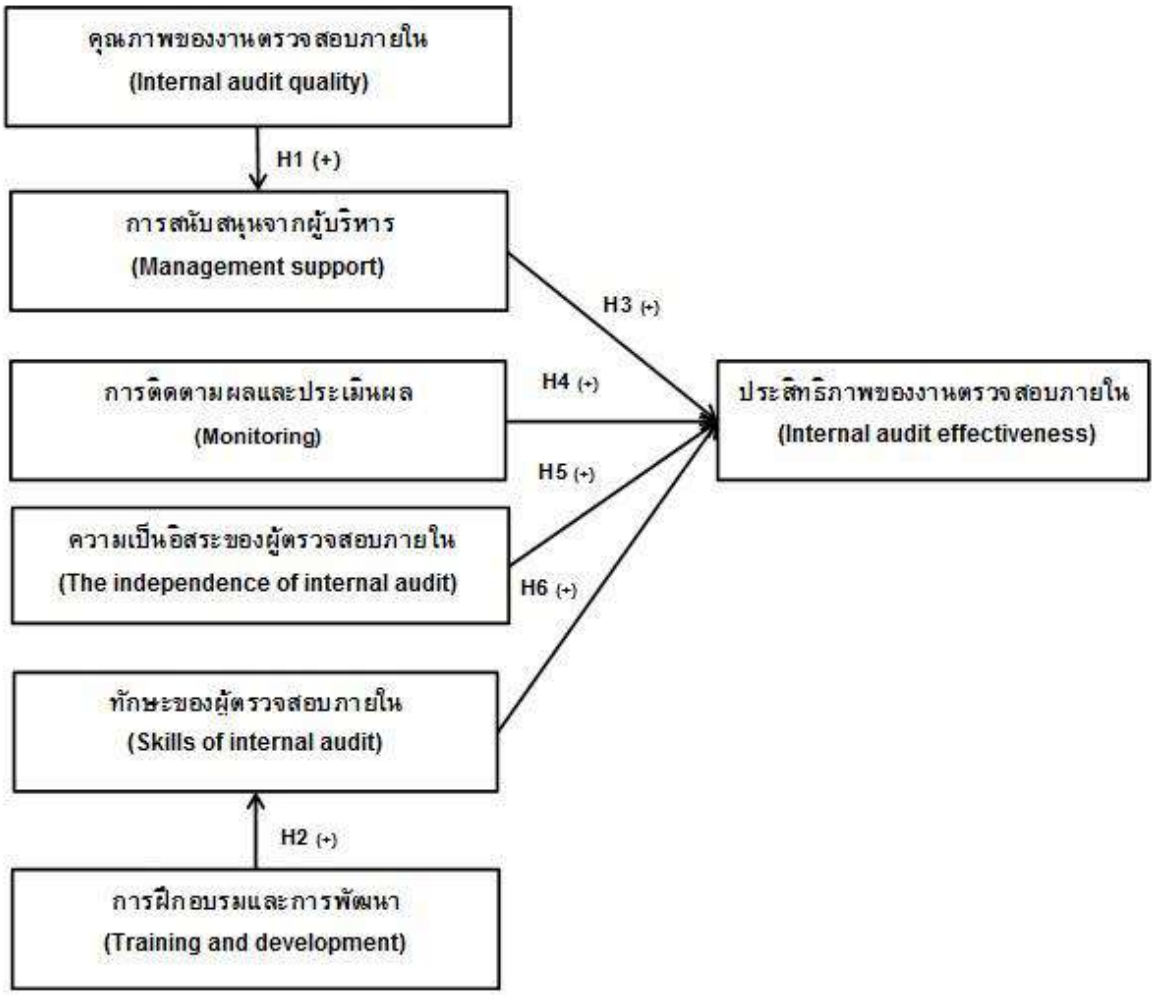
การติดตามผลและประเมินผล (**Monitoring)** หมายถึง กระบวนการตรวจสอบอย่างต่อเนื่องที่จะช่วยให้ฝ่ายบริหารสามารถทราบว่ากระบวนการทางธุรกิจได้มีการปฏิบัติตามกฎระเบียบและติดตามการเพิ่มขึ้นของระดับประสิทธิภาพและประสิทธิผลที่ตั้งใจไว้ (Deloitte Development LLC, 2010) วิธีนี้เป็นวิธีการที่ผู้ตรวจสอบภายในใช้ในการดำเนินกิจกรรมที่เกี่ยวข้องกับหลักการตรวจสอบอย่างต่อเนื่อง (Institute of internal auditors, 2013)

ความเป็นอิสระของผู้ตรวจสอบภายใน (The independence of internal audit) หมายถึง การปฏิบัติงานโดยมีมุมมองหรือทัศนคติที่ไม่ลำเอียง มีอิสระทางความคิด ซึ่งจะช่วยให้ผู้ตรวจสอบสามารถปฏิบัติงานได้ด้วยความเที่ยงธรรม (Usman, 2016) ทำให้เจ้าหน้าที่สามารถตรวจสอบขั้นตอนการปฏิบัติงานต่าง ๆ ที่นอกเหนือจากข้อมูลที่ถูกบันทึกตามความเป็นจริง (Dahir, 2016)

ประสิทธิภาพของงานตรวจสอบภายใน (Internal audit effectiveness) หมายถึง ระดับของคุณภาพรวมถึงการปฏิบัติงานได้บรรลุตามวัตถุประสงค์ที่ได้กำหนดไว้ (Institute of internal audit, 2013) รวมถึงผลลัพธ์หรือผลงานของบุคลากรที่มีวัตถุประสงค์เพื่อให้บรรลุเป้าหมายที่กำหนด ในขณะที่ประสิทธิภาพอาจถูกใช้เพื่อกำหนดสิ่งที่องค์กรประสบความสำเร็จในส่วนที่เกี่ยวข้องกับกระบวนการ ผลลัพธ์ ความเชื่อมโยงและความสำเร็จ (Nassazi, 2013)

3. กรอบแนวคิดการวิจัยและสมมติฐานการวิจัย

ในการศึกษาปัจจัยที่ส่งผลกระทบต่อประสิทธิภาพของงานตรวจสอบภายใน: มุมมองของผู้ตรวจสอบภายใน ได้พัฒนากรอบแนวคิดมาจากงานวิจัยต่างๆ ที่เกี่ยวข้อง โดยมีปัจจัยที่เกี่ยวข้องทั้งหมด 6 ปัจจัย คุณภาพของงานตรวจสอบภายใน การสนับสนุนจากผู้บริหาร การติดตามและประเมินผล ทักษะของผู้ตรวจสอบภายใน การฝึกอบรมและการพัฒนา และความเป็นอิสระของผู้ตรวจสอบภายใน ที่ส่งผลต่อประสิทธิภาพของงานตรวจสอบภายใน ดังภาพที่ 1



ภาพที่ 1 กรอบแนวคิดปัจจัยที่ส่งผลกระทบต่อประสิทธิภาพงานตรวจสอบภายใน: มุมมองของผู้ตรวจสอบภายใน

Hung and Hair (2013) กล่าวว่า คุณภาพหรือผลงานของผู้ตรวจสอบภายในนั้นส่งผลต่อการรับรู้และทัศนคติของผู้บริหาร หากผู้ตรวจสอบภายในไม่สามารถแสดงให้ผู้บริหารรับรู้และยอมรับในคุณภาพของงานตรวจสอบภายในอาจส่งผลต่อการได้รับการสนับสนุนจากผู้บริหาร ซึ่งสอดคล้องกับบทความของ Martin (2013) ที่ให้ความเห็นว่า คุณภาพของงานตรวจสอบภายในนั้นมาจากการวางแผน การดำเนินการตรวจสอบและการจัดทำระบบการควบคุมคุณภาพของบริษัท ซึ่งผู้บริหารระดับสูงอยู่ในฐานะที่จะต้องตรวจสอบและประเมินผลการปฏิบัติงานของผู้ตรวจสอบภายในด้านคุณภาพของการตรวจสอบ หากผู้ตรวจสอบภายในไม่สามารถปฏิบัติงานให้คุณภาพอยู่ในระดับที่ผู้บริหารพึงพอใจได้ก็จะส่งผลต่อการรับรู้และทัศนคติในการสนับสนุนจากผู้บริหารอีกด้วย

H1: คุณภาพของงานตรวจสอบภายในมีความสัมพันธ์เชิงบวกกับการสนับสนุนจากผู้บริหาร

Asfaw et al. (2015) กล่าวว่า กิจกรรมการฝึกอบรมและพัฒนาของบุคลากรมีส่วนในการที่จะนำเอาศักยภาพใหม่ๆ ของบุคลากรออกมาในการปฏิบัติงานและจะส่งผลในเชิงบวกต่อประสิทธิผลของบุคลากร ซึ่งสอดคล้องกับการศึกษาของ Falola et al. (2014) ที่แสดงให้เห็นว่า การฝึกอบรมและพัฒนาถือว่าเป็นปัจจัยสำคัญเพื่อความอยู่รอดขององค์กร นอกจากนี้ยังมีความจำเป็นต่อประสิทธิภาพของบุคลากร การเพิ่มขีดความสามารถของบุคลากรในการปรับตัวให้เข้ากับสภาพแวดล้อมและเทคโนโลยีทางธุรกิจที่เปลี่ยนไป รวมทั้งยังเป็นการท้าท้ายเพื่อเพิ่มพูนความรู้ความเข้าใจและประสิทธิภาพของบุคลากรในการพัฒนาทักษะ ความคิดสร้างสรรค์และการแก้ปัญหา

H2: การฝึกอบรมและพัฒนามีความสัมพันธ์เชิงบวกกับทักษะของผู้ตรวจสอบภายใน

Hailemariam (2014) ได้กล่าวว่า ผู้ตรวจสอบภายในควรมีความสัมพันธ์ที่ใกล้ชิดกับผู้บริหารขององค์กร เพราะความต้องการการสนับสนุนที่ดีและรับรู้ถึงความสำคัญจากผู้บริหารที่จะทำให้เกิดประสิทธิภาพมากขึ้นและบรรลุวัตถุประสงค์ของงานตรวจสอบ การสนับสนุนจากผู้บริหารอยู่ในรูปแบบของการสนับสนุนกระบวนการตรวจสอบไม่ว่าจะเป็นด้านทรัพยากร การเงิน การเดินทาง การฝึกอบรมด้านการตรวจสอบด้วยเทคโนโลยีสารสนเทศและขั้นตอนการปฏิบัติงานแบบใหม่ งบประมาณด้านการลงทุน การให้ได้วุฒิรับรองรวมทั้งสิ่งอำนวยความสะดวกต่าง ๆ ในงานตรวจสอบภายใน และการสนับสนุนในรูปแบบของจัดหาทรัพยากร จะกระตุ้นให้เกิดกระบวนการตรวจสอบภายในที่มีภาระผูกพันที่จะส่งเสริมและสื่อสารมูลค่าเพิ่มของงานตรวจสอบภายในให้เกิดประสิทธิภาพในการทำงานตรวจสอบ ซึ่งสอดคล้องกับการศึกษาของ Alzeban and Gwilliam (2014) ที่ได้ชี้ให้เห็นว่าการสนับสนุนจากผู้บริหารมีผลเชิงบวกและมีความหมายที่เกี่ยวข้องกับประสิทธิภาพของการตรวจสอบภายใน

H3: การสนับสนุนของผู้บริหารมีความสัมพันธ์เชิงบวกกับประสิทธิภาพของงานตรวจสอบภายใน

Onatuyeh and Aniefor (2013) กล่าวว่า การทดสอบและประเมินผลความน่าเชื่อถือจากผลการตรวจสอบครั้งก่อนที่หน่วยงานตรวจสอบภายในเคยรายงานไป จะช่วยส่งเสริมด้านความรับผิดชอบและประสิทธิภาพของงานตรวจสอบเพิ่มขึ้น ซึ่งสอดคล้องกับ Deloitte Development LLC (2010) ที่กล่าวว่า การติดตามและประเมินผลจะช่วยให้ฝ่ายบริหารสามารถตรวจสอบกระบวนการทางธุรกิจขององค์กรได้อย่างต่อเนื่อง เพื่อให้มีการปฏิบัติตามกฎระเบียบและเพิ่มระดับประสิทธิภาพและประสิทธิผลให้ดียิ่งขึ้น

H4: การติดตามและประเมินผลมีความสัมพันธ์เชิงบวกกับประสิทธิภาพของงานตรวจสอบภายใน

Dellai and Omri (2016) กล่าวว่า ปัจจัยด้านความเป็นอิสระของผู้ตรวจสอบภายในมีผลกระทบเชิงบวกต่อประสิทธิภาพของหน่วยงานตรวจสอบภายใน ซึ่งสอดคล้องกับผลการศึกษาของ Shamsuddin and Bharathii (2014) ที่พบว่า ความเป็นอิสระของผู้ตรวจสอบภายในนั้นส่งผลกระทบต่อประสิทธิภาพของงานตรวจสอบภายใน เนื่องจากเมื่อผู้ตรวจสอบภายในต้องปฏิบัติงานอย่างไม่เป็นอิสระจะต้องเผชิญหน้ากับสภาวะที่ยากลำบาก และจะส่งผลให้วัตถุประสงค์ของการปฏิบัติหน้าที่ของผู้ตรวจสอบภายในจะต้องประสบปัญหา

H5: ความเป็นอิสระของผู้ตรวจสอบภายในมีความสัมพันธ์เชิงบวกกับประสิทธิภาพของงานตรวจสอบภายใน

Badara and Saidin (2014) พบว่า ประสบการณ์ของผู้ตรวจสอบภายในส่งผลต่อประสิทธิภาพของงานตรวจสอบภายในอย่างเป็นสาระสำคัญและมีความสัมพันธ์เชื่อมโยงต่อคณะกรรมการตรวจสอบ กล่าวคือ การที่องค์กรจะบรรลุประสิทธิผลด้านงานตรวจสอบภายในควรมีบุคลากรที่มีประสบการณ์ด้านการตรวจสอบ ซึ่งสอดคล้องกับ การศึกษาของ Mahzan and Hassan (2015) ที่กล่าวว่า ทักษะของผู้ตรวจสอบภายในส่งผลต่อการเพิ่มประสิทธิภาพของหน่วยงานตรวจสอบด้วยการปรับปรุงการรับรู้ถึงบทบาทภายในองค์กร ดังนั้น จึงไม่ต้องสงสัยว่าทักษะของผู้ตรวจสอบภายในนั้นมีความสำคัญและสามารถนำไปสู่การสร้างประสิทธิภาพของงานตรวจสอบภายในได้

H6: ทักษะของผู้ตรวจสอบภายในมีความสัมพันธ์เชิงบวกกับประสิทธิภาพของงานตรวจสอบภายใน

4. วิธีการวิจัย

งานวิจัยนี้จัดเก็บข้อมูลจากกลุ่มตัวอย่างที่เป็นผู้ตรวจสอบภายในที่มีประสบการณ์มากกว่า 3 เดือนขึ้นไปผ่านสื่อสังคมออนไลน์ จำนวน 200 กลุ่มตัวอย่าง โดยใช้แบบสอบถามเป็นเครื่องมือ ซึ่งก่อนจัดเก็บข้อมูลจากกลุ่มตัวอย่าง งานวิจัยนี้ได้นำแบบสอบถามที่พัฒนามาจากวิจัยในอดีต (ประกอบด้วย Heres et al., 2012; Chadegani, 2011; Haque & Anwar, 2012; Ameeq & Hanif, 2013; Usman, 2016; Deloitte Development LLC, 2010; Institute of Internal Auditors, 2013; Dahir, 2016; Nassazi, 2013) ไปทดสอบกับกลุ่มตัวอย่าง เพื่อวิเคราะห์แบบสอบถามเบื้องต้นและปรับปรุงข้อคำถามให้มีความเหมาะสม เมื่อแบบสอบถามมีความเหมาะสมแล้วจึงทำการเก็บข้อมูลจริง โดยแจกแบบสอบถามออนไลน์ไปบนสื่อสังคมออนไลน์

5. ผลการวิจัย

5.1 การทดสอบข้อตกลงเบื้องต้นทางสถิติ

ข้อมูลที่จัดเก็บจากกลุ่มตัวอย่างถูกนำไปทดสอบข้อมูลขาดหาย (Missing data) และข้อมูลสุดโต่ง (Outliers) การกระจายแบบปกติ (Normal) ความสัมพันธ์เชิงเส้นตรง (Linearity) และภาวะร่วมเส้นตรงพหุ (Multicollinearity) ซึ่งผลการทดสอบพบว่าผ่านเกณฑ์ตามที่กำหนด

5.2 การประเมินความเที่ยงและความตรงของแบบสอบถาม

งานวิจัยนี้ได้ตรวจสอบความเที่ยงของเครื่องมือ โดยใช้ค่าประสิทธิ์แอลฟาของครอนบาซ (Cronbach's alpha) โดยใช้เกณฑ์มากกว่า 0.50 ซึ่งถือว่าเป็นเกณฑ์ที่เหมาะสมสำหรับงานวิจัยแบบการวิจัยพื้นฐาน (Basic research) (สุพิชญา อาชวจิรดา, 2557) ตารางที่ 1 แสดงค่าสถิติแต่ละข้อคำถามที่ผ่านเกณฑ์

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัยที่ 1: คุณภาพของงานตรวจสอบภายใน (% of variance = 62.594, Cronbach's alpha = 0.785)			
ท่านสามารถปฏิบัติงานเป็นไปตามมาตรฐานสากลสำหรับวิชาชีพด้านการตรวจสอบภายใน	3.800	0.501	0.738
หน่วยงานตรวจสอบภายในของท่านมีกระบวนการที่สามารถให้ความเชื่อมั่นต่อความน่าเชื่อถือในความสมบูรณ์ของงบการเงิน	3.715	0.660	0.802
หน่วยงานตรวจสอบภายในของท่านมีกระบวนการที่ช่วยในการตรวจพบความผิดพลาดและข้อมูลที่ขัดแย้งกับข้อเท็จจริง	3.820	0.556	0.842
หน่วยงานตรวจสอบภายในของท่านมีกระบวนการที่ช่วยในการควบคุมไม่ให้เกิดช่องโหว่ในการบริหารงาน	3.730	0.813	0.778

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด (ต่อ)

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัยที่ 2: การสนับสนุนของผู้บริหาร (% of variance = 68.765, Cronbach's alpha = 0.847)			
ผู้บริหารระดับสูงให้ความสนใจในประเด็นสำคัญที่หน่วยงานตรวจสอบภายในตรวจพบ	3.335	0.636	0.830
ผู้บริหารระดับสูงให้ความสำคัญในการนำผลที่ได้รับจากการตรวจสอบและคำแนะนำไปปฏิบัติตาม	3.310	0.596	0.817
ผู้บริหารระดับสูงให้ความสำคัญต่อการพัฒนาขีดความสามารถและความรู้ของพนักงานในหน่วยงานตรวจสอบภายใน	3.350	0.591	0.817
ผู้บริหารระดับสูงให้ความสำคัญในการสนับสนุนด้านงบประมาณกับหน่วยงานตรวจสอบภายใน	3.225	0.726	0.852
ปัจจัยที่ 3: การฝึกอบรมและการพัฒนา (% of variance = 62.800, Cronbach's alpha = 0.701)			
ท่านมีการพัฒนาตนเองในเรื่องงานให้เชี่ยวชาญและก้าวหน้าในงานมากขึ้นเรื่อยๆ	3.965	0.562	0.780
ท่านต้องมีการพัฒนาตนเองและเรียนรู้เรื่องใหม่ๆ เช่น เทคโนโลยีสารสนเทศ ปัจจัยด้านการเปลี่ยนแปลงของเศรษฐกิจและการเมือง เป็นต้นอย่างสม่ำเสมอ	4.045	0.711	0.843
หลักสูตรที่ท่านได้รับการฝึกอบรมที่ผ่านมาส่งผลให้มีการเพิ่มระดับทักษะความรู้และความสามารถในการปฏิบัติงาน	3.830	0.586	0.751
ปัจจัยที่ 4: ทักษะของผู้ตรวจสอบภายใน (% of variance = 60.659, Cronbach's alpha = 0.777)			
ท่านสามารถนำความรู้ที่ได้รับการศึกษามาประยุกต์ใช้ในการปฏิบัติงานได้	3.560	0.517	0.684
ผู้ตรวจสอบภายในควรมีความเข้าใจเกี่ยวกับหลักการบริหาร เพื่อใช้ในการประเมินกระบวนการปฏิบัติงานขององค์กร	4.165	0.468	0.828
ผู้ตรวจสอบภายในควรมีความรู้ด้านการบัญชี รวมถึงความเข้าใจในมาตรฐานอื่นๆ ที่เกี่ยวข้อง เพื่อให้บรรลุตามกิจกรรมและหน้าที่ที่รับผิดชอบ	4.055	0.569	0.738
ผู้ตรวจสอบภายในควรมีการศึกษาความรู้เพิ่มเติมอย่างสม่ำเสมอ	4.315	0.598	0.853
ปัจจัยที่ 5: การติดตามและประเมินผล (% of variance = 72.637, Cronbach's alpha = 0.810)			
หน่วยงานตรวจสอบภายในของท่านมีกระบวนการที่ใช้ในการติดตามความคืบหน้าของผลการตรวจสอบได้อย่างต่อเนื่อง	3.880	0.713	0.865
หน่วยงานตรวจสอบภายในของท่านมีกระบวนการติดต่อผู้รับตรวจเกี่ยวกับความคืบหน้าในการแก้ไขปรับปรุงตามรายงานผลการตรวจสอบ	3.900	0.673	0.852
กระบวนการตรวจสอบภายในของท่านสามารถช่วยให้ฝ่ายบริหารสามารถทราบถึงกระบวนการทางธุรกิจว่ามีการปฏิบัติเป็นไปตามกฎระเบียบ	3.830	0.619	0.840

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด (ต่อ)

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัยที่ 6: ความเป็นอิสระของผู้ตรวจสอบภายใน (% of variance = 69.271, Cronbach's alpha = 0.850)			
ท่านสามารถปฏิบัติงานตรวจสอบได้โดยไม่มีข้อจำกัด	3.440	0.662	0.859
ท่านสามารถตรวจสอบและบันทึกข้อมูลตามความเป็นจริง	3.855	0.553	0.839
ท่านสามารถตรวจสอบขั้นตอนการปฏิบัติงานต่าง ๆ ที่นอกเหนือจากข้อมูลที่ถูกบันทึกได้ตามความเป็นจริง	3.900	0.530	0.804
ท่านสามารถรายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบและผู้บริหารระดับสูงได้โดยไม่มีข้อจำกัด	3.570	0.535	0.826
ปัจจัยที่ 7: ประสิทธิภาพของงานตรวจสอบภายใน (% of variance = 68.552, Cronbach's alpha = 0.846)			
หน่วยงานตรวจสอบภายในของท่านสามารถประเมินการตอบสนองความเสี่ยงได้อย่างเหมาะสม	3.700	0.680	0.859
หน่วยงานตรวจสอบภายในของท่านสามารถช่วยให้องค์กรบรรลุวัตถุประสงค์ตามที่ได้วางไว้	3.745	0.672	0.808
หน่วยงานตรวจสอบภายในของท่านสามารถช่วยให้องค์กรมีความสามารถในการป้องกันการสูญเสียรายได้	3.330	0.717	0.813
หน่วยงานตรวจสอบภายในของท่านสามารถแสดงให้เห็นถึงการควบคุมที่สำคัญได้ครอบคลุมทั่วทั้งองค์กร	3.720	0.666	0.830

5.3 ลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่าง

กลุ่มตัวอย่างส่วนใหญ่เป็นเพศหญิง (ร้อยละ 61.50) อายุระหว่าง 25-30 ปี (ร้อยละ 73.00) ระดับการศึกษาปริญญาตรี (ร้อยละ 83.50) ปัจจุบันยังปฏิบัติงานตรวจสอบภายใน (ร้อยละ 99.50) ประสบการณ์ด้านงานตรวจสอบภายในตั้งแต่ 2 ปีขึ้นไป (ร้อยละ 45.00) ตำแหน่งงานในปัจจุบันเป็นเจ้าหน้าที่ตรวจสอบ (ร้อยละ 75.00) ไม่มีวุฒิทางวิชาชีพ (ร้อยละ 96.50) มีจำนวนบุคลากรในองค์กร มากกว่า 200 คน (ร้อยละ 63.50) และไม่มีการตรวจสอบบริษัทในเครือ (ร้อยละ 76.50)

5.4 การทดสอบสมมติฐานทางสถิติ

ในการทดสอบสมมติฐานการวิจัย ผู้วิจัยใช้วิธีการวิเคราะห์การถดถอยเชิงเส้นเดียว (Simple linear regression) และการถดถอยพหุคูณ (Multiple regression) โดยใช้ค่า p-value ที่น้อยกว่าหรือเท่ากับ 0.05 เป็นตัวกำหนดนัยสำคัญทางสถิติ โดยแบ่งการวิเคราะห์ออกเป็น 3 ส่วน ตามกรอบแนวคิดการวิจัยดังนี้

ส่วนที่ 1 ผลการวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรอิสระ คุณภาพของงานตรวจสอบภายในกับตัวแปรตาม การสนับสนุนจากผู้บริหาร พบว่า มีความสัมพันธ์โดยตรงกับตัวแปรตาม โดยผลการวิเคราะห์ความถดถอยได้แสดงให้เห็นว่าตัวแปรอิสระ กำหนดตัวแปรตามที่ระดับนัยสำคัญ p = 0.000 ($F_{1,198}$ = 86.306) เมื่อวิเคราะห์ในรายละเอียดของตัวแปรอิสระ จะพบว่าคุณภาพของงานตรวจสอบภายในเป็นตัวกำหนดการสนับสนุนจากผู้บริหาร ที่ระดับนัยสำคัญ p = 0.000 โดยความผันแปรของตัวแปรตามเท่ากับร้อยละ 30.4 (R^2 = 0.304) และมีค่าสัมประสิทธิ์การถดถอยของตัวแปรอิสระ (B) เท่ากับ 0.581 ดังตารางที่ 2 และ 3 ซึ่งสอดคล้องกับงานวิจัยของ Hung and Hair (2013) และ Martin

(2013) ที่กล่าวว่า คุณภาพหรือผลงานของผู้ตรวจสอบภายในนั้นส่งผลต่อการรับรู้และทัศนคติของผู้บริหารที่มีต่อหน่วยงานตรวจสอบภายใน หากผู้ตรวจสอบภายในสามารถปฏิบัติงานได้คุณภาพอยู่ในระดับที่ผู้บริหารพึงพอใจได้ก็จะส่งผลต่อระดับการให้การสนับสนุนจากผู้บริหารที่เพิ่มขึ้นอีกด้วย

ตารางที่ 2 ผลการวิเคราะห์การถดถอยของคุณภาพงานตรวจสอบภายในกับการสนับสนุนจากผู้บริหาร

Model	Sum of Squares	df	Mean Square	F	Sig
Regression	16.930	1	16.930	86.306	0.000
Residual	38.840	198	0.196		
Total	55.770	199			

* $p < 0.05$

ตารางที่ 3 ผลการวิเคราะห์ค่าสัมประสิทธิ์การถดถอยของคุณภาพงานตรวจสอบภายในกับการสนับสนุนจากผู้บริหาร

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig
	B	Std Error	Beta		
(Constant)	1.116	0.238		4.697	0.000
คุณภาพของงานตรวจสอบภายใน	0.581	0.063	0.551	9.290	0.000

* $p < 0.05$, R = 0.551, R2 = 0.304, SE = 0.443

ส่วนที่ 2 ผลการวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรอิสระ การฝึกอบรมและการพัฒนา กับตัวแปรตามทักษะของผู้ตรวจสอบภายใน พบว่า มีความสัมพันธ์โดยตรงกับตัวแปรตาม โดยผลการวิเคราะห์ความถดถอยได้แสดงให้เห็นว่าตัวแปรอิสระ กำหนดตัวแปรตามที่ระดับนัยสำคัญ $p = 0.000$ ($F_{1,198} = 15.101$) เมื่อวิเคราะห์ในรายละเอียดของตัวแปรอิสระ จะพบว่าการฝึกอบรมและพัฒนาเป็นตัวกำหนดทักษะของผู้ตรวจสอบภายใน ที่ระดับนัยสำคัญ $p = 0.000$ โดยความผันแปรของตัวแปรตามเท่ากับร้อยละ 7.10 ($R^2 = 0.071$) และมีค่าสัมประสิทธิ์การถดถอยของตัวแปรอิสระ (B) เท่ากับ 0.226 ดังตารางที่ 4 และ 5 ซึ่งสอดคล้องกับงานวิจัยของ Falola et al. (2014) ที่กล่าวว่า การฝึกอบรมและพัฒนาเป็นปัจจัยสำคัญที่จะเพิ่มขีดความสามารถให้กับบุคลากรในการปรับตัวให้เข้ากับสภาพแวดล้อมและเทคโนโลยีทางธุรกิจที่มีการเปลี่ยนแปลงไป เพื่อความอยู่รอดขององค์กร เมื่อผู้ตรวจสอบภายในได้รับการฝึกอบรมและพัฒนาอย่างเหมาะสมจะช่วยเพิ่มความสามารถในการปฏิบัติงานมากยิ่งขึ้น

ตารางที่ 4 ผลการวิเคราะห์การถดถอยของการฝึกอบรมและพัฒนากับทักษะของผู้ตรวจสอบภายใน

Model	Sum of Squares	df	Mean Square	F	Sig
Regression	2.468	1	2.468	15.101	0.000
Residual	32.357	98	0.163		
Total	34.825	99			

* $p < 0.05$

ตารางที่ 5 ผลการวิเคราะห์ค่าสัมประสิทธิ์การถดถอยของการฝึกอบรมและพัฒนากับทักษะของผู้ตรวจสอบภายใน

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig
	B	Std Error	Beta		
(Constant)	3.132	0.231		13.541	0.000
การฝึกอบรมและการพัฒนา	0.226	0.058	0.266	3.886	0.000

* $p < 0.05$, R = 0.266, R2 = 0.071, SE = 0.404

ส่วนที่ 3 ผลการวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรอิสระ ทักษะของผู้ตรวจสอบภายใน การสนับสนุนจากผู้บริหาร การติดตามผลและประเมินผล ความเป็นอิสระของผู้ตรวจสอบภายใน กับตัวแปรตาม ประสิทธิภาพของงานตรวจสอบภายใน พบว่า มีความสัมพันธ์โดยตรงกับตัวแปรตาม โดยผลการวิเคราะห์ความถดถอยได้แสดงให้เห็นว่าตัวแปรอิสระ กำหนดตัวแปรตามที่ระดับนัยสำคัญ p = 0.000 ($F_{4,195}$ = 105.350) เมื่อวิเคราะห์ในรายละเอียดของตัวแปรอิสระ จะพบว่าการสนับสนุนจากผู้บริหารกับการฝึกอบรมและพัฒนาเป็นตัวกำหนดประสิทธิภาพของงานตรวจสอบภายใน ที่ระดับนัยสำคัญ p = 0.000 และ p = 0.000 ตามลำดับ โดยความผันแปรของตัวแปรตามเท่ากับร้อยละ 68.40 (R^2 = 0.684) และมีค่าสัมประสิทธิ์การถดถอยของตัวแปรอิสระ (B) เท่ากับ 0.252 และ 0.539 ตามลำดับ ตามตารางที่ 6 และ 7 ซึ่งสอดคล้องกับงานวิจัยของ Alzeban and Gwilliam (2014) ที่ได้ชี้ให้เห็นว่าการสนับสนุนจากผู้บริหารมีผลเชิงบวกและมีความหมายที่เกี่ยวข้องกับประสิทธิภาพของการตรวจสอบภายใน หากฝ่ายบริหารให้การสนับสนุนและให้ความสำคัญมากก็จะส่งผลให้ประสิทธิภาพของงานตรวจสอบภายในเพิ่มขึ้น และ Onatuyeh et al. (2013) และ Deloitte Development LLC (2010) ได้กล่าวว่า กิจกรรมการติดตามผลและการประเมินผลความน่าเชื่อถือจากผลการตรวจสอบครั้งก่อนที่หน่วยงานตรวจสอบภายในเคยรายงานให้ทางหน่วยรับตรวจ จะช่วยส่งเสริมด้านความรับผิดชอบและประสิทธิภาพของงานตรวจสอบเพิ่มขึ้น นอกจากนี้ยังช่วยให้ฝ่ายบริหารสามารถสอบทานกระบวนการทางธุรกิจขององค์กรได้อย่างต่อเนื่อง

ตารางที่ 6 ผลการวิเคราะห์การถดถอยของทักษะของผู้ตรวจสอบภายใน การสนับสนุนจากผู้บริหาร การติดตามผลและประเมินผล ความเป็นอิสระของผู้ตรวจสอบภายใน กับประสิทธิภาพของงานตรวจสอบภายใน

Model	Sum of Squares	df	Mean Square	F	Sig
Regression	43.582	4	10.896	105.350	0.000
Residual	20.167	195	0.103		
Total	63.750	199			

* $p < 0.05$

ตารางที่ 7 ผลการวิเคราะห์ค่าสัมประสิทธิ์การถดถอยของทักษะของผู้ตรวจสอบภายใน การสนับสนุนจากผู้บริหาร การติดตามผลและประเมินผล ความเป็นอิสระของผู้ตรวจสอบภายใน กับประสิทธิภาพของงานตรวจสอบภายใน

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig
	B	Std Error	Beta		
(Constant)	-0.138	0.276		-0.499	0.619
ทักษะของผู้ตรวจสอบภายใน	0.075	0.055	0.055	1.360	0.175
การสนับสนุนจากผู้บริหาร	**0.252**	**0.066**	**0.236**	**3.843**	**0.000**
ความเป็นอิสระของผู้ตรวจสอบภายใน	0.147	0.081	0.123	1.802	0.073
การติดตามและประเมินผล	**0.539**	**0.062**	**0.543**	**8.742**	**0.000**

* $p < 0.05$, $R = 0.827^a$, $R^2 = 0.684$, SE = 0.322

6. สรุปผลการวิจัย

6.1 อภิปรายผลการวิจัย

ผลการวิเคราะห์ข้อมูลพบว่า ปัจจัยที่ส่งผลต่อประสิทธิภาพของงานตรวจสอบภายในอย่างเป็นนัยสำคัญประกอบด้วยการสนับสนุนจากผู้บริหารและการติดตามและประเมินผล ดังนี้

(1) การที่จะทำให้ผู้บริหารระดับสูงให้ความสนใจในประเด็นสำคัญที่หน่วยงานตรวจสอบภายในตรวจพบ มีการนำผลที่ได้รับและคำแนะนำไปปฏิบัติตาม ให้ความสำคัญต่อการพัฒนาขีดความสามารถและความรู้ของพนักงานภายในหน่วยงานตรวจสอบภายใน รวมทั้งให้การสนับสนุนด้านงบประมาณแก่หน่วยงานได้นั้น ผู้ตรวจสอบภายในต้องสามารถส่งมอบคุณภาพของงานตรวจสอบภายในให้ผู้บริหารรับรู้ และเกิดความตระหนักต่อความสำคัญของหน่วยงานตรวจสอบภายในที่มีต่อองค์กร อันจะช่วยสนับสนุนให้หน่วยงานตรวจสอบภายในสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ

(2) การติดตามและประเมินผล เป็นกระบวนการตรวจสอบอย่างต่อเนื่องที่จะช่วยให้ฝ่ายบริหารสามารถทราบว่ากระบวนการปฏิบัติงานนั้นมีประสิทธิภาพและประสิทธิผลเป็นไปตามที่ตั้งใจไว้ ซึ่งหน่วยงานตรวจสอบภายในจะต้องมีกระบวนการที่ใช้ในการติดตามความคืบหน้าของผลการตรวจสอบอย่างต่อเนื่อง มีการประสานงานกับ ผู้รับตรวจเกี่ยวกับความคืบหน้าในการแก้ไขปรับปรุงตามรายงานผลการตรวจสอบ รวมทั้งสามารถช่วยให้ฝ่ายบริหารทราบถึงกระบวนการทางธุรกิจว่ามีการปฏิบัติเป็นไปตามกฎระเบียบ เพื่อให้ความเชื่อมั่นกับผู้บริหารและคณะกรรมการตรวจสอบอย่างเพียงพอว่าการบริหารจัดการความเสี่ยงนั้นเป็นที่พอใจส่งผลต่อประสิทธิภาพของงานตรวจสอบภายใน

6.2 ข้อเสนอแนะในเชิงปฏิบัติ

องค์กรที่ต้องการเพิ่มประสิทธิภาพให้กับหน่วยงานตรวจสอบภายในสามารถนำผลการวิจัยไปปฏิบัติใช้ได้ดังนี้

(1) ผู้ตรวจสอบภายในควรให้ความสำคัญกับการวางแผนการตรวจสอบภายในที่สามารถครอบคลุมกระบวนการทำงานอย่างต่อเนื่องในด้านการติดตามและประเมินผล เพื่อให้สามารถปฏิบัติงานได้บรรลุวัตถุประสงค์และเพิ่มประสิทธิภาพให้กับหน่วยงาน

(2) หน่วยงานตรวจสอบภายในต้องให้ความสำคัญต่อผู้ใช้ข้อมูลจากผลการตรวจสอบ โดยการนำเสนอคุณภาพของงานตรวจสอบภายในเพื่อให้ผู้บริหารเกิดความตระหนักและให้การสนับสนุนอีกด้วย และเพื่อเพิ่มคุณภาพของงานตรวจสอบภายในมากยิ่งขึ้น รวมทั้งส่งผลต่อการรับรู้ของผู้บริหารถึงผลงานและความสำคัญของหน่วยงานตรวจสอบภายใน

6.3 ข้อเสนอแนะสำหรับงานวิจัยต่อเนื่อง

เพื่อให้เกิดประโยชน์ในด้านการสร้างองค์ความรู้ใหม่ ทางผู้วิจัยขอเสนอแนะการทำวิจัยครั้งต่อไป ดังนี้

(1) งานวิจัยนี้ศึกษามุมมองของผู้ตรวจสอบภายในในภาพรวม ไม่ได้แบ่งแยกตามประเภทของงานตรวจสอบภายในออกจากกันอย่างชัดเจน ดังนั้น งานวิจัยต่อเนื่องควรศึกษาในมุมมองของผู้ตรวจสอบภายในโดยแบ่งกลุ่มตัวอย่างของผู้ตรวจสอบภายในตามประเภทของงานตรวจสอบภายใน เช่น การตรวจสอบทางการเงิน (Financial auditing) การตรวจสอบการดำเนินงาน (Performance auditing) การตรวจสอบการปฏิบัติตามข้อกำหนด (Compliance auditing) การตรวจสอบระบบงานสารสนเทศ (Information system auditing) เป็นต้น เพื่อศึกษาปัจจัยเรื่องทักษะของผู้ตรวจสอบภายในที่ส่งผลต่อประสิทธิภาพของงานตรวจสอบภายในแต่ละประเภท

(2) งานวิจัยนี้ไม่ได้แบ่งกลุ่มตัวอย่างตามโครงสร้างการบริหารจัดการของกลุ่มงานตรวจสอบอย่างชัดเจน ดังนั้น งานวิจัยต่อเนื่องควรศึกษามุมมองของผู้ตรวจสอบภายในโดยแบ่งกลุ่มตัวอย่างของผู้ตรวจสอบภายในตามโครงสร้างการบริหารขององค์กร สำหรับกลุ่มที่มีคณะกรรมการตรวจสอบและไม่มีคณะกรรมการตรวจสอบเพื่อศึกษาปัจจัยด้านความเป็นอิสระของผู้ตรวจสอบภายใน

(3) อาจศึกษาปัจจัยในด้านอื่นๆ เช่น ความสามารถในหน้าที่ของผู้ตรวจสอบภายใน (Competence of internal audit) (Dellai & Omri, 2016) วัตถุประสงค์ของงานตรวจสอบภายใน (Objectivity of internal audit) (Dellai & Omri, 2016; Baharud-din et al., 2014) เพิ่มเติมหรืออาจศึกษาปัจจัยในลักษณะงานวิจัยเชิงคุณภาพต่อไป

บรรณานุกรม

สุพิชญา อาชวจิรดา. (2557). *ปัจจัยที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร.* (วิทยาศาตรมหาบัณฑิต). คณะพาณิชยศาสตร์และการบัญชี, มหาวิทยาลัยธรรมศาสตร์.

Alzeban, A., & Gwilliam, D. (2014). Factors affecting the internal audit effectiveness: A survey of the Saudi public sector*, Journal International Accounting Auditing Taxation,* 23(2), 74-86.

Ameeq, A. U., & Hanif, F. (2013). Impact of Traning on Employee's Development and Performance in Hotel Industry of Lahore Pakistan. *Journal of Business Studies Quarterly*, 4(4), 68-82.

Asfaw, A. M., Argaw, M. D., & Bayissa, L. (2015). The Impact of Traning and Development on Employee Performance and Effectiveness: Case Study of District Five Administration Office, Bole Sub-City, Addis Ababa, Ethiopia. *Journal of Human Resource and Sustainability Studies*, 3, 188-202.

Badara, M. S., & Saidin, S. Z. (2014). Empirical Evidence of the Moderating Effect of Effective Audit Committee on Audit Experience in the Public Sector: Perception of Internal Auditors. *Mediterranean Journal of Social Sciences*, 5(10), 176-184.

Baharud-din, Z., Shokiyah, A., & Ibrahim, M. S. (2014). Factors that Contribute to the Effectiveness of Internal Audit in Public Sector. IPDER, 70(24), 126-132.

Chadegani, A. A. (2011). Review of studies on audit quality. *International Conference on Humanities, Society and Culture*, USA, 312-317.

Dahir, A. A. (2016). Effects of Internal Audit Practice on organizational performane of remittance companies in Modadishu-Somalia. *Journal of Business Management,* 2(9), 12-33.

Dellai, H., & Omri, M. A. B. (2016). Factors Affecting the Internal Audit Effectiveness in Tunisian Organizations. *Research Journal of Finance and Accounting*, 7(16), 208-221.

Deloitte Development LLC. (2010). *Continuous monitoring and continuous auditing from idea to implementation*. USA: Deloitte Tohmatsu.

Falola, H. O., Osibanjo, A O., & Ojo, S. I. (2014). Effectiveness of Training and Development on Employees' Performance and Organisation Competitiveness in the Nigerian Banking Industry. *Economic Sciences*, 7(56), 161-170.

Haque, A. & Anwar, S. (2012). Linking Top Managment Support and IT Infrastructure with Organizational Performance: Mediating Role of Knowledge Application. *Canadian Social Science*, 8(1), 121-129.

Hailemariam, S. (2014). *Determinants of internal audit effectiveness in the public sector: Case study in selected Ethiopian Public Sector offices*. Unpublished master degree, Jimma University, Department of Accounting and Finance, Ethiopia.

Heras, E., Canibano, L. & Moreira. (2012), The Impact of the Spanish Financial Act on audit quality. *Revista Espanola de Financiacion y Contabilidad*, October-December, 521-546.

Hung, J. H., & Hair, H. L. (2013). An Empirical Study of Effectiveness of Internal Auditing for Listed Firms in Taiwan. *CiteSeer,* 1-21.

Institute of Internal Auditors. (2013). *The three lines of defense in effective risk management and control*. USA: The institute of internal auditors.

Mahzan, N., & Hassan, N. A. B. (2015). Internal Audit of Quality in 5s Environment: Perception on Critical Factors, Effectiveness and Impact on Organizational Performance. *International Journal Academic Research in Accounting, Finance and Management Sciences,* 5(1), 92-102.

Martin, R. D. (2013). Audit quality indicators: audit practice meets audit research. *Current Issues in Auditing,* 7(2), A17-A23.

Mihret, D. G., & Yismaw, A. W. (2007). Internal audit effectiveness: an Ethiopian public sector case study. *Managerial Auditing Journal,* 22(5), 470-484.

Nassazi, A. (2013). *Effects of Training on Employee Performance Evidence from Uganda.* Unpublished master degree, Vaasan Ammattikorkeakoulu, University of applied sciences, international business.

Onatuyeh, E. A., & Aniefor, S. J. (2013). Impact of effective internal audit functions on public sector management and accountability in Edo State, Nigeria. *International Journal of Economic Development Research and Investment,* 4(3), 91-103.

Shamsuddin, A., & Bharathii, D. (2014). Factors that determine the effectiveness of internal audit functions in the Malaysian Public Sectors. *International Journal of Business*, 5(1), 9-17.

Usman. (2016). Effect of Independence and Competence The Quality Of Internal Audit: Proposing A Research Framwork. *International Journal of Scientific & Technology Research*, 5(2), 221-226.

ปัจจัยที่ส่งเสริมให้พนักงานในองค์กรแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ

อภิญญา รัตนาตรานุรักษ์*
บริษัท อีวาย คอร์ปอเรท เซอร์วิสเซส จำกัด

***Correspondence:** apinya.ara@gmail.com
doi: 10.14456/jisb.2018.15
วันที่รับบทความ: 22 ก.ค. 2560 วันแก้ไขบทความ: 22 ส.ค. 2560 วันตอบรับบทความ: 5 ก.ย. 2560

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ส่งผลต่อการแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศของพนักงานในองค์กร ซึ่งเป็นงานวิจัยเชิงปริมาณ โดยทำการศึกษากลุ่มประชากรที่เป็นพนักงานในองค์กรที่มีนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศภายในองค์กรทั้งภาครัฐและเอกชน จำนวน 229 กลุ่มตัวอย่าง ด้วยวิธีการแจกแบบสอบถามทั้งรูปแบบกระดาษและอิเล็กทรอนิกส์ ผลการวิจัยพบว่า การรับรู้ภัยคุกคาม ความเชื่อในความสามารถของตนเอง การคล้อยตามกลุ่มอ้างอิง ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย การรับรู้ถึงความรับผิดรับชอบ และการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัตินโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศและยังส่งอิทธิพลทางอ้อมต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย หากพนักงานเกิดความตั้งใจที่จะปฏิบัติตามนโยบายและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยแล้วนั้นก็จะส่งผลโดยตรงทำให้เกิดการแสดงออกถึงพฤติกรรมในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศด้วย ทั้งนี้การรับรู้ภัยคุกคามที่เกิดขึ้นของพนักงานมีผลมาจากประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคามด้วยเช่นกัน ส่วนการให้รางวัลและความรู้สึกของการบีบบังคับโดยการลงโทษนั้นไม่ส่งผลกระทบต่อความตั้งใจที่จะปฏิบัติตามนโยบาย เนื่องจากการให้รางวัลและบทลงโทษอาจถูกตีความว่าเป็นเครื่องมือที่ใช้ในการควบคุมพฤติกรรม จึงทำให้พนักงานรู้สึกต่อต้าน และไม่อยากที่จะปฏิบัติตามนโยบาย ซึ่งผู้ที่เกี่ยวข้องหรือผู้ที่ต้องการสร้างสภาพแวดล้อมให้เกิดการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศสามารถนำไปปรับใช้เพื่อควบคุมให้พนักงานแสดงออกถึงพฤติกรรมในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศอย่างเหมาะสม

คำสำคัญ: พฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ความตั้งใจที่จะปฏิบัติตามนโยบาย

Factors affecting the Employees' Behavior towards Information Security Policy Compliance

Apinya Rattanatranurak*

EY Corporate Services Co., Ltd.

***Correspondence:** apinya.ara@gmail.com

doi: 10.14456/jisb.2018.15

Received: 22 Jul 2017 Revised: 22 Aug 2017 Accepted: 5 Sep 2017

Abstract

The objective of this study is to examine the factors influencing behavioral information security policy compliance in employee. This research is quantitative research. The study was collected from 229 Thai participants, who was an employee in organizations with information security policy including both government and private sectors. Data was gathered by printed and online questionnaires. According to the results, this research found that factors - perceived threat, self-efficacy, subjective norms, attitude towards compliance with policy, perceived accountability and security awareness - are directly affect to the intention to information security policy compliance and also indirectly affects to security behavior. If participants intend to follow and aware of the security policy, they will conform to the information security behavior. In addition, participants perceived threat after they had prior experience with safety hazard. However, the results show that reward and perceived of constraint by punishment do not affect to the intention security policy compliance. The reason could be that participants interpreted rewards and punishment as a tool used to control behavior. Thus, the participants feel opposed and do not need to follow the information security policy compliance. This research introduces who involved or make environment to maintain information security can be implemented to control employees' behaviors under proper information security practice.

Keywords: Behavioral information security policy compliance, Security awareness, Intention to compliance policy

1. บทนำ

1.1 ความสำคัญและที่มาของปัญหา

เทคโนโลยีในปัจจุบันมีการเปลี่ยนแปลงไปอย่างรวดเร็ว ส่งผลให้องค์กรต่าง ๆ ต้องปรับตัวให้ทันกับเทคโนโลยีใหม่ ๆ ที่เกิดขึ้น จึงได้นำเทคโนโลยีสารสนเทศมาใช้เป็นพื้นฐานในการเปลี่ยนแปลงรูปแบบทางธุรกิจและกลยุทธ์ทางธุรกิจ (Stanciu & Tinca, 2016) ได้แก่ การจัดหา laptop ให้กับพนักงานได้ใช้พกพาไปทำงานนอกสถานที่ อุปกรณ์สื่อสารที่ทันสมัยขึ้น การใช้สื่อสังคมออนไลน์ (Social media) คลาวด์คอมพิวติ้ง (Cloud computing) หรือแนวคิดของการนำอุปกรณ์สื่อสารส่วนตัวมาใช้ในการทำงาน (Bring your own device: BYOD) เป็นต้น เพื่อที่จะสามารถตอบสนองและสร้างความพึงพอใจให้กับลูกค้าได้อย่างสะดวกและรวดเร็วที่สุด อย่างไรก็ตามการนำเทคโนโลยีมาใช้นั้นส่งผลให้เกิดความเสี่ยงทางธุรกิจจากการไม่ได้คำนึงถึงการรักษาความมั่นคงปลอดภัยของข้อมูลในระดับที่เพียงพอ (PwC, 2014) โดยจากผลการสำรวจของบริษัท PwC ในปี 2015 พบว่า เหตุการณ์การละเมิดการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศเพิ่มสูงขึ้นจากในอดีตถึงร้อยละ 48 และมีแนวโน้มที่จะขยายตัวสูงขึ้น จึงทำให้เทคโนโลยีด้านการรักษาความมั่นคงปลอดภัยกลายเป็นกลยุทธ์ที่สำคัญสำหรับธุรกิจในปัจจุบัน (Zaharia, 2015; PwC, 2015) ซึ่งนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศเป็นวิธีการในการจัดการเรื่องการรักษาความมั่นคงปลอดภัยที่สำคัญที่องค์กรส่วนใหญ่นิยมใช้ โดยจะช่วยให้มั่นใจว่าพนักงานทุกคนเข้าใจบทบาทและความรับผิดชอบของตนเองและทำให้ธุรกิจบรรลุเป้าหมายขององค์กรได้อย่างแท้จริง (Trustwave, 2014) แต่องค์กรอาจเกิดช่องโหว่ที่เป็นอันตรายจากการที่องค์กรมีนโยบายการรักษาความมั่นคงปลอดภัย แต่พฤติกรรมของพนักงานที่เกิดขึ้นจริงไม่ได้ปฏิบัติตามนโยบายเหล่านั้น จึงทำให้องค์กรตกเป็นเป้าหมายของการโจมตีของผู้ไม่ประสงค์ดี และเป็นเหตุให้นำมาซึ่งการสูญเสียทั้งค่าใช้จ่าย เวลา และทรัพยากรอื่น ๆ จำนวนมหาศาล (Jouini & Rabai, 2016) ซึ่งการที่พนักงานไม่ปฏิบัติตามนโยบายหรือมีการปฏิบัติที่บกพร่อง ไม่ครบถ้วน อาจเกิดจากความประมาท ความไม่รู้ หรือการละเลยนโยบายการรักษาความมั่นคงปลอดภัยขององค์กรซึ่งถือเป็นสาเหตุหลักของการละเมิดการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ จนทำให้กลุ่มผู้ใช้ข้อมูลภายใน (Insider) หรือพนักงานภายในองค์กรเป็นต้นเหตุสำคัญที่ทำให้เกิดอาชญากรรมคอมพิวเตอร์มากที่สุด และมีแนวโน้มเพิ่มขึ้นอีกร้อยละ 10 จากที่ผ่านมา (PwC, 2015) ซึ่งตัวเลขนี้เป็นสัญญาณเตือนสำคัญที่องค์กรควรเริ่มตระหนักถึงความสำคัญในการดูแลและส่งเสริมให้พนักงานในองค์กรปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศที่องค์กรกำหนดขึ้น เพราะพนักงานถือเป็นผู้ที่มีความใกล้ชิดและเกี่ยวข้องกับข้อมูลสารสนเทศขององค์กรเป็นอย่างมาก อีกทั้งองค์กรส่วนใหญ่มักให้ความสำคัญกับการป้องกันภัยคุกคามจากภายนอกองค์กร โดยละเลยการปกป้องภัยคุกคามที่เกิดขึ้นจากภายในองค์กรทำให้ในบางครั้งพนักงานสามารถเข้าถึงระบบได้โดยง่ายเพราะองค์กรให้ความไว้วางใจกับพนักงาน (จตุชัย แพงจันทร์, 2550) ทำให้พนักงานในองค์กรเป็นปัจจัยสำคัญที่ส่งผลต่อความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร หากพนักงานในองค์กรปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรอย่างสม่ำเสมอจะเป็นการช่วยให้องค์กรสามารถใช้เทคโนโลยีต่าง ๆ ได้อย่างมีประสิทธิภาพและไม่ต้องกังวลกับปัญหาภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้น

ดังนั้นการศึกษาปัจจัยที่ส่งเสริมให้พนักงานในองค์กรแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศในองค์กรจึงเป็นสิ่งที่จำเป็นอย่างยิ่งที่จะใช้เป็นแนวทางในการเสริมสร้างแรงจูงใจให้พนักงานในองค์กรให้ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยเพื่อให้เกิดความมั่นใจว่าข้อมูลสารสนเทศขององค์กรจะไม่รั่วไหลไปยังคู่แข่งหรือในสถานที่ ๆ ไม่พึงประสงค์ และลดช่องโหว่ที่สำคัญจากการใช้เทคโนโลยีใหม่ ๆ ที่นำมาใช้ภายในองค์กร เพื่อที่จะได้นำเทคโนโลยีมาใช้ให้เกิดประสิทธิภาพสูงสุดแก่องค์กรโดยไม่ก่อให้เกิดความเสียหายต่อข้อมูลสารสนเทศในองค์กร

1.2 วัตถุประสงค์ของการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาถึงปัจจัยต่าง ๆ ที่ส่งผลต่อการแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร ประกอบด้วย ประสบการณ์ก่อนหน้าจากการเผชิญกับ

ภัยคุกคาม การรับรู้ภัยคุกคาม ความเชื่อในความสามารถของตนเอง การคล้อยตามกลุ่มอ้างอิง ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย การรับรู้ถึงความรับผิดรับชอบ การให้รางวัล ความรู้สึกของการบีบบังคับโดยการลงโทษ การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยที่ส่งผลต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัยผ่านความตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

จากการศึกษาทฤษฎีทางจิตวิทยาสังคม (Social psychology) ได้แก่ ทฤษฎีแรงจูงใจเพื่อป้องกันโรค ทฤษฎีพฤติกรรมตามแผน ทฤษฎีความรับผิดรับชอบ ทฤษฎีการข่มขู่ยับยั้งทั่วไป ทฤษฎีการปฏิบัติตาม และงานวิจัยในอดีตที่เกี่ยวข้องสามารถสรุปปัจจัยที่เกี่ยวข้องกับการศึกษาได้ดังนี้

ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคาม (Prior experience with safety hazard) หมายถึง ความรู้หรือการเรียนรู้ที่จะนำไปสู่ความคุ้นเคย ความสามารถ ทักษะและความเข้าใจเหตุการณ์ หรือการเรียนรู้ผ่านทางบุคคลอื่นที่เคยได้พบเจอกับเหตุการณ์หรือเป็นผู้เชี่ยวชาญในด้านที่เกี่ยวข้องกับอันตรายที่เกิดขึ้นกับระบบสารสนเทศขององค์กรของแต่ละบุคคลในอดีต ซึ่งมีส่วนช่วยในการตอบสนองและจัดการกับภัยคุกคามที่อาจเกิดขึ้น (สำนักงานราชบัณฑิตยสภา, 2532; Safa et al., 2016; Tsai et al., 2016)

การรับรู้ภัยคุกคาม (Perceived threats) หมายถึง การที่บุคคลประเมินระดับความเสี่ยงหรือรับรู้ถึงอันตรายจากเหตุการณ์ที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศขององค์กรจาก วัตถุ สิ่งของ หรือตัวบุคคล เพื่อหาวิธีในการปกป้องสารสนเทศขององค์กร ซึ่งประกอบด้วย การรับรู้ช่องโหว่ (perceived vulnerability) การรับรู้ความรุนแรง (perceived severity) และความกลัว (Fear) โดยภัยคุกคามทางด้านสารสนเทศนั้นสามารถสร้างความรู้สึกวิตกกังวลให้กับบุคคลในด้านความมั่นคงปลอดภัย และอาจสร้างความเสียหายกับข้อมูลที่เป็นความลับขององค์กรและทำให้สูญเสียทางด้านการเงินได้ (Liang & Xue, 2010; Ifinedo, 2012; Lee et al., 2016; Chen & Zahedi, 2016)

ความเชื่อในความสามารถของตนเอง (Self-efficacy) หมายถึง การที่บุคคลรับรู้ว่าตนสามารถที่จะตัดสินใจในการใช้ทักษะส่วนบุคคล หรือความรู้ของตนเอง เพื่อปกป้องสารสนเทศในองค์กรจากภัยคุกคามที่จะเข้ามาทำอันตรายได้อย่างเหมาะสม เช่น การใช้รหัสผ่าน การติดตั้งซอฟต์แวร์ป้องกันไวรัส การปิดการใช้ Cookies เป็นต้น (Ifinedo, 2012; Al-Omari et al., 2013)

การคล้อยตามกลุ่มอ้างอิง (Subjective norms) หมายถึง สิ่งที่สะท้อนให้เห็นถึงความเชื่อ การรับรู้ หรือแรงจูงใจของบุคคลที่จะปฏิบัติตามการกระทำหนึ่ง ๆ โดยการกระทำนั้นเป็นที่ยอมรับและได้รับการสนับสนุนจากบุคคลอื่นที่มีความสำคัญต่อบุคคลนั้น ซึ่งอาจมาจากการให้คำปรึกษาหรือสังเกตพฤติกรรมจากผู้อื่น เช่น ครอบครัว เพื่อน ผู้บังคับบัญชา ผู้ใต้บังคับบัญชา เป็นต้น เพื่อนำมาใช้ในการตัดสินใจที่จะปฏิบัติตามในแต่ละบุคคล (Ifinedo, 2012; Hu et al., 2012)

ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย (Attitude towards compliance with policy) หมายถึง การที่บุคคลมีความรู้สึกหรือความคิดทั้งในแง่บวกและแง่ลบต่อการมีส่วนร่วมในการแสดงออกถึงพฤติกรรมที่น่าสนใจ โดยบุคคลสามารถรับรู้ทัศนคติที่มีต่อสิ่ง ๆ หนึ่ง ได้จากสถานที่ บุคคล กิจกรรม หรือสิ่งต่าง ๆ ทั้งนี้ทัศนคติสามารถที่จะเปลี่ยนแปลงได้ผ่านการโน้มน้าวหรือชักจูงผ่านการตอบสนองจากการสื่อสารในหลาย ๆ ทาง เช่น การกำหนดนโยบาย เป็นต้น โดยทัศนคติที่ดีจะทำให้บุคคลมีแนวโน้มในการแสดงพฤติกรรมตามนโยบายมากขึ้น (Ajzen 1991; Fishbein & Ajzen, 1975; Dinev & Hu, 2007; Pahnila et al., 2007; Hu et al., 2012; Ifinedo, 2012; Hepler, 2015)

การรับรู้ถึงความรับผิดรับชอบ (Perceived accountability) หมายถึง การพร้อมรับผิดจากผลของการกระทำที่ส่งผลต่อตนเองและผู้อื่นทั้งในทางบวกและทางลบ เพื่อให้เป็นไปตามมาตรฐานที่กำหนดไว้ ทั้งในส่วนของภาระหน้าที่ ความคาดหวัง และค่าใช้จ่ายอื่น ๆ ซึ่งเป็นสิ่งที่จำเป็นในการดำเนินงานภายในองค์กรอย่างมีประสิทธิภาพ และเป็นการที่บุคคลมีความรู้สึกที่ต้องมีความรับผิดชอบซึ่งออกมาจากจิตสำนึกในการรักษาทรัพย์สินหรือปฏิบัติตามหน้าที่ที่ได้รับ

มอบหมายตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ (Schlenker et al., 1994; Hochwarter et al., 2005; Vance et al., 2015)

การให้รางวัล (Reward) หมายถึง แรงจูงใจที่จำเป็นสำหรับการให้บุคคลปฏิบัติตามสิ่งใด ๆ โดยบุคคลจะรับรู้ถึงความเป็นธรรมที่ได้รับจากผลตอบแทนทั้งที่เป็นตัวเงินและไม่เป็นตัวเงินว่ามีความเหมาะสมกับสิ่งที่ต้องกระทำหรือต้นทุนของบุคคลหรือไม่ และเพิ่มความเชื่อมั่นและความต้องการให้กับบุคคลในการกระทำตามสิ่งที่องค์กรอยากจะให้ปฏิบัติตาม เช่น การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ เป็นต้น (Siponen et al., 2009; Bulgurcu et al., 2010; Cavallari, 2011; Chen et al., 2012)

ความรู้สึกของการบีบบังคับโดยการลงโทษ (Perceived of constraint by punishment) หมายถึง การที่บุคคลรับรู้ถึงมาตรการหรือกฎระเบียบที่ใช้ในการควบคุมพฤติกรรมของบุคคลในองค์กร เพื่อยับยั้งและต่อต้านพฤติกรรมที่เบี่ยงเบน ซึ่งเป็นวิธีการควบคุมให้มีการปฏิบัติตามและทำโทษบุคคลจากการไม่ปฏิบัติตามกฎระเบียบ ได้แก่ การลดตำแหน่งหรืออำนาจลง การถูกตำหนิหรือเสื่อมเสียชื่อเสียง การถูกหักเงินเดือน เป็นต้น ทั้งนี้การลงโทษจะต้องเกิดขึ้นอย่างรวดเร็ว สม่ำเสมอ และมีระดับความรุนแรงเพียงพอที่จะทำให้บุคคลเหล่านั้นไม่ฝ่าฝืนกฎระเบียบและยอมที่จะปฏิบัติตามกฎระเบียบ (Straub, 1990; Peace et al., 2003; Son, 2011; Chen et al., 2012)

การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย (Security awareness) หมายถึง การที่บุคคลรับรู้ มีสติต่อเหตุการณ์หรือทางความคิดอย่างใดอย่างหนึ่งที่เกิดขึ้น โดยนำมาซึ่งการตอบสนองทั้งในเชิงบวกและเชิงลบ ซึ่งพนักงานต้องมีความรู้ทั่วไปและความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ โดยพนักงานต้องเข้าใจเกี่ยวกับปัญหาที่อาจจะเกิดขึ้นหากไม่มีการปฏิบัติตาม รวมถึงความต้องการและจุดมุ่งหมายที่ถูกกำหนดไว้ในนโยบายการรักษาความมั่นคงปลอดภัย เพื่อให้บรรลุวัตถุประสงค์ของการรักษาความมั่นคงปลอดภัยขององค์กร (Siponen, 2000; Bulgurcu et. al., 2010; Cavallari, 2011; สุพิชญา อาชวจริดา, 2557)

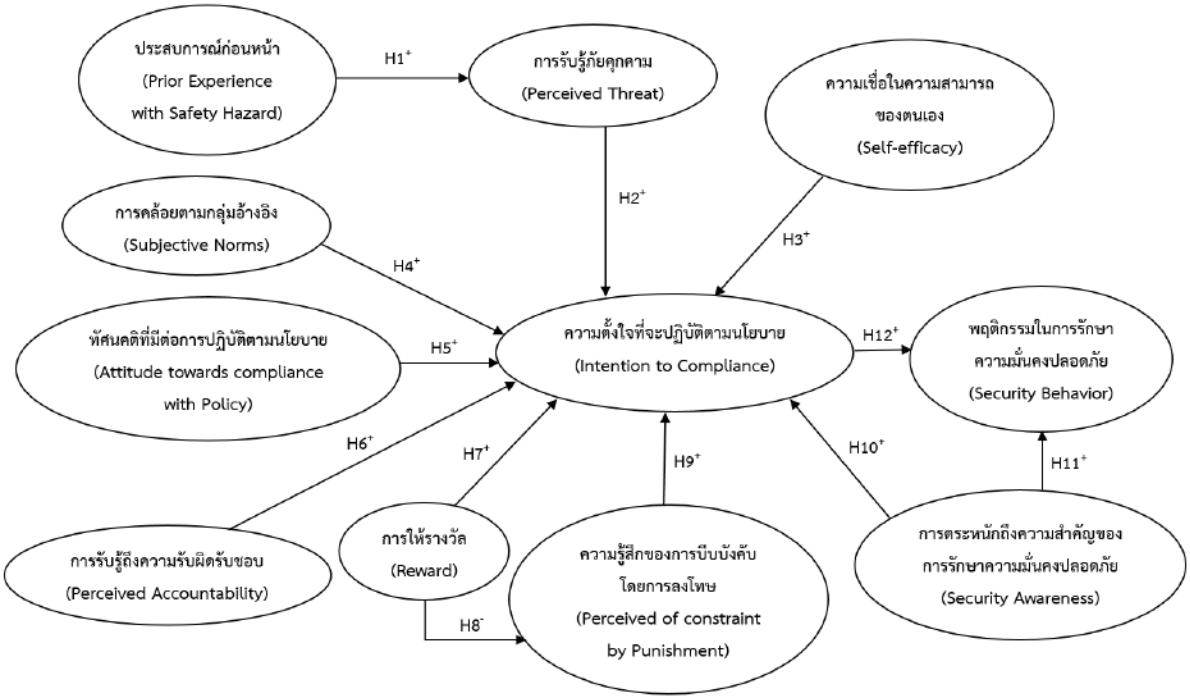
ความตั้งใจที่จะปฏิบัติตามนโยบาย (Intention to compliance) หมายถึง เจตนาหรือความพร้อมของแต่ละบุคคลที่จะแสดงออกถึงพฤติกรรมใดพฤติกรรมหนึ่ง ซึ่งถือเป็นความตั้งใจของพนักงานในการปกป้องเทคโนโลยีสารสนเทศขององค์กรและทรัพยากรขององค์กรจากการละเมิดความมั่นคงปลอดภัยจากการใช้งานที่อาจเกิดขึ้น โดยพร้อมที่จะแสดงออกถึงพฤติกรรมอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร (Chan et al., 2005; Herath & Rao, 2009; Bulgurcu et al., 2010; Son, 2011; Ifinedo, 2012)

พฤติกรรมในการรักษาความมั่นคงปลอดภัย (Security behavior) หมายถึง การกระทำที่แสดงออกเพื่อตอบสนองต่อสิ่งแวดล้อมและเสริมสร้างความมั่นใจของแต่ละบุคคลในการที่จะปกป้องเทคโนโลยีสารสนเทศจากการละเมิดนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศได้อย่างมีประสิทธิภาพและสม่ำเสมอ โดยมีการใช้เครื่องมือหรือเพียงปฏิบัติตามกฎระเบียบที่องค์กรได้กำหนดเอาไว้ และหลีกเลี่ยงความเสี่ยงจากพฤติกรรมที่ไม่พึงประสงค์อันจะก่อให้เกิดความเสียหายทางด้านข้อมูลสารสนเทศขององค์กรขึ้น เช่น การเปิดไฟล์เอกสารหรือโปรแกรมที่น่าสงสัย การไม่เข้ารหัสผ่านหรือไม่ทำตามข้อกำหนดเกี่ยวกับการใช้รหัสผ่านเบื้องต้น เป็นต้น (Siponen et al., 2007; Siponen et al., 2010; Merriam-Webster Online Dictionary, 2010; Bulgurcu et al., 2010; Kaur & Mustafa, 2013; Hanus & Wu, 2016)

3. กรอบแนวคิดการวิจัยและสมมติฐานการวิจัย

การวิจัยนี้ได้ประยุกต์ใช้ทฤษฎีพฤติกรรมตามแผน ทฤษฎีแรงจูงใจเพื่อป้องกันโรค ทฤษฎีความรับผิดรับชอบ ทฤษฎีการปฏิบัติตาม ทฤษฎีการข่มขู่ยับยั้งทั่วไป โมเดลความรู้ ทัศนคติและพฤติกรรมและงานวิจัยในอดีตที่เกี่ยวข้อง ประกอบด้วยปัจจัยการรับรู้ภัยคุกคาม ความเชื่อในความสามารถของตนเอง การคล้อยตามกลุ่มอ้างอิง ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย ความตั้งใจที่จะปฏิบัติตามนโยบาย และพฤติกรรมในการรักษาความมั่นคงปลอดภัย กับปัจจัยใหม่อีก 4 ปัจจัยซึ่งงานวิจัยนี้เพิ่มเข้ามา คือ ปัจจัยการรับรู้ถึงความรับผิดรับชอบ การให้รางวัล ความรู้สึกของการบีบ

บังคับโดยการลงโทษ และประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคาม เพื่อใช้เป็นกรอบการศึกษาเพื่อหาคำตอบของการวิจัยดังแสดงในภาพที่ 1



ภาพที่ 1 กรอบแนวคิดการวิจัยเพื่อการแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบาย
การรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศของพนักงานในองค์กร

Albrechtsen (2007) กล่าวว่า การขาดประสบการณ์ก่อนหน้าและความรู้ในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศของผู้ใช้งานยังคงเป็นปัญหาหลักในเรื่องของบทบาทและหน้าที่ที่ผู้ใช้ควรทราบในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ เนื่องจากการมีประสบการณ์ก่อนหน้าจะมีส่วนช่วยในการสร้างการรับรู้ถึงอันตรายที่อาจเกิดขึ้นและสร้างพฤติกรรมที่เหมาะสมในการรับมือกับสภาพแวดล้อมที่เกิดขึ้นจริงและมีการเปลี่ยนแปลงอยู่ตลอดเวลา ซึ่งสอดคล้องกับแนวคิดของ Lee et al. (2008) ที่กล่าวว่า เมื่อบุคคลมีประสบการณ์ก่อนหน้าจากการเผชิญหน้ากับภัยคุกคาม เช่น การติดไวรัสในคอมพิวเตอร์ บุคคลจะมีแนวโน้มที่จะรับรู้ถึงความรุนแรงของภัยคุกคามที่เกิดขึ้นและมีความตั้งใจที่จะหาวิธีป้องกันและรับมือกับภัยคุกคามที่เกิดขึ้นเพื่อไม่ให้ส่งผลกระทบร้ายแรงต่อองค์กร ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H1: ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคามส่งผลทางบวกต่อการรับรู้ภัยคุกคาม

Ifinedo (2012) กล่าวว่า การรับรู้ภัยคุกคามที่เกิดขึ้นเป็นการที่บุคคลประเมินภัยคุกคามที่อาจเกิดขึ้นจากการรักษาความมั่นคงปลอดภัยและอันตรายที่เกิดจากการไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ ซึ่งจะประเมินผลกระทบที่เกิดจากภัยคุกคามและความน่าจะเป็นที่ภัยคุกคามนั้นจะเกิดขึ้น โดยสอดคล้องกับแนวคิดของ Herath and Rao (2009) ที่กล่าวว่า หากพนักงานรับรู้ถึงภัยคุกคามด้านการรักษาความมั่นคงปลอดภัยและทราบว่าภัยคุกคามนั้นสามารถสร้างความเสียหายหรือรบกวนต่อการทำงานอย่างมีนัยสำคัญ บุคคลจะเริ่มมีความกังวลและมีแนวโน้มที่จะตั้งใจมีส่วนร่วมในกิจกรรมการรักษาความมั่นคงปลอดภัย เช่น นโยบายการรักษาความปลอดภัยทางด้านสารสนเทศภายในองค์กร ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H2: การรับรู้ภัยคุกคามส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

Bandura (1980) กล่าวว่า บุคคลจะประเมินความสามารถของตนเองและกำหนดทางเลือกในสิ่งที่ตนสามารถทำได้ขึ้นมาและพยายามที่จะทำให้สอดคล้องกับสิ่งที่ได้เลือกไว้ และ Stajkovic and Luthans (1988) ได้ประเมินเกี่ยวกับบทบาทของความเชื่อในความสามารถของตนเองกับพฤติกรรมในองค์กรในหลาย ๆ งานวิจัย ทำให้สรุปได้ว่า ความเชื่อในความสามารถของตนเองและสมรรถนะในการปฏิบัติงานที่เกี่ยวข้องกันมีความสัมพันธ์กันอย่างมาก ซึ่งสอดคล้องกับแนวคิดของ Herath and Rao (2009) ที่กล่าวว่า หากพนักงานมีความเชื่อว่าตนมีความสามารถที่จะทำตามนโยบายการรักษาความมั่นคงปลอดภัยได้ พนักงานก็จะมีแนวโน้มที่จะมีความรู้สึกในเชิงบวกมากขึ้นต่อนโยบายและยังมีแนวโน้มที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยเหล่านั้นด้วย ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H3: ความเชื่อในความสามารถของตนเองส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

Venkatesh et al. (2003) และ Ifinedo (2014) กล่าวว่า การคล้อยตามกลุ่มอ้างอิงเป็นการรับรู้ถึงแรงกดดันทางสังคมที่มีผลต่อการกระทำพฤติกรรมนั้น ๆ โดยความตั้งใจของบุคคลในการแสดงออกถึงพฤติกรรมต่าง ๆ ได้รับอิทธิพลจากความคาดหวัง การให้คำปรึกษาหรือการสังเกตพฤติกรรมของบุคคลอื่นที่กระทำเป็นเรื่องปกติในสภาพแวดล้อมของบุคคลนั้น ซึ่งสอดคล้องกับแนวคิดของ Cheng et al. (2013), Chan et al. (2005) และ Herath and Rao (2009) ที่กล่าวว่า หากพนักงานได้รับแรงกดดัน แรงจูงใจหรือการสังเกตเห็นการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรจากบุคคลที่มีอิทธิพลต่อพนักงาน ได้แก่ ผู้บังคับบัญชา เพื่อนร่วมงาน ผู้ใต้บังคับบัญชา หรือได้รับความคาดหวังจากองค์กรแล้วนั้น พนักงานจะมีมุมมองเชิงบวกและมีแนวโน้มที่จะมีความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H4: การคล้อยตามกลุ่มอ้างอิงส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

Karahanna et al. (1999) กล่าวว่า ทัศนคติของพนักงานต่อการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศเป็นการประเมินว่าหากพนักงานปฏิบัติหรือไม่ปฏิบัติตามพฤติกรรรมดังกล่าวจะนำไปสู่ผลกระทบต่อตนเองอย่างไรบ้าง เช่น ทำให้เกิดค่าใช้จ่ายหรือผลประโยชน์ที่ตามมาหรือไม่ โดยหากพนักงานมีทัศนคติที่ดีต่อการเปลี่ยนแปลงพฤติกรรมจะทำให้เกิดแรงผลักดันมากกว่าการต่อต้านการปฏิบัติตามนโยบายซึ่งนำไปสู่ความตั้งใจที่จะปฏิบัติตามนโยบายในที่สุด ทั้งนี้ Bulgurcu et al. (2010) ได้กล่าวว่า การเพิ่มการรับรู้ด้านการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศของพนักงานเป็นส่วนสำคัญที่ทำให้เกิดทัศนคติในเชิงบวกต่อการปฏิบัติตามนโยบาย ได้แก่ การสื่อสาร ฝึกอบรมหรือชี้แจงพนักงานเกี่ยวกับนโยบายที่มีการบังคับใช้ภายในองค์กร เพื่อให้พนักงานรับทราบและทำความเข้าใจเกี่ยวกับนโยบายดังกล่าว เมื่อพนักงานมีความรู้ความเข้าใจเกี่ยวกับนโยบายแล้วนั้น จะส่งผลให้พนักงานมีทัศนคติที่ดีต่อการปฏิบัติตามนโยบาย ซึ่งสอดคล้องกับแนวคิดของ Ifinedo (2014) ที่กล่าวว่า หากพนักงานมีความเชื่อและทัศนคติในเชิงบวกเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรแล้วนั้น จะมีแนวโน้มที่ดีในการปฏิบัติตามกฎระเบียบและแนวทางดังกล่าว ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H5: ทัศนคติที่มีต่อการปฏิบัติตามนโยบายส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

Vance et al. (2015) กล่าวว่า ความรับผิดรับชอบเป็นการรับรู้ถึงภาระหน้าที่ที่ต้องทำจากจิตสำนึกของบุคคลในการตัดสินใจกระทำสิ่งต่าง ๆ พร้อมรับผิดชอบผลลัพธ์จากการกระทำที่ตามมาทั้งในทางบวกหรือทางลบ ดังนั้นหาก

พนักงานมีความรู้สึกถึงการเป็นเจ้าของสิ่งที่ได้รับมอบหมายมานั้น พนักงานจะรู้สึกว่าสิ่งที่ได้รับมอบหมายเป็นสิ่งที่ตนต้องทำและรับผิดชอบ เพื่อให้ตนได้รับการยกย่องจากบุคคลอื่นในองค์กร และหากมีภัยคุกคามหรือสิ่งที่อาจจะเป็นอันตราย พนักงานจะรับรู้ถึงความรับผิดรับชอบในการรักษาทรัพย์สินหรือมีความตั้งใจที่จะปฏิบัติตามหน้าที่ที่ได้รับมอบหมายเสมือนทุกสิ่งที่ได้รับมานั้นเป็นของตน ซึ่งทำให้พนักงานยอมปรับเปลี่ยนพฤติกรรมให้มีการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศขององค์กร ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H6: การรับรู้ถึงความรับผิดรับชอบส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

Boss et al. (2009) กล่าวว่า การให้รางวัลเป็นการสร้างแรงจูงใจให้กับพนักงานที่ทำงานหรือมีพฤติกรรมที่ตอบสนองต่อความคาดหวังขององค์กร หรือเป็นสิ่งที่สามารถใช้แทนสัญญาที่องค์กรนำไปใช้ในการควบคุมการทำงานหรือการปฏิบัติตามกฎระเบียบของพนักงานภายในองค์กร โดยผ่านการให้รางวัลที่ไม่มีตัวตน เช่น การเลื่อนตำแหน่ง รางวัลพนักงานดีเด่นประจำเดือน เป็นต้น และการให้รางวัลที่มีตัวตน เช่น โบนัส หรือวันหยุด เป็นต้น การใช้วิธีการให้รางวัลอย่างเหมาะสมจะเป็นวิธีการควบคุมพฤติกรรมและประสิทธิภาพในการทำงานของพนักงานในองค์กรได้เป็นอย่างดี ได้แก่ การกำกับดูแลพฤติกรรมของพนักงาน การสร้างแรงจูงใจให้แก่พนักงาน การดึงดูดและรักษาความสามารถของพนักงาน อีกทั้งยังเพิ่มความพึงพอใจในการทำงานในตำแหน่งงานให้กับพนักงานด้วย ซึ่งสอดคล้องกับแนวคิดของ Bulgurcu et al. (2010) ที่กล่าวว่า การให้รางวัลสามารถช่วยในการบังคับให้พนักงานมีความตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศได้ หากพนักงานรับรู้ว่าได้รับสิ่งตอบแทนที่เหมาะสม ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H7: การให้รางวัลส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

Chen et al. (2012) กล่าวว่า การควบคุมให้ปฏิบัติตามกฎระเบียบขององค์กรนั้น หลายองค์กรมักจะไม่ค่อยมีการควบคุมโดยการบีบบังคับหรือการควบคุมโดยการให้รางวัลเพียงอย่างใดอย่างหนึ่ง แต่จะใช้การควบคุมทั้งสองอย่างควบคู่กันในการควบคุมเพื่อเพิ่มการปฏิบัติตามของพนักงานในองค์กร เนื่องจากการบีบบังคับโดยการลงโทษหรือการให้รางวัลเพียงอย่างเดียวถือว่าเป็นปัจจัยที่มีอิทธิพลน้อยหรือไม่มีเลยในการให้ความร่วมมือของบุคคลในองค์กร แต่หากนำมาใช้ร่วมกันกลับมีผลกระทบอย่างมีนัยสำคัญในการบังคับใช้นโยบายซึ่งมีความสัมพันธ์กันอย่างมาก ซึ่งสอดคล้องกับแนวคิดของ Greitemeyer and Weiner (2008) ที่พบว่า ผลกระทบของการลงโทษขึ้นอยู่กับการให้รางวัล ซึ่งแสดงให้เห็นว่าการให้รางวัลและความรู้สึกของการบีบบังคับโดยการลงโทษไม่สมมาตรกัน เมื่อมีการให้รางวัลแก่บุคคลเพื่อเป็นแรงจูงใจให้มีการปฏิบัติตาม บุคคลจะมีการปฏิบัติตามมากกว่าการปฏิบัติตามเนื่องจากการถูกบีบบังคับโดยการลงโทษ เพราะการลงโทษจะถูกตีความจากพนักงานว่าเป็นการข่มขู่ ดังนั้นเพื่อให้การต่อต้านลดลง จึงควรที่จะมีการให้รางวัลเพื่อลดการตอบโต้หรือปฏิกิริยาต่อต้านทางอารมณ์ลง ซึ่งจะเห็นได้ว่าการให้รางวัลมีผลต่อการเปลี่ยนแปลงของความรู้สึกจากการถูกบีบบังคับโดยการลงโทษ ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H8: การให้รางวัลส่งผลทางลบต่อความรู้สึกของการบีบบังคับโดยการลงโทษ

Straub (1990) และ D'Arcy and Herath (2011) กล่าวว่า การลงโทษเป็นกลไกการยับยั้งและต่อต้านพฤติกรรมที่ไม่พึงประสงค์ เมื่อบุคคลทราบว่าองค์กรมีการควบคุมพฤติกรรมที่ไม่พึงประสงค์ ก็จะมีโอกาสน้อยลงที่จะกระทำความผิด การลงโทษมีตัวชี้วัดหลักอยู่ 3 องค์ประกอบ ประกอบด้วย ความรวดเร็วของการลงโทษ ความรุนแรงของการลงโทษและความสม่ำเสมอของการลงโทษ รวมถึงการรับรู้ถึงความเสี่ยงและค่าใช้จ่ายของการลงโทษ เพื่อช่วยบุคคลใน

การตัดสินใจว่าจะแสดงพฤติกรรมอย่างไร ซึ่งสอดคล้องกับแนวคิดของ Peace et al. (2003) ที่กล่าวว่า เมื่อพนักงานรับรู้ถึงบทลงโทษที่รุนแรง รวดเร็วและสม่ำเสมอแล้วนั้น พนักงานจะเกิดความรู้สึกถูกบีบบังคับให้ไม่ปฏิบัติตามในพฤติกรรมที่ไม่พึงประสงค์ต่อองค์กร และมีแนวโน้มที่จะหันมาตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ เพื่อหลีกเลี่ยงการถูกลงโทษ ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H9: ความรู้สึกของการบีบบังคับโดยการลงโทษส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

Siponen (2000) กล่าวว่า การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศเป็นความรู้สึกนึกคิดของพนักงานที่รับรู้ถึงความสำคัญและเข้าใจถึงวัตถุประสงค์ของการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ ความเสี่ยงและภัยคุกคาม และแสวงหาความรู้ที่จำเป็นเกี่ยวกับหน้าที่ความรับผิดชอบในระบบสารสนเทศที่เกี่ยวข้อง ซึ่งสิ่งเหล่านี้เป็นส่วนสำคัญที่จะทำให้การรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศมีประสิทธิภาพมากขึ้น ทั้งนี้ Bulgurcu et al. (2010) กล่าวว่า การที่จะทำให้พนักงานในองค์กรปฏิบัติตามนโยบายที่จัดทำขึ้นนั้น ต้องทำให้เข้าใจง่ายและสามารถเข้าถึงได้ทุกที่ทุกเวลาที่พนักงานต้องการ ซึ่งสอดคล้องกับแนวคิดของ Dinev and Hu (2007) และ Haeussinger and Kranz (2013) ที่กล่าวว่า พนักงานจะมีการรับรู้และตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นและภัยคุกคามที่เป็นอันตรายจากการใช้เทคโนโลยีสารสนเทศในองค์กร เมื่อพนักงานมีความรู้และเข้าใจในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศมากขึ้น พนักงานจะมีแนวโน้มที่จะหาวิธีป้องกันโดยเกิดความตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศมากขึ้น ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H10: การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย

พฤติกรรมเป็นสิ่งที่เกิดจากการตระหนักโดยตรง ซึ่งการตระหนักถึงนั้นจะนำไปสู่พฤติกรรมที่ควรปฏิบัติ หากจะทำให้การตระหนักมีประสิทธิภาพนั้นต้องได้รับการสนับสนุนจากพนักงานและผู้มีส่วนได้เสียทุกคนที่ทำงานภายในองค์กร ซึ่งสอดคล้องกับแนวคิดของ Dinev and Hu (2007), D'Arcy et al. (2009) และ Bulgurcu et al. (2010) ที่กล่าวว่า หากบุคคลมีการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศแล้วนั้น ย่อมส่งผลให้บุคคลนั้นมีแนวโน้มที่จะแสดงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศด้วย ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H11: การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งผลทางบวกต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย

Shropshire et al. (2015) กล่าวว่า ความตั้งใจที่จะแสดงพฤติกรรมเป็นสิ่งที่ชี้วัดหรือทำนายการแสดงออกถึงพฤติกรรมที่แท้จริงทางด้านเทคโนโลยีสารสนเทศ โดยจากงานวิจัยต่าง ๆ ที่ทำการศึกษาในเรื่องนี้ได้ยอมรับว่า ความตั้งใจที่จะปฏิบัติตามนโยบายเป็นการที่บุคคลมีแรงจูงใจที่จะปกป้องทรัพย์สินทางด้านสารสนเทศขององค์กรจากภัยคุกคามต่างๆ ด้วยเครื่องมือที่องค์กรจัดทำขึ้น ได้แก่ นโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ ซึ่งส่งผลให้บุคคลนั้นเกิดความรู้สึกที่ดีและตั้งใจที่จะปฏิบัติตามนโยบายนั้น บุคคลก็จะมีแนวโน้มที่จะแสดงออกถึงพฤติกรรมการรักษาความปลอดภัยทางด้านสารสนเทศ ซึ่งสอดคล้องกับแนวคิดของ Yoon et al. (2012) ที่กล่าวว่า หากพนักงานมีความตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศแล้วนั้น พนักงาน

ก็จะมีแนวโน้มที่จะแสดงออกถึงพฤติกรรมในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศด้วย ดังนั้นจึงสามารถตั้งสมมติฐานได้ว่า

H12: ความตั้งใจที่จะปฏิบัติตามนโยบายส่งผลทางบวกต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย

4. วิธีการวิจัย

งานวิจัยนี้จัดเก็บข้อมูลจากกลุ่มตัวอย่างที่เป็นพนักงานในองค์กรทั้งภาครัฐบาลและภาคเอกชน โดยองค์กรดังกล่าวจะต้องมีนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ (Information security policy) จำนวน 229 กลุ่มตัวอย่าง ด้วยแบบสอบถามทั้งในรูปแบบกระดาษและอิเล็กทรอนิกส์ ซึ่งจัดสร้างขึ้นมาจากการค้นคว้าข้อมูลทางเอกสารและงานวิจัยที่เกี่ยวข้อง (ประกอบด้วย Tsai et al., 2016; Safa et al., 2016; Liang and Xue, 2010; Chen and Zahedi, 2016; Ifinedo, 2012; Lee et al., 2016; Al-Omari et al., 2013; Hu et al., 2012; Dinev and Hu, 2007; Hochwarter et al., 2005; Vance et al., 2015; Chen et al., 2012; Bulgurcu et al., 2010; Siponen et al., 2009; Cavallari, 2011; Peace et al., 2003; Son, 2011; Hanus and Wu, 2016; Siponen et al., 2007; Kaur and Mustafa, 2013; Siponen et al., 2010) นำไปทดสอบกับกลุ่มตัวอย่าง จำนวน 22 คน เพื่อวิเคราะห์แบบสอบถามเบื้องต้นและปรับปรุงข้อคำถามในแบบสอบถามให้มีความเหมาะสมก่อนนำไปจัดเก็บข้อมูลจริง โดยแจกแบบสอบถามอิเล็กทรอนิกส์ผ่านสื่อสังคมออนไลน์ และเริ่มจัดส่งแบบสอบถามตั้งแต่ต้นเดือนพฤษภาคมจนถึงสิ้นเดือนพฤษภาคม พ.ศ. 2560 พบว่า มีผู้ตอบแบบสอบถามไม่ครบตามจำนวนที่ต้องการ จึงแจกแบบสอบถามในรูปแบบกระดาษด้วยการส่งผ่านคนรู้จักที่ทำงานในองค์กรต่าง ๆ ที่มีนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ จนถึงวันที่ 10 มิถุนายน พ.ศ. 2560 รวมระยะเวลาในการจัดเก็บข้อมูลประมาณ 1 เดือน

5. ผลการวิจัย

5.1 การทดสอบข้อตกลงเบื้องต้นทางสถิติ

ข้อมูลที่จัดเก็บจากกลุ่มตัวอย่างถูกนำไปทดสอบข้อมูลขาดหาย (Missing data) ข้อมูลสุดโต่ง (Outliners) การกระจายแบบปกติ (Normal) ความสัมพันธ์เชิงเส้นตรง (Linearity) ภาวะร่วมเส้นตรงพหุ (Multicollinearity) และภาวะร่วมเส้นตรง (Singularity) ซึ่งจากการทดสอบพบว่า ข้อมูลไม่มีส่วนใดขาดหาย มีความสัมพันธ์เชิงเส้นตรง และไม่มีปัญหาภาวะร่วมเส้นตรงพหุและภาวะร่วมเส้นตรง ซึ่งถือว่าผ่านเกณฑ์ตามที่กำหนดทั้งหมด มีเพียงบางตัวแปรเท่านั้นที่ไม่ได้มีการกระจายแบบปกติ โดยมีการกระจายข้อมูลแบบเบ้ซ้าย แต่มีความเบ้ต่างจากเกณฑ์มาตรฐานไม่มากนัก ทางผู้วิจัยจึงยังคงใช้ข้อมูลดังกล่าววิเคราะห์ข้อมูลทางสถิติต่อไป

5.2 การประเมินความเที่ยงและความตรงของแบบสอบถาม

งานวิจัยนี้ทดสอบความเชื่อถือได้ของแบบสอบถาม โดยใช้การทดสอบความเที่ยงของแบบสอบถาม (Reliability) จากการวิเคราะห์ค่าประสิทธิ์แอลฟาของครอนบาซ (Cronbach's alpha) ที่มีค่ามากกว่า 0.70 ซึ่งถือว่ามีความเชื่อถือได้สำหรับงานวิจัยแบบ Basic research และได้ทดสอบความตรงของแบบสอบถาม (Validity) ด้วยการวิเคราะห์องค์ประกอบ (Factor analysis) โดยต้องมีค่าน้ำหนักองค์ประกอบ (Factor loading) มากกว่า 0.5 (สุพิชญา อาชวจิรดา, 2557) ดังแสดงค่าสถิติของแต่ละข้อคำถามที่ผ่านเกณฑ์ตามตารางที่ 1

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัย 1: ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคาม (% of variance = 83.222, Cronbach's alpha = 0.896)			
ท่านสามารถประเมินได้ว่าเหตุการณ์ใดเป็นภัยคุกคาม โดยใช้ประสบการณ์ของท่าน	3.900	0.6444	0.929
ท่านเชื่อว่าท่านสามารถใช้ประสบการณ์ที่ผ่านมาเพื่อจัดการกับเหตุการณ์ที่ท่านรู้สึกว่าจะเป็นภัยอันตรายต่อความมั่นคงปลอดภัยทางสารสนเทศที่อาจเกิดขึ้นในปัจจุบัน	3.917	0.5902	0.920
การเผชิญกับภัยคุกคามมาแล้ว ทำให้ท่านมีความระมัดระวังและช่วยทำให้ท่านหาวิธีป้องกันได้ง่ายขึ้น	4.083	0.6800	0.887
ปัจจัย 2: การรับรู้ภัยคุกคาม (% of variance = 52.212, Cronbach's alpha = 0.757)			
ท่านเชื่อว่าการพยายามที่จะปกป้องข้อมูลสารสนเทศขององค์กร จะช่วยลดการเข้าถึงที่ไม่ได้รับอนุญาตได้	3.860	0.6473	0.837
ท่านกังวลว่า ข้อมูลสารสนเทศและทรัพยากรขององค์กรจะได้รับความเสียหายจากการถูกบุกรุกที่เกิดจากช่องโหว่ของระบบสารสนเทศ	3.926	0.5687	0.780
ท่านมีความกังวลว่า ท่านจะตกเป็นเหยื่อและเกิดความสูญเสียจากการโจมตีที่เป็นอันตรายต่อความมั่นคงปลอดภัยทางด้านสารสนเทศ จากการใช้งานคอมพิวเตอร์ที่ไม่ถูกวิธีของท่าน	3.812	0.6975	0.748
หากคอมพิวเตอร์ของท่านติดไวรัส สปายแวร์ ท่านมีความรู้สึกเสี่ยงและไม่สบายใจในการใช้คอมพิวเตอร์ของท่าน	3.786	0.6899	0.687
ท่านเชื่อว่า องค์กรของท่านอาจเกิดความเสี่ยงต่อระบบสารสนเทศ เมื่อท่านฝ่าฝืนกฎระเบียบที่องค์กรกำหนด	3.965	0.7000	0.521

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด (ต่อ)

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัย 3: ความเชื่อในความสามารถของตนเอง (% of variance = 67.335, Cronbach's alpha = 0.879)			
ท่านมีทักษะในการใช้มาตรการป้องกันเพื่อหยุดผู้ที่จะเข้ามาโจมตีคอมพิวเตอร์ที่ท่านใช้ในการทำงาน เช่น การติดตั้งซอฟต์แวร์ป้องกันไวรัส การใช้รหัสผ่านอย่างเหมาะสม การปิดการใช้ cookies เป็นต้น	3.511	0.8915	0.863
การใช้งานโปรแกรมต่าง ๆ ทางด้านการรักษาความมั่นคงปลอดภัยบนคอมพิวเตอร์ที่ใช้ในการทำงานเป็นเรื่องง่ายสำหรับท่าน	3.563	0.8438	0.843
ท่านเชื่อว่า ท่านสามารถที่จะควบคุมและป้องกันตนเองจากการโจมตีระบบสารสนเทศขององค์กรได้	3.541	0.8399	0.809
ท่านเชื่อว่า ท่านมีทักษะที่เพียงพอสำหรับจัดการกับภัยคุกคาม ต่าง ๆ ที่องค์กรต้องจำกัดได้	3.389	0.7735	0.800
ท่านมีความเชี่ยวชาญในการดำเนินการตามมาตรการป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลที่เป็นความลับของท่านได้	3.371	0.7987	0.786
ปัจจัย 4: การคล้อยตามกลุ่มอ้างอิง (% of variance = 68.235, Cronbach's alpha = 0.878)			
ท่านทำในสิ่งที่เพื่อนร่วมงานของท่านคิดว่าท่านควรจะทำ	3.886	0.6249	0.900
ท่านทำในสิ่งที่ผู้บังคับบัญชาของท่านคิดว่าท่านควรจะทำ	4.017	0.5995	0.877
ท่านทำในสิ่งที่ผู้ใต้บังคับบัญชาของท่านคิดว่าท่านควรจะทำ	3.825	0.6590	0.862
ท่านทำในสิ่งที่แผนกเทคโนโลยีสารสนเทศขององค์กรของท่านคิดว่าท่านควรจะทำ	4.004	0.6589	0.799
ท่านมีแนวโน้มที่จะทำตามพฤติกรรมที่บุคคลที่มีอิทธิพลและมีความสำคัญกับท่านแสดงออกมา	3.782	0.6724	0.672

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด (ต่อ)

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัย 5: ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย (% of variance = 76.347, Cronbach's alpha = 0.922)			
ท่านเชื่อว่า การกำหนดนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศที่ชัดเจนขององค์กร จะเป็นประโยชน์ต่อการปฏิบัติตามและการใช้เทคโนโลยีของท่าน	4.293	0.6191	0.778
ท่านเชื่อว่า การบังคับใช้นโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ จะเป็นประโยชน์ต่อการปฏิบัติตามและการใช้เทคโนโลยีของท่าน	4.223	0.6270	0.768
ท่านคิดว่า การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศเป็นความคิดที่ดี	4.367	0.6254	0.770
ท่านคิดว่า การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศเป็นสิ่งที่จำเป็น	4.362	0.6520	0.784
สำหรับท่านแล้ว การจำกัดและปกป้องเครื่องคอมพิวเตอร์จากสปายแวร์หรือ ไวรัส เป็นความคิดที่ดี	4.393	0.6092	0.718
ปัจจัย 6: การรับรู้ถึงความรับผิดรับชอบ (% of variance = 53.632, Cronbach's alpha = 0.710)			
ท่านคิดว่า การใช้งานระบบสารสนเทศขององค์กรอย่างระมัดระวัง คือสิ่งที่ท่านควรทำ	4.371	0.6670	0.775
ท่านมีส่วนสำคัญในการทำให้เกิดความสำเร็จหรือความล้มเหลวของงานที่ได้รับมอบหมาย	3.978	0.6451	0.757
ท่านคิดว่า ท่านสามารถดูแลและรักษาทรัพย์สินในองค์กรของท่านเสมือนกับเป็นทรัพย์สินของท่านเอง	4.170	0.6700	0.752
องค์กรของท่านให้ท่านรับผิดชอบต่อการกระทำทั้งหมดของท่านในการใช้งานระบบสารสนเทศขององค์กร	3.716	0.6302	0.637
ปัจจัย 7: การให้รางวัล (% of variance = 59.711, Cronbach's alpha = 0.864)			
เมื่อท่านทำตามกฎระเบียบที่องค์กรกำหนด ท่านจะได้รับการ ชื่นชม	3.590	0.7707	0.802
เมื่อท่านทำตามสิ่งที่องค์กรต้องการ ท่านจะได้รับรางวัลที่เป็นตัวเงิน เช่น การขึ้นเงินเดือน เป็นต้น	3.555	0.8444	0.790
เมื่อท่านกระทำสิ่งที่เป็นประโยชน์หรือสร้างชื่อเสียงให้กับองค์กร ท่านจะได้รับรางวัลจากองค์กร เช่น เลื่อนตำแหน่ง รางวัลพนักงานดีเด่น เป็นต้น	3.690	0.8403	0.787

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด (ต่อ)

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัย 7: การให้รางวัล (ต่อ)			
ท่านรู้สึกว่า รางวัลทำให้ท่านเต็มใจที่จะทำสิ่งใด ๆ มากกว่าการถูกบีบบังคับให้ทำสิ่งนั้น	3.769	0.8903	0.785
เมื่อท่านทำตามสิ่งที่องค์กรต้องการ ท่านจะได้รับรางวัลที่ไม่เป็นตัวเงิน เช่น คำชมเชย ชื่อเสียง เป็นต้น	3.537	0.7693	0.772
ท่านคิดว่า องค์กรมีการให้รางวัลกับท่านอย่างเหมาะสม เมื่อเปรียบเทียบกับสิ่งที่ท่านกระทำ	3.402	0.8085	0.696
ปัจจัย 8: ความรู้สึกของการบีบบังคับโดยการลงโทษ (% of variance = 59.128, Cronbach's alpha = 0.826)			
เมื่อท่านไม่ทำในสิ่งที่กำหนดไว้ในกฎระเบียบขององค์กร ท่านมีแนวโน้มที่จะได้รับการลงโทษ	3.821	0.6807	0.849
องค์กรของท่านจะลงโทษบุคคลที่นำทรัพยากรทางคอมพิวเตอร์ขององค์กรไปใช้เพื่อประโยชน์ส่วนตัว	3.852	0.6785	0.773
ผู้บังคับบัญชาของท่านจะว่ากล่าวตักเตือนหรือกระทำการใด ๆ ซึ่งแสดงให้เห็นถึงความเข้มงวดในกฎระเบียบที่องค์กรกำหนดขึ้น	3.882	0.5990	0.772
หากท่านฝ่าฝืนกฎระเบียบที่องค์กรกำหนดและถูกจับได้ ท่านจะได้รับการลงโทษอย่างรุนแรงทันที	3.939	0.5966	0.722
ท่านรู้สึกว่า การลงโทษเป็นปัญหาใหญ่สำหรับท่าน	3.943	0.6361	0.722
ปัจจัย 9: การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย (% of variance = 69.032, Cronbach's alpha = 0.887)			
ท่านรู้และเข้าใจเหตุผลว่าทำไมองค์กรของท่านต้องมีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ	4.437	0.6567	0.873
ท่านรู้ว่าท่านต้องรับผิดชอบตามที่กำหนดในนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรของท่าน เพื่อเพิ่มการรักษาความมั่นคงปลอดภัยขององค์กรของท่าน	4.362	0.6587	0.860
ท่านทราบเกี่ยวกับผลกระทบที่ตามมาจากการที่ท่านไม่ปฏิบัติตามระเบียบที่องค์กรกำหนด	4.249	0.6908	0.845
เมื่อท่านเข้าใช้งานระบบสารสนเทศขององค์กร ท่านจะคิดถึงกฎระเบียบและข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยเสมอ	4.297	0.6616	0.823
การปกป้องข้อมูลของลูกค้า พนักงาน และคู่ค้า มีความสำคัญมากสำหรับองค์กรของท่าน	4.607	0.6020	0.747

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าประสิทธิ์แอลฟา ของครอนบาซของตัวแปรทั้งหมด (ต่อ)

ปัจจัย	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัย 10: ความตั้งใจที่จะปฏิบัติตามนโยบาย (% of variance = 76.508, Cronbach's alpha = 0.923)			
ท่านตั้งใจที่จะทำหน้าที่ของท่านตามที่ได้กำหนดไว้ในนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรของท่าน เมื่อท่านใช้ข้อมูลสารสนเทศและเทคโนโลยีในอนาคต	4.293	0.6400	0.909
ท่านตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรของท่านในอนาคต	4.288	0.6176	0.881
ท่านตั้งใจที่จะปกป้องข้อมูลสารสนเทศและทรัพยากรทางด้านเทคโนโลยีตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรของท่านในอนาคต	4.332	0.6310	0.877
ท่านมั่นใจว่า ท่านจะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร เมื่อเป็นไปได้	4.271	0.6113	0.861
สำหรับท่านแล้ว การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศอย่างต่อเนื่องเป็นความตั้งใจของท่าน	4.227	0.6495	0.845
ปัจจัย 11: พฤติกรรมในการรักษาความมั่นคงปลอดภัย (% of variance = 61.074, Cronbach's alpha = 0.832)			
ท่านปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศทุกครั้ง เมื่อท่านทำงานประจำวัน	4.192	0.7180	0.851
ท่านมีพฤติกรรมในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศตามที่นโยบายขององค์กรแนะนำ มากเท่าที่จะเป็นไปได้	4.205	0.7296	0.815
ท่านแนะนำและช่วยเหลือให้ผู้อื่นในองค์กร ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศเช่นเดียวกับท่าน	3.882	0.8579	0.805
ท่านมีโปรแกรมสแกนไวรัสติดตั้งไว้ที่เครื่องคอมพิวเตอร์ของท่าน และมีการอัปเดตอยู่ตลอดเวลา	4.192	0.9213	0.725
ท่านจะไม่เปิดอ่านไฟล์เอกสารที่แนบมากับอีเมล หากเนื้อหาในอีเมลนั้นดูน่าสงสัย	4.258	0.8319	0.701

5.3 ลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่าง

กลุ่มตัวอย่างส่วนใหญ่เป็นเพศหญิงมากกว่าเพศชาย (ร้อยละ 63.80) โดยอยู่ในช่วงอายุ 26-30 ปี (ร้อยละ 45.40) ระดับการศึกษาสูงสุดอยู่ในระดับปริญญาตรีและทำงานในองค์กรด้านธุรกิจบริการ (ร้อยละ 17.00) และธุรกิจการเงินและการธนาคาร (ร้อยละ 14.90) ทั้งนี้อายุการทำงานในหน่วยงานยังอยู่ในช่วงน้อยกว่า 3 ปี (ร้อยละ 36.20) ระดับความรู้เกี่ยวกับคอมพิวเตอร์และเทคโนโลยีอยู่ในระดับปานกลาง (ร้อยละ 53.30) ทั้งนี้องค์กรของกลุ่มตัวอย่างยังมีการให้ยืมเครื่องคอมพิวเตอร์พกพา (Laptop) หรืออนุญาตให้ใช้อุปกรณ์ Smart device ส่วนบุคคลในการทำงานด้วย (ร้อยละ 79.50)

5.4 การทดสอบสมมติฐานการวิจัย

งานวิจัยนี้ทดสอบสมมติฐานการวิจัยจากกรอบแนวคิดการวิจัยด้วยการวิเคราะห์การถดถอยแบบเชิงชั้น (Hierarchical regression) ผลลัพธ์ที่ได้แสดงในภาพที่ 2 และตารางที่ 2 โดยใช้ค่า p-value ที่น้อยกว่าหรือเท่ากับ 0.05 เป็นตัวกำหนดนัยสำคัญทางสถิติ ซึ่งแสดงคะแนนมาตรฐาน (Standardized score) โดยสามารถวิเคราะห์ผลทางสถิติได้ดังนี้

5.4.1 ความรู้สึกของการบีบบังคับโดยการลงโทษ ผลทางสถิติแสดงให้เห็นว่า การให้รางวัลส่งอิทธิพลทางตรงต่อความรู้สึกของการบีบบังคับโดยการลงโทษ ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.135 และมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 1.8 (R^2 = 0.018) ซึ่งจากการวิเคราะห์ข้อมูลพบว่า การให้รางวัลไม่สนับสนุนสมมติฐานการวิจัยที่ 8 ที่กล่าวว่า การให้รางวัลส่งผลทางลบต่อความรู้สึกของการบีบบังคับโดยการลงโทษ เนื่องจากค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายบวก ซึ่งมีทิศทางตรงกันข้ามกับสมมติฐานการวิจัยที่ตั้งไว้ โดยอาจมีสาเหตุจากบริบทของกลุ่มตัวอย่างในองค์กรของไทยมักจะปฏิเสธหรือหลีกเลี่ยงความเป็นจริง เพื่อให้ตนเองปลอดภัยและลดความเสี่ยงที่อาจเกิดขึ้น เพราะคำถามเกี่ยวกับเรื่องการให้รางวัลและความรู้สึกของการบีบบังคับโดยการลงโทษค่อนข้างเป็นเรื่องลึกซึ้งในความคิดของคนไทย ที่จะไม่ยอมให้ความไม่แน่นอนหรือภัยเกิดขึ้นกับตนเองและพยายามที่จะหาทางลดความไม่แน่นอนหรือความเสี่ยงที่เกิดขึ้นกับตน จึงอาจทำให้มีการตอบไม่ตรงกับความเป็นจริงทั้งหมด (สุธีรา เดชนครินทร์ และ สุธินี ฤกษ์ขำ, 2558) จึงส่งผลให้ข้อมูลที่ได้ไม่สนับสนุนสมมติฐานดังกล่าว

5.4.2 การรับรู้ภัยคุกคาม ผลทางสถิติแสดงให้เห็นว่า ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคามส่งอิทธิพลทางตรงต่อการรับรู้ภัยคุกคาม ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.272 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 7.4 (R^2 = 0.074) ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 1 ที่กล่าวว่า ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคามส่งผลทางบวกต่อการรับรู้ภัยคุกคาม ซึ่งสอดคล้องกับงานวิจัยของ Albrechtsen (2007) และ Lee et al. (2008) ที่กล่าวว่า ประสบการณ์ก่อนหน้าจะเกิดจากความคุ้นเคยหรือการรับรู้ถึงเหตุการณ์หรือภัยคุกคามที่เกิดขึ้นจากการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศในอดีตของแต่ละบุคคล ซึ่งมีส่วนช่วยในการตอบสนองและรับรู้ถึงภัยคุกคามที่เกิดขึ้น ทั้งนี้จะมีความตั้งใจที่จะพยายามจัดการ หาทางป้องกันและลดความเสี่ยงจากภัยคุกคามที่อาจเกิดขึ้น เพื่อไม่ให้ส่งผลกระทบร้ายแรงต่อองค์กร

5.4.3 ความตั้งใจที่จะปฏิบัติตามนโยบาย ผลทางสถิติแสดงให้เห็นว่า การรับรู้ภัยคุกคาม ความเชื่อในความสามารถของตนเอง การคล้อยตามกลุ่มอ้างอิง ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย การรับรู้ถึงความรับผิดรับชอบ การให้รางวัล ความรู้สึกของการบีบบังคับโดยการลงโทษ การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย และประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคาม ส่งอิทธิพลต่อความตั้งใจที่จะปฏิบัติตามนโยบาย โดยมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 65.70 (R^2 = 0.657) รายละเอียดของอิทธิพลแต่ละปัจจัยมีดังนี้

5.4.3.1 การรับรู้ภัยคุกคาม ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบายที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.228 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 2 ที่กล่าวว่า การรับรู้ภัยคุกคามส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งสอดคล้องกับงานวิจัยของ Ifinedo (2012); Herath and Rao (2009) และ Yoon et al. (2012) ที่กล่าวว่า การรับรู้ภัยคุกคามทางด้านความปลอดภัยจะเกิดขึ้น เมื่อบุคคลมีการประเมินภัยคุกคามและอันตรายจากการไม่ปฏิบัติตามหรือรับรู้ช่องโหว่ที่เกิดขึ้น จะทำให้บุคคลมีความตั้งใจที่จะมีส่วนร่วมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ

5.4.3.2 ความเชื่อในความสามารถของตนเอง ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.138 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 3 ที่กล่าวว่า ความเชื่อในความสามารถของตนเองส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งสอดคล้องกับงานวิจัยของ Stajkovic and Luthans (1988) และ Herath and Rao (2009) ที่กล่าวว่า ความเชื่อในความสามารถของตนเองได้รับการแสดงให้เป็นปัจจัยที่มีผลกระทบต่อการใช้งานด้านเทคโนโลยีสารสนเทศด้วย หากบุคคลมีความมั่นใจ

ว่าตนมีทักษะและความสามารถเพียงพอในการดำเนินกิจกรรมต่างๆ บุคคลก็จะมีแนวโน้มที่จะตั้งใจที่จะกระทำกิจกรรมต่างๆ นั้น

5.4.3.3 การคล้อยตามกลุ่มอ้างอิง ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.155 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 4 ที่กล่าวว่า การคล้อยตามกลุ่มอ้างอิงส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งสอดคล้องกับงานวิจัยของ Pahnila et al. (2007); Herath and Rao (2009); Bulgurcu et al. (2010) และ Ifinedo (2014) ที่กล่าวว่า การคล้อยตามกลุ่มอ้างอิงเป็นที่ยอมรับกันอย่างกว้างขวางในการทบทวนวรรณกรรมที่เกี่ยวข้องกับความตั้งใจที่จะแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศอย่างมีนัยสำคัญ เมื่อพนักงานได้เห็นหรือรับรู้ว่าบุคคลรอบข้างหรือมีความใกล้ชิดมีการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ พนักงานเหล่านี้ก็มีแนวโน้มที่จะปฏิบัติตามด้วย

5.4.3.4 ทัศนคติที่มีต่อการปฏิบัตินโยบาย ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.121 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 5 ที่กล่าวว่า ทัศนคติที่มีต่อการปฏิบัติตามนโยบายส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งสอดคล้องกับงานวิจัยของ Bulgurcu et al. (2010) และ Ifinedo (2014) ที่กล่าวว่า หากพนักงานมีความเชื่อและทัศนคติในเชิงบวกเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กรแล้วนั้น ก็จะมีแนวโน้มที่ดีในการปฏิบัติตามกฎระเบียบและแนวทางดังกล่าว

5.4.3.5 การรับรู้ถึงความรับผิดรับชอบ ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.193 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 6 ที่กล่าวว่า การรับรู้ถึงความรับผิดรับชอบส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งสอดคล้องกับงานวิจัยของ Vance et al. (2015) ที่กล่าวว่า หากพนักงานมีความรับผิดรับชอบเพิ่มขึ้นจะทำให้พนักงานลดความคิดที่จะละเมิดนโยบายฯ และหันมามีความตั้งใจที่จะปฏิบัติตามนโยบายเพิ่มขึ้น ซึ่งแสดงให้เห็นถึงการรับรู้ถึงความรับผิดรับชอบต่อการปฏิบัติตามนโยบายนั้น

5.4.3.6 การให้รางวัล ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.123 และส่งอิทธิพลทางอ้อมผ่านความรู้สึกของการบีบบังคับโดยการลงโทษไปยังความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.026 จากการวิเคราะห์ข้อมูลพบว่า การให้รางวัลไม่สนับสนุนสมมติฐานการวิจัยที่ 7 ที่กล่าวว่า การให้รางวัลส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย เนื่องจากค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายลบ ซึ่งมีทิศทางตรงกันข้ามกับสมมติฐานการวิจัยที่ตั้งไว้ อาจมีสาเหตุเนื่องจากกลุ่มตัวอย่างตีความว่าการให้รางวัลเป็นเสมือนเครื่องมือในการควบคุมพฤติกรรมและรู้สึกว่าได้รับสิ่งตอบแทนไม่คุ้มค่ากับสิ่งที่ตนจะต้องปฏิบัติตาม

5.4.3.7 ความรู้สึกของการบีบบังคับโดยการลงโทษ ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.195 จากการวิเคราะห์ข้อมูลพบว่า ความรู้สึกของการบีบบังคับโดยการลงโทษไม่สนับสนุนสมมติฐานการวิจัยที่ 9 ที่กล่าวว่า ความรู้สึกของการบีบบังคับโดยการลงโทษส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย เนื่องจากค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายลบ ซึ่งมีทิศทางตรงกันข้ามกับสมมติฐานการวิจัยที่ตั้งไว้ โดยอาจมีสาเหตุมาจากการวัดความรู้สึกของการบีบบังคับโดยการลงโทษเป็นเรื่องที่วัดค่อนข้างยากในบริบทของกลุ่มตัวอย่างองค์กรในประเทศไทยซึ่งพนักงานส่วนใหญ่ไม่มีการรับรู้ถึงบทลงโทษอย่างแน่ชัด ว่าหากตนกระทำความผิด ไม่ปฏิบัติตามหรือละเมิดนโยบายฯ แล้วนั้น จะส่งผลอย่างไรต่อตนเองบ้าง และรูปแบบการลงโทษที่รุนแรงอาจไม่ก่อให้เกิดความกลัวต่อผู้ใช้งานระบบสารสนเทศ แต่อาจเป็นการเพิ่มความรู้สึกต่อต้านของบุคคล จนนำไปสู่การไม่สนใจที่จะปฏิบัติตามนโยบายด้วย ซึ่งสอดคล้องกับงานวิจัยของ Herath and Rao (2009) ที่พบว่า ในการศึกษางานวิจัยต่างๆ ที่มีปัจจัยเรื่องของการยับยั้งการละเมิดนโยบายฯ โดยการลงโทษนั้น มีผลการวิจัยที่

แตกต่างกันออกไป ซึ่งมีทั้งทางบวกและทางลบ โดยสามารถชี้ให้เห็นว่า การลงโทษอาจไม่จำเป็นต้องรุนแรง แต่องค์กรควรควบคุมพนักงานโดยการติดตั้งระบบควบคุมในคอมพิวเตอร์ เพื่อเป็นการเฝ้าระวังและชดเชยการควบคุมด้วยวิธีการสังเกตการณ์หรือการสอบถามจะเหมาะสมกว่า

5.4.3.8 การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.474 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 10 ที่กล่าวว่า การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งผลทางบวกต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งสอดคล้องกับงานวิจัยของ Dinev and Hu (2007), Bulgurcu et al. (2010) และ Haeussinger and Kranz (2013) ที่กล่าวว่า การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของพนักงานเป็นส่วนสำคัญที่จะทำให้การจัดการเกี่ยวกับการรักษาความมั่นคงปลอดภัยมีประสิทธิภาพ

5.4.3.9 ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคาม ส่งอิทธิพลทางอ้อมผ่านการรับรู้ภัยคุกคามไปยังความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.062 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4 พฤติกรรมในการรักษาความมั่นคงปลอดภัย ผลทางสถิติแสดงให้เห็นว่า การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ความตั้งใจที่จะปฏิบัติตามนโยบาย การรับรู้ภัยคุกคาม ความเชื่อในความสามารถของตนเอง การคล้อยตามกลุ่มอ้างอิง ทัศนคติที่มีต่อการปฏิบัตินโยบาย การรับรู้ถึงความรับผิดรับชอบ การให้รางวัล ความรู้สึกของการบีบบังคับโดยการลงโทษ ส่งอิทธิพลต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย โดยมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 36.40 (R^2 = 0.364) รายละเอียดของอิทธิพลแต่ละปัจจัยมีดังนี้

5.4.4.1 การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ส่งอิทธิพลทางตรงต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.283 และส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.175 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 11 ที่กล่าวว่า การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งผลทางบวกต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย ซึ่งสอดคล้องกับงานวิจัยของ Bulgurcu et al. (2010) ที่กล่าวว่า พฤติกรรมเป็นสิ่งที่เกิดจากการตระหนักโดยตรง ซึ่งการตระหนักถึงนั้นจะนำไปสู่พฤติกรรมที่ควรปฏิบัติตาม

5.4.4.2 ความตั้งใจที่จะปฏิบัติตามนโยบาย ส่งอิทธิพลทางตรงต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.369 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 12 ที่กล่าวว่า ความตั้งใจที่จะปฏิบัติตามนโยบายส่งผลทางบวกต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย ซึ่งสอดคล้องกับงานวิจัยของ Yoon et al. (2012) ที่กล่าวว่า พนักงานที่มีความตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ จะมีแนวโน้มที่จะแสดงออกถึงพฤติกรรมในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศด้วย

5.4.4.3 การรับรู้ภัยคุกคาม ส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.084 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.4 ความเชื่อในความสามารถของตนเอง ส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.051 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

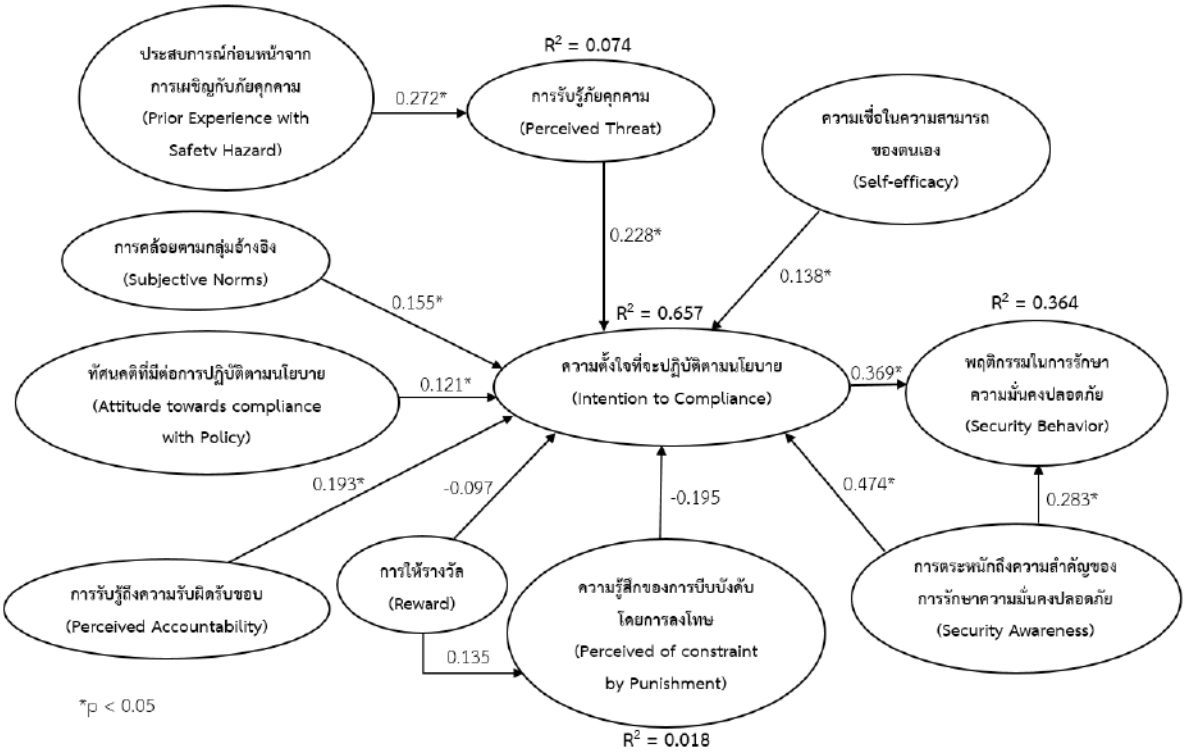
5.4.4.5 การคล้อยตามกลุ่มอ้างอิง ส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.057 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.6 ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย ส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.045 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.7 การรับรู้ถึงความรับผิดรับชอบ ส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.071 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.8 การให้รางวัล ส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.036 โดยค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายลบ

5.4.4.9 ความรู้สึกของการบีบบังคับโดยการลงโทษ ส่งอิทธิพลทางอ้อมผ่านความตั้งใจที่จะปฏิบัติตามนโยบายไปยังพฤติกรรมในการรักษาความมั่นคงปลอดภัย ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.072 โดยค่าสัมประสิทธิ์อิทธิพลมีเครื่องหมายลบ



ภาพที่ 2 ผลการวิเคราะห์กรอบแนวคิดการวิจัยเพื่อการแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศของพนักงานในองค์กร

ตารางที่ 2 ค่าสัมประสิทธิ์อิทธิพลทางตรง ทางอ้อม และอิทธิพลโดยรวมของตัวแปรแฝงในกรอบแนวคิดการวิจัย (แสดงเป็นคะแนนมาตรฐาน)

ตัวแปรตาม	R^2	อิทธิพล	ตัวแปรอิสระ									
			ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคาม	การรับรู้ภัยคุกคาม	ความเชื่อในความสามารถของตนเอง	การคล้อยตามกลุ่มอ้างอิง	ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย	การรับรู้ถึงความรับผิดชอบ	การให้รางวัล	ความรู้สึกของการบีบบังคับโดยการลงโทษ	การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย	ความตั้งใจที่จะปฏิบัติตามนโยบาย
พฤติกรรมในการรักษาความมั่นคงปลอดภัย	0.364	ทางตรง	-	-	-	-	-	-	-	-	0.283*	0.369*
		ทางอ้อม	-	0.084*	0.051*	0.057*	0.045*	0.071*	-0.036	-0.072	0.175*	-
		โดยรวม	-	0.084*	0.051*	0.057*	0.045*	0.071*	-0.036	-0.072	0.458*	0.369*
ความตั้งใจที่จะปฏิบัติตามนโยบาย	0.657	ทางตรง	-	0.228*	0.138*	0.155*	0.121*	0.193*	-0.097	-0.195	0.474*	-
		ทางอ้อม	0.062*	-	-	-	-	-	-0.026	-	-	-
		โดยรวม	0.062*	0.228*	0.138*	0.155*	0.121*	0.193*	-0.123	-0.195	0.474*	-
การรับรู้ภัยคุกคาม	0.074	ทางตรง	0.272*	-	-	-	-	-	-	-	-	-
		ทางอ้อม	-	-	-	-	-	-	-	-	-	-
		โดยรวม	0.272*	-	-	-	-	-	-	-	-	-
ความรู้สึกของการบีบบังคับโดยการลงโทษ	0.018	ทางตรง	-	-	-	-	-	-	0.135	-	-	-
		ทางอ้อม	-	-	-	-	-	-	-	-	-	-
		โดยรวม	-	-	-	-	-	-	0.135	-	-	-

* $p < 0.05$

6. สรุปผลการวิจัย

6.1 อภิปรายผลการวิจัย

ผลการวิเคราะห์ข้อมูลพบว่า ปัจจัยที่ส่งผลต่อการแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศของพนักงานในองค์กรมากที่สุด ประกอบด้วย ความตั้งใจที่จะปฏิบัติตามนโยบายการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย การรับรู้ภัยคุกคาม การรับรู้ถึงความรับผิดรับชอบการคล้อยตามกลุ่มอ้างอิง ความเชื่อในความสามารถของตนเอง ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย ตามลำดับ ซึ่งแสดงให้เห็นว่า กรอบแนวคิดพฤติกรรมในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศมีความสอดคล้องกับข้อมูลเชิงประจักษ์ ดังนี้

(1) ประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคามส่งผลต่อการรับรู้ภัยคุกคาม กล่าวคือ หากพนักงานในองค์กรเคยมีประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคามมาแล้วนั้น จะช่วยให้รับรู้ถึงภัยคุกคามที่อาจจะเกิดขึ้นและหาวิธีป้องกันและรับมือกับภัยคุกคาม เพื่อไม่ให้ส่งผลกระทบร้ายแรงต่อองค์กรได้ ซึ่งเป็นไปตามผลการวิจัยของ Lee at al. (2008)

(2) การรับรู้ภัยคุกคาม ความเชื่อในความสามารถของตนเอง การคล้อยตามกลุ่มอ้างอิง ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย การรับรู้ถึงความรับผิดรับชอบ และการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งผลต่อความตั้งใจที่จะปฏิบัติตามนโยบาย กล่าวคือ หากองค์กรต้องการให้พนักงานในองค์กรมีความตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศแล้ว องค์กรต้องส่งเสริมปัจจัยดังกล่าวข้างต้น เพื่อกระตุ้นและเป็นแรงจูงใจให้พนักงานในองค์กรเกิดความตั้งใจที่จะปฏิบัติตามนโยบาย ซึ่งเป็นไปตามผลการวิจัยของ Ifinedo (2012) และ Vance et al. (2015)

(3) ความตั้งใจที่จะปฏิบัติตามนโยบายและการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งผลต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัย กล่าวคือ หากพนักงานรับรู้และตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นและภัยคุกคามที่เป็นอันตรายจากการใช้เทคโนโลยีสารสนเทศในองค์กร ย่อมส่งผลให้มีแนวโน้มที่จะมีความตั้งใจในการปฏิบัติตามนโยบาย โดยเมื่อพนักงานเกิดความตั้งใจที่จะแสดงออกถึงพฤติกรรมแล้วก็จะแสดงออกพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศออกมา ซึ่งเป็นไปตามผลการวิจัยของ Bulgurcu et al. (2010) และ Shropshire et al. (2015)

นอกจากนี้ผลการวิเคราะห์ข้อมูลครั้งนี้ พบว่า ความสัมพันธ์ระหว่างปัจจัยการให้รางวัลและความรู้สึกของการบีบบังคับโดยการลงโทษที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบาย และความสัมพันธ์ระหว่างปัจจัยการให้รางวัลที่ส่งผลต่อความรู้สึกของการบีบบังคับโดยการลงโทษ ไม่มีความสอดคล้องกับข้อมูลเชิงประจักษ์ กล่าวคือ ปัจจัยการให้รางวัล ปัจจัยความรู้สึกของการบีบบังคับโดยการลงโทษ และปัจจัยความตั้งใจที่จะปฏิบัติตามนโยบาย มีความสัมพันธ์ในทิศทางตรงกันข้ามกับสมมติฐานการวิจัยที่ตั้งไว้ สาเหตุอาจมาจาก การให้รางวัลอาจเกิดผลกระทบในเชิงลบได้ เมื่อการให้รางวัลถูกตีความว่าเป็นเครื่องมือในการควบคุมพฤติกรรม เช่นเดียวกับความรู้สึกของการบีบบังคับโดยการลงโทษ ที่อาจมีสาเหตุมาจากการลงโทษอย่างรุนแรงอาจทำให้พนักงานรู้สึกต่อต้าน และไม่อยากที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ ตามผลการวิจัยของ Herath and Rao (2009) จึงส่งผลให้ข้อมูลที่ได้ไม่สนับสนุนสมมติฐานดังกล่าว

6.2 ข้อเสนอแนะในเชิงปฏิบัติ

ผู้ที่เกี่ยวข้องหรือผู้ที่ต้องการสร้างบรรยากาศให้เกิดการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศสามารถนำผลการวิจัยไปใช้เพื่อควบคุมให้พนักงานแสดงออกถึงพฤติกรรมในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศอย่างเหมาะสม ดังนี้

(1) องค์กรต้องจัดให้มีการฝึกอบรมและให้ความรู้เกี่ยวกับภัยคุกคาม วิธีรับมือหรือป้องกันภัยคุกคามที่อาจจะเกิดขึ้นกับระบบสารสนเทศขององค์กร และต้องมีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศที่ชัดเจน เพื่อสร้างประสบการณ์ การรับรู้ ทัศนคติที่ดีต่อการปฏิบัติตามนโยบายและทำให้พนักงานรู้สึกว่าตนสามารถที่จะรับมือกับภัยคุกคามที่อาจเกิดขึ้นกับระบบสารสนเทศขององค์กรในกรณีต่าง ๆ

(2) องค์กรต้องให้บุคคลที่มีความสำคัญกับพนักงานกระทำให้ดูเป็นแบบอย่าง เพื่อทำให้พนักงานคล้อยตามพฤติกรรมของบุคคลรอบข้าง ได้แก่ เพื่อนร่วมงาน ผู้บังคับบัญชา และผู้ใต้บังคับบัญชา ซึ่งเป็นสิ่งสำคัญที่องค์กรควรนำไปใช้ เมื่อมีการปลูกฝังหรือมีการปฏิบัติตามอย่างทั่วถึงทั้งองค์กร จะทำให้พนักงานรู้สึกถึงความรับผิดชอบในหน้าที่ที่ตนเองควรทำและคล้อยตามการกระทำที่บุคคลรอบข้างแสดงออกมา

(3) องค์กรต้องมีการแจ้งหรือประกาศให้พนักงานรับทราบว่า การกระทำทุกอย่างของพนักงานที่เกี่ยวข้องกับระบบสารสนเทศขององค์กรถือเป็นความรับผิดชอบของพนักงานด้วย ซึ่งอาจมีผลทำให้ระบบสารสนเทศขององค์กรเกิดโอกาสเสี่ยงจากภัยคุกคาม ซึ่งจะทำให้พนักงานมีความระมัดระวังในการใช้งานระบบสารสนเทศเพราะกลัวผลกระทบที่จะเกิดขึ้น

(4) องค์กรต้องสร้างการตระหนักถึงการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศในองค์กร โดยอาจต้องมีการสร้างความเข้าใจ เหตุผลและประโยชน์ที่จะได้รับในการปฏิบัติตามนโยบาย ซึ่งต้องมีการย้ำเตือนพนักงานอยู่เสมอ โดยอาจใช้การเผยแพร่ความรู้ผ่านช่องทางต่าง ๆ ขององค์กร เช่น การติดป้ายประกาศ การแจ้งข้อมูลข่าวสารผ่านอีเมลหรือแจ้งเตือนผ่านคอมพิวเตอร์ เพื่อให้พนักงานเคยชินและหันมาปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยอย่างเป็นประจำ

6.3 ข้อเสนอแนะสำหรับงานวิจัยต่อเนื่อง

เพื่อประโยชน์ในด้านการสร้างองค์ความรู้ใหม่ ทางผู้วิจัยจึงขอเสนอแนะการทำวิจัยครั้งต่อไป ดังต่อไปนี้

(1) การวิจัยครั้งนี้ พบว่า ผู้ตอบแบบสอบถามส่วนใหญ่อยู่ในช่วงอายุ 26-30 ปี ซึ่งความคิดและแรงจูงใจที่ส่งผลต่อการแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยอาจแตกต่างจากองค์กรที่มีพนักงานอาวุโสเป็นจำนวนมาก จึงขอเสนอแนะงานวิจัยต่อเนื่องว่าควรศึกษาเกี่ยวกับปัจจัยที่เสริมสร้างให้พนักงานแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศในแต่ละกลุ่มช่วงอายุ

(2) การวิจัยครั้งนี้ พบว่า ปัจจัยการให้รางวัลและปัจจัยความรู้สึกของการบีบบังคับโดยการลงโทษที่มีผลต่อความตั้งใจที่จะปฏิบัติตาม ไม่สนับสนุนสมมติฐานการวิจัยในครั้งนี้ เนื่องจากบริบทของกลุ่มตัวอย่างอาจตอบแบบปฏิเสธความเป็นจริงเพื่อหลีกเลี่ยงความเสี่ยงที่อาจเกิดขึ้นกับตนเอง และจากการศึกษางานวิจัยในอดีต ปรากฏว่าให้ข้อสรุปที่แตกต่างกันมีทั้งสนับสนุนและไม่สนับสนุนความสัมพันธ์ดังกล่าว ดังนั้นงานวิจัยต่อเนื่องจึงควรศึกษาปัจจัยการให้รางวัลและปัจจัยความรู้สึกของการบีบบังคับโดยการลงโทษโดยเปรียบเทียบกันระหว่างองค์กรข้ามชาติที่มีพนักงานส่วนใหญ่เป็นชาวต่างชาติและองค์กรที่ส่วนใหญ่เป็นพนักงานคนไทย เพื่อศึกษาว่าวัฒนธรรมของชาติและองค์กรมีส่วนในการกำหนดปัจจัยทั้ง 2 ปัจจัยดังกล่าวหรือไม่

(3) การวิจัยครั้งนี้ พบว่า ปัจจัยการรับรู้ภัยคุกคาม มีความผันแปรของตัวแปรตาม (R^2) ระหว่างประสบการณ์ก่อนหน้าจากการเผชิญกับภัยคุกคามที่ส่งอิทธิพลทางตรงต่อการรับรู้ภัยคุกคามมีค่าค่อนข้างน้อย ซึ่งเท่ากับร้อยละ 7.4 ($R^2 = 0.074$) จึงควรศึกษาว่ามีปัจจัยเพิ่มเติมใดบ้างที่ส่งผลต่อปัจจัยการรับรู้ภัยคุกคาม

(4) การวิจัยครั้งนี้ พบว่า ปัจจัยการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยส่งอิทธิพลทางตรงต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ที่ค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.474 และมีความผันแปรของตัวแปรตาม (R^2) เท่ากับร้อยละ 65.7 (R^2 = 0.657) ซึ่งมีค่าค่อนข้างสูง จึงควรศึกษาว่ามีปัจจัยใดบ้างที่ส่งผลต่อการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

บรรณานุกรม

จตุชัย แพงจันทร์. (2550). *Master in security รวบรวมเนื้อหาด้าน Security ไว้ครบทุกด้านสำหรับ Admin มืออาชีพ* (1). นนทบุรี: อินโฟเพรส.

สำนักงานราชบัณฑิตยสภา. (2532). ความหมายของประสบการณ์. ดึงข้อมูลวันที่ 10 มกราคม 2560, จาก http: / / www. royin. go. th/ ?knowledges= % E0% B8% 9B% E0% B8% A3% E0% B8% B0% E0 %B8%AA%E0%B8%9A%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%93%E0%B9%8C.

สุธีรา เดชนครินทร์ และ สุธินี ฤกษ์ขำ. (2558). *ผลกระทบของมิติทางวัฒนธรรมที่มีต่อระบบการบริหารงานที่มีประสิทธิภาพสูง: การบูรณาการทบทวนวรรณกรรม.* วิทยานิพนธ์ที่ยังไม่ได้ตีพิมพ์, คณะวิทยาการจัดการ, มหาวิทยาลัยสงขลานครินทร์.

สุพิชญา อาชวจิรดา. (2557). *ปัจจัยที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร.* (วิทยาศาตรมหาบัณฑิต). คณะพาณิชยศาสตร์และการบัญชี, มหาวิทยาลัยธรรมศาสตร์.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., & Aleassa, H. (2013). Information Security Policy Compliance: An Empirical Study of Ethical Ideology. *46th Hawaii International Conference on System Sciences*, Hawaii, 3018-3027.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers and Security, 26*(4), 276-289.

Bandura, A. (1980). Gauging the relationship between self-efficacy judgment and action. *Cognitive Therapy and Research*, *4,* 263-268.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

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.

Cavallari, M. (2011). The organizational relationship between compliance and information security. *International Journal of the Academic Business World, 5*(2), 63-76.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security, 1*(3), 18-41.

Chen, Y., Ramamurthy, K. R., & Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems, 29*(3), 157-188.

Chen, Y., & Zahedi, F. M. (2016). Indiviuals' Internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly, 40*(1), 205-222.

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

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems, 20*, 643-658.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research, 20*(1), 79-98.

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies *Journal of the Association for Information System, 8*(7), 386-408.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. MA: Addison-Wesley.

Greitemeyer, T., & Weiner, B. (2008). Asymmetrical effects of Reward and punishment on attributions of morality. *The Journal of Social Psychology, 148*(4), 407-420.

Haeussinger, F. J., & Kranz, J. J. (2013). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior *International Conference on Information Systems 2013*, 1-16.

Hanus, B., & Wu, Y. A. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management, 33*(1), 2-16.

Hepler, J. (2015). A good thing isn't always a good thing: dispositional attitudes predict non-normative judgments. *Personality and Individual Differences, 75*(0), 59-63.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*, 106-125.

Hochwarter, W. A., Perrewe, P. L., Hall, A. T., & Ferris, G. R. (2005). Negative affectivity as a moderator of the form and magnitude of the relationship between felt accountability and job tension. *Journal of Organizational Behavior, 26*, 517-534.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences, 43*(4), 615-660.

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

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management, 51*(1), 69-79.

Jouini, M., & Rabai, L. B. A. (2016). Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems. *Procedia Computer Science,* 83, 1084-1089.

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information Technology Adoption Across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs. *MIS Quarterly, 23*(2), 183-213.

Kaur, J., & Mustafa, N. (2013). Examining the Effects of Knowledge, Attitude and Behaviour on Information Security Awareness: A Case on SME. *3rd International Conference on Research and Innovation in Information Systems*, Malaysia, 286-290.

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computer and Security, 59*, 60-70.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour and Information Technology, 27*(5), 445-454.

Liang, H., & 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.

Merriam-Webster Online Dictionary (2010). Meaning of Behavior. Retrieved September 2, 2016, from https://www.merriam-webster.com/dictionary/behavior.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS'07)*, Hawaii, 231-254.

Peace, A. G., Galletta, D. F., & Thong, J. Y. L. (2003). Software Piracy in the Workplace: A Model and Empirical Test. *Journal of Management Information Systems, 20*(1), 153-177.

PwC. (2014). 2014 Information Security Breaches Survey. Retrieved October 3, 2016, from http://www.pwc.co.uk/services/audit-assurance/insights/2014-information-security-breaches-survey.html.

PwC. (2015). Information Security Breaches Survey 2015. Retrieved October 3, 2016, from http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html.

Safa, N. S., Solms, R. V., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computer and Security, 56*, 20-82.

Schlenker, B. R., Britt, T. W., Pennington, J., Murphy, R., & Doherty, K. (1994). The triangle model of responsibility. *Psychological Review, 101*(4), 632-652.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computer and Security, 49*, 177-191.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM, 52*(12), 145-147.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security, 8*(1), 31-41.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. *IFIP International Federation for Information Processing, 1,* 33-44.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer, 43*(2), 64-71.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information and Management, 48*(7), 296-302.

Stajkovic, A. D., & Luthans, F. (1988). Self-efficacy and work-related performance: A meta-analysis. *Psychological Bulletin, 124*(2), 240-261.

Stanciu, V., & Tinca, A. (2016). Students' awareness on information security between own perception and reality – an empirical study. *Accounting and Management Information Systems,* 15*(1)*, 112-130.

Straub, Jr., D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research, 1*(3), 255-276.

Trustwave. (2014). 2014 State of Risk Report. Retrieved October 3, 2016, from https://www.trustwave.com/Resources/Library/Documents/2014-State-of-Risk-Report/.

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computer and Security, 59*, 138-150.

Vance, A., Lowry, P. B., & Eggett, D. (2015). A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface. *MIS Quarterly*, 1-18.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly, 27*(3), 425-478.

Yoon, C., Hwang, J., & Kim, R. (2012). Exploring Factors That Influence Students' Behaviors in Information Security. *Journal of Information Systems Education, 23*(4), 407-415.

Zaharia, A. (2015). 10+ Critical Corporate Cyber Security Risks – A Data Driven List. Retrieved October 3, 2016, from https://heimdalsecurity.com/blog/10-critical-corporate-cyber-security-risks-a-data-driven-list/.

รูปแบบการฝึกอบรมที่เหมาะสมกับทักษะในงานทางด้านเทคโนโลยีสารสนเทศ

ณัฐพล ภมรคณเสวิต*
บริษัท โลตัส จำกัด
นิตยา วงศ์ภินันท์วัฒนา
คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

***Correspondence:** nattaphon.pam@gmail.com doi: 10.14456/jisb.2018.16
วันที่รับบทความ: 12 มี.ค. 2561 วันแก้ไขบทความ: 18 เม.ย. 2561 วันตอบรับบทความ: 2 พ.ค. 2561

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาวิธีการฝึกอบรมที่เหมาะสมในการพัฒนาทักษะด้านต่างๆ ของบุคคลากรทางด้านเทคโนโลยีสารสนเทศ ที่พึงมีในการปฏิบัติงานซึ่งประกอบด้วย ทักษะการคิด ทักษะการทำงานเป็นทีม ทักษะในการสื่อสาร ทักษะการเขียนโปรแกรมคอมพิวเตอร์ ทักษะด้านระบบฐานข้อมูล ทักษะด้านซอฟต์แวร์ ทักษะด้านฮาร์ดแวร์ ทักษะด้านระบบเครือข่าย ทักษะด้านระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ทักษะการบริหารโครงการระบบสารสนเทศ ทักษะการพัฒนาระบบสารสนเทศ ทักษะการบริหารการให้บริการระบบสารสนเทศ ทักษะการตรวจสอบระบบสารสนเทศ ทักษะการวางแผนระบบสารสนเทศเชิงกลยุทธ์ และทักษะการบริหารระบบสารสนเทศเชิงกลยุทธ์ นอกจากนี้ยังสำรวจวิธีการฝึกอบรมให้แก่บุคลากรทางด้านเทคโนโลยีสารสนเทศที่องค์กรต่างๆ ใช้อยู่ในปัจจุบัน โดยใช้วิธีการสำรวจขั้นต้นซึ่งคณะผู้วิจัยได้พัฒนาและจัดส่งแบบสอบถามไปยังบริษัทที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย 8 กลุ่มอุตสาหกรรม จำนวน 448 บริษัท ผลของการวิจัยพบว่าบริษัทเลือกใช้วิธีการฝึกอบรมแบบการบรรยายเป็นอันดับแรกมากที่สุด เพื่อให้เกิดทักษะในงานทางด้านเทคโนโลยีสารสนเทศด้านต่างๆ และยังพบว่ามีวิธีการฝึกอบรมอีกหลายวิธีที่สามารถทำให้บุคลากรทางด้านเทคโนโลยีสารสนเทศมีการพัฒนาทักษะในการปฏิบัติงานได้ แต่บางวิธียังไม่เป็นที่นิยมในการเลือกใช้ องค์กรต่างๆ สามารถนำผลการวิจัยไปประยุกต์ในการเลือกใช้วิธีการฝึกอบรมเพื่อให้บุคคลากรทางด้านเทคโนโลยีสารสนเทศมีทักษะที่เหมาะสมต่อการปฏิบัติงาน

คำสำคัญ: วิธีการฝึกอบรม ทักษะด้านเทคโนโลยีสารสนเทศ การบรรยาย

Matching Training Methods and IT Skills

Nattaphon Pamornkanasevit*

Lotus Co., Ltd.

Nitaya Wongpinunwatana

Thammasat Business School, Thammasat University

***Correspondence:** nattaphon.pam@gmail.com

doi: 10.14456/jisb.2018.16

Received: 12 Mar 2018 Revised: 18 Apr 2018 Accepted: 2 May 2018

Abstract

The objective of this study is to examine training method to develop skills of IT officer which shall consist of Thinking Skills, Teamwork, Communication Skill, Algorithm and Programming, Database, Software, Hardware, Network, Security, Project Management, System Development, Service Management, System Audit, System Planning, Technological Strategy Management. Furthermore, the study aims to survey the training methods which are currently applied in the workplace. Data were collected by questionnaire. Questionnaire was sent to 448 companies listed on the Stock Exchange of Thailand. This study found that there are numerous of the training methods for IT officer, one of the most popular techniques is the lecture method. The information of this study will help the employer to prepare the appropriate training program for IT officer to possess appropriate skill to perform task.

Keywords : Training method, IT skills, Lecture method

1. บทนำ

1.1 ความสำคัญและที่มาของปัญหา

การจัดทำโครงการและหลักสูตรฝึกอบรม (Training program design) เป็นกระบวนการที่จัดทำขึ้นอย่างเป็นระบบภายหลังการวิเคราะห์ความจำเป็นในการฝึกอบรม ซึ่งมีการกำหนดวัตถุประสงค์ที่ชัดเจนและสอดคล้องกับความจำเป็นในการฝึกอบรม โดยหลักสูตรการฝึกอบรมที่จัดทำขึ้นมักจะมุ่งเน้นให้เกิดความรู้ (Knowledge) ความเข้าใจ (Understanding) ในการปฏิบัติงาน ให้มีทัศนคติ (Attitude) ที่ดีต่องาน ต่อผู้บริหารและองค์กร ตลอดจนให้เกิดทักษะ (Skill) ความชำนาญในงานที่ปฏิบัติเพื่อให้บุคลากรสามารถปฏิบัติงานในความรับผิดชอบได้อย่างมีประสิทธิภาพ และเพื่อเป็นการเตรียมบุคลากรไว้รองรับการเติบโตขององค์กรที่อาจขยายตัวอย่างรวดเร็ว หรือเตรียมความพร้อมในการรับกับสภาพปัญหาที่อาจเกิดขึ้นได้ตลอดเวลา

แนวทางการออกแบบหลักสูตรการฝึกอบรมของ Personal Decisions International หรือ PDI ซึ่งเป็นที่ปรึกษาทางด้านการบริหารทรัพยากรมนุษย์ ได้ตั้งกรอบแนวความคิดไว้ 5 ส่วน คือ (1) ความเข้าใจอย่างถ่องแท้ (Insight) โดยวิเคราะห์จากความรู้และความสามารถของพนักงานแต่ละคนในขณะนั้นว่าเขาควรจะได้รับการฝึกอบรมในเรื่องใดบ้าง (2) แรงจูงใจ (Motivation) เป็นสิ่งที่ช่วยกระตุ้นให้ผู้เข้ารับการฝึกอบรมต้องการเรียนรู้ และยังทราบว่าจะได้รับประโยชน์อะไรบ้างจากการเข้ารับการฝึกอบรมในครั้งนี้ (3) ความรู้และทักษะใหม่ ๆ (New skill and knowledge) เป็นสิ่งที่ควรคำนึงถึงเพื่อเพิ่มความสามารถและความรู้ใหม่ ๆ ที่พนักงานผู้นั้นยังไม่มี (4) เรียนรู้จากสถานการณ์จริง (Rear world practice) เพื่อให้ผู้เข้ารับการฝึกอบรมมีทักษะเพิ่มขึ้นจากสถานการณ์จริงซึ่งจะทำให้การทำงานมีประสิทธิภาพที่ดียิ่งขึ้น (5) การรายงานผลหรืออธิบายผล (Accountability) เป็นการรายงานผลการฝึกอบรมของผู้เข้ารับการฝึกอบรมโดยผ่านผู้บังคับบัญชา เพื่อให้ทราบถึงความเข้าใจและความสนใจหลังการฝึกอบรมซึ่งจะสามารถนำไปใช้เป็นแนวทางในการจัดการฝึกอบรมครั้งต่อไปได้

1.2 วัตถุประสงค์ของการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อสำรวจวิธีการฝึกอบรมที่องค์กรต่างๆ นำมาใช้ เพื่อพัฒนาทักษะให้บุคคลากรทางด้านเทคโนโลยีสารสนเทศ รวมถึงการเปรียบเทียบวิธีการฝึกอบรมที่อบรมที่องค์กรใช้จริงเปรียบเทียบกับวิธีการฝึกอบรมที่ควรนำมาใช้

2. แนวคิดที่เกี่ยวข้อง

2.1 ประเภทของการฝึกอบรม

การฝึกอบรม คือ กระบวนการในการพัฒนาบุคลากรในองค์กรให้เกิด ความรู้ ทักษะ เพื่อให้บุคลากรสามารถใช้ศักยภาพของตนเองอย่างเต็มที่และสามารถนำไปประยุกต์ใช้ให้เป็นประโยชน์ต่อการปฏิบัติงานให้มีประสิทธิภาพรองรับความพร้อมขององค์กรต่อการแข่งขันทางธุรกิจ อีกทั้งยังเป็นการสร้างหนทางความก้าวหน้าในสายงานของบุคลากร (Blanchard & Thacker, 2007) โดยประเภทของการฝึกอบรม มีการแบ่งโดยยึดตามหลักต่าง ๆ ดังนี้

(1) แหล่งของการฝึกอบรม พิจารณาจากหน่วยงานที่ทำหน้าที่ฝึกอบรมซึ่งแบ่งได้เป็น 2 ลักษณะ คือ การฝึกอบรมจากหน่วยงานภายในองค์กร (Internal training) และการฝึกอบรมจากหน่วยงานภายนอกองค์กร (Public training)

(2) ผู้เข้ารับการอบรม แบ่งย่อยได้ 3 ลักษณะ คือ

- **จำนวนผู้เข้ารับการฝึกอบรม** มีทั้งการฝึกอบรมเป็นรายบุคคล (Individual training) ซึ่งเป็นการฝึกอบรมเฉพาะรายตามความจำเป็นของบุคคลนั้น และอาจเป็นการฝึกอบรมในเรื่องเฉพาะหรือขั้นสูง และการฝึกอบรมเป็นรายคณะ (Group training) ซึ่งเป็นการฝึกอบรมให้กับกลุ่มบุคลากรที่มีลักษณะความจำเป็นในการฝึกอบรมที่เหมือนกัน (Blanchard & Thacker, 2007; ชูชัย สมิทธิไกร, 2544)

- **กลุ่มโครงสร้างการบริหารงานของผู้เข้ารับการอบรม** ประกอบด้วย การฝึกอบรมเพื่อพัฒนาบุคลากรตามแนวนอนในโครงสร้างขององค์กร (Vertical) มีวัตถุประสงค์เพื่อให้ความรู้ทั่วไป ในลักษณะที่ต้องการสร้างกรอบแนวความคิดและแนวปฏิบัติอย่างกว้างๆ ได้แก่ การฝึกอบรมเบื้องต้น (Induction training) (ชูชัย สมิทธิไกร, 2544) และการฝึกอบรมเพื่อพัฒนาบุคลากรตามแนวตั้งในโครงสร้างขององค์กร (Horizontal) มีวัตถุประสงค์เพื่อให้ความรู้หรือสร้างทักษะเฉพาะสำหรับบุคลากรในแต่ละตำแหน่งหรือสายงาน โดยใช้หลักสูตรซึ่งกำหนดขึ้นโดยเฉพาะตามความจำเป็นในการฝึกอบรม ของตำแหน่งนั้นๆ และมักจะเน้นถึงแนวทางการปฏิบัติงานในรายละเอียด ซึ่งผู้เข้าอบรมจะนำไปใช้ในการทำงานได้มากกว่าการฝึกอบรมแนวนอน เช่น การฝึกอบรมสำหรับเจ้าหน้าที่บุคคล เลขานุการ หรือผู้บริหาร เป็นต้น (ชูชัย สมิทธิไกร, 2544)
- **ลักษณะของเนื้อหาหลักสูตรฝึกอบรม** การกำหนดหลักสูตรฝึกอบรมในแต่ละด้านจะมาจากการสำรวจหาความจำเป็นในการฝึกอบรมเนื่องจากเนื้องานมีความหลากหลายหรือมีความเจาะจงเฉพาะ โดยผู้เข้ารับการฝึกอบรมจะเป็นบุคลากรซึ่งดำรงตำแหน่งแตกต่างกัน และแบ่งประเภทการฝึกอบรมออกเป็นด้านต่างๆ ตามลักษณะของหลักสูตรฝึกอบรม เช่น การฝึกอบรมด้านเทคโนโลยีสารสนเทศ การฝึกอบรมด้านการบริหารทรัพยากรมนุษย์ การฝึกอบรมด้านมาตราฐานการบัญชี (ชูชัย สมิทธิไกร, 2544)

(3) วัตถุประสงค์ของการฝึกอบรม แบ่งออกเป็น 3 ลักษณะ คือ การฝึกอบรมเพื่อแก้ไขปัญหาที่ได้เกิดขึ้นมาแล้ว การฝึกอบรมเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นในอนาคต และการฝึกอบรมเพื่อพัฒนาบุคลากรให้มีศักยภาพสูงขึ้นในระยะยาว

(4) ช่วงเวลาในการฝึกอบรม การแบ่งประเภทของการฝึกอบรมมักจะพิจารณาจากช่วงเวลาในการฝึกอบรมที่ผู้เข้ารับการฝึกอบรมซึ่งแบ่งได้เป็น 2 ลักษณะ คือ การฝึกอบรมก่อนเริ่มเข้ารับหน้าที่ (Pre-service training) และการฝึกอบรมในระหว่างเข้ารับหน้าที่แล้ว (In-service training) (บรรยงค์ โตจินดา, 2543)

(5) ผลที่ได้จากการอบรม แบ่งได้เป็น 3 ลักษณะ คือ การฝึกอบรมที่จะช่วยให้มีการเรียนรู้หรือการเปลี่ยนแปลงด้านความรู้ เช่น การบรรยาย การสัมมนา การฝึกอบรมที่จะช่วยให้มีการเปลี่ยนแปลงพฤติกรรม ทักษะ หรือความสามารถ เช่น การสาธิต การฝึกปฏิบัติ กรณีศึกษา การสร้างสถานการณ์จำลอง การสอนงาน การแสดงบทบาทสมมติ และเทคนิคการฝึกอบรมที่จะช่วยให้มีการเปลี่ยนแปลงด้านเจตคติ เช่น การแสดงบทบาทสมมติ กรณีศึกษา การสัมมนา การฝึกปฏิบัติ เกมการบริหาร (ชูชัย สมิทธิไกร, 2544)

จากแนวคิดที่เกี่ยวข้องกับวิธีการฝึกอบรม คณะผู้วิจัยเลือกวิธีการฝึกอบรมที่นิยมนำมาใช้ในการฝึกอบรมแก่บุคลากรทางด้านเทคโนโลยีสารสนเทศมาประยุกต์ใช้ (ตารางที่ 1 และตารางที่ 2) ดังนี้

(1) การฝึกอบรมในขณะปฏิบัติงาน (On the job training)
(2) การฝึกอบรมแบบการบรรยาย (Lectures)
(3) การฝึกอบรมแบบการอภิปราย (Discussion)
(4) การฝึกอบรมแบบเรียนรู้ด้วยตัวเอง (Self-study)
(5) การฝึกอบรมแบบการให้คำปรึกษา (Coaching)
(6) การฝึกอบรมแบบการสาธิต (Demonstration)
(7) การฝึกอบรมแบบการฝึกปฏิบัติ (Practical exercise)
(8) การฝึกอบรมแบบการใช้กรณีศึกษา (Case study)
(9) การฝึกอบรมแบบการแสดงบทบาทสมมุติ (Role playing)
(10) การฝึกอบรมแบบการใช้สถานการณ์จำลอง (Simulation)

ตารางที่ 1 ลักษณะของวิธีการฝึกอบรม

วิธีการฝึกอบรม	วัตถุประสงค์	สิ่งที่ได้รับจากการอบรม	ประสิทธิผลในการอบรม
การฝึกอบรมในขณะปฏิบัติงาน (On the job training)	เพื่อถ่ายทอดประสบการณ์และเทคนิคในการทำงานจากผู้ทำการฝึกอบรมไปยังผู้เข้ารับการฝึกอบรม	- องค์ความรู้ในหัวข้อการฝึกอบรม - ทักษะ (Skills) และความชำนาญในการปฏิบัติงานจริง	ความสามารถในการปฏิบัติงาน และประสิทธิผลที่ได้รับจะสูงขึ้นเมื่อมีการกำหนดโครงสร้างในการฝึกอบรม
การฝึกอบรมแบบการบรรยาย (Lectures)	เพื่อพัฒนาองค์ความรู้ของผู้เข้ารับการฝึกอบรมให้เพิ่มมากขึ้น โดยมุ่งเน้นที่การพัฒนาแนวคิดมากกว่าการปฏิบัติงานจริง	- องค์ความรู้ในหัวข้อการฝึกอบรม - ความคิดเห็นในหัวข้อการฝึกอบรมจากผู้ทำการฝึกอบรม	ประสิทธิผลอยู่ที่การได้รับองค์ความรู้ใหม่และการนำองค์ความรู้นั้นไปประยุกต์ใช้
การฝึกอบรมแบบการอภิปราย (Discussion)	เพื่อให้ผู้เข้ารับการฝึกอบรมมีแนวคิดจากทรรศนะที่ต่างกันของผู้ทำการฝึกอบรม	- องค์ความรู้ในหัวข้อการฝึกอบรม - ความคิดเห็นในหัวข้อการฝึกอบรมจากผู้ทำการฝึกอบรม - ทัศนคติจากการร่วมฟังการอภิปราย	ประสิทธิผลที่ได้รับขึ้นอยู่กับสิ่งที่ได้รับรู้จากการมีส่วนร่วมในการแลกเปลี่ยนความคิดเห็นและประสบการณ์ของผู้ทำการฝึกอบรมและการนำความรู้ไปประยุกต์ใช้
การฝึกอบรมแบบเรียนรู้ด้วยตัวเอง (Self-directed learning)	เพื่อพัฒนาองค์ความรู้ของผู้เข้ารับการฝึกอบรมพิ่มเติมจากความรู้เดิมหรือเพื่อการหาความรู้ใหม่ โดยมุ่งเน้นให้ลดภาระของผู้ทำการฝึกอบรม	- องค์ความรู้ในหัวข้อการฝึกอบรม - เตรียมความพร้อมสำหรับการฝึกอบรมในเรื่องเดิมสำหรับวิธีการฝึกอบรมประเภทอื่น	ประสิทธิผลที่ได้รับขึ้นอยู่กับสื่อและเทคโนโลยีสำเร็จรูปที่ใช้ในการฝึกอบรม
การฝึกอบรมแบบการให้คำปรึกษา (Coaching)	เพื่อให้ผู้เข้ารับการฝึกอบรมมีความมั่นใจว่าในกรณีที่มีปัญหาในการทำงาน สามารถขอคำปรึกษาจากผู้ที่ทำหน้าที่ฝึกอบรมได้	- องค์ความรู้ (Knowledge) ทักษะ (Skills) และทัศนคติ (Attitudes)	ประสิทธิผลที่ได้รับขึ้นอยู่กับการปฏิบัติในการตอบสนองต่อเหตุการณ์
การฝึกอบรมแบบการสาธิต (Demonstration)	เพื่อให้ผู้เข้ารับการฝึกอบรมได้รับประสบการณ์ใกล้เคียงกับประสบการณ์ตรงมากที่สุด	- ทำให้มีความรู้ความเข้าใจในเรื่องที่ปฏิบัติชัดเจนขึ้น	การนำไปใช้ในสถานการณ์จริง

ตารางที่ 1 ลักษณะของวิธีการฝึกอบรม (ต่อ)

วิธีการฝึกอบรม	วัตถุประสงค์	สิ่งที่ได้รับจากการอบรม	ประสิทธิผลในการอบรม
การฝึกอบรมแบบการฝึกปฏิบัติ (Practical exercise)	เพิ่มทักษะความชำนาญของผู้เข้ารับการฝึกอบรม	- ทักษะและความชำนาญในการปฏิบัติงานจริง	ความคล่องแคล่ว ความเชี่ยวชาญ ความชำนาญในการปฏิบัติงาน
การฝึกอบรมแบบการใช้กรณีศึกษา (Case study)	เพื่อให้ผู้เข้ารับการฝึกอบรมได้รู้จักคิดอย่างเป็นระบบและแก้ไขปัญหาและตัดสินใจอย่างมีเหตุผล	- วิธีการคิด วิธีการนำข้อมูลมาประกอบการพิจารณาในการตัดสินใจเรื่องหนึ่งเรื่องใด	การนำไปใช้แก้ไขปัญหาในสถานการณ์จริง
การฝึกอบรมแบบการแสดงบทบาทสมมุติ (Role playing)	เพื่อให้ผู้เข้ารับการฝึกอบรมได้เข้าใจความรู้สึกและพฤติกรรมทั้งของตนเองและของผู้อื่น	- ทัศนคติจากการร่วมแสดงบทบาทสมมุติ	การนำไปประยุกต์ใช้ในสถานการณ์จริง
การฝึกอบรมแบบการใช้สถานการณ์จำลอง (Simulation)	เพื่อให้ผู้เข้ารับการฝึกอบรมได้เรียนรู้การแก้ไขปัญหาในสถานการณ์ใกล้เคียงของจริง	- ทำให้มีความเข้าใจในเรื่องที่ปฏิบัติชัดเจนขึ้น	การนำไปประยุกต์ใช้ในสถานการณ์จริง

ตารางที่ 2 ข้อดีและข้อเสียของแต่ละวิธีการฝึกอบรม

วิธีการฝึกอบรม	ข้อดี	ข้อเสีย
การฝึกอบรมในขณะปฏิบัติงาน (On the job training)	- ผู้เข้ารับการฝึกอบรมได้ปฏิบัติงานจริงทำให้เข้าใจถึงกระบวนการและขั้นตอนต่าง ๆโดยเรียนรู้จากผู้มีประสบการณ์จริง - ทราบจุดอ่อน - จุดแข็งของผู้เข้ารับการฝึกอบรมได้อย่างชัดเจน	- ผู้ทำการฝึกอบรมต้องสละเวลาทำงานมาดูแลผู้เข้ารับการฝึกอบรม - ผู้ทำการฝึกอบรมบางคนอาจไม่ใส่ใจสอนงานเต็มที่ - อาจมีความเสียหายเกิดขึ้น เนื่องจากผู้เข้ารับการฝึกอบรมยังไม่มีความเข้าใจและความชำนาญ - มีลักษณะของการฝึกอบรมแบบไม่เป็นทางการ
การฝึกอบรมแบบการบรรยาย (Lectures)	- ผู้เข้ารับการฝึกอบรม สามารถเตรียมตัวล่วงหน้าในหัวข้อที่จะรับฟังการบรรยาย - เหมาะกับผู้เข้ารับการฝึกกลุ่มใหญ่	- เป็นวิธีการฝึกอบรมที่มีการสื่อสารทางเดียว - ผู้ทำการฝึกอบรมสามารถถ่ายทอดความรู้และประสบการณ์ให้ผู้เข้ารับการฝึกอบรมในระยะเวลาสั้น ๆ จนไม่อาจอธิบายประเด็นบางอย่างให้เข้าใจได้อย่างชัดเจน
การฝึกอบรมแบบการอภิปราย (Discussion)	- ผู้เข้ารับการฝึกอบรมได้รับความรู้ และประสบการณ์ตลอดจนความคิดเห็นหลายแง่มุมจากผู้ทำการฝึกอบรมหลายท่านในคราวเดียว	- เวลาของผู้ทำการฝึกอบรมแต่ละท่านค่อนข้างน้อย บางครั้งความคิดเห็นที่ไม่ลงรอยกันของผู้ทำการฝึกอบรม อาจทำให้ผู้เข้ารับการฝึกอบรมเกิดความสับสนได้ - การตอบข้อซักถามของผู้เข้ารับการฝึกอบรมอาจไม่ละเอียด เพราะมักมีเวลาจำกัด
การฝึกอบรมแบบเรียนรู้ด้วยตัวเอง (Self-directed learning)	- ค่าใช้จ่ายในการฝึกอบรมต่ำ	- ผู้เข้ารับการฝึกอบรมอาจไม่สามารถนำไปปฏิบัติได้จริง เพราะไม่เคยเห็นของจริง

ตารางที่ 2 ข้อดีและข้อเสียของแต่ละวิธีการฝึกอบรม (ต่อ)

วิธีการฝึกอบรม	ข้อดี	ข้อเสีย
การฝึกอบรมแบบการให้คำปรึกษา (Coaching)	- ช่วยให้ผู้เข้ารับการฝึกอบรมได้ฝึกใช้ความสามารถในการวิเคราะห์และตัดสินใจภายใต้สถานการณ์ที่สมจริง - สามารถนำไปประยุกต์ใช้กับเหตุการณ์อื่น ๆ ได้ - ผู้เข้ารับการฝึกอบรมได้เรียนรู้กระบวนการแก้ปัญหามากขึ้น - สามารถแก้ไขปัญหาได้อย่างรวดเร็วและมีประสิทธิภาพ	- ผู้เข้ารับการฝึกอบรมได้เรียนรู้กระบวนการแก้ปัญหาเพียงเล็กน้อยเท่านั้น
การฝึกอบรมแบบการสาธิต (Demonstration)	- ผู้เข้ารับการฝึกอบรมได้เห็นสิ่งที่เรียนรู้อย่างเป็นรูปธรรมทำให้มีความเข้าใจและจดจำในเรื่องที่สาธิตได้	- ผู้เข้ารับการฝึกอบรมไม่ได้ลงมือทำเองจึงอาจไม่มีความรู้ที่ลึกซึ้งเพียงพอ - ไม่เหมาะกับผู้เข้าอบรมกลุ่มใหญ่
การฝึกอบรมแบบการฝึกปฏิบัติ (Practical exercise)	- ทำให้มีส่วนร่วมอย่างเต็มที่ในกระบวนการเรียนรู้ - มีความเข้าใจและมั่นใจที่จะนำไปปฏิบัติจริง - ได้ฝึกปฏิบัติและทราบผลการปฏิบัติในทันที	- ใช้เวลาในการเตรียมการฝึกอบรมมาก - สิ้นเปลืองค่าใช้จ่ายในการใช้วัสดุอุปกรณ์ในการฝึกอบรมเป็นจำนวนมาก
การฝึกอบรมแบบการใช้กรณีศึกษา (Case study)	- ผู้เข้ารับการฝึกอบรมได้มีโอกาสแสดงความคิดเห็นและแลกเปลี่ยนความคิดเห็นซึ่งกันและกัน - ผู้เข้ารับการฝึกอบรมเกิดทักษะในการคิดวิเคราะห์	- หากใช้กับกลุ่มเผู้เข้ารับการฝึกอบรมที่มีมากเกินไป ผู้เข้ารับการฝึกอบรมก็จะแสดงออกไม่ทั่วถึง - ถ้าผู้เข้ารับการฝึกอบรมไม่ร่วมมือ ไม่กระตือรือร้นก็จะทำให้ผลการฝึกอบรมไม่เป็นไปตามที่กำหนดไว้

ตารางที่ 2 ข้อดีและข้อเสียของแต่ละวิธีการฝึกอบรม (ต่อ)

วิธีการฝึกอบรม	ข้อดี	ข้อเสีย
การฝึกอบรมแบบการแสดงบทบาทสมมุติ (Role playing)	- หลังจากการประเมินผลทำให้ทราบจุดแข็ง จุดอ่อนของการปฏิบัติดังกล่าว - ผู้เข้าอบรมมีโอกาสสังเกต และทำความเข้าใจกับพฤติกรรมแบบต่าง ๆ	- อาจไม่สามารถนำความเข้าใจไปปรับใช้ในชีวิตจริงได้ เนื่องจากอาจมีเหตุการณ์อื่นที่อยู่นอกเหนือความควบคุมเข้ามาเกี่ยวข้องด้วย - เหมาะกับปัญหาหรือสถานการณ์ที่ไม่ซับซ้อนเท่านั้น
การฝึกอบรมแบบการใช้สถานการณ์จำลอง (Simulation)	- เป็นกระบวนการที่ทำให้ผู้เข้ารับการฝึกอบรมได้เรียนรู้สถานการณ์เสมือนจริงได้มากที่สุด	- ต้องได้รับความร่วมมือจากผู้เข้ารับการฝึกอบรมหากผู้เข้ารับการฝึกอบรมไม่ร่วมมือก็จะทำให้กิจกรรมติดขัดไม่บรรลุผลตามที่วางไว้

2.2 ทักษะด้านเทคโนโลยีสารสนเทศ

ลักษณะงานทางด้านเทคโนโลยีสารสนเทศ (IT function) สามารถแบ่งลักษณะงานทางด้านเทคโนโลยีสารสนเทศตามหน้าที่ความรับผิดชอบในการทำงานได้ (McKeen & Smith, 2007) ดังนี้คือ ลักษณะงานทางด้าน Networking, Hardware, Operating systems, Business analysis, Systems analysis, Application development, Quality assurance and testing, Strategy and planning, Project management, Data management, และ Application support

(1) ทักษะในงานทางด้านเทคโนโลยีสารสนเทศ (IT skills) จากลักษณะของงานทางด้านเทคโนโลยีสารสนเทศที่มีความหลากหลายนั้น มีนักวิจัยบางท่านได้จำแนกทักษะในงานทางด้านเทคโนโลยีสารสนเทศจากแต่ละลักษณะงานที่มีความเหมือนกันซึ่งแต่ละตำแหน่งหน้าที่นั้นต้องการทักษะแตกต่างกันไป (Todd et al., 1995) ดังนี้

(2) ทักษะพื้นฐาน (Foundation and employability skills) ประกอบด้วย ทักษะการคิด (Thinking skills) ซึ่งประกอบด้วยทฤษฎีย่อย 3 ด้าน ได้แก่ ด้านบริบททางสังคม ด้านประสบการณ์ และด้านกระบวนการคิด, ทักษะการทำงานเป็นทีม (Teamwork skills) และทักษะในการสื่อสาร (Communication skills)

(3) ทักษะทางด้านเทคโนโลยี (Technology skills) ประกอบด้วย ทักษะการเขียนโปรแกรมคอมพิวเตอร์ (Algorithm and programming), ทักษะด้านระบบฐานข้อมูล (Database), ทักษะด้านซอฟต์แวร์ (Software), ทักษะด้านฮาร์ดแวร์ (Hardware), ทักษะด้านระบบเครือข่าย (Network) และทักษะด้านระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Security)

(4) ทักษะด้านการจัดการ (Management) ประกอบด้วย ทักษะการบริหารโครงการระบบสารสนเทศ (Project management), ทักษะการพัฒนาระบบสารสนเทศ (System development technology), ทักษะการบริหารการให้บริการระบบสารสนเทศ (Service management), ทักษะการตรวจสอบระบบสารสนเทศ (System audit)

(5) ทักษะด้านกลยุทธ์ (Strategy) ประกอบด้วย ทักษะการวางแผนระบบสารสนเทศเชิงกลยุทธ์ (System planning) และทักษะการบริหารระบบสารสนเทศเชิงกลยุทธ์ (Technological strategy management)

3. วิธีการวิจัย

ประชากรของงานวิจัยนี้คือ บริษัทที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย จำนวน 448 บริษัท เลือกใช้วิธีการเก็บข้อมูลด้วยชุดแบบสอบถามกระดาษ โดยแจกแบบสอบถามกระดาษให้แก่กลุ่มตัวอย่างซึ่งเป็นบริษัทที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย ที่มีบุคลากรทางด้านระบบสารสนเทศปฏิบัติงานอยู่ ซึ่งรายละเอียดของแบบสอบถามที่ใช้ในการวิเคราะห์แบ่งออกเป็น 2 ส่วน โดยส่วนแรกเป็นข้อมูลเบื้องต้นของสถานประกอบการ จำนวน 3 ข้อ และส่วนที่ 2 เป็นคำถามเกี่ยวกับวิธีการฝึกอบรม (Training methods) มาผนวกรวมกับทักษะในงานทางด้านเทคโนโลยีสารสนเทศ (IT skills)

คณะผู้วิจัยคัดแยกแบบสอบถามที่มีความผิดพลาดออกไป เช่น ตอบไม่ครบถ้วน เป็นต้น และนำข้อมูลที่สามารถวิเคราะห์หาค่าสถิติมาแจกแจงความถี่และคำนวณค่าร้อยละ นอกจากนี้ก่อนการนำข้อมูลไปประมวลผลทางสถิติคณะผู้วิจัยได้ตรวจสอบความถูกต้องของการแปลงข้อมูลจากแบบสอบถามให้อยู่ในรูปของข้อมูลทางคอมพิวเตอร์ก่อนนำไปประมวลผลทางสถิติโดยเปรียบเทียบข้อมูลที่ป้อนกับแบบสอบถาม

4. ผลการวิจัย

4.1 ลักษณะประชากรศาสตร์

ผลจากการขอความร่วมมือในการตอบแบบสอบถามจากบริษัทที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย จำนวน 448 บริษัท พบว่าแบบสอบถามกระดาษได้รับการตอบกลับจำนวน 314 ชุด คิดเป็นอัตราผลตอบกลับที่สามารถใช้ทดสอบผลการวิจัยได้ร้อยละ 70.09 โดยบริษัทที่ตอบกลับประกอบด้วย 8 กลุ่ม ดังนี้

กลุ่มที่ 1 กลุ่มธุรกิจบริการ ได้รับแบบสอบถามที่ตอบกลับมาซึ่งสามารถนำมาวิเคราะห์ข้อมูลทางสถิติได้จำนวน 67 ชุด หรือร้อยละ 21.34 ของแบบสองถามที่ตอบกลับ

กลุ่มที่ 2 กลุ่มสินค้าอุตสาหกรรม ได้รับแบบสอบถามที่ตอบกลับมาซึ่งสามารถนำมาวิเคราะห์ข้อมูลทางสถิติได้จำนวน 63 ชุด หรือ ร้อยละ 20.06 ของแบบสองถามที่ตอบกลับ

กลุ่มที่ 3 กลุ่มอสังหาริมทรัพย์และก่อสร้าง ได้รับแบบสอบถามที่ตอบกลับมาซึ่งสามารถนำมาวิเคราะห์ข้อมูลทางสถิติได้จำนวน 59 ชุด หรือร้อยละ 18.79 ของแบบสองถามที่ตอบกลับ

กลุ่มที่ 4 กลุ่มธุรกิจการเงิน ได้รับแบบสอบถามที่ตอบกลับมาซึ่งสามารถนำมาวิเคราะห์ข้อมูลทางสถิติได้จำนวน 34 ชุด หรือร้อยละ 10.83 ของแบบสองถามที่ตอบกลับ

กลุ่มที่ 5 กลุ่มเทคโนโลยี ได้รับแบบสอบถามที่ตอบกลับมาซึ่งสามารถนำมาวิเคราะห์ข้อมูลทางสถิติได้จำนวน 29 ชุด หรือร้อยละ 9.23 ของแบบสองถามที่ตอบกลับ

กลุ่มที่ 6 กลุ่มเกษตรและอุตสาหกรรมอาหาร ได้รับแบบสอบถามที่ตอบกลับมาซึ่งสามารถนำมาวิเคราะห์ข้อมูลทางสถิติได้จำนวน 28 ชุด หรือร้อยละ 8.92 ของแบบสองถามที่ตอบกลับ

กลุ่มที่ 7 กลุ่มสินค้าอุปโภคบริโภค ได้รับแบบสอบถามที่ตอบกลับมาซึ่งสามารถนำมาวิเคราะห์ข้อมูลทางสถิติได้จำนวน 27 ชุด หรือร้อยละ 8.60 ของแบบสองถามที่ตอบกลับ

กลุ่มที่ 8 กลุ่มทรัพยากร ได้รับแบบสอบถามที่ตอบกลับมาซึ่งสามารถนำมาวิเคราะห์ข้อมูลทางสถิติได้จำนวน 7 ชุด หรือร้อยละ 2.23 ของแบบสองถามที่ตอบกลับ

4.2 วิธีการฝึกอบรมพนักงานในแผนกเทคโนโลยีสารสนเทศ

วิธีการฝึกอบรมที่บริษัทส่วนใหญ่เลือกใช้ในการพัฒนาองค์ความรู้ของบุคลากรทางด้านเทคโนโลยีสารสนเทศดังตารางที่ 3 ถึงตารางที่ 4 ซึ่งพบว่าวิธีการฝึกอบรมอันดับแรกคือ การฝึกอบรมแบบการบรรยาย เพื่อพัฒนาบุคลากรให้มีทักษะทางด้านเทคโนโลยี ได้แก่ ทักษะการเขียนโปรแกรมคอมพิวเตอร์ ทักษะด้านระบบฐานข้อมูล ทักษะด้านซอฟต์แวร์ ทักษะด้านฮาร์ดแวร์ ทักษะด้านระบบเครือข่าย ทักษะด้านระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และทักษะการบริหารโครงการระบบสารสนเทศ รองลงมาเป็น วิธีการฝึกอบรมแบบการอภิปราย เพื่อเพิ่มทักษะด้านการจัดการและทักษะด้านกลยุทธ์ ได้แก่ ทักษะการพัฒนาระบบสารสนเทศ ทักษะการบริหารการให้บริการระบบสารสนเทศ ทักษะการตรวจสอบระบบสารสนเทศ ทักษะการวางแผนระบบสารสนเทศเชิงกลยุทธ์ และทักษะการบริหารระบบสารสนเทศเชิงกลยุทธ์ สำหรับทักษะการคิด และทักษะการทำงานเป็นทีมนั้นบริษัทส่วนใหญ่เลือกใช้วิธีการฝึกอบรมแบบการใช้สถานการณ์จำลอง ส่วนทักษะในการสื่อสารจะเลือกใช้วิธีการฝึกอบรมแบบการฝึกปฏิบัติ

โดยภาพรวมแสดงให้เห็นว่าบริษัทส่วนใหญ่เน้นการพัฒนาองค์ความรู้ของบุคลากรให้เพิ่มมากขึ้นโดยมุ่งเน้นที่การพัฒนาแนวคิดมากกว่าการปฏิบัติงานจริง เนื่องจากวิธีการฝึกอบรมแบบการบรรยายและการอภิปรายเป็นเทคนิคที่ใช้ในการถ่ายทอดความรู้ ตลอดจนข้อมูล ข้อเท็จจริงให้แก่ผู้เข้ารับการฝึกอบรม เพื่อให้ผู้เข้ารับการฝึกอบรมมีแนวคิดและความคิดเห็นในหัวข้อการฝึกอบรมจากผู้ทำการฝึกอบรมได้ง่ายขึ้น

ตารางที่ 3 ร้อยละที่แต่ละบริษัทเลือกใช้วิธีการฝึกอบรมพนักงานในแผนกเทคโนโลยีสารสนเทศ

วิธีการฝึกอบรม / ทักษะ	การฝึกอบรมในขณะปฏิบัติงาน	การฝึกอบรมแบบการบรรยาย	การฝึกอบรมแบบการอภิปราย	การฝึกอบรมแบบเรียนรู้ด้วยตัวเอง	การฝึกอบรมแบบการให้คำปรึกษา	การฝึกอบรมแบบการสาธิต	การฝึกอบรมแบบการฝึกปฏิบัติ	การฝึกอบรมแบบการใช้กรณีศึกษา	การฝึกอบรมแบบการแสดงบทบาทสมมุติ	การฝึกอบรมแบบการใช้สถานการณ์จำลอง
ทักษะพื้นฐาน										
ทักษะการคิด	2.23%	16.88%	13.06%	1.59%	3.82%	-	10.19%	14.33%	7.96%	29.94%
ทักษะการทำงานเป็นทีม	-	11.78%	9.55%	-	3.82%	-	7.64%	2.23%	26.43%	38.54%
ทักษะในการสื่อสาร	-	27.71%	11.78%	4.78%	0.64%	-	43.95%	-	3.82%	7.32%
ทักษะทางด้านเทคโนโลยี										
ทักษะการเขียนโปรแกรมคอมพิวเตอร์	6.38%	32.21%	11.74%	2.35%	3.02%	12.42%	31.88%	-	-	-
ทักษะด้านระบบฐานข้อมูล	11.95%	42.32%	18.43%	2.39%	5.12%	14.68%	3.41%	1.71%	-	-
ทักษะด้านซอฟต์แวร์	30.25%	36.31%	5.41%	13.69%	3.50%	7.96%	2.87%	-	-	-
ทักษะด้านฮาร์ดแวร์	22.71%	26.44%	2.37%	17.29%	4.75%	6.44%	15.25%	2.03%	-	2.71%
ทักษะด้านระบบเครือข่าย	16.78%	31.51%	20.89%	1.71%	1.71%	8.56%	14.73%	1.71%	-	2.40%
ทักษะด้านระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	10.96%	36.99%	32.53%	-	6.51%	2.40%	3.42%	3.08%	-	4.11%

ตารางที่ 3 ร้อยละที่แต่ละบริษัทเลือกใช้วิธีการฝึกอบรมพนักงานในแผนกเทคโนโลยีสารสนเทศ (ต่อ)

วิธีการฝึกอบรม / ทักษะ	การฝึกอบรมในขณะปฏิบัติงาน	การฝึกอบรมแบบการบรรยาย	การฝึกอบรมแบบการอภิปราย	การฝึกอบรมแบบเรียนรู้ด้วยตัวเอง	การฝึกอบรมแบบการให้คำปรึกษา	การฝึกอบรมแบบการสาธิต	การฝึกอบรมแบบการฝึกปฏิบัติ	การฝึกอบรมแบบการใช้กรณีศึกษา	การฝึกอบรมแบบการแสดงบทบาทสมมุติ	การฝึกอบรมแบบการใช้สถานการณ์จำลอง
ทักษะด้านการจัดการ										
ทักษะการบริหารโครงการระบบสารสนเทศ	9.73%	31.54%	27.52%	-	13.09%	-	0.67%	17.45%	-	-
ทักษะการพัฒนาระบบสารสนเทศ	5.02%	23.75%	32.78%	-	8.36%	3.01%	9.03%	18.06%	-	-
ทักษะการบริหารการให้บริการระบบสารสนเทศ	15.69%	23.86%	33.33%	-	4.90%	0.65%	5.56%	16.01%	-	-
การตรวจสอบระบบสารสนเทศ	5.52%	19.81%	31.82%	-	17.53%	3.25%	4.55%	8.12%	-	9.42%
ทักษะด้านกลยุทธ์										
ทักษะการวางแผนระบบสารสนเทศเชิงกลยุทธ์	-	24.66%	29.45%	-	14.73%	-	7.53%	11.99%	-	11.64%
ทักษะการบริหารระบบสารสนเทศเชิงกลยุทธ์	-	25.34%	28.08%	-	15.41%	-	7.19%	12.67%	-	11.30%

ตารางที่ 4 ลำดับของการเลือกใช้วิธีการฝึกอบรมพนักงานในแผนกเทคโนโลยีสารสนเทศ

วิธีการฝึกอบรม / ทักษะ	การฝึกอบรมในขณะปฏิบัติงาน	การฝึกอบรมแบบการบรรยาย	การฝึกอบรมแบบการอภิปราย	การฝึกอบรมแบบเรียนรู้ด้วยตัวเอง	การฝึกอบรมแบบการให้คำปรึกษา	การฝึกอบรมแบบการสาธิต	การฝึกอบรมแบบการฝึกปฏิบัติ	การฝึกอบรมแบบการใช้กรณีศึกษา	การฝึกอบรมแบบการแสดงบทบาทสมมุติ	การฝึกอบรมแบบการใช้สถานการณ์จำลอง
ทักษะพื้นฐาน										
ทักษะการคิด		2						3		1
ทักษะการทำงานเป็นทีม		3							2	1
ทักษะในการสื่อสาร		2	3				1			
ทักษะทางด้านเทคโนโลยี										
ทักษะการเขียนโปรแกรมคอมพิวเตอร์		1				3	2			
ทักษะด้านระบบฐานข้อมูล		1	2			3				
ทักษะด้านซอฟต์แวร์	2	1		3						
ทักษะด้านฮาร์ดแวร์	2	1		3						
ทักษะด้านระบบเครือข่าย	3	1	2							
ทักษะด้านระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	3	1	2							

ตารางที่ 4 ลำดับของการเลือกใช้วิธีการฝึกอบรมพนักงานในแผนกเทคโนโลยีสารสนเทศ (ต่อ)

วิธีการฝึกอบรม / ทักษะ	การฝึกอบรมในขณะปฏิบัติงาน	การฝึกอบรมแบบการบรรยาย	การฝึกอบรมแบบการอภิปราย	การฝึกอบรมแบบเรียนรู้ด้วยตัวเอง	การฝึกอบรมแบบการให้คำปรึกษา	การฝึกอบรมแบบการสาธิต	การฝึกอบรมแบบการฝึกปฏิบัติ	การฝึกอบรมแบบการใช้กรณีศึกษา	การฝึกอบรมแบบการแสดงบทบาทสมมุติ	การฝึกอบรมแบบการใช้สถานการณ์จำลอง
ทักษะด้านการจัดการ										
ทักษะการบริหารโครงการระบบสารสนเทศ		1	2					3		
ทักษะการพัฒนาระบบสารสนเทศ		2	1					3		
ทักษะการบริหารการให้บริการระบบสารสนเทศ		2	1					3		
การตรวจสอบระบบสารสนเทศ		2	1		3					
ทักษะด้านกลยุทธ์										
ทักษะการวางแผนระบบสารสนเทศเชิงกลยุทธ์		2	1		3					
ทักษะการบริหารระบบสารสนเทศเชิงกลยุทธ์		2	1		3					

ตารางที่ 5 วิธีการฝึกอบรมที่บริษัทเลือกใช้ในการฝึกอบรมจริงและวิธีการฝึกอบรมที่ควรนำมาใช้ในการฝึกอบรมพนักงานในแผนกเทคโนโลยีสารสนเทศ

วิธีการฝึกอบรม / ทักษะ	การฝึกอบรมในขณะปฏิบัติงาน	การฝึกอบรมแบบการบรรยาย	การฝึกอบรมแบบการอภิปราย	การฝึกอบรมแบบเรียนรู้ด้วยตัวเอง	การฝึกอบรมแบบการให้คำปรึกษา	การฝึกอบรมแบบการสาธิต	การฝึกอบรมแบบการฝึกปฏิบัติ	การฝึกอบรมแบบการใช้กรณีศึกษา	การฝึกอบรมแบบการแสดงบทบาทสมมุติ	การฝึกอบรมแบบการใช้สถานการณ์จำลอง
ทักษะพื้นฐาน										
ทักษะการคิด		▲						● ▲	●	● ▲
ทักษะการทำงานเป็นทีม		▲							● ▲	● ▲
ทักษะในการสื่อสาร		▲	▲				● ▲			
ทักษะทางด้านเทคโนโลยี										
ทักษะการเขียนโปรแกรมคอมพิวเตอร์		● ▲				● ▲	● ▲			
ทักษะด้านระบบฐานข้อมูล		● ▲	▲			● ▲				
ทักษะด้านซอฟต์แวร์	● ▲	● ▲		● ▲		●				
ทักษะด้านฮาร์ดแวร์	● ▲	● ▲		● ▲						
ทักษะด้านระบบเครือข่าย	● ▲	● ▲	▲			●				
ทักษะด้านระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	▲	● ▲	● ▲							

ตารางที่ 5 วิธีการฝึกอบรมที่บริษัทเลือกใช้ในการฝึกอบรมจริงและวิธีการฝึกอบรมที่ควรนำมาใช้ในการฝึกอบรมพนักงานในแผนกเทคโนโลยีสารสนเทศ (ต่อ)

วิธีการฝึกอบรม / ทักษะ	การฝึกอบรมในขณะปฏิบัติงาน	การฝึกอบรมแบบการบรรยาย	การฝึกอบรมแบบการอภิปราย	การฝึกอบรมแบบเรียนรู้ด้วยตัวเอง	การฝึกอบรมแบบการให้คำปรึกษา	การฝึกอบรมแบบการสาธิต	การฝึกอบรมแบบการฝึกปฏิบัติ	การฝึกอบรมแบบการใช้กรณีศึกษา	การฝึกอบรมแบบการแสดงบทบาทสมมุติ	การฝึกอบรมแบบการใช้สถานการณ์จำลอง
ทักษะด้านการจัดการ										
ทักษะการบริหารโครงการระบบสารสนเทศ		▲	● ▲					● ▲		
ทักษะการพัฒนาระบบสารสนเทศ		▲	● ▲					● ▲		
ทักษะการบริหารการให้บริการระบบสารสนเทศ		▲	● ▲					● ▲		
การตรวจสอบระบบสารสนเทศ		▲	● ▲		● ▲			●		●
ทักษะด้านกลยุทธ์										
ทักษะการวางแผนระบบสารสนเทศเชิงกลยุทธ์		▲	● ▲		▲			●		●
ทักษะการบริหารระบบสารสนเทศเชิงกลยุทธ์		▲	● ▲		▲			●		●

● วิธีการฝึกอบรมที่แนะนำให้เลือกใช้ในการฝึกอบรม ▲ วิธีการฝึกอบรมที่บริษัทเลือกใช้ในการฝึกอบรมจริง

สำหรับวิธีการฝึกอบรมที่บริษัทเลือกใช้ในการฝึกอบรมจริงเมื่อเทียบกับวิธีการฝึกอบรมที่ควรนำมาใช้ในการฝึกอบรมพนักงานในแผนกเทคโนโลยีสารสนเทศ ดังแสดงในตารางที่ 5 ซึ่งสรุปแยกตามกลุ่มทักษะต่างๆ ได้ดังนี้

(1) กลุ่มทักษะพื้นฐาน ประกอบด้วยทักษะการคิด การทำงานเป็นทีม และการสื่อสาร ซึ่งบริษัทส่วนใหญ่เลือกใช้วิธีการฝึกอบรมตามที่แนะนำในวิธีการฝึกอบรมที่ควรนำมาใช้ คือ การฝึกอบรมแบบการใช้กรณีศึกษา การใช้สถานการณ์จำลอง การฝึกปฏิบัติ และการแสดงบทบาทสมมุติ เพื่อให้ผู้เข้ารับการฝึกอบรมได้ปรับเปลี่ยนทัศนคติ และค่านิยม แต่ยังมีบางบริษัทที่ให้ความสำคัญกับการฝึกอบรมภาคทฤษฎี โดยเฉพาะการฝึกอบรมทักษะในการสื่อสารที่จำเป็นต้องอาศัยการเรียนรู้ทั้งภาคทฤษฎีและการฝึกปฏิบัติควบคู่กันด้วย

(2) กลุ่มทักษะทางด้านเทคโนโลยี ประกอบด้วยทักษะการเขียนโปรแกรมคอมพิวเตอร์ ระบบฐานข้อมูล ซอฟแวร์ ฮาร์ดแวร์ ระบบเครือข่าย และระบบรักษาความปลอดภัยของระบบสารสนเทศ ซึ่งบริษัทส่วนใหญ่เลือกใช้วิธีการฝึกอบรมตามที่แนะนำในวิธีการฝึกอบรมที่ควรนำมาใช้ทั้งการเรียนรู้ภาคทฤษฎีและการฝึกปฏิบัติ ได้แก่ การฝึกอบรมในขณะปฏิบัติงาน การบรรยาย การอภิปราย การเรียนรู้ด้วยตนเอง การสาธิต และการฝึกปฏิบัติ แต่วิธีการฝึกอบรมตามที่แนะนำให้เลือกแบบสาธิตเพื่อเพิ่มทักษะด้านซอฟ์แวร์และระบบเครือข่ายนั้น ไม่มีบริษัทใดเลือกใช้ในการฝึกอบรมจริง

(3) กลุ่มทักษะด้านการจัดการ ประกอบด้วยทักษะการบริหารโครงการระบบสารสนเทศ การพัฒนาระบบสารสนเทศ การบริหารการให้บริการระบบสารสนเทศ และการตรวจสอบระบบสารสนเทศ ซึ่งบริษัทส่วนใหญ่เลือกใช้วิธีการฝึกอบรมตามที่แนะนำในวิธีการฝึกอบรมที่ควรนำมาใช้ คือ การฝึกอบรมแบบอภิปราย การให้คำปรึกษา และการใช้กรณีศึกษา แต่ยังมีบางบริษัทที่เห็นว่าควรเพิ่มพูนความรู้ด้วยการบรรยายด้วย นอกจากนี้วิธีการฝึกอบรมที่แนะนำให้เลือกแบบกรณีศึกษา และการใช้สถานการณ์จำลองสำหรับการตรวจสอบระบบสารสนเทศไม่มีบริษัทใดเลือกใช้ในการฝึกอบรมจริง

(4) กลุ่มทักษะด้านกลยุทธ์ ประกอบด้วยทักษะการวางแผนและการบริหารระบบสารสนเทศเชิงกลยุทธ์ ซึ่งทุกบริษัทจะเน้นการเพิ่มพูนความรู้เพียงอย่างเดียวด้วยการฝึกอบรมแบบการอภิปรายตามที่แนะนำ นอกจากนี้ยังมีการฝึกอบรมจริงด้วยวิธีการบรรยายและการให้คำปรึกษา โดยไม่เลือกใช้การฝึกอบรมแบบกรณีศึกษาและสถานการณ์จำลองตามที่แนะนำ

5. สรุปผลการวิจัย

5.1 อภิปรายผลการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาวิธีการฝึกอบรมที่เหมาะสมในการนำมาใช้พัฒนาทักษะของบุคคลากรทางด้านเทคโนโลยีสารสนเทศ ที่บุคลากรพึงมีในการปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศ ซึ่งประกอบด้วย ทักษะการคิด ทักษะการทำงานเป็นทีม ทักษะในการสื่อสาร ทักษะการเขียนโปรแกรมคอมพิวเตอร์ ทักษะด้านระบบฐานข้อมูล ทักษะด้านซอฟต์แวร์ ทักษะด้านฮาร์ดแวร์ ทักษะด้านระบบเครือข่าย ทักษะด้านระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ทักษะการบริหารโครงการระบบสารสนเทศ ทักษะการพัฒนาระบบสารสนเทศ ทักษะการบริหารการให้บริการระบบสารสนเทศ ทักษะการตรวจสอบระบบสารสนเทศ ทักษะการวางแผนระบบสารสนเทศเชิงกลยุทธ์ และทักษะการบริหารระบบสารสนเทศเชิงกลยุทธ์ โดยการฝึกอบรมที่ดีจะสามารถเพิ่มประสิทธิภาพของบุคลากร ซึ่งเท่ากับเป็นการเพิ่มผลผลิตให้กับองค์กร และยังทำให้องค์กรได้ประโยชน์อย่างเต็มที่จากความสามารถของบุคลากร (Blanchard & Thacker, 2007; ชูชัย สมิทธิไกร, 2544)

ผลจากการสำรวจขั้นต้นที่ทำการศึกษาในวิธีการฝึกอบรมที่บริษัทนำมาใช้ทำการฝึกอบรมให้แก่บุคลากรทางด้านเทคโลยีสารสนเทศแสดงให้เห็นว่าบริษัทเลือกใช้วิธีฝึกอบรมแบบการบรรยายเป็นอันดับแรกสำหรับการเพิ่มพูนความรู้จำนวน 7 ทักษะ จากทักษะทั้งหมด 15 ทักษะ ซึ่งประกอบด้วย ทักษะการเขียนโปรแกรมคอมพิวเตอร์ ทักษะด้านระบบฐานข้อมูล ทักษะด้านซอฟต์แวร์ ทักษะด้านฮาร์ดแวร์ ทักษะด้านระบบเครือข่าย ทักษะด้านระบบรักษาความ

มั่นคงปลอดภัยของระบบสารสนเทศ และทักษะการบริหารโครงการระบบสารสนเทศ รองลงมาเป็นการฝึกอบรมแบบการอภิปราย เพื่อเพิ่มทักษะในด้านทักษะการพัฒนาระบบสารสนเทศ ทักษะการบริหารการให้บริการระบบสารสนเทศ ทักษะการตรวจสอบระบบสารสนเทศ ทักษะการวางแผนระบบสารสนเทศเชิงกลยุทธ์ และทักษะการบริหารระบบสารสนเทศเชิงกลยุทธ์ สำหรับทักษะการคิด และทักษะการทำงานเป็นทีมนั้น บริษัทส่วนใหญ่เลือกใช้วิธีการฝึกอบรมแบบการใช้สถานการณ์จำลอง นอกจากนี้ยังเลือกใช้การฝึกอบรมแบบการฝึกปฏิบัติสำหรับทักษะในการสื่อสาร โดยภาพรวมสามารถแสดงให้เห็นถึงความต้องการของบริษัทในการดำเนินการฝึกอบรมเพื่อพัฒนาบุคลากรในการเพิ่มทักษะในงานทางด้านเทคโนโลยีสารสนเทศของบริษัทต่างๆ ซึ่งจะเน้นการพัฒนาองค์ความรู้ของบุคลากรให้เพิ่มมากขึ้น โดยมุ่งเน้นที่การพัฒนาแนวคิดมากกว่าการปฏิบัติงานจริง เนื่องจากวิธีการฝึกอบรมแบบการบรรยายและวิธีการฝึกอบรมแบบการอภิปรายที่บริษัทเลือกใช้ส่วนมากนั้น ทั้ง 2 วิธีเป็นเทคนิคที่ใช้ในการถ่ายทอดความรู้ ตลอดจนข้อมูลข้อเท็จจริงให้แก่ผู้เข้ารับการฝึกอบรม เพื่อให้ผู้เข้ารับการฝึกอบรมมีแนวคิดและความคิดเห็นในหัวข้อการฝึกอบรมจากผู้ทำการฝึกอบรม

เมื่อนำวิธีการฝึกอบรมที่แนะนำให้ใช้ในการฝึกอบรมแก่บุคลากรทางด้านเทคโนโลยีสารสนเทศมาเทียบกับการปฏิบัติจริงของกลุ่มบริษัท พบว่าในการปฏิบัติจริงส่วนใหญ่มีการเลือกใช้วิธีการฝึกอบรมเพื่อให้บุคคลากรทางด้านเทคโนโลยีสารสนเทศมีการพัฒนาทักษะในด้านต่างๆ ตามวิธีการฝึกอบรมที่ได้มีการแนะนำ และยังมีวิธีการฝึกอบรมบางวิธีที่ควรนำมาใช้แต่ยังไม่เป็นที่นิยมในการเลือกใช้

5.2 ข้อเสนอแนะในเชิงปฏิบัติ

ผู้ที่เกี่ยวข้องกับการฝึกอบรมบุคลากรทางด้านเทคโนโลยีสารสนเทศสามารถนำผลการสำรวจไปใช้ เพื่อให้บุคลากรทางด้านเทคโนโลยีสารสนเทศมีทักษะตามลักษณะงานทางด้านเทคโนโลยีสารสนเทศตามหน้าที่ความรับผิดชอบในการทำงานได้ โดยพิจารณาจากวิธีการฝึกอบรมที่องค์กรเลือกใช้และควรนำมาใช้ตามข้อดีและข้อเสียของวิธีการฝึกอบรมดังนี้

(1) การเสริมสร้างทักษะพื้นฐาน ควรใช้วิธีการฝึกอบรมประกอบด้วย การฝึกอบรมแบบการฝึกปฏิบัติ การฝึกอบรมแบบการใช้กรณีศึกษา การฝึกอบรมแบบการแสดงบทบาทสมมุติ และการฝึกอบรมแบบการใช้สถานการณ์จำลอง

(2) การเสริมสร้างทักษะด้านเทคโนโลยี ควรใช้วิธีการฝึกอบรมประกอบด้วย การฝึกอบรมในขณะปฏิบัติงาน การฝึกอบรมแบบการบรรยาย การฝึกอบรมแบบอภิปราย การฝึกอบรมแบบเรียนรู้ด้วยตัวเอง การฝึกอบรมแบบสาธิต และการฝึกอบรมแบบการฝึกปฏิบัติ

(3) การเสริมสร้างทักษะด้านการจัดการ ควรใช้วิธีการฝึกอบรมประกอบด้วย การฝึกอบรมแบบอภิปราย การฝึกอบรมแบบให้คำปรึกษา และการฝึกอบรมแบบการใช้กรณีศึกษา

(4) การเสริมสร้างทักษะด้านกลยุทธ์ ควรใช้วิธีการฝึกอบรมประกอบด้วย การฝึกอบรมแบบอภิปราย การ

5.3 ข้อเสนอแนะสำหรับงานวิจัยต่อเนื่อง

การศึกษานี้เป็นเพียงการสำรวจเบื้องต้น โดยมีจุดมุ่งหมายหลัก คือ ศึกษาวิธีการฝึกอบรมที่เหมาะสมในการพัฒนาทักษะของบุคคลากรทางด้านเทคโนโลยีสารสนเทศในทักษะด้านต่างๆ ที่พึงมีในการปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศเทียบกับวิธีการฝึกอบรมจริงขององค์กรต่างๆ ในปัจจุบัน ซึ่งไม่สามารถอธิบายถึงปัจจัยที่เกี่ยวข้องทั้งหมดที่มีผลต่อองค์กรในการตัดสินใจเลือกใช้วิธีการฝึกอบรมที่ใช้อยู่ในปัจจุบันได้ ดังนั้นงานวิจัยต่อเนื่องอาจจัดทำกรอบแนวคิดการวิจัยเพื่อศึกษาปัจจัยที่ส่งผลต่อการเลือกใช้วิธีการฝึกอบรมนั้นๆ

บรรณานุกรม

ชูชัย สมิทธิไกร. (2544). *การฝึกอบรมบุคลากรในองค์การ.* กรุงเทพมหานคร: สำนักพิมพ์แห่งจุฬาลงกรณ์.

บรรยงค์ โตจินดา. (2543). *การบริหารงานบุคคล.* กรุงเทพมหานคร: อมรการพิมพ์.

Blanchard, P., & Thacker, J. (2007). *Effective training: systems, strategies, and practices*. Englewood Cliffs, NJ : Prentice Hall.

McKeen, J., & Smith, H. (2007). Delivering IT Functions: A Decision Framework. *Communications of the Association for Information Systems*, 2(19), 725-739.

Todd, P., McKeen, J., & Gallupe, R. (1995). The Evolution of IS Job Skills: A Content Analysis of IS Job Advertisements from 1970 to1990. *MIS Quarterly*, 19(1), 1-27.

การศึกษาปัจจัยที่มีอิทธิพลต่อการสร้างแรงจูงใจในการสร้างองค์ความรู้ใหม่ในระบบการจัดการความรู้ขององค์การ

เมธาวี ไชยศิลป์*

บริษัทดีเอสที ไฟแนนเชียล เซอร์วิสเซส อินเตอรเนชั่นแนล ลิมิเต็ด

***Correspondence:** chaisilpbeam@gmail.com
doi: 10.14456/jisb.2018.17

วันที่รับบทความ: 15 มี.ค. 2561 วันแก้ไขบทความ: 20 เม.ย. 2561 วันตอบรับบทความ: 4 พ.ค. 2561

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่มีอิทธิพลต่อกิจกรรมเฉพาะทางด้านการนำความรู้ออกมาเพื่อสร้างองค์ความรู้ใหม่ขององค์การ โดยนำทฤษฎีการกระทำด้วยเหตุผล (The Theory of Reasoned Action: TRA) ตัวแบบความสำเร็จของระบบสารสนเทศ (Delone & Mclean's Model) และตัวแบบในการสร้างความรู้ของ Nonaka (SECI Model) ร่วมกับการทบทวนวรรณกรรมที่เกี่ยวข้องเพื่อกำหนดกรอบแนวคิดในการวิจัย ดำเนินการเก็บข้อมูลด้วยแบบสอบถามออนไลน์กับกลุ่มตัวอย่างที่เป็นบุคคลากรในองค์การที่มีการใช้ระบบการจัดการความรู้จำนวน 138 ราย ผลการวิจัยพบว่า ปัจจัยที่มีอิทธิพลต่อการสร้างแรงจูงใจในการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ขององค์การ ประกอบด้วย ปัจจัยด้านองค์การ และปัจจัยด้านบุคคล โดยปัจจัยทั้งสองจะมีอิทธิพลต่อปัจจัยด้านการใช้ระบบการจัดการความรู้ และปัจจัยด้านความตั้งใจในการแบ่งปันความรู้ ซึ่งมีอิทธิพลต่อการสร้างแรงจูงใจในการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ขององค์การอย่างมีนัยสาคัญ ส่วนปัจจัยด้านเทคโนโลยีนั้น ไม่มีอิทธิพลต่อปัจจัยด้านการใช้ระบบการจัดการความรู้ และปัจจัยด้านความตั้งใจในการแบ่งปันความรู้ จึงไม่มีอิทธิพลต่อการสร้างแรงจูงใจในการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ขององค์การ

คำสำคัญ: ระบบการจัดการความรู้ การสร้างองค์ความรู้ใหม่ ความรู้โดยนัย

A Study on Factors Influencing the Intention to Create New Knowledge into Knowledge Management System of the Organization

Metawee Chaisilp*

DST Financial Services International Limited

***Correspondence:** chaisilpbeam@gmail.com

doi: 10.14456/jisb.2018.17

Received: 15 Mar 2018 Revised: 20 Apr 2018 Accepted: 4 May 2018

Abstract

The objective of this study is to examine the factors influencing the specific activities of knowledge acquisition to create new knowledge into Knowledge Management System of the organization. This research integrated The Theory of Reasoned Action (TRA), Delone & Mclean's Model and SECI Model along with associated literature reviews for determining research model. The study uses an online survey to collect the information from a total of 138 questionnaires among representative employees who work in the organization that currently has procedures about knowledge management system. The study results showed that the factors which influence motivation to create new knowledge into Knowledge Management System of the organization consist of organizational factor and individual factor. According to those two factors, they influence other factors including KMS usage and intention to share knowledge. These two factors influence motivation to create new knowledge into Knowledge Management System of the organization significantly. In contrast, the technological factor does not have an influence on KMS usage and intention to share knowledge factors. Thus it does not influence the motivation to create new knowledge into Knowledge Management System.

Keywords: Knowledge management system, Creation knowledge, Tacit knowledge

1. บทนำ

1.1 ความสำคัญและที่มาของปัญหา

ปัจจุบันความรู้มีบทบาทสำคัญที่ช่วยผลักดันให้องค์การประสบความสำเร็จ และส่งผลกระทบอย่างมากต่อประสิทธิภาพในการดำเนินงานของธุรกิจอย่างยั่งยืน เนื่องจากสภาพแวดล้อมทางธุรกิจในยุคปัจจุบันมีการแข่งขันและมีความไม่แน่นอนมากขึ้นกว่าเดิมจึงเป็นเรื่องที่ท้าทายมากขึ้นสำหรับองค์การที่จะดำเนินงานได้ดีและประสบความสำเร็จ ความรู้ซึ่งได้รับการยอมรับกันอย่างกว้างขวางว่าเป็นแหล่งที่มาหลักของความได้เปรียบในการแข่งขัน จึงเข้ามามีบทบาทสำคัญในการสร้างความสามารถในการแข่งขันที่ยั่งยืนและกลายเป็นสินทรัพย์หลักสำหรับความสำเร็จขององค์การ (Chen & Huang, 2007) ความสามารถพื้นฐานขององค์การ เกิดจากความสามารถในการสร้างความรู้ การรับความรู้ การบูรณาการความรู้ และการใช้ความรู้ที่กระจายออกมาผ่านทางบุคคล ทีมงาน และองค์การ เพื่อการเติบโตและประสบความสำเร็จ แต่ละองค์การจะต้องไม่ใช้ประโยชน์จากความรู้ที่องค์การมีอยู่เท่านั้น แต่ต้องให้ความสำคัญและมีการลงทุนอย่างต่อเนื่องในการค้นหาความรู้ใหม่ไว้สำหรับเป็นทางเลือกในการสร้างกลยุทธ์ขององค์การในอนาคต อีกทั้งยังสามารถใช้ความรู้ใหม่เพื่อสร้างและรักษาความได้เปรียบในการแข่งขันขององค์การไว้อีกด้วย

ความรู้สามารถเป็นได้ทั้งความรู้ที่ชัดแจ้ง (Explicit Knowledge) และความรู้โดยนัย (Tacit Knowledge) (Nonaka, 1994) โดยความรู้ที่ชัดแจ้ง หมายถึง ความรู้ที่สามารถประมวลผลแยกส่วนออกมาแล้วสามารถถ่ายทอดออกมาผ่านการเขียนหรืออธิบายออกมาเป็นตัวอักษรได้ หรือเป็น “สิ่งที่รู้” ที่สามารถสกัดออกมาจากผู้ที่มีความรู้แล้วสามารถแบ่งปันกับบุคคลอื่นได้ แต่ในทางกลับกันความรู้โดยนัยจะเป็นความรู้ส่วนตัว ความรู้ตามประสบการณ์ หรือเป็นการรู้หรือความรู้ที่ฝังรากลึกซึ่งเกิดจากการกระทำในบริบทเฉพาะ จึงทำให้ยากที่จะถ่ายโอนออกมาผ่านการเขียนหรืออธิบายออกมาผ่านภาษาใดภาษาหนึ่ง มีองค์การจำนวนมากที่ประสบปัญหา เมื่อกลุ่มบุคคลที่มีบทบาทต่อความสำเร็จขององค์การได้ออกจากองค์การไปแล้ว ความรู้ความเชี่ยวชาญต่างๆ ที่เคยเป็นส่วนที่สร้างความเข้มแข็งให้กับองค์การก็หายไปด้วย ซึ่งในกรณีนี้จะส่งผลกระทบต่อองค์การอย่างมาก และเมื่อพิจารณาแล้วจะพบว่าปัญหาเหล่านี้ล้วนเป็นเรื่องของการจัดการความรู้ทั้งสิ้น โดยเกิดจากการที่องค์การไม่สามารถเปลี่ยนความรู้ที่มีอยู่ในตัวบุคคลให้กลายมาเป็นความรู้ขององค์การที่สามารถถ่ายทอดให้กับบุคคลอื่นในองค์การได้ (ศรีสมรัก อินทุจันทร์ยง, 2549)

การใช้ระบบการจัดการความรู้ (Knowledge Management Systems) เป็นส่วนหนึ่งของการประยุกต์ใช้ระบบสารสนเทศกับการจัดการความรู้ขององค์การ กล่าวคือ เป็นระบบที่ใช้เทคโนโลยีสารสนเทศเป็นพื้นฐาน ได้รับการพัฒนาขึ้นเพื่อสนับสนุนและพัฒนากระบวนการขององค์การในการสร้างความรู้ เก็บความรู้ เข้าถึงความรู้ ถ่ายโอนความรู้ และการประยุกต์ใช้ความรู้ (Alavi & Leidner, 2001) เพื่อเป็นเครื่องมืออำนวยความสะดวกในกิจกรรมการจัดการความรู้ในองค์การ กลายเป็นสิ่งที่ถูกนำไปใช้อย่างแพร่หลาย เนื่องจากหลายองค์การเชื่อว่าระบบจะช่วยเพิ่มคุณค่าในกระบวนการจัดการความรู้ (Oyefolahan et al., 2012)

จากผลการวิจัยจำนวนมาก พบว่า เทคโนโลยีสารสนเทศมีอิทธิพลเชิงบวกกับการประยุกต์ใช้ความรู้ แต่อย่างไรก็ตามผลการวิจัยก็ยังพบอีกว่า การนำระบบการจัดการความรู้ มาใช้ในองค์การยังไม่ประสบความสำเร็จเท่าที่ควร (Stenmark & Lindgren, 2004) พนักงานส่วนใหญ่จะใช้ระบบการจัดการความรู้เพื่อจัดเก็บความรู้และนำออกมาใช้มากกว่าการเพิ่มความรู้ใหม่หรือแบ่งปันความรู้ใหม่เข้าไป เนื่องจากองค์การไม่ประสบความสำเร็จในการนำเสนอและสร้างแรงจูงใจให้กับพนักงานในการใช้ระบบ (Hoong et al., 2012) ส่งผลให้ความรู้ที่เก็บไว้ไม่ถูกปรับปรุงให้ทันสมัย ไม่มีความสัมพันธ์กัน จำนวนความรู้ลดลง และความตระหนักถึงความรู้ที่สูญเสียไปมีเพิ่มขึ้น (Aggestam & Perrson, 2010) และจากการทบทวนวรรณกรรม พบว่า งานวิจัยส่วนมากจะกล่าวถึงปัจจัยทั่วไปที่นำไปสู่ความสำเร็จของการจัดการความรู้และระบบการจัดการความรู้ แต่ยังขาดข้อมูลเชิงลึกเกี่ยวกับปัจจัยที่มีอิทธิพลต่อกิจกรรมเฉพาะทางด้านการจับความรู้ออกมาเพื่อสร้างองค์ความรู้ใหม่ขององค์การ (Aggestam & Persson, 2010)

ดังนั้นผู้วิจัยจึงเห็นความสำคัญในการศึกษาถึงปัจจัยที่มีอิทธิพลต่อการสร้างแรงจูงใจในการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ขององค์การ เนื่องจากองค์การที่จะประสบความสำเร็จ จะต้องเป็นองค์การที่มีความสามารถ

ในการสร้างสรรค์ความรู้ใหม่และเผยแพร่ความรู้เหล่านั้นไปทั่วทั้งองค์การอยู่เสมอ รวมถึงการนำความรู้เหล่านั้นไปใช้ในการพัฒนาผลิตภัณฑ์ใหม่ ๆ ได้อย่างรวดเร็ว (Nonaka & Takeuchi, 1995) ความรู้จึงเป็นอีกหนึ่งปัจจัยสำคัญที่องค์การสามารถนำมาใช้ในการดำเนินงานเพื่อให้เกิดประโยชน์ในการเพิ่มความสามารถในการแข่งขันขององค์การได้อย่างยั่งยืน

1.2 วัตถุประสงค์ของการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยและระดับอิทธิพลของแต่ละปัจจัยที่มีต่อการสร้างแรงจูงใจในการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ขององค์การ

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

จากการศึกษาทฤษฎี และทบทวนวรรณกรรมที่เกี่ยวข้องกับปัจจัยที่มีอิทธิพลต่อการสร้างแรงจูงใจในการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ขององค์การ ผู้วิจัยได้นำทฤษฎีที่เกี่ยวข้องประกอบด้วย ทฤษฎีการกระทำด้วยเหตุผล (The Theory of Reasoned Action: TRA) ตัวแบบความสำเร็จของระบบสารสนเทศ (Delone & Mclean's Model) และตัวแบบในการสร้างความรู้ของ Nonaka (SECI Model) โดยมีปัจจัยที่มีความสัมพันธ์กับทฤษฎีเหล่านี้ประกอบไปด้วย ปัจจัยด้านองค์การ (Organization) ปัจจัยด้านบุคคล (Individual) ปัจจัยด้านเทคโนโลยี (Technological) ปัจจัยด้านการใช้ระบบการจัดการความรู้ (KMS Usage) ปัจจัยด้านความตั้งใจในการแบ่งปันความรู้ (Intention to share knowledge) และปัจจัยด้านการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ (Creation knowledge to KMS) อธิบายรายละเอียดแต่ละปัจจัยได้ ดังนี้

ปัจจัยทางด้านองค์การ (Organization) ปัจจัยด้านองค์การมีความสัมพันธ์ต่อการใช้ระบบการจัดการความรู้โดยบรรยากาศภายในองค์การ (Organization climate) ที่สนับสนุนให้พนักงานเกิดความคิดริเริ่มสร้างสรรค์ มีการทำงานร่วมกันภายในองค์การ มีรูปแบบโครงสร้างขององค์การ (Organization structure) ที่มีการทำงานแบบบูรณาการร่วมกันระหว่างแผนกงาน มีวัฒนธรรมการสื่อสารภายในองค์การที่เปิดกว้าง มีวัฒนธรรมในองค์การที่สนับสนุนให้พนักงานมีอิสระในการคิดแนวทางการปฏิบัติงานด้วยตนเอง และมีแนวทางในการปฏิบัติงานในองค์การที่เน้นนวัตกรรม (Innovative norm) จะทำให้พนักงานในองค์การเกิดแรงจูงใจในการใช้ระบบการจัดการความรู้ขององค์การโดยอัตโนมัติ (Oyefolahan et al., 2012) นอกจากนี้การให้รางวัล โบนัส หรือการเลื่อนขั้น (Reward of organization) ก็สามารถสร้างแรงจูงใจในการใช้ระบบการจัดการความรู้ขององค์การได้อีกด้วย (Hoong et al., 2012; Kankanhalli et al., 2005)

ปัจจัยด้านองค์การมีความสัมพันธ์ต่อการแบ่งปันความรู้ภายในองค์การ โดยต้นทุนทางสังคมที่ประกอบด้วยเครือข่ายสังคม (Social Network) และการมีเป้าหมายร่วมกันในการทำงาน (Shared goals) มีส่วนสำคัญต่อความตั้งใจของคนที่จะแบ่งปันความรู้ (Intention to share knowledge) อีกทั้งสภาพบรรยากาศภายในองค์การ ที่มีความยุติธรรม (Fairness) มีการติดต่อกันผูกพันกัน (Affiliation) และมีนวัตกรรม (Innovativeness) ก็ยังส่งผลต่อความตั้งใจส่วนบุคคลในการแบ่งปันความรู้ (Intention to share knowledge) อีกด้วย (Bock et al., 2005) นอกจากนี้แล้วองค์การยังสามารถสร้างแรงจูงใจในการแบ่งปันความรู้ได้ โดยการสนับสนุนของผู้บริหารและการให้รางวัลในองค์การ ซึ่งจะมีอิทธิพลอย่างมากต่อพฤติกรรมการแบ่งปันความรู้และการสร้างสรรค์นวัตกรรมของพนักงานในองค์การ (Lee et al., 2010)

ปัจจัยด้านบุคคล (Individual) ปัจจัยด้านบุคคล หมายถึง ลักษณะส่วนบุคคลของพนักงานหรือกลุ่มของพนักงานในองค์การ ซึ่งมีความโน้มเอียงที่จะใช้เทคโนโลยีโดยเฉพาะสำหรับการแบ่งปันความรู้ (Oyefolahan & Dominic, 2011) โดยเมื่อบุคคลเกิดแรงจูงใจในการใช้เทคโนโลยีโดยอัตโนมัติ (Autonomous motivation to technology use) มีความเป็นอิสระในการใช้งานซึ่งจะทำให้เกิดการรับรู้คุณค่าของความรู้ด้วยตนเอง (Knowledge self-worth) มีความมุ่งมั่นในการใช้ระบบการจัดการความรู้และมีความพึงพอใจต่อการใช้ระบบการจัดการความรู้ จะส่งผลโดยตรงต่อการใช้ระบบการจัดการความรู้ในองค์การ อีกทั้งการรับรู้การเข้ากันของงานและเทคโนโลยีและความสามารถในการใช้ระบบการ

จัดการความรู้ของแต่ละบุคคลก็เป็นอีกสองปัจจัยที่จะส่งผลในทางบวกต่อการใช้งานระบบการจัดการความรู้ของผู้ใช้งาน นอกจากนี้แล้วการรับรู้คุณค่าของความรู้ของผู้บริหารระดับสูงซึ่งมีบทบาทสำคัญในการเป็นผู้สนับสนุนให้เกิดการแบ่งปันความรู้ในองค์การ ก็เป็นคุณลักษณะที่มีบทบาทสำคัญที่จะช่วยสนับสนุนให้พนักงานในองค์การใช้ระบบการจัดการความรู้ขององค์การได้อย่างมีประสิทธิภาพ

ปัจจัยด้านบุคคลยังมีอิทธิพลต่อการแบ่งปันความรู้ โดยพนักงานถือว่าเป็นองค์ประกอบที่มีบทบาทสำคัญที่สุดของระบบการจัดการความรู้ (Chen et al., 2012) องค์การสามารถเพิ่มพฤติกรรมการแบ่งปันความรู้ของพนักงานในองค์การได้ โดยผ่านการบริหารจัดการพนักงาน ทำให้พนักงานเกิดทัศนคติที่ดีต่อการแบ่งปันความรู้ และรับรู้บรรทัดฐานในการแบ่งปันความรู้ซึ่งจะส่งผลให้พนักงานเกิดความตั้งใจที่จะแบ่งปันความรู้ ทำให้พฤติกรรมการแบ่งปันความรู้ของพนักงานในองค์การมีมากเพิ่มขึ้น และจากงานวิจัยของ Bock et al. (2005) ซึ่งได้ทำการศึกษาเพื่อหาปัจจัยที่สนับสนุนหรือปัจจัยที่ทำให้เกิดการลดพฤติกรรมการแบ่งปันความรู้ โดยใช้ทฤษฎีการกระทำด้วยเหตุผลเป็นทฤษฎีในการศึกษายังพบอีกว่า ความคาดหวังต่อรางวัลภายนอก (Anticipated extrinsic rewards) ความคาดหวังต่อความสัมพันธ์ซึ่งกันและกัน (Anticipated reciprocal relationships) และการรับรู้คุณค่าของตนเอง (Sense of self-worth) ก็ส่งผลต่อความตั้งใจที่จะแบ่งปันความรู้ (Intention to share knowledge) โดยผ่านทัศนคติในการแบ่งปันความรู้ (Attitude toward knowledge sharing) นอกจากนี้แล้ว ลักษณะส่วนบุคคลในเรื่องของความเต็มใจในการช่วยแบ่งปันความรู้ให้ผู้อื่น (Pleasure of knowledge sharing) การยอมรับและเข้าไปมีส่วนร่วมในกิจกรรมขององค์การ (Agreeableness) การมีจิตใต้สำนึกที่ดีในการทำงาน (Conscientiousness) ความไว้วางใจในเพื่อนร่วมงาน ความคาดหวังต่อรางวัลภายนอก (Anticipated extrinsic rewards) ความคาดหวังต่อความสัมพันธ์ซึ่งกันและกัน (Anticipated reciprocal relationships) และการรับรู้คุณค่าของตนเอง (Sense of self-worth) ต่างก็เป็นปัจจัยด้านบุคคลที่ส่งผลต่อพฤติกรรมการแบ่งปันความรู้ของพนักงานในองค์การเช่นกัน (Lee et al., 2010; Matzler et al., 2011; Ma et al., 2009; Bock et al., 2005)

ปัจจัยทางด้านเทคโนโลยี (Technologies) ปัจจัยทางด้านเทคโนโลยี หมายถึง คุณลักษณะหรือคุณสมบัติของแต่ละนวัตกรรมทางเทคโนโลยีที่สามารถมีอิทธิพลต่อการเลือกใช้นวัตกรรมทางเทคโนโลยีของแต่ละบุคคล โดย DeLone and McLean (1992) ได้แบ่งคุณสมบัติของเทคโนโลยีออกเป็น 2 คุณสมบัติ คือ คุณภาพของระบบ (System quality) และคุณภาพของสารสนเทศ (Information quality) การใช้ระบบการจัดการความรู้ของพนักงานในองค์การจะขึ้นอยู่กับคุณภาพของระบบและคุณภาพของความรู้ หรือสารสนเทศ (Knowledge/information quality) ที่อยู่ในระบบการจัดการความรู้บนความพึงพอใจและการรับรู้ประโยชน์จากการใช้งานระบบการจัดการความรู้ของพนักงานแต่ละคน (Oyefolahan & Dominic, 2010, 2011) อีกทั้งความสอดคล้องของการบูรณาการระบบการจัดการความรู้ (System integration) กับระบบอื่นๆ ภายในองค์การ (Oyefolahan & Dominic, 2010) คุณภาพของการเชื่อมโยง (Linkage quality) ที่มุ่งเน้นเกี่ยวกับวิธีการเชื่อมโยงระบบการจัดการความรู้ให้เกิดประโยชน์ต่อกลุ่มพนักงานมากที่สุด และจำนวนความรู้ของระบบการจัดการความรู้ (Knowledge richness) ที่มุ่งเน้นให้สารบัญความรู้ (Knowledge content) เป็นความรู้ที่สามารถนำไปประยุกต์ใช้กับการทำงานได้ง่ายและเป็นความรู้ที่สามารถนำไปใช้สนับสนุนการตัดสินใจได้ดี ก็เป็นปัจจัยที่มีอิทธิพลต่อการใช้ระบบการจัดการความรู้ของพนักงานในองค์การเช่นเดียวกัน (Oyefolahan et al., 2012)

คุณลักษณะของปัจจัยทางด้านเทคโนโลยียังมีอิทธิพลต่อการแบ่งปันความรู้ของพนักงานในองค์การด้วย จากงานวิจัยของ Chen et al. (2012) ซึ่งได้ทำการศึกษาเพื่อหาปัจจัยที่ส่งผลกระทบทั้งทางตรงและทางอ้อมต่อความตั้งใจในการแบ่งปันความรู้ (Intention to share knowledge) ในกระบวนการพัฒนาผลิตภัณฑ์ใหม่ พบว่านอกจากประสิทธิภาพของระบบการจัดการความรู้ (KMS self-efficacy) จะส่งผลในทางบวกโดยตรงต่อความตั้งใจที่จะแบ่งปันความรู้ (Intention to share knowledge) แล้ว ประสิทธิภาพของระบบการจัดการความรู้ (KMS self-efficacy) ก็ยังส่งผลทางบวกในทางอ้อมต่อความตั้งใจที่จะแบ่งปันความรู้ (Intention to share knowledge) โดยผ่านทัศนคติในการ

แบ่งปันความรู้ในทางบวก (Attitude toward knowledge sharing) นอกจากนี้การใช้ระบบสารสนเทศของพนักงานซึ่งสามารถวัดได้จากระดับของทัศนคติที่มีต่อการใช้เทคโนโลยีในการแบ่งปันความรู้ การรับรู้ความง่ายในการใช้งานระบบสารสนเทศของพนักงาน คุณภาพของระบบที่สูง (System quality) ซึ่งนำไปสู่การรับรู้การแบ่งปันความรู้ในเชิงบวกมากขึ้น ต่างก็เป็นปัจจัยด้านบุคคลที่ส่งผลต่อพฤติกรรมการแบ่งปันความรู้ของพนักงานในองค์การเช่นกัน (Ma et al., 2009; Lee et al., 2010; Kulkarni et al., 2007)

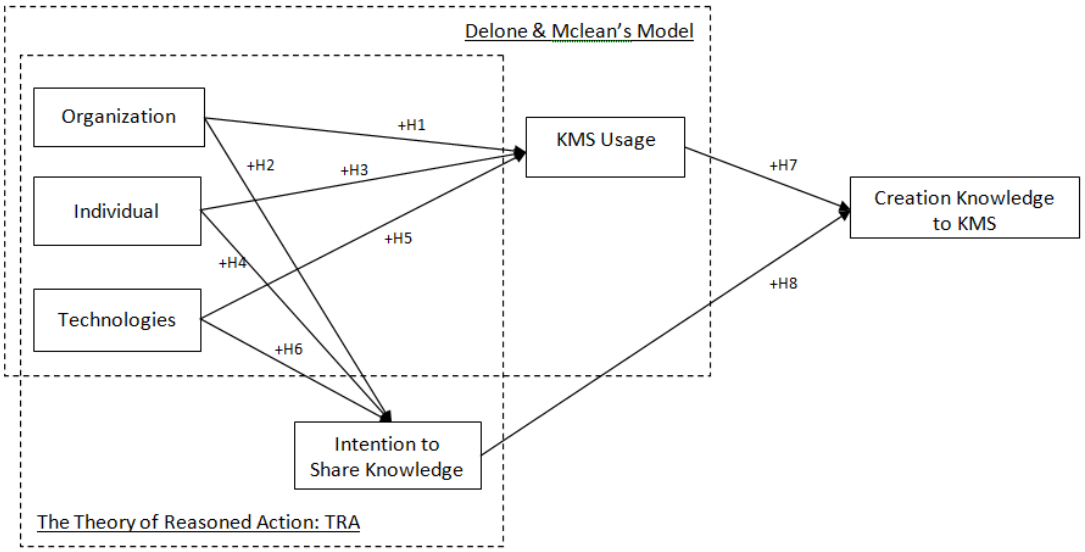
ปัจจัยด้านการใช้ระบบการจัดการความรู้ (KMS usage) การใช้ระบบการจัดการความรู้ คือ การที่พนักงานในองค์การใช้ระบบการจัดการความรู้เป็นเครื่องมืออำนวยความสะดวกในกิจกรรมการจัดการความรู้ภายในองค์การ โดยใช้ในการสร้างความรู้ จัดเก็บความรู้ ดึงความรู้ ถ่ายทอดความรู้ และการประยุกต์ใช้ความรู้ขององค์การ เช่น การนำระบบการจัดการความรู้มาใช้ในการเก็บบทเรียนที่ได้รับ เข้าถึงความเชี่ยวชาญ และสร้างเครือข่ายความรู้ ซึ่งจะทำให้เกิดการถ่ายทอดความรู้ที่ไม่ใช่เฉพาะระหว่างผู้ให้ความรู้และผู้รับความรู้เท่านั้น แต่ยังทำให้เกิดความรู้ใหม่ขึ้นมาผ่านการติดต่อกันในเครือข่ายสังคม (Oyefolahan & Dominic, 2010) อีกทั้งยังนำมาใช้ช่วยในการแลกเปลี่ยนและบูรณาการความรู้โดยนัย กระจายความรู้ชัดแจ้ง และทำให้ความรู้ที่ถูกประมวลผลขึ้นมามีความหมายยิ่งขึ้น โดยการเชื่อมโยงระหว่างผู้ให้ความรู้และผู้รับความรู้ (Oyefolahan & Dominic, 2011) นอกจากนี้แล้ว การใช้ระบบการจัดการความรู้ยังรวมไปถึงการที่พนักงานในองค์การใช้ระบบการจัดการความรู้ช่วยในการตัดสินใจ ช่วยเก็บความรู้ของตัวเอง ใช้ติดต่อสื่อสารความรู้และสารสนเทศกับเพื่อนร่วมงาน ใช้แบ่งปันความรู้ทั่วไป และใช้แบ่งปันความรู้เฉพาะอีกด้วย (Wu & Wang, 2006)

ปัจจัยด้านความตั้งใจในการแบ่งปันความรู้ (Intention to share knowledge) การแบ่งปันความรู้ถือว่าเป็นความตั้งใจของบุคคลที่จะแบ่งปันความรู้ที่บุคคลนั้นสร้างขึ้นมาหรือได้รับมาให้กับเพื่อนร่วมงานในองค์การ (Ma et al., 2009) การแบ่งปันความรู้ คือ กระบวนการที่เป็นระบบของการปฏิสัมพันธ์ระหว่างบุคคลผ่านหน่วยหนึ่งหน่วย เช่น กลุ่มคน แผนก หรือองค์การ เป็นต้น ซึ่งเป็นผลมาจากประสบการณ์ของแต่ละบุคคล หรืออาจกล่าวได้ว่า การแบ่งปันความรู้เป็นกระบวนการที่มีความละเอียดอ่อนและต้องการการมีส่วนร่วมของบุคคล โดยประเภทของการแบ่งปันความรู้นั้น จะขึ้นอยู่กับความแตกต่างของรูปแบบของความรู้หรือประเภทของความรู้ เช่น ความรู้โดยนัยหรือความรู้ชัดแจ้ง เป็นต้น ซึ่งจะทำให้ความยากง่ายของการแบ่งปันความรู้แตกต่างกัน (Matzler et al., 2011) เมื่อเกิดการแบ่งปันความรู้ขึ้นในองค์การ ก็จะทำให้ความรู้ของพนักงานในองค์การถูกปรับปรุงให้มีประสิทธิภาพมากขึ้น โดยความรู้จะถูกแบ่งปันจากองค์การสู่ตัวบุคคล และแบ่งปันจากตัวบุคคลไปยังบุคคลอื่น ซึ่งการแบ่งปันความรู้ไม่เพียงแต่เป็นการส่งต่อความรู้ระหว่างผู้รับและผู้ส่งเท่านั้น แต่ยังรวมไปถึงการสร้างความรู้ใหม่ให้เกิดขึ้นในองค์การอีกด้วย (Oyefolahan & Dominic, 2010)

ปัจจัยด้านการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ (Creation knowledge to KMS) การสร้างองค์ความรู้ในระบบการจัดการความรู้ หมายถึง การที่พนักงานในองค์การสร้างเอกสารความรู้ขึ้นมาในระบบการจัดการความรู้ เพื่อแบ่งปันความรู้ในเครือข่ายความรู้ขององค์การ (Hoong et al., 2012) หรือการสร้างความรู้ใหม่ที่เกิดขึ้นจากกระบวนการจัดการความรู้ขององค์การ ที่ประกอบด้วย 7 ขั้นตอน คือ การบ่งชี้ความรู้ การสร้างและแสวงหาความรู้ การจัดความรู้ให้เป็นระบบ การประมวลและกลั่นกรองความรู้ การเข้าถึงความรู้ การแบ่งปันแลกเปลี่ยนความรู้ และการเรียนรู้ (สำนักงานคณะกรรมการพัฒนาระบบราชการและสถาบันเพิ่มผลผลิตแห่งชาติ, 2548) โดยเอกสารความรู้ที่พนักงานสร้างขึ้นมานั้น เป็นเอกสารความรู้ที่เกิดจากความรู้ใหม่ที่ถูกสร้างผ่านการปฏิสัมพันธ์ระหว่างความรู้โดยนัย (Tacit knowledge) และความรู้ที่ชัดแจ้ง (Explicit knowledge) ตามตัวแบบในการสร้างความรู้ของ Nonaka (1994) ที่ชื่อว่า “SECI” ซึ่งประกอบด้วย “Socialization” การแปลงความรู้โดยนัยผ่านการปฏิสัมพันธ์กันระหว่างบุคคล “Externalization” การแปลงความรู้โดยนัยให้เป็นความรู้ชัดแจ้ง “Combination” การใช้กระบวนการทางสังคมในการรวมความรู้ชัดแจ้งหลายๆ ส่วนที่แตกต่างกันเข้าด้วยกันโดยตัวบุคคล “Internalization” การแปลงความรู้ชัดแจ้งให้เป็นความรู้โดยนัย

3. กรอบแนวคิดการวิจัยและสมมติฐานการวิจัย

จากทฤษฎีและการทบทวนวรรณกรรม ผลงานวิจัยที่เกี่ยวข้องดังกล่าวข้างต้น ผู้วิจัยสามารถกำหนดกรอบแนวคิดในการศึกษาปัจจัยที่มีอิทธิพลต่อการสร้างแรงจูงใจในการสร้างองค์ความรู้ใหม่ในระบบการจัดการความรู้ขององค์การ ดังภาพที่ 1



ภาพที่ 1 ตัวแบบงานวิจัย

ผู้วิจัยได้กำหนดสมมติฐานงานวิจัย ดังนี้

สมมติฐานที่ 1 (H1): ปัจจัยด้านองค์การ (Organization) มีผลเชิงบวกต่อการใช้ระบบการจัดการความรู้ (KMS Usage) ของพนักงานในองค์การ

สมมติฐานที่ 2 (H2): ปัจจัยด้านองค์การ (Organization) มีผลเชิงบวกต่อความตั้งใจในการแบ่งปันความรู้ (Intention to Share Knowledge) ของพนักงานในองค์การ

สมมติฐานที่ 3 (H3): ปัจจัยด้านบุคคล (Individual) มีผลเชิงบวกต่อการใช้ระบบการจัดการความรู้ (KMS Usage) ของพนักงานในองค์การ

สมมติฐานที่ 4 (H4): ปัจจัยด้านบุคคล (Individual) มีผลเชิงบวกต่อความตั้งใจในการแบ่งปันความรู้ (Intention to Share Knowledge) ของพนักงานในองค์การ

สมมติฐานที่ 5 (H5): ปัจจัยด้านเทคโนโลยี (Technologies) มีผลเชิงบวกต่อการใช้ระบบการจัดการความรู้ (KMS Usage) ของพนักงานในองค์การ

สมมติฐานที่ 6 (H6): ปัจจัยด้านเทคโนโลยี (Technologies) มีผลเชิงบวกต่อพฤติกรรมการแบ่งปันความรู้ (Intention to Share Knowledge) ของพนักงานในองค์การ

สมมติฐานที่ 7 (H7): การใช้ระบบการจัดการความรู้ (KMS Usage) มีผลเชิงบวกต่อการสร้างองค์ความรู้ใหม่ในระบบการจัดการความรู้ (Creation Knowledge to KMS)

สมมติฐานที่ 8 (H8): ความตั้งใจในการแบ่งปันความรู้ (Intention to share Knowledge) มีผลเชิงบวกต่อการสร้างองค์ความรู้ใหม่ในระบบการจัดการความรู้ (Creation Knowledge to KMS)

4. วิธีการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงปริมาณโดยใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างที่เป็นพนักงานของกลุ่มบริษัทที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย โดยไม่รวมกลุ่มบริษัทที่อยู่ในหมวดบริษัทจดทะเบียนที่อยู่ระหว่างฟื้นฟูการดำเนินงาน ผู้วิจัยคำนวณขนาดของกลุ่มตัวอย่างด้วยการวิเคราะห์อำนาจของการทดสอบสำหรับสถิติการวิเคราะห์การถดถอยแบบพหุคูณ ด้วยโปรแกรมสำเร็จรูป G*Power (Faul et al., 2007) โดยกำหนดอำนาจของการทดสอบที่ระดับ 0.95 ระดับนัยสำคัญทางสถิติที่ระดับ 0.05 (α = 0.05) และค่าอิทธิพลขนาดปานกลาง (f^2 = 0.15) ได้ขนาดของกลุ่มตัวอย่างจำนวน 138 ตัวอย่าง และวิเคราะห์ผลการวิจัยโดยใช้สถิติเชิงพรรณนาร่วมกับการวิเคราะห์ปัจจัยและการวิเคราะห์ความถดถอยเชิงพหุ

5. ผลการวิจัย

5.1 การทดสอบข้อตกลงเบื้องต้นทางสถิติ

ข้อมูลจากแบบสอบถาม 138 ชุด ได้ถูกสอบทานความครบถ้วนของข้อมูลก่อนการนำไปประมวลผล ผลการตรวจสอบพบว่า แบบสอบถามทั้ง 138 ชุด มีข้อมูลครบถ้วนสมบูรณ์ทุกชุด นอกจากนี้ ผู้วิจัยได้ดำเนินการทดสอบการกระจายของข้อมูลโดยพิจารณาจากค่าความเบ้ (Skewness) และค่าความโด่ง (Kurtosis) พบว่าข้อมูลทั้งหมดมีค่าความเบ้และค่าความโด่งในระหว่าง -1.058 ถึง 0.489 และ -1.336 ถึง 1.224 ซึ่งอยู่ในช่วงที่เหมาะสม

5.2 การประเมินความเที่ยงและความตรงของแบบสอบถาม

งานวิจัยนี้ได้ทดสอบความเที่ยงตรงของเครื่องมือ (Validity) โดยใช้ค่าประสิทธิ์แอลฟาของครอนบาซ (Cronbach's alpha) โดยเกณฑ์ค่าสัมประสิทธิ์ที่ยอมรับควรมากกว่าหรือเท่ากับ 0.7 (ศรีเพ็ญ ทรัพย์มนชัย และคณะ, 2555) จากการทดสอบพบว่า ค่าประสิทธิ์แอลฟาของครอนบาซของแต่ละตัวแปรมีค่ามากกว่า 0.7 ทุกตัวแปร ดังตารางที่ 1

ตารางที่ 1 แสดงค่าประสิทธิ์แอลฟาของครอนบาซของแต่ละตัวแปร

ตัวแปร	ค่าประสิทธิ์แอลฟาของครอนบาซ
ปัจจัยด้านองค์การ (Organization)	0.837
ปัจจัยด้านบุคคล (Individual)	0.923
ปัจจัยด้านเทคโนโลยี (Technologies)	0.923
ปัจจัยด้านการใช้ระบบการจัดการความรู้ (KMS usage)	0.936
ปัจจัยด้านความตั้งใจในการแบ่งปันความรู้ (Intention to share knowledge)	0.945
การสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ขององค์การ (Creation knowledge to KMS)	0.960

5.3 ลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่าง

กลุ่มตัวอย่างส่วนใหญ่เป็นเพศหญิง จำนวน 81 คน คิดเป็นร้อยละ 58.7 ระดับการศึกษาส่วนใหญ่อยู่ในระดับปริญญาตรี จำนวน 86 คน คิดเป็นร้อยละ 62.3 อายุการทำงานส่วนใหญ่อยู่ในช่วง 3-6 ปี จำนวน 74 คน คิดเป็นร้อยละ 53.6 โดยส่วนใหญ่มีตำแหน่งพนักงานปฏิบัติการ จำนวน 118 คน คิดเป็นร้อยละ 85.5 ในด้านประเภทสถานที่ทำงานมีสัดส่วนของผู้ตอบแบบสอบถามอยู่ในระบบดับใกล้เคียงกันที่ จำนวน 70 คน คิดเป็นร้อยละ 50.7 และ จำนวน 68 คน คิดเป็นร้อยละ 49.3 โดยปฏิบัติงานอยู่ในบริษัทประเภทสินค้าอุตสาหกรรม และบริษัทประเภทเทคโนโลยี ตามลำดับ

จากการสอบถามเกี่ยวกับระบบการจัดการความรู้พบว่า องค์การของกลุ่มตัวอย่างมีระบบการจัดการความรู้และกลุ่มตัวอย่างเคยใช้ระบบการจัดการความรู้ขององค์การ คิดเป็นร้อยละ 100 เมื่อพิจารณาถึงระดับความถี่ในการใช้งานระบบการจัดการความรู้ส่วนใหญ่มีความถี่ในการใช้ระบบการจัดการความรู้ขององค์การอยู่ที่ ใช้น้อยกว่า 1 ครั้งต่อสัปดาห์ คิดเป็นร้อยละ 63.8 รองลงมาคือ ใช้มากกว่า 1 ครั้งต่อสัปดาห์ ร้อยละ 20.3 ใช้สัปดาห์ละครั้ง ร้อยละ 13.0 มีการใช้ 1 ครั้งต่อวันและใช้มากกว่า 1 ครั้งต่อวัน ในสัดส่วนร้อยละที่เท่ากันที่ร้อยละ 1.4

5.4 การทดสอบสมมติฐานการวิจัย

ผลการวิเคราะห์ความถดถอยพหุคูณ (Multiple regression analysis) พบว่า ที่ระดับนัยสำคัญทางสถิติ 0.05 ปัจจัยด้านองค์การ (Organization) และปัจจัยด้านบุคคล (Individual) จะมีอิทธิพลทางบวกต่อปัจจัยด้านการใช้ระบบการจัดการความรู้ (KMS usage) อย่างมีนัยสำคัญ โดยมีค่าน้ำหนักของแต่ละปัจจัย (B) เท่ากับ 0.345 และ 0.749 ตามลำดับ นอกจากนี้ปัจจัยด้านองค์การ (Organization) และปัจจัยด้านบุคคล (Individual) ยังมีอิทธิพลทางบวกต่อปัจจัยด้านความตั้งใจในการแบ่งปันความรู้ (Intention to share knowledge) อย่างมีนัยสำคัญ โดยมีค่าน้ำหนักของแต่ละปัจจัย (B) เท่ากับ 0.328 และ 0.759 ตามลำดับ ส่วนปัจจัยด้านเทคโนโลยี (Technologies) นั้น ส่งผลต่อปัจจัยด้านการใช้ระบบการจัดการความรู้ (KMS usage) และปัจจัยด้านความตั้งใจในการแบ่งปันความรู้ (Intention to share knowledge) อย่างไม่มีนัยสำคัญ

ในส่วนของปัจจัยด้านการใช้ระบบการจัดการความรู้ (KMS usage) และปัจจัยด้านความตั้งใจในการแบ่งปันความรู้ (Intention to share knowledge) นั้น จะมีอิทธิพลทางบวกต่อปัจจัยด้านการสร้างแรงจูงใจในการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ขององค์การ (Creation knowledge to KMS) อย่างมีนัยสำคัญ โดยมีค่าน้ำหนักของแต่ละปัจจัย (B) เท่ากับ 0.290 และ 0.375 ตามลำดับ สรุปผลการทดสอบสมมติฐานดังตารางที่ 2

ตารางที่ 2 แสดงสรุปผลการทดสอบสมมติฐานตามกรอบแนวคิดงานวิจัย

สมมติฐาน	ผลการทดสอบ
H1: ปัจจัยด้านองค์การ (Organization) มีผลเชิงบวกต่อการใช้ระบบการจัดการความรู้ (KMS usage) ของพนักงานในองค์การ	ยอมรับ
H2: ปัจจัยด้านองค์การ (Organization) มีผลเชิงบวกต่อความตั้งใจในการแบ่งปันความรู้ (Intention to share knowledge) ของพนักงานในองค์การ	ยอมรับ
H3: ปัจจัยด้านบุคคล (Individual) มีผลเชิงบวกต่อการใช้ระบบการจัดการความรู้ (KMS usage) ของพนักงานในองค์การ	ยอมรับ
H4: ปัจจัยด้านบุคคล (Individual) มีผลเชิงบวกต่อความตั้งใจในการแบ่งปันความรู้ (Intention to share knowledge) ของพนักงานในองค์การ	ยอมรับ
H5: ปัจจัยด้านเทคโนโลยี (Technologies) มีผลเชิงบวกต่อการใช้ระบบการจัดการความรู้ (KMS usage) ของพนักงานในองค์การ	ไม่ยอมรับ
H6: ปัจจัยด้านเทคโนโลยี (Technologies) มีผลเชิงบวกต่อพฤติกรรมการแบ่งปันความรู้ (Intention to share knowledge) ของพนักงานในองค์การ	ไม่ยอมรับ
H7: การใช้ระบบการจัดการความรู้ (KMS usage) มีผลเชิงบวกต่อการสร้างองค์ความรู้ใหม่ในระบบการจัดการความรู้ (Creation knowledge to KMS)	ยอมรับ
H8: ความตั้งใจในการแบ่งปันความรู้ (Intention to share knowledge) มีผลเชิงบวกต่อการสร้างองค์ความรู้ใหม่ในระบบการจัดการความรู้ (Creation knowledge to KMS)	ยอมรับ

6. สรุปผลการวิจัย

6.1 อภิปรายผลการวิจัย

งายวิจัยนี้แสดงให้เห็นว่า ปัจจัยที่มีอิทธิพลต่อการสร้างแรงจูงใจในการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ขององค์การ ประกอบด้วย ปัจจัยด้านองค์การ (Organization) และปัจจัยด้านบุคคล (Individual) โดยปัจจัยทั้งสองจะมีอิทธิพลต่อปัจจัยด้านการใช้ระบบการจัดการความรู้ (KMS usage) และปัจจัยด้านความตั้งใจในการแบ่งปันความรู้ (Intention to share knowledge) ซึ่งมีอิทธิพลต่อการสร้างแรงจูงใจในการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ขององค์การ (Creation knowledge to KMS) และเมื่อพิจารณาค่าน้ำหนักของแต่ละปัจจัยแสดงให้เห็นว่าปัจจัยด้านบุคคลนั้น จะมีอิทธิพลต่อการใช้ระบบการจัดการความรู้และความตั้งใจในการแบ่งปันความรู้ (Intention to share knowledge) มากกว่าปัจจัยด้านองค์การ และปัจจัยด้านความตั้งใจในการแบ่งปันความรู้ (Intention to share knowledge) นั้น จะมีอิทธิพลต่อการสร้างแรงจูงใจในการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ขององค์การ (Creation knowledge to KMS) มากกว่าปัจจัยด้านการใช้ระบบการจัดการความรู้ (KMS usage) ส่วนปัจจัยด้านเทคโนโลยี (Technologies factors) นั้น ไม่มีอิทธิพลต่อปัจจัยด้านการใช้ระบบการจัดการความรู้ (KMS usage)

6.2 ข้อเสนอแนะในเชิงปฏิบัติ

การวิจัยนี้ทำให้ทราบถึงปัจจัยที่มีผลต่อการสร้างแรงจูงใจในการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ขององค์การนั้น องค์การสามารถนำไปใช้งานได้ ดังนี้

(1) องค์การสามารถนำปัจจัยเหล่านี้มาใช้เป็นแนวทางในการปรับปรุงหรือวางแผนการใช้ระบบการจัดการความรู้ในองค์การได้อย่างมีประสิทธิภาพ ประสบความสำเร็จในการสร้างแรงจูงใจให้กับผู้ใช้ระบบตระหนักถึงการสร้างองค์ความรู้ใหม่โดยการแปลงความรู้โดยนัยที่อยู่ภายในตัวบุคคล และความรู้ที่ชัดแจ้งขององค์การ ออกมาบันทึกลงสู่ระบบการจัดการความรู้ขององค์การ

(2) องค์การมีความรู้พร้อมใช้และเป็นความรู้ที่ถูกปรับปรุงให้ทันสมัยอยู่เสมอ พนักงานในองค์การสามารถนำความรู้เหล่านี้ไปใช้ในการทำงาน เพื่อให้การดำเนินงานขององค์การมีประสิทธิภาพและประสิทธิผล ซึ่งจะนำไปสู่ความสามารถในการแข่งขันที่ยั่งยืนขององค์การ

(3) องค์การไม่ประสบปัญหาการสูญหายของความรู้ขององค์การ เนื่องจากมีการสนับสนุนให้พนักงานในองค์การมีการเปลี่ยนความรู้ที่มีอยู่ในตัวบุคคลให้กลายมาเป็นความรู้ขององค์การที่สามารถถ่ายทอดให้กับบุคคลอื่นในองค์การได้

6.3 ข้อเสนอแนะสำหรับงานวิจัยต่อเนื่อง

ควรมีการศึกษาต่อในเรื่องของเทคโนโลยีที่แต่ละองค์การนำมาประยุกต์ใช้ช่วยจัดการข้อมูลความรู้ขององค์การ เช่น Business Intelligence Tools หรือ การทำ Big Data Analysis เป็นต้น ว่าส่งผลกระทบต่อการใช้ระบบการจัดการความรู้ (KMS usage) และสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ขององค์การ (Creation knowledge to KMS) หรือไม่ รวมทั้งทัศนคติของคนรุ่นใหม่ที่มีผลต่อการใช้เทคโนโลยีในการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ รวมถึงการศึกษาต่อในเรื่องของพฤติกรรมการใช้ระบบการจัดการความรู้ โดยศึกษาลึกลงไปถึงเรื่องระดับความถี่ในการใช้งานระบบการจัดการความรู้ว่าส่งผลกระทบต่อปัจจัยด้านเทคโนโลยีต่อการสร้างองค์ความรู้ใหม่ลงในระบบการจัดการความรู้ขององค์การ (Creation knowledge to KMS) หรือไม่

บรรณานุกรม

ศรีเพ็ญ ทรัพย์มนชัย, มนวิกา ผดุงสิทธิ์ และ นภดล ร่มโพธิ์. (2555). *การวิจัยทางธุรกิจ*. พิมพ์ครั้งที่1.กรุงเทพฯ: สำนักพิมพ์ฟิสิกส์เซ็นเตอร์.

ศรีสมรัก อินทุจันทร์ยง. (2549). *ระบบสารสนเทศเพื่อการจัดการ*. กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

สำนักงานคณะกรรมการพัฒนาระบบราชการและ สถาบันเพิ่มผลผลิตแห่งชาติ. (2548). *คู่มือการจัดทำแผนการจัดการความรู้.*

Aggestam, L., & Persson, A. (2010). Increasing the Quality in IT-supported Knowledge Repositories: Critical Success Factors for Identifying Knowledge. *Proceedings of the 43rd Hawaii International Conference on System Sciences - 2010*.

Alavi,M., & Leidner, D. E. (2001). Review: knowledge management and knowledge management systems: Conceptual foundation and research issues. *MIS Quarterly*., 25(1), 107-136.

Bock, G. W., Zmud, R. W., Kim, Y. G., & Lee, J. N. (2005). Behavioral Intention Formation in Knowledge Sharing: Examining the Roles of Extrinsic Motivators, Social-Psychological Forces, and Organizational Climate. *MIS Quarterly*, 29(1), 87-111.

Chen, C. J., & Huang, J. W. (2007). How organizational climate and structure affect knowledge management—The social interaction perspective. *International Journal of Information Management*., 27, 104–118.

Chen, S. S., Chuang, Y. W., & Chen, P. Y. (2012). Behavioral intention formation in knowledge sharing: Examining the roles of KMS quality, KMS self-efficacy, and organizational climate. *Knowledge-Based Systems*, 31, 106–118.

DeLone, W. H., & McLean, E. R. (1992). Information Systems Success: The Quest for Dependent Variable. *Information Systems Research (3:1)*. 60-95.

Hoong, A. L. S., Ming, T., & Lim. (2012). The Use of Knowledge Management Systems to Support Knowledge Creation and Sharing Activities among Employees – A Survey based Study of IT Shared Services Company. *2012 Ninth International Conference on Information Technology- New Generations*., 175-181.

Kankanhalli, A., Tan, B. C. Y., & Wei, K. K. (2005). Contributing Knowledge to Electronic Knowledge Repositories: An Empirical Investigation. *MIS Quarterly*, 29(1), 113-143.

Kulkarni, U. R., Ravindran, S., & Freeze, R. (2007). A Knowledge Management Success Model: Theoretical Development and Empirical Validation. *Journal of Management Information Systems,* 23(3), 309-347

Lee, J., Kim, J., & Han, Y. (2010). A Study on Factors Influencing Knowledge-Sharing Activity for the Innovation Activity of Team. *IEEE*, 270-274.

Ma, J., Du, R., Ma, S., & Zhang, W. (2009). Factors Affecting Knowledge Sharing in Governmental Fiscal Departments: An Empirical Study. *IEEE*, 1973-1977.

Matzler, K., Renzl, B., Mooradian, T., Krogh, G. V., & Mueller, J. (2011). Personality traits, affective commitment, documentation of knowledge, and knowledge sharing. *The International Journal of Human Resource Management*, 22(2), 296–310.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science*, 5(1), 14-37.

Nonaka, I., & Takeuchi, H. (1995). *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*. London & New York: Oxford University Press.

Oyefolahan, I. O., & Dominic, P. D. D. (2010). Conceptualization of the Antecedents and Impacts of KMS Utilization: A Preliminary Framework. *IEEE*, 1485-1489.

Oyefolahan, I. O., & Dominic, P. D. D. (2011). The Use of KMS in Organizations: A Conceptual Framework and Preliminary Tests of Instruments. *IEEE*, 140-156.

Oyefolahan, I. O., Dominic, P. D. D., & Karim, N. S. A. (2012). Towards an Effective KMS Usages: The Role of Socio-Technical Antecedents in the Building of Autonomous Motivation to Use. *2012 International Conference on Computer & Information Science (ICCIS)*, USA, 89-93.

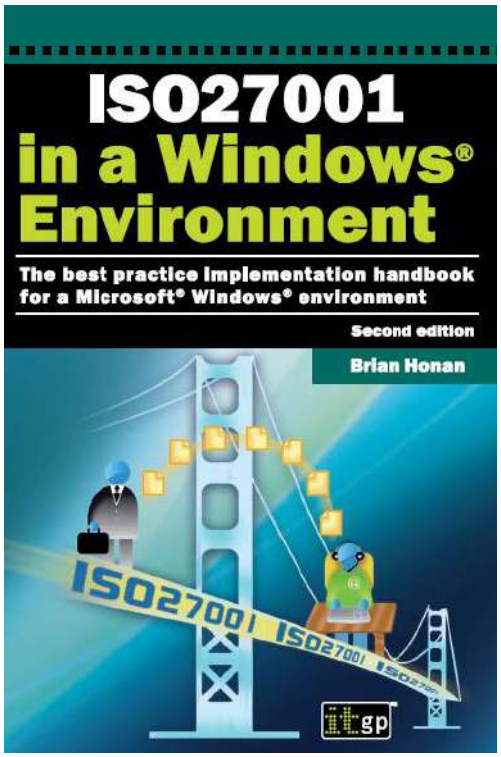
Stenmark, D., & Lindgren, R. (2004). Integrating Knowledge Management Systems with Everyday Work: Design Principles Leveraging User Practice. *Proceedings of the 37th Hawaii International Conference on System Sciences – 2004*, USA, 56-70.

Wu, J. H., & Wang, Y. M. (2006). Measuring KMS success: A respecification of the DeLone and McLean's model. *Information & Management*, 43, 728–739.

บทวิจารณ์หนังสือ

นิตยา วงศ์ภินันท์วัฒนา
คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

doi: 10.14456/jisb.2018.18



Title: ISO27001 in a Windows Environment: The best practice implementation handbook for a Microsoft Windows environment (Second edition)
Author: Brian Honan
Edition: 2010
Publisher: IT Governance Publishing
Number of pages: 312

หนังสือ ISO27001 in a Windows Environment เป็นสิ่งที่ต้องกำหนดเพื่อให้ระบบสารสนเทศขององค์กรมีความมั่นคงปลอดภัยตามมาตรฐานของ ISO27001 ประกอบด้วยการกำหนดนโยบายความมั่นคงปลอดภัยของสารสนเทศ การกำหนดหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ ความมั่นคงปลอดภัยสำหรับทรัพยากรมนุษย์ การบริหารจัดการทรัพย์สิน การควบคุมการเข้าถึง การเข้ารหัสข้อมูล สภาพแวดล้อมความมั่นคงปลอดภัยทางกายภาพ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล การจัดหา การพัฒนา และการบำรุงรักษาระบบ ความสัมพันธ์กับผู้ให้บริการภายนอก การบริหารจัดการอุบัติการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ การบริหารจัดการความต่อเนื่องของธุรกิจด้านความมั่นคงปลอดภัยสารสนเทศ และความสอดคล้อง นอกจากนี้ยังกล่าวถึงการกำหนดค่าการทำงานของ Windows Server เพื่อให้มีการรักษาความมั่นคงปลอดภัย โดยสรุปดังนี้

1. ระบบปฏิบัติการติดตั้ง service pack ที่เป็นปัจจุบัน
   คำสั่ง
   control panel -> system ดูที่ชื่อระบบปฏิบัติการว่าติดตั้ง service pack ใด (สามารถไปดูรุ่นของ service pack ที่เป็นปัจจุบันได้จาก web ของ Microsoft)
2. กำหนด account policies
   คำสั่ง
   start -> administrative tools -> domain security setting -> account policies
   2.1 minimum password length เป็นการกำหนดขนาดของรหัสผ่าน ขนาดของรหัสผ่านจะส่งผลต่อการแกะรหัสผ่าน กล่าวคือถ้ารหัสผ่านมีขนาดสั้นจะใช้เวลาในการแกะรหัสผ่านน้อย
   2.2 maximum password age เป็นการกำหนดวันที่รหัสผ่านจะหมดอายุใช้งาน เพื่อให้ผู้ใช้เปลี่ยนรหัสผ่านใหม่

2.3 minimum password age เป็นการกำหนดจำนวนวันที่ต้องใช้รหัสผ่านที่เปลี่ยนใหม่ เพื่อป้องกันไม่ให้ผู้ใช้เปลี่ยนไปใช้รหัสผ่านเดิมเร็วเกินไป

2.4 password complexity เป็นการกำหนดให้รหัสผ่านที่กำหนดต้องมีความซับซ้อน

2.5 password history เป็นการกำหนดประวัติของรหัสผ่านเพื่อไม่ใช้ผู้ใช้เปลี่ยนไปใช้รหัสผ่านเดิมเร็วเกินไป

2.6 store passwords using reversible encryption เป็นการเข้ารหัสรหัสผ่านที่เก็บอยู่ในระบบปฏิบัติการ

3. กำหนด audit policies

คำสั่ง

start -> administrative tools -> domain security setting -> local policies -> audit policy

3.1 audit account logon events เป็นการติดตามการเข้าถึง server เนื่องจากการ logon ที่ล้มเหลวแสดงว่ามีการโจมตีด้วยการเดารหัสผ่านอยู่

3.2 audit account management เป็นการติดตามการจัดการบัญชีผู้ใช้จะทำให้ทราบถึง การสร้าง เปลี่ยนแปลง หรือลบบัญชีผู้ใช้ ซึ่งจะทำให้ทราบเกี่ยวกับบัญชีผู้ใช้ปลอมหรือค้นหาสาเหตุของการที่บัญชีผู้ใช้ถูก lock

3.3 audit directory service access เพื่อจัดเก็บข้อมูลการเข้าถึงทรัพยากรใน active directory

3.4 audit logon events เพื่อมั่นใจว่ามีการติดตามการเข้าถึง server ของ local account

3.5 audit object access เป็นการติดตามการเข้าถึงทรัพยากรต่างๆ ในระบบ เช่น เครื่องพิมพ์ แฟ้มข้อมูล เป็นต้น แต่การกำหนดค่าดังกล่าวจะทำให้มีรายการการใช้งานทรัพยากรของระบบจำนวนมากเช่นกัน

3.6 audit policy change เพื่อให้จัดเก็บรายการเกี่ยวกับการเปลี่ยนแปลง user rights, account policies, group policies และอื่นๆ

3.7 audit privilege use เพื่อจัดเก็บข้อมูลการใช้สิทธิพิเศษในการปฏิบัติงาน เช่น การสำรองข้อมูล เป็นต้น นอกจากนี้ยังรวมถึงการทำกิจกรรมปลอมในระบบ

3.8 audit process tracking มักไม่ใช้งานเนื่องจากจะจัดเก็บรายการจำนวนมาก ไม่ว่าจะเป็นการเปิด ปิด และรายการเปลี่ยนแปลงต่างๆ

3.9 audit system events เพื่อจัดเก็บข้อมูลการเปิด ปิด server และระบบอื่นๆ

4. account lockout policy

คำสั่ง

start -> administrative tools -> domain security setting -> account logout policy

4.1 account lockout duration จะกำหนดช่วงเวลาไม่ให้บัญชีผู้ใช้สามารถใช้งานได้ โดยผู้บริหารจะสามารถปรับค่านี้ได้ นอกจากนี้ผู้โจมตีสามารถใช้หน้าที่งานนี้เพื่อโจมตีแบบ DoS (denial of service) ด้วยการ lock บัญชีผู้ใช้ทุกคน

4.2 account lockout threshold กำหนดจำนวนครั้งที่ผู้ใช้สามารถป้อนบัญชีผู้ใช้ผิดก่อนที่ระบบจะ lock out

4.3 reset account lockout counter after จะกำหนดร่วมกับ account lockout threshold โดย counter ของจำนวนครั้งที่ป้อนบัญชีผู้ใช้ผิดจะถูกเปลี่ยนให้เป็นศูนย์หลังจากระยะเวลาที่กำหนดในค่านี้

4.4 lockout after กำหนดจำนวนครั้งที่ผู้ใช้ถึงระบบและล้มเหลว ต่อจากนั้นผู้ใช้จะไม่สามารถเข้าถึงระบบได้

4.5 forcibly disconnect remote user from server when logon hours expire เป็นการกำหนดว่าผู้ที่เชื่อมต่อเข้ามาในระบบเครือข่ายคอมพิวเตอร์จะถูกปิดการติดต่อ

หมายเหตุ 4.4 และ 4.5 เป็นคำสั่งสำหรับ windows server 2008

5. event log settings

คำสั่ง

start -> administrative tools -> domain security setting -> event log

5.1 application log settings เป็นการจัดเก็บลงบันทึกการใช้งานโปรแกรมประยุกต์ ประกอบด้วย

- maximum application log size การกำหนดขนาดของลงบันทึกเพื่อใช้ในการจัดเก็บข้อมูล
- prevent local guests group from accessing application log กำหนดว่าไม่ให้ guest accounts เปิดข้อมูลในลงบันทึกนี้ได้
- retain application log กำหนดจำนวนวันจัดเก็บข้อมูลในลงบันทึกซึ่งจะต้องสอดคล้องกับ overwrite by days
- retention method for application log ประกอบด้วย
  + overwrite events as needed
  + overwrite by days
  + do not overwrite (clear logs manually)

5.2 security log settings เป็นการจัดเก็บลงบันทึกเกี่ยวกับการพยายามเข้าสู่ระบบด้วยรหัสที่ถูกต้องและไม่ถูกต้อง (logon attempt) รายละเอียดการกำหนดขนาดและวิธีการเก็บลงบันทึกเช่นเดียวกับ 5.1

5.3 system log settings เป็นการจัดเก็บลงบันทึกเกี่ยวกับการพยายามเข้าองค์ประกอบของระบบปฏิบัติการ เช่น ความล้มเหลวในการเปิดใช้งาน driver เป็นต้น รายละเอียดการกำหนดขนาดและวิธีการเก็บลงบันทึกเช่นเดียวกับ 5.1

6. การกำหนดการจัดเก็บลงบันทึกที่ web server และการ disable guest account

คำสั่ง

start -> administrative tools -> internet information services (IIS) manager -> web sites -> default web site คลิกขวาที่ default web site -> เลือก properties

6.1 เลือก tab web site -> enable logging

6.2 เลือก tab directory security -> ที่ authentication and access control กดปุ่ม edit ยกเลิก anonymous access

7. การ set up อื่นๆ ที่ควรให้ความสนใจ

7.1 การเปลี่ยนชื่อหรือกำหนดไม่ให้ใช้งานได้ (disable) บัญชี administrator account และ guest account

7.2 การกำหนดสิทธิในการ backup และ restore

7.3 ให้พิมพ์งานจาก print server เท่านั้น

7.4 ให้ server เลิกการสร้าง 8.3 file names ด้วยการทำให้ client ต้องใช้ชื่อเต็มเท่านั้น

7.5 ถ้าต้องการใช้บริการของ telnet ในการโอนข้อมูลให้ทำผ่าน secure shell (SSH) แทน

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. ส่งบทความให้ผู้ทรงคุณวุฒิจำนวน 2 ท่านเพื่อประเมินบทความ เมื่อผลการประเมินผ่านหรือไม่ผ่านหรือมีการแก้ไขจะแจ้งให้ผู้เขียนทราบ เมื่อบทความได้รับการตีพิมพ์ ผู้เขียนจะได้รับการแจ้งกลับรับรองการตีพิมพ์ พร้อมทั้งแจ้งวันที่จะสามารถ download วารสารที่ได้ตีพิมพ์บนเว็บไซต์ต่อไป

การส่งบทความ

ผู้ที่ประสงค์จะส่งบทความกับวารสารระบบสารสนเทศด้านธุรกิจ 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 A4 (8.27” x 11.69”)
3. ตารางต้องมีชื่อตารางกำกับบนตาราง และภาพต้องมีชื่อภาพกำกับใต้ภาพ พร้อมทั้งให้หมายเลขเรียงลำดับสำหรับตารางและภาพ และให้อยู่ในเนื้อหา (ภาพให้จัดทำเป็น .jpeg แล้วนำมา insert ในบทความ)

รูปแบบการพิมพ์บทความ

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

ประเภทข้อความ	**ขนาด**	**ชนิด**
ชื่อเรื่อง (ภาษาไทย)	20 (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)	20 (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 วงศ์วิวัฒน์นุกิจ, 2550ก, น. 22), (ศุภกิจ วงศ์วิวัฒน์นุกิจ, 2550ข, น. 22), (Yin, 1998a, p. 5-9) หรือ (Yin, 1998b, p. 31-40)

- **ผู้แต่งหลายคน เอกสารหลายเรื่อง และต้องการอ้างอิงถึงพร้อม ๆ กัน** ให้ระบุชื่อผู้แต่งเรียง ตามลำดับอักษรคั่นด้วยเครื่องหมาย ; 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 อ้างถึงในกรณีเป็น) 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.