แบบความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์ สำหรับองค์การภาครัฐ

Security Assessment Model of Cloud Computing for Government Organizations

ยุทธพล พิชัยณรงค์[1*], นัฐพงศ์ ส่งเนียม[2], ดุษณี ศุภวรรธนะกุล[3] และวรภัทร ไพรีเกรง[4]
Yuthtapon Pichainarong[1*] Nattapong Songneam[2] Dusanee Supawantanakul[3] and Worapat Paireekreng[4]
[1*,3]สาขาการจัดการเทคโนโลยี หลักสูตรปรัชญาดุษฎีบัณฑิต มหาวิทยาลัยราชภัฏพระนคร กรุงเทพฯ 10220
9 ถนนแจ้งวัฒนะ แขวงอนุสาวรีย์ เขตบางเขน กรุงเทพฯ 10220 โทร 08 7919 2959 E-mail: yuthtapon@hotmail.com
[2]สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏพระนคร กรุงเทพฯ 10220
[4]สาขาเทคโนโลยีสารสนเทศ หลักสูตรปรัชญาดุษฎีบัณฑิต มหาวิทยาลัยธุรกิจบัณฑิตย์ กรุงเทพฯ 10210
[1*,3]Technology Management, Doctor of Philosophy (Ph.D.), Phranakhon Rajabhat University, Bangkok 10220
9 Changwattana Road, Bangkhem Bangkoo 10220 Tel: +66(8) 7919 2959 E-mail: yuthtapon@hotmail.com
[2]Computer Science, Faculty of Science and Technology, Phranakhon Rajabhat University, Bangkok 10220
[4]Information Technology, Doctor of Philosophy (Ph.D.), Dhurakij Pundit University, Bangkok 10210

วันที่รับบทความ 26 กรกฎาคม 2562 **วันที่รับแก้ไขบทความ** 9 ตุลาคม 2562 **วันที่ตอบรับบทความ** 17 ธันวาคม 2562
Received: Jul. 26, 2019 **Revised:** Oct. 9, 2019 **Accepted:** Dec. 17, 2019

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์ 1) เพื่อสำรวจ วิเคราะห์ และประเมินปัจจัยความเสี่ยงในการใช้ระบบการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ 2) เพื่อออกแบบและพัฒนาตัวแบบความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ และ 3) เพื่อประเมินประสิทธิภาพของตัวแบบความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ ผลการวิจัยพบว่า การสำรวจ วิเคราะห์ และประเมินปัจจัยความเสี่ยงในระบบการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐมีลักษณะงานที่แตกต่างกัน การใช้งานการประมวลผลคลาวด์ไม่พบข้อแตกต่างกัน การประเมินความเสี่ยงมีค่าความรุนแรง และโอกาสที่จะเกิดความเสี่ยงเฉลี่ยอยู่ในระดับที่ต่ำมาก เนื่องด้วยมีหน่วยงานสำนักงานพัฒนารัฐบาลดิจิตอล เป็นหน่วยงานกลางของภาครัฐที่ให้บริการและช่วยกำกับดูแลในเรื่องของความมั่นคงปลอดภัยในการประมวลผลคลาวด์ ส่วนผลการออกแบบนโยบายที่สร้างมาจากมาตรฐานสากลจำนวน 3 มาตรฐาน ได้แก่ มาตรฐาน ISO, COBIT และ ITIL จากตารางการตัดสินใจ และรับรองมาตรฐานโดยผู้เชี่ยวชาญ (Focus Group) เพื่อให้ได้แนวนโยบายความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ (ICI) ประกอบไปด้วย 4 โดเมน 26 วัตถุประสงค์ 109 ข้อย่อย ผลการประเมินประสิทธิภาพของนโยบายความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐเดิม จากผู้เชี่ยวชาญด้วยการประเมินแบบรูบริคส์ เป็นการประเมินแบบเชิงคุณภาพ มีค่าโดยรวมเท่ากับ 3 คะแนน แปรผลเท่ากับค่าประสิทธิภาพปานกลาง และเมื่อได้ทำการจัดแนวนโยบายใหม่ทำให้มีค่าประสิทธิภาพเพิ่มขึ้นเท่ากับ 5 คะแนน แปลผลเท่ากับค่าประสิทธิภาพมากที่สุด โดยเพิ่มขึ้นจากเดิมร้อยละ 66.67 และตัวแบบดังกล่าวสามารถนำไปประยุกต์ใช้กับองค์การภาครัฐอื่น ๆ เพื่อให้เกิดประโยชน์ได้อีกด้วย

คำสำคัญ: การประเมินความเสี่ยง, ความมั่นคงปลอดภัย, การประมวลผลแบบคลาวด์, องค์การภาครัฐ

Abstract

The objectives of this study were to 1) survey, analyze and evaluate risk factors of Cloud computing systems of government organizations in Thailand, 2) design and develop a Cloud computing security model for government organizations, and 3) evaluate the efficiency of the model. The findings were as follows. The survey, analysis, and evaluation of risk of using Cloud computing systems revealed that usage patterns differed from organization to organization; meanwhile, no differences in Cloud computing among these organizations were found. Moreover, the level of risk was found to be very low, in spite of the high stakes, because Cloud computing systems were served and supervised by the Digital Government Development Agency (DGA). As for a security model of Cloud computing for government organizations, the researcher designed and constructed a security model according to three international standards (ISO, COBIT, ITIL) and criteria for selected items. This model was evaluated by experts whose opinions were solicited via a focus group. This model, featuring a security policy, consisted of 4 domains, 26 objectives and 109 sub-terms. The evaluation conducted by three experts according to qualitative rubrics showed that the overall security of the existing practice was at a moderate level, of which the mean was 3. After the security policy was introduced, its efficiency increased to a very high level of which the mean was 5, an increase of 66.67 percent. Our model can be applied in any government organization in Thailand in order to assess the risk of Cloud computing.

Keywords: risk assessment, security, cloud computing, government organization

1. บทนำ

ปัจจุบันการประมวลผลแบบคลาวด์ได้เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานทั้งในส่วนของการจัดเก็บข้อมูล การประมวลผลระบบงานโดยเฉพาะระบบงานที่เกี่ยวข้องกับระบบสารสนเทศ ระบบงานเครือข่าย ให้มีความสะดวก รวดเร็ว มีประสิทธิภาพการใช้เทคโนโลยีสารสนเทศก็อาจมีความเสี่ยงหลายประการ จึงนำการประมวลผลแบบคลาวด์ (Cloud Computing) เข้ามาช่วยแก้ปัญหา โดยข้อมูลส่วนใหญ่ของหน่วยงานราชการเป็นข้อมูลทางด้านความลับ จึงต้องมีการบริหารความเสี่ยง สามารถระบุความเสี่ยงของข้อมูล อุปกรณ์ บุคลากร ที่อาจก่อให้เกิดความเสียหายต่อทรัพย์สิน ความรุนแรง และโอกาสที่จะเกิด มาพิจารณาความเสี่ยง ซึ่งเดิมจะใช้มาตรฐาน ISO 27001 มาประเมินความเสี่ยง ซึ่งในปัจจุบันหากใช้มาตรฐาน ISO 27001 เพียงมาตรฐานเดียวก็ยังไม่เพียงพอต่อความเสี่ยงที่อาจเกิดขึ้น จึงต้องหามาตรฐานอื่น ๆ มาช่วยเสริมเพื่อปิดช่องโหว่ เช่น มาตรฐาน COBIT, ITIL มาช่วยออกแบบมาตรฐานเพื่อให้มีความมั่นคงปลอดภัยมากขึ้น

ดังนั้น เพื่อให้การทำงานมีความมั่นคงปลอดภัยที่เหมาะสม จึงต้องทำวิจัยเกี่ยวกับตัวแบบการประเมินความเสี่ยงและการออกแบบความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ เพื่อเป็นต้นแบบสนับสนุนงานตามภารกิจหลักขององค์การ ก่อให้เกิด

ผลประโยชน์สูงสุดในการลดโอกาสเสี่ยงต่อความเสียหายของข้อมูล ความซ้ำซ้อนของข้อมูล ลดภาระการบริหารจัดการ เพื่อให้สอดคล้องกับนโยบายแนวคิดประเทศไทย 4.0 ให้มีความมั่นคงปลอดภัย

2. วัตถุประสงค์ของการวิจัย

2.1 เพื่อสำรวจ วิเคราะห์และประเมินปัจจัยความเสี่ยงในระบบการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐของประเทศไทย

2.2 เพื่อออกแบบและพัฒนาตัวแบบความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐของประเทศไทย

2.3 เพื่อประเมินประสิทธิภาพของตัวแบบความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐของประเทศไทย

3. นิยามศัพท์เฉพาะ

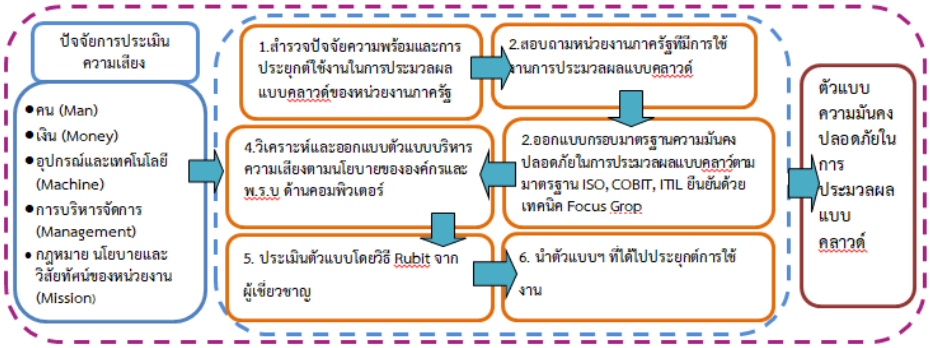
ตัวแบบ (Model) หมายถึง การวิจัยถึงกระบวนการ วิธีการและพฤติกรรมการดำเนินการให้ได้ตามวัตถุประสงค์หลักของการวิจัย

ตัวแบบความมั่นคงปลอดภัย (Security Assess Model) หมายถึง การวิจัยถึงกระบวนการ วิธีการและพฤติกรรมการดำเนินการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ ให้อยู่ในสถานะที่มีความปลอดภัย ที่เกิดขึ้นจากการจัดตั้ง การดำรงไว้ซึ่งมาตรการการปกป้อง ทำให้เกิดความมั่นใจว่าการกระทำหรืออิทธิพลที่ไม่เป็นมิตร ไม่สามารถจะมีผลกระทบได้และได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ

การประมวลผลแบบคลาวด์ (Cloud computing) หมายถึง ลักษณะการทำงานของระบบโดยใช้ทรัพยากรต่าง ๆ ที่มีอยู่บนระบบเครือข่ายอินเทอร์เน็ต เช่น พื้นที่การจัดเก็บข้อมูล แพลตฟอร์มการทำงาน แอปพลิเคชัน ที่ผู้ใช้งานเรียกใช้งานโปรแกรมต่าง ๆ ผ่านทางเครือข่ายอินเทอร์เน็ต และรับข้อมูลแสดงผลผ่านเว็บเบราว์เซอร์

องค์การภาครัฐ (Government organization) หมายถึง หน่วยงานตามกฎหมายว่าด้วยการบริหารราชการ อันได้แก่ กระทรวง ทบวง กรม รัฐวิสาหกิจ และหน่วยงานอิสระ ที่อยู่ภายใต้การจัดตั้ง กำกับดูแล และสนับสนุนงบประมาณของรัฐ เพื่อประโยชน์ต่อประชาชนโดยแบ่งส่วนการบริหารราชการออกเป็น 20 กระทรวง

4. วิธีดำเนินการวิจัย



ภาพที่ 1 กรอบแนวคิดในการทำวิจัย

กรอบแนวคิดในการวิจัยมีวิธีการดำเนินการในการวิจัยที่มีปัจจัยความเสี่ยงเข้ามามีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ 5 ปัจจัย ประกอบด้วย คน เงิน อุปกรณ์ และเทคโนโลยีการบริหารจัดการ และนโยบายและวิสัยทัศน์ โดยจะมีขั้นตอนการจัดการความเสี่ยงดังต่อไปนี้

(1) สำรวจปัจจัยและสภาพความพร้อมที่มีผลต่อการนำเทคโนโลยีสารสนเทศและการสื่อสารในการประมวลผลแบบคลาวด์ มาประยุกต์ใช้กับงานด้านต่าง ๆ สำหรับองค์การภาครัฐ

(2) ศึกษาสภาพการพร้อมใช้งานเทคโนโลยีสารสนเทศในการประมวลผลแบบคลาวด์ โดยสร้างแบบสอบถามและเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง จำนวน 20 กระทรวง

(3) ออกแบบกรอบมาตรฐานความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ โดยใช้มาตรฐาน ISO 27001:2013, ITIL3, COBIT5 มาเป็นกรอบในการออกแบบความมั่นคงปลอดภัยให้อยู่ในเกณฑ์ที่สามารถยอมรับได้ โดยใช้เทคนิคตารางการตัดสินใจ (Decision table) และใช้เทคนิคแบบการประชุมกลุ่ม (Focus group) โดยมีผู้เชี่ยวชาญจำนวนไม่น้อยกว่า 8 - 12 ท่าน เพื่อประเมินแบบสอบถามให้ได้กรอบมาตรฐานใหม่เรียกว่า ICI (ISO COBIT ITIL)

(4) ทำการวิเคราะห์ประเมินความเสี่ยงเพื่อนำเสนอแนวทางการป้องกันความมั่นคงปลอดภัยตามนโยบายขององค์กร รวมถึงการวิเคราะห์ข้อมูลจากแบบสอบถามด้วย

(5) ประเมินประสิทธิภาพของตัวแบบความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์จากผู้เชี่ยวชาญโดยใช้เทคนิคแบบ Rubit

(6) นำเสนอตัวแบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ มาประยุกต์ใช้งานจริงและประเมินการใช้งานโดยการทำข้อตกลงการให้บริการ (Service Level Agreement (SLA))

(7) สรุปการประมวลผลเพื่อให้ได้ตัวแบบการประเมินความเสี่ยงและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ เพื่อนำไปปรับปรุงการทำงานแบบเดิมรวมถึงการถ่ายทอดองค์ความรู้ให้กับหน่วยงานที่อยู่ภายใต้กระทรวง

4.1 ประชากรและกลุ่มตัวอย่าง

1) ประชากรที่ใช้ในการวิจัย ในหน่วยงานภาครัฐของประเทศไทย จำนวน 20 กระทรวง เฉพาะในส่วนของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของแต่ละกระทรวง

2) กลุ่มตัวอย่างที่ใช้ในการวิจัย ใช้การเปรียบเทียบตารางของกลุ่มตัวอย่างที่ระดับความเชื่อมั่นร้อยละ 95 และยอมให้เกิดความคลาดเคลื่อนร้อยละ 5 (Krejcie, R. V. & Morgan, D. W., 1970) แบ่งเป็น 3 กลุ่มตัวอย่างดังนี้

(1) กลุ่มผู้บริหารของหน่วยงานภาครัฐ (CIO) ทำหน้าที่รับผิดชอบในการบริหารเกี่ยวกับงานด้านเทคโนโลยีสารสนเทศขององค์การของแต่ละกระทรวง 20 กระทรวง กระทรวงละ 1 ท่าน ใช้หลักการสุ่มแบบเจาะจง (Purposive Sampling) จะได้กลุ่มตัวอย่าง 20 คน

(2) กลุ่มผู้ดูแลระบบ (Administrator) ที่ทำหน้าที่ในการกำกับ ควบคุมและดูแลระบบงานเครือข่ายคอมพิวเตอร์ ระบบการประมวลผลแบบคลาวด์ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของแต่ละกระทรวง 20 กระทรวง โดยใช้หลักการเปรียบเทียบอัตราส่วน กลุ่มตัวอย่างของ ทาโร ยามาเน่ (Taro Yamane) (Yamane, Taro., 1973 อ้างอิงใน ศิริพงศ์ พฤทธิพันธุ์, 2553 / Prithiphan, S., 2010) จากประชากร 290 ท่าน จะได้กลุ่มตัวอย่าง 165 คน

(3) กลุ่มผู้ใช้งาน (User) ที่เป็นผู้ใช้งานระบบการประมวลผลแบบคลาวด์ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จำนวน 20 กระทรวง ที่มีโดยใช้หลักการเปรียบเทียบอัตราส่วนของกลุ่มตัวอย่างของ ทาโร ยามาเน่ จากประชากร 10,766 คน จะได้กลุ่มตัวอย่าง 370 คน

3) กลุ่มผู้เชี่ยวชาญด้านไอซีที ด้วยวิธีการสนทนากลุ่ม (Focus Group) จากผู้เชี่ยวชาญหรือผู้ทรงคุณวุฒิจำนวนไม่น้อยกว่า 8 - 12 คน ที่เป็นยอมรับในแวดวงวิชาชีพด้านไอทีหรือหน่วยงานราชการ ด้วยเกณฑ์การพิจารณาจากผู้ที่มีความรู้ ความสามารถและประสบการณ์ทางด้านไอซีที ด้านความมั่นคงปลอดภัย ด้านมาตรฐานไอที การประมวลผลคลาวด์ และด้านงานวิจัยเป็นอย่างดี ดังนี้

(1) ผู้เชี่ยวชาญในการคัดเลือกข้อมาตรฐาน ให้ได้กรอบมาตรฐานใหม่ จะต้องมีคุณวุฒิทางการศึกษาไม่ต่ำกว่าระดับปริญญาเอก หรือมีตำแหน่งทางวิชาการ ผู้ช่วยศาสตราจารย์ขึ้นไป

(2) ผู้เชี่ยวชาญตรวจสอบเครื่องมือในการวิจัย เพื่อใช้ในการประเมินแบบสอบถามที่ผู้วิจัยที่กำหนดขึ้น เพื่อรับฟังความคิดเห็น การคาดการณ์ สถานการณ์ใดสถานการณ์หนึ่ง

(3) ผู้เชี่ยวชาญตรวจประเมินตัวแบบการประเมินความเสี่ยง และความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์ สำหรับองค์การภาครัฐ เพื่อเป็นผู้พิจารณาตรวจประเมินตัวแบบให้ครบถ้วนสมบูรณ์ตามวัตถุประสงค์ ตรงตามเนื้อหาของตัวแบบความมั่นคงปลอดภัย

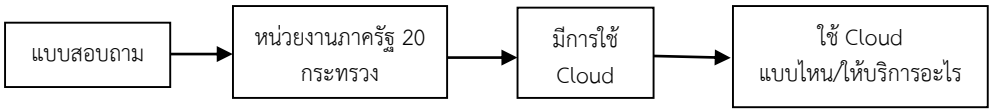
4.2 เครื่องมือที่ใช้ในการวิจัย แบ่งวิธีการเก็บข้อมูลมี 2 ส่วน ดังนี้

1) แบบสัมภาษณ์เชิงลึก (Indepth Interview) เป็นวิธีการสัมภาษณ์เกี่ยวกับการจัดการความมั่นคงปลอดภัย การควบคุมปัจจัยเสี่ยง ทิศทางการทำงาน และนโยบายที่ใช้ในการตั้งคำถาม

2) แบบสอบถาม (Questionnaire) ที่เกี่ยวข้องกับระดับโอกาส และระดับความรุนแรงที่จะเกิดความเสี่ยง พร้อมทั้งระบุผลเสียหายต่อปัจจัยความเสี่ยง

4.3 ขั้นตอนการดำเนินการวิจัย เพื่อให้ได้ตัวแบบแนวนโยบายความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ แบ่งระยะการดำเนินการ 4 ระยะ ดังนี้

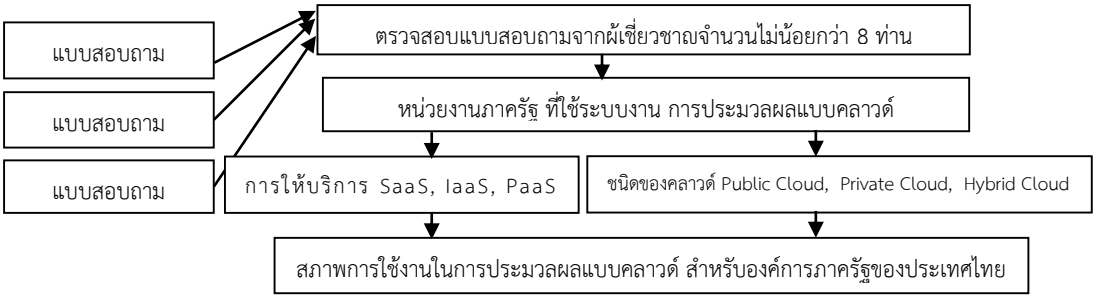
ระยะที่ 1 เพื่อสำรวจ วิเคราะห์ และประเมินผลจากปัจจัยความเสี่ยงในการประมวลผลแบบคลาวด์ สร้างแบบสอบถามและเก็บรวบรวมข้อมูลกลุ่มตัวอย่างในหน่วยงานภาครัฐ จำนวน 20 กระทรวง กระบวนการของการดำเนินงานในระยะที่ 1 ดังภาพที่ 1



ภาพที่ 2 กระบวนการของการดำเนินงานในระยะที่ 1

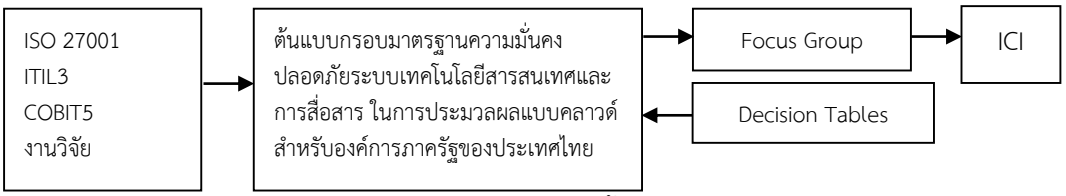
ระยะที่ 2 เพื่อออกแบบและพัฒนาตัวแบบความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์ ดังนี้

ขั้นตอนที่ 1 ศึกษาสภาพการพร้อมใช้งานในการประมวลผลแบบคลาวด์ และเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างนำมาพัฒนากรอบนโยบายความมั่นคงปลอดภัย โดยรับรองแบบสอบถามจากผู้เชี่ยวชาญตรวจสอบเครื่องมือในการวิจัย จำนวน 8 - 12 ท่าน กระบวนการของการดำเนินงานในระยะที่ 2 ดังภาพที่ 2



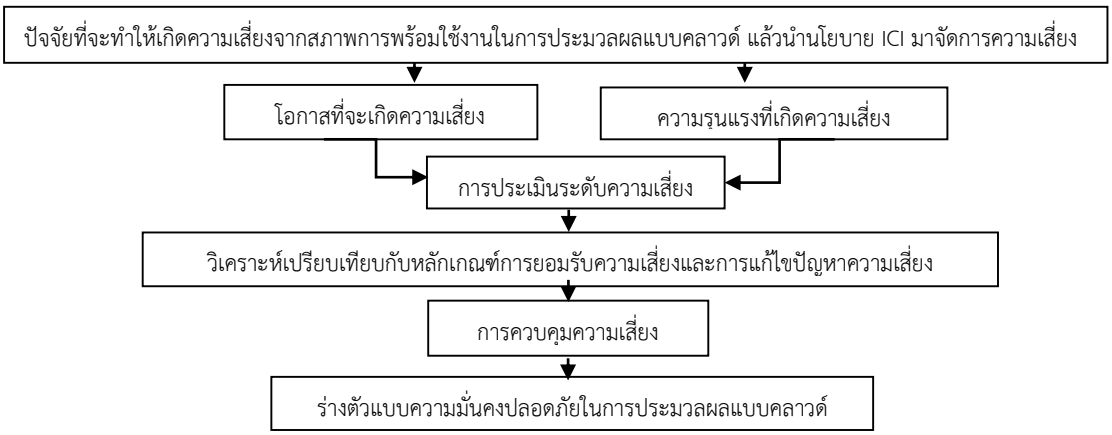
ภาพที่ 3 กระบวนการของการดำเนินงานในระยะที่ 2 ขั้นตอนที่ 1

ขั้นตอนที่ 2 ออกแบบกรอบมาตรฐานความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์เพื่อประเมินความเสี่ยง โดยใช้มาตรฐาน ISO 27001:2013, COBIT5 และ ITIL3 มาเป็นกรอบในการออกแบบและคัดเลือกข้อมาตรฐานจากตารางการตัดสินใจ รับรองโดยผู้เชี่ยวชาญในการคัดเลือกข้อมาตรฐานจำนวน 8 ท่าน โดยวิธีการประชุมกลุ่มได้กรอบนโยบายใหม่ เรียกว่า ICI (ISO COBIT ITIL) กระบวนการของการดำเนินงานในระยะที่ 2 ขั้นตอนที่ 2 ดังภาพที่ 4



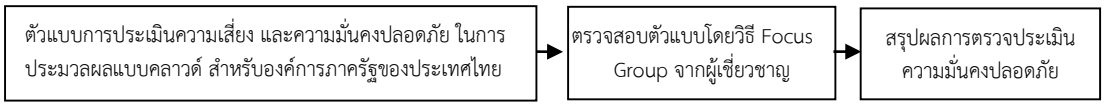
ภาพที่ 4 กระบวนการของการดำเนินงานในระยะที่ 2 ขั้นตอนที่ 2

ขั้นตอนที่ 3 วิเคราะห์และประเมินความเสี่ยงเพื่อหาแนวทางการป้องกันความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์ จากมาตรฐาน ICI มาวิเคราะห์ประเมินความเสี่ยง จำนวน 20 กระทรวง โดยใช้ขั้นตอนการวิเคราะห์ความเสี่ยงจากมาตรฐาน OCTAVE^{SM} มีขั้นตอนดังภาพที่ 5



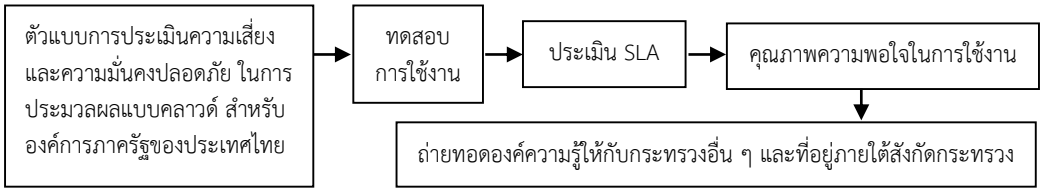
ภาพที่ 5 กระบวนการของการดำเนินงานในระยะที่ 2 ขั้นตอนที่ 3

ขั้นตอนที่ 4 เพื่อประเมินความพึงพอใจของตัวแบบจากผู้เชี่ยวชาญและผู้ใช้งานทั่วไป โดยวิธีการประชุมกลุ่ม จำนวน 8 - 12 ท่าน ประเมินตัวแบบและพิจารณาความถูกต้องของตัวแบบความมั่นคงปลอดภัย เพื่อรับรองสภาพความเป็นจริงของตัวแบบสามารถนำไปใช้เป็นต้นแบบใช้กับหน่วยงานภาครัฐอื่น ๆ ได้ กระบวนการของการดำเนินงานในระยะที่ 2 ขั้นตอนที่ 4 ดังภาพที่ 6



ภาพที่ 6 กระบวนการของการดำเนินงานในระยะที่ 2 ขั้นตอนที่ 4

ระยะที่ 3 เพื่อประเมินประสิทธิภาพของตัวแบบความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์ มาประยุกต์ใช้กับงานจริง และประเมินการใช้งานของระบบ (SLA: Service Level Agreement) และนำไปเผยแพร่ ถ่ายทอดองค์ความรู้ให้กับหน่วยงานอื่น ๆ มากกว่า 1 องค์กร ทั้ง 3 ตัวแบบ กระบวนการของการดำเนินงานในระยะที่ 3 ดังภาพที่ 7



ภาพที่ 7 กระบวนการของการดำเนินงานในระยะที่ 3

ระยะที่ 4 การนำเสนอ ตัวแบบการประเมินความเสี่ยงและความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ โดยนำหลักการมาตรฐาน OCTAVE^{SM} มาเป็นต้นแบบการประเมินความเสี่ยงในการประมวลผลแบบคลาวด์ โดยใช้นโยบาย ICI มาใช้ในการประเมินความเสี่ยง

5. ผลการวิจัย

ผลจากการวิเคราะห์ข้อมูลการวิจัย ระยะที่ 1 พบว่าในลักษณะส่วนบุคคล ได้แก่ ผู้ใช้งาน ผู้ดูแลระบบ ผู้บริหาร ตำแหน่งการทำงาน วุฒิการศึกษา ประสบการณ์ การใช้งานมีลักษณะที่แตกต่างกันไปตามหน้าที่การทำงานแต่ละลักษณะ ระยะเวลาของการใช้คอมพิวเตอร์ของแต่ละหน่วยงานไม่พบข้อแตกต่างกันและส่วนใหญ่จะมีการทำงานที่เกี่ยวข้องกับการใช้งาน การประมวลคลาวด์ทั้งสิ้น ซึ่งการบริหารจัดการความเสี่ยง มีปัจจัยที่สำคัญ 5 ด้าน ได้แก่ คน การเงิน อุปกรณ์ การบริหารจัดการและทางด้านนโยบาย ซึ่งมีค่าเฉลี่ยความรุ่นแรงและโอกาสที่จะเกิดความเสี่ยงโดยรวมอยู่ในระดับที่ต่ำมาก เนื่องด้วยมีหน่วยงานสำนักงานพัฒนารัฐบาลดิจิตอลช่วยดูแลในเรื่องความมั่นคงปลอดภัย

ผลการวิเคราะห์ข้อมูลการวิจัย ระยะที่ 2 ขั้นตอนที่ 1 พบว่าการศึกษาสภาพการพร้อมใช้งานในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ จากแบบสอบถามและเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง เพื่อนำมาพัฒนากรอบมาตรฐานความมั่นคงปลอดภัยทางด้านเทคโนโลยี

จากหน่วยงานที่มีการใช้งานระบบการประมวลผลแบบคลาวด์ และรับรองแบบสอบถามจากผู้เชี่ยวชาญจำนวน 8 ท่าน โดยมีเกณฑ์แนวการคิดระดับความเสี่ยงของ เบสต์ (Best, John W., 1981) สรุปได้ดังนี้

ตารางที่ 1 สภาพความพร้อมใช้งานในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ

โอกาสและความรุนแรงที่จะเกิดความเสี่ยง	ค่าสถิติความเสี่ยง		
ค่าสภาพความพร้อมใช้งานในการประมวลผลแบบคราวด์สำหรับองค์การภาครัฐ	$\bar{X}$	**S.D.**	**ระดับ**
1.ค่าโอกาสที่เกิดความเสี่ยงด้านใช้บริการซอฟต์แวร์ในการประมวลผลแบบคลาวด์	1.65	0.75	ต่ำมาก
2. ค่าความรุนแรงที่เกิดความเสี่ยงการบริการซอฟต์แวร์การประมวลผลแบบคลาวด์	1.65	0.75	ต่ำมาก
3. ค่าโอกาสที่เกิดความเสี่ยงการบริการแพลตฟอร์มในการประมวลผลแบบคลาวด์	1.80	0.90	ต่ำมาก
4. ค่าความรุนแรงเกิดความเสี่ยงการใช้บริการแพลตฟอร์มประมวลผลแบบคลาวด์	1.78	0.89	ต่ำมาก
5. ค่าโอกาสที่จะเกิดความเสี่ยงการบริการโครงสร้างพื้นฐาน	1.63	0.76	ต่ำมาก
6. ค่าความรุนแรงที่จะเกิดความเสี่ยงการใช้โครงสร้างพื้นฐาน	1.63	0.76	ต่ำมาก
ผลรวม	1.69	0.80	ต่ำมาก

ผลการวิเคราะห์การสัมภาษณ์ผู้บริหารด้านเทคโนโลยีสารสนเทศ สรุปได้ดังนี้

มีการติดตั้งการประมวลผลประเภทคลาวด์แบบส่วนตัว (Private Cloud) มีการให้บริการการประมวลผลแบบคลาวด์ประเภทโครงสร้างพื้นฐานเป็นส่วนใหญ่ มีแนวทางในการดูแลบำรุงรักษาระบบการประมวลผลแบบคลาวด์ 3 แบบ ดังนี้ 1) การเฝ้าสังเกตการณ์ 2) งานบำรุงรักษากรณีปกติ และ 3) งานซ่อมบำรุงกรณีชำรุด ทุกหน่วยงานใช้บริการระบบการประมวลผลแบบคลาวด์จากสำนักงานพัฒนารัฐบาลดิจิทัล ความถี่โดยเฉลี่ยการใช้งานมากกว่า 4 ครั้งต่อเดือน โดยปฏิบัติตามมาตรฐานสากล ISO 27001 การวิเคราะห์ความเสี่ยงตรวจสอบตามรายงานความปลอดภัยทุกเดือน ปัญหาที่ต้องเร่งแก้ไขด้านความมั่นคงปลอดภัยต้องมีการตรวจสอบความปลอดภัยของข้อมูลอย่างสม่ำเสมอ มีนโยบายแผนปฏิบัติการและความพร้อมการใช้งานพร้อมรับมือความเสี่ยง

ผลการวิเคราะห์ข้อมูลการวิจัย ระยะที่ 2 ขั้นตอนที่ 2 พบว่าการออกแบบนโยบายความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ สร้างจากมาตรฐานสากลจำนวน 3 มาตรฐาน ได้แก่ มาตรฐาน ISO 27001:2013, COBIT5, และ ITIL3 โดยการคัดเลือกแบบตารางการตัดสินใจเป็นตารางแบบ 2 มิติ จัดกลุ่มรวมเป็นนโยบายเดียวกันและส่วนที่คล้ายคลึงกันได้ทั้งสิ้น 18 ประเด็นและนำเสนอผู้เชี่ยวชาญ (Focus Group) เพื่อยืนยันข้อมาตรฐานต่าง ๆ เพื่อเป็นข้อนโยบายความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐของประเทศไทย (ICI)

ผลการวิเคราะห์ข้อมูลการวิจัย ระยะที่ 2 ขั้นตอนที่ 3 พบว่าการวิเคราะห์ประเมินความเสี่ยงเพื่อนำเสนอแนวทางการป้องกันความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ โดยจะเน้นที่กลุ่มตัวอย่างของสำนักงานปลัดกระทรวง อย่างน้อย 2 กระทรวง โดยนำผลที่ได้จากแบบสอบถาม มาวิเคราะห์ประเมินความเสี่ยง โดยใช้มาตรฐาน OCTAVE^{SM} มาเป็นต้นแบบการวิเคราะห์ความเสี่ยงอยู่ระดับที่ 4 มีทั้งหมด 67 ข้อ โดยมีระดับความเสี่ยงน้อย (Low) หมายถึงควรได้รับการตรวจสอบ และแผนการควบคุมที่มีอยู่สามารถแก้ไขปัญหาและรับมือกับความเสี่ยงได้

ตารางที่ 2 ค่าเมตริกซ์ระดับความเสี่ยงของหน่วยงานภาครัฐของประเทศไทย

Risk Assessment Matrix			ผลกระทบระดับความรุนแรงของความเสี่ยง Consequences (C)				
			น้อยมาก	น้อย	ปานกลาง	สูง	สูงมาก
			1	2	3	4	5
โอกาสที่จะเกิดความเสี่ยง Likelihood (L)	สูงมาก (Almost Certain)	5					
	สูง (Likely)	4					
	ปานกลาง(Moderate)	3					
	น้อย (Unlikely)	2		4 (67 ข้อ)			
	น้อยมาก (Rare)	1					

มากที่สุด มาก ปานกลาง ต่ำ ต่ำมาก

ผลการวิเคราะห์ข้อมูลการวิจัย ระยะที่ 2 ขั้นตอนที่ 4 พบว่าประเมินตัวแบบจากผู้เชี่ยวชาญและผู้ใช้งานทั่วไป ตรวจสอบตัวแบบการนำไปใช้โดยการใช้วิธีวิจัยแบบการประชุมกลุ่มเพื่อรวบรวมความคิดเห็นของกลุ่มผู้เชี่ยวชาญในการตรวจประเมินตัวแบบการประเมินความเสี่ยง จำนวน 8 ท่าน มาประเมินตัวแบบและพิจารณายืนยันความถูกต้องของตัวแบบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศในการประมวลผลแบบคลาวด์สำหรับหน่วยงานภาครัฐที่สมบูรณ์ตามมาตรฐานและยืนยันสภาพความเป็นจริงของตัวแบบและสามารถนำไปเป็นต้นแบบความมั่นคงปลอดภัยและยังสามารถตรวจสอบการประเมินได้ รวมทั้งสามารถสรุปผลการตรวจประเมินความมั่นคงปลอดภัยได้และยังสามารถใช้กับหน่วยงานภาครัฐอื่น ๆ ได้อีกด้วย

ผลการวิเคราะห์ข้อมูลการวิจัย ระยะที่ 3 การเปรียบเทียบประเมินค่าประสิทธิภาพความมั่นคงปลอดภัยจากผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจำนวน 10 ท่าน มีค่าการประเมินประสิทธิภาพจากมาตรฐาน ISO 27001 (เดิม) เท่ากับ 3 คะแนน สามารถแปลค่าประสิทธิภาพได้อยู่ในระดับปานกลาง เมื่อได้จัดแนวนโยบายใหม่ (ICI) จะมีค่าประสิทธิภาพเพิ่มขึ้นเท่ากับ 5 สามารถแปลค่าประสิทธิภาพอยู่ในระดับที่สูงมาก ทำให้ค่าประสิทธิภาพเพิ่มขึ้นเท่ากับร้อยละ 66.67 นำผลที่ได้ไปถ่ายทอดองค์ความรู้ให้กับกระทรวง 20 กระทรวง และหน่วยงานที่อยู่ภายใต้กระทรวง เพื่อเป็นแนวทางในการป้องกันความมั่นคงปลอดภัยกับอุปกรณ์ ข้อมูลข่าวสาร โดยการนำมาตรฐาน 3 มาตรฐาน ได้แก่ ISO, COBIT และ ITIL มาใช้เป็นต้นแบบในการกำหนดแนวนโยบายใหม่ที่ชื่อว่า ICI มาดำเนินการประเมินความเสี่ยงขององค์การภาครัฐ ตามหลักมาตรฐาน OCTAVE Framework เพื่อเป็นต้นแบบสำหรับองค์การภาครัฐ และสามารถนำไปใช้งานและเผยแพร่ต่อไปได้

ตารางที่ 3 สรุปภาพรวมการเปรียบเทียบค่าประสิทธิภาพความมั่นคงปลอดภัย

ข้อมาตรฐาน	คะแนนค่าประสิทธิภาพ				ค่า Coverage (%)
	ISO 27001		ICI		
	คะแนน	แปลผล	คะแนน	แปลผล	
1. ด้านบุคลากร	4	มาก	5	มากที่สุด	25.00
2. ด้านการเงิน	2	น้อย	5	มากที่สุด	150.00
3. ด้านอุปกรณ์	4	มาก	5	มากที่สุด	25.00
4. ด้านบริหารจัดการ	3	ปานกลาง	5	มากที่สุด	66.67
5. ด้านนโยบายของรัฐ	3	ปานกลาง	5	มากที่สุด	66.67
5. ด้านการบริการ	2	น้อย	5	มากที่สุด	150.00
ค่าเฉลี่ยประสิทธิภาพโดยรวม	**3**	**ปานกลาง**	**5**	**มากที่สุด**	**66.67**

ผลการวิเคราะห์ข้อมูลการวิจัย ระยะที่ 4 พบว่าการนำเสนอตัวแบบการประเมินความเสี่ยงและความมั่นคงปลอดภัย จากการรวมมาตรฐาน 3 มาตรฐาน ได้แก่ มาตรฐาน ISO 27001:2013, COBIT5 และ ITIL3 มาเป็นตัวแบบนโยบายความมั่นคงปลอดภัยในการประมวลผลคลาวด์สำหรับองค์การภาครัฐของประเทศไทย (ICI) โดยมีการรับรองจากผู้เชี่ยวชาญด้วยเทคนิคโฟกัสกรุ๊ป และนำหลักการมาตรฐาน OCTAVE^{SM} มาใช้เป็นต้นแบบในการประเมินความเสี่ยง ตามหลักขบวนการประเมินความเสี่ยง ประกอบไปด้วย 7 ขั้นตอน ดังนี้

1. กำหนดวัตถุประสงค์ (Risk Objective Setting) หรือทบทวนวัตถุประสงค์ จากการเก็บรวบรวมข้อมูลและแนวทางของภัยคุกคามที่จะเกิดความเสี่ยง

2. ระบุความเสี่ยง (Risk Identification) ที่มีค่าต่อวัตถุประสงค์ ภารกิจ สถานะ ระบุจุดอ่อนหรือช่องโหว่ที่อาจจะเกิดขึ้น โดยการวิเคราะห์ความสำคัญของทรัพย์สิน

3. ประเมินความเสี่ยงที่มีต่อสิ่งมีค่า (Risk Assessment) จากภัยคุกคามที่มีต่อสิ่งมีค่าโดยการนำแนวนโยบายความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐของประเทศไทย (ICI) มาเป็นข้อกำหนดในการประเมินความเสี่ยง

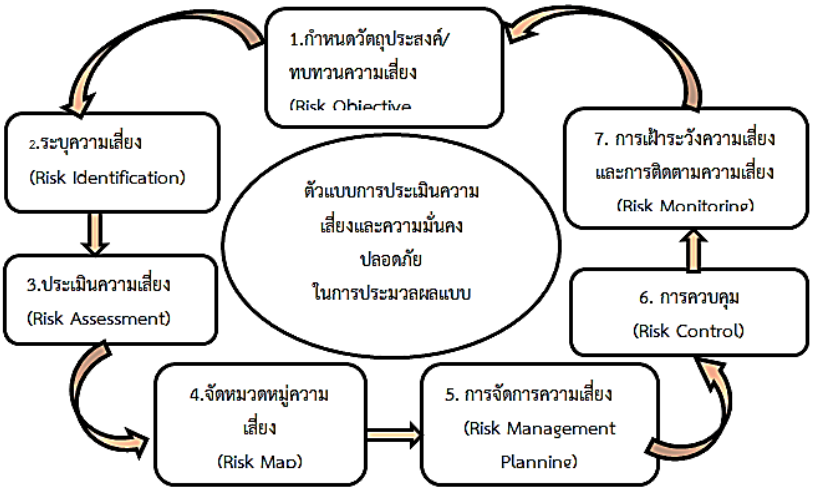
4. การจัดหมวดหมู่ความเสี่ยง (Risk Map) โดยนำปัจจัยความเสี่ยงที่ได้มาจัดระดับความรุนแรงเพื่อเลือกวิธีการที่จะสามารถรอรับความเสี่ยงได้อย่างเพียงพอและเหมาะสมต่อไป

5. การจัดการความเสี่ยง (Risk Management Planning) โดยดำเนินการแก้ไขความเสี่ยงจากระดับความเสี่ยงที่มีมากที่สุดก่อนเพื่อลดความรุนแรงและผลกระทบให้อยู่ในเกณฑ์ที่สามารถยอมรับได้ จากนั้นก็ดำเนินการแก้ไขความเสี่ยงอื่น ๆ รองลงไปจนหมด

6. การควบคุมความเสี่ยง (Risk Controllers) หาวิธีการจัดการความเสี่ยงไม่ให้เกิดขึ้นอีก

7. เฝ้าระวังและการติดตามความเสี่ยง (Risk Monitoring) ที่อาจกลับมาเกิดเหตุขึ้นใหม่และจัดหาวิธีการเพื่อป้องกันความเสี่ยงที่อาจจะกลับมาเกิดขึ้นอีก ให้อยู่ในระดับที่สามารถยอมรับได้

และสรุปได้ดังภาพที่ 8



ภาพที่ 8 ตัวแบบการประเมินความเสี่ยงและความมั่นคงปลอดภัย ในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ

6. สรุปผลและอภิปรายผล

6.1 สรุปผลจากการวิจัยการปะเมินความเสี่ยงและความมั่นคงปลอดภัยตามวัตถุประสงค์ได้ดังนี้

1) ผลการสำรวจ วิเคราะห์ และประเมินผลจากปัจจัยความเสี่ยงในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ พบว่าในลักษณะส่วนบุคคล อันได้แก่ ผู้ใช้งาน ผู้ดูแลระบบ ผู้บริหาร ตำแหน่งการทำงาน วุฒิการศึกษา ประสบการณ์ มีลักษณะที่แตกต่างกันไปตามหน้าที่การทำงาน แต่ระยะเวลาของการใช้คอมพิวเตอร์ของแต่ละหน่วยงานไม่พบข้อแตกต่างกัน ส่วนใหญ่จะมีการทำงานที่เกี่ยวข้องกับการใช้งานคลาวด์คอมพิวติ้งทั้งสิ้น โดยมีปัจจัยที่สำคัญ 5 ด้าน ได้แก่ คน การเงิน อุปกรณ์ การบริหารจัดการ และทางด้านนโยบาย มีค่าเฉลี่ยความรุนแรงและโอกาสที่จะเกิดความเสี่ยงมีค่าในระดับที่ต่ำมาก เนื่องจากมีสำนักงานพัฒนารัฐบาลดิจิตอลมาช่วยดูแลการใช้งานคลาวด์คอมพิวติ้งด้วย

2) ผลการออกแบบและพัฒนาตัวแบบความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ พบว่าการออกแบบนโยบายความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ สร้างจากมาตรฐานสากล 3 มาตรฐาน ได้แก่ มาตรฐาน ISO 27001 : 2013 COBIT5 และ ITIL3 มาออกแบบนโยบายความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ โดยการคัดเลือกแบบตารางการตัดสินใจ นำเสนอผู้เชี่ยวชาญ (Focus Group) เพื่อยืนยันข้อมาตรฐานต่าง ๆ เพื่อเป็นข้อนโยบายความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ (ICI) มีจำนวนทั้งสิ้น 4 โดเมน 26 วัตถุประสงค์ 109 ข้อย่อย เพื่อนำมาเป็นตัวแบบมาประเมินความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ

3) ผลการประเมินประสิทธิภาพของตัวแบบความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์สำหรับองค์การภาครัฐ พบว่าค่าประสิทธิภาพของตัวแบบเดิมมีค่าเท่ากับ 3 และเมื่อได้จัดทำแนวนโยบายใหม่มีค่าประสิทธิภาพการใช้งานเพิ่มขึ้นเท่ากับ 5 ทำให้ค่าประสิทธิภาพของตัวแบบ

มีค่าประสิทธิภาพเพิ่มขึ้นจากเดิมถึงร้อยละ 66.67 และตัวแบบ ICI สามารถนำถ่ายทอดองค์ความรู้ด้านตัวแบบความมั่นคงปลอดภัยให้กับหน่วยงานภาครัฐทั้งหมด 20 กระทรวง

6.2 การอภิปรายผลการวิจัย

1) ต้องมีการสร้างสมรรถนะในการใช้ไอทีให้มีประสิทธิภาพ ให้มีทักษะความรู้ความสามารถในการใช้งาน และลดช่องว่างระหว่างบุคลากร สร้างเสริมความรู้ความเข้าใจในเรื่องเทคโนโลยีมากยิ่งขึ้น เพื่อนำไปสู่การตัดสินใจในการแก้ไขปัญหาและเพิ่มขีดความสามารถให้แก่ตนเองได้

2) ต้องใช้ไอทีให้มีประสิทธิภาพ ทักษะความรู้ความสามารถในการใช้งาน มีความเข้าใจเพื่อมาตัดสินใจแก้ไขปัญหาที่สิ่งเกิดขึ้น และเพิ่มขีดความสามารถให้แก่ตนเองได้

3) ลักษณะบุคคลที่มีความแตกต่างกัน ใช้เทคโนโลยีที่แตกต่างกัน มีการใช้เทคโนโลยีที่มีความสอดคล้องกันกับวิทยานิพนธ์ของศิริวรรณ คร้ามกลาง (Khadkhang, S., 2014) ปัจจัยที่มีอิทธิพลต่อทัศนคติและความตั้งใจใช้บริการระบบการจัดเก็บข้อมูลบนก้อนเมฆของกลุ่มคนวัยทำงานในเขตกรุงเทพมหานคร จำแนกตามสถานที่ อายุ ตำแหน่ง อายุราชการ คุณวุฒิการศึกษา ลักษณะงานที่รับผิดชอบ ในการใช้ประโยชน์ทางด้านเทคโนโลยีสารสนเทศ มีความสัมพันธ์กับการยอมรับเทคโนโลยีสารสนเทศ ซึ่งลักษณะส่วนบุคคลต่าง ๆ จะมีความสอดคล้องกันและเกิดการยอมรับในการใช้งานเทคโนโลยี

7. เอกสารอ้างอิง

Best, John W. (1981). Research in Education. 3rd.ed. **Englewood cliffs**, New Jersey: Prentice. Hall Inc.

Boonsom, A. (2005). **Opinions of Provincial Electricity Authority employees, Information Division and communicate with the implementation of information technology systems in the operation.** Master of Arts Thesis in Political Science Department of Political Science and Public Administration, Kasetsart University.

Biswas, Sourya. (2011). **How Can Cloud Computing Help in Education?.** [Online] Available http://www.cloudweaks.com/2011/20/how-can-cloud-computing-help-in-education. Access on 18/08/2017.

Khadkhang, S. (2014). **Factors influencing attitude and the intention to use the storage system Information on clouds of working people in Bangkok.** Research Report, Bangkok University, Bangkok.

Khummanee, S. (2013). **Security of Cloud Computing Technology.** Master of Science Thesis in Computer Science Faculty of Information Science, Mahasarakham University.

Krejcie, R. V. & Morgan, D. W. (1970). Determining Sample Size for Research Activities. **Educational and Psychological Measurement,** 30(3), pp. 607-610.

Mell, P. and Grace, T. (2011). The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. **NIST Special Publication.** (800-145), 800-145.

Ministry of Information and Communication Technology. (2015). **Strategic Plan, ICT2020 Policy Framework.** Office of the Permanent Secretary for Information and Communication Technology.

Prithiphan, S. (2010). Research Methods for Business. 3rd.ed. Bangkok: **Hasun Printing.**

Yamane, Taro. (1973). **Statistics: An Introductory Analysis.** Third editio. Newyork: Harper and Row Publication.