การพัฒนากรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการบริการประมวลผลแบบคลาวด์
Development of Cyber Resilience Framework for Cloud Computing Services

เอกฉัตร บ่ายคล้อย (Ekkachat Baikloy)* ประสงค์ ปราณีตพลกรัง (Prasong Praneetpolgrang)*
และ นิเวศ จิระวิชิตชัย (Nivet Jirawichitchai)*

Received : November 28, 2017
Revised : May 30, 2018
Accepted : June 24, 2019

บทคัดย่อ

การวิจัยครั้งนี้ มีวัตถุประสงค์ 1) เพื่อสร้างกรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการบริการประมวลผลแบบคลาวด์ และ 2) เพื่อพัฒนาวิธีประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการบริการประมวลผลแบบคลาวด์ เป็นการวิจัยเชิงคุณภาพและเชิงประยุกต์ ทั้งนี้ได้ทำการศึกษาทฤษฎี และงานวิจัยที่เกี่ยวข้อง รวมทั้งอิงกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ สหรัฐอเมริกา (NIST) จากการสัมภาษณ์เชิงลึก การสนทนากลุ่มกับผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์ และเก็บข้อมูลจาก ผู้ให้บริการแบบคลาวด์ พบว่า แนวโน้มการโจมตีทาง ไซเบอร์มีความรุนแรง และใช้วิธีการโจมตีที่ชาญฉลาด มากขึ้น ผู้วิจัยได้นำข้อมูลที่ได้มาทำการสังเคราะห์กรอบการคืนสภาพได้ด้านไซเบอร์ของการบริการประมวลผลแบบคลาวด์ รวมทั้งพัฒนาแอปพลิเคชันสำหรับผู้ให้บริการแบบคลาวด์ สามารถนำไปประเมินองค์กรตนเอง เพื่อทำการปรับปรุงและพัฒนาระดับความมั่นคงปลอดภัยไซเบอร์ในระบบการบริการประมวลผลแบบคลาวด์และระดับ การคืนสภาพได้ด้านไซเบอร์ให้ดียิ่งขึ้นในอนาคต

คำสำคัญ: การบริการประมวลผลแบบคลาวด์ ความมั่นคงปลอดภัยไซเบอร์ การคืนสภาพได้ด้านไซเบอร์

Abstract

The purposes of this research were 1) to create a cyber resilience framework for cloud computing services and 2) to develop an evaluating method of cyber resilience for cloud computing services. The qualitative and applied researches were methodologies that underlied both in related theories and the NIST cybersecurity framework. The research focused on both in-depth interviews and focus group with cybersecurity experts include with collecting data from cloud service providers. With the data analysis process, it found that cyber attacks became more violent, sophisticated and smart attacks. However, researchers synthesized and developed cyber resilience framework for cloud computing services. In addition, application was developed for cloud computing service providers that they could adopt to self- evaluation in order to improve and develop on cybersecurity level for cloud computing services and cyber resilience in the future.

Keywords: Cloud Computing Services, Cybersecurity, Cyber Resilience.

1. บทนำ

เทคโนโลยีดิจิทัลโดยเฉพาะอย่างยิ่ง การบริการประมวลผลแบบคลาวด์ หรือคลาวด์คอมพิวติงเซอร์วิสนั้น ได้มีบทบาทความสำคัญต่อการพลิกฟื้น ปรับปรุงและยกระดับประสิทธิภาพการทำงานขององค์กร และหน่วยงานภาคธุรกิจ ซึ่งธุรกิจส่วนใหญ่ได้พยายามปรับรูปแบบการดำเนินงานมาอยู่บนแพลตฟอร์มของ การทำงานแบบคลาวด์ ทั้งนี้จะทำให้การทำงานสามารถประหยัดค่าใช้จ่ายและมีประสิทธิภาพมากยิ่งขึ้น ที่สำคัญคือสามารถขับเคลื่อนธุรกิจให้มีความคล่องตัว และสร้างมูลค่าเพิ่มให้กับผู้มีส่วนได้ส่วนเสียของธุรกิจได้เป็นอย่างดี นอกเหนือจากนั้น สิ่งที่ควร

* บัณฑิตศึกษา คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
* Graduate School, Faculty of Information Technology, Sripatum University.

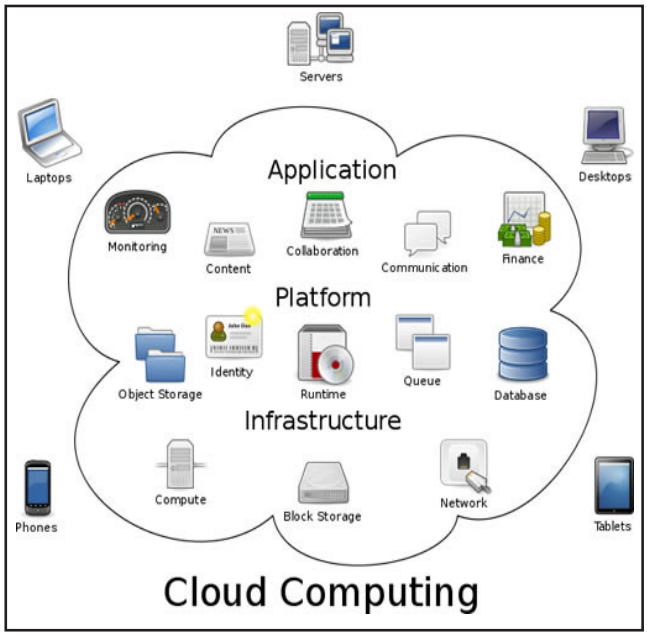
ต้องพิจารณาควบคู่กันไปด้วยคือเรื่องของความมั่นคงปลอดภัยไซเบอร์จากระบบการบริการประมวลผลแบบคลาวด์

ในปัจจุบัน ผู้ให้การบริการหรือตัวแทนผู้ให้การบริการประมวลผลแบบคลาวด์มีจำนวนมาก กลุ่มผู้ใช้หรือลูกค้าธุรกิจต่างพิจารณาเลือกใช้การบริการประมวลผลแบบคลาวด์ หากแต่ยังมีข้อกังวลในเรื่องความเสี่ยงและความมั่นคงปลอดภัยไซเบอร์ของการบริการประมวลผล แบบคลาวด์ ดังนั้น ผู้วิจัยจึงมีความสนใจที่จะศึกษาเกี่ยวกับกรอบการคืนสภาพได้ด้านไซเบอร์และวิธีประเมินการคืนสภาพได้ [4] ด้านไซเบอร์ สำหรับการบริการประมวลผลแบบคลาวด์ เพื่อสร้างความมั่นใจให้กลุ่มลูกค้าธุรกิจและผู้ให้การบริการดำเนินธุรกิจได้อย่างมั่นคงปลอดภัยและมีความยั่งยืน อีกทั้งฝั่งผู้ประกอบธุรกิจให้บริการแบบคลาวด์และผู้รับการบริการจะได้มีแนวทางหรือหลักอ้างอิงในการปฏิบัติซึ่งจะทำให้เกิดความสะดวกและมีประโยชน์ต่อผู้ที่เกี่ยวข้องทุกภาคส่วนในการดำเนินงานทางธุรกิจต่าง ๆ

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 การบริการประมวลผลแบบคลาวด์

การประมวลผลแบบคลาวด์ (Cloud Computing) หมายถึงรูปแบบหนึ่งของการประมวลผลโดยใช้ทรัพยากรร่วมกันผ่านเครือข่าย ตามความต้องการได้อย่างสะดวกรวดเร็วจากทุกแห่งหน และทุกเวลา ทั้งนี้ ผู้ใช้ไม่ต้องบริหารจัดการทรัพยากรเอง ตัวอย่างทรัพยากร เช่น เครือข่าย เครื่องแม่ข่าย หน่วยเก็บข้อมูล ซอฟต์แวร์ประยุกต์และการบริการแบบคลาวด์ ในขณะที่ การบริการแบบคลาวด์ (Cloud Services) หรือการบริการประมวลผลแบบคลาวด์ (Cloud Computing Services) จะหมายถึง การให้บริการผ่านการประมวลผลแบบคลาวด์ตามประเภทของการให้บริการหลัก ซึ่งผู้ใช้จะต้องสามารถเข้าถึงระบบอินเทอร์เน็ตบนอุปกรณ์อิเล็กทรอนิกส์ที่หลากหลาย ไม่ว่าจะเป็นเครื่องคอมพิวเตอร์ สมาร์ตโฟน หรือแท็บเล็ต ซึ่งจะช่วยให้ผู้ใช้สามารถทำงานได้อย่างคล่องตัว ประเภทของการให้บริการหลัก ได้แก่ 1) การบริการโครงสร้างพื้นฐาน (Infrastructure as a Service: IaaS) 2) การบริการแพลตฟอร์ม (Platform as a Service: PaaS) 3) การบริการซอฟต์แวร์ (Software as a Service: SaaS) ในกรณีของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) จะเน้นให้บริการคลาวด์ภาครัฐ (Government Cloud Service) เช่น การบริการโครงสร้างพื้นฐานด้านระบบเครือข่าย และการบริหารจัดการ 4) การบริการกระบวนการทางธุรกิจ (Business Process as a Service : BPaaS) ซึ่งเป็นการให้บริการทางธุรกิจอย่างเต็มระบบ ทั้ง 3 รูปแบบที่ได้กล่าวถึงข้างต้น (IaaS, PaaS, SaaS) [1] ดังภาพที่ 1 ได้แสดงการบริการประมวลผลแบบคลาวด์



ภาพที่ 1 *การบริการประมวลผลแบบคลาวด์*

รูปแบบการให้บริการแบบคลาวด์ ได้รับการออกแบบตามขั้นตอนการดำเนินธุรกิจ (Business Process) ซึ่งมีจุดมุ่งหมายหลักเพื่อให้ธุรกิจสามารถดำเนินงานได้ อย่างเต็มประสิทธิภาพ โดยเลือกใช้เฉพาะซอฟต์แวร์ และแอปพลิเคชันที่เหมาะสมกับกระบวนการทางธุรกิจแต่ละประเภท ทั้งนี้ผู้ใช้บริการไม่จำเป็นต้องกำหนดนโยบายในการบริหารจัดการใด ๆ ซึ่งการให้บริการแบบ BPaaS จะสามารถวัดผลประสิทธิภาพของกระบวนการทางธุรกิจที่เกิดขึ้นจากการใช้แอปพลิเคชันที่ใช้งานได้ ดังตารางที่ 1 ได้แสดงรูปแบบการให้บริการแบบคลาวด์โดยทั่วไป

การให้บริการแบบคลาวด์ นอกจากจะมีหลากหลายรูปแบบแล้ว ยังสามารถแบ่งลักษณะตามการใช้งานได้เป็น 3 ลักษณะ ได้แก่ คลาวด์องค์กร (Private Cloud), คลาวด์สาธารณะ (Public Cloud) และคลาวด์แบบผสมผสาน (Hybrid Cloud) ซึ่งเปรียบเสมือนผู้ใช้บริการนั้น มีระบบคอมพิวเตอร์ของตนเอง ทำการเชื่อมต่อกับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ของผู้ให้บริการ ซึ่งศูนย์ข้อมูลคอมพิวเตอร์จะต้อง

ตารางที่ 1 *รูปแบบการให้บริการแบบคลาวด์โดยทั่วไป*

Cloud Service Model	IaaS	PaaS	SaaS	BPaaS
Networking	Manage by Vendor	Manage by Vendor	Manage by Vendor	Manage by Vendor
Storage				
Operating System				
Virtualization				
Servers				
Data & Databases	Manage by User			
Security				
Middleware & Frameworks				
Platform & Frameworks				
Technical Services		Manage by User		
Business Services				
Applications				
BPM			Manage by User	
Monitoring				
Core Business				User

อยู่ภายใต้ระบบที่มีมาตรฐานและความมั่นคงปลอดภัยสูง เนื่องจากจะต้องสร้างความน่าเชื่อถือและความไว้วางใจในประสิทธิภาพของระบบทั้งหมดให้กับผู้ใช้บริการ

2.2 มาตรฐานปฏิบัติการบริการแบบคลาวด์

2.2.1 มาตรฐานปฏิบัติการบริการแบบคลาวด์ (Cloud Services Standard of Practice) โดยวิศวกรรมสถานแห่งประเทศไทย ในพระบรมราชูปถัมภ์ [2] กล่าวถึงการให้บริการประมวลผลแบบคลาวด์ หรือการให้บริการแบบคลาวด์ ว่าเป็นแนวความคิดใหม่ของการประยุกต์ใช้เทคโนโลยีดิจิทัลในปัจจุบัน โดยจะต้องมีระบบบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศหรือเทคโนโลยีดิจิทัลที่ทันสมัย และมีความยืดหยุ่น เพื่อจะได้สามารถรองรับธุรกิจได้ในหลายรูปแบบ ตามลักษณะการปฏิบัติงานของผู้ให้บริการและผู้ใช้บริการคลาวด์ในประเทศไทย ในด้านความมั่นคงปลอดภัยของข้อมูล และการเตรียมความพร้อมให้อยู่ในบรรทัดฐานเดียวกัน โดยมีข้อกำหนดให้ถือปฏิบัติดังนี้ 1) ระบบมาตรฐานเปิดและการทำงานร่วมกันของระบบ ทั้งข้อมูล โปรแกรม และฮาร์ดแวร์ 2) การเคลื่อนย้ายโปรแกรมและข้อมูล จาก ระบบหนึ่งไปสู่อีกระบบ และ 3) การบริหารจัดการสิทธิ์การเข้าถึงและเชื่อมต่อของข้อมูล

2.2.2 Cloud Security Alliance (CSA) เป็นองค์กรที่ออกแนวทางการปฏิบัติ โดยมีจุดประสงค์เพื่อให้ผู้ใช้บริการคลาวด์ มีความมั่นใจในการใช้บริการ โดยมีข้อกำหนดการควบคุมความมั่นคงปลอดภัยของระบบคลาวด์หลากหลายประเภท ภายใต้การประเมินและการรับรอง ในนาม CSA-STAR (Cloud Security Alliance – Security, Trust & Assurance Registry) การรับรองแบ่งออกเป็น 3 ประเภท คือ 1) STAR Entry – Self Assessment: มีการประเมินภายในองค์กรด้วยตนเอง โดยใช้แบบประเมิน CSA Consensus Assessment Initiative (CAI) หรือ Cloud Control Matrix (CCM) 2) STAR Certification/ Attestation: ต้องผ่านการประเมิน ISO27001 หรือ AICPA SOC2 จากบริษัทภายนอก และ 3) STAR Continuous: ต้องมีการตรวจสอบและประเมินความปลอดภัยของระบบคลาวด์ อย่างต่อเนื่อง

2.2.3 The Statement on Standards for Attestation Engagement (SSAE18) เป็นรายงาน การปฏิบัติตามกฎระเบียบขององค์กรที่เกี่ยวข้องกับการบริการ ซึ่งรวมถึงผู้ให้บริการแบบคลาวด์ เรียกรายงานนี้ว่า Service Organization Controls (SOC) แบ่งเป็น 3 ประเภท ดังนี้ SOC 1 เป็นรายงานเกี่ยวกับข้อมูลทางด้านการเงิน, SOC 2 เป็นรายงานประเมินประสิทธิภาพการควบคุมความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศภายในองค์กร โดยใช้หลักการ Trust Services ประกอบด้วย 5 เรื่อง คือ ความมั่นคงปลอดภัย, การรักษาสภาพพร้อมใช้งาน, การรักษาความถูกต้องของขั้นตอนการดำเนินงาน, การรักษาความลับ และ การรักษาข้อมูลความเป็นส่วนบุคคล สำหรับ SOC 3 จะเป็นรายงานการประเมินเฉพาะด้านความมั่นคงปลอดภัย, การรักษาสภาพพร้อมใช้งาน และการรักษาความลับ ซึ่งสามารถเผยแพร่สู่สาธารณะได้

2.2.4 ISO/IEC27001 เป็นมาตรฐานสากล ด้านระบบบริหารการรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security Management Systems – ISMS) ซึ่งมีข้อปฏิบัติ ตั้งแต่การเริ่มต้นทำระบบ, การดำเนินงาน, การทบทวน การปรับปรุงอย่างต่อเนื่อง ซึ่งสอดคล้องกับแนวคิดของหลักการ PDCA (Plan-Do-Check-Act)

2.2.5 ISO/IEC ISO 27002 ระบุถึงข้อควรปฏิบัติในการควบคุมความมั่นคงปลอดภัยของข้อมูล มีทั้งหมด 133 หัวข้อ สรุปทั้ง ISO/IEC 27001 และ ISO/IEC 27002

เน้นความสำคัญในเรื่อง “ระบบการบริหารจัดการ” โดยมีข้อกำหนดที่พึงปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อให้ได้รับการรับรองมาตรฐาน รวมถึงกำหนดให้มีการจัดทำแผนรับมือเหตุฉุกเฉินที่อาจเกิดขึ้นและคงไว้ซึ่งความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่อง [3]

2.2.6 ISO/IEC 27017 เป็นมาตรฐานสากล สำหรับการจัดการความมั่นคงปลอดภัยของการให้บริการคลาวด์ ซึ่งได้นำข้อปฏิบัติบางส่วน มาจาก ISO 27002 โดยเพิ่มข้อปฏิบัติด้านคลาวด์คอมพิวติง (Cloud Computing Service Set) เพื่อควบคุมการทำหน้าที่และความรับผิดชอบในเรื่องการจัดการความมั่นคงปลอดภัยของข้อมูลร่วมกัน ระหว่างผู้ใช้และผู้ให้บริการคลาวด์ ดังนี้ 1) ผู้ใช้บริการคลาวด์ต้องได้รับความคุ้มครองและได้รับสิทธิ์ในการเข้าถึงบริการคลาวด์อย่างชัดเจน ในสภาพแวดล้อมเสมือนที่ใช้ร่วมกันกับผู้ใช้บริการรายอื่นๆ 2) ข้อมูลลงบันทึกการปฏิบัติงาน (Operation Logs) และ ข้อมูลลงบันทึกเข้าออก (Logs) ในระบบบริการแบบคลาวด์ ต้องมีระบบการจัดการที่ถูกต้องเหมาะสม และ 3) การจัดการความเสี่ยงที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยข้อมูลบนคลาวด์ โดยมีข้อตกลงการรับประกันการบริการ (SLA) ระหว่างผู้ให้บริการกับผู้รับบริการ ในเรื่องของการรักษาความมั่นคงปลอดภัยของข้อมูลความเป็นส่วนบุคคลที่เก็บไว้ในระบบ

2.2.7 มาตรฐาน ISO/IEC 27018 เป็นแนวทางปฏิบัติงาน สำหรับผู้ให้บริการระบบคลาวด์สาธารณะ โดยเฉพาะเรื่อง การปกป้องรักษาข้อมูลส่วนบุคคล (Personal Identifiable Information) ซึ่งหมายถึง ข้อมูลที่สามารถระบุตัวบุคคลของผู้ใช้บริการ และเชื่อมโยงไปถึงบุคคลใดบุคคลหนึ่งบนเครือข่ายได้ อาทิ ชื่อ ที่อยู่ หมายเลขโทรศัพท์ หรือ อีเมล เป็นต้น

2.3 กรอบแนวคิดความมั่นคงปลอดภัยไซเบอร์

2.3.1 NIST Cybersecurity เวอร์ชัน 1.1 แสดงกรอบการปฏิบัติ Cybersecurity 5 เรื่อง [4] ประกอบด้วย 1) ระบุความเสี่ยง (Identify) ว่าด้วยเรื่องการจัดการทรัพยากร, สภาพแวดล้อมทางธุรกิจ, การกำกับดูแล 2) ป้องกันความเสี่ยง (Protect) เป็นการจัดทำมาตรการป้องกันที่เหมาะสมสำหรับการให้บริการโครงสร้างพื้นฐาน 3) ตรวจจับภัยคุกคาม (Detect) เพื่อตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจจะเกิดขึ้น 4) ตอบสนองต่อภัยคุกคาม (Respond) เตรียมการวางแผนรับมือ, การสื่อสาร, การวิเคราะห์, การลดความเสี่ยง และ 5) การกู้คืน (Recover) เป็นการปฏิบัติงานตามแผนอย่างต่อเนื่อง ซึ่งทั้ง 5 เรื่อง แบ่งออกเป็น 22 ประเด็นสำคัญ ดังตารางที่ 2

ตารางที่ 2 *กรอบการปฏิบัติงานของ NIST [5], [6]*

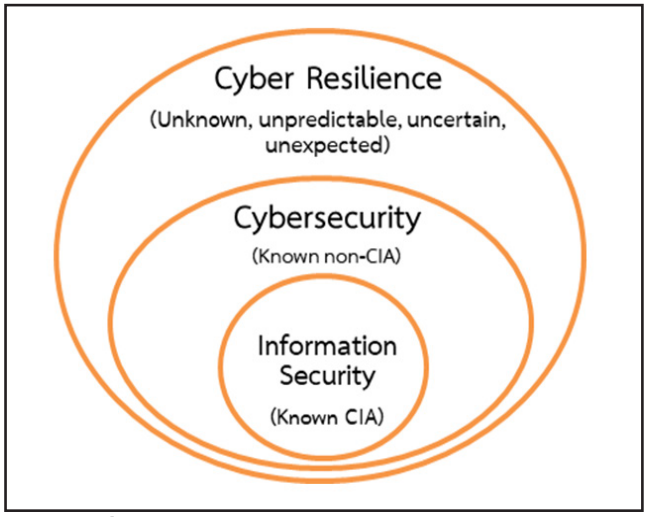
เรื่อง	ประเด็นภายใต้กรอบการทำงาน
1. ระบุความเสี่ยง (ID)	1.1 การจัดการสินทรัพย์ (Asset Management) (ID.AM)
	1.2 สภาพแวดล้อมทางธุรกิจ (Business Environment) (ID.BE)
	1.3 ธรรมาภิบาล (Governance) (ID.GV)
	1.4 การประเมินความเสี่ยง (Risk Assessment) (ID.RA)
	1.5 กลยุทธ์การบริหารความเสี่ยง (Risk Management Strategy) (ID.RM)
2. ป้องกันความเสี่ยง (PR)	2.1 การควบคุมสิทธิ์การเข้าถึง (Access Control) (PR.AC)
	2.2 การสร้างความตระหนักและการฝึกอบรม (Awareness and Training) (PR.AT)
	2.3 ความปลอดภัยของข้อมูล (Data Security) (PR.DS)
	2.4 กระบวนการและขั้นตอนการป้องกันข้อมูล (Information Protection Processes and Procedures) (PR.IP)
	2.5 การบำรุงรักษา (Maintenance) (PR.MA)
	2.6 เทคโนโลยีป้องกัน (Protective Technology) (PR.PT)
3.ตรวจจับภัยคุกคาม (DE)	3.1 ความผิดปรกติและเหตุการณ์ (Anomalies and Events) (DE.AE)
	3.2 การตรวจสอบความปลอดภัยอย่างต่อเนื่อง (Security Continuous Monitoring) (DE.CM)
	3.3 กระบวนการตรวจจับ (Detection Processes) (DE.DP)
4. ตอบสนองต่อภัยคุกคาม (RS)	4.1 การวางแผนตอบสนอง (Response Planning) (RS.RP)
	4.2 การสื่อสาร (Communications) (RS.CO)
	4.3 การวิเคราะห์ (Analysis) (RS.AN)
	4.4 การลดผลกระทบ (Mitigation) (RS.MI)
	4.5 การปรับปรุง (Improvements) (RS.IM)
5. คืนสภาพได้ (RC)	5.1 การวางแผนการกู้คืน/คืนสภาพ (Recovery Planning) (RC.RP)
	5.2 การปรับปรุง (Improvements) (RC.IM)
	5.3 การสื่อสาร (Communications) (RC.CO)

2.3.2 CIS Critical Security Controls [7], [8] เป็นแนวทางแก้ไขปัญหาด้านความมั่นคงปลอดภัย ขั้นวิกฤต โดยหน่วยงานศูนย์กลางด้านความมั่นคงปลอดภัย ในอินเทอร์เน็ต (Center for Internet Security) ได้แสดง 20 วิธีแก้ไขปัญหาเชิงปฏิบัติการที่สร้างมาเพื่อหยุดยั้งภัยคุกคาม โดยอ้างอิงกรอบการทำงานด้าน ความมั่นคงปลอดภัยไซเบอร์ของ NIST ดังตารางที่ 3

ตารางที่ 3 *กรอบการปฏิบัติงานความมั่นคงปลอดภัย CIS*

CIS Critical Security Control	อ้างอิง NIST
CSC 1: รายการอุปกรณ์ที่ได้รับอนุญาตและไม่ได้รับอนุญาต	ID.AM
CSC 2: รายการซอฟต์แวร์ที่ได้รับอนุญาตและไม่ได้รับอนุญาต	ID.AM
CSC 3: การกำหนดค่าความมั่นคงปลอดภัยของอุปกรณ์ผู้ใช้ปลายทาง	PR.IP
CSC 4: การประเมินและแก้ไขช่องโหว่อย่างต่อเนื่อง	ID.RA, RS.MI, DE.CM
CSC 5: การควบคุมการใช้สิทธิ์ผู้ดูแลระบบ	PR.AC
CSC 6: การบำรุงรักษาและการวิเคราะห์บันทึกการตรวจสอบ	DE.AE, RS.AN
CSC 7: การปกป้องอีเมลและเว็บเบราว์เซอร์	PR.PT
CSC 8: การป้องกันมัลแวร์	PR.PT, DE.CM
CSC 9: ข้อจำกัด และการควบคุมพอร์ตเครือข่ายโพรโทคอลและบริการ	PR.IP
CSC 10: ความสามารถในการกู้คืนข้อมูล	RC.RP
CSC 11: การกำหนดค่าความมั่นคงปลอดภัยของอุปกรณ์เครือข่าย	PR.IP
CSC 12: การป้องกันขอบเขตพื้นที่สำคัญ	DE.DP
CSC 13: การปกป้องข้อมูล	PR.DS
CSC 14: การควบคุมสิทธิ์เข้าถึงที่จำเป็น	PR.AC
CSC 15: การควบคุมการเข้าถึงแบบไร้สาย	PR.AC
CSC 16: การตรวจสอบและควบคุมบัญชี	PR.AC, DE.CM
CSC 17: การประเมินทักษะความมั่นคงปลอดภัยและการฝึกอบรมที่เหมาะสม	PR.AT
CSC 18: ความมั่นคงปลอดภัยของซอฟต์แวร์	PR.IP
CSC 19: การเผชิญเหตุการณ์และการจัดการ	DE.AE, RS.RP
CSC 20: การทดสอบการบุกรุก	RS.IM, RC.IM

2.3.3 Information Security Forum (ISF) เป็นคณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศจากประเทศอังกฤษ มีสมาชิกมากกว่า 500 หน่วยงานจากประเทศต่างๆ ทั่วโลก โดยมีจุดประสงค์เพื่อพัฒนามาตรฐาน คู่มือ ข้อแนะนำ และแนวปฏิบัติที่ดีด้านความมั่นคงปลอดภัยไซเบอร์ ISF ได้ทำการแบ่งภัยคุกคามและวิธีรับมือทางด้านความมั่นคงปลอดภัยไซเบอร์ 3 ระดับ [9] 1) ความมั่นคงปลอดภัยสารสนเทศ (Information Security) หรือ Known CIA คือ การรับมือภัยคุกคามที่ส่งผลกระทบกับเรื่อง CIA อันได้แก่เรื่อง การรักษาความลับ (Confidentiality), ความสมบูรณ์ของข้อมูล (Integrity) และ ความพร้อมใช้ (Availability) 2) ความมั่นคงปลอดภัย ไซเบอร์ (Cybersecurity) คือ การรับมือภัยคุกคามในระดับที่มีผลกระทบรุนแรงกว่าเรื่อง CIA 3) การคืนสภาพได้ด้าน ไซเบอร์ (Cyber Resilience) คือการจัดการกับภัยคุกคามที่ไม่เคยปรากฏมาก่อน แสดงแต่ละระดับไว้ ดังภาพที่ 2



ภาพที่ 2 *Cybersecurity and Cyber Resilience Model.*

2.3.4 Cyber Security Resilience Complete Self-Assessment Guide เป็นคู่มือประเมินความมั่นคงปลอดภัยและการคืนสภาพได้ทางไซเบอร์ โดยอ้างอิงจาก แนวปฏิบัติและมาตรฐาน [10] เพื่อให้องค์กรสามารถประเมินตนเองได้อย่างรวดเร็ว ในขอบเขต 7 เรื่อง คือ การตระหนักรู้ (Recognize), การกำหนดวิธีปฏิบัติ (Define), ชี้วัดความถูกต้อง (Measure), การวิเคราะห์ (Analyze), การปรับปรุง (Improve), การควบคุม (Control), การสนับสนุนให้เกิดการคืนสภาพได้ (Sustain)

2.4 งานวิจัยที่เกี่ยวข้อง

การศึกษาแบบการประเมินด้านการจัดการความเสี่ยงและความมั่นคงปลอดภัยไซเบอร์สำหรับให้บริการ ประมวลแบบคลาวด์ในแต่ละบริบท ซึ่งมีตัวอย่างงานวิจัยที่เกี่ยวข้องดังต่อไปนี้

ศุภลักษณ์และคณะ [11] ได้ศึกษาทฤษฎีเกี่ยวกับ Trust Model สำหรับการให้การบริการประมวลแบบคลาวด์ เพื่อจุดประสงค์ในการพัฒนาตัวแบบด้านความไว้วางใจในการให้บริการคลาวด์สำหรับภาครัฐ และนำผลที่ได้ไปศึกษาทำให้สามารถใช้ประโยชน์และนำไปสู่ความยั่งยืนของการพัฒนาด้านไอทีสำหรับองค์กรภาครัฐของไทย

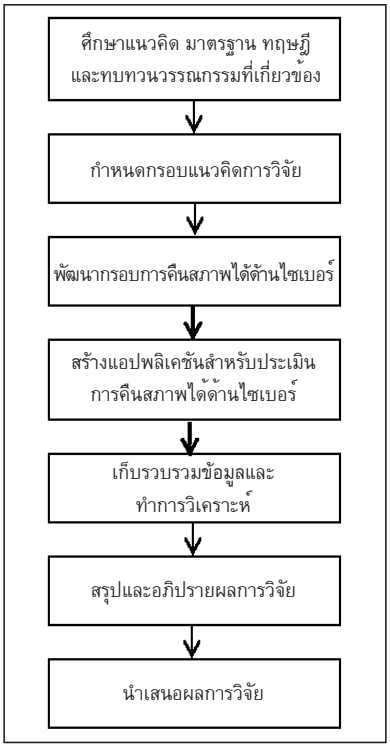
เทพฤทธิ์และคณะ [12] ได้ใช้แบบสำรวจข้อมูล ผู้ให้บริการโครงสร้างพื้นฐานคลาวด์ในประเทศ เพื่อศึกษาสถานภาพ ปัญหา เพื่อจะกระตุ้นศักยภาพในการแข่งขันด้านบุคลากรและเทคโนโลยีกับผู้ให้บริการคลาวด์รายใหญ่ ซึ่งจากผลสำรวจพบว่า ผู้ใช้บริการขาดความเชื่อมั่นด้านความมั่นคงปลอดภัยเกี่ยวกับข้อมูลส่วนบุคคล และ ผู้ให้บริการขาดบุคลากรที่มีความเชี่ยวชาญ ไม่มีการกำหนดมาตรฐานที่ชัดเจน

Ngoc T. Le และคณะ [6] ได้เสนอแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบการประมวลผลแบบคลาวด์ จำนวน 12 เรื่อง ซึ่งอ้างอิงมาจากมาตรฐานด้านความมั่นคงปลอดภัยของระบบคลาวด์และตัวแบบ วุฒิภาวะความสามารถต่างๆ อย่างเช่น ISO, NIST-CSF, SSE-CMM เพื่อนำมาจัดทำโมเดลในการวัดระดับความสามารถด้านความมั่นคงปลอดภัยของผู้ให้บริการระบบคลาวด์ (CSCMM) ซึ่งระบุเป็น 4 ระดับ SML0 (Undefined), SML1 (Initiated), SML2 (Managed) และ SML3 (Optimized) ซึ่งในระดับสูงสุดนี้เรียกได้ว่า เป็นระดับที่มีการปกป้องอย่างสมบูรณ์

Wendy และคณะ [13] ได้นำเสนอ 2 มาตรฐานการปฏิบัติงานด้านความมั่นคงปลอดภัยทางไซเบอร์ในเรื่อง Manage security (APO13), Manage security services (DSS05) ภายใต้ COBIT5.0 และหัวข้อ ในระบบบริหารการรักษาความปลอดภัยของข้อมูล (ISMS) ของ ISO27001/2013 มาใช้เป็นกรอบแนวทางการประเมินผู้ปฏิบัติงานในแผนกไอที ของมหาวิทยาลัย XYZ โดยนำผลค่าเฉลี่ยที่ได้นั้น มาจัดระดับวุฒิภาวะความสามารถเพื่อตรวจหาช่องโหว่ของความปลอดภัยในระบบประมวลผลแบบคลาวด์ พร้อมกับเสนอวิธีการแก้ปัญหาที่เกิดขึ้น ด้วยกระบวนการของ COBIT 5.0 และ ISO27001: 2013

3. วิธีดำเนินการวิจัย

ผู้วิจัยได้แสดงวิธีการดำเนินงานวิจัย ใน 7 ขั้นตอน โดยมีลำดับรายละเอียด ดังภาพที่ 3

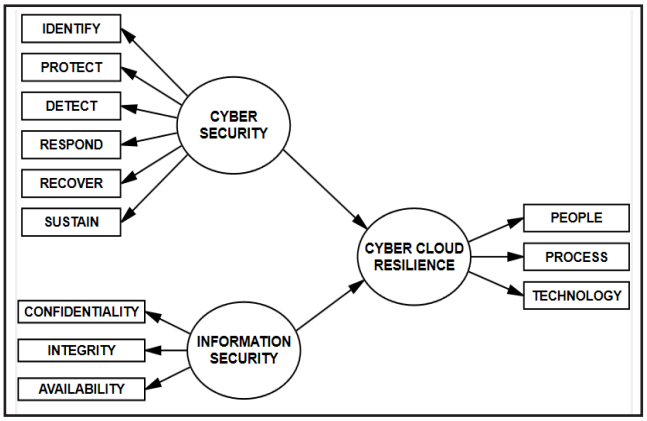


ภาพที่ 3 *วิธีการดำเนินงานวิจัย*

3.1 ขั้นตอนการวิจัย

3.1.1 ผู้วิจัยได้ทำการศึกษา สำรวจแนวคิด และงานวิจัยที่เกี่ยวข้อง ซึ่งอ้างอิงตาม กรอบความมั่นคงปลอดภัยไซเบอร์ของ NIST และปัจจัยที่ส่งผลให้เกิดความคืนสภาพได้ เพื่อต้องการสนับสนุนธุรกิจให้สามารถดำเนินงานอย่างต่อเนื่อง ร่วมกับศึกษาโมเดลความมั่นคงปลอดภัยข้อมูลของ ISF เพื่อให้ได้กรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ที่มีความสอดคล้องกับเป้าหมายของการวิจัย

3.1.2 กำหนดกรอบแนวคิดการวิจัย จะอิงหลักการของ NIST Cybersecurity Framework, Sustain, CIA Triad, รวมทั้งยึดถือปัจจัยในเรื่อง People, Process, Technology มาพิจารณาเป็นกรอบแนวคิดของการวิจัย ดังภาพที่ 4



ภาพที่ 4 *กรอบแนวคิดการวิจัย*

จากกรอบแนวคิดการวิจัยเรื่องการคืนสภาพได้ ด้านไซเบอร์สำหรับการให้บริการประมวลผลแบบคลาวด์นั้น จะมีองค์ประกอบและตัวชี้วัดภายในที่แสดงระดับความสามารถของผู้ให้บริการแบบคลาวด์ในเรื่องมาตรการตอบสนองจากภัยคุกคามที่เป็นการโจมตีและความสามารถในการคืนสภาพได้ด้านไซเบอร์ โดยมีเป้าหมายหลักเป็น 3 ส่วน คือ บุคลากร กระบวนการ และเทคโนโลยี

3.1.3 ผู้วิจัยได้อิงกรอบแนวคิดการวิจัยในการทำแบบสอบถามเบื้องต้นเพื่อหาปัจจัยที่เป็นไปได้ในการจัดทำกรอบการคืนสภาพได้ด้านไซเบอร์ ทั้งนี้ได้กำหนดปัจจัยเป็น 12 หัวข้อ รวม 43 ข้อคำถาม ระดับค่าคะแนนตามแบบของลิเคิร์ท (Linkert's Scale) มี 5 ระดับ ดังนี้

5 คะแนน หมายถึง ระดับมากที่สุด
4 คะแนน หมายถึง ระดับมาก
3 คะแนน หมายถึง ระดับปานกลาง
2 คะแนน หมายถึง ระดับน้อย
1 คะแนน หมายถึง ระดับน้อยที่สุด

เกณฑ์การแปลความหมายเพื่อจัดระดับคะแนนเฉลี่ยในแต่ละระดับดังนี้

ค่าเฉลี่ย 4.40 - 5.00 หมายถึง มากที่สุด
ค่าเฉลี่ย 3.40 - 4.39 หมายถึง มาก
ค่าเฉลี่ย 2.40 - 3.39 หมายถึง ปานกลาง
ค่าเฉลี่ย 1.40 - 2.39 หมายถึง น้อย
ค่าเฉลี่ย 1.00 - 1.39 หมายถึง น้อยที่สุด

4. ผลการดำเนินงาน

4.1 ผลการวิจัย

ผลการวิจัยแบ่งเป็น 4 ส่วน คือ 1) ผลจากการสัมภาษณ์เชิงลึกและการสนทนากลุ่มกับผู้เชี่ยวชาญ 2) การประเมินปัจจัยที่เป็นไปได้ในการจัดทำกรอบการคืนสภาพได้ด้านไซเบอร์ 3) กรอบการคืนสภาพได้ด้าน ไซเบอร์ และ 4) สร้างแอปพลิเคชันสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์

4.1.1 จากการสัมภาษณ์เชิงลึก (In-depth Interview) และการสนทนากลุ่ม (Focus Group) กับผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์ พบว่า แนวโน้มการโจมตีทางไซเบอร์ มีความรุนแรงและใช้วิธีการโจมตีที่ชาญฉลาดมากขึ้น ทำให้เทคโนโลยีการป้องกันภัยคุกคามด้านไซเบอร์ในปัจจุบันมีข้อจำกัดต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ จำเป็นอย่างยิ่งที่จะต้องมีการจัดการความเสี่ยงที่มีประสิทธิภาพ มีข้อปฏิบัติที่เป็นขั้นตอนและต้องตรวจสอบอย่างต่อเนื่อง ซึ่งการที่จะพัฒนาไปถึงระดับการคืนสภาพได้ของระบบบริการประมวลผลแบบคลาวด์นั้น ต้องเริ่มจากการกำหนดนโยบายและ กลยุทธ์เพื่อบริหารบุคลากร กระบวนการ และเทคโนโลยี โดยพร้อมกัน จึงจะสามารถยกระดับความมั่นคงปลอดภัยไซเบอร์ให้ไปถึงระดับการคืนสภาพได้อย่างแท้จริง

อย่างไรก็ดี การดำเนินงานให้ได้อย่างมี ประสิทธิภาพนั้น ต้องมีการทดสอบและประเมินผลว่า สามารถทำได้ตามแนวทางที่กำหนด และบุคลากรได้ตระหนักรู้ถึงหน้าที่และความรับผิดชอบของตนที่มีส่วนเกี่ยวข้องในระดับของการรักษาความมั่นคงปลอดภัย ไซเบอร์ ภายใต้การปฏิบัติงานด้วยความรู้ และมีความเข้าใจ อีกทั้ง การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เคยเกิดขึ้นในอดีต และนำประสบการณ์หรือบทเรียนนั้นไปทำการปรับปรุงอย่างต่อเนื่อง

4.1.2 แบบสอบถามเพื่อหาปัจจัยที่เป็นไปได้ในการจัดทำกรอบการคืนสภาพได้ด้านไซเบอร์ ผู้วิจัยทำการหาค่าสัมประสิทธิ์ความสอดคล้อง (IOC) ของแบบสอบถามจากผู้เชี่ยวชาญจำนวน 5 ท่าน แบบสอบถามมีค่าคะแนนดัชนีความสอดคล้องมากกว่า 0.50 ทุกข้อ รวมทั้งวัดความเชื่อมั่นของแบบสอบถามด้วย ค่าสัมประสิทธิ์แอลฟาของ ครอนบาค (Cronbach's Alpha Coefficient) กับกลุ่มตัวอย่างจำนวน 30 คน ได้ค่าสัมประสิทธิ์ความเชื่อมั่น

เฉลี่ยเท่ากับ 0.93 และเมื่อเก็บแบบสอบถามจากผู้ให้บริการแบบคลาวด์จำนวน 173 ชุด พบว่า ผลการประเมินโดยรวมแสดงดังตารางที่ 4 มีค่าเฉลี่ยของปัจจัยการคืนสภาพได้ด้านไซเบอร์อยู่ในระดับมาก ($\bar{x}$ = 3.87)

ตารางที่ 4 *ค่าเฉลี่ยปัจจัยการคืนสภาพได้ด้านไซเบอร์*

หัวข้อที่ทำการประเมิน	ระดับความคิดเห็น		
	ค่าเฉลี่ย	S.D.	การแปลผล
1. การระบุความเสี่ยง	3.94	0.31	มาก
2. การป้องกันความเสี่ยง	3.88	0.56	มาก
3. การตรวจจับภัยคุกคาม	3.86	0.67	มาก
4. การตอบสนอง	3.87	0.53	มาก
5. การกู้	3.90	0.52	มาก
6. การสนับสนุน	3.84	0.76	มาก
7. ความลับ	3.90	0.54	มาก
8. ความถูกต้องสมบูรณ์	3.87	0.55	มาก
9. ความพร้อมใช้งาน	3.85	0.76	มาก
10. บุคลากร	3.84	0.76	มาก
11. กระบวนการ	3.87	0.56	มาก
12. เทคโนโลยี	3.84	0.76	มาก
ผลรวมโดยเฉลี่ย	**3.87**	**0.61**	**มาก**

4.1.3 การสังเคราะห์ข้อมูล ผู้วิจัยได้ทำการวิเคราะห์และสังเคราะห์ข้อมูลจากผู้เชี่ยวชาญและงานวิจัยที่เกี่ยวข้อง การพิจารณาปัจจัยที่เป็นไปได้ในการจัดทำกรอบการคืนสภาพได้ด้านไซเบอร์ และพัฒนาเป็นกรอบการคืนสภาพได้ด้านไซเบอร์ของการบริการประมวลผลแบบคลาวด์ ทั้งนี้ ผลที่ได้นั้นนำไปให้ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์จำนวน 5 ท่าน ได้ประเมินความเหมาะสมของกรอบการคืนสภาพได้ด้านไซเบอร์ต่อการนำไปใช้งาน ทั้งนี้ ผู้เชี่ยวชาญได้แนะนำ พร้อมการปรับปรุงแก้ไขกรอบให้มีความเหมาะสม ดังที่ได้แสดงไว้ในตารางที่ 5

4.2 การสร้างแอปพลิเคชันสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์

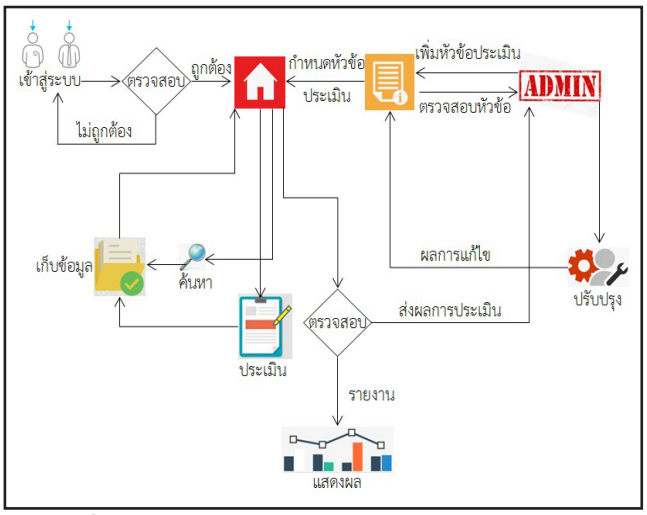
จากกรอบการคืนสภาพได้ด้านไซเบอร์ ในตารางที่ 5 ผู้วิจัยได้ใช้เป็นกรอบประเด็นในการจัดทำแบบประเมิน พร้อมทั้งได้ทำการพัฒนาเว็บแอปพลิเคชันที่อิงหลักการวัฏจักรของการพัฒนาซอฟต์แวร์ ทั้งนี้ มีด้วยกันทั้งหมด 7 ขั้นตอน ได้แก่ 1) การเข้าใจปัญหา 2) การศึกษาความเป็นไปได้ 3) การวิเคราะห์ 4) การออกแบบ 5) การพัฒนาระบบ 6) การนำไปใช้งาน และ 7) การบำรุงรักษา

ตารางที่ 5 *กรอบการคืนสภาพได้ด้านไซเบอร์*

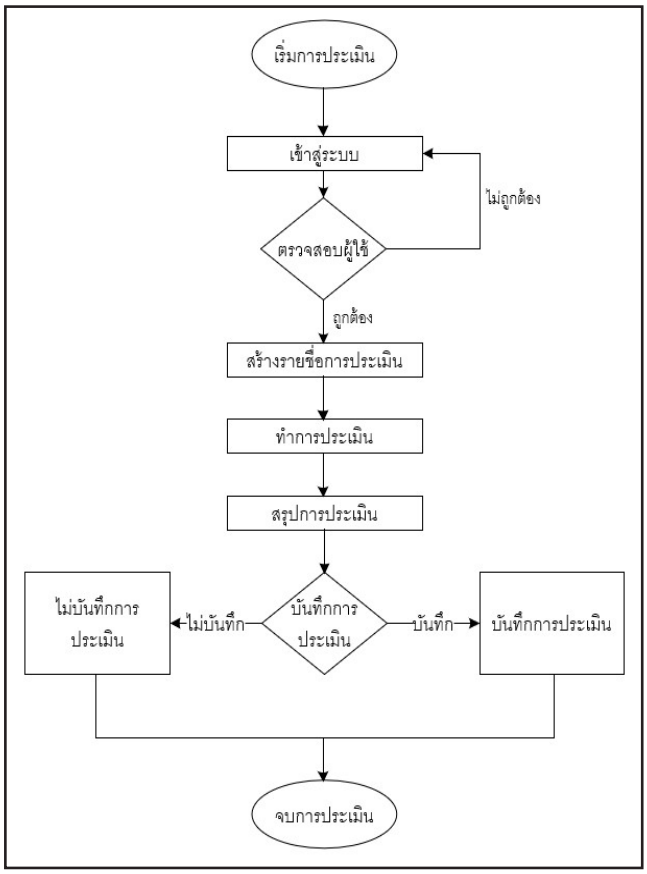
กรอบการคืนสภาพได้ด้านไซเบอร์		ด้านบุคลากร	ด้านกระบวนการ	ด้านเทคโนโลยี
Security, Risk, Compliance and Governance	การระบุความเสี่ยง	- บุคลากรมีความเชี่ยวชาญเฉพาะ	- การเก็บรักษาข้อมูลความลับ - การกำกับดูแล - การบริหารการใช้บริการภายนอก	- การจัดการช่องโหว่ - การทดสอบการเจาะระบบ
	การป้องกันความเสี่ยง	- การฝึกอบรม - การระวังภัยคุกคาม	- การรักษาความมั่นคงปลอดภัยด้านกายภาพ	- การรักษาความมั่นคงปลอดภัยด้านกายภาพ
	การตรวจจับภัยคุกคาม	- การตรวจสอบความมั่นคงปลอดภัย	- ความถูกต้องสมบูรณ์ของข้อมูล - การวิเคราะห์	- การตรวจสอบอย่างสม่ำเสมอ
Managed Incident Response and Recover	การกู้	- การตระหนักรู้ด้านการกู้	- แผนการกู้ที่มีการปรับปรุงในทุก 3 เดือน	- แผนการยกระดับเทคโนโลยี
	การสนับสนุน	- ประสบการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์	- แผนงานความต่อเนื่องทางธุรกิจ - การบริหารการเปลี่ยนแปลง	- ศูนย์กลางการบริหาร - การบริหารงานที่ทำการปรับปรุงอย่างต่อเนื่อง

4.2.1 ภาพรวมการทำงานของแอปพลิเคชันสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์ของการให้บริการประมวลผลแบบคลาวด์ ได้แสดงไว้ ดังภาพที่ 5

4.2.2 การเข้าสู่ระบบเว็บแอปพลิเคชันสำหรับประเมินผล ระดับความสามารถการรักษาความมั่นคงปลอดภัยของข้อมูลและการคืนสภาพได้ด้านไซเบอร์ สำหรับการให้บริการประมวลผลแบบคลาวด์นั้น ผู้ใช้งานจะได้รับชื่อผู้ใช้และรหัสผ่านเพื่อเข้าสู่ระบบและทำแบบประเมินในแต่ละหัวข้อได้ ดังภาพที่ 6



ภาพที่ 5 *ภาพรวมการทำงานของแอปพลิเคชันสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์*



ภาพที่ 6 *ผังกระบวนการประเมิน*

5. สรุป

ผู้วิจัยได้พัฒนากรอบการคืนสภาพได้ด้านไซเบอร์ พร้อมทั้ง พัฒนาวิธีประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการบริการประมวลผลแบบคลาวด์ผ่านทางการจัดทำแอปพลิเคชัน งานวิจัยนี้ได้เน้นการวิจัยเชิงคุณภาพประกอบกับการวิจัยเชิงประยุกต์ที่อิงกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ สหรัฐอเมริกา ข้อมูลการสำรวจจาก ผู้ให้บริการแบบคลาวด์ในประเทศไทยนั้น พบว่า แนวโน้มการโจมตีทางไซเบอร์มีความรุนแรง และใช้วิธีการโจมตีที่ชาญฉลาดและซับซ้อนมากยิ่งขึ้น กรอบการคืนสภาพได้ด้านไซเบอร์ของการบริการประมวลผลแบบคลาวด์ และแอปพลิเคชันที่พัฒนาขึ้นนี้ จะทำให้ผู้ใช้บริการแบบคลาวด์ได้ตัดสินใจเลือกใช้ผู้ให้บริการประมวลผล แบบคลาวด์ ซึ่งจะต้องดำเนินการภายใต้มาตรฐาน ทั้งกรอบการปฏิบัติ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ ให้สอดคล้องกับการดำเนินงาน โดยควรพิจารณาในด้านบุคลากร กระบวนการ และเทคโนโลยี อีกทั้ง ยังสามารถอำนวยความสะดวกต่อผู้ให้บริการ แบบคลาวด์ ได้นำกรอบที่พัฒนาขึ้นนี้ไปประเมินองค์กรตนเอง เพื่อทำการปรับปรุงและพัฒนาระดับความมั่นคงปลอดภัยไซเบอร์ในระบบการบริการประมวลผลแบบคลาวด์และประเมินระดับการคืนสภาพได้ด้านไซเบอร์ให้มีประสิทธิภาพดียิ่งขึ้นในอนาคตต่อไป

6. เอกสารอ้างอิง

[1] E. Roberts, J. Farrington and S. Skerratt, “Evaluating New Digital Technologies Through a Framework of Resilience.” *Scottish Geographical Journal*, Vol. 131, No. 3-4, pp. 253-264, October, 2015.

[2] The Engineering Institute of Thailand under H.M. The King’s Patronage. *Cloud Services Standard of Practice EIT Standard 102002-18*. 2018.

[3] Rosmiati, I. Riadi and Y. Prayudi. “A maturity level framework for measurement of information security performance.” *International Journal of Computer Applications*, Vol. 141, No.8, 2016.

[4] K. Mesker, “Adapting NIST Cybersecurity Framework for Risk Assessment.” *presented at NIST Conference*, 2014.

[5] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*, Draft Version 1.1, 2017.

[6] Ngoc T. Le and Doan B. Hoang. “Capability maturity

model and metrics framework for cyber cloud security." *Scalable Computing: Practice and Experience*, Vol. 18, No. 4, pp. 277–290, 2017.

[7] The Center for Internet Security. *The CIS Security Metrics-Quick Start Guide*, v1.0.0, 2010.

[8] The Center for Internet Security. *The CIS Critical Security Controls for Effective Cyber Defense version 6.1*, 2016.

[9] Hugh Boyes. "Cybersecurity and Cyber-Resilient Supply Chains." The Technology Innovation Management Review, No.4, pp. 28-34, 2015.

[10] Cyber Security Resilience. *Complete Self-Assessment Guide*, The Art of Services, 2018.

[11] S. Watthanasathian, P. Praneetpolgrang, R. Jairuk, and T. Banditwattanawong. "The Development of Trust Model in Government Cloud Services." *In Proceeding of the 9th National Conference on Computing and Information Technology (NCCIT2013)*, pp. 254-259. 2018.

[12] T. Banditwattanawong, C. Vorakulpipat and M. Masdisornchote. "The Survey of Cloud Infrastructure-as-a-Service Providers in Thailand." *Srinakharinwirot Science Journal*, Vol. 33, No. 1, pp. 175-190, 2017.

[13] Wendy and W. Gunawan. "Measuring information security and cybersecurity on private cloud computing." *Journal of Theoretical and Applied Information Technology*, Vol. 96, No. 1, 2019.