การประเมินความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงของผู้ให้บริการคลาวด์

นางสาวนันทพรรณ เป็นสุข

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2555

AN ASSESSMENT OF NON-FUNCTIONAL SECURITY REQUIREMENTS OF CLOUD PROVIDERS

Miss Nuntapun Bhensook

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Software Engineering

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2012

หัวข้อวิทยานิพนธ์	การประเมินความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงของผู้ให้บริการคลาวด์
โดย	นางสาวนันทพรรณ เป็นสุข
สาขาวิชา	วิศวกรรมซอฟต์แวร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

…….. คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

…… ประธานกรรมการ
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

…….. อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา)

…… กรรมการภายนอกมหาวิทยาลัย
(ผู้ช่วยศาสตราจารย์ ดร.ชวลิต ศรีสถาพรพัฒน์)

นันทพรรณ เป็นสุข : การประเมินความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงของผู้ให้บริการคลาวด์. (AN ASSESSMENT OF NON-FUNCTIONAL SECURITY REQUIREMENTS OF CLOUD PROVIDERS) อ. ที่ปรึกษาวิทยานิพนธ์หลัก: รศ.ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา, 80 หน้า.

การประเมินผู้ให้บริการคลาวด์มีความสำคัญต่อผู้ใช้บริการคลาวด์ในการพิจารณาเลือกใช้บริการจากภายนอกว่า ผู้ให้บริการรายใดสามารถตอบสนองต่อความต้องการของธุรกิจและระบบได้ การพิจารณาข้อมูลของผู้ให้บริการว่าเป็นไปตามความต้องการเชิงหน้าที่หรือไม่ เช่น การพิจารณาแพลตฟอร์มที่ให้บริการ หรือ ความสามารถในการคำนวณ สามารถทำได้ง่ายเนื่องจากมักมีรายละเอียดที่เป็นข้อมูลเชิงปริมาณระบุไว้ ในขณะที่ข้อมูลของผู้ให้บริการที่เกี่ยวข้องกับความต้องการที่ไม่ใช่เชิงหน้าที่ เช่น ข้อมูลความมั่นคง มักอยู่ในรูปคำบรรยายบนหน้าเว็บของผู้ให้บริการ จึงทำให้การเปรียบเทียบระหว่างผู้ให้บริการแต่ละรายทำได้ยาก งานวิจัยนี้ได้ใช้วิธีเป้าหมาย คำถาม ตัววัด เพื่อนำเสนอแบบจำลองการคำนวณแบบถ่วงน้ำหนักสำหรับประเมินผู้ให้บริการคลาวด์ในด้านการปฏิบัติตามความต้องการด้านความมั่นคง โดยที่เป้าหมายด้านความมั่นคงและคำถามที่สะท้อนถึงการบรรลุเป้าหมายนั้นนำมาจากเมตริกซ์ควบคุมคลาวด์และคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ ซึ่งกำหนดไว้แล้วโดยองค์กรความมั่นคงของคลาวด์ คำถามจะถูกแปลงให้เป็นคำถามที่ละเอียดขึ้นเพื่อให้สามารถกำหนดตัววัดเชิงปริมาณสำหรับตอบคำถามเหล่านั้นได้ ตัววัดจะอยู่ในรูปของจำนวนหลักฐานการปฏิบัติตามความต้องการด้านความมั่นคงซึ่งผู้ให้บริการคลาวด์ระบุไว้ การคิดคะแนนจะมีการถ่วงน้ำหนักตามคุณภาพของหลักฐานในแง่การเป็นไปตามตัววัด ร่วมกับการถ่วงน้ำหนักตามความสมบูรณ์ของหลักฐาน นอกจากนี้งานวิจัยยังได้นำเสนอเครื่องมือสนับสนุนการประเมินด้วย

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิศวกรรมซอฟต์แวร์ ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก .....

ปีการศึกษา 2555 .....

5371422521 : MAJOR SOFTWARE ENGINEERING
KEYWORDS : NON-FUNCTIONAL SECURTIY REQUIREMENTS / ASSESSMENT / CLOUD COMPUTING

NUNTAPUN BHENSOOK : AN ASSESSMENT OF NON-FUNCTIONAL SECURITY REQUIREMENTS OF CLOUD PROVIDERS. ADVISOR : ASSOC. PROF. TWITTIE SENIVONGSE, Ph.D., 80 pp.

Cloud provider assessment is important for cloud consumers to determine, when outsourcing computing work, which providers can serve their business and system requirements. Functional requirements described explicitly or as quantitative information, e.g. platform and computing capacity, are usually easier to determine, whereas non-functional requirements, e.g. security, have to be checked against descriptive information on providers' Web sites and therefore they are more difficult for cross-provider comparison. This research follows the Goal Question Metric approach and presents a weighted scoring model for assessing security requirements compliance of cloud providers. The security goals and questions that address the goals are taken from Cloud Security Alliance's Cloud Controls Matrix and Consensus Assessments Initiative Questionnaire. The questions are transformed into more detailed ones and metrics are defined to help provide quantitative answers to the transformed questions based on evidence of security compliance provided by the cloud providers. The scoring is weighted by the quality of the evidence with respect to their compliance with the associated metrics and their completeness. A scoring tool is also proposed to support the assessment.

Department : Computer Engineering Student's Signature .....
Field of Study : Software Engineering Advisor's Signature .....
Academic Year : 2012

กิตติกรรมประกาศ

วิทยานิพนธ์นี้สำเร็จลงด้วยความกรุณาเป็นอย่างสูงของรองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งได้ให้โอกาส ความรู้และคำแนะนำในการทำวิทยานิพนธ์ ตลอดจนความเมตตาและความอดทนในการตรวจผลงานของข้าพเจ้า ได้แก่ โครงร่างวิทยานิพนธ์ ผลงานวิจัยภาษาไทยและภาษาอังกฤษ และวิทยานิพนธ์ ทำให้ผลงานทุกชิ้นสำเร็จลุล่วงเป็นอย่างดี รวมทั้งความเอาใจใส่และความเสียสละเวลาร่วมเดินทางไปนำเสนอผลงานวิชาการที่ประเทศไต้หวัน ขอขอบพระคุณอาจารย์เป็นอย่างสูงไว้ ณ ที่นี้

ขอขอบพระคุณ อาจารย์ ดร.ยรรยง เต็งอำนวย ประธานกรรมการสอบวิทยานิพนธ์ และผู้ช่วยศาสตราจารย์ ดร.ชวลิต ศรีสถาพรพัฒน์ กรรมการสอบวิทยานิพนธ์ที่กรุณาให้คำแนะนำและชี้แนะแนวทางที่เป็นประโยชน์ต่อการทำวิทยานิพนธ์ในครั้งนี้

ขอขอบพระคุณอาจารย์ทุกท่านที่ให้ความรู้และคำแนะนำที่เป็นประโยชน์ รวมถึงความเมตตาและความเอาใจใส่มาโดยตลอด

ขอขอบพระคุณครอบครัว ได้แก่ บิดาและมารดา ที่ให้กำลังใจในทุกเรื่อง และสอนให้มองแต่ในแง่ดีและมองเห็นโอกาสและความเป็นไปได้ จนทำให้ข้าพเจ้ามีผลงานที่สำเร็จได้

ขอขอบคุณเพื่อนร่วมชั้นเรียนวิศวกรรมซอฟต์แวร์ และเพื่อนสาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ภาคนอกเวลาราชการทุกคนที่ให้ความช่วยเหลือ แจ้งข่าวสารของมหาวิทยาลัยและการประชุมวิชาการที่เป็นประโยชน์ รวมถึงมิตรภาพและกำลังใจที่มีให้เสมอ

สารบัญ

หน้า

หน้า

หน้า

สารบัญตาราง

หน้า

หน้า

สารบัญภาพ

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

บริการคลาวด์ เป็นบริการที่มีจุดเด่นในด้านความยืดหยุ่นต่อความต้องการของผู้ใช้บริการ และช่วยลดกิจกรรมและงบประมาณในการดำเนินงานในอุตสาหกรรมซอฟต์แวร์ เช่น การติดตั้ง การบำรุงรักษาฮาร์ดแวร์ เป็นต้น ด้วยเหตุนี้บริการคลาวด์จึงเป็นที่นิยมในอุตสาหกรรมซอฟต์แวร์หลายประเภท

เช่นเดียวกับการใช้บริการด้านอื่น ผู้ใช้บริการคลาวด์จำเป็นต้องมีการประเมินผู้ให้บริการคลาวด์ก่อนการตัดสินใจใช้บริการ การประเมินอาจทำได้โดยศึกษาข้อมูลของผู้ให้บริการคลาวด์ผ่านหน้าเว็บของผู้ให้บริการคลาวด์เอง หรือศึกษาข้อมูลของผู้ที่เคยใช้บริการคลาวด์มาแล้ว และข้อมูลที่ผู้ใช้บริการคลาวด์คาดหวัง เพื่อนำมาใช้ตัดสินใจ แบ่งเป็น

ข้อมูลความต้องการเชิงหน้าที่ (Functional Requirement) เช่น รายละเอียดของเครื่องเซิร์ฟเวอร์ รายละเอียดของระบบฐานข้อมูล ระยะเวลาที่ใช้ในการจัดเตรียมระบบ ความสามารถในการขยายตัวของระบบเพื่อรองรับความต้องการใช้บริการที่เพิ่มขึ้นหรือลดลง

ข้อมูลความต้องการที่ไม่ใช่เชิงหน้าที่ (Non-functional Requirement) เช่น นโยบายความมั่นคงและความเป็นส่วนตัวของข้อมูล ข้อตกลงในการให้บริการ (Service Level Agreement)

ข้อมูลความต้องการเชิงหน้าที่ สามารถประเมินได้โดยง่ายเนื่องจากมักมีตัวเลขและรายละเอียดที่สามารถวัดได้ ในขณะที่ข้อมูลที่ไม่ใช่ความต้องการเชิงหน้าที่ ผู้ใช้บริการคลาวด์จะทราบเพียงรายละเอียดที่อยู่ภายในหน้าเว็บหรือเอกสารนโยบายของผู้ให้บริการคลาวด์เท่านั้น แต่ไม่สามารถทราบได้ว่าผู้ให้บริการคลาวด์ มีการปฏิบัติตามรายละเอียดที่กล่าวไว้จริงหรือไม่ อีกทั้งรายละเอียดที่ผู้ให้บริการคลาวด์นำเสนออาจไม่มีประโยชน์ในการพิจารณาตัดสินใจเลือกใช้บริการคลาวด์

จากประเด็นดังกล่าว งานวิจัยนี้จึงมีวัตถุประสงค์เพื่อนำเสนอระบบที่ช่วยผู้ใช้บริการคลาวด์ในการประเมินเพื่อตัดสินใจเลือกผู้ให้บริการคลาวด์ โดยพิจารณาเฉพาะความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงของผู้ให้บริการคลาวด์จากเมตริกซ์ควบคุมคลาวด์ (Cloud Control

Matrix) [1] ที่จัดทำโดยองค์กรความมั่นคงของคลาวด์หรือซีเอสเอ (Cloud Security Alliance: CSA) ซึ่งกำหนดความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงที่ผู้ให้บริการคลาวด์จำเป็นต้องมีไว้ 11 ด้าน ร่วมกับการใช้คำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ (Consensus Assessment Questions) [2] ซึ่งระบุคำถามที่สอดคล้องกับการประเมินเป้าหมายการควบคุมความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงทั้ง 11 ด้านที่ระบุไว้ในเมตริกซ์ควบคุมคลาวด์

ความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงที่เมตริกซ์ควบคุมคลาวด์กำหนด ได้แก่ [1]

1) การปฏิบัติตาม (Compliance)
2) การกำกับดูแลข้อมูล (Data Governance)
3) ความมั่นคงด้านสิ่งอำนวยความสะดวก (Facility Security)
4) ความมั่นคงด้านทรัพยากรมนุษย์ (Human Resources Security)
5) ความมั่นคงด้านสารสนเทศ (Information Security)
6) กฎหมาย (Legal)
7) การจัดการการดำเนินการ (Operation Management)
8) การจัดการความเสี่ยง (Risk Management)
9) การจัดการการปล่อย/เริ่มต้นให้บริการ (Release Management)
10) การคืนสภาพได้ (Resiliency)
11) สถาปัตยกรรมความมั่นคง (Security Architecture)

ความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคง 11 ด้านข้างต้น จะถูกกำหนดเป็นนิยามของคำว่าความมั่นคงที่กล่าวถึงทั้งหมดในงานวิจัย การวิจัยจะใช้เมตริกซ์ควบคุมคลาวด์และคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่มาวิเคราะห์หาตัววัดความมั่นคงของผู้ให้บริการคลาวด์โดยใช้วิธีจีคิวเอ็ม (Goal Question Metric: GQM) [4] คำถามจะถูกแปลงให้เป็นคำถามที่ละเอียดขึ้นเพื่อให้สามารถกำหนดตัววัดเชิงปริมาณสำหรับตอบคำถามเหล่านั้นได้ ตัววัดจะอยู่ในรูปของจำนวนหลักฐานการปฏิบัติตามความต้องการด้านความมั่นคงซึ่งผู้ให้บริการคลาวด์ระบุไว้ การคิดคะแนนความมั่นคงจะมีการถ่วงน้ำหนักตัววัดโดยผู้ให้บริการเองหรือโดยผู้ตรวจสอบด้านความมั่นคง (Cloud Security Auditor) ค่าน้ำหนักจะเป็นไปตามคุณภาพของหลักฐานในแง่การเป็นไปตามตัววัด และในแง่ความสมบูรณ์ของหลักฐาน จากนั้นจึงคำนวณคะแนนการปฏิบัติตามความต้องการด้านความมั่นคงของผู้ให้บริการคลาวด์ได้ งานวิจัยนี้ได้เสนอเครื่องมือสนับสนุนการคำนวณคะแนนความมั่นคงเพื่อให้ผู้ให้บริการคลาวด์และผู้ตรวจสอบ

สามารถระบุหลักฐานและค่าน้ำหนักที่เกี่ยวข้อง และให้ผู้ใช้บริการคลาวด์สามารถเรียกดูและเปรียบเทียบคะแนนของผู้ให้บริการคลาวด์แต่ละรายเพื่อประกอบการตัดสินใจเลือกใช้บริการให้เหมาะสมกับองค์กรได้

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อกำหนดตัววัดความมั่นคงของผู้ให้บริการคลาวด์

1.2.2 เพื่อกำหนดวิธีประเมินคะแนนความมั่นคงของผู้ให้บริการคลาวด์

1.2.3 เพื่อพัฒนาเครื่องมือสนับสนุนการประเมินคะแนนความมั่นคงของผู้ให้บริการคลาวด์

1.3 ขอบเขตของการวิจัย

1.3.1 พิจารณาความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงที่ผู้ให้บริการคลาวด์จำเป็นต้องมีรวม 11 ด้าน ตามที่กำหนดโดยเมตริกซ์ควบคุมคลาวด์

1.3.2 วิเคราะห์เป้าหมายของความมั่นคงจากเมตริกซ์ควบคุมคลาวด์และกำหนดตัววัดที่สอดคล้องกับเป้าหมายโดยใช้วิธีจีคิวเอ็ม

1.3.3 กำหนดวิธีการวัดคะแนนความมั่นคงของการให้บริการคลาวด์

1.3.4 พัฒนาเครื่องมือวัดคะแนนที่สามารถคำนวณ แสดง และเปรียบเทียบคะแนนความมั่นคงของผู้ให้บริการคลาวด์แต่ละราย

1.3.5 ทดสอบเครื่องมือที่พัฒนากับผู้ให้บริการคลาวด์ 3 รายเป็นอย่างน้อย

1.4 ขั้นตอนการวิจัย

1.4.1 เลือกเป้าหมายของการประเมินความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงของผู้ให้บริการคลาวด์

1.4.2 ตั้งคำถามให้สอดคล้องกับเป้าหมายโดยใช้คำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ [2]

1.4.3 กำหนดตัววัดความมั่นคงของผู้ให้บริการคลาวด์โดยวิธีจีคิวเอ็ม

1.4.4 กำหนดวิธีการให้คะแนนความมั่นคงของผู้ให้บริการคลาวด์

1.4.5 จัดลำดับผู้ให้บริการคลาวด์ตามคะแนนความมั่นคง

1.4.6 พัฒนาเครื่องมือสนับสนุนงานวิจัย

1.4.7 ทดลองและประเมินผลการวิจัย

1.4.8 สรุปผลการวิจัย

1.4.9 จัดทำบทความวิจัย และวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ได้ตัววัดและวิธีประเมินคะแนนความมั่นคงของผู้ให้บริการคลาวด์

1.5.2 ได้เครื่องมือวัดคะแนนที่สามารถกำหนดน้ำหนัก คำนวณคะแนน แสดงผลคะแนน และเปรียบเทียบคะแนนความมั่นคงของผู้ให้บริการคลาวด์แต่ละรายได้

1.6 ผลงานตีพิมพ์

ส่วนหนึ่งของวิทยานิพนธ์นี้ได้ตีพิมพ์และนำเสนอในการประชุมวิชาการต่อไปนี้

1.6.1 บทความเรื่อง An assessment of security requirements compliance of cloud providers โดยผู้แต่งคือ Nuntapun Bhensook และ Twittie Senivongse ในการประชุมวิชาการ 4th IEEE International Conference on Cloud Computing Technology and Science (IEEE CloudCom 2012), Taipei, Taiwan (December 03-06, 2012): 520 - 525

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎี

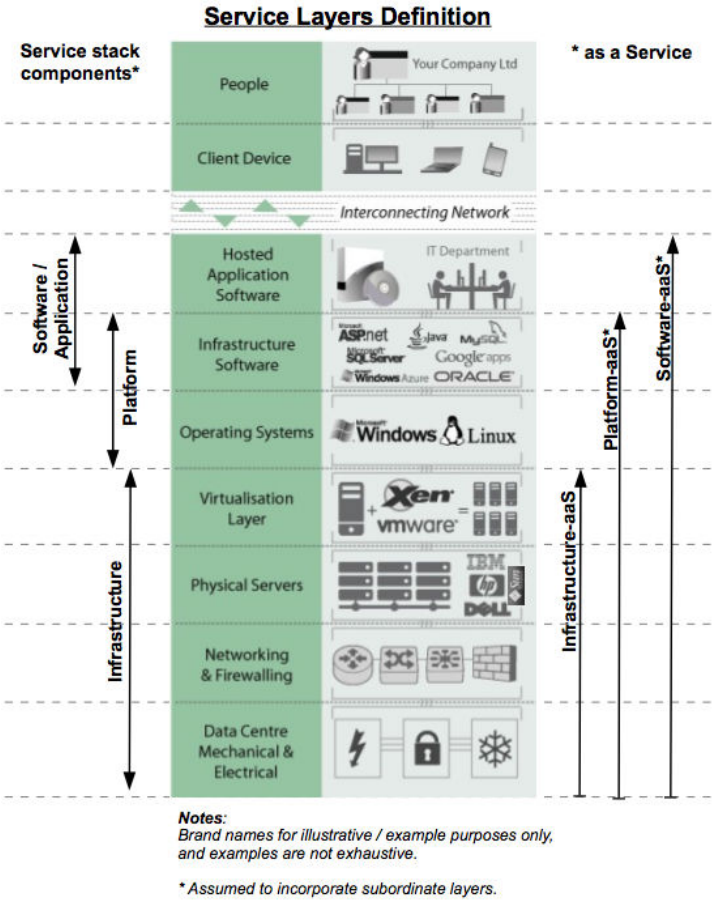
ทฤษฎีที่เกี่ยวข้องกับงานวิจัยมีดังนี้

2.1.1 การคำนวณแบบคลาวด์

การคำนวณแบบคลาวด์ (Cloud Computing) ตามนิยามของสถาบันมาตรฐานและเทคโนโลยีระดับชาติ (National Institute of Standards and Technology: NIST) [5] เป็นแบบจำลองการคำนวณที่มีความสามารถในการใช้งานได้ทุกหนทุกแห่ง ให้ความสะดวกสบาย สามารถเข้าถึงเครือข่ายได้ตามความต้องการ สนับสนุนการแบ่งปันการใช้ทรัพยากรคอมพิวเตอร์ เช่น เครือข่าย ผู้ให้บริการ อุปกรณ์เก็บข้อมูล แอพพลิเคชัน และบริการ ใช้เวลาในการเตรียมการใช้งานและแรงงานในการบริหารจัดการน้อย โดยแบบจำลองคลาวด์นี้มีลักษณะเด่น 5 ลักษณะ ได้แก่

1) การบริการตนเองแบบออนดีมานด์ (On-Demand Self Service) คือ สามารถจัดเตรียมการใช้งานได้ตามความต้องการของผู้ใช้บริการเอง โดยไม่ต้องมีปฏิสัมพันธ์กับผู้ให้บริการ
2) การเข้าถึงเครือข่ายแบบกว้าง (Broad Network Access) คือ มีความสามารถในการให้บริการระหว่างเครือข่ายที่แตกต่างกัน มาตรฐานที่แตกต่างกัน และแพลตฟอร์มที่แตกต่างกัน
3) แหล่งรวมทรัพยากร (Resource Pooling) คือ มีการรวบรวมทรัพยากรเพื่อให้บริการโดยสามารถรองรับผู้ใช้งานได้พร้อมกันหลายรายในเวลาเดียวกัน (Multi-Tenant Model) นอกจากนี้การขยายตัวของทรัพยากรยังเป็นไปโดยอัตโนมัติ คือผู้ใช้บริการสามารถเพิ่มการใช้บริการหรือลดการใช้บริการได้ตามความต้องการ
4) ความยืดหยุ่นสูง (Rapid Elasticity) คือ มีการจัดเตรียมทรัพยากรที่เหมาะสมและสอดคล้องกับความต้องการของผู้ใช้บริการ
5) บริการที่สามารถวัดได้ (Measured Service) คือ ผู้ใช้บริการคลาวด์สามารถติดตาม ควบคุม ตรวจสอบรายงานการใช้ทรัพยากร ซึ่งคุณสมบัติเหล่านี้ถือเป็นคุณสมบัติความโปร่งใสของผู้ให้บริการที่มีต่อผู้ใช้บริการ

เมื่อแบ่งบริการคลาวด์ตามลักษณะการให้บริการ สามารถแบ่งได้เป็น 3 ประเภท ดังภาพที่ 2.1 คือ



ภาพที่ 2.1 ลักษณะการให้บริการคลาวด์ [6]

1) การให้บริการซอฟต์แวร์ (Software as a Service: SaaS) คือ บริการที่ผู้ใช้งานกลุ่มใดๆ สามารถเข้าถึงซอฟต์แวร์ได้จากสถานที่ที่แตกต่างกันหรือด้วยชนิดของอุปกรณ์ที่แตกต่างกัน เช่น เว็บเบราว์เซอร์ อินเทอร์เฟซโปรแกรม โดยผู้เป็นเจ้าของซอฟต์แวร์ที่ให้บริการไม่จำเป็นต้องจัดการหรือควบคุมระบบโครงสร้างพื้นฐานเอง จากภาพที่ 2.1 ผู้ให้บริการคลาวด์จะให้บริการและจัดการในระดับศูนย์ข้อมูลไปจนถึงระดับแอพพลิเคชันที่ผู้ใช้บริการคลาวด์ฝากไว้
2) การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS) คือ ผู้ใช้บริการคลาวด์มีหน้าที่ควบคุมการตั้งค่าและการวางโปรแกรมเท่านั้น แต่ไม่จำเป็นต้องจัดการหรือควบคุมระบบโครงสร้างพื้นฐานของซอฟต์แวร์ จากภาพที่ 2.1 ผู้ให้บริการคลาวด์จะ

ให้บริการและจัดการในระดับศูนย์ข้อมูลไปจนถึงระดับโครงสร้างพื้นฐานของซอฟต์แวร์

3) การให้บริการโครงสร้างพื้นฐาน (Infrastructure as a Service: IaaS) คือ ผู้ใช้บริการคลาวด์มีหน้าที่ควบคุมการตั้งค่าและการวางโปรแกรม ระบบโครงสร้างพื้นฐานของซอฟต์แวร์ ระบบปฏิบัติการเอง จากภาพที่ 2.1 ผู้ให้บริการ คลาวด์จะให้บริการและจัดการในระดับศูนย์ข้อมูลไปจนถึงระดับการสร้างสภาพแวดล้อมเสมือนสำหรับซอฟต์แวร์เท่านั้น

เมื่อแบ่งบริการคลาวด์ตามลักษณะการใช้งานคลาวด์ สามารถแบ่งได้เป็น 4 ประเภท ได้แก่

1) คลาวด์ส่วนบุคคล (Private Cloud) คือ การให้บริการคลาวด์สำหรับกลุ่มผู้ใช้งานเฉพาะด้านหรือการใช้งานภายในองค์กร โดยผู้ใช้บริการอาจมีส่วนร่วมในการบริหารจัดการทรัพยากรเองและนโยบายและความต้องการที่ไม่ใช่เชิงหน้าที่ของบริการคลาวด์ต้องเป็นไปตามมาตรฐานที่กำหนดขึ้นภายในองค์กร
2) คลาวด์กลุ่มสังคม (Community Cloud) คือ การให้บริการคลาวด์สำหรับกลุ่มผู้ใช้งานที่มีวัตถุประสงค์หรือลักษณะการทำงานที่คล้ายกัน หรือเป็นกลุ่มผู้ใช้งานที่เป็นลักษณะการรวมตัวกัน เช่น องค์กรสาธารณะหรือฟอรัม
3) คลาวด์สาธารณะ (Public Cloud) คือ การให้บริการคลาวด์สำหรับผู้ใช้บริการทุกกลุ่มและสำหรับลักษณะการใช้งานทุกรูปแบบ
4) คลาวด์ผสม (Hybrid Cloud) คือ การให้บริการคลาวด์ที่ผสมผสานการให้บริการมากกว่า 1 แบบ ขึ้นอยู่กับวัตถุประสงค์ของผู้ใช้บริการคลาวด์

2.1.2 มาตรฐานความมั่นคงและความต้องการที่ไม่ใช่เชิงหน้าที่ของการคำนวณแบบคลาวด์

การให้บริการคลาวด์จำเป็นต้องมีนโยบายด้านความมั่นคงเช่นเดียวกับการให้บริการด้านอื่น ๆ นอกเหนือจากสร้างความไว้วางใจให้ผู้ใช้บริการคลาวด์แล้ว ยังช่วยลดความเสี่ยงขององค์กรของผู้ใช้บริการคลาวด์ด้วย

องค์กรที่นำเสนอมาตรฐานความมั่นคงรวมถึงความต้องการที่ไม่ใช่เชิงหน้าที่ด้านอื่น ๆ ที่จำเป็นในการให้บริการคลาวด์ เช่น องค์กรความมั่นคงของคลาวด์หรือซีเอสเอซึ่งเป็นองค์กรไม่แสวงผลกำไรที่เกิดจากการร่วมมือกันระหว่างภาคอุตสาหกรรม บริษัท และ

สมาคมต่าง ๆ และมีวัตถุประสงค์เพื่อสนับสนุนแนวทางปฏิบัติที่ดีสำหรับการสร้างความเชื่อมั่นในด้านต่าง ๆ ของความต้องการที่ไม่ใช่เชิงหน้าที่ในการให้บริการคลาวด์ได้ให้ความสำคัญกับการนำมาตรฐานความมั่นคงที่ถูกนิยามโดยองค์กรที่เชื่อถือได้ดังต่อไปนี้มาประยุกต์ใช้กับบริการคลาวด์ [1]

1) ISO 27001 หรือ องค์กรมาตรฐานนานาชาติ (International Organization for Standardization) กำหนดมาตรฐานเลขที่ 27001 ซึ่งอยู่ในชุดมาตรฐานความมั่นคงสารสนเทศ (เลขที่ 20000) มาตรฐานนี้ถูกตีพิมพ์ในเดือนตุลาคม ปีค.ศ. 2005 เพื่อเป็นแบบจำลองสำหรับการติดตั้ง การดำเนินการ การปฏิบัติการ การควบคุม การทบทวน การบำรุงรักษา และการปรับปรุงระบบจัดการความมั่นคงสารสนเทศ (Information Security Management System: ISMS)
2) ISACA (Information Systems Audit and Control Association) เป็นองค์กรที่เกิดจากการรวมตัวของกลุ่มบริษัทเอกชนโดยมีความต้องการรวมข้อมูลให้เป็นศูนย์กลาง (Centralized) และให้แนวทางในด้านการควบคุมการตรวจสอบระบบคอมพิวเตอร์ ปัจจุบัน ISACA นำเสนอแนวทางและกรอบด้านต่าง ๆ ในระบบสารสนเทศ เช่น การกำกับดูแลเทคโนโลยีสารสนเทศ การควบคุมและให้ความเชื่อมั่นด้านความมั่นคง ISACA นำเสนอ COBIT (Control Objectives for Information and Related Technology) ซึ่งเป็นกรอบการกำกับดูแลเทคโนโลยีสารสนเทศโดยมีชุดเครื่องมือสำหรับกลุ่มผู้บริหารเพื่อเชื่อมโยงช่องว่างระหว่างการควบคุมความต้องการ ประเด็นทางเทคนิคและความเสี่ยงทางธุรกิจ นอกจากนี้ยังนำเสนอนโยบายและแนวทางปฏิบัติที่ดีสำหรับการควบคุมเทคโนโลยีสารสนเทศเพื่อช่วยเพิ่มมูลค่าทางธุรกิจให้แก่องค์กร
3) PCI Security Standard Council เป็นฟอรัมเปิดขนาดใหญ่ที่ถูกจัดตั้งขึ้นในปีค.ศ. 2006 เพื่อวัตถุประสงค์ในการพัฒนา จัดการ ให้ความรู้และความตระหนักเกี่ยวกับความมั่นคง โดยจัดทำมาตรฐานความมั่นคง PCI DSS (Data Security Standard) ซึ่งเป็นมาตรฐานที่รวบรวมความต้องการที่ไม่ใช่เชิงหน้าที่ด้านการจัดการความมั่นคง นโยบาย ขั้นตอน สถาปัตยกรรมเครือข่าย การออกแบบซอฟต์แวร์ และความต้องการที่ไม่ใช่เชิงหน้าที่ด้านอื่น ๆ
4) NIST (National Institute of Standards and Technology) ถูกจัดตั้งขึ้นในปีค.ศ. 1901 และเป็นส่วนหนึ่งของกระทรวงพาณิชย์สหรัฐฯ เป็นองค์กรที่จัดตั้งมาตรฐานใน

ด้านต่าง ๆ รวมถึงมาตรฐานความมั่นคงของคลาวด์ซึ่งเป็นมาตรฐานชุดที่ 800-144 ซึ่งมีวัตถุประสงค์เพื่อสร้างมาตรฐานความมั่นคงและนโยบายความเป็นส่วนตัวสำหรับการใช้งานคลาวด์สาธารณะ

นอกจากนี้ยังมี Jericho Forum ซึ่งเป็นกลุ่มเปิดที่จัดทำมาตรฐานสำหรับเทคโนโลยีสารสนเทศ NERC CIP (North American Electric Reliability Corporation) ซึ่งเป็นองค์กรที่จัดทำมาตรฐานเกี่ยวกับความเชื่อถือได้ HIPAA (Health Information Portability and Accountability Act) ซึ่งเป็นองค์กรที่จัดทำนโยบายความเป็นส่วนตัวของข้อมูลผู้ป่วย FedRAMP (Federal Risk and Authorization Management Program) ซึ่งเป็นโครงการของรัฐบาลอเมริกาเพื่อจัดทำมาตรฐานความมั่นคงและการควบคุมการให้บริการคลาวด์ GAPP (Generally Accepted Privacy Principles) ซึ่งเป็นองค์กรที่เสนอหลักการความเชื่อมั่นในบริการ โดยนำเสนอบรรทัดฐานการป้องกันความเป็นส่วนตัวของข้อมูลและ BITS Shared Assessment ซึ่งเป็นองค์กรที่จัดทำแม่แบบการประเมินการให้บริการด้านต่าง ๆ

องค์กรข้างต้น มีวัตถุประสงค์เดียวกันคือ เพื่อสร้างมาตรฐานเพื่อใช้ควบคุมกระบวนการการให้บริการให้เป็นไปตามความต้องการที่ไม่ใช่เชิงหน้าที่ด้านต่าง ๆ เช่น ด้านความมั่นคง ด้านความเป็นส่วนตัวของข้อมูล ด้านการตรวจสอบ เป็นต้น อย่างไรก็ตามผู้ใช้บริการคลาวด์จำเป็นต้องพิจารณาลักษณะขององค์กรของผู้ใช้บริการเอง และความต้องการที่ไม่ใช่เชิงหน้าที่ที่ผู้ให้บริการคลาวด์เสนอ ก่อนตัดสินใจเปลี่ยนไปใช้บริการคลาวด์เพื่อลดความเสี่ยง โดยสิ่งที่ต้องคำนึงถึง ได้แก่

1) กระบวนการหรือลักษณะการทำงานที่จะเปลี่ยนมาใช้บริการคลาวด์มีลักษณะสอดคล้องกับลักษณะของการให้บริการคลาวด์หรือไม่
2) เทคโนโลยีและสถาปัตยกรรมโครงสร้างพื้นฐานของผู้ให้บริการคลาวด์ ส่งผลกระทบต่อข้อตกลงในการให้บริการและมาตรการด้านความมั่นคงของผู้ใช้บริการคลาวด์หรือไม่
3) ควรเลือกลักษณะการใช้งานคลาวด์แบบใด ได้แก่ แบบสาธารณะ แบบส่วนบุคคล หรือแบบผสม เพื่อให้เหมาะสมกับองค์กร
4) ผู้ให้บริการคลาวด์มีการจัดการอย่างไรกับข้อมูลที่มีความอ่อนไหวสูง

5) ความโปร่งใสของผู้ให้บริการคลาวด์ ครอบคลุมประเภทของการให้บริการทั้งหมดที่ผู้ให้บริการคลาวด์มีหรือไม่ ได้แก่ การให้บริการซอฟต์แวร์ การให้บริการแพลตฟอร์ม และการให้บริการโครงสร้างพื้นฐาน
6) ปัญหาของความต้องการแบนด์วิดท์ (Bandwidth Requirement) เมื่อเปลี่ยนมาใช้บริการคลาวด์ เช่น การเกิดสภาพคอขวด (Bottleneck) มีโอกาสเกิดขึ้นได้หรือไม่ [7]
7) ผลกระทบทางการเงินระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์ ได้แก่ ค่าบริการที่ไม่มีการรับประกัน ปัญหาทางกฎหมายที่อาจเกิดขึ้นกับผู้ให้บริการคลาวด์มีโอกาสเกิดขึ้นได้หรือไม่ [7]
8) การสูญเสียการควบคุมข้อมูล อาจนำมาซึ่งปัญหาการรักษาความลับของข้อมูล [7]

2.1.3 วิธีจีคิวเอ็ม

จีคิวเอ็ม (Goal Question Metric: GQM) นำเสนอโดย Victor R. Basili, Gianluigi Caldiera และ H.Dieter Rombach [4] เป็นแนวทางที่อยู่บนสมมติฐานที่ว่าการประเมินองค์กรอย่างมีประสิทธิภาพ จำเป็นต้องระบุเป้าหมายที่จะทำการประเมิน เป้าหมายนี้ จะเป็นตัวกำหนดกระบวนการและลักษณะข้อมูล เพื่อให้ข้อมูลที่เกิดจากกระบวนการต่าง ๆ สามารถวัดในเชิงปริมาณและใช้วิเคราะห์ได้ว่ากระบวนการและข้อมูลเป็นไปตามเป้าหมายที่ตั้งไว้หรือไม่ ดังแสดงในภาพที่ 2.2

วิธีการวัดแบบจีคิวเอ็ม แบ่งเป็น 3 ระดับ ได้แก่

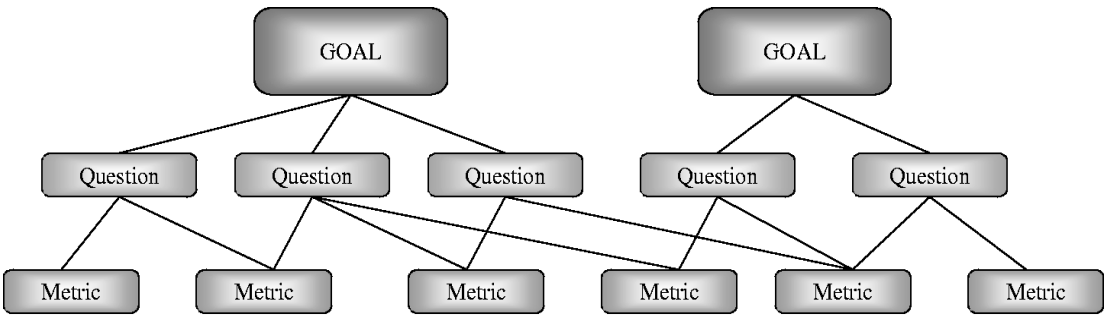
1) ระดับแนวคิด (Conceptual Level) หรือเป้าหมาย ในระดับนี้จะเป็นการกำหนดเป้าหมายสำหรับวัตถุประสงค์อย่างใดอย่างหนึ่ง โดยเป้าหมายจะมี 3 แบบ คือ

    - เป้าหมายด้านผลิตภัณฑ์ (Products) ได้แก่ สิ่งที่เป็นผลจากการดำเนินงานในขั้นตอนต่าง ๆ เช่น ข้อกำหนด (Specification) การออกแบบ (Designs) โปรแกรม (Programs) ชุดทดสอบ (Test Suites) เป็นต้น
    - เป้าหมายด้านกระบวนการ (Processes) ได้แก่ กิจกรรมที่ดำเนินไปในการทำซอฟต์แวร์และมีความเกี่ยวข้องกับเวลา เช่น รายละเอียด การออกแบบ การทดสอบ การสัมภาษณ์
    - เป้าหมายด้านทรัพยากร (Resources) ได้แก่ สิ่งที่ถูกใช้ในกระบวนการเพื่อให้เกิดผลลัพธ์ เช่น แรงงานคน ฮาร์ดแวร์ ซอฟต์แวร์ พื้นที่สำนักงาน

2) ระดับการปฏิบัติการ (Operational Level) หรือการตั้งคำถาม เป็นชุดของคำถามที่ตั้งขึ้นเพื่อให้สอดคล้องกับลักษณะของเป้าหมาย

3) ระดับการวัดเชิงปริมาณ (Quantitative Level) เป็นชุดของข้อมูลที่เกี่ยวข้องกับคำถามเพื่อใช้ในการตอบคำถามเชิงปริมาณ โดยลักษณะของข้อมูลแบ่งเป็น

- เชิงวัตถุวิสัย (Objective) คือ ข้อมูลที่เกิดจากเป้าหมายที่กำหนด มีวัตถุประสงค์เพียงเพื่อต้องการวัดและไม่มีมุมมองใดที่ต้องพิจารณาเป็นพิเศษ เช่น จำนวนชุดเอกสาร จำนวนชั่วโมงทำงานของพนักงาน ขนาดของโปรแกรม
- เชิงนามธรรม (Subjective) คือ ข้อมูลที่เกิดจากเป้าหมายที่กำหนด มีวัตถุประสงค์เพื่อต้องการวัดและมีมุมมองที่ต้องพิจารณา เช่น ความสามารถในการอ่านได้ของข้อความ ระดับความพึงพอใจของผู้ใช้งาน



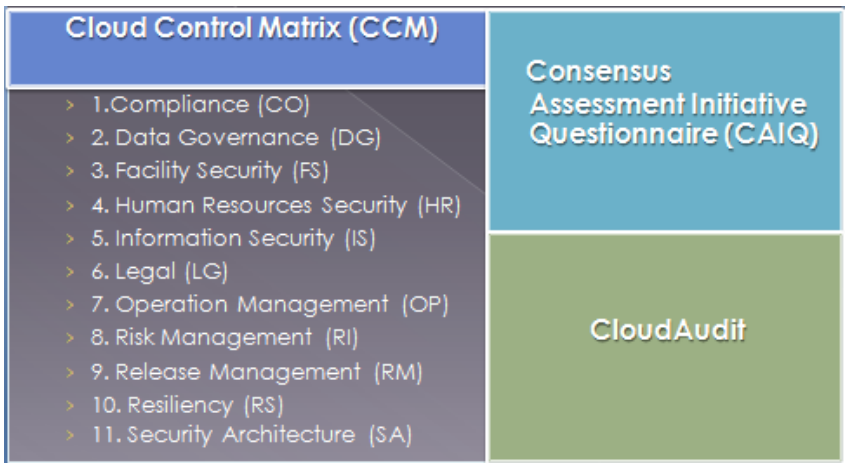
Source: Basili *et al.* (1994)

ภาพที่ 2.2 ความสัมพันธ์ของระดับวิธีวัดแบบจีคิวเอ็ม [4]

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง

ความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงเป็นประเด็นสำคัญในการใช้และการให้บริการคลาวด์ งานวิจัยที่นำเสนอโดยองค์กรความมั่นคงของคลาวด์หรือซีเอสเอ เป็นงานวิจัยหลักที่ถูกนำมาใช้เป็นแนวคิดของวิทยานิพนธ์

จากภาพที่ 2.3 งานวิจัยขององค์กรความมั่นคงของคลาวด์ที่ถูกนำมาใช้ในวิทยานิพนธ์แบ่งเป็น 3 งานวิจัย ได้แก่ เมตริกซ์ควบคุมคลาวด์ [1] คำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ [2] และการตรวจสอบคลาวด์ (CloudAudit)



ภาพที่ 2.3 งานวิจัยที่นำเสนอโดยองค์กรความมั่นคงของคลาวด์

เมตริกซ์ควบคุมคลาวด์เป็นเมตริกซ์ที่รวบรวมความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคง 11 ด้าน พร้อมทั้งกำหนดเป้าหมายการควบคุมความมั่นคง ส่วนคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ เป็นการระบุคำถามที่สอดคล้องกับการประเมินเป้าหมายการควบคุมความมั่นคงที่ระบุไว้ในเมตริกซ์ควบคุมคลาวด์ ทั้งนี้เพื่อให้ผู้ให้บริการคลาวด์ใช้เป็นแนวทางในการนำไปปฏิบัติเพื่อสร้างความเชื่อมั่นให้กับผู้ใช้บริการคลาวด์ และเพื่อให้ผู้ใช้บริการคลาวด์ใช้เป็นแนวทางในการตรวจสอบผู้ให้บริการคลาวด์ โดยเมตริกซ์ควบคุมคลาวด์และคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ จัดทำขึ้นโดยรวบรวมมาตรฐานขององค์กรที่ภาคอุตสาหกรรมให้การยอมรับ ได้แก่ ISO 27001, ISACA, COBIT, PCI, NIST, Jericho Forum และ NERC CIP โดยลักษณะของเมตริกซ์ควบคุมคลาวด์และคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ เป็นไปตามตารางที่ 2.1 และตารางที่ 2.2

ตารางที่ 2.1 ลักษณะของเมตริกซ์ควบคุมคลาวด์

ความมั่นคง	รหัสความมั่นคง	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
การปฏิบัติตาม (Compliance)	CO	การวางแผนการตรวจสอบ	CO-01	ผู้ให้บริการคลาวด์มีแผนการตรวจสอบ กิจกรรมการดำเนินการตรวจสอบการทำงานเพื่อป้องกันการหยุดชะงักของระบบ
การกำกับดูแลข้อมูล (Data Governance)	DG	ความเป็นเจ้าของ/การดูแลข้อมูล	DG-01	ข้อมูลทั้งหมดจะต้องถูกกำหนดการดูแลข้อมูลในรูปแบบของการกำหนดหน้าที่ความรับผิดชอบ เอกสาร และการสื่อสาร
ความมั่นคงด้านสิ่งอำนวยความสะดวก (Facility Security)	FS	นโยบายความมั่นคงด้านสิ่งอำนวยความสะดวก	FS-01	นโยบายและขั้นตอนจะต้องถูกจัดตั้งขึ้นเพื่อรักษาความปลอดภัยและเพื่อให้เกิดความมั่นคงในสภาพแวดล้อมการทำงาน

ตารางที่ 2.1 ลักษณะของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัสความมั่นคง	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
ความมั่นคงด้านทรัพยากรมนุษย์ (Human Resources Security)	HR	การคัดกรองภูมิหลัง	HR-01	ตามกฎหมาย ข้อบังคับ จริยธรรม และข้อจำกัดตามสัญญาการจ้างงาน ลูกจ้าง ผู้สมัครร่วมงาน ผู้รับจ้าง และผู้ที่เกี่ยวข้องกับการดำเนินงาน ต้องได้รับการตรวจสอบและคัดกรองภูมิหลัง โดยความเข้มงวดในการตรวจสอบ จะขึ้นอยู่กับความสามารถของลูกจ้างหรือผู้ร่วมงานในการเข้าถึงข้อมูลที่สำคัญ และความเสี่ยงที่ยอมรับได้

ตารางที่ 2.1 ลักษณะของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัสความมั่นคง	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
ความมั่นคงด้านสารสนเทศ (Information Security)	IS	โปรแกรมการจัดการความมั่นคงด้านสารสนเทศ	IS-01	โปรแกรมการจัดการความมั่นคง ควรมีความเกี่ยวข้องในด้านการจัดการความเสี่ยง, นโยบายความมั่นคง, องค์กรเกี่ยวกับความมั่นคงทางสารสนเทศ, การจัดการทรัพย์สิน, ทรัพยากรมนุษย์, สภาพแวดล้อมขององค์กร, การจัดการการสื่อสารและการปฏิบัติการ, การควบคุมการเข้าถึงข้อมูล, การพัฒนาบำรุงรักษา ระบบสารสนเทศ
กฎหมาย (Legal)	LG	ข้อตกลงในการไม่เปิดเผย	LG-01	ผู้ให้บริการคลาวด์ต้องระบุความต้องการด้านการไม่เปิดเผยข้อมูลของผู้ใช้บริการคลาวด์

ตารางที่ 2.1 ลักษณะของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัสความมั่นคง	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
การจัดการการดำเนินการ (Operation Management)	OP	นโยบายการจัดการการดำเนินการ	OP-01	นโยบายและขั้นตอนจะต้องถูกจัดตั้งขึ้นและเพียงพอสำหรับให้บุคลากรที่ปฏิบัติงานนำไปใช้ในการดำเนินการตามหน้าที่ของตน
การจัดการความเสี่ยง (Risk Management)	RI	โปรแกรมการจัดการความเสี่ยง	RI-01	ผู้ให้บริการคลาวด์ต้องมีการพัฒนาและบำรุงรักษากรอบการจัดการความเสี่ยงเพื่อจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
การจัดการการปล่อย/เริ่มต้นให้บริการ (Release Management)	RM	การพัฒนาหรือการได้มาซึ่งสิ่งใหม่	RM-01	นโยบายจะต้องถูกจัดตั้งขึ้นเพื่อจำกัดสิทธิ์การพัฒนาแอพพลิเคชัน ระบบ ฐานข้อมูล โครงสร้างพื้นฐาน และสิ่งอำนวยความสะดวก

ตารางที่ 2.1 ลักษณะของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัสความมั่นคง	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
การคืนสภาพได้ (Resiliency)	RS	โปรแกรมการจัดการการคืนสภาพได้	RS-01	นโยบาย กระบวนการ และขั้นตอนการดำเนินธุรกิจอย่างต่อเนื่องและการฟื้นฟูธุรกิจจากเหตุภัยพิบัติจะต้องถูกกำหนดเพื่อลดผลกระทบที่จะเกิดขึ้นและเพื่ออำนวยความสะดวกในการฟื้นฟู และต้องมีการสื่อสารให้บุคลากรในองค์กรได้รับทราบ
สถาปัตยกรรมความมั่นคง (Security Architecture)	SA	ความต้องการการเข้าถึงข้อมูลของลูกค้า	SA-01	ผู้ให้บริการคลาวด์ต้องกำหนดสัญญาและข้อกำหนดสิทธิ์สำหรับผู้ใช้บริการคลาวด์ในการเข้าถึงข้อมูล ทรัพย์สิน และระบบสารสนเทศ

สำหรับลักษณะของคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ จะถูกกำหนดแยกจากเมตริกซ์ควบคุมคลาวด์ แต่จะเกี่ยวข้องกันโดยคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่เป็นการตั้งคำถามที่สอดคล้องกับเป้าหมายการควบคุมความมั่นคงทั้ง 11 ด้านของเมตริกซ์ควบคุมคลาวด์ และมีลักษณะของคำตอบเป็น “ใช่/ไม่ใช่” นอกจากนี้ยังระบุลักษณะการให้บริการคลาวด์ที่ถูกประเมินได้จากคำถาม และผู้เกี่ยวข้องได้แก่ ผู้ให้บริการคลาวด์หรือผู้ตรวจสอบความมั่นคงของคลาวด์ สามารถนำคำถามไปประยุกต์ใช้ในการประเมินได้ ดังตัวอย่างตามตารางที่ 2.2

ตารางที่ 2.2 ลักษณะของคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่

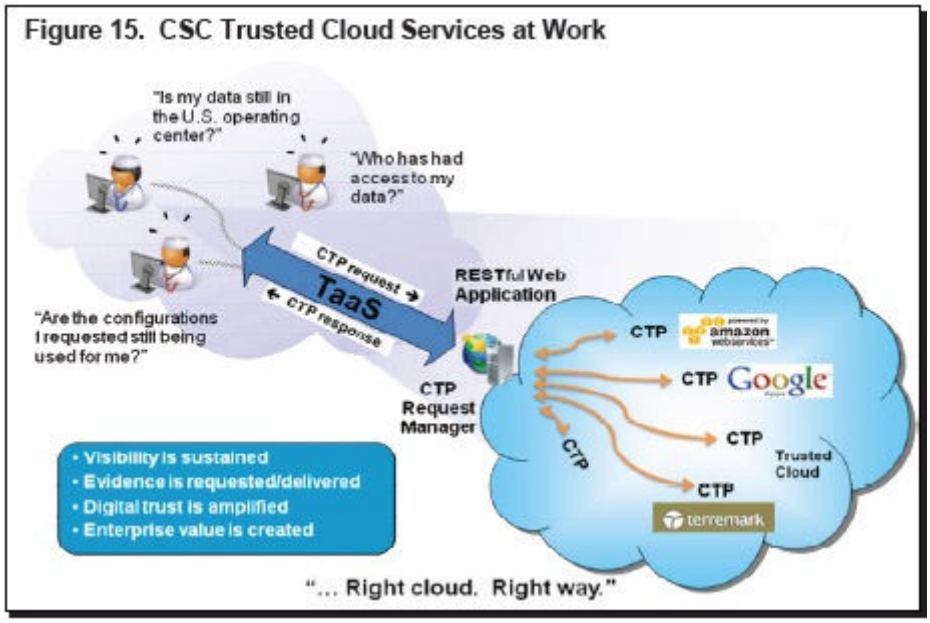
รหัสเป้าหมาย	รหัสคำถาม	คำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่	ลักษณะการให้บริการคลาวด์ที่ถูกประเมินได้จากคำถาม	ผู้เกี่ยวข้องที่สามารถนำคำถามไปประยุกต์ใช้ในการประเมินได้
CO-01	CO-01.1	CO-01.1 ผู้ให้บริการคลาวด์มีการยืนยันการตรวจสอบที่อยู่ในรูปแบบมาตรฐานที่เป็นที่ยอมรับในภาคอุตสาหกรรม เช่น CloudAudit/A6 URI Ontology หรือไม่	1. การให้บริการโครงสร้างพื้นฐาน 2. การให้บริการแพลตฟอร์ม 3. การให้บริการซอฟต์แวร์	1. ผู้ให้บริการคลาวด์ 2. ผู้ตรวจสอบความมั่นคงของคลาวด์

งานวิจัยการตรวจสอบคลาวด์ขององค์กรเดียวกันนี้ ได้ประยุกต์เมตริกซ์ควบคุมคลาวด์เพื่อวัตถุประสงค์ในการตรวจสอบ ยืนยัน ประเมินผลและสร้างความเชื่อมั่นให้กับบริการของผู้ให้บริการคลาวด์ โดยพัฒนาส่วนต่อประสานและเนมสเปซเพื่อให้การตรวจสอบสามารถทำได้โดยอัตโนมัติ

นอกจากนี้งานวิจัยของ Ron Knode และ Doug Egan [8] ได้นำแนวคิดของเมตริกซ์ควบคุมคลาวด์มาประยุกต์เช่นเดียวกัน โดยสร้างบริการความโปร่งใส (Transparency as a Service) เพื่อให้บริการแก่ผู้ใช้บริการคลาวด์ในการสอบถามข้อตกลงรวมถึงหลักฐานตามข้อตกลงจากผู้ให้บริการคลาวด์ ทั้งนี้เพื่อให้ผู้ใช้บริการคลาวด์มั่นใจว่าผู้ให้บริการคลาวด์ได้ทำตามข้อตกลงที่ให้ไว้จริง ประเด็นสำคัญของงานวิจัยของ Knode และ Egan คือการแสดงความโปร่งใสของผู้ให้บริการคลาวด์ต่อผู้ใช้บริการคลาวด์ ผ่านหลักฐานตามข้อตกลง และความโปร่งใสนี้จะนำมาซึ่ง

การตัดสินใจเลือกใช้บริการคลาวด์ที่เพิ่มมากขึ้น อย่างไรก็ตาม งานวิจัยของ Knode และ Egan เป็นการตรวจสอบระหว่างการใช้บริการคลาวด์ นั่นคือ ผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ตกลงทำธุรกรรมร่วมกันแล้วจึงจะสามารถตรวจสอบการให้บริการตามข้อตกลงได้ และการใช้บริการความโปร่งใสนี้ จะใช้รูปแบบการถามตอบ (Question and Response Pattern) ระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์

จากภาพที่ 2.4 แสดงให้เห็นว่าในกระบวนการทำงานของการให้บริการความโปร่งใสจำเป็นต้องอาศัยคนเพื่อพิจารณาหาหลักฐานที่เหมาะสมกับคำถามที่ผู้ใช้บริการคลาวด์สอบถาม นอกจากนี้บริการความโปร่งใส ยังเป็นการให้บริการประเภทไม่ประสานเวลา (Asynchronous Service) นั่นคือ หลังการสอบถาม ผู้ใช้บริการคลาวด์จะไม่ได้รับคำตอบในทันที เนื่องจากต้องอาศัยเวลาให้ผู้ให้บริการคลาวด์พิจารณาหาหลักฐานที่เหมาะสมกับคำถาม ดังที่ได้กล่าวมาแล้ว



ภาพที่ 2.4 กระบวนการการให้บริการความโปร่งใส [8]

อย่างไรก็ตามงานวิจัยของ Knode และ Egan ได้นำมาซึ่งแนวความคิดของการทำงานวิจัยนี้ โดยเฉพาะประเด็นการตรวจสอบที่ทำได้ภายหลังการเลือกใช้บริการคลาวด์แล้วเท่านั้น ดังนั้นส่วนหนึ่งของการทำงานวิจัยจึงเป็นไปเพื่อต้องการปรับปรุงประเด็นดังกล่าว โดยทำให้การตรวจสอบเป็นประโยชน์ต่อการตัดสินใจของผู้ใช้บริการคลาวด์มากขึ้น นั่นคือ ผู้ใช้บริการคลาวด์สามารถตรวจสอบผู้ให้บริการคลาวด์ได้ก่อนการตัดสินใจเลือกใช้บริการ โดยการตัดสินใจจะ

พิจารณาจากคะแนนความมั่นคงทั้ง 11 ด้านของซีเอสเอ หรือจะพิจารณาจากการจัดลำดับผู้ให้บริการคลาวด์ก็สามารถทำได้

นอกจากงานวิจัยของ Knode และ Egan ที่เป็นแนวคิดในการทำงานวิจัยนี้แล้ว ยังมีงานวิจัยที่เกี่ยวข้องในด้านต่าง ๆ ดังนี้

2.2.1 งานวิจัยที่เกี่ยวข้องกับการประเมินความมั่นคงของผู้ให้บริการคลาวด์

นอกเหนือจากงานวิจัยของ Ron Knode และ Doug Egan ที่ได้กล่าวถึงข้างต้น ยังมีงานวิจัยอื่นที่เกี่ยวข้องกับการพิจารณาความมั่นคงเพื่อสร้างความน่าเชื่อถือให้ผู้ให้บริการคลาวด์เช่น

1) งานวิจัยของ Wayne A. Pauley [9]

นำเสนอการประเมินความโปร่งใสของผู้ให้บริการคลาวด์ในด้านความมั่นคง ความเป็นส่วนตัว ความสามารถในการตรวจสอบได้ และข้อตกลงในการให้บริการ บนแนวความคิดที่ว่า ความพร้อมของข้อมูลที่เกี่ยวข้องกับการประเมินทั้งสี่ด้านดังกล่าว ทำให้เกิดความโปร่งใสและเกิดความสามารถในการนำข้อมูลมาประเมินความเสี่ยงได้

Pauley ได้เสนอรูปแบบการประเมินผู้ให้บริการคลาวด์ในลักษณะของบัตรลงคะแนน (Scorecard) บนเว็บไซต์ ทั้งนี้เพื่อลดการใช้คนในการทำการประเมิน จากนั้นผู้วิจัยจะเก็บรวบรวมข้อมูลจากผู้ให้บริการคลาวด์รายต่าง ๆ เพื่อนำมาตอบคำถามที่อยู่ในบัตรลงคะแนน โดยลักษณะของคำถามจะเป็นคำถามที่ตอบได้ด้วย “ใช่” หรือ “ไม่ใช่” ถ้าคำตอบคือ “ใช่” คะแนนของคำถามจะถูกคิดเป็น 1 คะแนน แต่ถ้าคำตอบคือ “ไม่ใช่” คะแนนของคำถามจะถูกคิดเป็น 0 คะแนน และคำถามที่สร้างขึ้นจะอ้างอิงมาตรฐานขององค์กรความมั่นคงของคลาวด์ NIST และสภาความมั่นคงด้านเครือข่ายและข้อมูลของยุโรป (European Network and Information Security Agency: ENISA) โดยกระบวนการในการประเมินแบ่งเป็น 3 ขั้นตอน ได้แก่

- ขั้นตอนก่อนการประเมิน (Pre-assessment) ในขั้นตอนนี้ผู้ใช้บริการคลาวด์จะถามคำถามชี้นำประเภท ลักษณะการให้บริการคลาวด์ ลักษณะการใช้งานคลาวด์ หรือผู้ให้บริการคลาวด์เป็นองค์กรเพื่อแสวงผลกำไรหรือไม่ คำถามเหล่านี้จะสามารถคัดกรองผู้ให้บริการคลาวด์ได้ในเบื้องต้น ว่า

ลักษณะของผู้ให้บริการคลาวด์เหมาะสมกับลักษณะทางธุรกิจของผู้ใช้บริการคลาวด์หรือไม่

- ขั้นตอนการลงรายละเอียดการประเมิน (Detailed Assessment) ในขั้นตอนนี้จะเป็นการสำรวจผู้ให้บริการคลาวด์แต่ละรายจากเว็บไซต์ของผู้ให้บริการคลาวด์เองเพื่อเก็บรวบรวมข้อมูลทั้ง 4 ด้าน ได้แก่
    - ข้อมูลที่เก็บรวบรวมเพื่อนำมาประเมินในด้านความมั่นคง ตัวอย่างเช่น ผู้ให้บริการมีการทำตามมาตรฐานด้านความมั่นคง เช่น COBIT, ISO27000 หรือ NIST หรือไม่
    - ข้อมูลที่เก็บรวบรวมเพื่อนำมาประเมินในด้านความเป็นส่วนตัว ตัวอย่างเช่น ผู้ให้บริการมีนโยบายการรักษาความเป็นส่วนตัวของผู้ใช้บริการหรือไม่ หรือถ้าผู้ให้บริการคลาวด์มีการเรียกใช้บริการจากผู้ให้บริการรายอื่น จะมีข้อตกลงร่วมกันเกี่ยวกับนโยบายความเป็นส่วนตัวหรือไม่
    - ข้อมูลที่เก็บรวบรวมเพื่อนำมาประเมินความสามารถในการตรวจสอบได้ ตัวอย่างเช่น ผู้ให้บริการคลาวด์มีการทำตามมาตรฐานด้านความสามารถในการตรวจสอบได้ เช่น ISACA หรือไม่
    - ข้อมูลที่เก็บรวบรวมเพื่อนำมาประเมินในด้านข้อตกลงในการให้บริการ ตัวอย่างเช่น ผู้ให้บริการมีการนำเสนอข้อตกลงในการให้บริการหรือไม่ และข้อตกลงนี้มีการประยุกต์ใช้ได้กับทุกบริการของผู้ให้บริการคลาวด์หรือไม่

- ขั้นตอนหลังการประเมิน (Post-assessment) ในขั้นตอนนี้จะเป็นการเปรียบเทียบข้อมูลที่รวบรวมได้กับนโยบายหรือมาตรฐานที่จัดทำขึ้นภายในองค์กร เพื่อดูว่าผู้ให้บริการคลาวด์ ให้ข้อมูลที่เพียงพอกับนโยบายหรือมาตรฐานขององค์กรหรือไม่

ผลการประเมินผู้ให้บริการคลาวด์แต่ละราย จะใช้วิธีการนับคะแนนจากคำถามแต่ละข้อและพิจารณาจากผลรวมคะแนน รวมทั้งเปรียบเทียบคะแนนในด้านต่าง ๆ ทั้งสี่ด้านของผู้ให้บริการคลาวด์แต่ละราย

ถึงแม้ว่าแนวความคิดของงานวิจัยของ Pauley จะเป็นไปเพื่อลดเวลาและลดการใช้คนในการประเมิน แต่ขั้นตอนในการรวบรวมข้อมูลซึ่งต้องอาศัยผู้ใช้บริการคลาวด์หรือองค์กรที่สามในการรวบรวมข้อมูลจากผู้ให้บริการคลาวด์ก็เป็นขั้นตอนที่ต้องใช้คนและใช้เวลา อีกทั้งคำถามที่ใช้ในการประเมินสามารถวัดได้ในเชิงปริมาณคือใช่หรือไม่ใช่เท่านั้น แต่ไม่สามารถวัดได้ว่าคำตอบของแต่ละข้อมีคุณภาพหรือไม่ในระดับใด นั่นคือ เอกสารหรือกระบวนการที่ผู้ให้บริการคลาวด์จัดทำขึ้นสอดคล้องกับวัตถุประสงค์ที่ระบุในตัววัดหรือไม่ และเอกสารหรือกระบวนการนั้นเสร็จสมบูรณ์ดีแล้วหรือดำเนินการไปแล้วมากน้อยเพียงใด

2) บทความของ Bret Michael [10] และงานวิจัยของ Sun Microsystems, Inc. [11]

ให้ความสำคัญกับประเด็นความน่าเชื่อถือและความโปร่งใสของคลาวด์ โดย Bret Michael ตั้งคำถามถึงปริมาณข้อมูลที่ใช้ในการประเมินความโปร่งใส ว่าต้องมีข้อมูลเท่าไรถึงจะเพียงพอ และมุ่งเน้นให้ผู้ให้บริการคลาวด์ให้ความสำคัญกับการสร้างความน่าเชื่อถือแก่ผู้ใช้บริการคลาวด์

เช่นเดียวกับงานวิจัยของ Sun Microsystems, Inc. ที่นำเสนอความโปร่งใสในด้านความมั่นคงโดยอ้างอิงมาตรฐานความมั่นคง ISO27001 และได้กำหนดข้อมูลที่ผู้ให้บริการคลาวด์ควรเปิดเผยและไม่ควรเปิดเผย 8 ข้อ ได้แก่

- ควรเปิดเผยข้อมูลและแนวทางปฏิบัติด้านการรักษาความมั่นคง
- ควรเปิดเผยข้อมูลตามคำสั่งหรือข้อตกลง เช่น ข้อมูลตามบัญญัติกฎหมายหรือตามที่บัญญัติไว้ในองค์กรว่าต้องมีการเปิดเผย
- ควรเปิดเผยข้อมูลด้านสถาปัตยกรรมความมั่นคง
- ควรเปิดเผยหน้าที่ความรับผิดชอบของผู้ให้บริการคลาวด์ต่อผู้ใช้บริการคลาวด์อย่างชัดเจน
- ไม่ควรเปิดเผยข้อมูลที่จะทำให้เกิดความเสี่ยงต่อศูนย์ข้อมูล (Data Center) เช่น ข้อมูลการเข้าถึงฐานข้อมูลที่อยู่ภายในศูนย์ข้อมูล

- ไม่ควรเปิดเผยข้อมูลที่จะเป็นอันตรายต่อผู้ใช้บริการคลาวด์หรือผู้เกี่ยวข้อง เช่น ข้อมูลส่วนตัวของผู้ใช้บริการคลาวด์หรือผู้เกี่ยวข้อง
- ไม่ควรเปิดเผยข้อมูลที่ไม่เหมาะสมเกี่ยวกับการแสดงความรับผิดชอบของผู้ให้บริการคลาวด์ เช่น การเปิดเผยข้อมูลระดับความมั่นคงที่สูงเกินกว่าผู้ให้บริการคลาวด์จะรับผิดชอบได้
- ไม่ควรเปิดเผยข้อมูลที่ผิดกฎหมายหรือกฎบัญญัติ เช่น การส่งผ่านข้อมูลออกนอกสหภาพยุโรปเป็นการกระทำที่ผิดตามข้อตกลงของสหภาพยุโรป

อย่างไรก็ตามงานวิจัยทั้งสอง ได้เสนอเพียงแนวคิดและหลักการเท่านั้น แต่ไม่ได้นำไปสู่วิธีการประเมินหรือชี้วัดค่าความมั่นคงของการให้บริการคลาวด์

3) งานวิจัยของ Catherine Everett [12]

ได้ตั้งประเด็นเกี่ยวกับการตั้งคำถามที่นำไปสู่การประเมินความมั่นคง โดยกล่าวว่าหากผู้ใช้บริการคลาวด์ไม่สามารถตั้งคำถามต่อผู้ให้บริการคลาวด์ได้ว่าคาดหวังความมั่นคงจากสิ่งใดบ้าง (คำถามเหล่านี้สะท้อนให้เห็นว่าผู้ใช้บริการคลาวด์มีลักษณะองค์กรแบบใด และต้องการการให้บริการคลาวด์และการใช้งานคลาวด์แบบใด ซึ่งจะนำไปสู่การหาหลักฐานความมั่นคงจากผู้ให้บริการคลาวด์) นั่นถือเป็นความเสี่ยงที่ต้องเฝ้าระวัง ซึ่งนำมาสู่แนวความคิดในการพิจารณาตัววัดความมั่นคงของผู้ให้บริการคลาวด์ในงานวิจัยนี้

4) งานวิจัยของ Burton S. Kaliski Jr. และ Wayne Pauley [13]

ได้นำเสนอบริการการประเมินความเสี่ยง (Risk Assessment as a Service) โดยมีวัตถุประสงค์เพื่อให้องค์กรนำผลการประเมินความเสี่ยงมาใช้ในการตัดสินใจว่าจะประยุกต์ใช้ทรัพยากรใหม่ที่ยังไม่เคยใช้บริการมาก่อนอย่างไร เพื่อให้ทรัพยากรเหล่านั้นสามารถปกป้องสินทรัพย์ที่มีความสำคัญขององค์กรได้โดยการประเมินความเสี่ยงประกอบด้วยการประเมินความมั่นคง การตรวจสอบและการประเมินผลจากองค์กรภายนอก และการประเมินความเป็นส่วนตัว

งานวิจัยยังได้ให้เหตุผลในการประเมินความเสี่ยงของการใช้บริการคลาวด์ว่า การบริการคลาวด์เปรียบเสมือนการทำการค้าทางอิเล็กทรอนิกส์ (E-Commerce) ซึ่งประเด็นความมั่นคงและความเป็นส่วนตัวในการทำการค้าทางอิเล็กทรอนิกส์ถือเป็นเรื่องสำคัญ เนื่องจากนำมาซึ่งความเชื่อใจและความไว้วางใจของผู้ใช้บริการ เช่นเดียวกันกับการ

ให้บริการคลาวด์ที่ความเชื่อใจของผู้ใช้บริการคลาวด์มีความสำคัญ ดังนั้น ผู้ให้บริการคลาวด์จึงควรมีสิ่งที่แสดงให้เห็นถึงกระบวนการรักษาความมั่นคงและความเป็นส่วนตัวของข้อมูลหรือหลักฐานอ้างอิง เพื่อให้ผู้ใช้บริการคลาวด์ประเมินได้ เช่น Amazon.com ที่ออกประกาศว่าได้ผ่านการตรวจสอบ SAS70 Type 2 ซึ่งเป็นการตรวจสอบว่าองค์กรได้ทำตามวัตถุประสงค์และกิจกรรมด้านความมั่นคงตามที่กำหนดไว้หรือไม่ โดยส่วนใหญ่จะเน้นไปที่เทคโนโลยีสารสนเทศ อย่างไรก็ตาม หลายองค์กรพยายามสร้างมาตรฐานการรักษาความมั่นคงและความเป็นส่วนตัวในการให้บริการคลาวด์ เช่น ซีเอสเอ แต่มาตรฐานที่สร้างขึ้นก็เป็นเพียงคำถามปลายเปิดที่ไม่สามารถวัดความมั่นคงและความเป็นส่วนตัวได้อย่างชัดเจน

สำหรับการประเมินผู้ให้บริการคลาวด์ ในงานวิจัยของ Burton มองว่า เนื่องจากบริการคลาวด์เป็นบริการที่สามารถจัดเตรียมการใช้งานได้ตามความต้องการของผู้ใช้บริการเอง โดยไม่ต้องมีการปฏิสัมพันธ์กับผู้ให้บริการดังนั้น การประเมินก็ควรเป็นไปในลักษณะเดียวกัน คือผู้ใช้บริการคลาวด์สามารถประเมินผู้ให้บริการคลาวด์ได้ตามต้องการ โดยไม่ต้องมีปฏิสัมพันธ์กับผู้ให้บริการคลาวด์ และจากลักษณะการเป็นบริการของคลาวด์ (As a Service) การประเมินจึงควรทำได้แบบเป็นบริการด้วยเช่นเดียวกัน ดังนั้นงานวิจัยจึงเสนอบริการการประเมินความเสี่ยงซึ่งเป็นการประเมินแบบทันทีทันใด (Real Time Assessment) เช่น ผู้ให้บริการคลาวด์ มีการแสดงหลักฐานอ้างอิงตลอดระยะเวลาที่มีการปฏิบัติการ (Run-Time) โดยหลักฐานอ้างอิงอาจเป็น ล็อกไฟล์ (Log Files) ที่แสดงให้เห็นว่าผู้ให้บริการมีหลักฐานที่บันทึกข้อมูลที่ผ่านเข้าออกสู่ระบบ นอกจากนี้ Burton ยังให้เหตุผลว่าควรมีการออกแบบการประเมินให้เข้ากับลักษณะการทำงานของคลาวด์ เช่น บริการคลาวด์ที่มีการทำงานร่วมกันระหว่างผู้ให้บริการคลาวด์หลายเจ้า เป็นต้น

ถึงแม้ว่าผลสรุปจากงานวิจัยของ Kaliski Jr. และ Pauley จะมีเพียงแนวคิดในการออกแบบการประเมินเท่านั้น แต่แนวคิดในการพยายามทำให้การประเมินเป็นไปแบบทันทีทันใดเป็นสิ่งที่น่าสนใจสำหรับผู้วิจัยเนื่องจากมีความแตกต่างจากการประเมินโดยทั่วไปที่อาศัยการพิจารณาจากหลักฐานซึ่งอาจจะเป็นหลักฐานที่ไม่มีการเปลี่ยนแปลงมานานแล้ว ผู้วิจัยจึงมีแนวคิดในการนำฟีดมาใช้ในการรับข้อมูลจากผู้ให้บริการคลาวด์ เนื่องจากลักษณะของฟีดเป็นการทำงานแบบดึงข้อมูลที่มีการแจ้งการเปลี่ยนแปลง ดังนั้นหากผู้ให้บริการคลาวด์มีการเปลี่ยนแปลงข้อมูลหรือหลักฐานอ้างอิงความมั่นคง ระบบที่

พัฒนาขึ้นก็สามารถดึงข้อมูลเหล่านั้นเพื่อมาวิเคราะห์หาคะแนนใหม่ได้ อย่างไรก็ตาม การออกแบบระบบลักษณะนี้อาจยังไม่เป็นการทำงานแบบทันทีทันใด แต่ก็เป็นวิธีหนึ่งที่ทำให้ได้ข้อมูลที่มีการปรับปรุงล่าสุดของผู้ให้บริการคลาวด์

5) งานวิจัยของ David Tancock และคณะ [14]

นำเสนอเครื่องมือที่ใช้วัดความเป็นส่วนตัวของการคำนวณแบบคลาวด์โดยเครื่องมือที่พัฒนาขึ้น จะเป็นการนำเสนอความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความเป็นส่วนตัวที่อาจก่อให้เกิดความเสี่ยงในองค์กร โดย Tancock และคณะเน้นกลุ่มผู้ใช้งานซึ่งเป็นองค์กรที่ไม่มีความเชี่ยวชาญทางความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความเป็นส่วนตัว เพื่อให้องค์กรวางแนวทางในการป้องกันการเกิดความเสี่ยง โดยวิธีนี้จะทำให้การป้องกันความเสี่ยงด้านความเป็นส่วนตัวถูกนำมาใช้ตั้งแต่ขั้นตอนการเริ่มต้นโครงการนอกจากนี้ผู้ใช้บริการคลาวด์ยังสามารถนำข้อมูลความเสี่ยงมาวิเคราะห์ในการริเริ่มโครงการต่าง ๆ ว่าเหมาะสมหรือไม่ ส่วนการออกแบบเครื่องมือ จะมีการออกแบบในลักษณะของแบบสอบถามเพื่อให้ผู้ให้บริการคลาวด์ตอบคำถามเกี่ยวกับนโยบายการรักษาความเป็นส่วนตัวในด้านต่าง ๆ แล้วนำคำตอบมาเก็บบันทึกเป็นฐานความรู้ (Knowledge Base) เพื่อใช้วิเคราะห์ความเสี่ยงด้านความเป็นส่วนตัวต่อไป

งานวิจัยด้านการประเมินความมั่นคงของผู้ให้บริการคลาวด์สามารถสรุปได้ดังตารางที่ 2.3

ตารางที่ 2.3 สรุปงานวิจัยด้านการประเมินความมั่นคงของผู้ให้บริการคลาวด์

ผู้วิจัย	ประเด็นในงานวิจัย	แนวคิดของงานวิจัย	ปัญหาของงานวิจัย
Ron Knode และ Doug Egan	ความโปร่งใสของผู้ให้บริการคลาวด์ในการแสดงความไว้วางใจดิจิทัล	Cloud Transparency Protocol	1. มีลักษณะการให้บริการแบบไม่ประสานเวลา 2. อาศัยคนควบคุมในกระบวนการ 3. ถูกประเมินหลังจากมีการเลือกใช้งานแล้ว

ตารางที่ 2.3 สรุปงานวิจัยด้านการประเมินความมั่นคงของผู้ให้บริการคลาวด์ (ต่อ)

ผู้วิจัย	ประเด็นในงานวิจัย	แนวคิดของงานวิจัย	ปัญหาของงานวิจัย
Wayne A. Pauley	การประเมินความโปร่งใสของผู้ให้บริการคลาวด์ด้านความมั่นคง ความเป็นส่วนตัว ความสามารถในการตรวจสอบได้ และข้อตกลงในการให้บริการ	บัตรคะแนน (Scorecard)	เป็นการประเมินจากปริมาณ แต่ไม่มีการพิจารณาคุณภาพของตัววัด
Burton S., Kaliski Jr., Wayne Pauley	1. ความท้าทายในการประเมินการให้บริการคลาวด์ 2. แนวคิดในการประเมินแบบทันทีทันใด	Risk Assessment as a Service	เป็นเพียงแนวคิด
Bret Michael, Sun Microsystems, Inc., Catherine Everett, David Tancock	การประเมินความโปร่งใสของการให้บริการคลาวด์	หลักการพิจารณาความโปร่งใส	เป็นเพียงแนวคิด

2.2.2 งานวิจัยที่เกี่ยวข้องกับการประเมินโดยใช้วิธีเป้าหมาย/คำถาม/ตัววัด หรือจีคิวเอ็ม

งานวิจัยที่เกี่ยวข้องกับการพิจารณาความมั่นคงและการตรวจสอบคุณสมบัติของผู้ให้บริการคลาวด์ ได้นำเสนอแนวคิดรวมถึงแนวทางปฏิบัติสำหรับการตรวจสอบด้านความมั่นคง รวมถึงคุณสมบัติด้านต่าง ๆ แล้ว แต่ยังขาดการกำหนดตัววัดที่ชัดเจน ซึ่งจะนำไปสู่การคำนวณคะแนนความมั่นคง ในงานวิจัยนี้ ได้นำวิธีจีคิวเอ็มมาวิเคราะห์หาตัววัดความมั่นคง เนื่องจากเป็นวิธีที่สอดคล้องกับลักษณะของเมตริกซ์ควบคุมคลาวด์และคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ที่มีเป้าหมายและคำถาม แต่ขาดตัววัด และได้แนวคิดจากงานวิจัยซึ่งเกี่ยวข้องกับการใช้วิธีจีคิวเอ็มในการกำหนดตัววัด ดังนี้

1) งานวิจัยของ Norazlina Khamis, Sufian Idris และ Rodina Ahmad [15]

ได้นำเสนอแบบจำลองในการประเมินผลการเขียนโปรแกรมเชิงวัตถุ โดยใช้วิธีจีคิวเอ็ม เนื่องจากเป็นวิธีที่ช่วยกำหนดตัววัด ซึ่งในงานวิจัยของ Khamis และคณะ มองเป็นระดับการวัดเชิงปริมาณ เพื่อช่วยในการประเมิน โดยแบ่งขั้นตอนของวิธีจีคิวเอ็มออกเป็น 3 ระดับ ได้แก่

- ระดับแนวความคิด (Conceptual Level) เปรียบเทียบได้กับวิธีจีคิวเอ็มในขั้นตอนการกำหนดเป้าหมาย โดยเป้าหมายจะกำหนดจากวัตถุประสงค์ของการเรียน เช่น ผู้เรียนเข้าใจหลักการของการโปรแกรมเชิงวัตถุ หรือ ผู้เรียนสามารถออกแบบ ดำเนินการ ทดสอบ แก้ปัญหาโปรแกรมอย่างง่ายที่เขียนด้วยภาษาเชิงวัตถุได้ หรือ ผู้เรียนต้องเข้าใจความเชื่อมโยงของวัตถุภายในโครงสร้างใด ๆ
- ระดับปฏิบัติการ (Operational Level) เปรียบเทียบได้กับวิธีจีคิวเอ็มในขั้นตอนการตั้งคำถาม โดยคำถามจะเกี่ยวข้องกับแนวความคิดที่กำหนด เช่น

ระดับแนวความคิด:ผู้เรียนต้องเข้าใจความเชื่อมโยงของวัตถุภายในโครงสร้างใดๆ
ระดับปฏิบัติการ : ผู้เรียนรู้วิธีสร้างการเชื่อมต่อระหว่างวัตถุหรือไม่
: ผู้เรียนเข้าใจการเชื่อมต่อระหว่างวัตถุหรือไม่

- ระดับการวัดเชิงปริมาณ (Quantitative Level) เปรียบเทียบได้กับวิธีจีคิวเอ็มในขั้นตอนการกำหนดตัววัด เช่น

ระดับแนวความคิด:ผู้เรียนต้องเข้าใจความเชื่อมโยงของวัตถุภายในโครงสร้างใดๆ

ระดับปฏิบัติการ : ผู้เรียนรู้วิธีสร้างการเชื่อมต่อระหว่างวัตถุ

: ผู้เรียนเข้าใจการเชื่อมต่อระหว่างวัตถุ

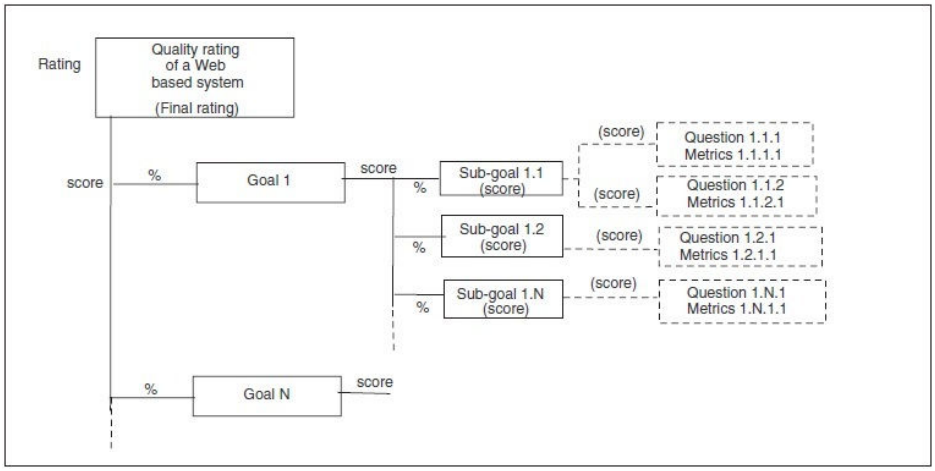
ระดับการวัดเชิงปริมาณ : จำนวนของวัตถุ

: ผลลัพธ์ของวัตถุที่มีความสัมพันธ์กัน

2) งานวิจัยของ Khaled M. Khan [16]

นำเสนอแม่แบบการประเมินความต้องการที่ไม่ใช่เชิงหน้าที่ของระบบที่ใช้เว็บ (Web-Based System) โดยใช้วิธีจีคิวเอ็ม แนวคิดคือ ทำตัวแปรที่มีผลต่อความต้องการที่ไม่ใช่เชิงหน้าที่ให้อยู่ในรูปแบบที่สามารถวัดได้ โดยความต้องการที่ไม่ใช่เชิงหน้าที่ทำการวัด คือคุณภาพของระบบที่ใช้เว็บ

งานวิจัยนี้ดำเนินการตามวิธีจีคิวเอ็ม คือ กำหนดเป้าหมาย ตั้งคำถาม และกำหนดตัววัด แต่สิ่งที่เป็นประเด็นสำคัญในงานวิจัย คือ การกำหนดเป้าหมายในเชิงคุณภาพ เนื่องจากคุณภาพของระบบที่ใช้เว็บเป็นสิ่งที่ขึ้นอยู่กับความพึงพอใจของผู้ใช้แต่ละบุคคล โดยเป้าหมายที่ถือว่าเป็นคุณภาพของบุคคลหนึ่ง อาจไม่ใช่สำหรับอีกบุคคลหนึ่ง ดังนั้นงานวิจัยนี้จึงแก้ปัญหาโดยการกำหนดเป้าหมายย่อย (Sub-goals) เพื่อให้เป้าหมายครอบคลุมนิยามของคุณภาพสำหรับบุคคลที่หลากหลาย โดยเป้าหมายย่อย จะถูกให้น้ำหนักแตกต่างกันแล้วแต่การให้ความสำคัญของเป้าหมายย่อยในแต่ละบุคคล และจะมีผลต่อการคำนวณคะแนนคุณภาพ นั่นคือจะไม่สนใจเฉพาะคะแนนจากตัววัดเท่านั้น แต่จะให้ความสำคัญกับน้ำหนักของเป้าหมายย่อยแต่ละเป้าหมายด้วย ดังภาพที่ 2.5 ซึ่งแสดงการกำหนดเป้าหมาย ตั้งคำถาม และกำหนดตัววัดของระบบที่ใช้เว็บ



ภาพที่ 2.5 การกำหนดเป้าหมาย ตั้งคำถาม และกำหนดตัววัดของระบบที่ใช้เว็บ [16]

แนวคิดของ Khan เป็นส่วนหนึ่งของการที่งานวิจัยนี้นำวิธีจีคิวเอ็มมาใช้ในการกำหนดตัววัดและแบ่งเป้าหมายออกเป็นเป้าหมายย่อย แต่จะแตกต่างตรงที่งานวิจัยนี้ไม่ได้กำหนดน้ำหนักตามเป้าหมายย่อย แต่กำหนดน้ำหนักให้กับตัววัดแทน นั่นคือ ในหนึ่งคำถามจะมีตัววัดได้มากกว่าหนึ่งตัววัด และเนื่องจากตัววัดเป็นการวัดในเชิงคุณภาพ น้ำหนักของตัววัดจึงแตกต่างกันไป

งานวิจัยด้านการประเมินโดยใช้วิธีเป้าหมาย/คำถาม/ตัววัด หรือจีคิวเอ็มสามารถสรุปได้ดังตารางที่ 2.4

ตารางที่ 2.4 สรุปงานวิจัยด้านการประเมินโดยใช้วิธีเป้าหมาย/คำถาม/ตัววัด หรือจีคิวเอ็ม

ผู้วิจัย	ประเด็นในงานวิจัย	แนวคิดของงานวิจัย	ปัญหาของงานวิจัย
Norazlina Khamis และคณะ	การประเมินความสามารถด้านการโปรแกรมเชิงวัตถุ	ประยุกต์วิธีจีคิวเอ็ม	เป็นการประเมินจากปริมาณแต่ไม่มีการพิจารณาคุณภาพของตัววัด
Khaled M. Khan	การประเมินคุณสมบัติที่ไม่ใช่เชิงหน้าที่ของระบบเว็บ	ประยุกต์วิธีจีคิวเอ็ม	เป็นการประเมินจากปริมาณแต่ไม่มีการพิจารณาคุณภาพของตัววัด

บทที่ 3
แนวคิดและวิธีดำเนินการวิจัย

แนวคิดของงานวิจัยนี้ ตั้งอยู่บนพื้นฐานของความคิดที่ว่า ทำอย่างไรผู้ใช้บริการคลาวด์จะสามารถประเมินผู้ให้บริการคลาวด์ในแง่ของความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคง เพื่อนำมาซึ่งการตัดสินใจเลือกใช้บริการ

ในธุรกิจการให้บริการ ความมั่นคงของผู้ให้บริการ เป็นปัจจัยสำคัญที่นำมาซึ่งความเชื่อถือได้ของผู้ให้บริการ เนื่องจากเป็นส่วนหนึ่งที่ถูกประเมินในขั้นตอนของการตรวจสอบ โดยกระบวนการในการตรวจสอบสามารถเกิดขึ้นได้ตลอดเวลาของการทำงาน ขึ้นอยู่กับเป้าหมายหรือสิ่งที่ต้องการทำการตรวจสอบว่าได้มาจากขั้นตอนใดของการทำงาน ในขั้นตอนการเลือกใช้บริการการตรวจสอบความมั่นคงเบื้องต้นของผู้ให้บริการมีผลต่อการตัดสินใจของผู้ใช้บริการ เช่นเดียวกับการเลือกผู้ให้บริการคลาวด์ ผู้ใช้บริการคลาวด์จำเป็นต้องตรวจสอบและประเมินความมั่นคงเบื้องต้นของผู้ให้บริการคลาวด์ก่อนตัดสินใจเลือกใช้บริการคลาวด์

งานวิจัยนี้ มีวัตถุประสงค์เพื่อนำเสนอระบบการให้คะแนนความมั่นคงของผู้ให้บริการคลาวด์ เพื่อให้ผู้ตรวจสอบความมั่นคงของคลาวด์ใช้ในการประเมินคะแนนความมั่นคงของผู้ให้บริการคลาวด์ และเพื่อให้ผู้ใช้บริการคลาวด์มีข้อมูลในการประกอบการตัดสินใจก่อนการเลือกใช้บริการคลาวด์ โดยความมั่นคงที่นำมาประเมินจะอ้างอิงจากเมตริกซ์ควบคุมคลาวด์และคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ที่นำเสนอโดยองค์กรความมั่นคงของคลาวด์

การให้คะแนนจะอาศัยวิธีเป้าหมาย/คำถาม/ตัววัด หรือจีคิวเอ็ม เพื่อให้ได้มาซึ่งตัววัดที่สามารถวัดเป็นปริมาณได้ โดยกระบวนการวิจัยในการให้คะแนนความมั่นคงของผู้ให้บริการคลาวด์ ประกอบด้วย 7 ขั้นตอน ได้แก่

1) ขั้นตอนการเลือกเป้าหมายของการประเมินความมั่นคงของผู้ให้บริการคลาวด์
2) ขั้นตอนการตั้งคำถามให้สอดคล้องกับเป้าหมาย
3) ขั้นตอนการกำหนดตัววัดความมั่นคงของผู้ให้บริการคลาวด์โดยวิธีจีคิวเอ็ม
4) ขั้นตอนการกำหนดวิธีการให้คะแนนความมั่นคงของผู้ให้บริการคลาวด์
5) ขั้นตอนการจัดลำดับผู้ให้บริการคลาวด์ตามคะแนนความมั่นคง
6) ขั้นตอนการพัฒนาเครื่องมือสนับสนุนงานวิจัย
7) ขั้นตอนการทดลองและประเมินผล

3.1 ขั้นตอนการเลือกเป้าหมายของการประเมินความมั่นคงของผู้ให้บริการคลาวด์

งานวิจัยนี้เลือกใช้เมตริกซ์ควบคุมคลาวด์ในการกำหนดเป้าหมาย ตัวอย่างดังตารางที่ 3.1

ตารางที่ 3.1 ตัวอย่างเป้าหมายที่ใช้ประเมิน

รหัสเป้าหมาย	รายละเอียดเป้าหมาย
CO-01	ผู้ให้บริการคลาวด์มีแผนการตรวจสอบ กิจกรรม การดำเนินการตรวจสอบการทำงานเพื่อป้องกันการหยุดชะงักของระบบ
IS-13	ผู้ให้บริการคลาวด์ต้องบันทึกหน้าที่และความรับผิดชอบของผู้รับจ้าง ลูกจ้าง และองค์กรภายนอกที่มีส่วนเกี่ยวข้องกับความมั่นคงของข้อมูล ในรูปแบบของเอกสาร
OP-02	ผู้ให้บริการคลาวด์ต้องมีเอกสารของระบบสารสนเทศ เช่น คู่มือผู้ใช้งานและผู้ดูแลระบบ โครงสร้างสถาปัตยกรรม เพื่อให้พนักงานผู้มีสิทธิ์ดำเนินการแน่ใจว่ามีกระบวนการออกแบบ การติดตั้ง การดำเนินการเกี่ยวกับระบบสารสนเทศมีการใช้ระบบรักษาความมั่นคงอย่างมีประสิทธิภาพ

3.2 ขั้นตอนการตั้งคำถามให้สอดคล้องกับเป้าหมายและการแปลงคำถาม

งานวิจัยตั้งคำถามโดยอ้างอิงจากคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ที่นำเสนอโดยซีเอสเอ [2] แต่ลักษณะของคำถามยังไม่สามารถนำมากำหนดตัววัดได้ เนื่องจากเป็นคำถามที่ต้องการคำตอบประเภท “ใช่” หรือ “ไม่ใช่” เท่านั้น ซึ่งไม่แสดงให้เห็นถึงหลักฐานที่ยืนยันว่าผู้ให้บริการคลาวด์ปฏิบัติตามคำถามนั้นจริง

จากประเด็นดังกล่าว ผู้วิจัยจึงแปลงคำถามโดยแบ่งตามมุมมองของผู้เกี่ยวข้อง ได้แก่ ผู้ให้บริการคลาวด์และผู้ตรวจสอบความมั่นคงของคลาวด์ ดังนี้

3.2.1 คำถามสำหรับผู้ให้บริการคลาวด์ เป็นคำถามที่ต้องการให้ผู้ให้บริการคลาวด์แสดงให้เห็นถึงหลักฐานที่สอดคล้องกับคำถาม เช่น อะไรคือหลักฐานที่แสดงให้เห็นว่าผู้ให้บริการคลาวด์มีการตรวจสอบภายในองค์กร

3.2.2 คำถามสำหรับผู้ตรวจสอบความมั่นคงของคลาวด์ เป็นคำถามที่ต้องการให้ผู้ตรวจสอบความมั่นคงของคลาวด์ระบุคุณภาพของหลักฐานที่ผู้ให้บริการคลาวด์แสดง เช่น อะไรคือคุณภาพของหลักฐานที่แสดงให้เห็นว่าผู้ให้บริการคลาวด์มีการ

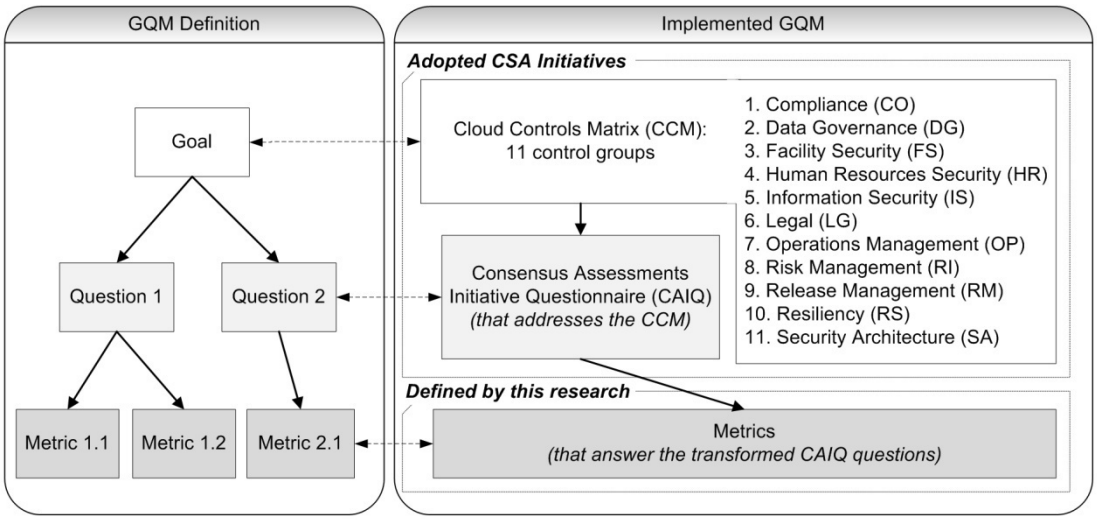
ตรวจสอบภายในองค์กร (งานวิจัยกำหนดนิยามคุณภาพของหลักฐานไว้ในหัวข้อ 3.4)

ตารางที่ 3.2 ตัวอย่างคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่และการแปลงคำถามตามมุมมองของผู้เกี่ยวข้อง

รหัสคำถาม	คำถามเดิม	คำถามที่ถูกแปลงสำหรับผู้ให้บริการคลาวด์ /คำถามที่ถูกแปลงสำหรับผู้ตรวจสอบความมั่นคงของคลาวด์
CO-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	What is the evidence that shows that you conduct internal audits regularly as prescribed by industry best practices and guidance? / What is the quality of the evidence that shows that the cloud provider conducts internal audits regularly as prescribed by industry best practices and guidance?

3.3 ขั้นตอนการกำหนดตัววัดความมั่นคงของผู้ให้บริการคลาวด์โดยวิธีจีคิวเอ็ม

วิธีจีคิวเอ็มถูกนำมาใช้เป็นแนวทางในการกำหนดตัววัดความมั่นคงของผู้ให้บริการคลาวด์ เนื่องจากวิธีจีคิวเอ็มประกอบด้วยการกำหนดเป้าหมาย (ระดับแนวความคิด) การตั้งคำถามที่สอดคล้องกับเป้าหมาย (ระดับการปฏิบัติการ) และการกำหนดตัววัดที่สอดคล้องกับคำถาม (ระดับการวัดปริมาณ) [4] ซึ่งสอดคล้องกับเมตริกซ์ควบคุมคลาวด์ที่มีการกำหนดเป้าหมายและคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ที่สอดคล้องกับเป้าหมาย แต่ยังขาดตัววัดที่สอดคล้องกับคำถามซึ่งนำไปสู่การประเมินเป้าหมาย งานวิจัยนี้จึงอาศัยแนวทางของวิธีจีคิวเอ็มในการเพิ่มขั้นตอนการกำหนดตัววัด เพื่อให้เป้าหมายแต่ละเป้าหมายสามารถวัดได้ ดังภาพที่ 3.1 ที่แสดงความสัมพันธ์ของเมตริกซ์ควบคุมคลาวด์และคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่กับวิธีจีคิวเอ็ม พร้อมทั้งแสดงขอบเขตของงานวิจัย ซึ่งนิยามเพิ่มเติมในส่วนของการกำหนดตัววัด



ภาพที่ 3.1 ความสัมพันธ์ของเมตริกซ์ควบคุมคลาวด์และคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่กับวิธีจีคิวเอ็ม

งานวิจัยได้กำหนดตัววัดในรูปแบบของจำนวนของหลักฐานที่สอดคล้องกับคำถามและเป้าหมาย โดยระบุหลักฐานจากการวิเคราะห์มาตรฐานที่เกี่ยวข้องกับเป้าหมาย ได้แก่ ISO 27001, ISACA, COBIT, PCI, NIST, Jericho Forum และ NERC CIP (รายละเอียดเพิ่มเติมระบุไว้ในหัวข้อ 2.1.2) โดยเนื้อหาแต่ละส่วนของมาตรฐานดังกล่าว จะสอดคล้องกับเป้าหมายแต่ละข้อแตกต่างกัน ตามที่กำหนดไว้ในเมตริกซ์ควบคุมคลาวด์ ดังตัวอย่างในตารางที่ 3.3

ตารางที่ 3.3 ตัวอย่างความสอดคล้องของมาตรฐาน ISO27001 กับเป้าหมาย CO-01 และ CO-03

รหัสเป้าหมาย	มาตรฐาน ISO 27001 ที่สอดคล้องกับเป้าหมาย	เนื้อหาของมาตรฐาน ISO 27001 ส่วนที่สอดคล้องกับเป้าหมาย
CO-01	Clause 4.2.3 e)	Monitor & Review the ISMS: e) Are internal ISMS audits at planned intervals conducted?
CO-03	A.10.6.2	Security of Network Services: Are security features, service levels and mgmt requirements of all network services identified and included in any network services agreement, whether these services are provided in-house or out-sourced?

การวิเคราะห์มาตรฐานที่เกี่ยวข้องกับเป้าหมาย ผู้วิจัยได้แบ่งลักษณะเนื้อหาของมาตรฐานเพื่อระบุหลักฐานออกเป็น 3 ประเภท ได้แก่

1) Activity หรือเนื้อหาประเภทกิจกรรม เช่น การตรวจสอบ การจัดการ ซึ่งเนื้อหาประเภทนี้ ไม่สามารถระบุหลักฐานได้
2) Productivity หรือเนื้อหาประเภทก่อให้เกิดผลผลิต เช่น กระบวนการจัดทำเอกสาร ซึ่งเนื้อหาประเภทนี้ สามารถระบุหลักฐานได้จากผลลัพธ์ของกระบวนการ
3) Both หรือเนื้อหาที่เป็นกิจกรรมและก่อให้เกิดผลผลิตด้วย เช่น การตรวจสอบและจัดทำเอกสาร ซึ่งเนื้อหาประเภทนี้ สามารถระบุหลักฐานได้จากผลลัพธ์ของกิจกรรม

กรณีตัวอย่างของการวิเคราะห์มาตรฐาน ISO 27001 ที่เกี่ยวข้องกับเป้าหมาย CO-01 เป็นไปดังตารางที่ 3.4 โดยเนื้อหาส่วน Clause 4.2.3 e), Clause 4.2.3 b) และ Clause 6 ของมาตรฐาน ISO 27001 มีความสอดคล้องกับเป้าหมายดังกล่าว และเมื่อแบ่งลักษณะเนื้อหาและวิเคราะห์เนื้อหาแล้วพบว่า เนื้อหาของมาตรฐาน ISO 27001 ที่สอดคล้องกับเป้าหมาย CO-01 แบ่งเป็น 3 ประเภท คือ Clause 4.2.3 e) เป็นเนื้อหาประเภทกิจกรรม Clause 4.2.3 b) เป็นเนื้อหาประเภทก่อให้เกิดผลผลิต และ Clause 6 เป็นเนื้อหาประเภทที่เป็นกิจกรรมและก่อให้เกิดผลผลิต ดังนั้น เป้าหมาย CO-01 จึงมีหลักฐานที่สอดคล้องกับเป้าหมาย 2 อย่าง คือ Information Security Management System (ISMS) Policy และ Internal audit reports ซึ่งมาจากเนื้อหาประเภทก่อให้เกิดผลผลิตและเนื้อหาประเภทที่เป็นกิจกรรมและก่อให้เกิดผลผลิตตามลำดับ

ตารางที่ 3.4 ตัวอย่างของหลักฐานที่ระบุได้จากเนื้อหาประเภท Activity, Productivity และ Both

ส่วนของมาตรฐาน ISO 27001	เนื้อหา	ประเภทของเนื้อหา	หลักฐาน
Clause 4.2.3 e)	Monitor & Review the ISMS: e) Are internal ISMS audits at planned intervals conducted?	Activity	ไม่ระบุ
Clause 4.2.3 b)	Monitor & Review the ISMS: b) Are regular reviews of the effectiveness of the ISMS (including meeting of ISMS policy and objectives and review of security controls) undertaken? • Are the results of security audits, incidents, and results from effectiveness measurements, suggestions and feedback from interested parties taken into account?	Productivity	Information Security Management System (ISMS) Policy

ตารางที่ 3.4 ตัวอย่างของหลักฐานที่ระบุได้จากเนื้อหาประเภท Activity, Productivity และ Both (ต่อ)

ส่วนของมาตรฐาน ISO 27001	เนื้อหา	ประเภทของเนื้อหา	หลักฐาน
Clause 6	Internal ISMS Audits: Does the organization conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of the ISMS: a) Conform to the requirements of this standard and relevant legislation or regulations? …	Both	Internal audit reports

เนื่องจากหลักฐานที่ได้ เป็นหลักฐานที่สอดคล้องในระดับของเป้าหมาย ผู้วิจัยจึงจัดกลุ่มหลักฐานตามความสอดคล้องกับคำถามอีกครั้งหนึ่ง เพื่อให้ได้เป็นหลักฐานที่สอดคล้องกับคำถาม ซึ่งทำให้คำถามบางกลุ่มมีหลักฐานที่ซ้ำกัน แต่ต่างกันตรงเนื้อหาภายในหลักฐานที่แสดงถึงความสอดคล้องกับคำถามแต่ละข้อ ดังตัวอย่างในตารางที่ 3.5 ที่แสดงให้เห็นถึงหลักฐานที่ถูกจัดกลุ่มตามความสอดคล้องกับคำถามและเป้าหมายทั้ง 11 ด้าน นอกจากนี้ หลักฐานบางข้อซึ่งเวลามีนัยสำคัญ เช่น เอกสารการตรวจสอบที่ต้องปรับปรุงให้ทันสมัยทุก 1 ปี จะถูกทำเครื่องหมาย [*T] เพื่อให้ผู้ให้บริการคลาวด์ตระหนักถึงความสำคัญของการปรับปรุงหลักฐาน และเพื่อให้ผู้ตรวจสอบความมั่นคงของคลาวด์ ใช้เพื่อพิจารณาคะแนนความสมบูรณ์ของหลักฐาน

ตารางที่ 3.5 ตัวอย่างเป้าหมาย คำถาม และหลักฐานที่ถูกจัดกลุ่มตามความสอดคล้องกับคำถามและเป้าหมาย

Goal Category	Goal Code: Goal Description	Question Code: Question Description	Evidence Code: Evidence Description
CO	CO-01: Audit Planning	CO-01.1: What is the quality of the evidence that shows that the cloud provider produces audit assertions, using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	CO-01.1.1: Information Security Management System (ISMS) Policy [20] that follows structured, industry accepted format.
DG	DG-01: Ownership / Stewardship	DG-01.1: What is the quality of the evidence that shows that the cloud provider follows a structured data-labeling standard (ex. ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	DG-01.1.1: Information labeling and handling policy and procedures [20] that follow a structured data-labeling standard (ex. ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)

ตารางที่ 3.5 ตัวอย่างเป้าหมาย คำถาม และหลักฐานที่ถูกจัดกลุ่มตามความสอดคล้องกับคำถามและเป้าหมาย (ต่อ)

Goal Category	Goal Code: Goal Description	Question Code: Question Description	Evidence Code: Evidence Description
FS	FS-01: Policy	FS-01.1: What is the quality of the evidence that shows that the cloud provider establishes policies and procedures for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	FS-01.1.1: Physical and environmental protection policy and procedures [5]
HR	HR-02: Employment Agreements	HR-02.1: What is the quality of the evidence that shows that the cloud provider specifically trains employees regarding their role vs. the tenant's role in providing information security controls?	HR-02.1.1: Human resource security policy and procedures [20] that specify employee training policy
IS	IS-05: Policy Reviews	IS-05.1: What is the quality of the evidence that shows that the cloud provider notifies their tenants when material changes are made to information security and/or privacy policies?	IS-05.1.1: [*T] Information security and privacy policies and procedures or ISMS policy [20] that are distributed or published when making change.

ตารางที่ 3.5 ตัวอย่างเป้าหมาย คำถาม และหลักฐานที่ถูกจัดกลุ่มตามความสอดคล้องกับคำถามและเป้าหมาย (ต่อ)

Goal Category	Goal Code: Goal Description	Question Code: Question Description	Evidence Code: Evidence Description
LG	LG-01: Nondisclosure Agreements	LG-01.1: What is the quality of the evidence that shows that the cloud provider's requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details are identified, documented and reviewed at planned intervals?	LG-01.1.1: [*T] Confidentiality agreement or non-disclosure agreement that identify the organization's needs for the protection of data and operational details
OP	OP-04: Equipment Maintenance	OP-04.2: If using virtual infrastructure, what is the quality of the evidence which shows that the cloud provider provides tenants with a capability to restore a Virtual Machine to a previous state in time?	OP-04.2.1: System maintenance policy and procedures [5] that allow a tenant to restore a Virtual Machine to a previous state in time
RI	RI-05: Third Party Access	RI-05.5: What is the quality of the evidence that shows that the cloud provider provides the tenant the ability to declare a disaster?	RI-05.1.1: Disaster recovery and contingency plan and procedures [5]

ตารางที่ 3.5 ตัวอย่างเป้าหมาย คำถาม และหลักฐานที่ถูกจัดกลุ่มตามความสอดคล้องกับคำถามและเป้าหมาย (ต่อ)

Goal Category	Goal Code: Goal Description	Question Code: Question Description	Evidence Code: Evidence Description
RM	RM-04: Outsourced Development	RM-04.1: What is the quality of the evidence that shows that the cloud provider has controls in place to ensure that standards of quality are being met for all software development?	RM-04.1.1: Trustworthiness information system policy and procedures [5]
RS	RS-08: Power / Telecommunications	RS-08.1: What is the quality of the evidence which shows that the cloud provider provides tenants with documentation showing the transport route of their data between their systems?	RS-08.1.1: Physical and environmental protection policy and procedures that identify the transport route of data between systems [5]
SA	SA-15: Mobile Code	SA-15.2: What is the quality of the evidence which shows that the cloud provider prevents all unauthorized mobile code from executing?	SA-15.2.1: System and communications protection policy and procedures [5] that identify mobile code usage restriction and guidance

3.4 ขั้นตอนการกำหนดวิธีการให้คะแนนความมั่นคงของผู้ให้บริการคลาวด์

วิธีการให้คะแนนความมั่นคงของผู้ให้บริการคลาวด์ จะให้คะแนนโดยวิธีการหาผลรวมค่าเฉลี่ยของน้ำหนัก โดยการให้น้ำหนักจะพิจารณาจากคุณภาพของหลักฐานที่อ้างอิงถึง ได้แก่

3.4.1 การแสดงการปฏิบัติตามเป้าหมายของหลักฐานที่อ้างอิงถึง (Quality of Compliance) โดยเทียบหลักฐานที่อ้างอิงถึงกับความสอดคล้องกับตัววัด โดยแบ่งระดับการปฏิบัติตามเป้าหมายออกเป็น 3 ระดับ และมีเกณฑ์การให้น้ำหนักดังตารางที่ 3.6

ตารางที่ 3.6 น้ำหนักของคุณภาพการแสดงการปฏิบัติตามเป้าหมายของหลักฐานที่อ้างอิงถึง

การแสดงการปฏิบัติตามเป้าหมายของหลักฐานที่อ้างอิงถึง	เปอร์เซ็นต์การปฏิบัติตามเป้าหมาย	น้ำหนัก
หลักฐานที่อ้างอิงถึงแสดงถึงการปฏิบัติตามเป้าหมายอย่างเต็มที่ (Full Compliance)	100%	1
หลักฐานที่อ้างอิงถึงแสดงถึงการปฏิบัติตามเป้าหมายเพียงบางส่วน (Partial Compliance)	50%	0.5
ไม่มีหลักฐานที่อ้างอิงถึงหรือหลักฐานที่อ้างอิงถึงไม่แสดงถึงการปฏิบัติตามเป้าหมาย (Non-compliance)	0%	0

ผู้ตรวจสอบความมั่นคงของคลาวด์สามารถกำหนดน้ำหนักของคุณภาพด้านการแสดงการปฏิบัติตามเป้าหมายได้เอง โดยน้ำหนักที่มีค่ามากที่สุดต้องเป็น 1 หรือใช้โครงร่างการกำหนดน้ำหนักในงานวิจัยนี้ ดังตารางที่ 3.6 ข้างต้น ตัวอย่างการกำหนดน้ำหนักเป็นดังตารางที่ 3.7

ตารางที่ 3.7 การปฏิบัติตามเป้าหมายของหลักฐานที่อ้างอิงถึงโดยเทียบหลักฐานที่อ้างอิงถึงกับความสอดคล้องกับตัววัด

Question Code: Question Description	Evidence Code: Evidence Description	Evidence of Cloud Provider	Compliance Level
CO-01.1 What is the quality of the evidence that shows that the cloud provider produces audit assertions, using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	CO-01.1.1 Information Security Management System (ISMS) Policy [20] that follows structured, industry accepted format.	-	None
	CO-01.1.2 Audit requirements [20] that focus on data duplication, access, and data boundary limitations, and use a structured, industry accepted format.	Audit requirements that identify data duplication management.	Partial

3.4.2 ความสมบูรณ์ของหลักฐานที่อ้างอิงถึง (Quality of Completeness) จะพิจารณาบนพื้นฐานของการมองการดำเนินการต่าง ๆ เพื่อปฏิบัติตามตัววัดว่าเปรียบเสมือนการจัดการโครงการ (Project Management) ซึ่งประกอบด้วยกระบวนการดำเนินงานหลายขั้นตอน กระบวนการแต่ละขั้นตอนจะมีผลผลิตต่าง ๆ ออกมา ดังนั้นหลักฐานที่อ้างอิงซึ่งเป็นผลผลิตของการดำเนินโครงการจึงมี

ระดับความสมบูรณ์แตกต่างกันได้ ขึ้นกับว่าหลักฐานนั้นอยู่ในขั้นตอนใดของการจัดการโครงการเมื่อเทียบเทียบกับการปฏิบัติตามตัววัด เกณฑ์การให้น้ำหนักความสมบูรณ์ของหลักฐานเป็นดังตารางที่ 3.8

ตารางที่ 3.8 น้ำหนักของคุณภาพด้านความสมบูรณ์ของหลักฐานที่อ้างอิงถึง

ความสมบูรณ์ของหลักฐานที่อ้างอิงถึง [18]	เปอร์เซ็นต์ความสมบูรณ์ของหลักฐานที่อ้างอิงถึง	น้ำหนัก
ไม่มีหลักฐานที่อ้างอิงถึง	0%	0
มีหลักฐานที่อ้างอิงถึง และหลักฐานที่อ้างอิงถึงอยู่ในขั้นตอนการเริ่มต้น (Initial Process)	10%	0.1
มีหลักฐานที่อ้างอิงถึง และหลักฐานที่อ้างอิงถึงอยู่ในขั้นตอนการวางแผน (Planning Process)	30%	0.3
มีหลักฐานที่อ้างอิงถึง และหลักฐานที่อ้างอิงถึงอยู่ในขั้นตอนการดำเนินการ (Executing Process)	50%	0.5
มีหลักฐานที่อ้างอิงถึง และหลักฐานที่อ้างอิงถึงอยู่ในขั้นตอนการติดตามและควบคุม (Monitoring and Controlling Process)	80%	0.8
มีหลักฐานที่อ้างอิงถึง และหลักฐานที่อ้างอิงถึงอยู่ในขั้นตอนการปิดการดำเนินการ (Closing Process)	100%	1

ผู้ใช้บริการคลาวด์สามารถกำหนดน้ำหนักความสมบูรณ์ได้เอง โดยน้ำหนักที่มีค่ามากที่สุดต้องเป็น 1 หรือใช้โครงร่างการกำหนดน้ำหนักในงานวิจัยนี้ ดังตารางที่ 3.8 ข้างต้น ตัวอย่างความสมบูรณ์ของหลักฐานที่อ้างอิงถึงเทียบกับตัววัดเป็นดังตารางที่ 3.9

ตารางที่ 3.9 ความสมบูรณ์ของหลักฐานที่อ้างอิงถึงเทียบกับตัววัด

Question Code: Question Description	Evidence Code: Evidence Description	Evidence of Cloud Provider	Compliance Level
CO-01.1 What is the quality of the evidence that shows that the cloud provider produces audit assertions, using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	CO-01.1.1 Information Security Management System (ISMS) Policy [20] that follows structured, industry accepted format.	-	None
	CO-01.1.2 Audit requirements [20] that focus on data duplication, access, and data boundary limitations, and use a structured, industry accepted format.	Audit requirements that identify data duplication management.	Closing

การคำนวณคะแนนความมั่นคงตามวิธีจีคิวเอ็มจะคำนวณได้จากสมการต่อไปนี้

คะแนนความมั่นคง (Security Score: S_s) คำนวณได้จาก (1)

$$S_S = \frac{\sum_{i=1}^{k} S_{g_i}}{k} \quad (1)$$

โดยที่ S_s คือ คะแนนความมั่นคงเป็นเปอร์เซ็นต์ (%)

S_g คือ คะแนนของเป้าหมายหลัก i ใด ๆ ซึ่งคำนวณได้จากสมการ (2)

k คือ จำนวนเป้าหมายหลักทั้งหมด

คะแนนของเป้าหมายหลัก (Goal Score: S_g) คำนวณได้จาก (2)

$$S_g = \frac{(\sum_{i=1}^{m} ActualS_{sg_i})*100}{\sum_{i=1}^{m} TotalS_{sg_i}} \quad (2)$$

โดยที่ S_g คือ คะแนนของเป้าหมายหลักเป็นเปอร์เซ็นต์ (%)

$ActualS_{sgi}$ คือ คะแนนที่ได้จริงของเป้าหมายย่อย sg_i ใด ๆ ซึ่งคำนวณได้จากสมการ (3)

$TotalS_{sgi}$ คือ คะแนนรวมสูงสุดของเป้าหมายย่อย sg_i ใด ๆ ซึ่งคำนวณได้จากสมการ (3)

m คือ จำนวนเป้าหมายย่อยทั้งหมดของเป้าหมายหลัก

คะแนนของเป้าหมายย่อย (Sub-goal Score: S_{sg}) คำนวณได้จาก (3)

$$S_{sg} = \frac{(\sum_{i=1}^{n} ActualS_{q_i})*100}{\sum_{i=1}^{n} TotalS_{q_i}} \quad (3)$$

โดยที่ S_{sg} คือ คะแนนของเป้าหมายย่อยเป็นเปอร์เซ็นต์ (%)

$ActualS_{qi}$ คือ คะแนนที่ได้จริงของคำถาม q_i ใด ๆ ซึ่งคำนวณได้จากสมการ (4)

$TotalS_{qi}$ คือ คะแนนรวมสูงสุดของคำถาม q_i ใด ๆ ซึ่งคำนวณได้จากสมการ (4)

n คือ จำนวนคำถามทั้งหมดของเป้าหมายย่อย

คะแนนของคำถาม (Score of Question: S_q) คำนวณได้จาก (4)

$$S_q = \frac{(\sum_{i=1}^{p} ActualS_{m_i})*100}{\sum_{i=1}^{p} TotalS_{m_i}} \quad (4)$$

โดยที่ S_q คือ คะแนนของคำถามเป็นเปอร์เซ็นต์ (%)

$ActualS_{mi}$ คือ คะแนนที่ได้จริงของตัววัด m_i ใด ๆ ซึ่งคำนวณได้จากสมการ (5)

$TotalS_{mi}$ คือ คะแนนรวมสูงสุดของตัววัด m_i ใด ๆ ซึ่งคำนวณได้จากสมการ (5)

p คือ จำนวนตัววัดทั้งหมดของคำถาม

คะแนนของตัววัด (Metric Score: S_m) คำนวณได้จาก (5)

$$S_m = \frac{(\sum_{i=1}^{r}\left(S_{e_i} * W_{qcpl_i}\right) + \sum_{i=1}^{r}\left(S_{e_i} * W_{qcpt_i}\right)) * 100}{(max(W_{qcpl}) + max(W_{qcpt})) * r} \quad (5)$$

โดยที่ S_m คือ คะแนนของตัววัดเป็นเปอร์เซ็นต์ (%)

s_e คือ คะแนนการมีอยู่ของหลักฐาน e_i ใดๆ ซึ่งมีค่าตามนิยามที่ (6)

w_{qcpl} คือ น้ำหนักของคุณภาพด้านการแสดงการปฏิบัติตามเป้าหมายจากหลักฐานที่อ้างอิงถึง e_i ใด ๆ ตามตารางที่ 3.6

w_{qcpt} คือ น้ำหนักของคุณภาพด้านความสมบูรณ์ของหลักฐานที่อ้างอิงถึง e_i ใด ๆ ตามตารางที่ 3.8

$max(w_{qcpl})$ คือ น้ำหนักที่มากที่สุดของคุณภาพด้านการแสดงการปฏิบัติตามเป้าหมายจากหลักฐานที่อ้างอิงถึงคือ 1

$max(w_{qcpt})$ คือ น้ำหนักที่มากที่สุดของคุณภาพด้านความสมบูรณ์ของหลักฐานที่อ้างอิงถึงคือ 1

r คือ จำนวนหลักฐานทั้งหมดของตัววัด

นิยามคะแนนของหลักฐาน (Evidence Score: s_e) (6)

$s_e = 1$ เมื่อมีหลักฐานที่อ้างอิงถึง

$s_e = 0$ เมื่อไม่มีหลักฐานที่อ้างอิงถึง

ตัวอย่างการคำนวณคะแนนของเป้าหมายหลัก สำหรับข้อมูลในตารางที่ 3.7 และตารางที่ 3.9 เมื่อแปลงเป็นค่าน้ำหนักตามเกณฑ์ที่กำหนดไว้ในตารางที่ 3.6 และ 3.8 ผลที่ได้แสดงดังตารางที่ 3.10

ตารางที่ 3.10 น้ำหนักระดับคุณภาพของหลักฐานที่อ้างอิงถึง

ประเภทเป้าหมาย	ตัววัด	หลักฐานที่อ้างอิงถึง	คะแนนการมีอยู่ของหลักฐานที่อ้างอิงถึง	ระดับการปฏิบัติตามเป้าหมาย	น้ำหนัก	ความสมบูรณ์ของหลักฐานที่อ้างอิงถึง	น้ำหนัก
CO	CO-01.1.1: Information Security Management System (ISMS) Policy [20] that follows structured, industry accepted format.	-	0	-	0	-	0
	CO-01.1.2: Audit requirements [20] that focus on data duplication, access, and data boundary limitations, and use a structured, industry accepted format.	Audit requirements that identify data duplication management.	1	Partial	0.5	Closing	1

จาก (5) จะได้ว่า

คะแนนของตัววัด CO-01.1.1 = 0%

คะแนนของตัววัด CO-01.1.2 = [(1*0.5 + 1*1) *100] / (1+1)*1

= 75%

จาก (4) จะได้ว่า

คะแนนของคำถาม CO-01.1 = (0+75) *100 / 200

= 37.5%

จาก (3) จะได้ว่า

คะแนนของเป้าหมายย่อย CO-01= (37.5*100) / 100

= 37.5%

จาก (2) จะได้ว่า

คะแนนของเป้าหมายหลัก CO = (37.5*100) / 100

= 37.5%

สมมติให้เป้าหมายหลักที่ใช้พิจารณาความมั่นคงมีเพียง 3 เป้าหมายหลัก คือ CO, IS และ OP และกำหนดให้คะแนนของเป้าหมายหลัก IS และ OP เป็น 30% และ 70% ตามลำดับ เมื่อใช้การคำนวณลักษณะเดียวกับตัวอย่างของเป้าหมายหลัก CO ข้างต้น

จาก (1) จะได้ว่า

คะแนนความมั่นคง = (37.5+30+70)/3

= 45.83%

3.5 ขั้นตอนการจัดลำดับผู้ให้บริการคลาวด์ตามคะแนนความมั่นคง

งานวิจัยจะพิจารณาการจัดลำดับผู้ให้บริการคลาวด์โดยดูจากคะแนนความมั่นคงเป็นเปอร์เซ็นต์ โดยผู้ให้บริการคลาวด์ที่มีคะแนนความมั่นคงมากกว่า จะถือว่ามีการปฏิบัติตามความต้องการด้านความมั่นคงของซีเอสเอมากกว่า

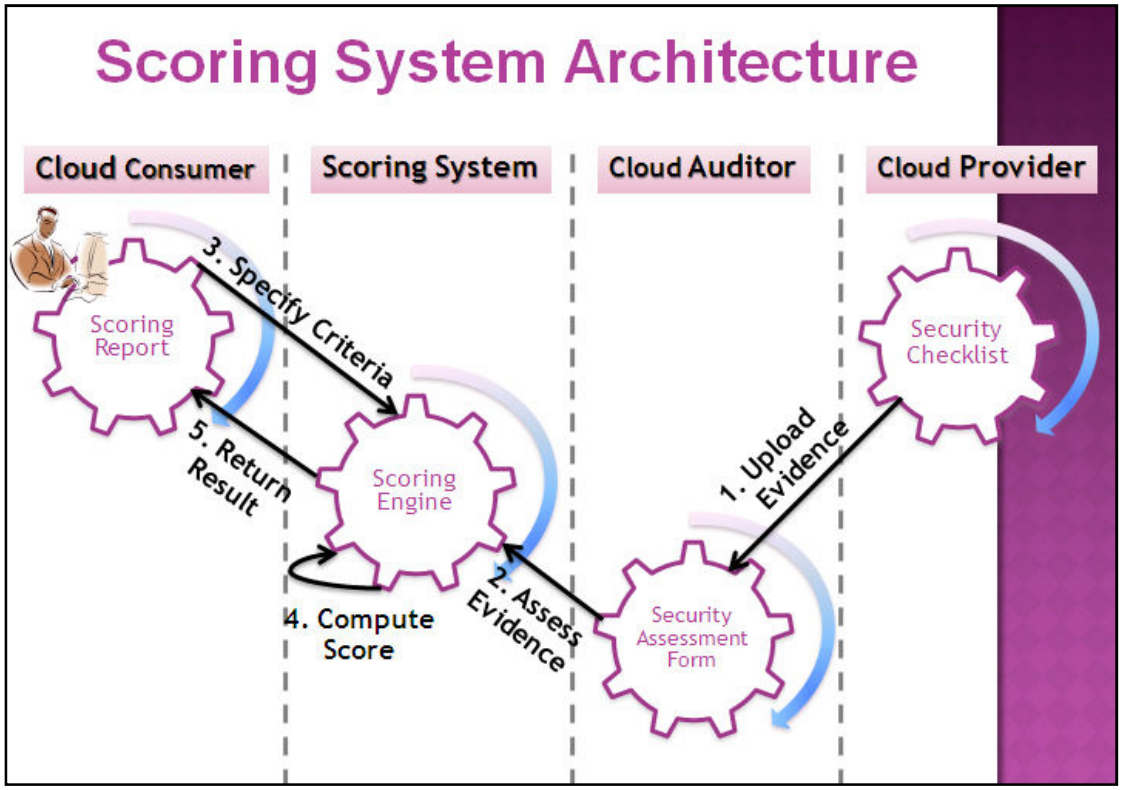
อย่างไรก็ตาม ยังมีปัจจัยนอกเหนือจากคะแนนความมั่นคงที่ได้นี้ เช่น ลักษณะการให้บริการคลาวด์ ขนาดของผู้ให้บริการคลาวด์ หรือประสบการณ์การให้บริการคลาวด์ ที่อาจมีผลต่อการพิจารณาเลือกผู้ให้บริการคลาวด์ แต่ปัจจัยเหล่านี้จะไม่กล่าวถึงในงานวิจัย

3.6 ขั้นตอนการพัฒนาเครื่องมือสนับสนุนงานวิจัย

แนวคิดในการพัฒนาเครื่องมือสนับสนุนงานวิจัย คือการนำเว็บแอพพลิเคชันมาใช้ในการรับข้อมูล ประมวลผลคะแนนความมั่นคงของผู้ให้บริการคลาวด์ และแสดงคะแนนความมั่นคงของผู้ให้บริการคลาวด์ โดยจุดเด่นของเว็บแอพพลิเคชัน คือ ผู้ใช้สามารถเข้าใช้งานได้ตลอดเวลาผ่านเว็บเบราว์เซอร์ ดังนั้นผู้ให้บริการคลาวด์จึงสามารถให้หลักฐานที่มีความสมบูรณ์หรือทันสมัยได้ตลอดเวลา

3.6.1 การออกแบบเว็บแอพพลิเคชัน

งานวิจัยได้ออกแบบโครงสร้างของเว็บแอพพลิเคชันตามการใช้งานของผู้ใช้ที่มีบทบาทแตกต่างกัน ดังภาพที่ 3.2

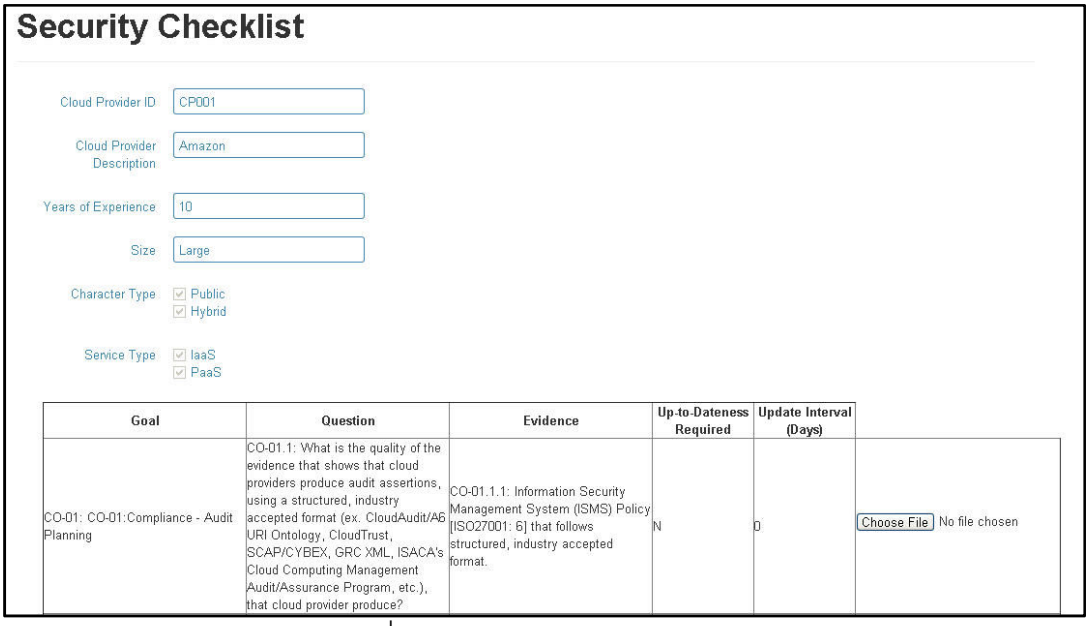


ภาพที่ 3.2 โครงสร้างของเว็บแอพพลิเคชันสำหรับประเมินคะแนนความมั่นคง

จากโครงสร้างของเว็บแอพพลิเคชันดังภาพที่ 3.2 งานวิจัย ได้แบ่งกลุ่มผู้ใช้งานออกเป็น 3 กลุ่ม ได้แก่

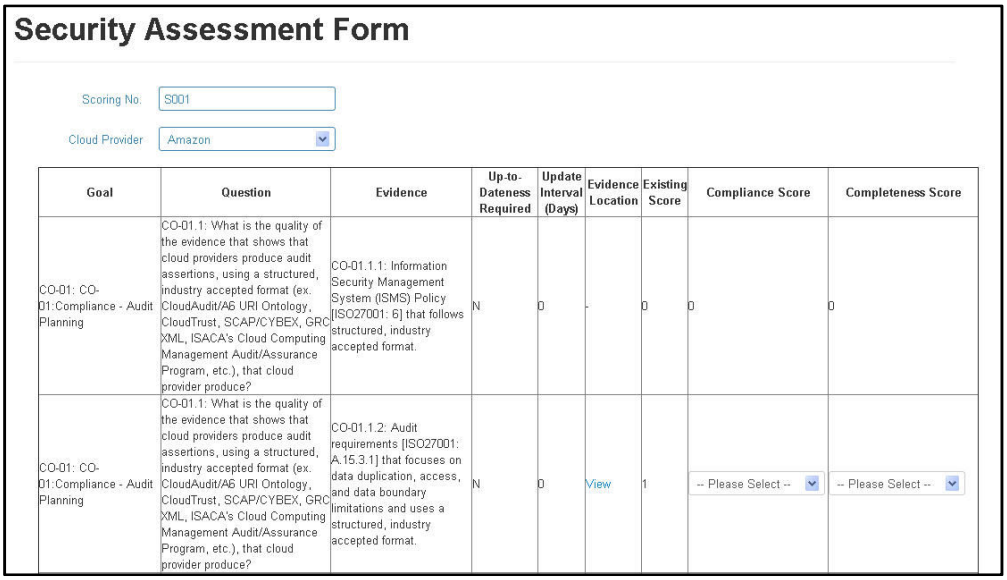
1) Cloud Provider ทำหน้าที่ให้หลักฐานที่สอดคล้องกับคำถาม (จากภาพที่ 3.2 คือ ขั้นตอนที่ 1. Upload Evidence) ผ่านหน้าจอ Security Checklist ในภาพที่ 3.3 โดยระบบจะทำการจัดเก็บข้อมูลประสบการณ์การให้บริการคลาวด์ (จำนวนปี) ขนาดของ

ผู้ให้บริการคลาวด์ (เล็ก กลาง ใหญ่) ลักษณะการให้บริการคลาวด์ และลักษณะการใช้งานคลาวด์ โดยลักษณะการให้บริการคลาวด์และลักษณะการใช้งานคลาวด์ จะถูกนำมาเป็นปัจจัยในการเปรียบเทียบคะแนนความมั่นคงกับผู้ให้บริการคลาวด์ที่มีลักษณะการให้บริการคลาวด์และลักษณะการใช้งานคลาวด์ประเภทเดียวกัน และในตารางสำหรับให้หลักฐาน ระบบจะแสดงค่า Y หรือ N ที่คอลัมน์ Up-to-Dateness Required เพื่อแสดงให้เห็นว่าหลักฐานนั้นต้องการความทันสมัยอยู่เสมอ โดยผู้ให้บริการคลาวด์ควรจะปรับปรุงหลักฐานครั้งล่าสุดไม่เกินจำนวนวันที่กำหนดไว้ในคอลัมน์ Update Interval



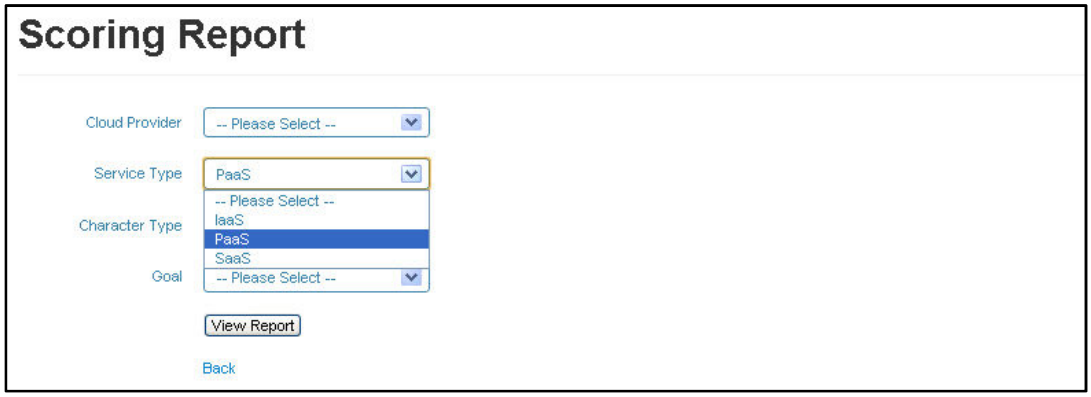
ภาพที่ 3.3 หน้าจอ Security Checklist

2) Cloud Auditor ทำหน้าที่ประเมินหลักฐานของผู้ให้บริการคลาวด์ โดยให้คะแนนการปฏิบัติตามเป้าหมายและความสมบูรณ์ของหลักฐาน (จากภาพที่ 3.2 คือ ขั้นตอนที่ 2. Assess Evidence) ผ่านหน้าจอ Security Assessment Form ในภาพที่ 3.4 ซึ่งผู้ประเมินสามารถกดปุ่ม View ที่คอลัมน์ Evidence Location เพื่อดูหลักฐานของผู้ให้บริการคลาวด์ ให้คะแนนการปฏิบัติตามเป้าหมายของหลักฐานที่คอลัมน์ Compliance Score และให้คะแนนความสมบูรณ์ของหลักฐานที่คอลัมน์ Completeness Score หากคำถามข้อใดที่ผู้ให้บริการคลาวด์ไม่ได้ให้หลักฐานไว้ ระบบจะให้ค่า Existing Score, Compliance Score และ Completeness Score เป็น 0

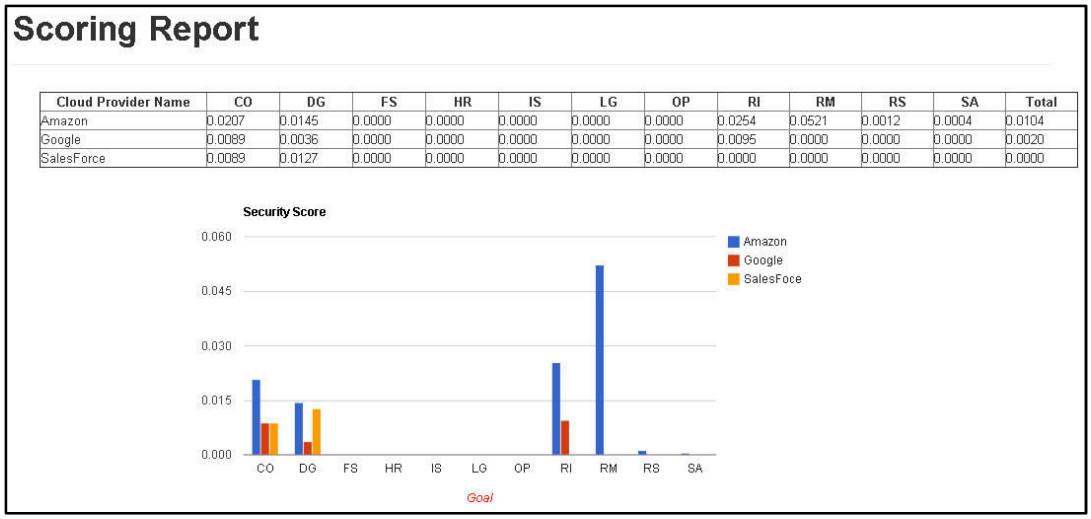


ภาพที่ 3.4 หน้าจอ Security Assessment Form

3) Cloud Consumer สามารถดูคะแนนความมั่นคงของผู้ให้บริการคลาวด์ โดยเลือกดูตามผู้ให้บริการคลาวด์ที่สนใจ ลักษณะการให้บริการคลาวด์ ลักษณะการใช้งานคลาวด์ หรือประเภทของเป้าหมายด้านความมั่นคงที่สนใจผ่านหน้าจอ Scoring Report ส่วนเลือก Criteria ดังภาพที่ 3.5 (จากภาพที่ 3.2 คือ ขั้นตอนที่ 3. Specify Criteria) โดยระบบจะประมวลผลคะแนนความมั่นคงของผู้ให้บริการคลาวด์ตามตัวเลือกและแสดงผล (จากภาพที่ 3.2 คือ ขั้นตอนที่ 4. Compute Score และขั้นตอนที่ 5. Return Result) ผ่านหน้าจอ Scoring Report ในภาพที่ 3.6 หากมีผู้ให้บริการคลาวด์มากกว่า 1 ราย ผู้ใช้บริการคลาวด์สามารถเปรียบเทียบคะแนนความมั่นคงของผู้ให้บริการคลาวด์ได้จากตารางแสดงคะแนนความมั่นคง ซึ่งจะแสดงคะแนนของเป้าหมายทั้ง 11 ประเภท และคะแนนความมั่นคงของผู้ให้บริการคลาวด์



ภาพที่ 3.5 หน้าจอ Scoring Report ส่วนเลือก Criteria ในการแสดงผล



ภาพที่ 3.6 หน้าจอ Scoring Report ส่วนแสดงผล

3.6.2 เครื่องมือที่ใช้ในการพัฒนา

จาวาเวอร์ชัน 1.6.2 เป็นภาษาในการพัฒนาแอพพลิเคชัน

Google Chart เป็นเครื่องมือสร้างกราฟ

MySQL เป็นฐานข้อมูล

Tomcat เวอร์ชัน 7.0.37 เป็นแอพพลิเคชันเซิร์ฟเวอร์

3.7 ขั้นตอนการทดลองและประเมินผล

การทดลองจะเป็นการรวบรวมข้อมูลจากผู้ให้บริการคลาวด์ 3 ราย โดยจำลองข้อมูลที่ใช้ในการคำนวณมาจากเว็บไซต์ของผู้ให้บริการคลาวด์ และข้อมูลดังกล่าวจะถูกนำมาประมวลผลคะแนนความมั่นคงโดยใช้ระบบที่พัฒนาขึ้นโดยมีวิธีการประเมินผล ดังนี้

1) ทดสอบการประเมินคะแนนความมั่นคงของผู้ให้บริการคลาวด์แต่ละราย
2) ทดสอบการจัดลำดับความมั่นคงของผู้ให้บริการคลาวด์แต่ละรายโดยไม่ระบุตัวแปรใดเลย
3) ทดสอบการจัดลำดับความมั่นคงของผู้ให้บริการคลาวด์ที่มีลักษณะการให้บริการคลาวด์ประเภทเดียวกัน โดยระบุลักษณะการให้บริการคลาวด์
4) ทดสอบการจัดลำดับความมั่นคงของผู้ให้บริการคลาวด์ที่มีลักษณะการใช้งานคลาวด์ประเภทเดียวกัน โดยระบุลักษณะการใช้งานคลาวด์
5) ทดสอบการจัดลำดับความมั่นคงของผู้ให้บริการคลาวด์โดยพิจารณาเฉพาะเป้าหมายความมั่นคงประเภทใดประเภทหนึ่ง

บทที่ 4
การประเมินผลการวิจัย

ผู้วิจัยได้คัดเลือกผู้ให้บริการคลาวด์เพื่อรวบรวมหลักฐานของเป้าหมายความมั่นคงจากเว็บไซต์ 3 ราย ได้แก่ Amazon [21], Google [22] และ SalesForce [23] โดยมีรายละเอียด ดังนี้

1) ผู้ให้บริการคลาวด์ Amazon ให้บริการคลาวด์ทั้งด้าน Infrastructure as a Service เช่น Amazon EC2 [24] ซึ่งเป็นการให้บริการเกี่ยวกับ Virtual Computing Environment และ Platform as a Service เช่น Amazon RDS [25] ซึ่งเป็นการให้บริการเกี่ยวกับ Database Server โดย Amazon EC2 และ Amazon RDS จัดเป็นการใช้งานคลาวด์ทั้งแบบ Public และ Private
2) ผู้ให้บริการคลาวด์ Google ให้บริการคลาวด์ทั้งด้าน Platform as a Service เช่น Google Cloud Platform [22] และ Software as a Service เช่น Google Drive [26] ซึ่งเป็นการให้บริการเกี่ยวกับแอพพลิเคชันสำหรับจัดการเอกสาร โดย Google Cloud Platform และ Google Drive จัดเป็นการใช้งานคลาวด์แบบ Public
3) ผู้ให้บริการคลาวด์ SalesForce ให้บริการคลาวด์ทั้งด้าน Platform as a Service เช่น SalesForce Platform [27] และ Software as a Service เช่น CRM Sales app [28] โดย SalesForce Platform และ CRM Sales app จัดเป็นการใช้งานคลาวด์แบบ Public

การทดสอบและประเมินผลการวิจัย จะจำลองข้อมูลที่ใช้ในการทดสอบมาจากเว็บไซต์ของผู้ให้บริการคลาวด์ทั้ง 3 ราย โดยแสดงและเปรียบเทียบผลคะแนนความมั่นคงของผู้ให้บริการคลาวด์ทั้งหมด นอกจากนี้ เมื่อพิจารณาจากประเภทการให้บริการคลาวด์และลักษณะการใช้งานคลาวด์ของผู้ให้บริการคลาวด์บางรายที่แตกต่างกัน ผู้วิจัยได้จับกลุ่มผู้ให้บริการคลาวด์เพื่อทำการทดสอบในกรณีต่าง ๆ เพิ่มเติม ดังตารางที่ 4.1

ตารางที่ 4.1 การจัดกลุ่มผู้ให้บริการคลาวด์เพื่อทำการทดสอบ

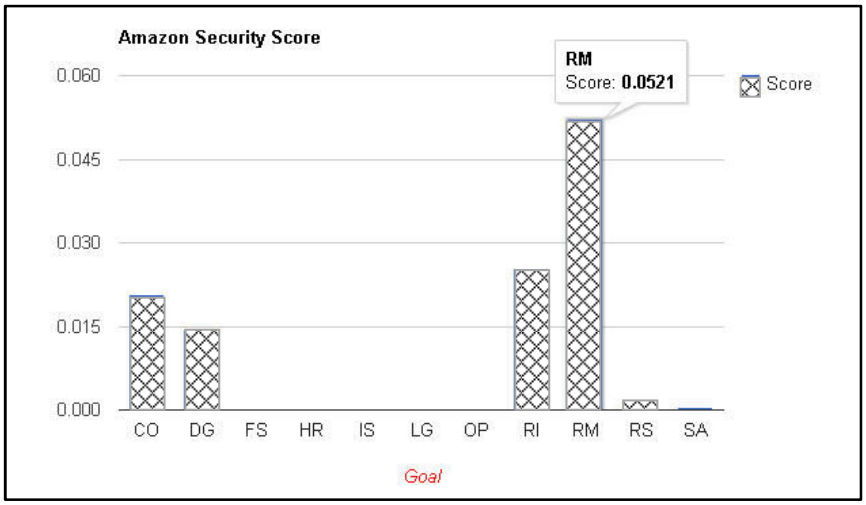
กรณีทดสอบ	ผู้ให้บริการคลาวด์รายที่ 1	ผู้ให้บริการคลาวด์รายที่ 2
การจัดลำดับความมั่นคงของผู้ให้บริการคลาวด์ที่มีลักษณะการให้บริการคลาวด์ประเภทเดียวกัน คือ Platform as a Service	Amazon	Google
การจัดลำดับความมั่นคงของผู้ให้บริการคลาวด์ที่มีลักษณะการใช้งานคลาวด์ประเภทเดียวกัน คือ Public	Google	SalesForce

4.1 กรณีทดสอบการประเมินคะแนนความมั่นคงของผู้ให้บริการคลาวด์

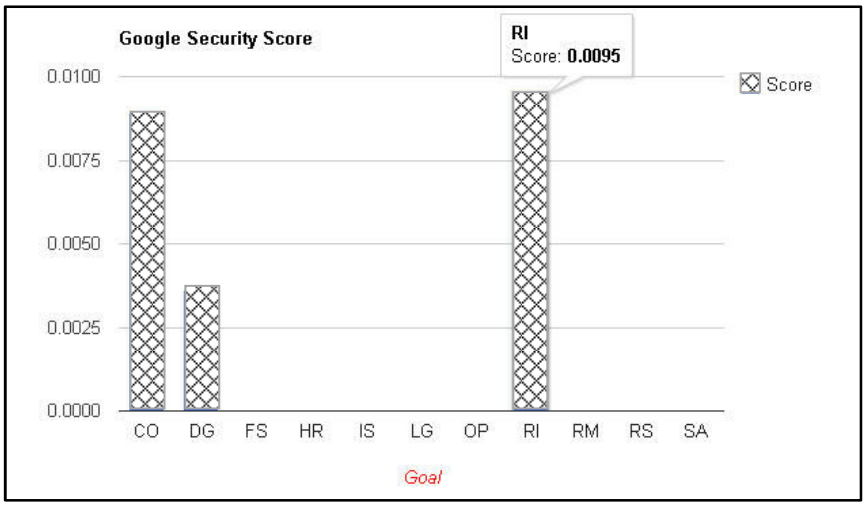
Amazon, Google และ SalesForce มีจำนวนหลักฐานที่ได้คะแนนการปฏิบัติตามเป้าหมายในทุกระดับ จำนวนหลักฐานที่ได้คะแนนความสมบูรณ์ในทุกระดับ คะแนนรวมของประเภทเป้าหมายความมั่นคงแต่ละประเภท (ทศนิยม 4 ตำแหน่ง) และคะแนนความมั่นคง (ทศนิยม 4 ตำแหน่ง) แสดงดังตารางที่ 4.2 ตารางที่ 4.3 และ ตารางที่ 4.4 ตามลำดับ

ระบบจะนำเสนอผลการประเมินคะแนนความมั่นคงของผู้ให้บริการคลาวด์แต่ละราย ในรูปแบบของกราฟแท่ง เพื่อแสดงความแตกต่างของคะแนนความมั่นคงของเป้าหมายความมั่นคงในแต่ละด้าน ดังตัวอย่างกราฟแสดงคะแนนความมั่นคงของเป้าหมายความมั่นคงทั้งหมดของผู้ให้บริการคลาวด์ Amazon ในภาพที่ 4.1 ซึ่งสามารถสรุปได้ว่า หลักฐานของเป้าหมายความมั่นคงของผู้ให้บริการคลาวด์ Amazon ที่มีการแสดงบนเว็บไซต์และมีการปฏิบัติตามเป้าหมายความมั่นคง รวมถึงมีความสมบูรณ์ของหลักฐานมากที่สุด คือ หลักฐานของเป้าหมายความมั่นคงด้าน Release Management รองลงมาอีก 2 อันดับเรียงจากมากไปน้อย คือ เป้าหมายความมั่นคงด้าน Risk Management และเป้าหมายความมั่นคงด้าน Compliance โดยหลักฐานของเป้าหมายความมั่นคงด้าน Facility Security, Human Resources Security, Information Security, Legal และ Operation Management ไม่ถูกแสดงบนเว็บไซต์ของผู้ให้บริการคลาวด์ Amazon

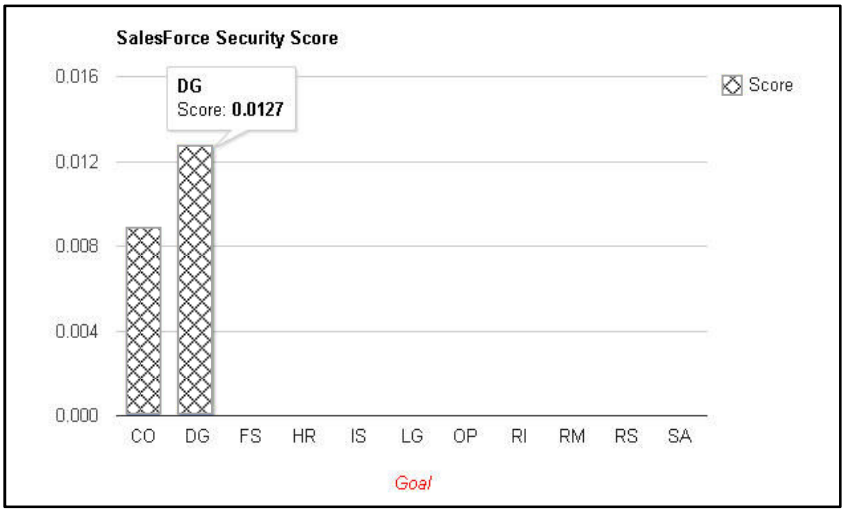
สำหรับกราฟแสดงคะแนนความมั่นคงของเป้าหมายความมั่นคงทั้งหมดของผู้ให้บริการคลาวด์ Google และ SalesForce ถูกแสดงในภาพที่ 4.2 และ 4.3 ตามลำดับ



ภาพที่ 4.1 กราฟแสดงคะแนนความมั่นคงของเป้าหมายทั้งหมดของ Amazon



ภาพที่ 4.2 กราฟแสดงคะแนนความมั่นคงของเป้าหมายทั้งหมดของ Google



ภาพที่ 4.3 กราฟแสดงคะแนนความมั่นคงของเป้าหมายทั้งหมดของ SalesForce

ตารางที่ 4.2 รายละเอียดหลักฐานของเป้าหมายความมั่นคงของ Amazon

Goal Category	No. of Goal	No. of Question	No. of Evidence	No. of Cloud Provider's Evidence	Compliance Level			Completeness Level						Total Score (%)
					No. of None	No. of Partial	No. of Full	No. of None	No. of Initial	No. of Planning	No. of Executing	No. of Monitoring and Controlling	No. of Closing	
CO	6	14	20	9	11	7	2	11	0	0	0	3	6	0.0207
DG	8	16	18	7	11	4	3	11	0	0	0	0	7	0.0145
FS	8	9	12	0	12	0	0	12	0	0	0	0	0	0
HR	3	4	4	0	4	0	0	4	0	0	0	0	0	0
IS	34	74	86	16	70	11	5	70	0	0	0	0	11	0
LG	2	4	5	0	5	0	0	5	0	0	0	0	0	0
OP	4	9	9	0	9	0	0	9	0	0	0	0	0	0
RI	5	14	15	4	11	0	4	11	0	0	0	0	4	0.0254
RM	5	6	8	1	7	0	1	7	0	0	0	0	1	0.0521
RS	8	12	13	2	11	0	2	11	0	0	0	0	2	0.0012
SA	15	32	34	2	32	0	2	32	0	0	0	0	2	0.0004
Total	**98**	**194**	**224**	**41**	**183**	**22**	**19**	**183**	**0**	**0**	**0**	**3**	**33**	0.0104

ตารางที่ 4.3 รายละเอียดหลักฐานของเป้าหมายความมั่นคงของ Google

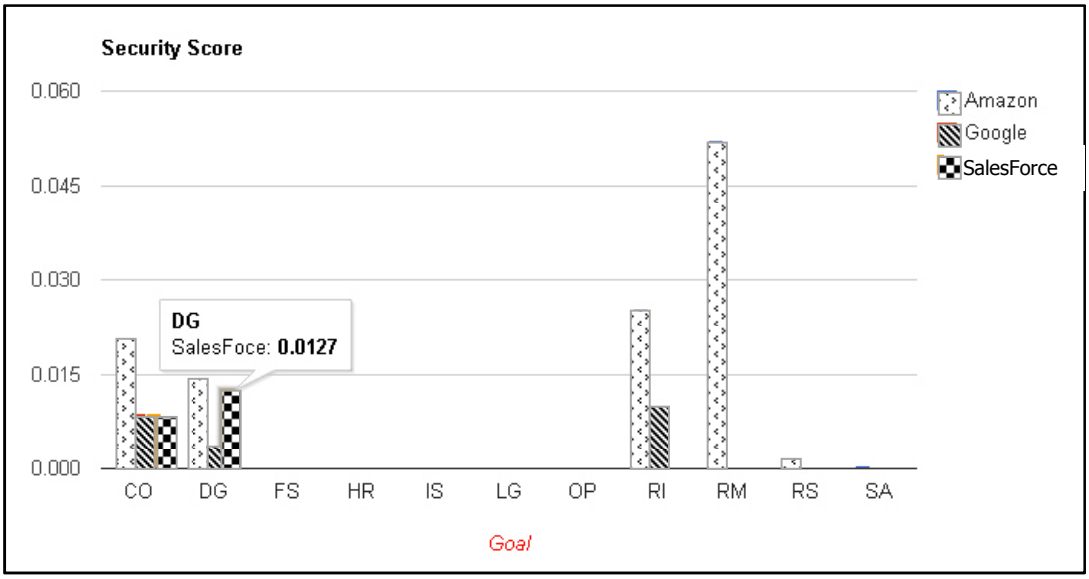
Goal Category	No. of Goal	No. of Question	No. of Evidence	No. of Cloud Provider's Evidence	Compliance Level			Completeness Level						Total Score (%)
					No. of None	No. of Partial	No. of Full	No. of None	No. of Initial	No. of Planning	No. of Executing	No. of Monitoring and Controlling	No. of Closing	
CO	6	14	20	4	16	4	0	16	0	0	0	0	4	0.0089
DG	8	16	18	2	16	2	0	16	0	0	0	0	2	0.0036
FS	8	9	12	0	12	0	0	12	0	0	0	0	0	0
HR	3	4	4	0	4	0	0	4	0	0	0	0	0	0
IS	34	74	86	7	79	5	2	79	0	0	0	0	7	0
LG	2	4	5	0	5	0	0	5	0	0	0	0	0	0
OP	4	9	9	0	9	0	0	9	0	0	0	0	0	0
RI	5	14	15	2	13	2	0	13	0	0	0	0	2	0.0095
RM	5	6	8	0	8	0	0	8	0	0	0	0	0	0
RS	8	12	13	0	13	0	0	13	0	0	0	0	0	0
SA	15	32	34	0	34	0	0	34	0	0	0	0	0	0
Total	**98**	**194**	**224**	**15**	**209**	**13**	**2**	**209**	**0**	**0**	**0**	**0**	**15**	**0.0020**

ตารางที่ 4.4 รายละเอียดหลักฐานของเป้าหมายความมั่นคงของ SalesForce

Goal Category	No. of Goal	No. of Question	No. of Evidence	No. of Cloud Provider's Evidence	Compliance Level			Completeness Level						Total Score (%)
					No. of None	No. of Partial	No. of Full	No. of None	No. of Initial	No. of Planning	No. of Executing	No. of Monitoring and Controlling	No. of Closing	
CO	6	14	20	4	16	4	0	16	0	0	0	0	4	0.0089
DG	8	16	18	7	11	7	0	11	0	0	0	0	7	0.0127
FS	8	9	12	0	12	0	0	12	0	0	0	0	0	0
HR	3	4	4	0	4	0	0	4	0	0	0	0	0	0
IS	34	74	86	5	83	5	0	83	0	0	0	0	5	0
LG	2	4	5	0	5	0	0	5	0	0	0	0	0	0
OP	4	9	9	0	9	0	0	9	0	0	0	0	0	0
RI	5	14	15	0	15	0	0	15	0	0	0	0	0	0
RM	5	6	8	0	8	0	0	8	0	0	0	0	0	0
RS	8	12	13	0	13	0	0	13	0	0	0	0	0	0
SA	15	32	34	0	34	0	0	34	0	0	0	0	0	0
Total	**98**	**194**	**224**	**16**	**210**	**16**	**0**	**210**	**0**	**0**	**0**	**0**	**16**	0.0019

4.2 กรณีทดสอบการจัดลำดับความมั่นคงของผู้ให้บริการคลาวด์ทั้งหมด

ผลการประเมินคะแนนความมั่นคงของผู้ให้บริการคลาวด์ทั้ง 3 ราย พบว่า คะแนนความมั่นคงที่พิจารณาจากหลักฐานของเป้าหมายความมั่นคงบนเว็บไซต์ของผู้ให้บริการคลาวด์ เรียงจากมากไปน้อย ได้แก่ Amazon มีคะแนนความมั่นคง 0.0104% Google มีคะแนนความมั่นคง 0.0020% และ SalesForce มีคะแนนความมั่นคง 0.0019% โดยคะแนนของเป้าหมายความมั่นคงแต่ละด้านของผู้ให้บริการคลาวด์ทั้ง 3 รายสามารถสรุปได้ ดังภาพที่ 4.4



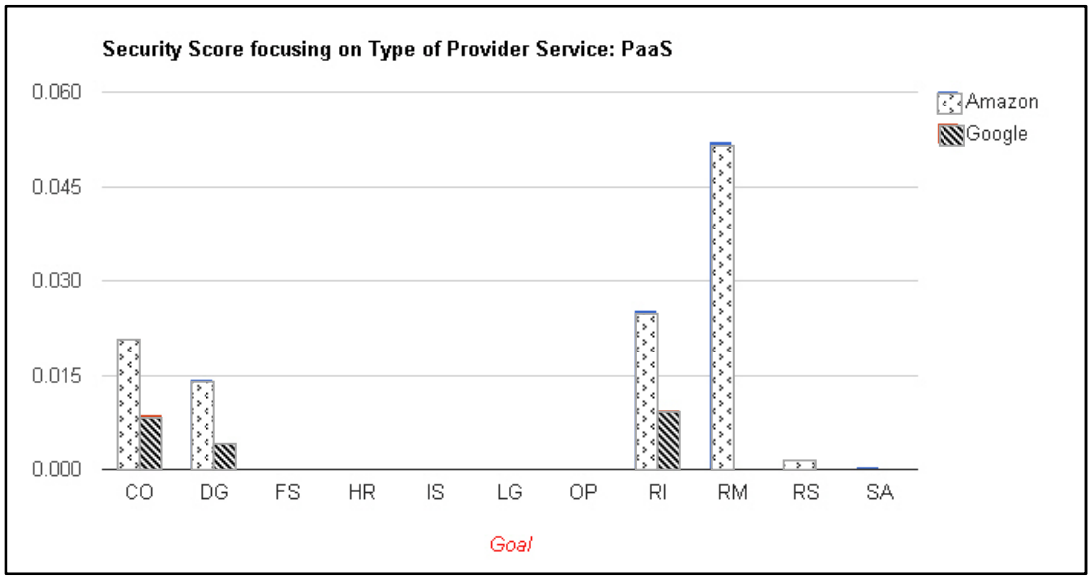
ภาพที่ 4.4 กราฟแสดงคะแนนความมั่นคงของเป้าหมายทั้ง 11 ด้าน ของผู้ให้บริการคลาวด์ทั้งหมด 3 ราย

กรณีทดสอบนี้ สามารถสรุปได้ว่า หลักฐานของเป้าหมายความมั่นคงทั้ง 11 ด้านของผู้ให้บริการคลาวด์ที่มีการแสดงบนเว็บไซต์ซึ่งแสดงถึงการปฏิบัติตามเป้าหมายความมั่นคง รวมถึงมีความสมบูรณ์ของหลักฐานมากที่สุด คือ ผู้ให้บริการคลาวด์ Amazon

อย่างไรก็ตาม ไม่สามารถสรุปได้ว่าผู้ให้บริการคลาวด์ Amazon มีความมั่นคงมากที่สุด เนื่องจากในความเป็นจริง ผู้ให้บริการคลาวด์ Google และ SalesForce อาจมีหลักฐานของเป้าหมายความมั่นคงที่ไม่ถูกแสดงบนเว็บไซต์ เช่นเดียวกันกับเป้าหมายความมั่นคงด้านที่ไม่มีคะแนนจะไม่สามารถสรุปได้ว่าคะแนนความมั่นคงของเป้าหมายด้านนั้นเป็น 0 หรือผู้ให้บริการคลาวด์ไม่ปฏิบัติตามเป้าหมายความมั่นคงนั้น

4.3 กรณีทดสอบการจัดลำดับความมั่นคงของผู้ให้บริการคลาวด์ที่มีลักษณะการให้บริการคลาวด์ประเภทเดียวกัน คือ Platform as a Service

จากตารางที่ 4.1 คะแนนความมั่นคงของผู้ให้บริการคลาวด์ Amazon และผู้ให้บริการคลาวด์ Google จะถูกนำมาเปรียบเทียบกัน เนื่องจากมีลักษณะการให้บริการคลาวด์ประเภทเดียวกัน คือ Platform as a Service โดยคะแนนความมั่นคงของ Amazon คือ 0.0104%รวมถึงคะแนนความมั่นคงของเป้าหมายแต่ละด้าน มากกว่าคะแนนความมั่นคงของ Google คือ 0.0020% ดังภาพที่ 4.5



ภาพที่ 4.5 กราฟแสดงคะแนนความมั่นคงของเป้าหมายทั้ง 11 ด้าน ของผู้ให้บริการคลาวด์ที่มีลักษณะการให้บริการประเภทเดียวกัน

กรณีทดสอบนี้ สามารถสรุปได้ว่า ผู้ให้บริการคลาวด์ Amazon ซึ่งมีลักษณะการให้บริการคลาวด์ประเภทเดียวกับผู้ให้บริการคลาวด์ Google คือ Platform as a Service มีการแสดงหลักฐานของเป้าหมายความมั่นคงบนเว็บไซต์ซึ่งแสดงถึงการปฏิบัติตามเป้าหมายความมั่นคง รวมถึงมีความสมบูรณ์ของหลักฐานมากกว่า

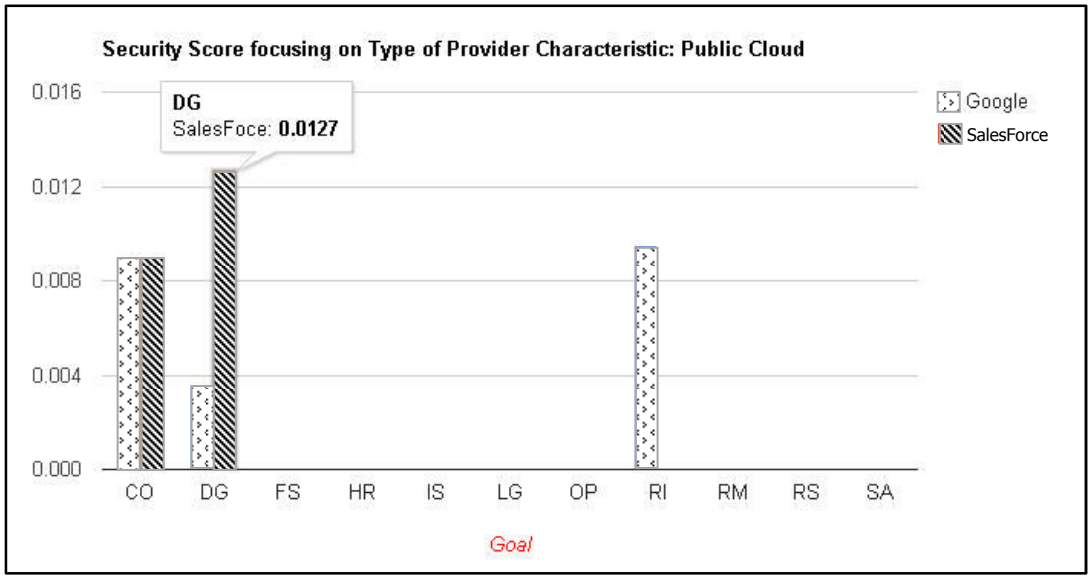
สำหรับการพิจารณาเลือกผู้ให้บริการคลาวด์ที่มีลักษณะการให้บริการคลาวด์ประเภทเดียวกัน ผู้ใช้บริการคลาวด์อาจไม่มีความจำเป็นต้องพิจารณาคะแนนความมั่นคงโดยรวม แต่อาจสนใจให้น้ำหนักกับเป้าหมายความมั่นคงด้านใดด้านหนึ่งมากกว่า ดังนั้น การแสดงผลเป็นกราฟ

แท่ง จึงมีวัตถุประสงค์เพื่อให้ผู้ใช้บริการคลาวด์สามารถพิจารณาและเปรียบเทียบความมั่นคงด้านต่าง ๆ ของผู้ให้บริการคลาวด์ที่มีลักษณะการให้บริการคลาวด์ประเภทเดียวกันได้ชัดเจนขึ้น

อย่างไรก็ตาม กรณีทดสอบนี้ไม่สามารถสรุปได้ว่าผู้ให้บริการคลาวด์ Amazon มีความมั่นคงมากกว่าผู้ให้บริการคลาวด์ Google เนื่องจากในความเป็นจริงผู้ให้บริการคลาวด์ Google อาจมีหลักฐานของเป้าหมายความมั่นคงที่ไม่ถูกแสดงบนเว็บไซต์ เช่นเดียวกันกับเป้าหมายความมั่นคงด้านที่ไม่มีคะแนน จะไม่สามารถสรุปได้ว่าคะแนนความมั่นคงของเป้าหมายด้านนั้นเป็น 0 หรือผู้ให้บริการคลาวด์ไม่ปฏิบัติตามเป้าหมายความมั่นคงนั้น

4.4 กรณีทดสอบการจัดลำดับความมั่นคงของผู้ให้บริการคลาวด์ที่มีลักษณะการใช้งานคลาวด์ประเภทเดียวกัน คือ Public Cloud

จากตารางที่ 4.1 คะแนนความมั่นคงของผู้ให้บริการคลาวด์ Google และผู้ให้บริการคลาวด์ SalesForce จะถูกนำมาเปรียบเทียบกัน เนื่องจากมีลักษณะการใช้งานคลาวด์ประเภทเดียวกัน คือ Public Cloud โดยคะแนนความมั่นคงของ Google คือ 0.0020% มากกว่าคะแนนความมั่นคงของ SalesForce คือ 0.0019% ดังภาพที่ 4.6



ภาพที่ 4.6 กราฟแสดงคะแนนความมั่นคงของเป้าหมายทั้ง 11 ด้าน ของผู้ให้บริการคลาวด์ที่มีลักษณะการใช้งานคลาวด์ประเภทเดียวกัน

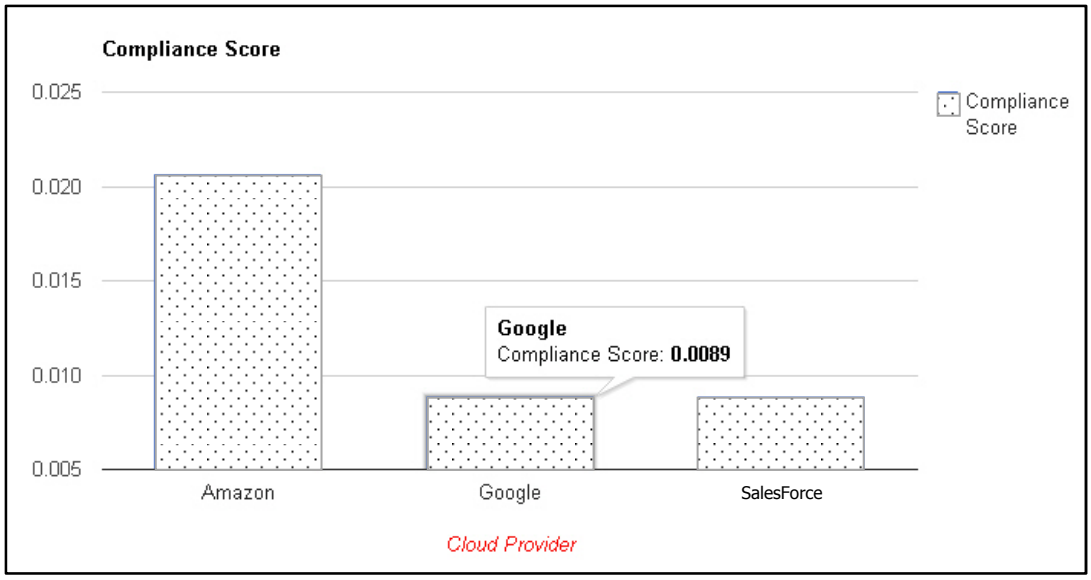
กรณีทดสอบนี้ สามารถสรุปได้ว่า ผู้ให้บริการคลาวด์ Google ซึ่งมีลักษณะการใช้งานคลาวด์ประเภทเดียวกับผู้ให้บริการคลาวด์ SalesForce คือ Public Cloud มีการแสดงหลักฐานของเป้าหมายความมั่นคงบนเว็บไซต์ซึ่งแสดงถึงการปฏิบัติตามเป้าหมายความมั่นคง รวมถึงมีความสมบูรณ์ของหลักฐานมากกว่า หากเปรียบเทียบตามเป้าหมายความมั่นคงแต่ละด้าน พบว่าผู้ให้บริการคลาวด์ทั้ง 2 ราย มีคะแนนความมั่นคงของเป้าหมายด้าน Compliance (CO) เท่ากัน

สำหรับการพิจารณาเลือกผู้ให้บริการคลาวด์ที่มีลักษณะการใช้งานคลาวด์ประเภทเดียวกัน ผู้ใช้บริการคลาวด์อาจไม่มีความจำเป็นต้องพิจารณาคะแนนความมั่นคงโดยรวม แต่อาจสนใจให้น้ำหนักกับเป้าหมายความมั่นคงด้านใดด้านหนึ่งมากกว่า ดังนั้น การแสดงผลเป็นกราฟแท่ง จึงมีวัตถุประสงค์เพื่อให้ผู้ใช้บริการคลาวด์สามารถพิจารณาและเปรียบเทียบความมั่นคงด้านต่าง ๆ ของผู้ให้บริการคลาวด์ที่มีลักษณะการใช้งานคลาวด์ประเภทเดียวกันได้ชัดเจนขึ้น

อย่างไรก็ตาม กรณีทดสอบนี้ไม่สามารถสรุปได้ว่าผู้ให้บริการคลาวด์ Google มีความมั่นคงมากกว่าผู้ให้บริการคลาวด์ SalesForce เนื่องจากในความเป็นจริงผู้ให้บริการคลาวด์ SalesForce อาจมีหลักฐานของเป้าหมายความมั่นคงที่ไม่ถูกแสดงบนเว็บไซต์ เช่นเดียวกันกับเป้าหมายความมั่นคงด้านที่ไม่มีคะแนน จะไม่สามารถสรุปได้ว่าคะแนนความมั่นคงของเป้าหมายด้านนั้นเป็น 0 หรือผู้ให้บริการคลาวด์ไม่ปฏิบัติตามเป้าหมายความมั่นคงนั้น

4.5 กรณีทดสอบการจัดลำดับความมั่นคงของผู้ให้บริการคลาวด์โดยพิจารณาเฉพาะเป้าหมายความมั่นคงประเภท Compliance (CO)

ผลการประเมินคะแนนความมั่นคงของเป้าหมายด้าน Compliance ของผู้ให้บริการคลาวด์ทั้ง 3 ราย พบว่า คะแนนความมั่นคงที่พิจารณาจากหลักฐานของเป้าหมายความมั่นคงด้าน Compliance บนเว็บไซต์ของผู้ให้บริการคลาวด์ เรียงจากมากไปน้อย ได้แก่ Amazon มีคะแนนความมั่นคงของเป้าหมายด้าน Compliance คือ 0.0027% Google มีคะแนนความมั่นคงของเป้าหมายด้าน Compliance คือ 0.0089% เท่ากันกับ SalesForce โดยคะแนนของเป้าหมายความมั่นคงด้าน Compliance ของผู้ให้บริการคลาวด์ทั้ง 3 รายสามารถสรุปได้ ดังภาพที่ 4.7



ภาพที่ 4.7 กราฟแสดงคะแนนความมั่นคงของเป้าหมายด้าน Compliance ของผู้ให้บริการคลาวด์ทั้ง 3 ราย

การแสดงผลเป็นกราฟแท่งจะช่วยให้ผู้ใช้บริการคลาวด์ เห็นความแตกต่างของคะแนนความมั่นคงของเป้าหมายด้านใดด้านหนึ่งของผู้ให้บริการคลาวด์แต่ละรายได้ชัดเจน อย่างไรก็ตาม กรณีทดสอบนี้ไม่สามารถสรุปได้ว่าผู้ให้บริการคลาวด์ Amazon มีความมั่นคงด้าน Compliance มากกว่าผู้ให้บริการคลาวด์ Google และ SalesForce เนื่องจากในความเป็นจริงผู้ให้บริการคลาวด์ Google และ SalesForce อาจมีหลักฐานของเป้าหมายความมั่นคงด้าน Compliance ที่ไม่ถูกแสดงบนเว็บไซต์

บทที่ 5
สรุปผลการวิจัย

5.1 สรุปผลการวิจัย

งานวิจัยนี้นำเสนอวิธีการประเมินคะแนนความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงของผู้ให้บริการคลาวด์ โดยนำวิธีจีคิวเอ็มมาใช้กำหนดหลักฐานที่แสดงให้เห็นถึงนโยบายหรือกระบวนการที่ผู้ให้บริการคลาวด์จัดทำขึ้นเพื่อเป็นวิธีปฏิบัติในการรักษาความมั่นคงของทรัพยากรคลาวด์ที่ให้บริการ ผู้วิจัยนำแนวคิดของวิธีจีคิวเอ็มซึ่งประกอบด้วยการกำหนดเป้าหมาย คำถาม และตัววัด มาประยุกต์ใช้กับเมตริกซ์ควบคุมคลาวด์และคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ที่ถูกกำหนดโดยองค์กรความมั่นคงของคลาวด์ ทำให้ผู้วิจัยสามารถวิเคราะห์หาตัววัดซึ่งหมายถึงหลักฐานจำนวน 224 ข้อ ที่แสดงให้เห็นถึงวิธีปฏิบัติด้านความมั่นคงของผู้ให้บริการคลาวด์

จากแนวคิดและวิธีการดังกล่าว ผู้ให้บริการคลาวด์จะถูกประเมินความมั่นคง 11 ด้าน ได้แก่ การปฏิบัติตาม การกำกับดูแลข้อมูล ความมั่นคงด้านสิ่งอำนวยความสะดวก ความมั่นคงด้านทรัพยากรมนุษย์ ความมั่นคงด้านสารสนเทศ กฎหมาย การจัดการการดำเนินการ การจัดการความเสี่ยง การจัดการการปล่อย/เริ่มต้นให้บริการ การคืนสภาพได้ และสถาปัตยกรรมความมั่นคงโดยใช้ระบบที่พัฒนาขึ้น ซึ่งผู้ให้บริการคลาวด์จะต้องให้หลักฐานตามที่กำหนดในงานวิจัย และผู้ตรวจสอบความมั่นคงของคลาวด์ จะเป็นผู้ให้คะแนนแก่หลักฐานผ่านระบบ ได้แก่ คะแนนการปฏิบัติตามเป้าหมายของหลักฐานและคะแนนความสมบูรณ์ของหลักฐาน จากนั้นระบบจะทำการประมวลผลและแสดงคะแนนความมั่นคงของผู้ให้บริการคลาวด์ตามความมั่นคงทั้ง 11 ด้าน รวมทั้งคะแนนความมั่นคงโดยรวมของผู้ให้บริการคลาวด์

การประเมินคะแนนความมั่นคงทั้ง 11 ด้านของผู้ให้บริการคลาวด์จากเป้าหมาย 98 ข้อ คำถามที่สอดคล้องกับเป้าหมาย 194 ข้อ และหลักฐาน 224 ข้อ นำไปสู่ผลการวิจัยที่สามารถสรุปได้ว่า คะแนนความมั่นคงของผู้ให้บริการคลาวด์ สามารถแสดงถึงความโปร่งใสในการแสดงให้เห็นถึงการปฏิบัติตามความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงทั้ง 11 ด้าน ซึ่งผู้ใช้บริการคลาวด์สามารถมั่นใจได้ว่านอกจากผู้ให้บริการคลาวด์จะให้บริการตรงตามความต้องการเชิงหน้าที่แล้วยังมีการปฏิบัติตามความมั่นคงด้านต่าง ๆ ซึ่งเป็นการรับรองว่า ทรัพยากรหรือข้อมูลของผู้ใช้บริการคลาวด์จะมีความมั่นคงตามมาตรฐาน นอกจากนี้ ผู้ใช้บริการคลาวด์ยังสามารถ

เปรียบเทียบคะแนนความมั่นคงของผู้ให้บริการคลาวด์รายต่าง ๆ เพื่อเลือกผู้ให้บริการคลาวด์ให้เหมาะสมกับการใช้งาน

5.2 ปัญหาและข้อจำกัด

5.2.1 งานวิจัยนี้ยึดแนวคิดเรื่องความโปร่งใสด้านความมั่นคง ซึ่งมีสมมติฐานว่าผู้ให้บริการคลาวด์ควรมีการเปิดเผยข้อมูลความมั่นคงอย่างเหมาะสมเพื่อให้การตรวจสอบหรือเลือกใช้ผู้ให้บริการแต่ละรายได้เป็นไปได้ง่ายขึ้น แต่เนื่องจากข้อมูลด้านความมั่นคงถือเป็นข้อมูลลับ ผู้ให้บริการคลาวด์จะเปิดเผยได้เฉพาะลูกค้าหรือองค์กรที่มีความน่าเชื่อถือ แนวทางของงานวิจัยจึงยังประสบปัญหาในทางปฏิบัติ ข้อมูลที่นำมาทดลองเป็นข้อมูลจำลองโดยการรวบรวมจากเว็บไซต์ของผู้ให้บริการคลาวด์ ซึ่งทำให้ได้ข้อมูลด้านความมั่นคงเป็นส่วนน้อย และทำให้คะแนนความมั่นคงของเป้าหมายบางด้านเป็นศูนย์ ซึ่งในงานวิจัย คะแนนที่เป็นศูนย์หมายถึงการไม่ปฏิบัติตามนโยบาย แต่ในการทดลองจะหมายถึงไม่สามารถหารายละเอียดได้ ดังนั้น จึงไม่สามารถสรุปได้แน่ชัดว่าผู้ให้บริการคลาวด์ไม่ปฏิบัติตามความมั่นคงด้านนั้น ๆ

5.2.2 เพื่อความโปร่งใสและตรวจสอบได้ งานวิจัยได้ออกแบบให้มีผู้ตรวจสอบความมั่นคงของคลาวด์เป็นผู้วิเคราะห์และให้คะแนนหลักฐานความมั่นคงของผู้ให้บริการคลาวด์ ทำให้การทำงานของระบบที่ออกแบบยังไม่เป็นอัตโนมัติ

5.3 แนวทางการวิจัยต่อไป

ผู้วิจัยมีแนวคิดจะจัดกลุ่มหลักฐานความมั่นคงตามมาตรฐานด้านความมั่นคงที่เป็นที่นิยม เช่น ISO 27001 เพื่อลดการทำงานของผู้ให้บริการคลาวด์และผู้ตรวจสอบความมั่นคงของคลาวด์ โดยผู้ให้บริการคลาวด์ที่มีการปฏิบัติตามมาตรฐานดังกล่าวและได้รับการรับรอง ไม่จำเป็นต้องให้หลักฐานทุกข้อ แต่สามารถอ้างถึงมาตรฐานที่ได้รับการรับรองแทนได้

รายการอ้างอิง

[1] Cloud Security Alliance. Cloud Control Matrix [Online]. 2011. Available from : https://cloudsecurityalliance.org/research/ccm [2011, August].

[2] Cloud Security Alliance. Consensus Assessments Initiative Questionnaire [Online]. 2011. Available from : https://cloudsecurityalliance.org /research/cia [2011, September].

[3] Gerring, J. and Thacker, S. C. Political institutions and corruption. The role of unitarism and parliamentarism. British Journal of Political Science (2004).

[4] Basili, V., Caldiera, G., and Rombach H. D. Goal Question Metric Paradigm. Encyclopedia of Software Engineering Volume 1 (1994) : 528-532.

[5] Jansen, W., and Grance, T. Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144 (December 2011).

[6] Craig-Wood, K. IAAS VS. PAAS VS. SAAS Definition [Online]. 2010. Available from : http://www.katescomment.com/iaas-paas-saas-definition/ [2010, May].

[7] Walker, G. Cloud Computing Fundamentals [Online]. 2010. Available from : https://www.ibm.com/developerworks/cloud/library/cl-cloudintro/index.html [2010, December].

[8] Knode, R. and Egan, D. Digital Trust in the Cloud, Into the Cloud with CTP. A Precis for the CloudTrust Protocol. Computer Sciences Corporation (2010).

[9] Pauley, W. A. Cloud Provider Transparency. An Empirical Evaluation. IEEE Security & Privacy November (December 2010) : 32-39.

[10] Michael, B. In Clouds Shall We Trust. IEEE Security & Privacy September (October 2009) : 3.

[11] Sun Microsystems, Inc. Building Customer Trust in Cloud Computing with Transparent Security. Sun Microsystems, Inc., 2009.

[12] Everett, C. Cloud Computing – A Question of Trust. Computer Fraud &

Security (June 2009) : 5-7.

[13] Kaliski, B. S. Jr. and Pauley, W. Toward Risk Assessment as a Service in Cloud Environments. In Proceedings of 2nd USENIX Conference on Hot Topics in Cloud Computing (HotCloud'10), pp.1-7. 2010.

[14] Tancock, D., Pearson, S., and Charlesworth, A. A Privacy Impact Assessment Tool for Cloud Computing. In Proceedings of 2nd IEEE International Conference on Cloud Computing Technology and Science, pp.667-676. 2010.

[15] Khamis, N., Idris, S., and Ahmad, R. Applying GQM Approach towards Development of Criterion-Referenced Assessment Model for OO Programming Courses. International Journal of Human and Social Sciences 3,5 (2008).

[16] Khan, K. M. Assessing Quality of Web Based Systems. In Proceedings of IEEE/ACS International Conference on Computer Systems and Applications (AICCSA 2008), pp.763-769. 2008.

[17] Abran, A., Moore, J. W., Bourque. P., Dupuis, R., and Tripp, L.L. Guide to the Software Engineering Body of Knowledge 2004 Version (SWEBOK). IEEE Computer Society (2004).

[18] Project Management Institute (PMI) Standards Committee. A Guide to the Project Management Body of Knowledge (PMBOK Guide) Fourth Edition. Project Management Institute, 2008.

[19] Nottingham, M. and Sayre, R. The Atom Syndication Format [Online]. 2005. Available from : www.ietf.org/rfc/rfc4287 [2010, December].

[20] ISO27001. ISO 27001:2005 ISMS Implementation Checklist [Online]. 2007. Available from : http://webstore.ansi.org [2007, October].

[21] Amazon.com Company. Amazon Web Services [Online]. 2013. Available from : https://aws.amazon.com/ [2013, April].

[22] Google. Google Cloud Platform [Online]. 2013. Available from : https://cloud.google.com/ [2013, April].

[23] Salesforce.com, inc. Salesforce.com [Online]. 2013. Available from : http://www.salesforce.com/company/ [2013, April].

[24] Amazon.com Company. Amazon Elastic Compute Cloud (Amazon EC2) [Online]. 2013. Available from : http://aws.amazon.com/ec2/ [2013, April].

[25] Amazon.com Company. Amazon Relational Database Service (Amazon RDS) [Online]. 2013. Available from : http://aws.amazon.com/rds/ [2013, April].

[26] Amazon.com Company. Google Drive [Online]. 2013. Available from : https://www.google.com/intl/en_US/drive/start/index.html [2013, April].

[27] Salesforce.com, inc. Salesforce Platform [Online]. 2013. Available from : http://www.salesforce.com/platform/overview/ [2013, April].

[28] Salesforce.com, inc. Sales Cloud [Online]. 2013. Available from : http://www.salesforce.com/sales-cloud/resources/ [2013, April 01].

ภาคผนวก

ตัวอย่างรายละเอียดของเป้าหมาย คำถามที่ถูกแปลง และหลักฐานความมั่นคงที่สอดคล้องกับเป้าหมายและคำถาม

ตารางที่ ก.1 ตัวอย่างรายละเอียดของเป้าหมายและคำถามที่ถูกแปลง

รหัสเป้าหมาย	รายละเอียดเป้าหมาย	รหัสคำถาม	คำถามที่ถูกแปลง
Compliance (CO)			
CO-01	Audit Planning	CO-01.1	What is the quality of the evidence that shows that cloud providers produce audit assertions, using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.), that cloud provider produce?
CO-02	Independent Audits	CO-02.1	What is the quality of the evidence that shows that cloud providers allow tenant to view their SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?
		CO-02.2	What is the quality of the evidence that shows that cloud providers conduct network penetration tests of their cloud service infrastructure that they conduct regularly as prescribed by industry best practices and guidance?
		CO-02.3	What is the quality of the evidence that shows that cloud providers conduct regular application penetration tests of their cloud infrastructure as prescribed by industry best practices and guidance?
		CO-02.4	What is the quality of the evidence that shows that cloud providers conduct internal audits regularly as prescribed by industry best practices and guidance?
		CO-02.5	What is the quality of the evidence that shows that cloud providers conduct external audits regularly as prescribed by industry best practices and guidance?
		CO-02.6	What is the quality of the evidence that shows that cloud providers make results of the network penetration tests available to tenants at their request?

ตารางที่ ก.1 ตัวอย่างรายละเอียดของเป้าหมายและคำถามที่ถูกแปลง (ต่อ)

รหัสเป้าหมาย	รายละเอียดเป้าหมาย	รหัสคำถาม	คำถามที่ถูกแปลง
Compliance (CO)			
CO-02	Independent Audits	CO-02.7	What is the quality of the evidence that shows that cloud providers make results of internal and external audits available to tenants at their request?
CO-03	Third Party Audits	CO-03.1	What is the quality of the evidence that shows that cloud providers permit tenants to perform independent vulnerability assessments?
		CO-03.2	What is the quality of the evidence that shows that cloud providers have external third-party conduct vulnerability scans and periodic penetration tests on their applications and networks?
Data Governance (DG)			
DG-01	Ownership / Stewardship	DG-01.1	What is the quality of the evidence that shows that cloud providers follow a structured data-labeling standard (ex. ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?
DG-02	Classification	DG-02.1	What is the quality of the evidence that shows that cloud providers provide a capability to identify virtual machines via policy tags/metadata (ex. Tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country, etc.)?
		DG-02.2	What is the quality of the evidence that shows that cloud providers provide a capability to identify hardware via policy tags/metadata/hardware tags (ex. TXT/TPM, VN-Tag, etc.)?
		DG-02.3	What is the quality of the evidence that shows that cloud providers have a capability to use system geographic location as an authentication factor?
		DG-02.4	What is the quality of the evidence that shows that cloud providers provide the physical location or geography of storage of a tenant\s data upon request?
		DG-02.5	What is the quality of the evidence that shows that cloud providers allow tenants to define acceptable geographical locations for data routing or resource instantiation?

ตารางที่ ก.1 ตัวอย่างรายละเอียดของเป้าหมายและคำถามที่ถูกแปลง (ต่อ)

รหัสเป้าหมาย	รายละเอียดเป้าหมาย	รหัสคำถาม	คำถามที่ถูกแปลง
Facility Security (FS)			
FS-01	Policy	FS-01.1	What is the quality of the evidence that shows that cloud providers established policies and procedures for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?
FS-02	User Access	FS-02.1	What is the quality of the evidence that shows that cloud providers have pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification?
FS-03	Controlled Access Points	FS-03.1	What is the quality of the evidence that shows that cloud providers implement physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols)?
Human Resources Security (HR)			
HR-01	Background Screening	HR-01.1	What is the quality of the evidence that shows that cloud providers have pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification?
HR-02	Employment Agreements	HR-02.1	What is the quality of the evidence that shows that cloud providers specifically train employees regarding their role vs. the tenant\s role in providing information security controls?
		HR-02.2	What is the quality of the evidence that shows that cloud providers document employee acknowledgment of training they have completed?

ตารางที่ ก.1 ตัวอย่างรายละเอียดของเป้าหมายและคำถามที่ถูกแปลง (ต่อ)

รหัสเป้าหมาย	รายละเอียดเป้าหมาย	รหัสคำถาม	คำถามที่ถูกแปลง
Information Security (IS)			
IS-01	Management Program	IS-01.1	What is the quality of the evidence that shows that cloud providers provide tenants with documentation describing their Information Security Management Program (ISMP)?
IS-02	Management Support / Involvement	IS-02.1	What is the quality of the evidence that shows that cloud providers have a policy in place to ensure executive and line management take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution?
IS-03	Policy	IS-03.1	What is the quality of the evidence that shows that cloud providers provide information security and privacy policies align with particular industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?
		IS-03.2	What is the quality of the evidence that shows that cloud providers have agreements which ensure their providers adhere to their information security and privacy policies?
		IS-03.3	What is the quality of evidence of due diligence mapping of cloud providers\s controls, architecture and processes to regulations and/or standards which is provided by cloud providers?
IS-04	Baseline Requirements	IS-04.1	What is the quality of the evidence that shows that cloud providers have documented information security baselines for every component of their infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)?
		IS-04.2	What is the quality of the evidence that shows that cloud providers have a capability to continuously monitor and report the compliance of their infrastructure against their information security baselines?
		IS-04.3	What is the quality of evidence to show about information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)?
IS-05	Policy Reviews	IS-05.1	What is the quality of the evidence that shows that cloud providers notify their tenants when they make material changes to their information security and/or privacy policies?

ตารางที่ ก.1 ตัวอย่างรายละเอียดของเป้าหมายและคำถามที่ถูกแปลง (ต่อ)

รหัสเป้าหมาย	รายละเอียดเป้าหมาย	รหัสคำถาม	คำถามที่ถูกแปลง
Legal (LG)			
LG-01	Disclosure Agreements	LG-01.1	What is the quality of the evidence that shows that cloud provider's requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?
LG-02	Third Party Agreements	LG-02.1	What is the quality of the evidence that shows that cloud provider select and monitor outsourced providers in compliance with laws in the country where the data is processed and stored and transmitted?
		LG-02.2	What is the quality of the evidence that shows that cloud provider select and monitor outsourced providers in compliance with laws in the country where the data originates?
		LG-02.3	What is the quality of the evidence that shows that cloud provider's legal counsel review all third party agreements?
Operations Management (OP)			
OP-01	Policy	OP-01.1	What is the quality of the evidence that shows that cloud provider established policy and procedures and made available for all personnel to adequately support services operations roles?
OP-02	Documentation	OP-02.1	What is the quality of the evidence that shows that cloud provider made information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) available to authorized personnel to ensure Configuring, installing, and operating the information system?
Risk Management (RI)			
RI-01	Program	RI-01.1	What is the quality of the evidence that shows that cloud provider's organization insured by a 3rd party for losses?
RI-02	Assessments	RI-02.1	What is the quality of the evidence that shows that cloud provider's formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?

ตารางที่ ก.1 ตัวอย่างรายละเอียดของเป้าหมายและคำถามที่ถูกแปลง (ต่อ)

รหัสเป้าหมาย	รายละเอียดเป้าหมาย	รหัสคำถาม	คำถามที่ถูกแปลง
Release Management (RM)			
RM-01	New Development / Acquisition	RM-01.1	What is the quality of the evidence that shows that cloud provider's policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities?
RM-02	Production Changes	RM-02.1	What is the quality of the evidence that shows that cloud providers provide tenants with documentation which describes your production change management procedures and their roles/rights/responsibilities within it?
RM-03	Quality Testing	RM-03.1	What is the quality of the evidence that shows that cloud providers provide their tenants with documentation which describes their quality assurance process?
Resiliency (RS)			
RS-01	Management Program	RS-01.1	What is the quality of the evidence that shows that cloud provider policy, process and procedures defining business continuity and disaster recovery in place to minimize the impact of a realized risk event and properly communicated to tenants?
RS-02	Impact Analysis	RS-02.1	What is the quality of the evidence that shows that cloud providers provide tenants with documentation which describes your production change management procedures and their roles/rights/responsibilities within it?
		RS-02.2	What is the quality of the evidence that shows that cloud providers make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?
Security Architecture (SA)			
SA-01	Customer Access Requirements	SA-01.1	What is the quality of the evidence that shows that cloud provider's all identified security, contractual and regulatory requirements for customer access contractually are addressed and remediated prior to granting customers access to data, assets and information systems?
SA-02	User ID Credentials	SA-02.1	What is the quality of the evidence that shows that cloud providers support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?

ตารางที่ ก.2 ตัวอย่างรายละเอียดของหลักฐานความมั่นคงที่สอดคล้องกับเป้าหมายและคำถามที่ถูกแปลง

รหัสเป้าหมาย	รหัสคำถาม	รหัสหลักฐาน	รายละเอียดหลักฐานความมั่นคง
Compliance (CO)			
CO-01	CO-01.1	CO-01.1.1	Information Security Management System (ISMS) Policy [ISO27001: 6] that follows structured, industry accepted format.
		CO-01.1.2	Audit requirements [ISO27001: A.15.3.1] that focuses on data duplication, access, and data boundary limitations and uses a structured, industry accepted format.
		CO-01.1.3	Audit plans and activities [ISO27001: A.15.3.1] that focuses on data duplication, access, and data boundary limitations and uses a structured, industry accepted format.
		CO-01.1.4	Internal audit reports [GAPP: 10.2.5] that focuses on data duplication, access, and data boundary limitations and uses a structured, industry accepted format.
		CO-01.1.5	Independent audit reports covering controls at service organizations [GAPP: 10.2.5] that focuses on data duplication, access, and data boundary limitations and uses a structured, industry accepted format.
CO-02	CO-02.1	CO-02.1.1	Published SAS70 Type2/SSAE 16 SOC2/ISAE3402 or third party audit report
	CO-02.2	CO-02.2.1	Network penetration test result which is prescribed by industry best practices and guidance
	CO-02.3	CO-02.3.1	Application penetration test result which is prescribed by industry best practices and guidance
	CO-02.4	CO-02.4.1	Internal audit reports [GAPP: 10.2.5] that is prescribed by industry best practices and guidance
	CO-02.5	CO-02.5.1	External audit reports which is prescribed by industry best practices and guidance
	CO-02.6	CO-02.6.1	Network penetration testing policy and procedure [NIST: CA-2] that specified published network penetration test results to tenants policy
	CO-02.7	CO-02.7.1	Audit and accountability policy and procedures [NIST: AC-1] that specified published internal and external audit reports to tenants policy
CO-03	CO-03.1	CO-03.1.1	Vulnerability scanning information policy and procedures which specified independent vulnerability assessments policy
	CO-03.2	CO-03.2.1	Vulnerability scanning information policy and procedures which specified the ability of external third-party to conduct vulnerability scans
		CO-03.2.2	Penetration testing policy and procedures which specified the ability of external third-party to conduct periodic penetration tests

ตารางที่ ก.2 ตัวอย่างรายละเอียดของหลักฐานความมั่นคงที่สอดคล้องกับเป้าหมายและคำถามที่ถูกแปลง (ต่อ)

รหัสเป้าหมาย	รหัสคำถาม	รหัสหลักฐาน	รายละเอียดหลักฐานความมั่นคง
Data Governance (DG)			
DG-01	DG-01.1	DG-01.1.1	Information labeling and handling policy and procedures [ISO27001: A.7.2.2] which followed a structured data-labeling standard (ex. ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)
DG-02	DG-02.1	DG-02.1.1	Infrastructure and system management policy and procedures [GAPP: 1.2.6] which specified that virtual machines is identified via policy tags/metadata identification
	DG-02.1	DG-02.1.2	Configuration management policy and procedures [NIST: CM-1] which specified scope of guest operating systems management
	DG-02.2	DG-02.2.1	Infrastructure and system management policy and procedures [GAPP: 1.2.6] which specified that hardware is identified via policy tags/metadata identification
	DG-02.3	DG-02.3.1	Physical and environmental protection policy and procedures [NIST: PE-1] which specified capability to use system geographic location as an authentication factor
	DG-02.4	DG-02.4.1	Location data acquisition and disclosure policy and procedures [NIST: SC-1]
	DG-02.5	DG-02.5.1	Location data acquisition and disclosure policy and procedures [NIST: SC-1] which specified role of tenant to define acceptable geographical locations.
Facility Security (FS)			
FS-01	FS-01.1	FS-01.1.1	Physical and environmental protection policy and procedures [NIST: PE-1, GAPP: 8.2.3]
FS-02	FS-02.1	FS-02.1.1	Physical and environmental protection policy and procedures [NIST: PE-1, GAPP: 8.2.3]
FS-03	FS-03.1	FS-03.1.1	Physical and environmental protection policy and procedures [NIST: PE-1, GAPP: 8.2.3] which specified physical security perimeters
Human Resources Security (HR)			
HR-01	HR-01.1	HR-01.1.1	Physical and environmental protection policy and procedures [NIST: PE-1, GAPP: 8.2.3]
HR-02	HR-02.1	HR-02.1.1	Human resource security policy and procedures [ISO27001: A.8.1.2] which specified employee training policy
	HR-02.2	HR-02.1.2	Human resource security policy and procedures [ISO27001: A.8.1.2] which specified employee training policy

ตารางที่ ก.2 ตัวอย่างรายละเอียดของหลักฐานความมั่นคงที่สอดคล้องกับเป้าหมายและคำถามที่ถูกแปลง (ต่อ)

รหัสเป้าหมาย	รหัสคำถาม	รหัสหลักฐาน	รายละเอียดหลักฐานความมั่นคง
Information Security (IS)			
IS-01	IS-01.1	IS-01.1.1	Information Security Management System (ISMS) Policy [ISO27001: 6] which followed structured, industry accepted format.
IS-02	IS-02.1	IS-01.1.2	Information Security Management System (ISMS) Policy [ISO27001: 6] which followed structured, industry accepted format.
IS-03	IS-03.1	IS-03.1.1	Information security and privacy policies and procedures aligned with particular industry standard e.g. ISO-27001, ISO-22307, CoBIT, etc.
	IS-03.2	IS-03.2.1	Third party agreement which specified information security and privacy policy adherence
	IS-03.3	IS-03.3.1	Information security and privacy policies and procedures OR ISMS policy [ISO27001: 4.2.1]
IS-04	IS-04.1	IS-04.1.1	Information security and privacy policies and procedures [ISO27001: 4.2.1] which specified information security baseline for every component of cloud provider's infrastructure
	IS-04.2	IS-04.2.1	Information security and privacy policies and procedures OR ISMS policy [ISO27001: 4.2.1] which specified a capability to continuously monitor and report the compliance of cloud provider's infrastructure against cloud provider's information security baselines
	IS-04.3	IS-04.3.1	Baseline configuration of information system [NIST: CM-2]
IS-05	IS-05.1	IS-05.1.1	Information security and privacy policies and procedures OR ISMS policy [ISO27001: 4.2.1] which is distributed or published when making change.
Legal (LG)			
LG-01	LG-01.1	LG-01.1.1	Confidentiality agreement OR Non-disclosure agreement which identified the organization's needs for the protection of data and operational details
LG-02	LG-02.1	LG-02.1.1	Third party personnel security requirements [NIST: PS-7]
		LG-02.1.2	External information system service guidance [NIST: SA-9]
	LG-02.2	LG-02.2.1	Third party personnel security requirements [NIST: PS-7]
	LG-02.3	LG-02.3.1	Third party agreement reviewed result

ตารางที่ ก.2 ตัวอย่างรายละเอียดของหลักฐานความมั่นคงที่สอดคล้องกับเป้าหมายและคำถามที่ถูกแปลง (ต่อ)

รหัสเป้าหมาย	รหัสคำถาม	รหัสหลักฐาน	รายละเอียดหลักฐานความมั่นคง
Operations Management (OP)			
OP-01	OP-01.1	OP-01.1.1	Information system documentation [NIST: SA-5]
OP-02	OP-02.1	OP-02.1.1	Information system documentation [NIST: SA-5]
Risk Management (RI)			
RI-01	RI-01.1	RI-01.1.1	Information system documentation [NIST: SA-5]
	RI-01.2	RI-01.2.1	Service level agreement
RI-02	RI-02.1	RI-02.1.1	Risk assessment policy and procedures [NIST: RA-1]
		RI-02.1.2	Risk assessment result [NIST: RA-3]
	RI-02.2	RI-02.2.1	Risk assessment policy and procedures [NIST: RA-1]
Release Management (RM)			
RM-01	RM-01.1	RM-01.1.1	Information system documentation [NIST: SA-5]
RM-02	RM-02.1	RM-02.1.1	Configuration change control for information system documentation [NIST: CM-3]
RM-03	RM-03.1	RM-03.1.1	Information system documentation [NIST: SA-5]
Resiliency (RS)			
RS-01	RS-01.1	RS-01.1.1	Disaster recovery and contingency plan and procedures [GAPP: 8.2.7, NIST: CP-1]
RS-02	RS-02.1	RS-02.1.1	Configuration change control for information system documentation [NIST: CM-3]
	RS-02.2	RS-02.2.1	Information Security Management System (ISMS) Policy [ISO27001: 6] OR ISO 27001 certification (Clause 4.2.3)
Security Architecture (SA)			
SA-01	SA-01.1	SA-01.1.1	The security authorization process for information systems [NIST: PM-10]
SA-02	SA-02.1	SA-02.1.1	Access control policies and procedures [NIST: AC-1, NIST: AC-3, NIST: AC-6]
SA-03	SA-03.1	SA-03.1.1	Data security architecture which is designed using an industry standard

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวนันทพรรณ เป็นสุข เกิดเมื่อวันที่ 25 มีนาคม พ.ศ. 2528 จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาระดับปริญญาวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์ จากคณะวิศวกรรมศาสตร์ มหาวิทยาลัยธรรมศาสตร์ และได้เข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมซอฟต์แวร์ ณ ภาควิชาคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัยในปีการศึกษา 2553