การประเมินความไว้ใจได้ของผู้ให้บริการโดยอิงเมตริกซ์ควบคุมคลาวด์

นายจิรายุ กานต์ปริยสุนทร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2559

Provider Trustworthiness Assessment Based on Cloud Control Matrix

Mr. Jirayu Kanpariyasoontorn

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Computer Science
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2016

หัวข้อวิทยานิพนธ์	การประเมินความไว้ใจได้ของผู้ให้บริการโดยอิงเมตริกซ์ควบคุมคลาวด์
โดย	นายจิรายุ กานต์ปริยสุนทร
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.สุพจน์ เตชวรสินสกุล)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(รองศาสตราจารย์ ดร.วิวัฒน์ วัฒนาวุฒิ)

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

.....กรรมการภายนอกมหาวิทยาลัย
(ผู้ช่วยศาสตราจารย์ ดร.ชวลิต ศรีสถาพรพัฒน์)

จิรายุ กานต์ปริยสุนทร : การประเมินความไว้ใจได้ของผู้ให้บริการโดยอิงเมตริกซ์ควบคุมคลาวด์ (Provider Trustworthiness Assessment Based on Cloud Control Matrix) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: รศ. ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา, 147 หน้า.

ระบบการประมวลผลแบบคลาวด์ได้รับความนิยมอย่างแพร่หลายในปัจจุบันทั้งในภาคธุรกิจและบุคคลทั่วไป เนื่องมาจากการมีแบบจำลองการให้บริการแบบแบ่งปันทรัพยากร ซึ่งอนุญาตให้ผู้ใช้สามารถเข้าถึงบริการการประมวลผลที่มีประสิทธิภาพสูงและรองรับการขยายขนาดของระบบได้ตามต้องการ ระบบการประมวลผลแบบคลาวด์มีการเจริญเติบโตขึ้นอย่างรวดเร็วและเกิดผู้ให้บริการระบบการประมวลผลแบบคลาวด์เป็นจำนวนมากซึ่งเปิดให้บริการในลักษณะเดียวกัน ด้วยเหตุนี้คุณลักษณะเชิงคุณภาพของบริการจึงถูกนำมาใช้เป็นเกณฑ์ในการเลือกบริการคลาวด์ งานวิจัยนี้มุ่งเน้นในประเด็นความไว้ใจได้ของบริการคลาวด์ ซึ่งประกอบไปด้วยคุณลักษณะทางด้านความมั่นคงและคุณสมบัติทางด้านความพึ่งพาได้ โดยได้เสนอวิธีการประเมินความไว้ใจได้โดยอิงแนวทางความมั่นคงที่มีชื่อว่าเมตริกซ์ควบคุมคลาวด์หรือซีซีเอ็มของซีเอสเอซึ่งเชื่อมโยงกับเอกสารคำแนะนำด้านความมั่นคงและความเป็นส่วนตัวหมายเลขเอสพี 800-53 ของนิสต์ และเอกสารเกณฑ์และหลักการสำหรับบริการที่ไว้ใจได้ของเอไอซีพีเอ เพื่อทำการจำแนกว่าแต่ละการควบคุมด้านความมั่นคงในเมตริกซ์ควบคุมคลาวด์ สะท้อนถึงลักษณะด้านความมั่นคงและความพึ่งพาได้ในแง่มุมใดบ้าง จากข้อมูลการเชื่อมโยงที่ได้ งานวิจัยนี้นำเสนอการประเมินความสามารถด้านความมั่นคงของบริการคลาวด์จากข้อมูลแบบประเมินซึ่งเป็นที่เห็นพ้องต้องกันหรือซีเอไอคิวของซีเอสเอ เพื่อคำนวณค่าความไว้ใจได้ของบริการ วิธีการประเมินนี้ช่วยให้ผู้ใช้บริการสามารถพิจารณาเปรียบเทียบคุณลักษณะความไว้ใจได้ของผู้ให้บริการแต่ละราย ซึ่งเป็นปัจจัยหนึ่งที่ต้องคำนึงถึงในการเลือกบริการคลาวด์

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

ปีการศึกษา 2559

5670142921 : MAJOR COMPUTER SCIENCE

KEYWORDS: TRUSTWORTHINESS / SECURITY / DEPENDABILITY / CLOUD COMPUTING / ASSESSMENT

JIRAYU KANPARIYASOONTORN: Provider Trustworthiness Assessment Based on Cloud Control Matrix. ADVISOR: ASSOC. PROF. TWITTIE SENIVONGSE, Ph.D., 147 pp.

Cloud computing has been widely adopted by corporate and individual customers due to its resource-sharing model that allows on-demand access to scalable and high performance computing services. The growth of such services means there are a lot of service providers who can provide similar services, and hence quality attributes of the services become the criteria for cloud service selection. This research focuses on cloud service trustworthiness that embraces both security and dependability attributes. A trustworthiness assessment method is proposed based on the CSA Cloud Controls Matrix (CCM) security guidelines that are mapped to NIST SP800-53 security and privacy recommendations and AICPA trust services principles and criteria in order to classify security and dependability characteristics of each CCM security control. Based on the mapping, the security provision capabilities of a cloud service as listed in the CSA Consensus Assessments Initiative Questionnaire (CAIQ) are assessed and the trustworthiness score of the service is calculated. The assessment method then can assist service consumers in determining and comparing trustworthiness of candidate cloud services as one factor to consider in the service selection process.

Department:	Computer Engineering	Student's Signature	.....
Field of Study:	Computer Science	Advisor's Signature	.....
Academic Year:	2016		

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลงด้วยความกรุณาเป็นอย่างสูงของรองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่กรุณาให้คำปรึกษา แนะนำแนวทางการวิจัย ตรวจทานงานวิจัย และแนะนำแนวทางการแก้ไขปัญหาจากงานวิจัย ตลอดจนมีความเมตตาในการให้ความรู้ที่เป็นประโยชน์ในการทำงานวิจัย ทำให้งานวิจัยสำเร็จลุล่วงไปได้ด้วยดี ขอขอบพระคุณอาจารย์เป็นอย่างสูง ไว้ ณ ที่นี้

ขอขอบพระคุณ รองศาสตราจารย์ ดร.วิวัฒน์ วัฒนาวุฒิ ประธานกรรมการการสอบวิทยานิพนธ์ และผู้ช่วยศาสตราจารย์ ดร.ชวลิต ศรีสถาพรพัฒน์ กรรมการสอบวิทยานิพนธ์ที่กรุณาให้ความรู้และคำแนะนำที่เป็นประโยชน์ในการทำวิทยานิพนธ์

ขอขอบพระคุณอาจารย์ทุกท่านที่ให้ความรู้ สั่งสอน และให้คำแนะนำที่เป็นประโยชน์จนสามารถนำมาใช้ในการทำวิทยานิพนธ์ได้

ขอขอบพระคุณบิดาและมารดาที่ให้โอกาส กำลังใจในการเรียน สั่งสอน อบรม และสนับสนุนข้าพเจ้าในหลายๆด้าน จนข้าพเจ้าประสบความสำเร็จ

ขอบคุณเพื่อนนิสิตวิทยาศาสตร์คอมพิวเตอร์ วิศวกรรมซอฟต์แวร์ และวิศวกรรมคอมพิวเตอร์ ที่คอยช่วยเหลือในหลายๆด้าน เช่นข่าวสารมหาวิทยาลัย แหล่งข้อมูลงานประชุมวิชาการ เป็นต้น

สารบัญ

หน้า

หน้า

หน้า

สารบัญตาราง

สารบัญรูปภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบัน การประมวลผลแบบคลาวด์ (Cloud Computing) เป็นลักษณะการทำงานของเครือข่ายคอมพิวเตอร์ขนาดใหญ่บนอินเทอร์เน็ต โดยมีระบบการจัดสรรทรัพยากรตามลักษณะความต้องการของผู้ใช้ ซึ่งมีลักษณะการทำงานที่ยืดหยุ่น (Flexibility) และมีประสิทธิภาพสูง (Performance) ระบบจะมีการแบ่งปันทรัพยากรตามลักษณะการใช้งานและความต้องการของผู้ใช้ ทำให้ตัดปัญหาเรื่องของฮาร์ดแวร์และแบนด์วิดธ์ไปได้ ข้อดีของการประมวลผลแบบคลาวด์นั้นมีมากมายหลายด้าน ยกตัวอย่างเช่น ความสะดวกรวดเร็ว โดยผู้ใช้ไม่จำเป็นต้องคำนึงถึงว่าระบบทำงานอยู่บนเครือข่ายแบบใด มีพื้นที่จัดเก็บเท่าไร มีสมรรถนะของเครื่องเซิร์ฟเวอร์อย่างไร เป็นต้น ส่งผลให้ประหยัดค่าใช้จ่ายเนื่องมาจากผู้ใช้ไม่จำเป็นต้องทำการซื้อเครื่องเซิร์ฟเวอร์และอุปกรณ์ต่าง ๆ เอง รวมไปจนถึงไม่จำเป็นต้องจ้างบุคลากรทางด้านคอมพิวเตอร์มาคอยดูแลซึ่งเป็นการผลักภาระหน้าที่ให้เป็นหน้าที่ของผู้ให้บริการระบบประมวลผลแบบคลาวด์ (Cloud Provider) แทน ผู้ให้บริการคลาวด์ในปัจจุบันมีมากมายหลายบริษัท ตัวอย่างผลิตภัณฑ์จากบริษัทระดับโลก เช่น Amazon EC2, Amazon S3, Windows Azure, Google App Engine และ Salesforce.com เป็นต้น แต่ละบริษัทมีจุดแข็งและจุดอ่อนแตกต่างกันออกไป อยู่ที่ผู้ใช้บริการจะเลือกใช้บริการ ซึ่งในเมื่อมีผู้ให้บริการที่หลากหลายรูปแบบหลายบริษัทแล้วนั้น การเลือกผู้ให้บริการจึงเป็นสิ่งสำคัญ จึงเกิดประเด็นที่ว่า ผู้ใช้บริการจะทราบได้อย่างไรว่าผลิตภัณฑ์ที่กำลังจะเลือกใช้บริการหรือใช้บริการอยู่นั้นสามารถไว้ใจได้ เนื่องจากข้อมูลของผู้ใช้บริการเป็นข้อมูลที่มีความสำคัญ ถ้าเกิดเหตุการณ์ข้อมูลรั่วไหลหรือเกิดความเสียหายอาจส่งผลกระทบร้ายแรงให้กับผู้ใช้บริการได้ ซึ่งเหตุการณ์ดังกล่าวสามารถเกิดขึ้นได้เนื่องจากผู้ให้บริการไม่มีระบบการจัดการทางด้านความมั่นคงที่ดีพอ

ดังนั้นจากที่กล่าวมาข้างต้น จึงได้เกิดแนวคิดในการประเมินความไว้ใจได้ (Trustworthiness) ของผู้ให้บริการคลาวด์ โดยใช้การวิเคราะห์องค์ประกอบทางด้านความมั่นคง (Security) และความพึ่งพาได้ (Dependability) ผู้วิจัยได้ทำการวิเคราะห์เมตริกซ์ควบคุมคลาวด์ (Cloud Control Matrix : CCM) ซึ่งเป็นเมตริกซ์ที่รวบรวมการควบคุมด้านความมั่นคง 16 ด้าน เพื่อให้ผู้ให้บริการคลาวด์ใช้เป็นแนวปฏิบัติ ร่วมกับการวิเคราะห์แบบประเมินที่เป็นที่เห็นพ้องต้องกันของผู้ให้บริการคลาวด์ซึ่งเรียกว่า CAIQ (Consensus Assessments Initiative Questionnaire : CAIQ) ซึ่งประกอบด้วยรายการคำถามเกี่ยวกับแนวปฏิบัติด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ สำหรับใช้สอบถามว่าผู้ให้บริการได้ทำตามแนวปฏิบัติทางด้านความมั่นคงนั้น ๆ หรือไม่ โดยที่ผู้ให้บริการจะทำการประเมิน

ตนเองตามรายการคำถามและบันทึกไว้ใน CSA STAR (Security, Trust & Assurance Registry) ซึ่งเมตริกซ์ควบคุมคลาวด์และแบบประเมินที่เป็นที่เห็นพ้องต้องกัน กำหนดโดย CSA (Cloud Security Alliance) ผู้วิจัยจะทำการวิเคราะห์เมตริกซ์ควบคุมคลาวด์เพื่อทำการเชื่อมโยงกับคุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้ ซึ่งแบ่งออกเป็น 6 ด้าน ได้แก่ การรักษาความลับ (Confidentiality) บูรณภาพ (Integrity) สภาพพร้อมใช้งาน (Availability) ความเชื่อถือได้ (Reliability) ความปลอดภัย (Safety) และความสามารถในการบำรุงรักษา (Maintainability) โดยทำการพิจารณาว่าแต่ละแนวปฏิบัติทางด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ เกี่ยวข้องกับคุณลักษณะใดใน 6 ด้าน แล้วเสนอการประเมินค่าความไว้ใจได้ ค่าที่ได้จากการประเมินจะสะท้อนถึงความไว้ใจได้ของผู้ให้บริการคลาวด์ ซึ่งมีประโยชน์ต่อผู้ใช้บริการคลาวด์ โดยช่วยให้ผู้ใช้บริการคลาวด์สามารถทราบได้ว่า ผู้ให้บริการคลาวด์แต่ละรายที่กำลังใช้บริการอยู่หรือกำลังจะเลือกใช้บริการนั้น มีค่าความไว้ใจได้อยู่ในระดับใด และทำให้สามารถเลือกผู้ให้บริการคลาวด์ได้อย่างเหมาะสม

1.2 วัตถุประสงค์ของงานวิจัย

1) เพื่อเสนอวิธีการประเมินความไว้ใจได้ของผู้ให้บริการคลาวด์
2) เพื่อพัฒนาเครื่องมือสนับสนุนการประเมิน

1.3 ขอบเขตของงานวิจัย

1) ประเมินความไว้ใจได้ของผู้ให้บริการคลาวด์บนพื้นฐานของการประเมินความมั่นคงและความพึ่งพาได้
2) ใช้เมตริกซ์ควบคุมคลาวด์และคำถามใน CAIQ ที่กำหนดโดย CSA ร่วมกับมาตรฐานการควบคุมความมั่นคงของ NIST SP 800-53 และ AICPA เป็นหลัก ในการวิเคราะห์เพื่อประเมินความไว้ใจได้
3) ในการเชื่อมโยงคุณลักษณะด้านความมั่นคงและความพึ่งพาได้กับเมตริกซ์ควบคุมคลาวด์ จะมีการทวนสอบความถูกต้องของการเชื่อมโยงโดยพิจารณาจากนิยามของคุณลักษณะและวิธีการที่ทำให้ได้มาซึ่งคุณลักษณะนั้น ร่วมกับเอกสารอื่น ๆ ที่เกี่ยวข้องกับแนวปฏิบัติทางด้านความมั่นคง เช่นเอกสารมาตรฐาน เป็นต้น และสร้างตารางแสดงความสัมพันธ์กับคุณลักษณะ
4) ใช้ข้อมูลการปฏิบัติตามการควบคุมความมั่นคงของผู้ให้บริการที่มีเผยแพร่อยู่ใน STAR เป็นอย่างน้อย ในการประเมินผู้ให้บริการ

5) พัฒนาเครื่องมือสนับสนุนการประเมินที่สามารถคำนวณ แสดง และเปรียบเทียบคะแนนความไว้ใจได้ ของผู้ให้บริการคลาวด์แต่ละราย
6) ทดสอบเครื่องมือที่พัฒนากับข้อมูลผู้ให้บริการคลาวด์จำนวน 20 รายเป็นอย่างน้อย

1.4 ขั้นตอนการดำเนินงาน

1) กำหนดเกณฑ์ในการพิจารณาทางด้านความไว้ใจได้ ซึ่งประกอบไปด้วยคุณลักษณะทั้ง 6 ด้านของความมั่นคงและความพึ่งพาได้ โดยทำการรวบรวมข้อมูลจากหลายแหล่งข้อมูล
2) ทำการเชื่อมโยงคุณลักษณะด้านความไว้ใจได้จากเกณฑ์การพิจารณา เข้ากับแนวปฏิบัติทางด้านความมั่นคง CCM
3) กำหนดตัววัดความไว้ใจได้ของผู้ให้บริการคลาวด์
4) พัฒนาเครื่องมือสนับสนุนงานวิจัย
5) ทดสอบการประเมินผู้ให้บริการคลาวด์เพื่อเปรียบเทียบความไว้ใจได้
6) จัดทำบทความวิจัยและวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) ได้วิธีการประเมินคะแนนความไว้ใจได้ของผู้ให้บริการคลาวด์และเครื่องมือสนับสนุนการประเมิน
2) ผู้ใช้บริการคลาวด์สามารถประเมินและเปรียบเทียบคะแนนความไว้ใจได้ของผู้ให้บริการคลาวด์แต่ละรายได้

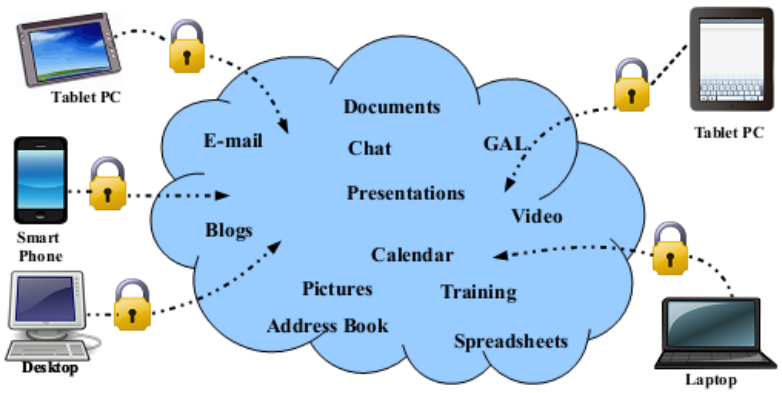
บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎี

2.1.1 การประมวลผลแบบคลาวด์

การประมวลผลแบบคลาวด์ (Cloud Computing) [1] คือเทคโนโลยีล่าสุดที่พัฒนาต่อจากการประมวลผลแบบกระจาย (Distributed Computing) การประมวลแบบขนาน (Parallel Processing) และการประมวลผลแบบกริด (Grid Computing) โดยมีการทำงานอยู่บนพื้นฐานของการจำลองรูปแบบการทำงานเสมือน (Virtualization) บนระบบการทำงานที่มีการรวมตัวของอุปกรณ์ที่มีประสิทธิภาพและความหลากหลายทางด้านการใช้งาน เช่น ฮาร์ดดิสก์ ข้อมูล ซอฟต์แวร์ และทรัพยากร เป็นต้น โดยผู้ใช้งานสามารถใช้งานคอมพิวเตอร์และการเก็บข้อมูลที่มีประสิทธิภาพสูงผ่านทางระบบเครือข่ายอินเทอร์เน็ต

การประมวลผลแบบคลาวด์ตามนิยามของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST: National Institute of Standard and Technology) [2] ได้กล่าวไว้ว่า การประมวลผลแบบคลาวด์คือโมเดลการทำงานที่ช่วยให้เกิดความสะดวกสบายและสามารถเข้าถึงข้อมูลที่ต้องการจากสถานที่ใดก็ได้ สนับสนุนการทำงานของระบบต่าง ๆ ร่วมกัน เช่น ระบบเครือข่าย เซิร์ฟเวอร์ อุปกรณ์จัดเก็บข้อมูล และการให้บริการในรูปแบบต่าง ๆ ที่สามารถจัดเตรียมการใช้งานได้อย่างรวดเร็วและมีการจัดการที่ง่าย ดังภาพที่ 2.1



ภาพที่ 2.1 การทำงานของระบบการประมวลผลแบบคลาวด์

คุณลักษณะเด่นของการประมวลผลแบบคลาวด์ คือมีรูปแบบการทำงานของคอมพิวเตอร์บนเครือข่ายที่ช่วยในเรื่องของความสะดวกสบายโดยที่ผู้ใช้งานสามารถเข้าถึงข้อมูลจากที่ใดก็ได้ มีการแบ่งปันทรัพยากรตามความต้องการใช้งานของผู้ใช้ (On-Demand Self Service) ต้องการการดูแลและบำรุงรักษาน้อย และมีความยืดหยุ่นทางด้านการใช้งานสูง

การประมวลผลแบบคลาวด์ สามารถแบ่งรูปแบบการให้บริการออกเป็น 3 รูปแบบ ได้แก่

1) การให้บริการซอฟต์แวร์ (SaaS : Software as a service) หมายถึง โมเดลของการให้บริการโปรแกรมประยุกต์ที่สามารถเข้าใช้งานร่วมกันและพร้อมกันได้ ซึ่งประเด็นสำคัญของการทำงานแบบ SaaS คือการลดต้นทุนของอุปกรณ์และซอฟต์แวร์ในการสร้าง การบำรุงรักษา และการใช้งาน ผู้ใช้บริการไม่จำเป็นต้องจัดการหรือควบคุมการทำงานของระบบ ยกเว้นการตั้งค่าบางอย่างหรือการกำหนดสิทธิในการเข้าถึงโปรแกรมประยุกต์

2) การให้บริการแพลตฟอร์ม (PaaS : Platform as a service) หมายถึง โมเดลของการให้บริการทางด้านแพลตฟอร์มที่สามารถให้ผู้ใช้พัฒนาโปรแกรมประยุกต์ได้ เพื่อให้ผู้พัฒนา (Developer) ทำการพัฒนาได้ง่ายและประหยัดค่าใช้จ่าย การให้บริการแพลตฟอร์มนั้นมีการสนับสนุนทางด้านซอฟต์แวร์ มิดเดิลแวร์ และฐานข้อมูล เป็นต้น

3) การให้บริการโครงสร้างพื้นฐาน (IaaS : Infrastructure as a service) หมายถึง โมเดลของการให้บริการที่ผู้ให้บริการจะให้บริการในส่วนของโครงสร้างพื้นฐานต่าง ๆ เช่น ฮาร์ดแวร์ และระบบเครือข่าย เป็นต้น ผู้ใช้บริการมีการจ่ายชำระค่าบริการตามการใช้งานจริง โดยผู้ให้บริการจะเป็นผู้ดูแลทางด้านการทำงานของโครงสร้างพื้นฐานและบำรุงรักษา

2.1.2 ความมั่นคงและความพึ่งพาได้

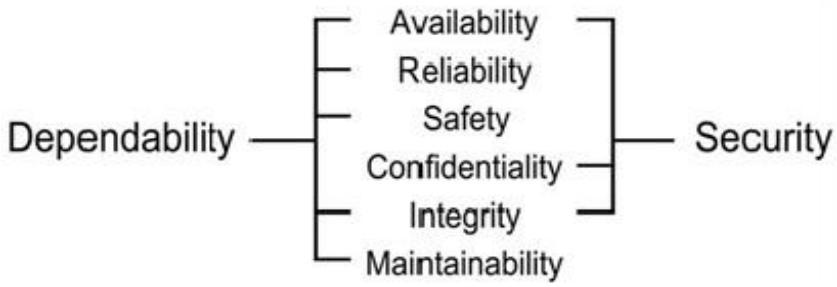
ความมั่นคง (Security) หมายถึง ความสามารถของระบบในการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต [3] หรือมีความสามารถในการป้องกันระบบสารสนเทศจากการปฏิสัมพันธ์ที่ไม่เป็นมิตรหรือจากการโจมตีระบบ เช่น ข้อมูล ฮาร์ดแวร์ และซอฟต์แวร์ ความมั่นคงแบ่งได้เป็น 3 อย่างคือ การรักษาความลับ (Confidential) บูรณภาพ (Integrity) และสภาพพร้อมใช้งาน (Availability) เรียกโดยย่อว่า CIA

ความพึ่งพาได้ (Dependability) หมายถึง ความสามารถในการทำงานที่เชื่อถือได้ [4] มีความสามารถในการทนต่อความผิดพร่อง (Fault Tolerance) ซึ่งเป็นความสามารถของระบบที่จะสามารถทำงานต่อไปได้ในสภาวะที่มีความเสียหายเกิดขึ้น และมีความสามารถในการหลีกเลี่ยงการทำงานที่ผิดพลาดที่มีความรุนแรงเกินกว่าจะยอมรับได้

The International Federation for Information Processing Group 10.4 [5] ได้กำหนดให้ความพึ่งพาได้ คือ “ความไว้ใจได้ (Trustworthiness) ของระบบคอมพิวเตอร์ ซึ่งจะช่วยให้เกิดการทำงานที่มีความน่าเชื่อถืออย่างมีเหตุผล (Dependability is the trustworthiness of a computing system which allows reliance to be justifiably placed on services it delivers.)”

การรักษาความมั่นคงจัดเป็นส่วนหนึ่งในคุณลักษณะของความพึ่งพาได้ โดยทั้ง 2 คุณลักษณะมีความเกี่ยวเนื่องกันดังภาพที่ 2.2 [4] ประกอบไปด้วยคุณลักษณะ 6 ประการ ดังนี้

1) สภาพพร้อมใช้งาน (Availability) หมายถึง ความพร้อมของการให้บริการ
2) ความเชื่อถือได้ (Reliability) หมายถึง ความต่อเนื่องของการให้บริการ
3) ความปลอดภัย (Safety) หมายถึง ระบบมีความปลอดภัย ไม่เกิดผลกระทบซึ่งเป็นอันตรายต่อผู้ใช้งานและสภาพแวดล้อม
4) การรักษาความลับ (Confidentiality) หมายถึง การรักษาความลับของข้อมูล
5) บูรณภาพ (Integrity) หมายถึง ไม่เกิดการเปลี่ยนแปลงของข้อมูลที่ไม่เหมาะสม
6) ความสามารถในการบำรุงรักษา (Maintainability) หมายถึง มีความสามารถในการซ่อมแซม



ภาพที่ 2.2 ความสัมพันธ์ของความมั่นคงและความพึ่งพาได้ [4]

2.1.3 เมตริกซ์ควบคุมคลาวด์

เมตริกซ์ควบคุมคลาวด์ (Cloud Control Matrix) เป็นเมตริกซ์ที่รวบรวมความต้องการด้านความมั่นคง 16 ด้าน เพื่อให้ผู้ให้บริการคลาวด์ใช้เป็นแนวปฏิบัติ [6] และช่วยให้ผู้ใช้บริการคลาวด์สามารถประเมินความเสี่ยงทางด้านความมั่นคงของผู้ให้บริการคลาวด์ เมตริกซ์ควบคุมคลาวด์นั้น จัดทำขึ้นโดยรวบรวมมาตรฐาน กฎระเบียบ และกรอบงานการควบคุม (Control Framework) ขององค์กรที่ภาคอุตสาหกรรมให้การยอมรับ ได้แก่ ISO 27001/27002, ISACA COBIT, PCI, AICPA, NIST, Jericho Forum และ NERC CIP

เมตริกซ์ควบคุมคลาวด์ (เวอร์ชัน 3.0.1) แบ่งออกเป็นทั้งหมด 16 โดเมนการควบคุม (Control Domain) ได้แก่

1. ความมั่นคงของโปรแกรมประยุกต์และส่วนต่อประสาน (Application & Interface Security)
2. การรับประกันและการปฏิบัติตามด้านการตรวจสอบ (Audit Assurance & Compliance)
3. การบริหารจัดการความต่อเนื่องทางธุรกิจและการคืนสภาพได้ของการปฏิบัติงาน (Business Continuity Management & Operational Resilience)
4. การควบคุมการเปลี่ยนแปลงและการจัดการโครงแบบ (Change Control & Configuration Management)
5. ความมั่นคงของข้อมูลและการบริหารจัดการวงจรชีวิตสารสนเทศ (Data Security & Information Lifecycle Management)
6. ความมั่นคงของศูนย์ข้อมูล (Datacenter Security)
7. การเข้ารหัสลับและการจัดการกุญแจ (Encryption & Key Management)
8. การกำกับดูแลและการจัดการความเสี่ยง (Governance and Risk Management)
9. ทรัพยากรบุคคล (Human Resources)
10. การระบุตัวตนและการจัดการการเข้าถึง (Identity & Access Management)
11. โครงสร้างพื้นฐานและความมั่นคงของเทคโนโลยีเสมือนจริง (Infrastructure & Virtualization Security)
12. ความสามารถในการทำงานร่วมกันและความสามารถในการเคลื่อนย้ายได้ (Interoperability & Portability)
13. ความมั่นคงของอุปกรณ์เคลื่อนที่ (Mobile Security)

14. การจัดการเหตุการณ์ด้านความมั่นคง การค้นพบแบบอิเล็กทรอนิกส์ และการตรวจสอบทางกฎหมายของคลาวด์ (Security Incident Management, E-Discovery & Cloud Forensics)
15. การจัดการห่วงโซ่อุปทาน ความโปร่งใส และความรับผิดชอบ (Supply Chain Management, Transparency and Accountability)
16. การจัดการภัยคุกคามและจุดอ่อน (Threat and Vulnerability Management)

แต่ละด้านยังแบ่งออกเป็นการควบคุมความมั่นคง (Security Control) ย่อย ๆ และแต่ละการควบคุมสอดคล้องกับการควบคุมความมั่นคงตามมาตรฐานต่างๆ เช่น มาตรฐาน SP800-53 ของ NIST และมาตรฐาน AICPA เป็นต้น

ตัวอย่างของเมตริกซ์ควบคุมคลาวด์แสดงในตารางที่ 2.1

ตารางที่ 2.1 ตัวอย่างเมตริกซ์ควบคุมคลาวด์ [6]

Control Domain	Control Domain ID	Control	Control ID	Control Specification
1.ความมั่นคงของโปรแกรมประยุกต์และส่วนต่อประสาน (Application & Interface Security)	AIS	Application Security	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.
2.การรับประกันและการปฏิบัติตามด้านการตรวจสอบ (Audit Assurance & Compliance)	AAC	Audit Planning	AAC-01	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.

ตารางที่ 2.1 ตัวอย่างเมตริกซ์ควบคุมคลาวด์ [6] (ต่อ)

Control Domain	Control Domain ID	Control	Control ID	Control Specification
3.การบริหารจัดการความต่อเนื่องทางธุรกิจและการคืนสภาพได้ของการปฏิบัติงาน (Business Continuity Management & Operational Resilience)	BCR	Business Continuity Planning	BCR-01	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant Dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities

ตารางที่ 2.1 ตัวอย่างเมตริกซ์ควบคุมคลาวด์ [6] (ต่อ)

Control Domain	Control Domain ID	Control	Control ID	Control Specification
4.การควบคุมการเปลี่ยนแปลงและการจัดการโครงแบบ (Change Control & Configuration Management)	CCC	New Development / Acquisition	CCC-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.
5.ความมั่นคงของข้อมูลและการบริหารจัดการวงจรชีวิตสารสนเทศ (Data Security & Information Lifecycle Management)	DSI	Classification	DSI-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.

ตารางที่ 2.1 ตัวอย่างเมตริกซ์ควบคุมคลาวด์ [6] (ต่อ)

Control Domain	Control Domain ID	Control	Control ID	Control Specification
6.ความมั่นคงของศูนย์ข้อมูล (Datacenter Security)	DCS	Classification	DCS-01	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.
7.การเข้ารหัสลับและการจัดการกุญแจ (Encryption & Key Management)	EKM	Entitlement	EKM-01	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.
8.การกำกับดูแลและการจัดการความเสี่ยง (Governance and Risk Management)	GRM	Baseline Requirements	GRM-01	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.

ตารางที่ 2.1 ตัวอย่างเมตริกซ์ควบคุมคลาวด์ [6] (ต่อ)

Control Domain	Control Domain ID	Control	Control ID	Control Specification
9.ทรัพยากรบุคคล (Human Resources)	HRS	Asset Returns	HRS-01	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.
10.การระบุตัวตนและการจัดการการเข้าถึง (Identity & Access Management)	IAM	Audit Tools Access	IAM-01	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.
11.โครงสร้างพื้นฐานและความมั่นคงของเทคโนโลยีเสมือนจริง (Infrastructure & Virtualization Security)	IVS	Audit Logging / Intrusion Detection	IVS-01	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network Behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.

ตารางที่ 2.1 ตัวอย่างเมตริกซ์ควบคุมคลาวด์ [6] (ต่อ)

Control Domain	Control Domain ID	Control	Control ID	Control Specification
12.ความสามารถในการทำงานร่วมกันและความสามารถในการเคลื่อนย้ายได้ (Interoperability & Portability)	IPY	APIs	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.
13.ความมั่นคงของอุปกรณ์เคลื่อนที่ (Mobile Security)	MOS	Anti-Malware	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.
14.การจัดการเหตุการณ์ด้านความมั่นคง การค้นพบแบบอิเล็กทรอนิกส์และการตรวจสอบทางกฎหมายของคลาวด์(Security Incident Management, E-Discovery & Cloud Forensics)	SEF	Contact / Authority Maintenance	SEF-01	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.

ตารางที่ 2.1 ตัวอย่างเมตริกซ์ควบคุมคลาวด์ [6] (ต่อ)

Control Domain	Control Domain ID	Control	Control ID	Control Specification
15.การจัดการห่วงโซ่อุปทาน ความโปร่งใส และความรับผิดชอบ (Supply Chain Management, Transparency and Accountability)	STA	Data Quality and Integrity	STA-01	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.
16.การจัดการภัยคุกคามและจุดอ่อน (Threat and Vulnerability Management)	TVM	Anti-Virus / Malicious Software	TVM-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.

2.1.4 คำถามการประเมินที่เป็นที่เห็นพ้องต้องกัน

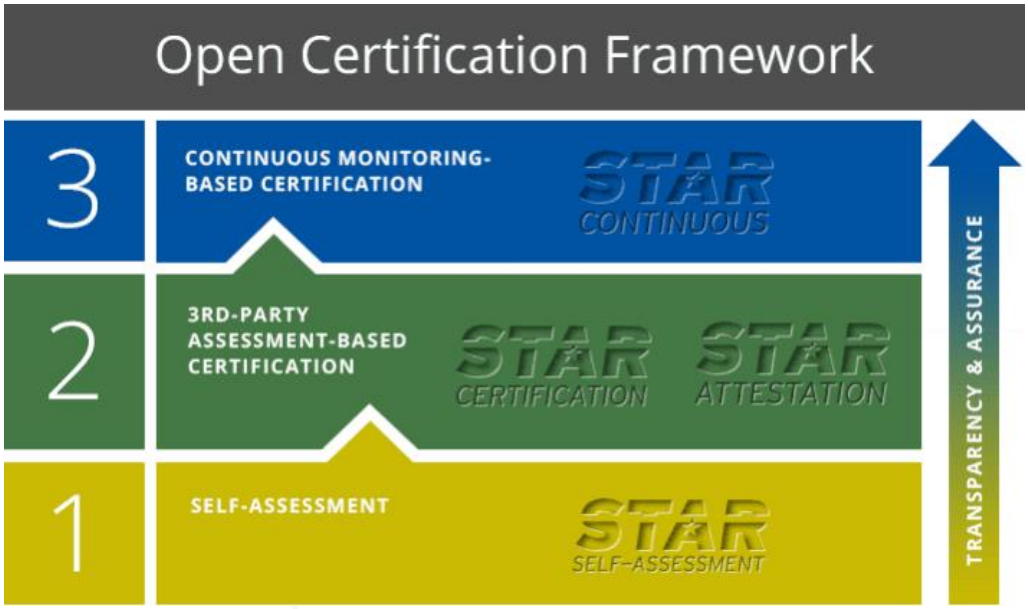
คำถามการประเมินที่เป็นที่เห็นพ้องต้องกัน (Consensus Assessment Initiative Questionnaire) หรือ CAIQ [7] เป็นชุดคำถามที่ผู้ใช้บริการและผู้ตรวจสอบคลาวด์ใช้ในการสอบถามผู้ให้บริการคลาวด์หรือให้ผู้ให้บริการใช้ในการประเมินตนเอง โดยเป็นการตอบคำถามในรูปแบบ “ใช่ (Yes)” หรือ “ไม่ใช่ (No)” CAIQ เป็นแบบสอบถามที่สอดคล้องกับการประเมินการควบคุมความมั่นคงที่ระบุไว้ในเมตริกซ์ควบคุมคลาวด์ ทั้ง 16 ด้าน จึงเป็นแนวทางให้กับผู้ให้บริการคลาวด์ใช้เป็นแนวปฏิบัติ และช่วยให้ผู้ใช้บริการคลาวด์และผู้ตรวจสอบคลาวด์สามารถประเมินความเสี่ยงทางด้านความมั่นคงของผู้ให้บริการคลาวด์ ดังตัวอย่างตามตารางที่ 2.2

ตารางที่ 2.2 ตัวอย่างคำถามใน CAIQ [7]

Control Group ID	Control ID	Consensus Assessment Questions
AIS-01	AIS-01.1	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?
	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?
AIS-02	AIS-02.1	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?

2.1.5 ซีเอสเอ สตาร์

ซีเอสเอ สตาร์ (CSA STAR) หรือชื่อเต็ม ๆ ว่า Cloud Security Alliance – Security, Trust & Assurance Registry คือทะเบียนสาธารณะทางด้านความมั่นคงและการรับประกันของผู้ให้บริการคลาวด์ [8] ซึ่งเปิดเผยแก่สาธารณะเพื่อเป็นประโยชน์แก่ผู้ใช้บริการ ผู้ให้บริการอุตสาหกรรม และหน่วยงานของรัฐบาลทั่วโลก STAR จะแบ่งการรับประกันออกเป็น 3 ระดับ โดยอิงกับงานวิจัยทั้ง 2 ชิ้นของซีเอสเอ ได้แก่ เมตริกซ์ควบคุมคลาวด์และคำถามการประเมินที่เป็นที่เห็นพ้องต้องกัน ดังภาพที่ 2.3



ภาพที่ 2.3 ระดับทั้ง 3 ระดับของ STAR [8]

ระดับที่ 1 การประเมินตนเอง (Self-Assessment)

การประเมินตนเอง คือ การที่ผู้ให้บริการคลาวด์ตอบคำถามตามแบบประเมิน CAIQ ว่าได้ปฏิบัติตามแนวปฏิบัติในเมตริกซ์ควบคุมคลาวด์หรือไม่ แล้วเปิดเผยแก่สาธารณะ แบบประเมินตนเองจะช่วยให้ผู้ใช้บริการทราบถึงลักษณะทางด้านความมั่นคงของผู้ให้บริการที่กำลังใช้บริการอยู่ หรือกำลังเลือกใช้บริการ ว่ามีลักษณะเป็นอย่างไร

ระดับที่ 2 การออกใบรับรอง (Certification)

การออกใบรับรองทำโดยการประเมินผู้ให้บริการโดยบุคคลที่ 3 โดยใช้มาตรฐาน ISO/IEC 27001:2005 ร่วมกับเมตริกซ์ควบคุมคลาวด์

ระดับที่ 3 การตรวจสอบอย่างต่อเนื่อง (Continuous Monitoring)

การตรวจสอบอย่างต่อเนื่องอยู่ในระหว่างการพัฒนาและจะเปิดให้ใช้งานภายในปี 2015 โดยจะมีระบบอัตโนมัติสำหรับตรวจสอบการปฏิบัติตามทางด้านความมั่นคงของผู้ให้บริการคลาวด์ในการให้บริการจริง ผู้ให้บริการคลาวด์จะเปิดเผยข้อมูลการปฏิบัติตามความมั่นคงในรูปแบบที่ซีเอสเอกำหนด

2.1.6 ความต้องการด้านความมั่นคงขั้นต่ำสำหรับสารสนเทศและระบบสารสนเทศของรัฐบาลกลาง

เอกสาร FIPS PUB 200 : Minimum Security Requirements for Federal Information and Information Systems [9] เป็นความต้องการขั้นพื้นฐานทางด้านความมั่นคงสำหรับสารสนเทศและระบบสารสนเทศของรัฐบาลกลางของสหรัฐอเมริกา ประกอบไปด้วย 17 ขอบเขตความมั่นคง

1) การควบคุมการเข้าถึง (Access Control : AC)
2) ความตระหนักและการฝึกอบรม (Awareness and Training : AT)
3) การตรวจสอบและความรับผิดชอบ (Audit and Accountability : AU)
4) การออกใบรับรอง การได้รับการรับรอง และการประเมินความมั่นคง (Certification, Accreditation, and Security Assessments : CA)
5) การจัดการโครงแบบ (Configuration Management : CM)
6) การวางแผนรับมือเหตุการณ์ที่อาจเกิดขึ้นได้ (Contingency Planning : CP)
7) การระบุตัวตนและการพิสูจน์ตัวจริง (Identification and Authentication : IA)
8) การตอบสนองต่อเหตุการณ์ (Incident Response : IR)
9) การบำรุงรักษา (Maintenance : MA)
10) การป้องกันสื่อ (Media Protection : MP)
11) การป้องกันทางด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Protection : PE)
12) การวางแผน (Planning : PL)
13) ความมั่นคงที่เกี่ยวข้องกับบุคลากร (Personnel Security : PS)
14) การประเมินความเสี่ยง (Risk Assessment : RA)
15) การได้มาซึ่งระบบและบริการ (System and Services Acquisition : SA)
16) การป้องกันระบบและการสื่อสาร (System and Communications Protection : SC)
17) บูรณภาพของสารสนเทศ (System and Information Integrity : SI)

ภายในขอบเขตความมั่นคงทั้ง 17 ด้าน ในแต่ละด้านนั้นจะแบ่งความมั่นคงออกเป็นหัวข้อย่อยตามที่ระบุไว้ในมาตรฐาน NIST SP800-53 [10] ยกตัวอย่างเช่น การควบคุมการเข้าถึง Access Control ใช้รหัสย่อคือ AC จะแบ่งออกเป็นการควบคุมความมั่นคงย่อย ๆ อีกหลายข้อ เช่น AC-1, AC-2, AC-3 เป็นต้น ดังภาพที่ 2.4 และในข้อย่อยยังมีการแบ่งย่อยลงไปอีก เช่น AC-2 มีการแบ่งออกเป็น AC-2 (1), AC-2 (2), AC-2 (3) เป็นต้น เครื่องหมายกากบาทจะแสดงถึงการควบคุมความมั่นคงขั้นต่ำ (Control Baseline) ที่ควรดำเนินการสำหรับระบบสารสนเทศประเภทต่างๆ ได้แก่ ระบบที่มีผลกระทบมาก (High Impact System) ระบบที่มีผลกระทบปานกลาง (Moderate Impact System) และระบบที่มีผลกระทบน้อย (Low Impact System) โดยที่การแบ่งประเภทระบบจะเป็นไปตามผลกระทบที่จะเกิดแก่องค์กรว่ามีมาก ปานกลาง หรือน้อย หากระบบนั้นเกิดการสูญเสียการรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน [11] นอกจากนี้การควบคุมความมั่นคงบางรายการจะมีเครื่องหมายกากบาทที่ Assurance แสดงว่าเป็นการควบคุมที่เกี่ยวข้องกับการรับประกัน (Assurance Related Control) ซึ่งหมายถึงการควบคุมที่เป็นมาตรการที่ทำให้เกิดความเชื่อมั่นว่า ระบบมีฟังก์ชันทางด้านความมั่นคงที่ถูกต้องและทำงานตามที่ควรเป็นจริงๆ โดยจะเป็นการควบคุมที่เกี่ยวข้องกับ

1) กระบวนการ วิธีการ หรือเทคนิคในการออกแบบและพัฒนาส่วนต่างๆของระบบ

2) กระบวนการทำงานที่เป็นการปรับปรุงคุณภาพในส่วนต่างๆของระบบ

3) กิจกรรมที่ก่อให้เกิดหลักฐานด้านความมั่นคง (Security Evidence) จากการทำงาน

4) การประเมินประสิทธิภาพหรือความเสี่ยงของการควบคุมความมั่นคงที่ได้ปฏิบัติ หรือ

5) การเพิ่มทักษะความเชี่ยวชาญ ความเข้าใจ ในด้านความมั่นคงให้แก่บุคลากรที่เกี่ยวข้อง

ตัวอย่างเช่น การควบคุมความมั่นคง AC-1 เป็นการควบคุมที่เกี่ยวข้องกับการรับประกัน เพราะกล่าวถึงการพัฒนาการจัดทำเอกสารและการเผยแพร่ให้ผู้ที่เกี่ยวข้อง ในเรื่องของนโยบายและกระบวนงานด้านการควบคุมการเข้าถึงระบบ (Access Control Policy and Procedures) ส่วนการควบคุมที่ไม่มีเครื่องหมายกากบาทที่ Assurance จะเป็นการควบคุมที่เกี่ยวข้องกับฟังก์ชันงานด้านความมั่นคง (Functionality-Related Control)

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-1	**Access Control Policy and Procedures**		X	X	X	X
AC-2	**Account Management**			X	X	X
AC-2(1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*				X	X
AC-2(2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*				X	X
AC-2(3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*				X	X
AC-2(4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*				X	X
AC-2(5)	*ACCOUNT MANAGEMENT | INACTIVITY LOGOUT*					X
AC-2(6)	*ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT*					
AC-2(7)	*ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES*					
AC-2(8)	*ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION*					
AC-2(9)	*ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS*					
AC-2(10)	*ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION*					
AC-2(11)	*ACCOUNT MANAGEMENT | USAGE CONDITIONS*					X
AC-2(12)	*ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE*					X
AC-2(13)	*ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS*					X
AC-3	**Access Enforcement**			X	X	X

ภาพที่ 2.4 ตัวอย่างรายการการควบคุมความมั่นคงของ NIST SP800-53 [10]

คุณภาพของการควบคุมที่เกี่ยวข้องกับการรับประกันจะพิจารณาจากทั้งความลึก (Depth) และความครอบคลุม (Coverage) ของการดำเนินการตามการควบคุมนั้น ซึ่งดูได้จากหลักฐานต่างๆ จากการควบคุม เช่น สิ่งที่เป็นผลผลิตจากการออกแบบและพัฒนาระบบ ผลการประเมิน ใบรับรอง เป็นต้น ส่วนคุณภาพของการควบคุมที่เกี่ยวข้องกับฟังก์ชันงานด้านความมั่นคงจะพิจารณาจากความเข้มแข็ง (Strength) ของการดำเนินงาน ซึ่งดูได้จากการที่ระบบมีการดำเนินงานตามนโยบายที่ดี มีการออกแบบอย่างเป็นระบบเป็นไปตามหลักการความมั่นคง มีการทดสอบ มีการรายงานปัญหาและการแก้ไข มีการเฝ้าสังเกต และทำตามกฎหมายและมาตรฐานที่เกี่ยวข้อง ทั้งนี้การควบคุมบางรายการอาจเกี่ยวข้องกับทั้งการรับประกันและฟังก์ชันงานด้านความมั่นคง

2.1.7 หลักการและเกณฑ์การให้บริการที่ไว้ใจได้ของสมาคมผู้สอบบัญชีรับอนุญาตแห่งสหรัฐอเมริกา

หลักการและเกณฑ์การให้บริการที่ไว้ใจได้ของสมาคมผู้สอบบัญชีรับอนุญาตแห่งสหรัฐอเมริกา (AICPA Trust Service Principle and Criteria) [12] เป็นหลักเกณฑ์แนวปฏิบัติทางด้านความมั่นคงของระบบสารสนเทศ สำหรับใช้ในการรับรอง ตรวจสอบและรายงานผลทางด้านความมั่นคงของระบบสารสนเทศ ซึ่งแบ่งเกณฑ์ออกเป็น 5 ด้านได้แก่

1) ด้านความมั่นคง (Security)
2) ด้านการรักษาความลับ (Confidentiality)
3) ด้านบูรณภาพ (Integrity)
4) ด้านสภาพพร้อมใช้งาน (Availability)
5) ด้านความเป็นส่วนตัว (Privacy)

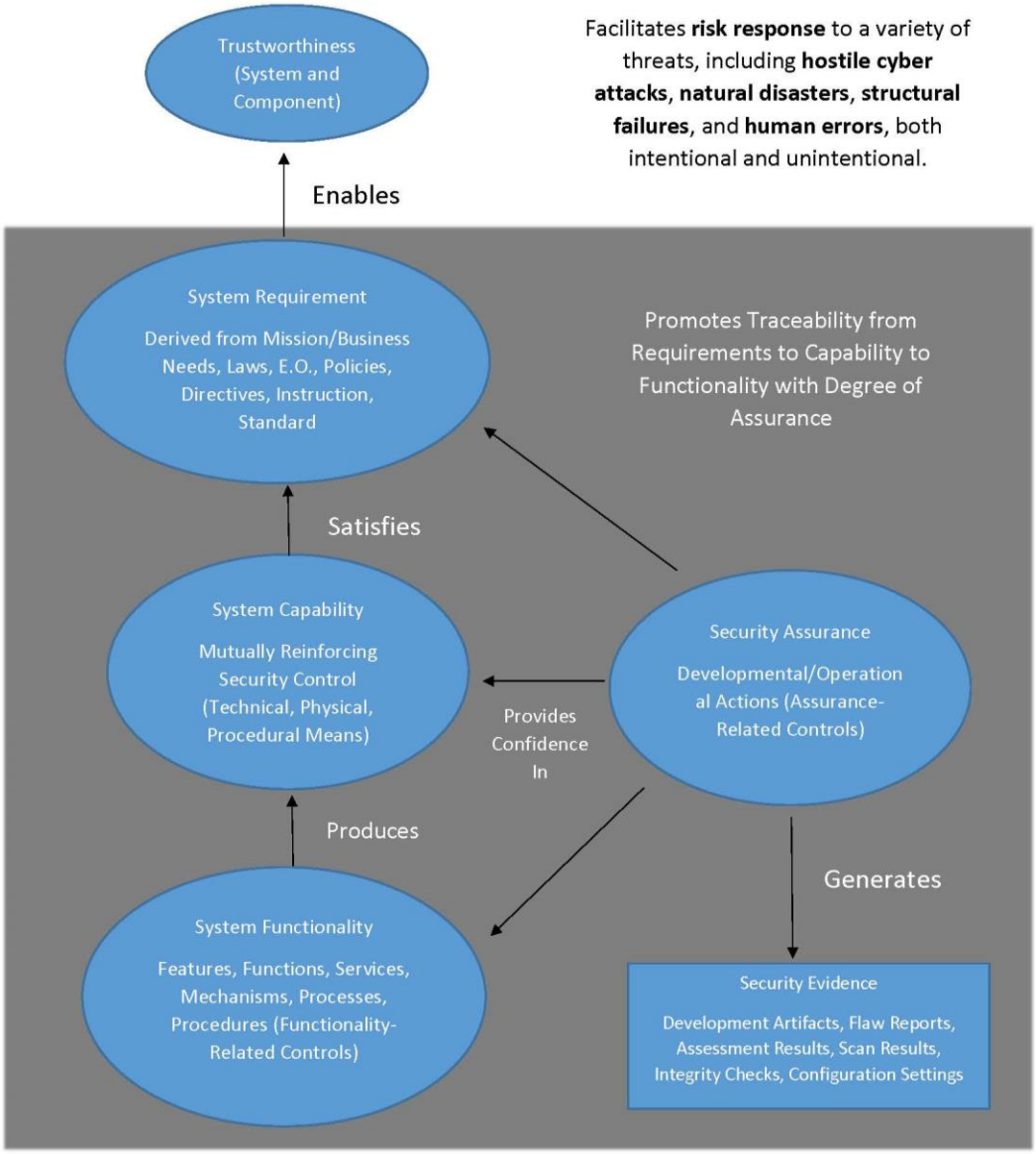
2.1.8 ความไว้ใจได้

ความไว้ใจได้ (Trustworthiness) [10] ในความหมายโดยทั่วไปจะหมายถึงความเชื่อ (Belief) ว่าเอนทิตีจะมีพฤติกรรมที่สามารถคาดการณ์ได้ ในขณะที่กำลังทำงานบางอย่างภายใต้สภาพแวดล้อมและเงื่อนไขที่กำหนดไว้ ซึ่งเอนทิตีอาจหมายถึงบุคคล กระบวนการ ระบบ ส่วนของระบบ หรือหลายอย่างเหล่านี้ร่วมกัน

ในระบบสารสนเทศ ความไว้ใจได้จะแสดงถึงระดับของการรักษาไว้ซึ่งการรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งานของสารสนเทศในขณะที่กำลังถูกประมวลผล จัดเก็บ และเคลื่อนย้ายแม้ว่าระบบจะมีภัยคุกคาม เช่น การขัดขวางการทำงาน ความผิดพลาดของมนุษย์ ความล้มเหลวของส่วนต่างๆในระบบ หรือการโจมตีจากภายนอก ระบบยังสามารถทนต่อภัยคุกคามเหล่านี้และยังสามารถทำงานได้สำเร็จลุล่วงตามภารกิจที่ได้รับมอบหมาย

ภาพที่ 2.5 แสดงแบบจำลองความไว้ใจได้ (Trustworthiness Model) สององค์ประกอบพื้นฐานที่ทำให้ระบบไว้ใจได้คือ ฟังก์ชันงานด้านความมั่นคง (Security Functionality) และการรับประกันด้านความมั่นคง (Security Assurance) ฟังก์ชันงานด้านความมั่นคงหมายถึงการควบคุมที่เกี่ยวข้องกับฟังก์ชัน กลไก บริการ กระบวนงาน และสถาปัตยกรรมด้านความมั่นคงที่พัฒนาในระบบ สิ่งเหล่านี้ก่อให้เกิดความสามารถด้านความมั่นคง (Security Capability) ของระบบ ความสามารถนี้จะตอบสนองต่อความต้องการด้านความมั่นคงของผู้ใช้ระบบ และเมื่อความต้องการได้รับการตอบสนองแล้วจะทำให้ผู้ใช้เกิดความไว้ใจในตัวระบบ องค์ประกอบพื้นฐานอีกอย่างหนึ่งซึ่งก็คือ การรับประกันด้านความมั่นคงนั้น หมายถึง การควบคุมที่ก่อให้เกิดความเชื่อมั่นว่า ฟังก์ชันงานด้านความมั่นคงนั้นดำเนินไปอย่างถูกต้องเหมาะสม ระบบมีความสามารถด้านความมั่นคงและตอบสนองความ

ต้องการได้จริง ในการรับประกันด้านความมั่นคงจะมีการสร้างผลผลิตต่างๆของการทำงานตามการควบคุม ซึ่งจะใช้เป็นหลักฐานในการรับประกัน



ภาพที่ 2.5 แบบจำลองความไว้ใจได้ [10]

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง

ในงานวิจัยของ Habib, Varadharajan และ Muhlhauser [13] ได้นำเสนอกรอบงานความไว้วางใจ (Trust-aware Framework) เพื่อทำการวิเคราะห์และประเมินค่าความไว้ใจได้ของผู้ให้บริการคลาวด์ จากข้อมูลการประเมินตนเองตามข้อคำถามใน CAIQ ซึ่งได้ประกาศไว้กับ STAR งานวิจัยนี้ ได้ทำการวิเคราะห์ว่า การควบคุมความมั่นคงแต่ละข้อในเมตริกซ์ควบคุมคลาวด์ซึ่ง CAIQ อ้างอิงถึงนั้น มีคุณสมบัติการไว้วางใจ (Trust Properties) เป็นแบบใด และมีการแยกประเภทการตรวจสอบความสมเหตุสมผล (Validate) ว่าผู้ให้บริการมีคุณสมบัตินั้นๆหรือไม่ ออกเป็น 3 ประเภท ได้แก่

1) การรับรองโดยบุคคลที่ 3 (Third Party Certified)
2) การรับรองโดยผู้ให้บริการเอง แต่มีกระบวนการตรวจสอบแบบที่บุคคลที่ 3 ใช้ (Self-Certified)
3) การอ้างโดยผู้ให้บริการเอง (Self-Claim)

Habib, Varadharajan และ Muhlhauser ได้ทำการสร้างแบบจำลองการตัดสินใจ ซึ่งมีพื้นฐานอยู่บนภาษาตรรกศาสตร์ที่ชื่อว่า ALOPA และ Certainlogic คุณสมบัติความไว้วางใจต่างๆที่ผู้ให้บริการประกาศว่ามีอยู่ใน STAR จะถูกแปลงเป็นกฎความสัมพันธ์ เพื่อนำไปตรวจสอบกับความต้องการของผู้ใช้บริการ การตรวจสอบจะพิจารณาทั้งในแง่ของ Hard Trust ซึ่งเป็นความไว้วางใจที่ได้มาจากการตรวจสอบกลไกด้านความมั่นคงโดยตรง เช่น การตรวจสอบคุณสมบัติจากใบรับรองต่างๆ และในแง่ของ Soft Trust ซึ่งเป็นความไว้วางใจที่ได้มาโดยอ้อมจากการพิจารณาประสบการณ์และพฤติกรรมของผู้ให้บริการหรือหน่วยงานที่เกี่ยวข้องกับการให้บริการ

ในงานวิจัยของ Bedi, Kuar และ Gupta [14] ได้นำเสนอวิธีการเลือกผู้ให้บริการระบบประมวลผลแบบคลาวด์ที่ไว้ใจได้ โดยใช้วิธีวัดจากชื่อเสียง (Reputation) และการแนะนำที่เชื่อถือได้จากบุคคลที่เคยใช้บริการระบบประมวลผลแบบคลาวด์นั้น ๆ ซึ่งผลลัพธ์ที่ได้สามารถยืนยันได้ว่า ระบบการเลือกผู้ให้บริการระบบการประมวลผลแบบคลาวด์ที่ไว้ใจได้นั้น มีประสิทธิภาพและเป็นระบบที่ช่วยประมาณค่าความเชื่อมั่นของผู้ให้บริการคลาวด์ได้เป็นอย่างดี

บทความของ Bret Michael [15] และงานวิจัยของ Sun Microsystems, Inc. [16] ให้ความสำคัญกับประเด็นความไว้วางใจและความโปร่งใสของคลาวด์ โดย Bret Michael ตั้งคำถามถึงปริมาณข้อมูลที่ใช้ในการประเมินความโปร่งใส ว่าต้องมีข้อมูลเท่าไรถึงจะเพียงพอ และมุ่งเน้นให้ผู้ให้บริการคลาวด์ให้ความสำคัญกับการสร้างความไว้วางใจแก่ผู้ใช้บริการคลาวด์

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

1) ควรเปิดเผยข้อมูลและแนวทางปฏิบัติด้านการรักษาความมั่นคง
2) ควรเปิดเผยข้อมูลตามคำสั่งหรือข้อตกลง เช่น ข้อมูลตามบัญญัติกฎหมายหรือตามที่บัญญัติไว้ในองค์กรว่าต้องมีการเปิดเผย
3) ควรเปิดเผยข้อมูลด้านสถาปัตยกรรมความมั่นคง
4) ควรเปิดเผยหน้าที่ความรับผิดชอบของผู้ให้บริการคลาวด์ต่อผู้ใช้บริการคลาวด์อย่างชัดเจน
5) ไม่ควรเปิดเผยข้อมูลที่จะทำให้เกิดความเสี่ยงต่อศูนย์ข้อมูล (Data Center) เช่น ข้อมูลการเข้าถึงฐานข้อมูลที่อยู่ภายในศูนย์ข้อมูล
6) ไม่ควรเปิดเผยข้อมูลที่จะเป็นอันตรายต่อผู้ใช้บริการคลาวด์หรือผู้เกี่ยวข้อง เช่น ข้อมูลส่วนตัวของผู้ใช้บริการคลาวด์หรือผู้เกี่ยวข้อง
7) ไม่ควรเปิดเผยข้อมูลที่ไม่เหมาะสมเกี่ยวกับการแสดงความรับผิดชอบของผู้ให้บริการคลาวด์ เช่น การเปิดเผยข้อมูลระดับความมั่นคงที่สูงเกินกว่าผู้ให้บริการคลาวด์จะรับผิดชอบได้
8) ไม่ควรเปิดเผยข้อมูลที่ผิดกฎหมายหรือกฎบัญญัติ เช่น การส่งผ่านข้อมูลออกนอกสหภาพยุโรปเป็นการกระทำที่ผิดตามข้อตกลงของสหภาพยุโรป

อย่างไรก็ตามงานวิจัยทั้งสอง ได้เสนอเพียงแนวคิดและหลักการเท่านั้น แต่ไม่ได้นำไปสู่วิธีการประเมินหรือชี้วัดค่าความมั่นคงของการให้บริการคลาวด์

ในงานวิจัยของ Pumvarapruek และ Senivongse [17] ได้นำเสนอระบบสนับสนุนผู้ใช้บริการคลาวด์ในการประเมินเพื่อตัดสินใจเลือกผู้ให้บริการคลาวด์ โดยพิจารณาเฉพาะความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงของผู้ให้บริการคลาวด์จากเมตริกซ์ควบคุมคลาวด์ และแบบสอบถาม CAIQ แล้วนำมาสร้างออนโทโลจีความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ เพื่อให้สามารถนำมาใช้ในการจำแนกคำศัพท์ที่สกัดมาจากหน้าเว็บของผู้ให้บริการคลาวด์ ว่ามีความสอดคล้องกับความต้องการด้านความมั่นคงตามที่ระบุในเมตริกซ์ควบคุมคลาวด์ในด้านใดบ้างและในระดับใด ผู้ใช้สามารถเปรียบเทียบผู้ให้บริการคลาวด์ที่แตกต่างกันเพื่อตัดสินใจเลือกใช้บริการที่มีความมั่นคงในระดับที่เหมาะสมกับลักษณะขององค์กรผ่านระบบที่พัฒนาขึ้นได้

ในงานวิจัยของ Bhensook และ Senivongse [18] ได้นำเสนอระบบที่ช่วยผู้ใช้บริการคลาวด์ในการประเมินเพื่อตัดสินใจเลือกผู้ให้บริการคลาวด์ โดยพิจารณาเฉพาะความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงของผู้ให้บริการคลาวด์จากเมตริกซ์ควบคุมคลาวด์ และคำถาม CAIQ จากนั้นวิเคราะห์

หาตัววัดความมั่นคงของผู้ให้บริการคลาวด์โดยใช้วิธีจีคิวเอ็ม (Goal Question Metric: GQM) แล้วคำนวณคะแนนความมั่นคงจากหลักฐานที่ผู้ให้บริการคลาวด์แสดงไว้และสอดคล้องกับตัววัดที่กำหนด

ในงานวิจัยของ Mayayise และ Osunmakinde [19] ได้นำเสนอโมเดลการรับประกันสำหรับใช้ประเมินความไว้ใจได้ของระบบการค้าอิเล็กทรอนิกส์ (E-Commerce) ที่ทำงานบนคลาวด์ โดยใช้ประเด็นความไว้ใจได้ของเว็บไซต์เป็นสำคัญ ซึ่งตรวจสอบจากคุณลักษณะต่างๆ ได้แก่ การปฏิบัติตามกฎหมาย มาตรฐานไอเอสโอ นโยบาย กลไกความมั่นคงที่ใช้ และสภาพพร้อมใช้งานของเว็บไซต์ โมเดลการรับประกันคำนวณคะแนนความไว้ใจได้โดยใช้กระบวนการลำดับชั้นเชิงวิเคราะห์ (Analytic Hierarchy Process) ร่วมกับอัลกอริทึมการจัดลำดับหน้าเว็บ (Page Ranking) และทำการแสดงผลบนหน้าเว็บไซต์เพื่อเป็นแนวทางแนะนำให้กับผู้ใช้บริการในเรื่องของความไว้ใจได้ของเว็บไซต์ผู้ให้บริการ

โดยสรุปแล้วงานวิจัยที่เกี่ยวข้องต่างให้ความสำคัญกับความโปร่งใสด้านความมั่นคงของผู้ให้บริการและใช้ข้อมูลด้านความมั่นคงของผู้ให้บริการซึ่งเปิดเผยอยู่ในการประเมินความสามารถด้านความมั่นคง แต่ใช้วิธีการที่แตกต่างกันในการประเมิน และมีข้อดีข้อด้อยแตกต่างกัน สรุปได้ดังตารางที่ 2.3

ตารางที่ 2.3 สรุปงานวิจัยด้านการประเมินความมั่นคงของผู้ให้บริการคลาวด์

ผู้วิจัย	ประเด็นในงานวิจัย	แนวคิดของงานวิจัย	ปัญหาของงานวิจัย
Habib S., Varadharajan V., Muhlhauser M	สร้างกรอบงานในการประเมินความไว้วางใจของผู้ให้บริการคลาวด์	แปลงข้อมูลการประเมินตนเองของผู้ให้บริการที่บันทึกใน STAR เป็นกฎความสัมพันธ์ เพื่อนำไปตรวจสอบกับความต้องการของผู้ใช้บริการ	การแปลงข้อมูลใน STAR ไปเป็นกฎความสัมพันธ์มีความซับซ้อน และยังไม่แสดงการนำข้อมูลจริงจากผู้ให้บริการคลาวด์มาทำการประเมิน
Bedi P., Kuar H., Gupta B	สร้างโมเดลความไว้ใจได้ของผู้ให้บริการคลาวด์	ใช้การคำนวณจากชื่อเสียงและการแนะนำจากบุคคลที่ไว้ใจได้ที่เคยใช้คลาวด์นั้นๆ	คะแนนจากการแนะนำจากบุคคลที่เคยใช้คลาวด์นั้นไม่มีมาตรฐานกำหนดที่ชัดเจน
Bret Michael, Sun Microsystems, Inc.,	การประเมินความโปร่งใสของการให้บริการคลาวด์	หลักการพิจารณาความโปร่งใส	เป็นเพียงแนวคิด

ตารางที่ 2.3 สรุปงานวิจัยด้านการประเมินความมั่นคงของผู้ให้บริการคลาวด์ (ต่อ)

ผู้วิจัย	ประเด็นในงานวิจัย	แนวคิดของงานวิจัย	ปัญหาของงานวิจัย
Pumvarapruek, N. and T. Senivongse	ระบบสนับสนุนผู้ใช้บริการคลาวด์ในการประเมินเพื่อตัดสินใจเลือกผู้ใช้บริการคลาวด์	สร้างออนโทโลจีความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ เพื่อนำมาใช้ในการจำแนกคำศัพท์ที่สกัดมาจากหน้าเว็บของผู้ให้บริการคลาวด์ ว่าปฏิบัติตามเมตริกซ์ควบคุมคลาวด์ในระดับใด	เว็บไซต์ของผู้ให้บริการไม่มีข้อมูลทางด้านความมั่นคงที่เพียงพอ ซึ่งข้อมูลบางอย่างเป็นข้อมูลที่ไม่เปิดเผย หรือบางผู้ให้บริการไม่ได้ลงข้อมูลบนหน้าเว็บไซต์ให้ครบถ้วน
Bhensook, N. and T. Senivongse	ระบบที่ช่วยผู้ใช้บริการคลาวด์ในการประเมินเพื่อตัดสินใจเลือกผู้ให้บริการคลาวด์	พิจารณาเฉพาะความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงของผู้ให้บริการคลาวด์ และนำมาวิเคราะห์โดยใช้วิธีจีคิวเอ็ม โดยมีการให้คะแนนหลักฐาน โดยให้คะแนนจากคุณภาพและปริมาณของหลักฐาน	การประเมินทำได้ยากและไม่เป็นอัตโนมัติ เนื่องจากต้องอาศัยหลักฐานจากผู้ให้บริการคลาวด์ เพื่อตรวจสอบว่าผู้ให้บริการคลาวด์ได้ทำตามเมตริกซ์ควบคุมคลาวด์และคำถามซึ่งปรับมาจาก CAIQ หรือไม่
Mayayise, T. O. and I. O. Osunmakinde	โมเดลการรับประกันสำหรับประเมินความไว้ใจได้ของระบบการค้าอิเล็กทรอนิกส์ที่ทำงานบนคลาวด์	พิจารณาคุณลักษณะหลากหลายด้านของคลาวด์ และใช้อัลกอริทึมในการจัดลำดับเว็บไซต์และกระบวนการลำดับชั้นเชิงวิเคราะห์ในการประเมินความไว้ใจได้ของผู้ให้บริการคลาวด์	ไม่มีเกณฑ์การให้คะแนนที่ชัดเจนของคุณลักษณะในแต่ละด้าน

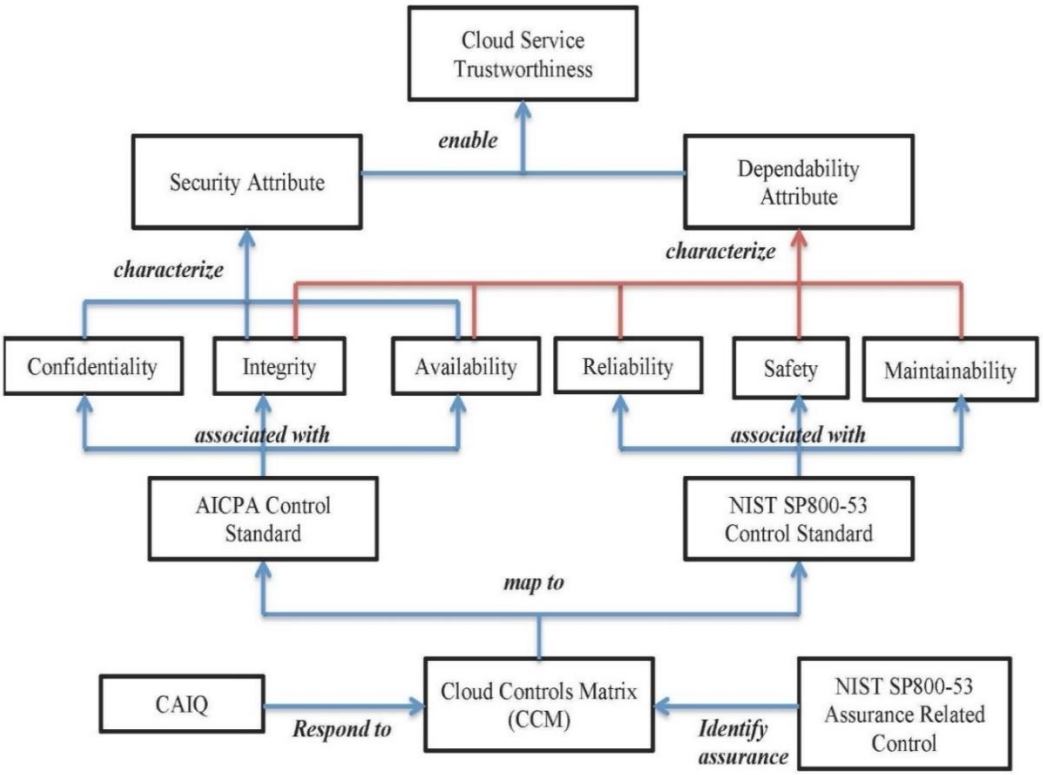
บทที่ 3
การประเมินความไว้ใจได้ของผู้ให้บริการโดยอิงเมตริกซ์ควบคุมคลาวด์

ภาพรวมของการประเมินความไว้ใจได้ของผู้ให้บริการคลาวด์แสดงดังภาพที่ 3.1 โดยตั้งอยู่บนพื้นฐานของการนำเอาคุณลักษณะทางด้านความมั่นคง (Security) และความพึ่งพาได้ (Dependability) ทั้ง 6 คุณลักษณะย่อย ได้แก่ การรักษาความลับ (Confidentiality) บูรณภาพ (Integrity) สภาพพร้อมใช้งาน (Availability) ความเชื่อถือได้ (Reliability) ความปลอดภัย (Safety) และความสามารถในการบำรุงรักษา (Maintainability) ดังที่กล่าวไว้ในหัวข้อที่ 2.1.2 มาเป็นองค์ประกอบในการประเมินคุณลักษณะความไว้ใจได้ (Trustworthiness) ของผู้ให้บริการคลาวด์ ซึ่งผู้วิจัยเล็งเห็นว่าการควบคุมความมั่นคง (Security Control) ในเมตริกซ์ควบคุมคลาวด์ (Cloud Control Matrix) สามารถสะท้อนถึงคุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้ทั้ง 6 คุณลักษณะย่อย โดยใช้มาตรฐานการควบคุมความมั่นคงของ NIST SP800-53 Control Standard และ AICPA Control Standard [6] ซึ่งเชื่อมโยงอยู่กับเมตริกซ์ควบคุมคลาวด์เป็นตัวจำแนก โดยผู้วิจัยจะนำเอาคำตอบจากผู้ให้บริการคลาวด์ซึ่งได้ทำแบบประเมินคำถามซึ่งเป็นที่เห็นพ้องต้องกัน (CAIQ) ร่วมกับค่าน้ำหนักของการควบคุมที่เกี่ยวข้องกับการรับประกัน (Assurance Related-Control) ของมาตรฐาน NIST SP800-53 ซึ่งเชื่อมโยงอยู่กับเมตริกซ์ควบคุมคลาวด์ มาทำการหาค่าคะแนนความไว้ใจได้ของผู้ให้บริการคลาวด์

ขั้นตอนการประเมินความไว้ใจได้ของผู้ให้บริการประกอบด้วย

1) ขั้นตอนการกำหนดเกณฑ์ในการเชื่อมโยงคุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้กับเมตริกซ์ควบคุมคลาวด์
2) ขั้นตอนการเชื่อมโยงคุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้กับเมตริกซ์ควบคุมคลาวด์
3) ขั้นตอนการสร้างเมตริกซ์คุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้ของโดเมนการควบคุม
4) ขั้นตอนการหาค่าน้ำหนักของการควบคุมที่เกี่ยวข้องกับการรับประกันของโดเมนการควบคุมของเมตริกซ์ควบคุมคลาวด์

5) ขั้นตอนการคำนวณคะแนนการปฏิบัติตาม CAIQ ของผู้ให้บริการคลาวด์ในแต่ละโดเมนการควบคุม
6) ขั้นตอนการสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของผู้ให้บริการคลาวด์ในแต่ละโดเมนการควบคุม
7) ขั้นตอนการประเมินความไว้ใจได้ของผู้ให้บริการคลาวด์
8) การพัฒนาระบบสนับสนุนการประเมินความไว้ใจได้ของผู้ให้บริการโดยอิงเมตริกซ์ควบคุมคลาวด์



ภาพที่ 3.1 ภาพรวมของงานวิจัย

3.1 ขั้นตอนการกำหนดเกณฑ์ในการเชื่อมโยงคุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้กับเมตริกซ์ควบคุมคลาวด์

ในขั้นตอนนี้จะเป็นการกำหนดเกณฑ์ในการเชื่อมโยงคุณลักษณะด้านความมั่นคงและความพึ่งพาได้เข้ากับเมตริกซ์ควบคุมคลาวด์ การกำหนดเกณฑ์เริ่มจากการทำความเข้าใจนิยามและวิธีการให้ได้มาซึ่งคุณลักษณะย่อยทั้ง 6 ประการของความมั่นคงและความพึ่งพาได้ โดยนิยามและวิธีการของคุณลักษณะย่อยทั้ง 6 ประการ ผู้วิจัยได้ทำการรวบรวมจากงานวิจัยที่เกี่ยวข้อง หนังสือ และเอกสารทางวิชาการ [3, 4, 20-27] โดยผู้วิจัยจะพิจารณาจากนิยาม คำศัพท์และวิธีการของคุณลักษณะย่อยในแต่ละด้าน ในตารางที่ 3.1 เป็นเกณฑ์ในการวิเคราะห์ว่ามาตรฐานการควบคุมทางด้านความมั่นคง คือ NIST SP800-53 และ AICPA ซึ่งเชื่อมโยงเข้ากับเมตริกซ์ควบคุมคลาวด์ แต่ละข้อเกี่ยวข้องกับนิยามหรือวิธีการของคุณลักษณะย่อยด้านใด

ตารางที่ 3.1 เกณฑ์ในการเชื่อมโยงคุณลักษณะด้านความมั่นคงและความพึ่งพาได้กับมาตรฐานการควบคุมทางด้านความมั่นคง NIST และ AICPA

Security and Dependability Attribute	Criteria	
	Characteristic	Method
Confidentiality	Confidentiality is an ability of a computing system or service to prevent disclosure of information to unauthorized parties [3]. Confidentiality is roughly equivalent to privacy.	1. Encryption for data at rest (whole disk, database encryption) 2. Encryption for data in transit (IPSec, SSL, PPTP, SSH) 3. Access control (physical and technical) 4. Cryptography 5. Authentication 6. Authorization 7. Verification 8. Biometric 9. Password Protection 10. Two Factor Authentication [20].

ตารางที่ 3.1 เกณฑ์ในการเชื่อมโยงคุณลักษณะด้านความมั่นคงและความพึ่งพาได้กับมาตรฐานการควบคุมทางด้านความมั่นคง NIST และ AICPA (ต่อ)

Security and Dependability Attribute	Criteria	
	Characteristic	Method
Integrity	Integrity is an ability of a computing system or service to avoid the transition of incorrect data [4] and have the ability to make the data faultless and prevent unauthorized modification or deletion [21].	1. Hashing (data integrity) 2. Configuration management (system integrity) 3. Change control (process integrity) 4. Access control (physical and technical) 5. Privileged Access 6. Software digital signing 7. Transmission CRC functions 8. Permission 9. Consistency 10. Accuracy 11. Version Control 11. Checksum [20].

ตารางที่ 3.1 เกณฑ์ในการเชื่อมโยงคุณลักษณะด้านความมั่นคงและความพึ่งพาได้กับมาตรฐานการควบคุมทางด้านความมั่นคง NIST และ AICPA (ต่อ)

Security and Dependability Attribute	Criteria	
	Characteristic	Method
Availability	Availability is an ability of a computing system or service to be ready to use [4]. It can be described as the probability that the system will be available at a certain instant in time [3]. Availability is the degree to which a system, subsystem or equipment is in a specified operable and committable state at the start of a mission.	1. Redundant array of inexpensive disks (RAID) 2. Clustering 3. Load balancing 4. Redundant data and power lines 5. Software and data backups 6. Disk shadowing 7. Co-location and off-site facilities 8. Roll-back functions 9. Fail-over configurations 10. Redundancy 11. Replication [20].

ตารางที่ 3.1 เกณฑ์ในการเชื่อมโยงคุณลักษณะด้านความมั่นคงและความพึ่งพาได้กับมาตรฐานการควบคุมทางด้านความมั่นคง NIST และ AICPA (ต่อ)

Security and Dependability Attribute	Criteria	
	Characteristic	Method
Reliability	Reliability is an ability of a computing system or service's probability to perform a specified service throughout a specified interval of time [22]. It is the probability that the system has not failed once it started to service. It is a measure of the continuity of service [23].	1. Contingency Plan 2. Recovery 3. Restoration 4. Alternative Mission / Business Process 5. Alternate information system site 6. System Impact Analyses 7. Disaster Recovery Plans 8. Continuity of Operations Plans 9. Crisis Communications Plans 10. Critical Infrastructure Plans 11. Cyber Incident Response Plans 12. Insider Threat Implementation Plan 13. Occupant Emergency Plans 14. System Resiliency 15. Resume Essential System 16. Continue Essential System [26].

ตารางที่ 3.1 เกณฑ์ในการเชื่อมโยงคุณลักษณะด้านความมั่นคงและความพึ่งพาได้กับมาตรฐานการควบคุมทางด้านความมั่นคง NIST และ AICPA (ต่อ)

Security and Dependability Attribute	Criteria	
	Characteristic	Method
Safety	Safety is an ability of the system to avoid catastrophic consequences that may affect the environment, including users, non-users and other environment, or the system itself [22].	1. Facility Protection 2. Physical Access Control 3. Physical Access Authorizations 4. Physical Access Records 5. Physical Safeguards 6. Physical Equipment Protection 7. Monitoring Physical Access 8. Visitor Access Records 9. Emergency Power Supply 10. Surrounding Hazardous Materials 11. Natural Access Control 12. Natural Surveillance 13. Power Distribution Systems 14. Power System Protection 15. Fences 16. Security Guard Procedures 17. Damage Assessment Criteria 18. Warning Signs 19. Smoke Detectors 20. Motion Detectors 21. CCTV 22. Fire Suppression Mechanisms 23. Emergency Response Procedures 24. Emergency Training 25. Intrusion Detection System 26. Hazard Avoidance

ตารางที่ 3.1 เกณฑ์ในการเชื่อมโยงคุณลักษณะด้านความมั่นคงและความพึ่งพาได้กับมาตรฐานการควบคุมทางด้านความมั่นคง NIST และ AICPA (ต่อ)

Security and Dependability Attribute	Criteria	
	Characteristic	Method
		27. Hazard Detection and Removal 28. Damage Limitation 29. Emergency Lighting 30. Fire Protection 31. Temperature and Humidity Controls 32. Water Damage Protection 33. Natural Disaster Protection 34. Location of Information System 35. Components 36. Electromagnetic Signals Emanations [20, 24].
Maintainability	Maintainability is an ability of a computing system or service to be maintained [25], whereas maintenance constitutes a series of actions necessary to restore or retain an item in effective operation state.	1. Maintenance 2. Maintainability Prediction 3. Repair 4. Diagnostic 5. System Monitoring 6. Hardware Monitoring 7. Log Analysis 8. Hardware Replacing [27].

3.2 ขั้นตอนการเชื่อมโยงคุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้กับเมตริกซ์ควบคุมคลาวด์

ในขั้นตอนนี้ผู้วิจัยจะทำการเชื่อมโยงคุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้ทั้ง 6 คุณลักษณะย่อยเข้ากับเมตริกซ์ควบคุมคลาวด์ ผ่านทางมาตรฐานการควบคุมความมั่นคง คือ NIST SP800-53 และ AICPA ซึ่ง CSA ได้เชื่อมโยงเข้ากับเมตริกซ์ควบคุมคลาวด์ไว้แล้ว จากนั้นทำการวิเคราะห์เพื่อทำการจำแนกว่ามาตรฐานการควบคุมความมั่นคงของ NIST และ AICPA ในแต่ละข้อนั้นเกี่ยวข้องทางด้านใดกับคุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้ โดยขั้นตอนการเชื่อมโยงนี้จะแบ่งออกเป็น 2 ขั้นตอน ต่อไปนี้

3.2.1 ขั้นตอนการเชื่อมโยงคุณลักษณะ ด้านการรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งานผ่านมาตรฐานการควบคุมความมั่นคง AICPA

จากตัวอย่างมาตรฐานการควบคุมความมั่นคง AICPA ในตารางที่ 3.2 จะเห็นได้ว่ามาตรฐานการควบคุมความมั่นคง AICPA นั้นมีทั้งหมด 4 รูปแบบ ได้แก่

1) มาตรฐานการควบคุมความมั่นคงที่ใช้ตัวอักษรย่อ CC คือมาตรฐานที่เกี่ยวข้องกับ 3 คุณลักษณะได้แก่ การรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน
2) มาตรฐานการควบคุมความมั่นคงที่ใช้ตัวอักษรย่อ C คือมาตรฐานที่เกี่ยวข้องกับคุณลักษณะทางด้าน การรักษาความลับ
3) มาตรฐานการควบคุมความมั่นคงที่ใช้ตัวอักษรย่อ PI คือมาตรฐานที่เกี่ยวข้องกับคุณลักษณะทางด้าน บูรณภาพ
4) มาตรฐานการควบคุมความมั่นคงที่ใช้ตัวอักษรย่อ A คือมาตรฐานที่เกี่ยวข้องกับคุณลักษณะทางด้าน สภาพพร้อมใช้งาน

ตารางที่ 3.2 ตัวอย่างของมาตรฐานการควบคุมความมั่นคง AICPA [12]

AICPA Criteria (Attribute)	AICPA ID	Control Specification
Criteria common to all subattributes of security (confidentiality, integrity, availability)	CC5.6	Logical access security measures have been implemented to protect against [insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof] threats from sources outside the boundaries of the system.
Additional criteria for confidentiality	C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition in accordance with confidentiality commitments and requirements.
Additional criteria for availability	A1.2	Environmental protection, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, monitored, and maintained to meet availability commitments and requirements.
Additional criteria for processing integrity	PI1.3	Data is processed completely, accurately, and timely as authorized in accordance with processing integrity commitments and requirements.

จากตัวอย่างมาตรฐานการควบคุมความมั่นคง AICPA ในตารางที่ 3.2 ผู้วิจัยจะใช้นิยามและวิธีการให้ได้มาซึ่งคุณลักษณะย่อยทั้ง 3 ด้านของความมั่นคง ได้แก่ การรักษาความลับ (Confidentiality) บูรณภาพ (Integrity) และสภาพพร้อมใช้งาน (Availability) ในตารางที่ 3.1 เพื่อมาเป็นเกณฑ์ในการวิเคราะห์ว่ามาตรฐานการควบคุมทางด้านความมั่นคง AICPA ในแต่ละข้อนั้นเกี่ยวข้องกับคุณลักษณะทางด้านความมั่นคงในด้านใด ยกตัวอย่างเช่น

มาตรฐาน AICPA หมายเลข C1.2 มีความเกี่ยวข้องกับคุณลักษณะทางด้านการรักษาความลับ เนื่องจากมีการทำ “Protect Against Unauthorized Access” ซึ่งตรงกับนิยามและวิธีการทางด้านคุณลักษณะของ การรักษาความลับ (Confidentiality) ในตารางที่ 3.1 ในด้านการทำ Authentication และ Authorization

ดังนั้นจากการที่ CSA ได้เชื่อมโยง การควบคุมความมั่นคงในเมตริกซ์ควบคุมคลาวด์ไว้กับมาตรฐานการควบคุมความมั่นคงของ AICPA ไว้แล้ว [6] ผู้วิจัยจึงสรุปความเชื่อมโยงระหว่างการควบคุมความมั่นคงในเมตริกซ์ควบคุมคลาวด์กับคุณลักษณะทางด้านความมั่นคง คือ การรักษาความลับ (C) บูรณภาพ (I) และสภาพพร้อมใช้งาน (A) ได้ดังตัวอย่างในตารางที่ 3.3 โดยในคอลัมน์คุณลักษณะ C หมายถึง Confidentiality, I หมายถึง Integrity และ A หมายถึง Availability ผู้วิจัยได้ทำการเชื่อมโยงคุณลักษณะทางด้านความมั่นคงเข้ากับเมตริกซ์ควบคุมคลาวด์ โดยที่ 1 หมายถึงเชื่อมโยง และ 0 หมายถึงไม่เชื่อมโยง ทั้งนี้การเชื่อมโยงทั้งหมดแสดงไว้ในภาคผนวก ก.

ตารางที่ 3.3 ตัวอย่างการเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA เข้ากับเมตริกซ์ควบคุมคลาวด์

CCM Control Domain	CCM Control	Control ID	CCM Control Specification	AICPA	Attributes		
					C	I	A
Change Control & Configuration Management (CCC)	Unauthorized Software Installations	CCC-04	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	CC5.5 CC5.8 CC7.4	1	1	1

ตารางที่ 3.3 ตัวอย่างการเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

CCM Control Domain	CCM Control	CCM Control ID	CCM Control Specification	AICPA	Attributes		
					C	I	A
Application & Interface Security (AIS)	Data Integrity	AIS-03	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	PI1.2 PI1.3 PI1.5	0	1	0
Business Continuity Management & Operational Resilience (BCR)	Datacenter Utilities / Environmental Conditions	BCR-03	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	A1.1 A1.2 A1.3	0	0	1
Data Security & Information Lifecycle Management (DSI)	Nonproduction Data	DSI-05	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	C1.1 C1.3 CC5.6	1	1	1

3.2.2 ขั้นตอนการเชื่อมโยงคุณลักษณะด้านความเชื่อถือได้ ความปลอดภัย และความสามารถในการบำรุงรักษาผ่านมาตรฐานการควบคุมความมั่นคง NIST SP800-53

ในขั้นตอนนี้ผู้วิจัยจะใช้มาตรฐานการควบคุมความมั่นคง NIST SP800-53 ในกลุ่มต่อไปนี้ ดังตัวอย่างในตารางที่ 3.4

1) กลุ่ม Contingency Planning (CP) สำหรับเชื่อมโยงกับคุณลักษณะทางด้าน ความเชื่อถือได้ หรือ R (Reliability)
2) กลุ่ม Physical and Environmental Protection (PE) สำหรับเชื่อมโยงกับคุณลักษณะทางด้าน ความปลอดภัย หรือ S (Safety)
3) กลุ่ม Maintenance (MA) สำหรับเชื่อมโยงกับคุณลักษณะทางด้านความสามารถในการบำรุงรักษา หรือ M (Maintainability)

ตารางที่ 3.4 ตัวอย่างมาตรฐานการควบคุมความมั่นคง NIST SP800-53 [10]

Control Family	Control ID	NIST SP800-53 Control Specification
Physical and Environmental Protection (PE)	PE-9 : Power Equipment and Cabling	The organization protects power equipment and power cabling for the information system from damage and destruction.
Contingency Planning (CP)	CP -6 : Alternate Storage Site	a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.
Maintenance (MA)	MA-2 : Controlled Maintenance	This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement).

จากตัวอย่างมาตรฐานการควบคุมความมั่นคง NIST SP800-53 ในตารางที่ 3.4 ผู้วิจัยจะใช้นิยามและวิธีการให้ได้มาซึ่งคุณลักษณะย่อยทั้ง 3 ด้านของความพึ่งพาได้ ได้แก่ ความเชื่อถือได้ (Reliability) ความปลอดภัย (Safety) และความสามารถในการบำรุงรักษา (Maintainability) ในตารางที่ 3.1 เพื่อมาเป็นเกณฑ์ในการวิเคราะห์ว่ามาตรฐานการควบคุมทางด้านความมั่นคง NIST SP800-53 ในแต่ละข้อนั้นเกี่ยวข้องกับคุณลักษณะทางด้านความพึ่งพาได้ในด้านใด ยกตัวอย่างเช่น

มาตรฐาน NIST SP800-53 หมายเลข PE-9 : Power Equipment and Cabling มีความเกี่ยวข้องกับคุณลักษณะทางด้านความปลอดภัย เนื่องจากมีการทำ “Protects Power Equipment and Power Cabling” ซึ่งตรงกับนิยามและวิธีการทางด้านคุณลักษณะของ ความปลอดภัย (Safety) ในตารางที่ 3.1 ในด้านการทำ Power System Protection และ Physical Equipment Protection

ดังนั้นจากการที่ CSA ได้เชื่อมโยงการควบคุมความมั่นคงในเมตริกซ์ควบคุมคลาวด์ไว้กับมาตรฐานการควบคุมความมั่นคง NIST SP 800-53 ไว้แล้ว [6] ผู้วิจัยจึงสรุปความเชื่อมโยงระหว่างการควบคุมความมั่นคงในเมตริกซ์ควบคุมคลาวด์ กับคุณลักษณะทางด้านความพึ่งพาได้ คือ ความเชื่อถือได้ (R), ความปลอดภัย (S), และความสามารถในการบำรุงรักษา (M) ได้ดังตัวอย่างในตารางที่ 3.5 โดยในคอลัมน์คุณลักษณะ R หมายถึง Reliability, S หมายถึง Safety และ M หมายถึง Maintainability ผู้วิจัยได้ทำการเชื่อมโยงคุณลักษณะทางด้านความพึ่งพาได้กับเมตริกซ์ควบคุมคลาวด์ โดยที่ 1 หมายถึงเชื่อมโยง และ 0 หมายถึงไม่เชื่อมโยง ทั้งนี้การเชื่อมโยงทั้งหมดแสดงไว้ในภาคผนวก ก.

ตารางที่ 3.5 ตัวอย่างการเชื่อมโยงมาตรฐานทางด้านความมั่นคง NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์

Control Domain	Control	Control ID	CCM Control Specification	NIST SP800-53	Attributes		
					R	S	M
Business Continuity Management & Operational Resilience (BCR)	Business Continuity Testing	BCR-02	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	CP-2 CP-3 CP-4	1	0	0

ตารางที่ 3.5 ตัวอย่างการเชื่อมโยงมาตรฐานทางด้านความมั่นคง NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain	Control	Control ID	CCM Control Specification	NIST SP800-53	Attributes		
					R	S	M
Business Continuity Management & Operational Resilience (BCR)	Datacenter Utilities / Environmental Conditions	BCR-03	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	PE-1 PE-4 PE-13	0	1	0
Business Continuity Management & Operational Resilience (BCR)	Equipment Maintenance	BCR-07	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	MA-2 MA-3 MA-4 MA-5 MA-6	0	0	1

3.2.3 ขั้นตอนสรุปการเชื่อมโยงคุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้ กับเมตริกซ์ควบคุมคลาวด์

จากหัวข้อที่ 3.2.1 และ 3.2.2 สามารถรวมผลการเชื่อมโยงแต่ละการควบคุมในเมตริกซ์ควบคุมคลาวด์ เข้ากับแต่ละคุณลักษณะย่อยของคุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้ ดังตัวอย่างตารางที่ 3.6 ผลการเชื่อมโยงทั้งหมดแสดงไว้ในภาคผนวก ก

ตารางที่ 3.6 ตัวอย่างสรุปการเชื่อมโยงระหว่างเมตริกซ์ควบคุมคลาวด์กับคุณลักษณะด้านความมั่นคงและความพึ่งพาได้

Control Domain	Control	Control ID	AICPA	NIST SP800-53	Attributes					
					C	I	A	R	S	M
Change Control & Configuration Management (CCC)	Unauthorized Software Installations	CCC-04	CC5.5 CC5.8 CC7.4	CM-1 CM-2 CM-3 CM-5 CM-7 CM-8 CM-9 SA-6 SA-7 SI-1 SI-3 SI-4 SI-7	1	1	1	0	0	0
Application & Interface Security (AIS)	Data Integrity	AIS-03	PI1.2 PI1.3 PI1.5	SI-10 SI-11 SI-2 SI-3 SI-4 SI-6 SI-7 SI-9	0	1	0	0	0	0

ตารางที่ 3.6 ตัวอย่างสรุปการเชื่อมโยงระหว่างเมตริกซ์ควบคุมคลาวด์กับคุณลักษณะด้านความมั่นคงและความพึ่งพาได้ (ต่อ)

Control Domain	Control	Control ID	AICPA	NIST SP800-53	Attributes					
					C	I	A	R	S	M
Business Continuity Management & Operational Resilience (BCR)	Datacenter Utilities / Environmental Conditions	BCR-03	A1.1 A1.2 A1.3	PE-1 PE-4 PE-13	0	0	1	0	1	0
Data Security & Information Lifecycle Management (DSI)	Nonproduction Data	DSI-05	C1.1 C1.3 CC5.6	SA-11 CM-4	1	1	1	0	0	0
Business Continuity Management & Operational Resilience (BCR)	Business Continuity Testing	BCR-02	A1.2	CP-2 CP-3 CP-4	0	0	1	1	0	0
Business Continuity Management & Operational Resilience (BCR)	Equipment Maintenance	BCR-07	A1.1 A1.2 CC4.1	MA-2 MA-3 MA-4 MA-5 MA-6	1	1	1	0	0	1

3.3 ขั้นตอนการสร้างเมตริกซ์คุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้ของโดเมนการควบคุม

จากหัวข้อที่ 3.2.3 การคำนวณระดับความเชื่อมโยงของแต่ละโดเมนการควบคุม (Control Domain) กับคุณลักษณะด้านความมั่นคงและความพึ่งพาได้ สามารถคำนวณได้โดย

$$d_{n,k} = \frac{\sum_{i=1}^{m} a_{n,k,i}}{m} \qquad (1)$$

โดยที่ $d_{n,k}$ คือ ค่าระดับความเชื่อมโยงของโดเมนการควบคุมที่ n กับคุณลักษณะย่อยที่ k และมีค่าในช่วง [0, 1]

$a_{n,k,i}$ คือ ค่าความเชื่อมโยงของการควบคุมที่ i ในโดเมนการควบคุมที่ n กับคุณลักษณะย่อยที่ k โดยที่ 1 หมายถึงเชื่อมโยงและ 0 หมายถึง ไม่เชื่อมโยง

m คือจำนวนของการควบคุม ในโดเมนการควบคุมที่ n

จากค่า $d_{n,k}$ ที่ได้ จะทำให้สามารถสร้างเมตริกซ์คุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้ของโดเมนการควบคุมทั้งหมดในเมตริกซ์ควบคุมคลาวด์ ซึ่งเมตริกซ์ที่ได้มีขนาด 16x6 โดยแต่ละเอลิเมนต์ของเมตริกซ์นี้ คือค่า $d_{n,k}$ ของแต่ละคุณลักษณะย่อยของโดเมนการควบคุม

$$D = \begin{array}{c} \begin{matrix} C & I & A & R & S & M \end{matrix} \\ \begin{bmatrix} d_{1,1} & \cdots & d_{1,6} \\ \vdots & \ddots & \vdots \\ d_{16,1} & \cdots & d_{16,6} \end{bmatrix} \end{array} \begin{matrix} AIS \\ \vdots \\ TVM \end{matrix}$$

ค่าของแต่ละเอลิเมนต์ในเมตริกซ์ D แสดงดังตารางที่ 3.7

ตารางที่ 3.7 ระดับความเชื่อมโยงของโดเมนการควบคุมกับคุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้

Control Domain	Confidentiality	Integrity	Availability	Reliability	Safety	Maintainability
AIS	0.75	1	0.75	0	0	0
AAC	1	1	1	0.33	0.33	0.33
BCR	0.63	0.72	1	0.45	0.45	0.18
CCC	1	1	1	0	0	0
DSI	0.85	0.85	0.85	0	0.28	0
DCS	1	1	1	0	0.66	0.22
EKM	0.5	0.5	0.5	0	0	0
GRM	0.81	0.81	0.81	0.18	0.18	0.18
HRS	0.9	0.9	0.9	0	0	0
IAM	0.61	0.61	0.61	0	0	0.23
IVS	0.53	0.46	0.46	0	0.07	0
IPY	0	0	0	0	0	0
MOS	0	0	0	0	0	0
SEF	1	1	1	0	0	0
STA	0.33	0.33	0.33	0.1	0.1	0.1
TVM	1	1	1	0.33	0	0

3.4 ขั้นตอนการหาค่าน้ำหนักของการควบคุมที่เกี่ยวข้องกับการรับประกันของโดเมนการควบคุมของเมตริกซ์ควบคุมคลาวด์

การรับประกันของโดเมนการควบคุม (Assurance-Related Control) เป็นมาตรฐานการควบคุมความมั่นคงของ NIST SP800-53 ซึ่งหมายถึงการควบคุมที่เป็นมาตรการที่ทำให้เกิดความเชื่อมั่นว่า ระบบมีฟังก์ชันทางด้านความมั่นคงที่ถูกต้องและทำงานตามที่ควรเป็นจริงๆ โดยจะเป็นการควบคุมที่เกี่ยวข้องกับ

1) กระบวนการ วิธีการ หรือเทคนิคในการออกแบบและพัฒนาส่วนต่างๆของระบบ

2) กระบวนการทำงานที่เป็นการปรับปรุงคุณภาพในส่วนต่างๆของระบบ

3) กิจกรรมที่ก่อให้เกิดหลักฐานด้านความมั่นคง (Security Evidence) จากการทำงาน

4) การประเมินประสิทธิภาพหรือความเสี่ยงของการควบคุมความมั่นคงที่ได้ปฏิบัติ หรือ

5) การเพิ่มทักษะความเชี่ยวชาญ ความเข้าใจ ในด้านความมั่นคงให้แก่บุคลากรที่เกี่ยวข้อง

CSA ได้เชื่อมโยงการควบคุมในเมตริกซ์ควบคุมคลาวด์ไว้กับมาตรฐานการควบคุม NIST SP800-53 โดยมาตรฐานการควบคุมที่เชื่อมโยงไว้ทั้งหมดนั้น อาจมีบางส่วนที่เป็นการควบคุมที่เกี่ยวข้องกับการรับประกัน ตัวอย่างของการควบคุมที่เกี่ยวข้องกับการรับประกัน แสดงในตารางที่ 3.8

ตารางที่ 3.8 ตัวอย่างการควบคุมที่เกี่ยวข้องกับการรับประกันในโดเมนการควบคุม AIS

Control Domain	Control ID	NIST SP800-53 Control	Assurance Related-Control
AIS	AIS-01	SC-2, SC-3, SC-4, SC-5, SC-6, SC-7, SC-8, SC-9, SC-10, SC-11, SC-12, SC-13, SC-14, SC-17, SC-18, SC-20, SC-21, SC-22, SC-23	SC-2, SC-3, SC-6, SC-11
	AIS-02	CA-1, CA-2, CA-5, CA-6	CA-1, CA-2, CA-5, CA-6
	AIS-03	SI-10, SI-11, SI-2, SI-3, SI-4, SI-6, SI-7, SI-9	SI-10, SI-4, SI-6, SI-7
	AIS-04	AC-1, AC-4, SC-1, SC-16	AC-1, SC-1

ผู้วิจัยมีแนวคิดในการให้น้ำหนักกับการควบคุมที่เกี่ยวข้องกับการรับประกัน เนื่องจากหากปฏิบัติตามการควบคุมนี้ จะยิ่งช่วยเพิ่มความไว้ใจได้ให้กับบริการคลาวด์

ค่าน้ำหนักของการรับประกันสามารถคำนวณได้โดยใช้สมการ

$$as_n = 1 + \left(\frac{ac_n}{ct_n}\right) \quad (2)$$

โดยที่ as_n คือค่าน้ำหนักของการควบคุมที่เกี่ยวข้องกับการรับประกันของโดเมนการควบคุมที่ n และมีค่าอยู่ในช่วง [1, 2]

ac_n คือ จำนวนการควบคุมของ NIST SP800-53 ที่เชื่อมโยงกับโดเมนการควบคุมที่ n และเกี่ยวข้องกับการรับประกัน

ct_n คือ จำนวนการควบคุมของ NIST SP800-53 ที่เชื่อมโยงกับโดเมนการควบคุมที่ n

สาเหตุที่ต้องนำค่า 1 มาบวก เนื่องจากในบางโดเมนการควบคุม ไม่มีรายการการควบคุมของ NIST SP800-53 ที่เกี่ยวข้องกับการรับประกัน เชื่อมโยงอยู่ด้วยเลย จึงเป็นสาเหตุทำให้น้ำหนักของการควบคุมที่เกี่ยวข้องกับการรับประกันของโดเมนการควบคุมที่ n มีค่าเท่ากับ 0 และเนื่องจากจำเป็นต้องนำค่าน้ำหนักไปคูณ เพื่อหาคะแนนความมั่นคงและความพึ่งพาได้ของผู้ให้บริการคลาวด์ในแต่ละโดเมนการควบคุมในหัวข้อที่ 3.6 ดังนั้นหากน้ำหนักของการควบคุมที่เกี่ยวข้องกับการรับประกันของโดเมนการควบคุมที่ n มีค่าเท่ากับ 0 จะส่งผลให้คะแนนความมั่นคงและความพึ่งพาได้ของผู้ให้บริการคลาวด์ในโดเมนการควบคุมที่ n นั้นมีค่าเท่ากับ 0 แม้ว่าผู้ให้บริการคลาวด์จะมีการปฏิบัติตามโดเมนการควบคุมนั้นๆก็ตาม ผู้วิจัยจึงจำเป็นต้องนำค่า 1 มาบวกด้วย เพื่อให้ในกรณีข้างต้น ผู้ให้บริการคลาวด์ยังได้คะแนนจากการปฏิบัติตามโดเมนการควบคุมนั้นๆอยู่ ทั้งนี้ค่าน้ำหนักของการควบคุมที่เกี่ยวข้องกับการรับประกันมีค่าอยู่ระหว่าง 1-2

ซึ่งจากสมการดังกล่าวข้างต้น จะทำให้สามารถคำนวณค่าน้ำหนักของการควบคุมที่เกี่ยวข้องกับการรับประกันของแต่ละโดเมนการควบคุมได้ดังตารางที่ 3.9

ตารางที่ 3.9 ค่าน้ำหนักของการควบคุมที่เกี่ยวข้องกับการรับประกันของแต่ละโดเมนการควบคุม

Control Domain	Assurance Weight
AIS	1.4 = (1+14/35)
AAC	1.86
BCR	1.31
CCC	1.76
DSI	1.28
DSC	1.3
EKM	1
GRM	1.65
HRS	1.55
IAM	1.28
IVS	1.44
IPY	1
MOS	1
SEF	1.5
STA	1.72
TVM	1.53

3.5 ขั้นตอนการคำนวณคะแนนการปฏิบัติตาม CAIQ ของผู้ให้บริการคลาวด์ในแต่ละโดเมนการควบคุม

คะแนนการปฏิบัติตาม CAIQ ของผู้ให้บริการคลาวด์ขึ้นอยู่กับจำนวนการตอบคำถามในแบบประเมิน CAIQ ซึ่งอยู่ใน STAR (CSA Security, Trust & Assurance Registry) [8] ซึ่งสามารถคำนวณคะแนนการปฏิบัติตามได้โดยใช้สมการ

$$\boldsymbol{cp_n} = \frac{\sum_{i=1}^{q} \boldsymbol{y_i}}{\boldsymbol{q}} \quad (3)$$

เมื่อ cp_n คือคะแนนการปฏิบัติตามในโดเมนการควบคุมที่ n และมีค่าอยู่ในช่วง [0, 1]

y_i คือคำตอบของคำถามที่ i ในโดเมนการควบคุมที่ n และมีค่า 1 ถ้าตอบ yes หรือ 0 ถ้าตอบ no

q จำนวนคำถามในโดเมนการควบคุมที่ n

ตัวอย่างผลลัพธ์ของคะแนนการปฏิบัติตาม CAIQ ของ Microsoft Azure ได้ผลดังตารางที่ 3.10

ตารางที่ 3.10 ตัวอย่างคะแนนการปฏิบัติตาม CAIQ ของผู้ให้บริการคลาวด์ Microsoft Azure

Microsoft Azure Cloud Service			
Control Domain	**Total of CAIQ Questions**	**Compliance (No. of Yes Answers)**	**Compliance Score**
AIS	9	8	0.89
AAC	13	13	1
BCR	23	21	0.91
CCC	10	10	1
DSI	17	14	0.82
DCS	11	11	1
EKM	14	13	0.93
GRM	22	22	1
HRS	24	22	0.92
IAM	40	37	0.93
IVS	33	30	0.91
IPY	8	8	1
MOS	29	0	0
SEF	13	13	1
STA	20	20	1
IVM	10	9	0.9

3.6 ขั้นตอนการสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของผู้ให้บริการคลาวด์ในแต่ละโดเมนการควบคุม

คะแนนความมั่นคงและความพึ่งพาได้ของผู้ให้บริการคลาวด์ในแต่ละโดเมนการควบคุม สามารถคำนวณได้ด้วยสมการ

$$p_n = cp_n \times as_n \quad (4)$$

โดยที่ p_n คือ คะแนนความมั่นคงและความพึ่งพาได้ของผู้ให้บริการคลาวด์ในโดเมนการควบคุมที่ n และมีค่าอยู่ในช่วง [0, 2]

cp_n คือ คะแนนการปฏิบัติตามโดเมนการควบคุมที่ n

as_n คือ ค่าน้ำหนักของการควบคุมที่เกี่ยวข้องกับการรับประกันของโดเมนการควบคุมที่ n

สาเหตุที่ต้องนำคะแนนการปฏิบัติตามโดเมนการควบคุมของผู้ให้บริการคลาวด์หรือ cp_n มาคูณกับค่าน้ำหนักของการควบคุมที่เกี่ยวข้องกับการรับประกันหรือ as_n เนื่องจากคะแนนการปฏิบัติตามโดเมนการควบคุมของผู้ให้บริการคลาวด์มีค่าอยู่ระหว่าง [0, 1] และค่าน้ำหนักของการควบคุมที่เกี่ยวข้องกับการรับประกันมีค่าอยู่ระหว่าง [1, 2] หากผู้ให้บริการคลาวด์มีการปฏิบัติตาม CAIQ ในโดเมนการควบคุมที่เกี่ยวข้องกับการรับประกันด้วยแล้ว ผู้ให้บริการจะได้คะแนนเพิ่มตามค่าน้ำหนักที่นำมาคูณ เนื่องจากการปฏิบัติตาม CAIQ ในโดเมนการควบคุมนั้นทำให้เกิดหลักฐานเพิ่มเติม ซึ่งช่วยเสริมในด้านความไว้ใจได้ให้เพิ่มมากขึ้นได้

จากค่า p_n ที่ได้จะทำให้สามารถสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ P ของผู้ให้บริการคลาวด์ สำหรับทุกโดเมนการควบคุมในเมตริกซ์ควบคุมคลาวด์ ซึ่งมีขนาด 1x16 โดยแต่ละเอลิเมนต์ของเวกเตอร์นี้คือค่า p_n ของแต่ละโดเมนการควบคุม ดังสมการ

$$P = [\underset{\text{AIS}}{p_1}, \underset{\text{AAC}}{p_2}, \ldots, \underset{\text{TVM}}{p_{16}}] \quad (5)$$

ตัวอย่างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ ของ Microsoft Azure แสดงดังตารางที่ 3.11

ตารางที่ 3.11 ตัวอย่างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของผู้ให้บริการคลาวด์ Microsoft Azure

Microsoft Azure			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.89	1.4	1.25
AAC	1	1.86	1.86
BCR	0.91	1.31	1.19
CCC	1	1.76	1.76
DSI	0.82	1.28	1.05
DCS	1	1.3	1.3
EKM	0.93	1	0.93
GRM	1	0.64	1.65
HRS	0.92	1.55	1.43
IAM	0.93	1.28	1.19
IVS	0.91	1.44	1.31
IPY	1	1	1
MOS	0	1	0
SEF	1	1.5	1.5
STA	1	1.72	1.72
IVM	0.9	1.53	1.38

3.7 ขั้นตอนการประเมินความไว้ใจได้ของผู้ให้บริการคลาวด์

เวกเตอร์ความไว้ใจได้ T ของผู้ให้บริการจะเป็นเวกเตอร์ขนาด 1x6 ซึ่งคำนวณได้จากสมการ

$$T = P \times D = [\text{C I A R S M}] \quad (6)$$

โดยที่ C I A R S M คือคะแนนของ การรักษาความลับ, บูรณภาพ, สภาพพร้อมใช้งาน, ความเชื่อถือได้, ความปลอดภัย, ความสามารถในการบำรุงรักษา ตามลำดับ ดังตัวอย่างในตารางที่ 3.12

ตารางที่ 3.12 ตัวอย่างเวกเตอร์คะแนนค่าความมั่นคงและความพึ่งพาได้ของ Microsoft Azure

Subattribute	Confidentiality	Integrity	Availability	Reliability	Safety	Maintainability
Score	15.46	15.78	15.80	2.07	2.86	1.86

จากเวกเตอร์ T ที่ได้จะนำมานอร์มัลไลซ์ (Normalize) ด้วยค่าสูงสุดของค่าคะแนนคุณลักษณะย่อยแต่ละด้านที่เป็นไปได้ โดย $T_{Normalize}$ จะคำนวณจาก

$$T_{Normalize} = [C_{Normalize} \ I_{Normalize} \ A_{Normalize} \ R_{Normalize} \ S_{Normalize} \ M_{Normalize}]$$

$$= \left[\frac{C}{MAX\ (C)} \quad \frac{I}{MAX\ (I)} \quad \frac{A}{MAX\ (A)} \quad \frac{R}{MAX\ (R)} \quad \frac{S}{MAX\ (S)} \quad \frac{M}{MAX\ (M)}\right]$$

$$= \left[\frac{C}{16.26} \quad \frac{I}{16.62} \quad \frac{A}{16.63} \quad \frac{R}{2.18} \quad \frac{S}{2.99} \quad \frac{M}{1.86}\right]$$

จากนั้นนำมาหาค่าเฉลี่ยเพื่อหาค่าความไว้ใจได้ ของผู้ให้บริการคลาวด์

$$TR = average\ (C_{Normalize} \ I_{Normalize} \ A_{Normalize} \ R_{Normalize} \ S_{Normalize} \ M_{Normalize})$$

ตัวอย่างคะแนนความไว้ใจได้ ***TR*** ของผู้ให้บริการคลาวด์ Microsoft Azure จะมีค่าเป็น

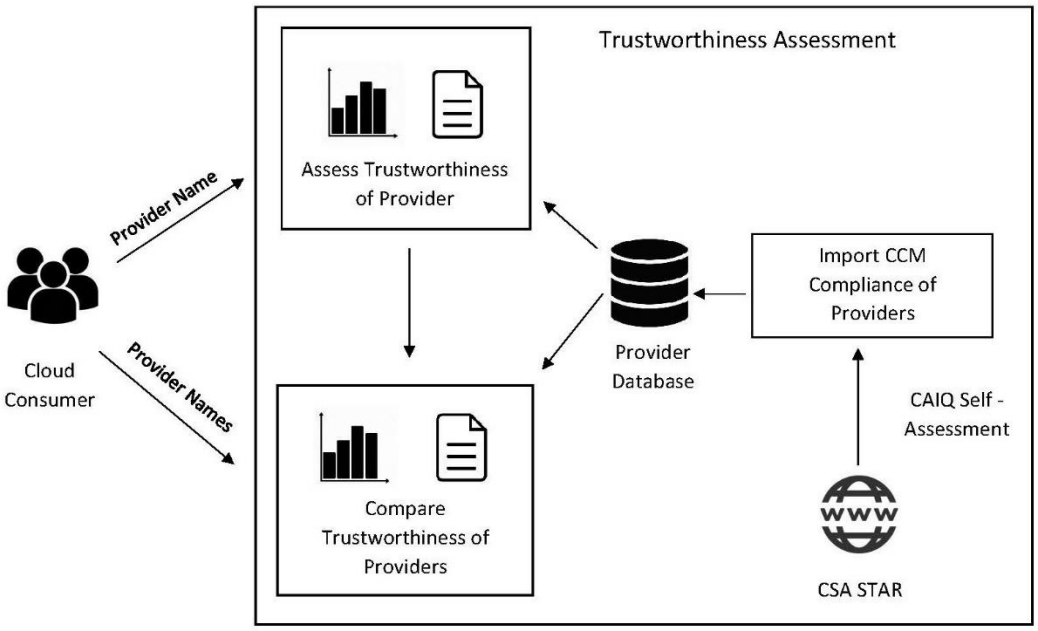
$$TR = average\left(\frac{15.46}{16.26}\ \frac{15.78}{16.62}\ \frac{15.80}{16.64}\ \frac{2.07}{2.18}\ \frac{2.86}{2.99}\ \frac{1.86}{1.9}\right) = 0.96$$

3.8 การพัฒนาระบบสนับสนุนการประเมินความไว้ใจได้ของผู้ให้บริการโดยอิงเมตริกซ์ควบคุมคลาวด์

การพัฒนาระบบสนับสนุนการประเมินความไว้ใจได้ของผู้ให้บริการมีการพัฒนาแบบ Windows Application โดยภาษาที่ใช้ในการพัฒนาคือ VB.NET ระบบสามารถสนับสนุนผู้ใช้บริการในการประเมินความไว้ใจได้ของผู้ให้บริการ และสามารถประเมินคุณลักษณะย่อยทั้ง 6 ด้าน ได้แก่ การรักษาความลับ บูรณภาพ สภาพพร้อมใช้งาน ความเชื่อถือได้ ความปลอดภัย และความสามารถในการบำรุงรักษา

3.8.1 ส่วนประกอบของระบบ

ระบบจะสนับสนุนผู้ใช้บริการโดยผู้ใช้บริการนำข้อมูลการประเมินตนเองของผู้ให้บริการที่เผยแพร่อยู่บนเว็บไซต์ CSA STAR [8] มาเป็นข้อมูลนำเข้าให้กับตัวระบบ หรือเลือกข้อมูลจากรายชื่อผู้ให้บริการในฐานข้อมูลของระบบ เพื่อทำการคำนวณ, แสดง และเปรียบเทียบค่าความไว้ใจได้ของผู้ให้บริการ ภาพรวมของระบบดังภาพที่ 3.2



ภาพที่ 3.2 ระบบการประเมินความไว้ใจได้ของผู้ให้บริการโดยอิงเมตริกซ์ควบคุมคลาวด์

Input CCM Compliance of Providers ระบบรับข้อมูลการปฏิบัติตามเมตริกซ์ควบคุมคลาวด์ซึ่งผู้ให้บริการได้ประเมินตนเองไว้ตามแบบประเมิน CAIQ และเผยแพร่ไว้ที่ CSA STAR ทั้งนี้ข้อมูลที่นำเข้ามีการจัดเตรียมไว้แล้วโดยงานวิจัย [28] แล้วนำมาจัดเก็บในฐานข้อมูลผู้ให้บริการของระบบ

Assess Trustworthiness of Provider ระบบนำข้อมูลการปฏิบัติตามเมตริกซ์ควบคุมคลาวด์ของผู้ให้บริการที่ผู้ใช้บริการระบุ มาทำการคำนวณค่าความไว้ใจได้ของผู้ให้บริการ โดยสามารถแสดงค่าที่ได้ออกเป็นทั้งหมด 6 ด้านได้แก่ Confidentiality, Integrity, Availability, Reliability, Safety, Maintainability ผลการประเมินที่ได้สามารถแสดงในรูปแบบตัวเลขและรูปแบบกราฟ

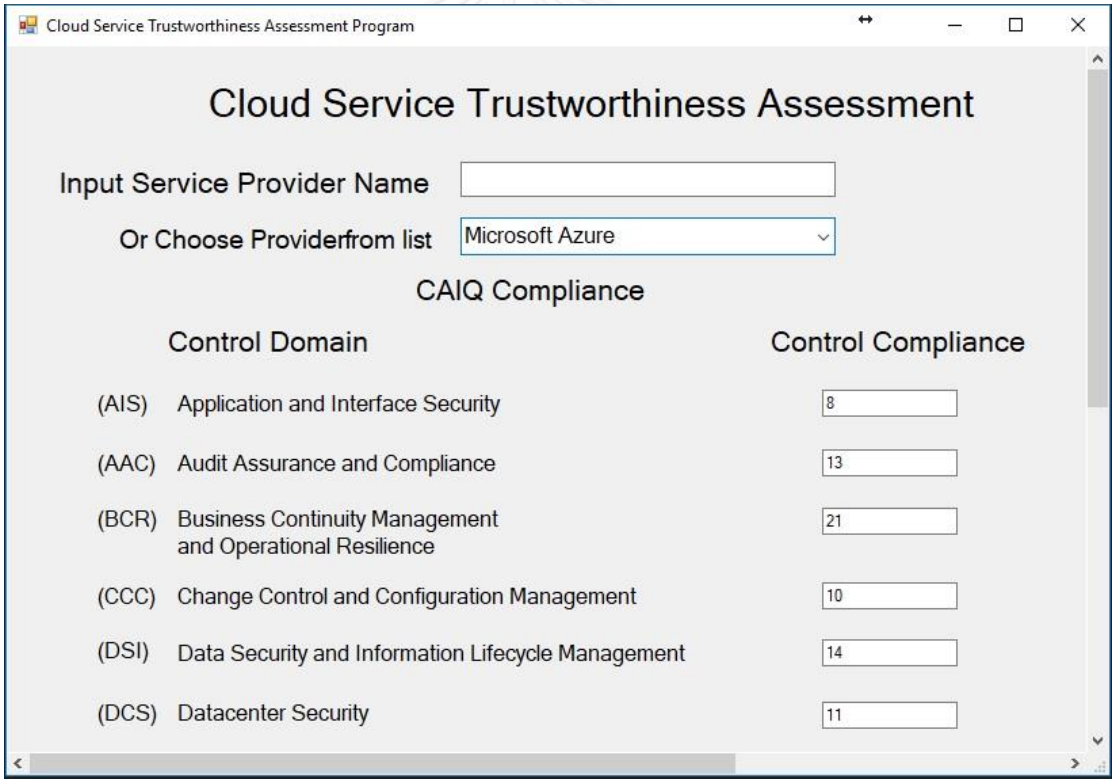
Compare Trustworthiness of Providers ระบบทำการคำนวณค่าความไว้ใจได้ของผู้ให้บริการรายต่างๆตามที่ผู้ใช้บริการระบุ เพื่อเปรียบเทียบคะแนนของแต่ละคุณลักษณะที่ต้องการได้

3.8.2 ส่วนต่อประสานผู้ใช้ของระบบ

ส่วนต่อประสานของผู้ใช้ระบบประกอบด้วย

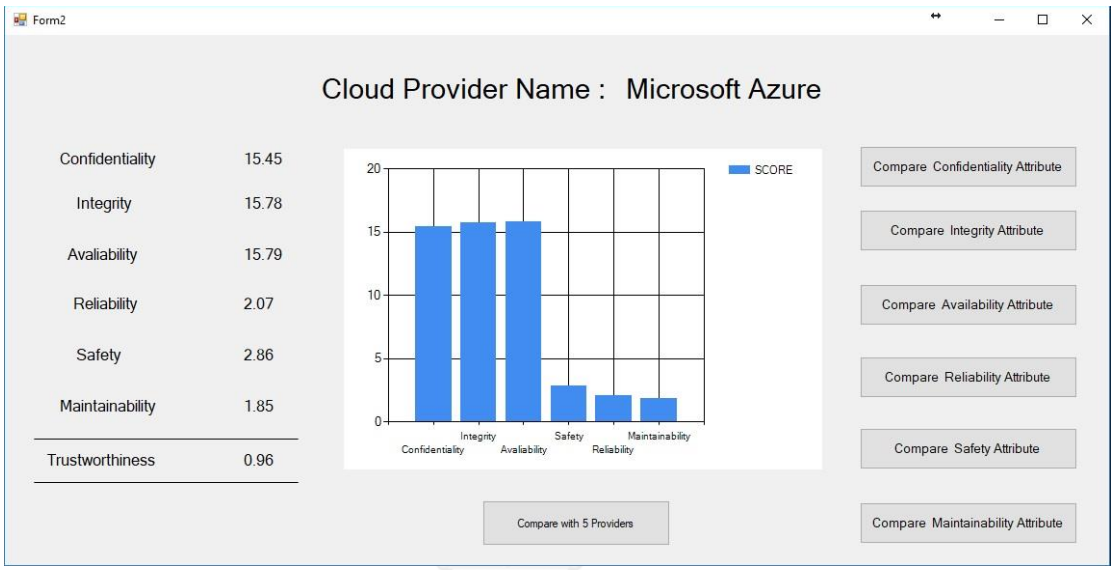
1) หน้าจอหลักสำหรับรับชื่อผู้ให้บริการที่ต้องการประเมินความไว้ใจได้ซึ่งมีข้อมูลอยู่ในระบบ
2) หน้าจอการแสดงผลค่าความไว้ใจได้ของผู้ให้บริการคลาวด์
3) หน้าจอสำหรับเปรียบเทียบแต่ละคุณลักษณะย่อยที่ต้องการ
4) หน้าจอสำหรับเปรียบเทียบค่าความไว้ใจได้กับผู้ให้บริการคลาวด์รายอื่น

1. หน้าจอหลัก ประกอบด้วยช่อง Input ข้อมูลชื่อของผู้ให้บริการคลาวด์ หรือเลือกข้อมูลผู้ให้บริการคลาวด์จากฐานข้อมูล ดังภาพที่ 3.3



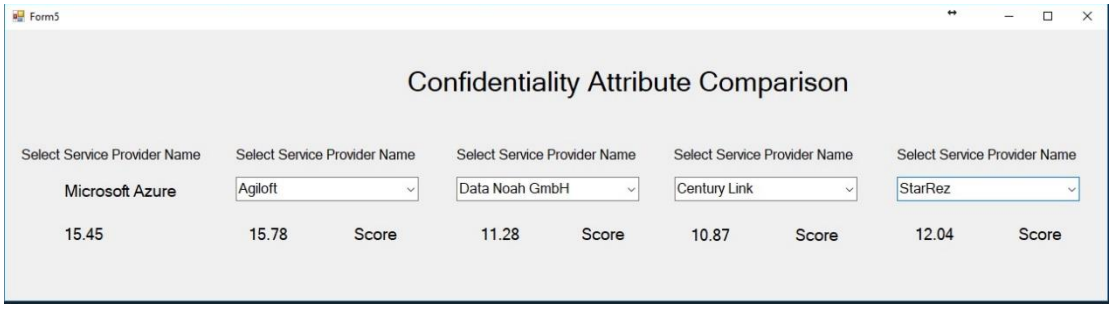
ภาพที่ 3.3 หน้าจอหลักของระบบประเมินความไว้ใจได้ของผู้ให้บริการโดยอิงเมตริกซ์ควบคุมคลาวด์

2. หน้าจอแสดงผลค่าความไว้ใจได้ของผู้ให้บริการคลาวด์ โดยจะแสดงคะแนนความไว้ใจได้และคุณลักษณะย่อยทั้ง 6 ด้าน ได้แก่ การรักษาความลับ บูรณภาพ สภาพพร้อมใช้งาน ความเชื่อถือได้ ความปลอดภัย และความสามารถในการบำรุงรักษา ของผู้ให้บริการคลาวด์ สามารถแสดงผลในรูปแบบตัวเลขและในรูปแบบกราฟ ดังภาพที่ 3.4 ผู้ใช้บริการสามารถเลือกทำการเปรียบเทียบคะแนนของผู้ให้บริการรายนี้กับผู้ให้บริการรายอื่นต่อไปอีกได้



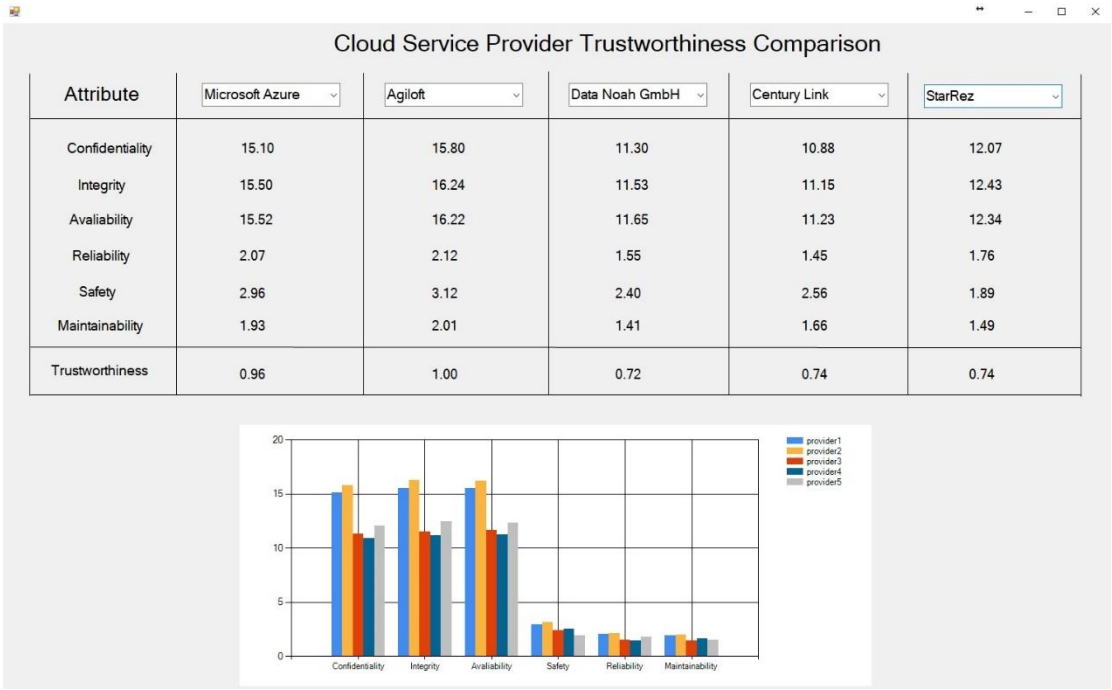
ภาพที่ 3.4 หน้าจอแสดงคะแนนความไว้ใจได้ของผู้ให้บริการคลาวด์

3. หน้าจอสำหรับเปรียบเทียบแต่ละคุณลักษณะย่อยที่ต้องการ โดยสามารถเลือกคุณลักษณะใดลักษณะหนึ่งของทั้ง 6 คุณลักษณะย่อย ที่ต้องการเปรียบเทียบกับผู้ให้บริการคลาวด์รายอื่น ดังภาพที่ 3.5



ภาพที่ 3.5 หน้าจอเปรียบเทียบคุณลักษณะย่อยที่ต้องการกับผู้ให้บริการรายอื่น

4. หน้าจอแสดงการเปรียบเทียบค่าความไว้ใจได้ของผู้ให้บริการคลาวด์ หลังจากผู้ใช้บริการระบุชื่อผู้ให้บริการที่ต้องการเปรียบเทียบโดยใช้หน้าจอในภาพที่ 3.3 แล้วระบบจะแสดงคะแนนความไว้ใจได้และคุณลักษณะทั้ง 6 ด้าน ได้แก่ การรักษาความลับ, บูรณภาพ, สภาพพร้อมใช้งาน, ความเชื่อถือได้, ความปลอดภัย, ความสามารถในการบำรุงรักษา ของผู้ให้บริการคลาวด์ที่ทำการเปรียบเทียบกัน ในรูปแบบตัวเลขและรูปแบบกราฟ ดังภาพที่ 3.6



ภาพที่ 3.6 หน้าจอแสดงการเปรียบเทียบคะแนนความไว้ใจได้ของผู้ให้บริการคลาวด์

บทที่ 4
การทดสอบและการประเมินผลการวิจัย

ในบทนี้จะกล่าวถึงการทดสอบการประเมินค่าความไว้ใจได้ของผู้ให้บริการ และการประเมินความสมเหตุสมผลของค่าความไว้ใจได้โดยการวิเคราะห์สหสัมพันธ์

4.1 การทดสอบการประเมินค่าความไว้ใจได้ของผู้ให้บริการ

ในการทดลองการประเมินความไว้ใจได้ของผู้ให้บริการคลาวด์โดยอิงเมตริกซ์ควบคุมคลาวด์ ผู้วิจัยใช้ข้อมูลที่เผยแพร่อยู่บนเว็บไซต์ของ CSA Security, Trust & Assurance Registry (STAR) [8] เพื่อมาทำการประเมินผล โดยใช้ผู้ให้บริการ 20 ราย ได้แก่ Amazon AWS, Microsoft Azure, Dropbox, IBM SoftLayer, EBRC, Squiz, Acquria, Outreach, Capriza, StarRez, VMWare AirWatch, Data Noah Gmbh, CenturyLink, Tableau, Optimizely, Collab9, Perspectium, Develloucus, Siteimprove, และ Eagle.io

การทดสอบจะเป็นการแสดงและเปรียบเทียบผลคะแนนความไว้ใจได้ของผู้ให้บริการคลาวด์แต่ละราย รายละเอียดในการทดสอบมีดังนี้

4.1.1 การปฏิบัติตามแบบประเมิน CAIQ ของผู้ให้บริการคลาวด์ในแต่ละโดเมนการควบคุม

ผู้วิจัยได้รวบรวมข้อมูลการประเมินตนเอง (Self-Assessment) จากเว็บไซต์ของ CSA STAR ซึ่งผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ในแต่ละโดเมนการควบคุมของแต่ละผู้ให้บริการ ได้แก่ Amazon AWS, Microsoft Azure, Dropbox, IBM SoftLayer, EBRC, Squiz, Acquria, Outreach, Capriza, StarRez, VMWare AirWatch, Data Noah Gmbh, CenturyLink, Tableau, Optimizely, Collab9, Perspectium, Develloucus, Siteimprove และ Eagle.io ตามสมการในหัวข้อที่ 3.5 จะได้ผลดังตารางที่ 4.1 – 4.20 ตามลำดับ

ตารางที่ 4.1 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Amazon AWS

1.Amazon AWS Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	8	0.89
AAC	13	13	1
BCR	23	23	1
CCC	10	10	1
DSI	17	15	0.89
DCS	11	11	1
EKM	14	14	1
GRM	22	22	1
HRS	24	24	1
IAM	40	38	0.95
IVS	33	31	0.94
IPY	8	6	0.75
MOS	29	20	0.69
SEF	13	13	1
STA	20	20	1
IVM	10	10	1

ตารางที่ 4.2 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Microsoft Azure

2.Microsoft Azure Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	8	0.89
AAC	13	13	1
BCR	23	21	0.91
CCC	10	10	1
DSI	17	14	0.82
DCS	11	11	1
EKM	14	13	0.93
GRM	22	22	1
HRS	24	22	0.92
IAM	40	37	0.93
IVS	33	30	0.91
IPY	8	8	1
MOS	29	0	0
SEF	13	13	1
STA	20	20	1
IVM	10	9	0.9

ตารางที่ 4.3 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Dropbox

3.Dropbox Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	8	0.89
AAC	13	11	0.85
BCR	23	14	0.61
CCC	10	10	1
DSI	17	14	0.82
DCS	11	10	0.91
EKM	14	13	0.93
GRM	22	20	0.91
HRS	24	21	0.88
IAM	40	32	0.80
IVS	33	31	0.94
IPY	8	8	1
MOS	29	27	0.93
SEF	13	11	0.85
STA	20	18	0.9
IVM	10	9	0.9

ตารางที่ 4.4 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ IBM SoftLayer

4.IBM SoftLayer Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	7	0.78
AAC	13	12	0.92
BCR	23	20	0.87
CCC	10	9	0.9
DSI	17	14	0.82
DCS	11	11	1
EKM	14	5	0.36
GRM	22	20	0.91
HRS	24	22	0.92
IAM	40	33	0.83
IVS	33	27	0.82
IPY	8	4	0.5
MOS	29	0	0
SEF	13	11	0.85
STA	20	18	0.9
IVM	10	8	0.8

ตารางที่ 4.5 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ EBRC

5.EBRC Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	4	0.44
AAC	13	13	1
BCR	23	20	0.87
CCC	10	7	0.7
DSI	17	12	0.71
DCS	11	10	0.91
EKM	14	13	0.93
GRM	22	22	1
HRS	24	20	0.83
IAM	40	27	0.68
IVS	33	30	0.91
IPY	8	8	1
MOS	29	0	0
SEF	13	13	1
STA	20	1	0.05
IVM	10	8	0.8

ตารางที่ 4.6 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Squiz

6.Squiz Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	7	0.78
AAC	13	12	0.92
BCR	23	18	0.78
CCC	10	9	0.9
DSI	17	13	0.76
DCS	11	8	0.73
EKM	14	7	0.5
GRM	22	19	0.86
HRS	24	21	0.88
IAM	40	33	0.83
IVS	33	28	0.85
IPY	8	8	1
MOS	29	0	0
SEF	13	8	0.62
STA	20	13	0.65
IVM	10	7	0.7

ตารางที่ 4.7 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Acquria

7.Acquria Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	7	0.78
AAC	13	11	0.85
BCR	23	16	0.7
CCC	10	10	1
DSI	17	7	0.41
DCS	11	4	0.36
EKM	14	3	0.21
GRM	22	21	0.95
HRS	24	21	0.88
IAM	40	33	0.83
IVS	33	24	0.73
IPY	8	0	0
MOS	29	0	0
SEF	13	13	1
STA	20	18	0.9
IVM	10	7	0.7

ตารางที่ 4.8 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Outreach

8.Outreach Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	8	0.89
AAC	13	12	0.92
BCR	23	12	0.52
CCC	10	7	0.7
DSI	17	12	0.71
DCS	11	8	0.73
EKM	14	9	0.64
GRM	22	18	0.82
HRS	24	23	0.96
IAM	40	39	0.98
IVS	33	23	0.7
IPY	8	0	0
MOS	29	0	0
SEF	13	9	0.69
STA	20	15	0.75
IVM	10	7	0.7

ตารางที่ 4.9 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Capriza

9.Capriza Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	8	0.89
AAC	13	11	0.85
BCR	23	14	0.61
CCC	10	9	0.9
DSI	17	4	0.24
DCS	11	7	0.64
EKM	14	11	0.79
GRM	22	19	0.86
HRS	24	20	0.83
IAM	40	37	0.93
IVS	33	26	0.79
IPY	8	2	0.25
MOS	29	5	0.17
SEF	13	8	0.62
STA	20	18	0.9
IVM	10	9	0.9

ตารางที่ 4.10 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ StarRez

10.StarRez Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	8	0.89
AAC	13	11	0.85
BCR	23	14	0.61
CCC	10	9	0.9
DSI	17	6	0.35
DCS	11	4	0.36
EKM	14	9	0.64
GRM	22	21	0.95
HRS	24	18	0.75
IAM	40	33	0.83
IVS	33	24	0.73
IPY	8	8	1
MOS	29	0	0
SEF	13	10	0.77
STA	20	17	0.85
IVM	10	9	0.9

ตารางที่ 4.11 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ VMWare AirWatch

11.VMWare AirWatch Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	7	0.78
AAC	13	11	0.85
BCR	23	14	0.61
CCC	10	8	0.8
DSI	17	7	0.41
DCS	11	8	0.73
EKM	14	13	0.93
GRM	22	17	0.77
HRS	24	21	0.88
IAM	40	32	0.8
IVS	33	22	0.67
IPY	8	0	0
MOS	29	0	0
SEF	13	7	0.54
STA	20	11	0.55
IVM	10	9	0.9

ตารางที่ 4.12 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Data Noah GMBH

12.Data Noah GMBH Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	4	0.44
AAC	13	9	0.69
BCR	23	18	0.78
CCC	10	7	0.7
DSI	17	13	0.76
DCS	11	11	1
EKM	14	8	0.57
GRM	22	12	0.55
HRS	24	20	0.83
IAM	40	28	0.7
IVS	33	25	0.76
IPY	8	0	0
MOS	29	0	0
SEF	13	9	0.69
STA	20	12	0.6
IVM	10	8	0.8

ตารางที่ 4.13 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ CenturyLink

13.CenturyLink Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	5	0.56
AAC	13	12	0.92
BCR	23	17	0.74
CCC	10	8	0.8
DSI	17	13	0.76
DCS	11	9	0.82
EKM	14	6	0.43
GRM	22	16	0.73
HRS	24	17	0.71
IAM	40	32	0.8
IVS	33	26	0.79
IPY	8	4	0.5
MOS	29	1	0.03
SEF	13	7	0.54
STA	20	16	0.8
IVM	10	2	0.2

ตารางที่ 4.14 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Tableau

14.Tableau Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	7	0.78
AAC	13	11	0.85
BCR	23	10	0.43
CCC	10	5	0.50
DSI	17	10	0.59
DCS	11	5	0.45
EKM	14	3	0.21
GRM	22	17	0.77
HRS	24	16	0.67
IAM	40	29	0.73
IVS	33	19	0.58
IPY	8	7	0.88
MOS	29	6	0.21
SEF	13	8	0.62
STA	20	13	0.65
IVM	10	8	0.8

ตารางที่ 4.15 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Optimizely

15.Optimizely Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	9	1
AAC	13	13	1
BCR	23	17	0.74
CCC	10	10	1
DSI	17	8	0.47
DCS	11	7	0.64
EKM	14	8	0.57
GRM	22	10	0.45
HRS	24	16	0.67
IAM	40	17	0.43
IVS	33	23	0.7
IPY	8	8	1
MOS	29	0	0
SEF	13	4	0.31
STA	20	13	0.65
IVM	10	4	0.4

ตารางที่ 4.16 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Collab9

16.Collab9 Cloud Service			
Control Domain	Total of CAIQ Questions	Compliance (No. of Yes Answers)	Compliance Score
AIS	9	5	0.56
AAC	13	10	0.77
BCR	23	15	0.65
CCC	10	4	0.4
DSI	17	8	0.47
DCS	11	6	0.55
EKM	14	0	0
GRM	22	16	0.73
HRS	24	16	0.67
IAM	40	31	0.78
IVS	33	22	0.67
IPY	8	0	0
MOS	29	0	0
SEF	13	10	0.77
STA	20	8	0.4
IVM	10	8	0.8

ตารางที่ 4.17 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Perspectium

17.Perspectium Cloud Service			
Control Domain	**Total of CAIQ Questions**	**Compliance (No. of Yes Answers)**	**Compliance Score**
AIS	9	7	0.78
AAC	13	5	0.38
BCR	23	17	0.74
CCC	10	7	0.7
DSI	17	8	0.47
DCS	11	7	0.64
EKM	14	8	0.57
GRM	22	9	0.41
HRS	24	16	0.67
IAM	40	17	0.43
IVS	33	23	0.7
IPY	8	4	0.5
MOS	29	1	0.03
SEF	13	4	0.31
STA	20	13	0.65
IVM	10	4	0.4

*ตารางที่ 4.18 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Develloc*us

18.Develloc*us* Cloud Service			
Control Domain	**Total of CAIQ Questions**	**Compliance (No. of Yes Answers)**	**Compliance Score**
AIS	9	8	0.89
AAC	13	3	0.23
BCR	23	7	0.30
CCC	10	8	0.80
DSI	17	7	0.41
DCS	11	11	1
EKM	14	4	0.29
GRM	22	11	0.5
HRS	24	16	0.67
IAM	40	25	0.63
IVS	33	1	0.03
IPY	8	0	0
MOS	29	0	0
SEF	13	0	0
STA	20	5	0.25
IVM	10	10	1

ตารางที่ 4.19 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Siteimprove

19.Siteimprove Cloud Service			
Control Domain	**Total of CAIQ Questions**	**Compliance (No. of Yes Answers)**	**Compliance Score**
AIS	9	5	0.56
AAC	13	3	0.23
BCR	23	13	0.57
CCC	10	7	0.7
DSI	17	10	0.59
DCS	11	9	0.82
EKM	14	1	0.07
GRM	22	8	0.36
HRS	24	12	0.5
IAM	40	18	0.45
IVS	33	18	0.55
IPY	8	0	0
MOS	29	0	0
SEF	13	6	0.46
STA	20	12	0.6
IVM	10	2	0.2

ตารางที่ 4.20 ผลการประเมินการปฏิบัติตามแบบประเมิน CAIQ ของ Eagle.io

20.Eagle.io Cloud Service			
Control Domain	**Total of CAIQ Questions**	**Compliance (No. of Yes Answers)**	**Compliance Score**
AIS	9	3	0.33
AAC	13	8	0.62
BCR	23	12	0.52
CCC	10	5	0.50
DSI	17	8	0.47
DCS	11	0	0
EKM	14	0	0
GRM	22	17	0.77
HRS	24	6	0.25
IAM	40	15	0.38
IVS	33	17	0.52
IPY	8	0	0
MOS	29	0	0
SEF	13	1	0.08
STA	20	5	0.25
IVM	10	0	0

4.1.2 การทดสอบการสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของผู้ให้บริการคลาวด์ในแต่ละโดเมนการควบคุม

การทดสอบการสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของผู้ให้บริการคลาวด์ในแต่ละโดเมนการควบคุม ทำโดยใช้ค่าน้ำหนักของการควบคุมที่เกี่ยวข้องกับการรับประกัน (Assurance–Related Control) ของแต่ละโดเมนการควบคุมซึ่งได้จากหัวข้อที่ 3.4 มาทำการคำนวณร่วมกับผลการประเมินตาม CAIQ ในหัวข้อที่ 4.1.1 ตามสมการในหัวข้อที่ 3.6 เวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของผู้ให้บริการคลาวด์ใน 16 โดเมนการควบคุม ของผู้ให้บริการคลาวด์ทั้ง 20 ราย แสดงดังตารางที่ 4.21-4.40 ตามลำดับ

ตารางที่ 4.21 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Amazon AWS

Amazon AWS Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.89	1.4	1.25
AAC	1	1.86	1.86
BCR	1	1.31	1.31
CCC	1	1.76	1.76
DSI	0.89	1.28	1.13
DCS	1	1.3	1.3
EKM	1	1	1
GRM	1	0.64	1.65
HRS	1	1.55	1.55
IAM	0.95	1.28	1.22
IVS	0.94	1.44	1.35
IPY	0.75	1	0.75
MOS	0.69	1	0.69
SEF	1	1.5	1.5
STA	1	1.72	1.72
IVM	1	1.53	1.53

ตารางที่ 4.22 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Microsoft Azure

Microsoft Azure Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.89	1.4	1.25
AAC	1	1.86	1.86
BCR	0.92	1.31	1.19
CCC	1	1.76	1.76
DSI	0.83	1.28	1.05
DCS	1	1.3	1.3
EKM	0.93	1	0.93
GRM	1	0.64	1.65
HRS	0.92	1.55	1.43
IAM	0.93	1.28	1.19
IVS	0.91	1.44	1.31
IPY	1	1	1
MOS	0	1	0
SEF	1	1.5	1.5
STA	1	1.72	1.72
IVM	0.9	1.53	1.38

ตารางที่ 4.23 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Dropbox

Dropbox Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.89	1.4	1.25
AAC	0.85	1.86	1.58
BCR	0.61	1.31	0.8
CCC	1	1.76	1.76
DSI	0.83	1.28	1.05
DCS	0.91	1.3	1.18
EKM	0.93	1	0.93
GRM	0.91	0.64	1.50
HRS	0.88	1.55	1.36
IAM	0.8	1.28	1.02
IVS	0.94	1.44	1.35
IPY	1	1	1
MOS	0.94	1	0.93
SEF	0.85	1.5	1.28
STA	0.9	1.72	1.55
IVM	0.9	1.53	1.38

ตารางที่ 4.24 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ IBM SoftLayer

IBM SoftLayer Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.78	1.4	1.09
AAC	0.93	1.86	1.71
BCR	0.87	1.31	1.14
CCC	0.9	1.76	1.58
DSI	0.83	1.28	1.05
DCS	1	1.3	1.3
EKM	0.36	1	0.36
GRM	0.91	0.64	1.50
HRS	0.92	1.55	1.43
IAM	0.83	1.28	1.06
IVS	0.82	1.44	1.18
IPY	0.5	1	0.5
MOS	0	1	0
SEF	0.85	1.5	1.28
STA	0.9	1.72	1.55
IVM	0.8	1.53	1.22

ตารางที่ 4.25 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ EBRC

EBRC Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.45	1.4	0.62
AAC	1	1.86	1.86
BCR	0.87	1.31	1.14
CCC	0.7	1.76	1.23
DSI	0.71	1.28	0.91
DCS	0.91	1.3	1.18
EKM	0.93	1	0.93
GRM	1	0.64	1.65
HRS	0.84	1.55	1.29
IAM	0.68	1.28	0.87
IVS	0.91	1.44	1.31
IPY	1	1	1
MOS	0	1	0
SEF	1	1.5	1.5
STA	0.05	1.72	0.09
IVM	0.8	1.53	1.22

ตารางที่ 4.26 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Squiz

Squiz Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.78	1.4	1.09
AAC	0.93	1.86	1.71
BCR	0.79	1.31	1.02
CCC	0.9	1.76	1.58
DSI	0.77	1.28	0.97
DCS	0.73	1.3	0.95
EKM	0.5	1	0.5
GRM	0.87	0.64	1.42
HRS	0.88	1.55	1.36
IAM	0.83	1.28	1.06
IVS	0.85	1.44	1.22
IPY	1	1	1
MOS	0	1	0
SEF	0.62	1.5	0.93
STA	0.65	1.72	1.12
IVM	0.7	1.53	1.07

ตารางที่ 4.27 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Acquria

Acquria Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.78	1.4	1.09
AAC	0.85	1.86	1.58
BCR	0.7	1.31	0.92
CCC	1	1.76	1.76
DSI	0.42	1.28	0.52
DCS	0.37	1.3	0.47
EKM	0.22	1	0.21
GRM	0.96	0.64	1.57
HRS	0.88	1.55	1.36
IAM	0.83	1.28	1.06
IVS	0.73	1.44	1.05
IPY	0	1	0
MOS	0	1	0
SEF	1	1.5	1.5
STA	0.9	1.72	1.55
IVM	0.7	1.53	1.07

ตารางที่ 4.28 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Outreach

Outreach Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.89	1.4	1.25
AAC	0.93	1.86	1.71
BCR	0.53	1.31	0.68
CCC	0.7	1.76	1.23
DSI	0.71	1.28	0.91
DCS	0.73	1.3	0.95
EKM	0.65	1	0.64
GRM	0.82	0.64	1.35
HRS	0.96	1.55	1.49
IAM	0.98	1.28	1.25
IVS	0.7	1.44	1.01
IPY	0	1	0
MOS	0	1	0
SEF	0.7	1.5	1.04
STA	0.75	1.72	1.29
IVM	0.7	1.53	1.07

ตารางที่ 4.29 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Capriza

Capriza Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.89	1.4	1.25
AAC	0.85	1.86	1.58
BCR	0.61	1.31	0.8
CCC	0.9	1.76	1.58
DSI	0.24	1.28	0.31
DCS	0.64	1.3	0.83
EKM	0.79	1	0.79
GRM	0.87	0.64	1.42
HRS	0.84	1.55	1.29
IAM	0.93	1.28	1.19
IVS	0.79	1.44	1.14
IPY	0.25	1	0.25
MOS	0.18	1	0.17
SEF	0.62	1.5	0.93
STA	0.9	1.72	1.55
IVM	0.9	1.53	1.38

ตารางที่ 4.30 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ StarRez

StarRez Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.89	1.4	1.25
AAC	0.85	1.86	1.58
BCR	0.61	1.31	0.8
CCC	0.9	1.76	1.58
DSI	0.36	1.28	0.45
DCS	0.37	1.3	0.47
EKM	0.65	1	0.64
GRM	0.96	0.64	1.57
HRS	0.75	1.55	1.16
IAM	0.83	1.28	1.05
IVS	0.73	1.44	1.06
IPY	1	1	1
MOS	0	1	0
SEF	0.77	1.5	1.16
STA	0.85	1.72	1.46
IVM	0.9	1.53	1.38

ตารางที่ 4.31 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ VMWare AirWatch

VMWare AirWatch Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.78	1.4	1.09
AAC	0.85	1.86	1.58
BCR	0.61	1.31	0.8
CCC	0.8	1.76	1.41
DSI	0.42	1.28	0.52
DCS	0.73	1.3	0.95
EKM	0.93	1	0.93
GRM	0.78	0.64	1.27
HRS	0.88	1.55	1.36
IAM	0.8	1.28	1.02
IVS	0.67	1.44	0.96
IPY	0	1	0
MOS	0	1	0
SEF	0.54	1.5	0.81
STA	0.55	1.72	0.95
IVM	0.9	1.53	1.38

ตารางที่ 4.32 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Data Noah Gmbh

Data Noah Gmbh Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.45	1.4	0.62
AAC	0.7	1.86	1.28
BCR	0.79	1.31	1.02
CCC	0.7	1.76	1.23
DSI	0.77	1.28	0.97
DCS	1	1.3	1.3
EKM	0.58	1	0.57
GRM	0.55	0.64	0.91
HRS	0.84	1.55	1.29
IAM	0.7	1.28	0.9
IVS	0.76	1.44	1.09
IPY	0	1	0
MOS	0	1	0
SEF	0.7	1.5	1.04
STA	0.6	1.72	1.03
IVM	0.8	1.53	1.22

ตารางที่ 4.33 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ CenturyLink

CenturyLink Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.56	1.4	0.78
AAC	0.93	1.86	1.71
BCR	0.74	1.31	0.97
CCC	0.8	1.76	1.41
DSI	0.77	1.28	0.97
DCS	0.82	1.3	1.07
EKM	0.43	1	0.43
GRM	0.73	0.64	1.20
HRS	0.71	1.55	1.10
IAM	0.8	1.28	1.02
IVS	0.79	1.44	1.14
IPY	0.5	1	0.5
MOS	0.04	1	0.03
SEF	0.54	1.5	0.81
STA	0.8	1.72	1.38
IVM	0.2	1.53	0.31

ตารางที่ 4.34 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Tableau

Tableau Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.78	1.4	1.09
AAC	0.85	1.86	1.58
BCR	0.44	1.31	0.56
CCC	0.5	1.76	0.88
DSI	0.59	1.28	0.76
DCS	0.46	1.3	0.59
EKM	0.22	1	0.21
GRM	0.78	0.64	1.27
HRS	0.67	1.55	1.04
IAM	0.73	1.28	0.93
IVS	0.58	1.44	0.84
IPY	0.88	1	0.88
MOS	0.21	1	0.21
SEF	0.62	1.5	0.93
STA	0.65	1.72	1.12
IVM	0.8	1.53	1.22

ตารางที่ 4.35 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Optimizely

Optimizely Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	1	1.4	1.4
AAC	1	1.86	1.86
BCR	0.74	1.31	0.97
CCC	1	1.76	1.76
DSI	0.48	1.28	0.60
DCS	0.64	1.3	0.83
EKM	0.58	1	0.57
GRM	0.46	0.64	0.74
HRS	0.67	1.55	1.04
IAM	0.43	1.28	0.55
IVS	0.7	1.44	1.01
IPY	1	1	1
MOS	0	1	0
SEF	0.31	1.5	0.47
STA	0.65	1.72	1.12
TVM	0.4	1.53	0.61

ตารางที่ 4.36 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Collab9

Collab9 Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.56	1.4	0.78
AAC	0.77	1.86	1.43
BCR	0.66	1.31	0.85
CCC	0.4	1.76	0.70
DSI	0.48	1.28	0.60
DCS	0.55	1.3	0.72
EKM	0	1	0
GRM	0.73	0.64	1.20
HRS	0.67	1.55	1.04
IAM	0.78	1.28	1
IVS	0.67	1.44	0.96
IPY	0	1	0
MOS	0	1	0
SEF	0.77	1.5	1.16
STA	0.4	1.72	0.69
IVM	0.8	1.53	1.22

ตารางที่ 4.37 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Perspectium

Perspectium Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.78	1.4	1.09
AAC	0.39	1.86	0.71
BCR	0.74	1.31	0.97
CCC	0.7	1.76	1.23
DSI	0.48	1.28	0.60
DCS	0.64	1.3	0.83
EKM	0.58	1	0.57
GRM	0.41	0.64	0.68
HRS	0.67	1.55	1.04
IAM	0.43	1.28	0.55
IVS	0.7	1.44	1.01
IPY	0.5	1	0.5
MOS	0.04	1	0.03
SEF	0.31	1.5	0.47
STA	0.65	1.72	1.12
IVM	0.4	1.53	0.61

*ตารางที่ 4.38 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Develloc*us

Develloc*us* Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.89	1.4	1.25
AAC	0.24	1.86	0.43
BCR	0.31	1.31	0.39
CCC	0.8	1.76	1.41
DSI	0.42	1.28	0.52
DCS	1	1.3	1.3
EKM	0.29	1	0.29
GRM	0.5	0.64	0.83
HRS	0.67	1.55	1.04
IAM	0.63	1.28	0.81
IVS	0.04	1.44	0.04
IPY	0	1	0
MOS	0	1	0
SEF	0	1.5	0
STA	0.25	1.72	0.43
IVM	1	1.53	1.53

ตารางที่ 4.39 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Siteimprove

Siteimprove Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.56	1.4	0.78
AAC	0.24	1.86	0.43
BCR	0.57	1.31	0.75
CCC	0.7	1.76	1.23
DSI	0.59	1.28	0.76
DCS	0.82	1.3	1.07
EKM	0.08	1	0.07
GRM	0.37	0.64	0.59
HRS	0.5	1.55	0.78
IAM	0.45	1.28	0.58
IVS	0.55	1.44	0.79
IPY	0	1	0
MOS	0	1	0
SEF	0.47	1.5	0.69
STA	0.6	1.72	1.03
IVM	0.2	1.53	0.31

ตารางที่ 4.40 การสร้างเวกเตอร์คะแนนความมั่นคงและความพึ่งพาได้ของ Eagle.io

Eagle.io Cloud Service			
Control Domain	Compliance Score (cp_n)	Assurance Weight (as_n)	Provider Score (p_n)
AIS	0.34	1.4	0.46
AAC	0.62	1.86	1.15
BCR	0.53	1.31	0.68
CCC	0.5	1.76	0.88
DSI	0.48	1.28	0.60
DCS	0	1.3	0
EKM	0	1	0
GRM	0.78	0.64	1.27
HRS	0.25	1.55	0.39
IAM	0.38	1.28	0.49
IVS	0.52	1.44	0.75
IPY	0	1	0
MOS	0	1	0
SEF	0.08	1.5	0.12
STA	0.25	1.72	0.43
IVM	0	1.53	0

4.1.3 การทดสอบการประเมินความไว้ใจได้ของผู้ให้บริการคลาวด์

ในการทดสอบการประเมินความไว้ใจได้ของผู้ให้บริการคลาวด์จะใช้วิธีการคำนวณจากสมการในหัวข้อที่ 3.7 จะได้ผลการทดสอบการประเมินความไว้ใจได้ของผู้ให้บริการคลาวด์ในแต่ละรายดังตารางที่ 4.11 โดยจะแสดงค่าคุณลักษณะย่อยทั้ง 6 ด้านของความมั่นคงและความพึ่งพาได้ ของผู้ให้บริการคลาวด์ 20 ราย

ตารางที่ 4.41 ผลการทดสอบการประเมินความไว้ใจได้ของผู้ให้บริการคลาวด์ทั้ง 20 ราย

Cloud Provider	Confidentiality	Integrity	Availability	Reliability	Safety	Maintainability	Trustworthiness
Amazon AWS	15.93	16.27	16.32	2.18	2.94	1.89	0.99
Microsoft Azure	15.46	15.78	15.80	2.07	2.86	1.86	0.96
Dropbox	14.27	14.56	14.47	1.76	2.47	1.58	0.85
IBM SoftLayer	13.98	14.28	14.32	1.90	2.74	1.72	0.88
EBRC	13.16	13.33	13.49	1.84	2.56	1.58	0.83
Squiz	12.81	13.09	13.1	1.74	2.37	1.57	0.80
Acquria	12.53	12.82	12.80	1.73	1.90	1.47	0.75
Outreach	12.62	12.92	12.80	1.60	2.19	1.56	0.77
Capriza	12.55	12.86	12.77	1.75	2.01	1.53	0.77
StarRez	12.31	12.63	12.54	1.77	1.82	1.44	0.74
VMWare AirWatch	12.06	12.33	12.28	1.66	2.04	1.43	0.74
Data Noah Gmbh	11.65	11.82	11.95	11.55	2.35	1.37	0.73
CenturyLink	11.19	11.39	11.47	1.46	2.41	1.56	0.73
Tableau	10.47	10.73	10.62	1.52	1.78	1.31	0.65
Optimizely	10.76	11.13	11.05	1.50	2.08	1.34	0.68
Collab91	10.12	10.32	1036	1.54	1.85	1.30	0.65
Perspectium	8.80	9.09	9.09	1.11	1.69	5.12	0.54
Develocus	8.71	9.05	8.85	1.01	1.52	0.08	0.51
Siteimprove	7.76	7.97	7.98	0.79	1.66	0.85	0.47
Eagle.io	5.65	5.78	5.85	0.96	1.18	0.89	0.39

จากตารางแสดงผลการทดลองจะเห็นได้ว่าค่าคุณลักษณะด้าน ความเชื่อถือได้ ความปลอดภัย และความสามารถในการบำรุงรักษา ของผู้ให้บริการคลาวด์ทั้ง 20 ราย อยู่ในระดับที่ต่ำกว่าคุณลักษณะด้าน การรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน เนื่องจากในตารางที่ 3.7 ซึ่งแสดงระดับความเชื่อมโยงระหว่างคุณลักษณะย่อยทางด้านความมั่นคงและความพึ่งพาได้กับแต่ละโดเมนการควบคุมของเมตริกซ์ควบคุมคลาวด์ จะพบว่าโดเมนการควบคุมต่างๆจะสะท้อนคุณลักษณะทางด้านความมั่นคง ทั้ง 3 คุณลักษณะ ได้แก่ การรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน มากกว่าคุณลักษณะทางด้านความพึ่งพาได้ ดังนั้นการแปลผลการประเมินค่าความไว้ใจได้จึงไม่ควรนำค่าคะแนนของต่างคุณลักษณะย่อยของผู้ให้บริการรายเดียวกันมาเปรียบเทียบกัน เช่น ไม่สามารถสรุปได้ว่า Microsoft Azure มีค่าคุณลักษณะด้านการรักษาความลับ (15.46) ดีกว่าด้านความเชื่อถือได้ (2.07) แต่สามารถเปรียบเทียบค่าคุณลักษณะย่อยในด้านเดียวกันของผู้ให้บริการต่างรายได้ เช่น สามารถสรุปได้ว่า Microsoft Azure มีค่าคุณลักษณะด้านการรักษาความลับ (15.46) ที่ดีกว่า Optimizely (10.76)

นอกจากนี้หากผู้ใช้บริการต้องการพิจารณาความแตกต่างระหว่างค่าคะแนนคุณลักษณะในแต่ละด้านของผู้ให้บริการว่ามากน้อยกว่ากันเพียงใด เช่น Microsoft Azure กับ Optimizely ซึ่งมีคะแนนด้านการรักษาความลับต่างกัน 4.70 หน่วย (15.46-10.76) นั้น ความแตกต่างนี้แสดงถึงคุณภาพที่แตกต่างกันมากหรือยังถือว่าไม่มาก ผู้ใช้บริการสามารถพิจารณาความอ่อนไหวของคะแนนได้จากความแตกต่างของจำนวนการปฏิบัติตามข้อคำถามใน CAIQ ซึ่งเกี่ยวข้องกับคุณลักษณะย่อยด้านนั้นๆ เพิ่มเติมด้วย โดยดูจากภาคผนวก ข. ผู้ใช้บริการจะสรุปได้ว่า คะแนนด้านการรักษาความลับของ Microsoft Azure และ Optimizely ซึ่งต่างกัน 4.70 หน่วย เกิดจากการที่ Microsoft Azure มีจำนวนการปฏิบัติตามข้อคำถามใน CAIQ ซึ่งเกี่ยวข้องกับคุณลักษณะด้านการรักษาความลับมากกว่า Optimizely อยู่ประมาณ 60 ข้อ

4.2 การประเมินความสมเหตุสมผลของค่าความไว้ใจได้โดยการวิเคราะห์สหสัมพันธ์

การประเมินความสมเหตุสมผล (Validation) ของค่าความไว้ใจได้จะทำโดยการวิเคราะห์สหสัมพันธ์ (Correlation) ระหว่างค่าความไว้ใจได้ กับผลการประเมินโดยบุคคลที่ 3 ซึ่งในที่นี้คือผลการประเมินการรับประกันได้ (Cloud Assurance Rating) โดยบริษัท Cloud eAssurance an efortresses Company (https://www.cloudeassurance.com) ซึ่งทำการประเมินผู้ให้บริการคลาวด์โดยองค์รวม (Holistic Approach) ในด้านการจัดการความมั่นคง (Security Management) การกำกับดูแล (Governance) การจัดการความเสี่ยง (Risk Management) การปฏิบัติตาม (Compliance) และวุฒิภาวะ (Maturity) เป็นต้น

การประเมินความสมเหตุสมผลนั้นจะทำโดยนำคะแนนความไว้ใจได้ของผู้ให้บริการ 20 ราย ได้แก่ Amazon AWS, Windows Azure, Dropbox, IBM SoftLayer, EBRC, Squiz laaS, Acquria, Outreach, Capriza, StarRez, VMware AirWatch, Data Noah GmbH, CenturyLink, Tableau, Optimizely, Collab9 laaS, Perspectium, Develloc us, Siteimprove และ eagle.io มาทดสอบสหสัมพันธ์อย่างง่าย (Simple Correlation) กับคะแนนการประเมินที่ได้จาก Cloud eAssurance ดังแสดงในตารางที่ 4.42 โดยมีสมมติฐานคือ

H0: คะแนนความไว้ใจได้ไม่มีความสัมพันธ์ในรูปแบบเชิงเส้นกับคะแนนการประเมินที่ได้จากบุคคลที่ 3 (Cloud eAssurance)

H1: คะแนนความไว้ใจได้มีความสัมพันธ์ในรูปแบบเชิงเส้นเป็นเชิงบวกกับคะแนนการประเมินที่ได้จากบุคคลที่ 3 (Cloud eAssurance)

ตารางที่ 4.42 คะแนนความไว้ใจได้ของผู้ให้บริการคลาวด์กับคะแนนการประเมินที่ได้จากบุคคลที่ 3 (Cloud eAssurance)

Provider Name	Trustworthiness Score	Third Party Score
Amazon AWS	0.99	488
Windows Azure	0.96	479
Dropbox	0.85	441
IBM SoftLayer	0.88	471
EBRC	0.83	419
Squiz laaS	0.80	373
Acquia	0.75	367
Outreach	0.77	347
Capriza	0.77	338
StarRez	0.74	200
VMware AirWatch	0.74	249
Data Noah GmbH	0.73	226
CenturyLink	0.73	273
Tableau	0.65	194
Optimizely	0.68	171
Collab9 laaS	0.65	158
Perspectium	0.54	152

ตารางที่ 4.42 คะแนนความไว้ใจได้ของผู้ให้บริการคลาวด์กับคะแนนการประเมินที่ได้จากบุคคลที่ 3 (Cloud eAssurance) (ต่อ)

Provider Name	Trustworthiness Score	Third Party Score
Develocus	0.51	123
Siteimprove	0.47	136
eagle.io	0.39	91

การคำนวณค่าสัมประสิทธิ์สหสัมพันธ์ r ทำได้โดย

$$r = \frac{\mathrm{n}\sum xy - \sum x \sum y}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}}$$

จากตารางที่ 4.42 คำนวณค่า r ได้เป็น

$$r = \frac{20(4466.99) - (14.43)(5696)}{\sqrt{[20(10.8689) - (208.2249)][20(1952396) - (32444416)]}}$$

$$r = \frac{7146.52}{7774.48}$$

r = 0.919

จากค่า r ที่ได้ สรุปได้ว่าค่าความไว้ใจได้ของผู้ให้บริการคลาวด์มีความสัมพันธ์ในรูปแบบเชิงเส้นเป็นเชิงบวกในระดับสูงมากกับคะแนนการประเมินที่ได้จากบุคคลที่ 3 (Cloud eAssurance) เมื่อทดสอบนัยสำคัญทางสถิติ โดยคำนวณค่า t ด้วยสมการ

$$t = r\sqrt{\frac{n-2}{1-r^2}}$$

จะได้ว่า $t = 0.919\sqrt{\frac{20-2}{1-0.919^2}}$ = 9.9052

เมื่อ α = 0.05, df = n-2 =18 พบว่า ค่า t=9.9052 ที่คำนวณได้ มากกว่าค่า $t_{(.05,18)}$ ซึ่งเท่ากับ 1.7341 ดังนั้น จึงปฏิเสธ H0 และยอมรับ H1 นั่นคือคะแนนความไว้ใจได้มีความสัมพันธ์ในรูปแบบเชิงเส้นเป็นเชิงบวกกับคะแนนการประเมินที่ได้จากบุคคลที่ 3 (Cloud eAssurance) อย่างมีนัยสำคัญที่ระดับความเชื่อมั่น 95%

บทที่ 5
สรุปผลการวิจัย

5.1 สรุปผลการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อกำหนดวิธีการประเมินความไว้ใจได้ของผู้ให้บริการคลาวด์โดยอิงเมตริกซ์ควบคุมคลาวด์ โดยผู้วิจัยได้ทำการกำหนดเกณฑ์ในการพิจารณาทางด้านความไว้ใจได้ ซึ่งประกอบไปด้วยคุณลักษณะย่อยทั้ง 6 ด้านของความมั่นคงและความพึ่งพาได้ ได้แก่ การรักษาความลับ บูรณภาพ สภาพพร้อมใช้งาน ความเชื่อถือได้ ความปลอดภัย และความสามารถในการบำรุงรักษา และทำการเชื่อมโยงคุณลักษณะทางด้านความไว้ใจได้จากเกณฑ์พิจารณาเข้ากับมาตรฐานการควบคุมความมั่นคง NIST SP800-53 และ AICPA Trust Service Criteria ซึ่งเป็นมาตรฐานการควบคุมความมั่นคงที่เชื่อมโยงกับเมตริกซ์ควบคุมคลาวด์ จากนั้นทำการสร้างเมตริกซ์คุณลักษณะของความมั่นคงและความพึ่งพาได้ของแต่ละโดเมนการควบคุมในเมตริกซ์ควบคุมคลาวด์ และนำข้อมูลการปฏิบัติตามแบบประเมิน CAIQ ที่ผู้ให้บริการคลาวด์เผยแพร่อยู่บนเว็บไซต์ของ CSA STAR (Security, Trust & Assurance Registry) มาเพื่อใช้ในการประเมินระดับความไว้ใจได้ของผู้ให้บริการคลาวด์

ผู้วิจัยได้พัฒนาแอปพลิเคชันที่สามารถใช้ในการประเมินความไว้ใจได้ของผู้ให้บริการคลาวด์และสามารถเปรียบเทียบผู้ให้บริการคลาวด์ในแต่ละรายโดยสามารถแสดงผลในรูปแบบตัวเลขและกราฟได้ จากการประเมินความสมเหตุสมผลของค่าความไว้ใจได้ของผู้ให้บริการคลาวด์เปรียบเทียบกับผลการประเมินของบุคคลที่ 3 พบว่ามีความสัมพันธ์กันในเชิงบวกในระดับสูงมากอย่างมีนัยสำคัญที่ระดับความเชื่อมั่น 95%

5.2 ปัญหาและข้อจำกัด

ปัญหาและข้อจำกัดของงานวิจัยมีดังนี้

1) ข้อมูลของผู้ให้บริการคลาวด์ที่นำมาประเมิน เป็นเพียงข้อมูลที่เผยแพร่ต่อสาธารณะบนเว็บไซต์ของ CSA STAR เท่านั้น และเป็นเพียงการประเมินตนเอง (Self-Assessment) ของผู้ให้บริการคลาวด์ซึ่งข้อมูลบางอย่างอาจคลาดเคลื่อนจากความเป็นจริง และผู้ใช้บริการไม่สามารถรู้เทคนิคเชิงลึกว่าผู้ให้บริการคลาวด์ได้ทำการควบคุมความมั่นคงข้อนั้นๆจริงหรือไม่ ต่างจากการประเมินโดยให้บุคคลที่ 3 มาทำการประเมินให้และทำการออกใบรับรอง (Certification) ซึ่งจะทำให้ข้อมูลที่เผยแพร่มีความน่าเชื่อถือมากยิ่งขึ้น วิธีการประเมินความไว้ใจได้ที่เสนอจึงนับว่าเป็นประโยชน์ต่อผู้ใช้บริการในการประเมินเบื้องต้น

2) คะแนนความไว้ใจได้ของผู้ให้บริการคลาวด์นั้น เป็นเพียงข้อมูลส่วนหนึ่งที่ใช้ในการตัดสินใจเลือกใช้บริการคลาวด์ ซึ่งในการตัดสินใจเลือกใช้ผู้ให้บริการคลาวด์จำเป็นต้องดูปัจจัยอย่างอื่นประกอบเช่น ราคา (Price) ประสิทธิภาพ (Performance) ข้อตกลงด้านการใช้งาน (Service Level Agreement) เป็นต้น

5.3 แนวทางการวิจัยต่อไป

แนวทางในการพัฒนางานวิจัยนี้ต่อมีดังนี้

1) พัฒนาโดยการเพิ่มมาตรฐานหรือวิธีการที่นำมาใช้ในการแยกแยะคุณลักษณะของความมั่นคงและความพึ่งพาได้ให้มีความหลากหลายมากยิ่งขึ้น เพื่อเพิ่มความแม่นยำและความหลากหลายในการแยกแยะคุณลักษณะของความมั่นคงและความพึ่งพาได้
2) ปรับปรุงเครื่องมือสนับสนุนให้มีความสามารถเพิ่มมากขึ้น เช่นทำเป็นระบบ ที่สามารถเชื่อมต่อโดยตรงกับข้อมูลใน CSA STAR และเพิ่มเติมในส่วนของข้อมูลผู้ใช้ในการตัดสินใจเลือกใช้บริการคลาวด์ในส่วนอื่นๆ เช่น ราคา (Price) ประสิทธิภาพ (Performance) ใบรับรอง (Certificate) ชื่อเสียง (Reputation) เป็นต้น

รายการอ้างอิง

[1] M. B. Mollah, K. R. Islam, and S. S. Islam, "Next generation of computing through cloud computing technology," in 2012 25*th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2012, pp. 1-6.

[2] *Guidelines on Security and Privacy in Public Cloud Computing*, December 2011.

[3] E. Jonsson, "Towards an integrated conceptual model of security and dependability," in *First International Conference on Availability, Reliability and Security (ARES'*06), 2006, p. 8 pp.

[4] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing,* vol. 1, no. 1, pp. 11-33, 2004.

[5] V. Basili, P. Donzelli, and S. Asgari, "A unified model of dependability: capturing dependability in context," *IEEE Software,* vol. 21, no. 6, pp. 19-25, 2004.

[6] Cloud Security Alliance. (2016. June 10). *Cloud Controls Matrix*. Available: https://cloudsecurityalliance.org/research/ccm/

[7] Cloud Security Alliance. (2016. May 12). *Consensus Assessments Initiative Questionnaire*. Available: https://cloudsecurityalliance.org/group/consensus-assessments/

[8] Cloud Security Alliance. (2017). *Security, Trust & Assurance Registry (STAR)*. Available: https://cloudsecurityalliance.org/star

[9] *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

[10] *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

[11] *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

[12] *Trust Services Principle and Criteria*, June 2015.

[13] S. M. Habib, V. Varadharajan, and M. Mühlhäuser, "A Trust-Aware Framework for Evaluating Security Controls of Service Providers in Cloud Marketplaces," in 2013 12*th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2013, pp. 459-468.

[14] P. Bedi, H. Kaur, and B. Gupta, "Trustworthy Service Provider Selection in Cloud Computing Environment," in 2012 *International Conference on Communication Systems and Network Technologies*, 2012, pp. 714-719.

[15] B. Michael, "In Clouds Shall We Trust?," *IEEE Security & Privacy,* vol. 7, no. 5, pp. 3-3, 2009.

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

[17] N. Pumvarapruek and T. Senivongse, "Classifying cloud provider security conformance to cloud controls matrix," in 2014 11*th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, 2014, pp. 268-273.

[18] N. Bhensook and T. Senivongse, "An assessment of security requirements compliance of cloud providers," in 4*th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, 2012, pp. 520-525.

[19] T. O. Mayayise and I. O. Osunmakinde, "A compliant assurance model for assessing the trustworthiness of cloud-based e-commerce systems," in 2013 *Information Security for South Africa*, 2013, pp. 1-8.

[20] S. Harris, *CISSP Exam Guide*. Mcgraw Hill, 2013.

[21] *National Information Assurance (IA) Glossary*, April 2010.

[22] D. M. Nicol, W. H. Sanders, and K. S. Trivedi, "Model-based evaluation: from dependability to security," *IEEE Transactions on Dependable and Secure Computing,* vol. 1, no. 1, pp. 48-65, 2004.

[23] K. S. Trivedi, D. S. Kim, A. Roy, and D. Medhi, "Dependability and security models," in 2009 7*th International Workshop on Design of Reliable Communication Networks*, 2009, pp. 11-20.

[24] H. I. Yang and A. Helal, "Safety Enhancing Mechanisms for Pervasive Computing Systems in Intelligent Environments," in 2008 *Sixth Annual IEEE*

International Conference on Pervasive Computing and Communications (PerCom), 2008, pp. 525-530.

[25] J. Hao and Y. Yu, "Computer-aided maintainability in China," in *Annual Reliability and Maintainability Symposium.* 1998 *Proceedings. International Symposium on Product Quality and Integrity*, 1998, pp. 274-278.

[26] Allen B. Tucker, *Computer Science Handbook*. 2004.

[27] Benjamin S. Blanchard, Dinesh C. Verma, and Elmer L. Peterson, *Maintainability: A Key to Effective Serviceability and Maintenance Management*. 1995.

[28] C. Phattanateeradej and T. Senivongse, "Storage and search tool for cloud provider security information in CSA STAR," in 2016 13*th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, 2016, pp. 1-8.

ภาคผนวก

ภาคผนวก ก
ตารางการเชื่อมโยงมาตรฐานทางด้านความมั่นคง

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Application & Interface Security Application Security	AIS-01	CC7.1	SC-2 SC-3 SC-4 SC-5 SC-6 SC-7 SC-8 SC-9 SC-10 SC-11 SC-12 SC-13 SC-14 SC-17 SC-18 SC-20 SC-21 SC-22 SC-23	1	1	1	0	0	0
Application & Interface Security Customer Access Requirements	AIS-02	CC5.1	CA-1 CA-2 CA-5 CA-6	1	1	1	0	0	0
Application & Interface Security Data Integrity	AIS-03	PI1.2 PI1.3 PI1.5	SI-10 SI-11 SI-2 SI-3 SI-4 SI-6 SI-7 SI-9	0	1	0	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Application & Interface Security Data Security / Integrity	AIS-04	CC5.6	AC-1 AC-4 SC-1 SC-16	1	1	1	0	0	0
Audit Assurance & Compliance Audit Planning	AAC-01	CC4.1	CA-2 CA-7 PL-6	1	1	1	0	0	0
Audit Assurance & Compliance Independent Audits	AAC-02	CC4.1	CA-1 CA-2 CA-6 RA-5	1	1	1	0	0	0
Audit Assurance & Compliance Information System Regulatory Mapping	AAC-03	CC3.1	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IA-7 IR-1 MA-1 MP-1 PE-1 PL-1 PM-1 PS-1 RA-1 RA-2 SA-1 SA-6 SC-1 SC-13 SI-1	1	1	1	1	1	1

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Business Continuity Management & Operational Resilience Business Continuity Planning	BCR-01	CC3.1 A1.2 A1.3	CP-1 CP-2 CP-3 CP-4 CP-6 CP-7 CP-8 CP-9 CP-10 PE-17	1	1	1	1	1	0
Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02	A1.2	CP-2 CP-3 CP-4	0	0	1	1	0	0
Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental Conditions	BCR-03	A1.1 A1.2 A1.3	PE-1 PE-4 PE-13	0	0	1	0	1	0
Business Continuity Management & Operational Resilience Documentation	BCR-04	CC1.3 CC1.4 CC2.1	CP-9 CP-10 SA-5 SA-10 SA-11	1	1	1	1	0	0
Business Continuity Management & Operational Resilience Environmental Risks	BCR-05	CC3.1 A1.1 A1.2	PE-1 PE-13 PE-14 PE-15 PE-18	1	1	1	0	1	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Business Continuity Management & Operational Resilience Equipment Location	BCR-06	CC3.1 A1.1 A1.2	PE-1 PE-5 PE-14 PE-15 PE-18	1	1	1	0	1	0
Business Continuity Management & Operational Resilience Equipment Maintenance	BCR-07	A1.1 A1.2 CC4.1	MA-2 MA-3 MA-4 MA-5 MA-6	1	1	1	0	0	1
Business Continuity Management & Operational Resilience Equipment Power Failures	BCR-08	A1.1 A1.2	CP-8 PE-1 PE-9 PE-10 PE-11 PE-12 PE-13 PE-14	0	0	1	1	1	0
Business Continuity Management & Operational Resilience Impact Analysis	BCR-09	CC3.1 A1.2 A1.3	RA-3	1	1	1	0	0	0
Business Continuity Management & Operational Resilience Policy	BCR-10	CC3.2	CM-2 CM-3 CM-4 CM-5 CM-6 CM-9 MA-4 SA-3 SA-4 SA-5 SA-8 SA-10 SA-11 SA-12	1	1	1	0	0	1

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Business Continuity Management & Operational Resilience Retention Policy	BCR-11	A1.2 A1.3 I3.21	CP-2 CP-6 CP-7 CP-8 CP-9 SI-12 AU-11	0	1	1	1	0	0
Change Control & Configuration Management New Development / Acquisition	CCC-01	CC7.2 CC7.1 CC7.4	CA-1 CM-1 CM-9 PL-1 PL-2 SA-1 SA-3 SA-4	1	1	1	0	0	0
Change Control & Configuration Management Outsourced Development	CCC-02	CC7.1 CC7.4	SA-4 SA-5 SA-8 SA-9 SA-10 SA-11 SA-12 SA-13	1	1	1	0	0	0
Change Control & Configuration Management Quality Testing	CCC-03	CC7.1 CC7.4	CM-1 CM-2 SA-3 SA-4 SA-5 SA-8 SA-10 SA-11 SA-13	1	1	1	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Change Control & Configuration Management Unauthorized Software Installations	CCC-04	CC5.5 CC5.8 CC7.4	CM-1 CM-2 CM-3 CM-5 CM-7 CM-8 CM-9 SA-6 SA-7 SI-1 SI-3 SI-4 SI-7	1	1	1	0	0	0
Change Control & Configuration Management Production Changes	CCC-05	CC7.4	CA-1 CA-6 CA-7 CM-2 CM-3 CM-5 CM-6 CM-9 PL-2 PL-5 SI-2 SI-6 SI-7	1	1	1	0	0	0
Data Security & Information Lifecycle Management Classification	DSI-01	CC3.1	RA-2 AC-4	1	1	1	0	0	0
Data Security & Information Lifecycle Management Data Inventory / Flows	DSI-02			0	0	0	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Data Security & Information Lifecycle Management Ecommerce Transactions	DSI-03	CC5.7 PI1.5	AC-14 AC-21 AC-22 IA-8 AU-10 SC-4 SC-8 SC-9	1	1	1	0	0	0
Data Security & Information Lifecycle Management Handling / Labeling / Security Policy	DSI-04	CC5.1	AC-16 MP-1 MP-3 PE-16 SI-12 SC-9	1	1	1	0	1	0
Data Security & Information Lifecycle Management Non-Production Data	DSI-05	C1.3 CC5.6 C1.1	SA-11 CM-04	1	1	1	0	0	0
Data Security & Information Lifecycle Management Ownership / Stewardship	DSI-06	CC2.3 CC3.1	CA-2 PM-5 PS-2 RA-2 SA-2	1	1	1	0	0	0
Data Security & Information Lifecycle Management Secure Disposal	DSI-07	C1.3 CC5.6	MP-6 PE-1	1	1	1	0	1	0
Datacenter Security Asset Management	DCS-01	CC3.1		1	1	1	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Datacenter Security Controlled Access Points	DCS-02	CC5.5	PE-2 PE-3 PE-6 PE-7 PE-8 PE-18	1	1	1	0	1	0
Datacenter Security Equipment Identification	DCS-03	CC5.1	IA-3 IA-4	1	1	1	0	0	0
Datacenter Security Off-Site Authorization	DCS-04	CC5.1 CC5.5	AC-17 MA-1 PE-1 PE-16 PE-17	1	1	1	0	1	1
Datacenter Security Off-Site Equipment	DCS-05	CC5.7	CM-8	1	1	1	0	0	0
Datacenter Security Policy	DCS-06	CC5.5	PE-2 PE-3 PE-4 PE-5 PE-6	1	1	1	0	1	0
Datacenter Security Secure Area Authorization	DCS-07	CC5.5	PE-7 PE-16 PE-18	1	1	1	0	1	0
Datacenter Security Unauthorized Persons Entry	DCS-08	CC5.5	MA-1 MA-2 PE-16	1	1	1	0	1	1
Datacenter Security User Access	DCS-09	CC5.5	PE-2 PE-3 PE-6 PE-18	1	1	1	0	1	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Encryption & Key Management Entitlement	EKM-01			0	0	0	0	0	0
Encryption & Key Management Key Generation	EKM-02	CC5.7 CC5.6	SC-12 SC-13 SC-17 SC-28	1	1	1	0	0	0
Encryption & Key Management Sensitive Data Protection	EKM-03	CC5.7 CC5.6	AC-18 IA-3 IA-7 SC-7 SC-8 SC-9 SC-13 SC-16 SC-23 SI-8	1	1	1	0	0	0
Encryption & Key Management Storage and Access	EKM-04			0	0	0	0	0	0
Governance and Risk Management Baseline Requirements	GRM-01	CC3.2	CM-2 SA-2 SA-4	1	1	1	0	0	0
Governance and Risk Management Data Focus Risk Assessments	GRM-02	CC3.1	CA-3 RA-2 RA-3 MP-8 PM-9 SI-12	1	1	1	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Governance and Risk Management Management Oversight	GRM-03	CC3.2	AT-2 AT-3 CA-1 CA-5 CA-6 CA-7 PM-10	1	1	1	0	0	0
Governance and Risk Management Management Program	GRM-04		PM-1 PM-2 PM-3 PM-4 PM-5 PM-6 PM-7 PM-8 PM-9 PM-10 PM-11	0	0	0	0	0	0
Governance and Risk Management Management Support/Involvement	GRM-05	CC1.2	CM-1 PM-1 PM-11	1	1	1	0	0	0
Governance and Risk Management Policy	GRM-06	CC3.2 CC1.2 CC2.3	AC-1 AT-1 AU-1 CA-1 CM-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PS-1 SA-1 SC-1 SI-1	1	1	1	0	1	1
Governance and Risk Management Policy Enforcement	GRM-07	CC6.2 CC2.5	PL-4 PS-1 PS-8	1	1	1	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Governance and Risk Management Policy Impact on Risk Assessments	GRM-08		CP-2 RA-2 RA-3	0	0	0	1	0	0
Governance and Risk Management Policy Reviews	GRM-09	CC3.2	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IA-5 IR-1 MA-1 MP-1 PE-1 PL-1 PM-1 PS-1 RA-1 SA-1 SC-1 SI-1	1	1	1	1	1	1
Governance and Risk Management Risk Assessments	GRM-10	CC3.1 CC3.3	PL-5 RA-2 RA-3	1	1	1	0	0	0
Governance and Risk Management Risk Management Framework	GRM-11	CC3.1	AC-4 CA-2 CA-6 PM-9 RA-1	1	1	1	0	0	0
Human Resources Asset Returns	HRS-01	CC5.6	PS-4	1	1	1	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Human Resources Background Screening	HRS-02	CC1.3 CC1.4	PS-2 PS-3	1	1	1	0	0	0
Human Resources Employment Agreements	HRS-03	CC2.2 CC2.3	PL-4 PS-6 PS-7	1	1	1	0	0	0
Human Resources Employment Termination	HRS-04	CC5.4	PS-4 PS-5	1	1	1	0	0	0
Human Resources Mobile Device Management	HRS-05	CC5.6	AC-17 AC-18 AC-19 MP-2 MP-4 MP-6	1	1	1	0	0	0
Human Resources Non-Disclosure Agreements	HRS-06	CC4.1	PL-4 PS-6 SA-9	1	1	1	0	0	0
Human Resources Non-Disclosure Agreements	HRS-07		AT-3 PL-4 PM-10 PS-1 PS-6 PS-7	0	0	0	0	0	0
Human Resources Technology Acceptable Use	HRS-08	CC3.2 CC6.2	AC-8 AC-20 PL-4	1	1	1	0	0	0
Human Resources Training / Awareness	HRS-09	CC2.2 CC2.3	AT-1 AT-2 AT-3 AT-4	1	1	1	0	0	0
Human Resources User Responsibility	HRS-10	CC3.2	AT-2 AT-3 AT-4 PL-4	1	1	1	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Human Resources Workspace	HRS-11	CC5.5 CC5.6	AC-11 MP-2 MP-3 MP-4	1	1	1	0	0	0
Identity & Access Management Audit Tools Access	IAM-01	CC5.1	AU-9 AU-11 AU-14	1	1	1	0	0	0
Identity & Access Management Credential Lifecycle / Provision Management	IAM-02		AC-1 IA-1	0	0	0	0	0	0
Identity & Access Management Diagnostic / Configuration Ports Access	IAM-03	CC5.1	CM-7 MA-3 MA-4 MA-5	1	1	1	0	0	1
Identity & Access Management Policies and Procedures	IAM-04			0	0	0	0	0	0
Identity & Access Management Segregation of Duties	IAM-05	CC5.1	AC-1 AC-2 AC-5 AC-6 AU-1 AU-6 SI-1 SI-4	1	1	1	0	0	0
Identity & Access Management Source Code Access Restriction	IAM-06	CC7.4	CM-5 CM-6	1	1	1	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Identity & Access Management Third Party Access	IAM-07	CC3.1	CA-3 MA-4 RA-3	1	1	1	0	0	1
Identity & Access Management Trusted Sources	IAM-08	CC3.3		1	1	1	0	0	0
Identity & Access Management User Access Authorization	IAM-09		AC-3 AC-5 AC-6 IA-2 IA-4 IA-5 IA-8 MA-5 PS-6 SA-7 SI-9	0	0	0	0	0	1
Identity & Access Management User Access Reviews	IAM-10		AC-2 AU-6 PM-10 PS-6 PS-7	0	0	0	0	0	0
Identity & Access Management User Access Revocation	IAM-11		AC-2 PS-4 PS-5	0	0	0	0	0	0
Identity & Access Management User ID Credentials	IAM-12	CC5.3	AC-1 AC-2 AC-3 AC-11 AU-2 AU-11 IA-1 IA-2 IA-5 IA-6 IA-8 SC-10	1	1	1	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Identity & Access Management Utility Programs Access	IAM-13	CC5.1	AC-5 AC-6 CM-7 SC-3 SC-19	1	1	1	0	0	0
Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	IVS-01	CC6.2	AU-1 AU-2 AU-3 AU-4 AU-5 AU-6 AU-7 AU-9 AU-11 AU-12 AU-14 SI-4	1	1	1	0	0	0
Infrastructure & Virtualization Security Change Detection	IVS-02			0	0	0	0	0	0
Infrastructure & Virtualization Security Clock Synchronization	IVS-03	CC6.2	AU-1 AU-8	1	1	1	0	0	0
Infrastructure & Virtualization Security Information System Documentation	IVS-04	A1.1 A1.2 CC4.1	SA-4	1	1	1	0	0	0
Infrastructure & Virtualization Security Vulnerability Management	IVS-05			0	0	0	0	0	0
Infrastructure & Virtualization Security Network Security	IVS-06	CC5.6	SC-7	1	1	1	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Infrastructure & Virtualization Security OS Hardening and Base Controls	IVS-07			0	0	0	0	0	0
Infrastructure & Virtualization Security Production / Non-Production Environments	IVS-08	CC5.6	SC-2	1	1	1	0	0	0
Infrastructure & Virtualization Security Segmentation	IVS-09	CC5.6	AC-4 SC-2 SC-3 SC-7	1	1	1	0	0	0
Infrastructure & Virtualization Security VM Security - Data Protection	IVS-10			0	0	0	0	0	0
Infrastructure & Virtualization Security Hypervisor Hardening	IVS-11			0	0	0	0	0	0
Infrastructure & Virtualization Security Wireless Security	IVS-12	CC5.6	AC-1 AC-18 CM-6 PE-4 SC-3 SC-7	1	1	1	0	1	0
Infrastructure & Virtualization Security Network Architecture	IVS-13			0	0	0	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Interoperability & Portability APIs	IPY-01			0	0	0	0	0	0
Interoperability & Portability Data Request	IPY-02			0	0	0	0	0	0
Interoperability & Portability Policy & Legal	IPY-03			0	0	0	0	0	0
Interoperability & Portability Standardized Network Protocols	IPY-04			0	0	0	0	0	0
Interoperability & Portability Virtualization	IPY-05			0	0	0	0	0	0
Mobile Security Anti-Malware	MOS-01			0	0	0	0	0	0
Mobile Security Application Stores	MOS-02			0	0	0	0	0	0
Mobile Security Approved Applications	MOS-03			0	0	0	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800 -53	Attribute					
				C	I	A	R	S	M
Mobile Security Approved Software for BYOD	MOS-04			0	0	0	0	0	0
Mobile Security Awareness and Training	MOS-05			0	0	0	0	0	0
Mobile Security Cloud Based Services	MOS-06			0	0	0	0	0	0
Mobile Security Compatibility	MOS-07			0	0	0	0	0	0
Mobile Security Device Eligibility	MOS-08			0	0	0	0	0	0
Mobile Security Device Inventory	MOS-09			0	0	0	0	0	0
Mobile Security Device Management	MOS-10			0	0	0	0	0	0
Mobile Security Encryption	MOS-11			0	0	0	0	0	0
Mobile Security Jailbreaking and Rooting	MOS-12			0	0	0	0	0	0
Mobile Security Legal	MOS-13			0	0	0	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Mobile Security Lockout Screen	MOS-14			0	0	0	0	0	0
Mobile Security Operating Systems	MOS-15			0	0	0	0	0	0
Mobile Security Passwords	MOS-16			0	0	0	0	0	0
Mobile Security Policy	MOS-17			0	0	0	0	0	0
Mobile Security Remote Wipe	MOS-18			0	0	0	0	0	0
Mobile Security Security Patches	MOS-19			0	0	0	0	0	0
Mobile Security Users	MOS-20			0	0	0	0	0	0
Security Incident Management, E-Discovery, & Cloud Forensics Contact / Authority Maintenance	SEF-01	CC3.3	AT-5 IR-6 SI-5	1	1	1	0	0	0
Security Incident Management, E-Discovery, & Cloud Forensics Incident Management	SEF-02	CC5.5 CC6.2	IR-1 IR-2 IR-3 IR-4 IR-5 IR-7 IR-8	1	1	1	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Security Incident Management, E-Discovery, & Cloud Forensics Incident Reporting	SEF-03	CC2.3 CC2.5 C1.4 C1.5	IR-2 IR-6 IR-7 SI-4 SI-5	1	1	1	0	0	0
Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Legal Preparation	SEF-04	CC2.5 CC6.2	AU-6 AU-7 AU-9 AU-11 IR-5 IR-7 IR-8	1	1	1	0	0	0
Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Metrics	SEF-05	CC6.2 CC4.1	IR-4 IR-5 IR-8	1	1	1	0	0	0
Supply Chain Management, Transparency, and Accountability Data Quality and Integrity	STA-01			0	0	0	0	0	0
Supply Chain Management, Transparency, and Accountability Incident Reporting	STA-02			0	0	0	0	0	0
Supply Chain Management, Transparency, and Accountability Network / Infrastructure Services	STA-03	CC2.2 CC2.3	SC-20 SC-21 SC-22 SC-23 SC-24	1	1	1	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Supply Chain Management, Transparency, and Accountability Provider Internal Assessments	STA-04			0	0	0	0	0	0
Supply Chain Management, Transparency, and Accountability Supply Chain Agreements	STA-05	CC2.2 CC2.3 CC5.5 C1.4 C1.5	CA-3 MP-5 PS-7 SA-6 SA-7 SA-9	1	1	1	0	0	0
Supply Chain Management, Transparency, and Accountability Supply Chain Governance Reviews	STA-06			0	0	0	0	0	0
Supply Chain Management, Transparency, and Accountability Supply Chain Metrics	STA-07			0	0	0	0	0	0

ตารางที่ ก.1 การเชื่อมโยงมาตรฐานทางด้านความมั่นคง AICPA และ NIST SP800-53 เข้ากับเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain and Control	Control ID	AICPA 2014 TSC	NIST SP800-53	Attribute					
				C	I	A	R	S	M
Supply Chain Management, Transparency, and Accountability Third Party Assessment	STA-08			0	0	0	0	0	0
Supply Chain Management, Transparency, and Accountability Third Party Audits	STA-09	CC2.2 CC2.3 C1.4 C1.5	CA-3 SA-9 SA-12 SC-7	1	1	1	0	0	0
Threat and Vulnerability Management Anti-Virus / Malicious Software	TVM-01	CC5.8	SA-7 SC-5 SI-3 SI-5 SI-7 SI-8	1	1	1	0	0	0
Threat and Vulnerability Management Vulnerability / Patch Management	TVM-02	CC7.1	CM-3 CM-4 CP-10 RA-5 SA-7 SI-1 SI-2 SI-5	1	1	1	1	0	0
Threat and Vulnerability Management Mobile Code	TVM-03	CC5.6 CC7.1	SC-18	1	1	1	0	0	0

ภาคผนวก ข
การวิเคราะห์ความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้

การวิเคราะห์ความอ่อนไหว (Sensitivity) ของคะแนนทางด้านความมั่นคงและความพึ่งพาได้ เป็นการพิจารณาระดับความอ่อนไหวหรือระดับความแตกต่างของคะแนนในแต่ละคุณลักษณะย่อย ของผู้ให้บริการต่างรายกัน เช่นเมื่อคะแนนการรักษาความลับของผู้ให้บริการรายหนึ่ง มีค่าเท่ากับ 15.87 เมื่อเทียบกับผู้ให้บริการรายที่สอง ซึ่งมีค่าเท่ากับ 14.22 แล้วความแตกต่างของคะแนนเป็น 1.65 หน่วยนั้น แสดงว่าผู้ให้บริการรายที่หนึ่งมีคุณภาพด้านการรักษาความลับมากกว่า ผู้ให้บริการรายที่สองเป็นอย่างมากหรือไม่ หรือยังถือว่าเป็นเพียงเล็กน้อย โดยผู้ใช้บริการสามารถพิจารณาระดับความอ่อนไหวได้จากความแตกต่างของจำนวนการปฏิบัติตาม (No. of Yes Answers) คำถามใน CAIQ ที่เกี่ยวข้องกับคุณลักษณะย่อยนั้นๆ สำหรับการคำนวณหาจำนวนการปฏิบัติตามสำหรับคำถามใน CAIQ ที่เกี่ยวข้องกับแต่ละคุณลักษณะทางด้านความมั่นคงและความพึ่งพาได้ สามารถทำได้โดย

$$y_n = \frac{b_n \; x \; c_n}{a_n}$$

เมื่อ y_n คือจำนวนการปฏิบัติตาม CAIQ ที่เกี่ยวข้องกับ คุณลักษณะย่อยที่ n

b_n คือค่าคะแนนของคุณลักษณะย่อยที่ n

c_n คือจำนวนคำถามทั้งหมดใน CAIQ ที่เกี่ยวข้องกับคุณลักษณะย่อยที่ n

a_n คือค่าคะแนนรวมสูงสุดในกรณีที่ปฏิบัติตามคำถามทุกข้อใน CAIQ ที่เกี่ยวข้องกับคุณลักษณะ ย่อยที่ n

ตัวอย่างเช่น หากคะแนนการรักษาความลับของผู้ให้บริการมีค่าเท่ากับ 14.22 โดยที่มีจำนวนคำถามใน CAIQ ที่เกี่ยวข้องกับคุณลักษณะทางด้านการรักษาความลับทั้งหมด 207 ข้อ และมีค่าคะแนนสูงสุดของการรักษาความลับเท่ากับ 16.26 คะแนน สามารถแทนค่าได้ดังนี้

$$\frac{14.22 \; x \; 207}{16.26} = 181$$

ดังนั้นคะแนนคุณลักษณะของการรักษาความลับ 14.22 คือค่าคะแนนจำนวนการปฏิบัติตาม CAIQ เท่ากับ 181 ข้อ

ตารางที่ ข.1 สรุปจำนวนการปฏิบัติตาม CAIQ เมื่อผู้ให้บริการได้คะแนนในแต่ละคุณลักษณะย่อยทั้ง 6 ด้าน เป็นค่าต่างๆ เพื่อใช้ประกอบการพิจารณาเปรียบเทียบคะแนนคุณลักษณะย่อยระหว่างผู้ให้บริการต่างราย โดยพิจารณาความแตกต่างระหว่างจำนวนการปฏิบัติตามประกอบด้วย ดังนั้นผู้ให้บริการรายที่หนึ่งและรายที่สองดังข้างต้นมีความแตกต่างของคะแนนการรักษาความลับ 1.65 หน่วย จะมีจำนวนการปฏิบัติตามต่างกัน 21 ข้อ

ตารางที่ ข.1 จำนวนการปฏิบัติตาม CAIQ เพื่อประกอบการพิจารณาความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้

Confidentiality		Integrity		Availability		Reliability		Safety		Maintainability	
No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score
207	16.26	212	16.62	215	16.64	22	2.18	31	2.99	28	1.9
206	16.18	211	16.56	214	16.58	21	2.09	30	2.89	27	1.83
205	16.1	210	16.48	213	16.5	20	1.99	29	2.8	26	1.76
204	16.02	209	16.4	212	16.42	19	1.89	28	2.7	25	1.7
203	15.95	208	16.32	211	16.35	18	1.79	27	2.6	24	1.63
202	15.87	207	16.24	210	16.27	17	1.69	26	2.51	23	1.56
201	15.79	206	16.16	209	16.19	16	1.59	25	2.41	22	1.49
200	15.71	205	16.09	208	16.11	15	1.49	24	2.31	21	1.43
199	15.63	204	16.01	207	16.04	14	1.39	23	2.22	20	1.36
198	15.55	203	15.93	206	15.96	13	1.29	22	2.12	19	1.29

ตารางที่ ข.1 จำนวนการปฏิบัติตาม CAIQ เพื่อประกอบการพิจารณาความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้ (ต่อ)

Confidentiality		Integrity		Availability		Reliability		Safety		Maintainability	
No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score
197	15.47	202	15.85	205	15.88	12	1.19	21	2.03	18	1.22
196	15.4	201	15.77	204	15.8	11	1.09	20	1.93	17	1.15
195	15.32	200	15.69	203	15.73	10	1	19	1.83	16	1.09
194	15.24	199	15.62	202	15.65	9	0.9	18	1.74	15	1.02
193	15.16	198	15.54	201	15.57	8	0.8	17	1.64	14	0.95
192	15.08	197	15.46	200	15.49	7	0.7	16	1.54	13	0.88
191	15	196	15.38	199	15.42	6	0.6	15	1.45	12	0.81
190	14.92	195	15.3	198	15.34	5	0.5	14	1.35	11	0.75
189	14.85	194	15.22	197	15.26	4	0.4	13	1.25	10	0.68
188	14.77	193	15.14	196	15.18	3	0.3	12	1.16	9	0.61
187	14.69	192	15.07	195	15.11	2	0.2	11	1.06	8	0.54
186	14.61	191	14.99	194	15.03	1	0.1	10	0.96	7	0.48
185	14.53	190	14.91	193	14.95	0	0	9	0.87	6	0.41
184	14.45	189	14.83	192	14.87			8	0.77	5	0.34
183	14.37	188	14.75	191	14.8			7	0.68	4	0.27

ตารางที่ ข.1 จำนวนการปฏิบัติตาม CAIQ เพื่อประกอบการพิจารณาความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้ (ต่อ)

Confidentiality		Integrity		Availability		Reliability		Safety		Maintainability	
No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score
182	14.3	187	14.67	190	14.72			6	0.58	3	0.2
181	14.22	186	14.6	189	14.64			5	0.48	2	0.14
180	14.14	185	14.52	188	14.56			4	0.39	1	0.07
179	14.06	184	14.44	187	14.49			3	0.29	0	0
178	13.98	183	14.36	186	14.41			2	0.19		
177	13.9	182	14.28	185	14.33			1	0.1		
176	13.82	181	14.2	184	14.25			0	0		
175	13.75	180	14.12	183	14.18						
174	13.67	179	14.05	182	14.1						
173	13.59	178	13.97	181	14.02						
172	13.51	177	13.89	180	13.94						
171	13.43	176	13.81	179	13.87						
170	13.35	175	13.73	178	13.79						
169	13.28	174	13.65	177	13.71						
168	13.2	173	13.58	176	13.63						

ตารางที่ ข.1 จำนวนการปฏิบัติตาม CAIQ เพื่อประกอบการพิจารณาความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้ (ต่อ)

Confidentiality		Integrity		Availability		Reliability		Safety		Maintainability	
No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score
167	13.12	172	13.5	175	13.56						
166	13.04	171	13.42	174	13.48						
165	12.96	170	13.34	173	13.4						
164	12.88	169	13.26	172	13.32						
163	12.8	168	13.18	171	13.25						
162	12.73	167	13.11	170	13.17						
161	12.65	166	13.03	169	13.09						
160	12.57	165	12.95	168	13.02						
159	12.49	164	12.87	167	12.94						
158	12.41	163	12.79	166	12.86						
157	12.33	162	12.71	165	12.78						
156	12.25	161	12.63	164	12.71						
155	12.18	160	12.56	163	12.63						
154	12.1	159	12.48	162	12.55						
153	12.02	158	12.4	161	12.47						

ตารางที่ ข.1 จำนวนการปฏิบัติตาม CAIQ เพื่อประกอบการพิจารณาความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้ (ต่อ)

Confidentiality		Integrity		Availability		Reliability		Safety		Maintainability	
No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score
152	11.94	11.94	12.32	160	12.4						
151	11.86	11.86	12.24	159	12.32						
149	11.7	11.78	12.16	158	12.24						
148	11.62	11.7	12.09	157	12.16						
147	11.54	11.63	12.01	156	12.09						
146	11.47	11.55	11.93	155	12.01						
145	11.39	11.47	11.85	154	11.93						
144	11.31	11.39	11.77	153	11.85						
143	11.23	11.31	11.69	152	11.78						
142	11.15	11.23	11.61	151	11.7						
141	11.07	11.15	11.54	150	11.62						
140	11	11.08	11.46	149	11.54						
139	10.92	11	11.38	148	11.47						
138	10.84	10.92	11.3	147	11.39						
137	10.76	10.84	11.22	146	11.31						

ตารางที่ ข.1 จำนวนการปฏิบัติตาม CAIQ เพื่อประกอบการพิจารณาความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้ (ต่อ)

Confidentiality		Integrity		Availability		Reliability		Safety		Maintainability	
No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score
136	10.68	10.76	11.14	145	11.23						
135	10.6	10.68	11.07	144	11.16						
134	10.52	10.6	10.99	143	11.08						
133	10.45	10.53	10.91	142	11						
132	10.37	138	10.83	141	10.92						
131	10.29	137	10.75	140	10.85						
130	10.21	136	10.67	139	10.77						
129	10.13	135	10.59	138	10.69						
128	10.05	134	10.52	137	10.61						
127	9.98	133	10.44	136	10.54						
126	9.9	132	10.36	135	10.46						
125	9.82	131	10.28	134	10.38						
124	9.74	130	10.2	133	10.3						
123	9.66	129	10.12	132	10.23						
122	9.58	128	10.05	131	10.15						
121	9.5	127	9.97	130	10.07						

ตารางที่ ข.1 จำนวนการปฏิบัติตาม CAIQ เพื่อประกอบการพิจารณาความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้ (ต่อ)

Confidentiality		Integrity		Availability		Reliability		Safety		Maintainability	
No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score
120	9.43	126	9.89	129	9.99						
119	9.35	125	9.81	128	9.92						
118	9.27	124	9.73	127	9.84						
117	9.19	123	9.65	126	9.76						
116	9.11	122	9.58	125	9.69						
115	9.03	121	9.5	124	9.61						
114	8.95	120	9.42	123	9.53						
113	8.88	119	9.34	122	9.45						
112	8.8	118	9.26	121	9.38						
111	8.72	117	9.18	120	9.3						
110	8.64	116	9.1	119	9.22						
109	8.56	115	9.03	118	9.14						
108	8.48	114	8.95	117	9.07						
107	8.4	113	8.87	116	8.99						
106	8.33	112	8.79	115	8.91						
105	8.25	111	8.71	114	8.83						

ตารางที่ ข.1 จำนวนการปฏิบัติตาม CAIQ เพื่อประกอบการพิจารณาความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้ (ต่อ)

Confidentiality		Integrity		Availability		Reliability		Safety		Maintainability	
No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score
104	8.17	110	8.63	113	8.76						
103	8.09	109	8.56	112	8.68						
102	8.01	108	8.48	111	8.6						
101	7.93	107	8.4	110	8.52						
100	7.86	106	8.32	109	8.45						
99	7.78	105	8.24	108	8.37						
98	7.7	104	8.16	107	8.29						
97	7.62	103	8.08	106	8.21						
96	7.54	102	8.01	105	8.14						
95	7.46	101	7.93	104	8.06						
94	7.38	100	7.85	103	7.98						
93	7.31	99	7.77	102	7.9						
92	7.23	98	7.69	101	7.83						
91	7.15	97	7.61	100	7.75						
90	7.07	96	7.54	99	7.67						
89	6.99	95	7.46	98	7.59						

ตารางที่ ข.1 จำนวนการปฏิบัติตาม CAIQ เพื่อประกอบการพิจารณาความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้ (ต่อ)

Confidentiality		Integrity		Availability		Reliability		Safety		Maintainability	
No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score
88	6.91	94	7.38	97	7.52						
87	6.83	93	7.3	96	7.44						
86	6.76	92	7.22	95	7.36						
85	6.68	91	7.14	94	7.28						
84	6.6	90	7.06	93	7.21						
83	6.52	89	6.99	92	7.13						
82	6.44	88	6.91	91	7.05						
81	6.36	87	6.83	90	6.97						
80	6.28	86	6.75	89	6.9						
79	6.21	85	6.67	88	6.82						
78	6.13	84	6.59	87	6.74						
77	6.05	83	6.52	86	6.66						
76	5.97	82	6.44	85	6.59						
75	5.89	81	6.36	84	6.51						
74	5.81	80	6.28	83	6.43						
73	5.73	79	6.2	82	6.36						

ตารางที่ ข.1 จำนวนการปฏิบัติตาม CAIQ เพื่อประกอบการพิจารณาความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้ (ต่อ)

Confidentiality		Integrity		Availability		Reliability		Safety		Maintainability	
No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score
72	5.66	78	6.12	81	6.28						
71	5.58	77	6.05	80	6.2						
70	5.5	76	5.97	79	6.12						
69	5.42	75	5.89	78	6.05						
68	5.34	74	5.81	77	5.97						
67	5.26	73	5.73	76	5.89						
66	5.18	72	5.65	75	5.81						
65	5.11	71	5.57	74	5.74						
64	5.03	70	5.5	73	5.66						
63	4.95	69	5.42	72	5.58						
62	4.87	68	5.34	71	5.5						
61	4.79	67	5.26	70	5.43						
60	4.71	66	5.18	69	5.35						
59	4.63	65	5.1	68	5.27						
58	4.56	64	5.03	67	5.19						
57	4.48	63	4.95	66	5.12						

ตารางที่ ข.1 จำนวนการปฏิบัติตาม CAIQ เพื่อประกอบการพิจารณาความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้ (ต่อ)

Confidentiality		Integrity		Availability		Reliability		Safety		Maintainability	
No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score
56	4.4	62	4.87	65	5.04						
55	4.32	61	4.79	64	4.96						
54	4.24	60	4.71	63	4.88						
53	4.16	59	4.63	62	4.81						
52	4.08	58	4.55	61	4.73						
51	4.01	57	4.48	60	4.65						
50	3.93	56	4.4	59	4.57						
49	3.85	55	4.32	58	4.5						
48	3.77	54	4.24	57	4.42						
47	3.69	53	4.16	56	4.34						
46	3.61	52	4.08	55	4.26						
45	3.53	51	4.01	54	4.19						
44	3.46	50	3.93	53	4.11						
43	3.38	49	3.85	52	4.03						
42	3.3	48	3.77	51	3.95						
41	3.22	47	3.69	50	3.88						

ตารางที่ ข.1 จำนวนการปฏิบัติตาม CAIQ เพื่อประกอบการพิจารณาความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้ (ต่อ)

Confidentiality		Integrity		Availability		Reliability		Safety		Maintainability	
No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score
40	3.14	46	3.61	49	3.8						
39	3.06	45	3.53	48	3.72						
38	2.98	44	3.46	47	3.64						
37	2.91	43	3.38	46	3.57						
36	2.83	42	3.3	45	3.49						
35	2.75	41	3.22	44	3.41						
34	2.67	40	3.14	43	3.33						
33	2.59	39	3.06	42	3.26						
32	2.51	38	2.99	41	3.18						
31	2.44	37	2.91	40	3.1						
30	2.36	36	2.83	39	3.03						
29	2.28	35	2.75	38	2.95						
28	2.2	34	2.67	37	2.87						
27	2.12	33	2.59	36	2.79						
26	2.04	32	2.52	35	2.72						
25	1.96	31	2.44	34	2.64						

ตารางที่ ข.1 จำนวนการปฏิบัติตาม CAIQ เพื่อประกอบการพิจารณาความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้ (ต่อ)

Confidentiality		Integrity		Availability		Reliability		Safety		Maintainability	
No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score
24	1.89	30	2.36	33	2.56						
23	1.81	29	2.28	32	2.48						
22	1.73	28	2.2	31	2.41						
21	1.65	27	2.12	30	2.33						
20	1.57	26	2.04	29	2.25						
19	1.49	25	1.97	28	2.17						
18	1.41	24	1.89	27	2.1						
17	1.34	23	1.81	26	2.02						
16	1.26	22	1.73	25	1.94						
15	1.18	21	1.65	24	1.86						
14	1.1	20	1.57	23	1.79						
13	1.02	19	1.5	22	1.71						
12	0.94	18	1.42	21	1.63						
11	0.86	17	1.34	20	1.55						
10	0.79	16	1.26	19	1.48						
9	0.71	15	1.18	18	1.4						

ตารางที่ ข.1 จำนวนการปฏิบัติตาม CAIQ เพื่อประกอบการพิจารณาความอ่อนไหวของคะแนนทางด้านความมั่นคงและความพึ่งพาได้ (ต่อ)

Confidentiality		Integrity		Availability		Reliability		Safety		Maintainability	
No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score	No. of Questions with Yes Answers	Score
8	0.63	14	1.1	17	1.32						
7	0.55	13	1.02	16	1.24						
6	0.47	12	0.95	15	1.17						
5	0.39	11	0.87	14	1.09						
4	0.31	10	0.79	13	1.01						
3	0.24	9	0.71	12	0.93						
2	0.16	8	0.63	11	0.86						
1	0.08	7	0.55	10	0.78						
0	0	6	0.48	9	0.7						
		5	0.4	8	0.62						
		4	0.32	7	0.55						
		3	0.24	6	0.47						
		2	0.16	5	0.39						
		1	0.08	4	0.31						
		0	0	3	0.24						
				2	0.16						
				1	0.08						
				0	0						

ประวัติผู้เขียนวิทยานิพนธ์

นายจิรายุ กานต์ปริยสุนทร เกิดเมื่อวันที่ 30 กันยายน พ.ศ. 2533 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาระดับปริญญาวิทยาศาสตรบัณฑิต สาขาคอมพิวเตอร์เพื่อการสื่อสาร คณะวิทยาลัยนวัตกรรมสื่อสารสังคม มหาวิทยาลัยศรีนครินทรวิโรฒ และได้เข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิทยาศาสตรคอมพิวเตอร์ ณ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ปีการศึกษา 2556