การจำแนกความสอดคล้องด้านความมั่นคงของผู้ให้บริการคลาวด์กับเมตริกซ์ควบคุมคลาวด์

นายณัฐพงศ์ ภุมวารพฤษภ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2556

CLASSIFICATION OF CLOUD PROVIDER SECURITY CONFORMANCE TO CLOUD CONTROLS MATRIX

Mr. Nuttapong Pumvarapruek

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Software Engineering
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2013

หัวข้อวิทยานิพนธ์	การจำแนกความสอดคล้องด้านความมั่นคงของผู้ให้บริการคลาวด์กับเมตริกซ์ควบคุมคลาวด์
โดย	นายณัฐพงศ์ ภุมวารพฤษภ์
สาขาวิชา	วิศวกรรมซอฟต์แวร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร. ทวิตีย์ เสนีวงศ์ ณ อยุธยา

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์

(ศาสตราจารย์ ดร. บัณฑิต เอื้ออาภรณ์)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ

(อาจารย์ ดร. ยรรยง เต็งอำนวย)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(รองศาสตราจารย์ ดร. ทวิตีย์ เสนีวงศ์ ณ อยุธยา)

.....กรรมการภายนอกมหาวิทยาลัย

(ผู้ช่วยศาสตราจารย์ ดร. ชวลิต ศรีสถาพรพัฒน์)

ณัฐพงศ์ ภุมวารพฤษภ์ : การจำแนกความสอดคล้องด้านความมั่นคงของผู้ให้บริการคลาวด์กับเมตริกซ์ควบคุมคลาวด์. (CLASSIFICATION OF CLOUD PROVIDER SECURITY CONFORMANCE TO CLOUD CONTROLS MATRIX) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: รศ. ดร. ทวิตีย์ เสนีวงศ์ ณ อยุธยา, 105 หน้า.

ความมั่นคงของบริการคลาวด์เป็นหนึ่งในประเด็นหลักที่ผู้ใช้บริการคลาวด์ให้ความสนใจในขณะทำการเลือกผู้ให้บริการ ข้อมูลด้านความมั่นคงของบริการควรได้รับการเปิดเผยแก่ผู้ใช้บริการอย่างเพียงพอเพื่อสร้างความเชื่อมั่นในบริการ แต่ในทางปฏิบัติ ข้อมูลด้านความมั่นคงมักเป็นข้อมูลที่สำคัญและไม่เปิดเผยต่อบุคคลทั่วไป ดังนั้นในการเลือกใช้บริการคลาวด์ ผู้ใช้บริการจึงต้องศึกษาจากข้อมูลที่เปิดเผยอยู่บนเว็บไซต์ของผู้ให้บริการหรือในคลังข้อมูลเกี่ยวกับผู้ให้บริการเพื่อที่จะประเมินความมั่นคงของบริการคลาวด์ เพื่อเป็นการช่วยผู้ใช้บริการในการเลือกใช้บริการคลาวด์ งานวิจัยนี้เสนอวิธีการเบื้องต้นในการประยุกต์ใช้การจำแนกข้อความเพื่อทำการจำแนกข้อมูลที่เปิดเผยอยู่บนเว็บไซต์ของผู้ให้บริการ ว่าผู้ให้บริการรายนั้นได้ทำตามวิธีการปฏิบัติที่ดีหรือแนวทางด้านความมั่นคงใดบ้างในการให้บริการ ผู้วิจัยศึกษาวิธีการปฏิบัติด้านความมั่นคงที่กำหนดไว้ในเมตริกซ์ควบคุมคลาวด์และแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน แล้วทำการรวบรวมคำศัพท์ในด้านความมั่นคง เพื่อมาใช้ในการจำแนกข้อมูลหน้าเว็บของผู้ให้บริการ ผู้วิจัยได้พัฒนาเครื่องมือเพื่อช่วยในการจำแนกและแสดงผลการจำแนกในรูปแบบกราฟ ซึ่งผลการจำแนกที่ได้ถือเป็นข้อมูลประมาณการระดับความสอดคล้องกับวิธีการปฏิบัติในเมตริกซ์ควบคุมคลาวด์ของผู้ให้บริการแต่ละรายที่นำมาเปรียบเทียบกัน ในการประเมินผลการจำแนกผู้ให้บริการคลาวด์ห้ารายโดยใช้วิธีสหสัมพันธ์แบบเพียร์สัน พบว่าผลการจำแนกด้วยวิธีที่เสนอกับผลการจำแนกด้วยมือมีความสอดคล้องกัน

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิศวกรรมซอฟต์แวร์ ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก .....

ปีการศึกษา 2556

5570974621 : MAJOR SOFTWARE ENGINEERING
KEYWORDS: CLOUD COMPUTING / SECURITY / CLASSIFICATION / CLOUD CONTROLS MATRIX

NUTTAPONG PUMVARAPRUEK: CLASSIFICATION OF CLOUD PROVIDER SECURITY CONFORMANCE TO CLOUD CONTROLS MATRIX. ADVISOR: ASSOC. PROF. TWITTIE SENIVONGSE, Ph.D., 105 pp.

Security of cloud services is a major concern to cloud consumers when selecting cloud providers. Sufficient security information should be provided so that consumer trust in cloud services can be built, but in practice, security information is critical and may not be publicized. During the service selection process, cloud consumers therefore have to study published information on the cloud providers' Web sites or the cloud providers registry in order to assess how secure the services are. To assist cloud consumers in service selection, this research presents an initial attempt to apply text classification to classify published information on the providers' Web pages to determine which security best practices and guidelines the providers have followed in providing their services. We take the security best practices and guidelines from the Cloud Controls Matrix (CCM) and the accompanying Consensus Assessments Initiative Questionnaire (CAIQ), and compile a set of security concepts before using it as a basis for classifying the providers' Web pages. We develop a classification tool to classify and present graphically the classification results which can roughly signify the security conformance level of different providers in comparison. In an evaluation using Pearson Correlation on the case of five cloud providers, the classification results of the proposed method correlate well with manual classification.

Department: Computer Engineering Student's Signature .....
Field of Study: Software Engineering Advisor's Signature .....
Academic Year: 2013

กิตติกรรมประกาศ

วิทยานิพนธ์นี้สำเร็จลงด้วยความกรุณาเป็นอย่างสูงของรองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งได้ให้โอกาส ความรู้และคำแนะนำในการทำวิทยานิพนธ์ ตลอดจนความเมตตาและความอดทนในการตรวจผลงานของข้าพเจ้าได้แก่ โครงร่างวิทยานิพนธ์ ผลงานวิจัยภาษาอังกฤษ และวิทยานิพนธ์ ทำให้ผลงานทุกชิ้นสำเร็จลุล่วงเป็นอย่างดี ขอขอบพระคุณอาจารย์เป็นอย่างสูงไว้ ณ ที่นี้

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

ขอขอบพระคุณอาจารย์ทุกท่านที่ให้ความรู้และคำแนะนำที่เป็นประโยชน์ รวมถึงความเมตตาและความเอาใจใส่มาโดยตลอด

ขอขอบพระคุณครอบครัว ได้แก่ บิดามารดา ที่ให้กำลังใจในทุกเรื่อง สอนให้มีความมานะขยัน อดทน และคอยสนับสนุนในทุกด้านจนทำให้ข้าพเจ้ามีผลงานที่สำเร็จได้

ขอขอบคุณเพื่อนร่วมชั้นเรียนวิศวกรรมซอฟต์แวร์ และเพื่อนสาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ภาคนอกเวลาราชการทุกคนที่ให้ความช่วยเหลือ แจ้งข่าวสารของมหาวิทยาลัยและการประชุมวิชาการที่เป็นประโยชน์ รวมถึงมิตรภาพและกำลังใจที่มีให้เสมอ

สารบัญ

หน้า

หน้า

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การให้บริการคลาวด์เป็นวิธีการประมวลผลที่อิงกับความต้องการของผู้ใช้ โดยผู้ใช้สามารถระบุความต้องการไปยังซอฟต์แวร์ของระบบคลาวด์ จากนั้นซอฟต์แวร์จะร้องขอให้ระบบจัดสรรทรัพยากรและบริการให้ตรงกับความต้องการของผู้ใช้ ทั้งนี้ระบบสามารถเพิ่มและลดจำนวนของทรัพยากร รวมถึงเสนอบริการให้พอเหมาะกับความต้องการของผู้ใช้ได้ตลอดเวลา โดยที่ผู้ใช้ไม่จำเป็นต้องทราบเลยว่าการทำงานหรือเหตุการณ์เบื้องหลังเป็นเช่นไร อีกทั้งยังช่วยลดกิจกรรมและค่าใช้จ่ายในการติดตั้งและบำรุงรักษาซอฟต์แวร์ ด้วยเหตุนี้คลาวด์จึงเป็นที่นิยมในอุตสาหกรรมซอฟต์แวร์หลายประเภท

ในการเลือกผู้ให้บริการคลาวด์ ผู้ใช้บริการคลาวด์จำเป็นต้องมีการประเมินผู้ให้บริการคลาวด์ก่อนการตัดสินใจใช้บริการ ซึ่งในการประเมินทำได้โดยศึกษาข้อมูลจากผู้ที่เคยใช้บริการคลาวด์ หรือ ศึกษาข้อมูลของผู้ให้บริการคลาวด์ผ่านหน้าเว็บของผู้ให้บริการคลาวด์เอง ซึ่งข้อมูลที่ผู้ใช้บริการคลาวด์จะนำมาใช้ตัดสินใจแบ่งออกเป็น 2 ประเภท คือ

1. ข้อมูลความต้องการเชิงหน้าที่ (Functional Requirement) เช่น รายละเอียดของเครื่องเซิร์ฟเวอร์ รายละเอียดของระบบฐานข้อมูลที่ใช้ ระยะเวลาที่ใช้ในการจัดเตรียมระบบ ความสามารถในการขยายตัวของระบบเพื่อรองรับความต้องการใช้บริการที่เพิ่มขึ้นหรือลดลง
2. ข้อมูลความต้องการที่ไม่ใช่เชิงหน้าที่ (Non-functional Requirement) เช่น ความสามารถในการเชื่อมต่อระบบอื่น ๆ นโยบายความมั่นคงและความเป็นส่วนตัวของข้อมูล ข้อตกลงในการให้บริการ (Service Level Agreement)

ข้อมูลความต้องการเชิงหน้าที่สามารถประเมินได้โดยง่ายเนื่องจากมีตัวเลขและรายละเอียดที่สามารถวัดได้ ในขณะที่ข้อมูลที่ไม่ใช่ความต้องการเชิงหน้าที่ ผู้ใช้บริการคลาวด์จำเป็นจะต้องอ่านรายละเอียดจากหน้าเว็บซึ่งอาจจะเป็นคำโฆษณาหรือเอกสารนโยบายของผู้ให้บริการคลาวด์แต่ละราย เพื่อการพิจารณาตัดสินใจเลือกใช้บริการคลาวด์ ซึ่งในส่วนของเอกสารด้านความมั่นคงมีค่อนข้างมากต้องใช้เวลานานในการอ่านพิจารณาว่าข้อมูลด้านความมั่นคงนั้นครอบคลุมในเรื่องใดบ้างและ ครบตามมาตรฐานความมั่นคงหรือไม่

จากเหตุผลดังกล่าว งานวิจัยนี้จึงมีวัตถุประสงค์เพื่อนำเสนอระบบสนับสนุนผู้ใช้บริการคลาวด์ในการประเมินเพื่อตัดสินใจเลือกผู้ให้บริการคลาวด์ โดยพิจารณาเฉพาะความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงของผู้ให้บริการคลาวด์จากเมตริกซ์ควบคุมคลาวด์ (Cloud Controls Matrix) [1] ที่จัดทำโดยองค์กรความมั่นคงของคลาวด์ (Cloud Security Alliance: CSA) ซึ่งกำหนดความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงที่ผู้ให้บริการคลาวด์จำเป็นต้องมีไว้ 16 ด้าน

ความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงที่เมตริกซ์ควบคุมคลาวด์กำหนด ได้แก่ [1]

1. ความมั่นคงของโปรแกรมประยุกต์และส่วนต่อประสาน (Application & Interface Security)
2. การรับรองการตรวจสอบและการปฏิบัติตาม (Audit Assurance & Compliance)
3. การจัดการความต่อเนื่องทางธุรกิจและความยืดหยุ่นเชิงปฏิบัติการ (Business Continuity Management & Operational Resilience)
4. การควบคุมการเปลี่ยนแปลงและการจัดการโครงแบบ (Change Control & Configuration Management)
5. ความมั่นคงของข้อมูลและการจัดการวัฏจักรชีวิตสารสนเทศ (Data Security & Information Lifecycle Management)
6. ความมั่นคงของศูนย์ข้อมูล (Datacenter Security)
7. การเข้ารหัสลับและการจัดการกุญแจ (Encryption & Key Management)
8. วิธีการปกครองและการจัดการความเสี่ยง (Governance and Risk Management)
9. ทรัพยากรมนุษย์ (Human Resources)
10. เอกลักษณ์และการจัดการการเข้าถึง (Identity & Access Management)
11. โครงสร้างพื้นฐานและความมั่นคงของเทคโนโลยีเสมือน (Infrastructure & Virtualization Security)
12. การทำงานร่วมกันและใช้ได้หลายระบบ (Interoperability & Portability)
13. ความมั่นคงของระบบเคลื่อนที่ (Mobile Security)
14. การจัดการเหตุการณ์ด้านความมั่นคง การค้นพบอิเล็กทรอนิกส์ และกระบวนการทางกฎหมายของคลาวด์ (Security Incident Management, E-Discovery & Cloud Forensics)
15. การจัดการสายโซ่อุปทาน ความโปร่งใส และภาระรับผิดชอบ (Supply Chain Management, Transparency and Accountability)
16. การคุกคามและการจัดการจุดอ่อน (Threat and Vulnerability Management)

ความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคง 16 ด้านข้างต้น จะถูกกำหนดเป็นนิยามของคำว่าความมั่นคงที่กล่าวถึงทั้งหมดในงานวิจัย โดยการวิจัยจะใช้เมตริกซ์ควบคุมคลาวด์ และ แบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน (Consensus Assessments Initiative Questionnaire) [2] มาสร้างออนโทโลจีความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ เพื่อให้ระบบสนับสนุนผู้ใช้บริการคลาวด์ในการประเมินเพื่อตัดสินใจเลือกผู้ให้บริการคลาวด์ที่ผู้วิจัยจะพัฒนาขึ้น สามารถนำมาใช้ในการพิจารณาคำศัพท์ที่สกัดมาจากหน้าเว็บของผู้ให้บริการคลาวด์ แล้วนำคำศัพท์ที่ได้มาจำแนกว่า ผู้ให้บริการ

คลาวด์มีความสอดคล้องกับความต้องการด้านความมั่นคงตามที่ระบุในเมตริกซ์ควบคุมคลาวด์ในด้านใดบ้างและในระดับใด โดยใช้การจัดกลุ่มข้อมูลอย่างง่าย (Naïve Text Classification) ซึ่งอิงออนโทโลจีที่สร้างขึ้น ผลการจำแนกที่ได้ถือเป็นข้อมูลประมาณการระดับความสอดคล้องกับวิธีการปฏิบัติที่ดีในด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ ของผู้ให้บริการแต่ละราย ตามข้อมูลที่ได้เปิดเผยไว้บนหน้าเว็บ ผู้ใช้สามารถเปรียบเทียบผู้ให้บริการคลาวด์ที่แตกต่างกันในเบื้องต้นว่าแต่ละรายมีการแสดงข้อมูลการปฏิบัติตามเมตริกซ์ควบคุมคลาวด์หรือไม่อย่างไร เพื่อประกอบการตัดสินใจเลือกใช้บริการที่มีความมั่นคงในระดับที่เหมาะสมกับลักษณะขององค์กรผ่านระบบที่พัฒนาขึ้นได้

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อกำหนดวิธีการจำแนกความสอดคล้องด้านความมั่นคงของผู้ให้บริการคลาวด์เพื่อใช้ประเมินระดับความมั่นคงของการให้บริการ

1.2.2 เพื่อพัฒนาเครื่องมือสนับสนุนการจำแนกความสอดคล้องด้านความมั่นคงของผู้ให้บริการคลาวด์

1.3 ขอบเขตของการวิจัย

1.3.1 พิจารณาความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงที่ผู้ให้บริการคลาวด์จำเป็นต้องมี ตามที่กำหนดโดยเมตริกซ์ควบคุมคลาวด์

1.3.2 สร้างออนโทโลจีความมั่นคงของคลาวด์โดยอิงแนวปฏิบัติด้านความมั่นคงตามที่กำหนดโดยเมตริกซ์ควบคุมคลาวด์เป็นหลัก และเสริมด้วยแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน

1.3.3 พัฒนาเครื่องมือที่สามารถคำนวณ แสดง และเปรียบเทียบคะแนนความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงของผู้ให้บริการคลาวด์แต่ละราย จากการประมวลผลข้อมูลบนหน้าเว็บของผู้ให้บริการคลาวด์และการจำแนกข้อมูลด้วยวิธีการจำแนกข้อมูลอย่างง่าย

1.3.4 ทดสอบเครื่องมือที่พัฒนาและประเมินวิธีการจำแนกและคะแนนความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงที่ได้ โดยใช้ข้อมูลผู้ให้บริการคลาวด์ 5 รายเป็นอย่างน้อย

1.4 ขั้นตอนการวิจัย

1.4.1 พิจารณาข้อมูลด้านความมั่นคงของการบริการคลาวด์ จากเมตริกซ์ควบคุมคลาวด์ แบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน และ ผู้ให้บริการคลาวด์

1.4.2 สร้างออนโทโลจีความมั่นคงของคลาวด์

1.4.3 กำหนดวิธีการที่ใช้ในการสกัดข้อมูลจากหน้าเว็บของผู้ให้บริการคลาวด์

1.4.4 กำหนดรูปแบบการจัดเก็บข้อมูลที่ได้จากการสกัดข้อมูลจากหน้าเว็บ

1.4.5 ประยุกต์อัลกอริทึมการจำแนกข้อมูลอย่างง่ายในการจำแนกข้อมูล

1.4.6 พัฒนาเครื่องมือสนับสนุนงานวิจัย

1.4.7 ทดสอบและประเมินผล

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ได้วิธีการจำแนกที่สามารถใช้ประเมินความสอดคล้องด้านความมั่นคงของผู้ให้บริการคลาวด์แต่ละรายได้

1.5.2 ได้เครื่องมือที่สามารถใช้ประเมินและเปรียบเทียบคะแนนความสอดคล้องด้านความมั่นคงในด้านต่าง ๆ ของผู้ให้บริการคลาวด์ได้

1.6 ผลงานตีพิมพ์

ส่วนหนึ่งของวิทยานิพนธ์นี้ได้ตีพิมพ์และนำเสนอในการประชุมวิชาการต่อไปนี้

1.6.1 บทความเรื่อง Classification of Cloud Provider Security Conformance to Cloud Controls Matrix โดยผู้แต่งคือ Nuttapong Pumvarapruek และ Twittie Senivongse ในการประชุมวิชาการ The11th International Joint Conference on Computer Science and Software Engineering (JCSSE 2014), Chonburi, Thailand (May 14-16, 2014)

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

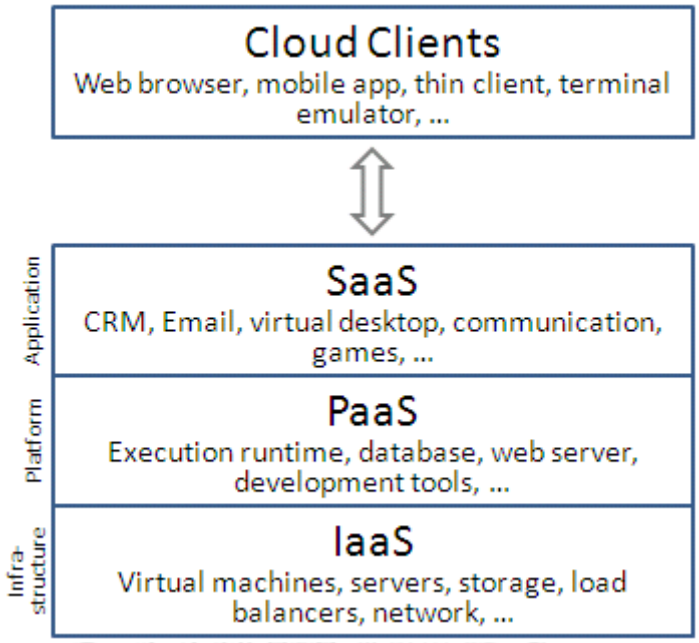
2.1 แนวคิดและทฤษฎี

2.1.1 การคำนวณแบบคลาวด์

การคำนวณแบบคลาวด์ (Cloud Computing) ตามนิยามของสถาบันมาตรฐานและเทคโนโลยีระดับชาติ (National Institute of Standards and Technology: NIST) [3] เป็นแบบจำลองการคำนวณที่มีความสามารถในการใช้งานได้ทุกที่ สามารถเข้าถึงเครือข่ายได้ตามความต้องการ สนับสนุนการแบ่งปันการใช้ทรัพยากรต่าง ๆ เช่น ระบบเครือข่าย ผู้ให้บริการ อุปกรณ์ที่ใช้ในการเก็บข้อมูล แอปพลิเคชัน และบริการ ใช้เวลาในการเตรียมการใช้งานและแรงงานในการบริหารจัดการน้อย โดยแบบจำลองคลาวด์มีลักษณะเด่น 6 ลักษณะ ได้แก่

1) ความคล่องตัว (Agility) คือ สามารถช่วยเพิ่มความสามารถของผู้ใช้ในการจัดเตรียมโครงสร้างพื้นฐานทางเทคโนโลยี
2) ค่าใช้จ่าย (Cost) คือ สามารถลดต้นทุนในการลงทุนทางด้านโครงสร้างพื้นฐานทางเทคโนโลยี
3) ความอิสระของอุปกรณ์ และ สถานที่ (Device and Location Independence) คือ ผู้ใช้สามารถเข้าถึงระบบได้จากทุกที่โดยใช้เว็บเบราว์เซอร์โดยไม่ต้องคำนึงถึงสถานที่หรืออุปกรณ์ที่ใช้
4) เทคโนโลยีเสมือน (Virtualization) คือ ช่วยให้เกิดการแบ่งปันของเครื่องบริการ และ อุปกรณ์จัดเก็บข้อมูลที่เพิ่มขึ้น และ สามารถย้ายเครื่องบริการได้ง่าย
5) ความมั่นคง (Security) คือ สามารถจัดการความมั่นคงของข้อมูลได้ดีเนื่องจากข้อมูลรวมอยู่ที่เดียวกัน โครงสร้างพื้นฐานทางเทคโนโลยีมีขนาดใหญ่จึงคุ้มค่ากับการลงทุนด้านความมั่นคง
6) การบำรุงรักษา (Maintenance) คือ สามารถดูแลรักษาได้ง่าย เนื่องจากไม่จำเป็นต้องติดตั้งระบบในคอมพิวเตอร์ของผู้ใช้แต่ละคน

เมื่อแบ่งบริการคลาวด์ตามลักษณะการให้บริการ สามารถแบ่งได้เป็น 3 ประเภท ดังภาพที่ 2.1



ภาพที่ 2.1 ลักษณะการให้บริการคลาวด์

1) การให้บริการซอฟต์แวร์ (Software as a Service: SaaS) คือ การให้บริการโปรแกรมซอฟต์แวร์ให้แก่ผู้ใช้งานในรูปแบบของบริการผ่านทางเบราว์เซอร์ โดยที่ผู้ใช้ไม่จำเป็นต้องลงทุนซื้อโปรแกรมสำเร็จรูปและเครื่องคอมพิวเตอร์ เพื่อมาติดตั้งใช้บนเครื่องคอมพิวเตอร์ของตนเอง เช่น ระบบอีเมล (E-mail) ระบบจัดการลูกค้าสัมพันธ์ (Customer Relationship Management) เป็นต้น

2) การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS) คือ การให้บริการด้านแพลตฟอร์ม ซึ่งเป็นการให้บริการแพลตฟอร์มที่รองรับการทำงานของแอปพลิเคชันโดยผู้ใช้บริการสามารถปรับใช้และจัดการได้เอง การให้บริการแพลตฟอร์มนั้นประกอบด้วยระบบปฏิบัติการ ระบบฐานข้อมูล และระบบมิดเดิลแวร์ ตัวอย่างเช่น เครื่องบริการวินโดวส์ ลินุกซ์ ระบบฐานข้อมูลออราเคิล เป็นต้น

3) การให้บริการโครงสร้างพื้นฐาน (Infrastructure as a Service: IaaS) คือ การให้บริการด้านโครงสร้างพื้นฐาน ซึ่งเป็นการให้บริการฮาร์ดแวร์สำหรับเซิร์ฟเวอร์สตอเรจ ระบบเครือข่ายและระบบรักษาความมั่นคง ในรูปแบบเทคโนโลยีเสมือน (Virtualization) ซึ่งทำให้เราสามารถจัดสรรทรัพยากรได้แบบพลวัต (Dynamic) เช่น การเพิ่ม-ลดขนาดของหน่วยประมวลผลกลาง (Central Processing Unit) ฮาร์ดดิสก์ (Hard disk) หรือ แรม (Ram) ของเครื่องเซิร์ฟเวอร์ เป็นต้น

2.1.2 มาตรฐานความมั่นคงและความต้องการที่ไม่ใช่เชิงหน้าที่ของการคำนวณแบบคลาวด์

การให้บริการคลาวด์มีนโยบายด้านความมั่นคงเช่นเดียวกับการให้บริการด้านอื่น ๆ เพื่อสร้างความไว้วางใจให้กับผู้ใช้บริการคลาวด์ และ ช่วยลดความเสี่ยงที่จะเกิดกับการบริการคลาวด์

องค์กรที่นำเสนอมาตรฐานความมั่นคงที่จำเป็นต้องมีสำหรับการให้บริการคลาวด์ เช่น องค์กรความมั่นคงของคลาวด์ (ซีเอสเอ) เกิดจากความร่วมมือระหว่างภาคอุตสาหกรรม บริษัทเอกชน และสมาคมต่าง ๆ โดยมีวัตถุประสงค์เพื่อสนับสนุนแนวทางปฏิบัติที่ดีสำหรับการสร้างความเชื่อมั่นในด้านต่าง ๆ ของความต้องการที่ไม่ใช่เชิงหน้าที่ ในการให้บริการคลาวด์ได้ให้ความสำคัญกับการนำมาตรฐานความมั่นคงที่ถูกนิยามโดยองค์กรที่เชื่อถือได้ดังต่อไปนี้มาประยุกต์ใช้กับบริการคลาวด์ [1]

1) ISO (International Organization for Standardization) เป็นองค์กรมาตรฐานนานาชาติที่สร้างข้อกำหนดมาตรฐานของผลิตภัณฑ์ บริการ และ แนวปฏิบัติ ที่ครอบคลุมทุกด้านของธุรกิจและเทคโนโลยี ISO ได้กำหนดมาตรฐานเลขที่ 27001 ซึ่งอยู่ในชุดมาตรฐานความมั่นคงสารสนเทศ โดยมีหลักการเพื่อควบคุมการรักษาความมั่นคงของระบบสารสนเทศและเครือข่าย ลดความเสี่ยง และเพิ่มความมั่นคงเพื่อตอบสนองความจำเป็นของกระบวนการภายในขององค์กร และ ข้อกำหนดทางกฎหมาย
2) ISACA (Information Systems Audit and Control Association) เป็นองค์กรที่ดูแลเกี่ยวกับมาตรฐานและการทดสอบสำหรับสายงานทางด้านการตรวจสอบและการควบคุมระบบสารสนเทศ ปัจจุบัน ISACA นำเสนอแนวทางและกรอบด้านต่าง ๆ ในระบบสารสนเทศ เช่น การนำเสนอ COBIT (Control Objectives for Information and Related Technology) ซึ่งเป็นกรอบการกำกับดูแลเทคโนโลยีสารสนเทศโดยมีชุดเครื่องมือสำหรับกลุ่มผู้บริหารเพื่อเชื่อมโยงช่องว่างระหว่างการควบคุมความต้องการ ประเด็นทางเทคนิคและความเสี่ยงทางธุรกิจ นอกจากนี้ยังนำเสนอนโยบายและแนวทางปฏิบัติที่ดีสำหรับการควบคุมเทคโนโลยีสารสนเทศเพื่อช่วยเพิ่มมูลค่าทางธุรกิจให้แก่องค์กร
3) PCI Security Standard Council เป็นฟอรัมเปิดขนาดใหญ่ที่ก่อตั้งเพื่อวัตถุประสงค์ในการพัฒนา จัดการ ให้ความรู้และความตระหนักเกี่ยวกับความมั่นคง โดยจัดทำมาตรฐานความมั่นคง PCI DSS (Data Security Standard) ซึ่งเป็นมาตรฐานที่รวบรวมความต้องการที่ไม่ใช่เชิงหน้าที่ด้านการจัดการความมั่นคง นโยบาย ขั้นตอน สถาปัตยกรรมเครือข่าย การออกแบบซอฟต์แวร์ และความต้องการที่ไม่ใช่เชิงหน้าที่ด้านอื่น ๆ นอกจากนี้ยังจัดทำมาตรฐานด้านความมั่นคงของโปรแกรมประยุกต์ทางด้านการเงิน Payment Application Data Security Standard (PA-DSS) เป็นมาตรฐานที่ระบุความมั่นคงทางด้านการเงินที่ใช้งานผ่านโปรแกรมประยุกต์ต่าง ๆ เช่น แอปพลิเคชันจ่ายค่าบริการต่าง ๆ บนโทรศัพท์เคลื่อนที่ เว็บไซต์ทำธุรกรรมทางด้านการเงินของธนาคารต่าง ๆ

4) NIST (National Institute of Standards and Technology) สถาบันมาตรฐานและเทคโนโลยีระดับชาติเป็นหน่วยงานที่เป็นส่วนหนึ่งของกระทรวงพาณิชย์ประเทศสหรัฐฯ เป็นองค์กรที่สนับสนุนการพัฒนานวัตกรรมและการสร้างความสามารถทางอุตสาหกรรม และ จัดตั้งมาตรฐานในด้านต่าง ๆ รวมถึงมาตรฐานความมั่นคงของคลาวด์ซึ่งเป็นมาตรฐานชุดที่ 800-144 ซึ่งมีวัตถุประสงค์เพื่อสร้างมาตรฐานความมั่นคงและนโยบายความเป็นส่วนตัวสำหรับการใช้งานคลาวด์สาธารณะ

องค์กรข้างต้น มีวัตถุประสงค์คือ เพื่อสร้างมาตรฐานเพื่อใช้ควบคุมกระบวนการ การให้บริการให้เป็นไปตามความต้องการที่ไม่ใช่เชิงหน้าที่ด้านต่าง ๆ เช่น ด้านความมั่นคง ด้านความเป็นส่วนตัวของข้อมูล ด้านการตรวจสอบ เป็นต้น อย่างไรก็ตามผู้ใช้บริการคลาวด์จำเป็นต้องพิจารณาลักษณะขององค์กรของผู้ใช้บริการ และความต้องการที่ไม่ใช่เชิงหน้าที่ที่ผู้ให้บริการคลาวด์เสนอ ก่อนตัดสินใจเปลี่ยนไปใช้บริการคลาวด์เพื่อลดความเสี่ยง โดยสิ่งที่ต้องคำนึงถึง ได้แก่

1) ความโปร่งใสของผู้ให้บริการคลาวด์ ไม่ว่าจะเป็นการให้บริการคลาวด์ในลักษณะที่เป็นการให้บริการซอฟต์แวร์ การให้บริการแพลตฟอร์ม หรือการให้บริการโครงสร้างพื้นฐาน ก็ตาม
2) สถาปัตยกรรมโครงสร้างพื้นฐาน และ เทคโนโลยี ของผู้ให้บริการคลาวด์ ส่งผลกระทบต่อข้อตกลงในการให้บริการและมาตรการด้านความมั่นคงของหน่วยงานผู้ใช้บริการคลาวด์หรือไม่
3) กระบวนการหรือลักษณะการทำงานมีลักษณะสอดคล้องกับลักษณะของการให้บริการคลาวด์หรือไม่
4) ลักษณะการใช้งานคลาวด์แบบใดที่เหมาะสมกับองค์กร ได้แก่ แบบสาธารณะ แบบส่วนบุคคล หรือแบบผสม
5) ปัญหาของความต้องการแบนด์วิดท์ (Bandwidth Requirement) เมื่อเปลี่ยนมาใช้บริการคลาวด์ เช่น การเกิดสภาพคอขวด (Bottleneck) มีโอกาสเกิดขึ้นได้หรือไม่ [4]
6) ผลกระทบทางการเงินระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์ ได้แก่ ค่าบริการที่ไม่มีการรับประกัน ปัญหาทางกฎหมายที่อาจเกิดขึ้นกับผู้ให้บริการคลาวด์ มีโอกาสเกิดขึ้นได้หรือไม่ [4]
7) การสูญเสียการควบคุมข้อมูล อาจนำมาซึ่งปัญหาการรักษาความลับของข้อมูล [4]
8) การถูกโจมตีจากภายนอกมีโอกาสเกิดขึ้นได้หรือไม่และผู้ให้บริการคลาวด์มีวิธีป้องกันอย่างไร [4]

2.1.3 ความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงขององค์กรความมั่นคงของคลาวด์

ความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงเป็นประเด็นสำคัญในการใช้และการให้บริการคลาวด์ งานวิจัยที่นำเสนอโดยองค์กรความมั่นคงของคลาวด์หรือซีเอสเอ เป็นงานวิจัยหลักที่ถูกนำมาใช้เป็นแนวคิดของวิทยานิพนธ์นี้ งานวิจัยขององค์กรความมั่นคงของคลาวด์ที่ถูกนำมาใช้ในวิทยานิพนธ์นี้

แบ่งเป็น 2 งานวิจัย ได้แก่ เมตริกซ์ควบคุมคลาวด์ [1] และแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน [2]

เมตริกซ์ควบคุมคลาวด์เป็นเมตริกซ์ที่รวบรวมความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคง 16 ด้าน พร้อมทั้งกำหนดเป้าหมายการควบคุมความมั่นคง (Control Domain) ส่วนแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกันเป็นการระบุคำถามที่สอดคล้องกับการประเมินเป้าหมายการควบคุมความมั่นคงที่ระบุไว้ในเมตริกซ์ควบคุมคลาวด์ ทั้งนี้เพื่อให้ผู้ให้บริการคลาวด์ใช้เป็นแนวทางในการนำไปปฏิบัติเพื่อสร้างความเชื่อมั่นให้กับผู้ใช้บริการคลาวด์ และเพื่อให้ผู้ใช้บริการคลาวด์ใช้เป็นแนวทางในการตรวจสอบผู้ให้บริการคลาวด์ เมตริกซ์ควบคุมคลาวด์และคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ จัดทำขึ้นโดยรวบรวมมาตรฐานขององค์กรที่ภาคอุตสาหกรรมให้การยอมรับ ได้แก่ ISO 27001, ISACA, NIST, COBIT, PCI, Jericho Forum และ NERC CIP โดยลักษณะของเมตริกซ์ควบคุมคลาวด์และคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ เป็นไปดังตัวอย่างตามตารางที่ 2.1 และตารางที่ 2.2

ตารางที่ 2.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์

ความมั่นคง	รหัส	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
1. ความมั่นคงของโปรแกรมประยุกต์และส่วนต่อประสาน (Application & Interface Security)	AIS	Application Security	AIS-01	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.
2. การรับรองการตรวจสอบและการปฏิบัติตาม (Audit Assurance & Compliance)	AAC	Audit Planning	AAC-01	Audit plans, activities, and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.

ตารางที่ 2.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัส	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
3. การจัดการความต่อเนื่องทางธุรกิจและความยืดหยุ่นเชิงปฏิบัติการ (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

ตารางที่ 2.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัส	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
				• Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation

ตารางที่ 2.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัส	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
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.

ตารางที่ 2.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัส	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
5. ความมั่นคงของข้อมูลและการจัดการวัฏจักรชีวิตสารสนเทศ (Data Security & Information Lifecycle Management)	DSI	Classification	DSI-01	Data and objects containing data shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization, third-party obligation for retention, and prevention of unauthorized disclosure or misuse.

ตารางที่ 2.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัส	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
6. ความมั่นคงของศูนย์ข้อมูล (Datacenter Security)	DCS	Asset Management	DCS-01	Assets must be classified in terms of business criticality in support of dynamic and distributed physical and virtual computing environments, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly (or in real-time), and assigned ownership supported by defined roles and responsibilities, including those assets used, owned, or managed by customers (tenants).

ตารางที่ 2.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัส	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
7. การเข้ารหัสลับและการจัดการกุญแจ (Encryption & Key Management)	EKM	Entitlement	EKM-01	All entitlement decisions shall be derived from the identities of the entities involved. These shall be managed in a corporate identity management system. Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.

ตารางที่ 2.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัส	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
8. วิธีการปกครองและการจัดการความเสี่ยง (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 established and authorized based on business need.

ตารางที่ 2.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัส	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
9. ทรัพยากรมนุษย์ (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. เอกลักษณ์และการจัดการการเข้าถึง (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.

ตารางที่ 2.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัส	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
11. โครงสร้างพื้นฐานและความมั่นคงของเทคโนโลยีเสมือน (Infrastructure & Virtualization Security)	IVS	Audit Logging / Intrusion Detection	IVS-01	Higher levels of assurance are required for protection, retention, and lifecyle 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.
12. การทำงานร่วมกันและ ใช้ได้หลายระบบ (Interoperability & Portability)	IPY	APIs	IPY-01	The provider shall use open and published APIs to ensure the broadest support for interoperability between components and to facilitate migrating applications.

ตารางที่ 2.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัส	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
13. ความมั่นคงของระบบเคลื่อนที่ (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 การค้นพบอิเล็กทรอนิกส์ และกระบวนการทางกฎหมายของคลาวด์ (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 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัส	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
15.การจัดการสายโซ่อุปทาน ความโปร่งใส และภาระรับผิดชอบ (Supply Chain Management, Transparency and Accountability)	STA	Data Quality and Integrity	STA-01	Providers shall inspect, account for, and correct data quality errors and risks inherited from partners within their cloud supply-chain. 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.

ตารางที่ 2.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

ความมั่นคง	รหัส	ตัวอย่าง		
		เป้าหมายการควบคุมความมั่นคง	รหัสเป้าหมายการควบคุมความมั่นคง	รายละเอียดเป้าหมายการควบคุมความมั่นคง
16.การคุกคามและการจัดการจุดอ่อน (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.

ตารางที่ 2.2 ตัวอย่างของแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน

รหัสเป้าหมาย	รหัสคำถาม	คำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่	ลักษณะการให้บริการคลาวด์ที่ถูกประเมินได้จากคำถาม	ผู้เกี่ยวข้องที่สามารถนำคำถามไปประยุกต์ใช้ในการประเมินได้
AIS-01	AIS-01.1	Do you utilize 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)?	1. การให้บริการโครงสร้างพื้นฐาน 2. การให้บริการแพลตฟอร์ม 3. การให้บริการซอฟต์แวร์	1. ผู้ให้บริการคลาวด์ 2. ผู้ใช้บริการคลาวด์

2.1.4 การสกัดข้อมูลและการจัดเก็บสารสนเทศ

2.1.4.1 การสกัดข้อมูล

การสกัดข้อมูล [5] เป็นกระบวนการนำข้อมูลจากเว็บไซต์ (Website) โดยระบุยูอาร์แอล (URL) ที่ต้องการดึง จากนั้นจึงทำการเก็บข้อมูลในคลังเก็บเอกสารส่วนกลาง (Central Repository) เพื่อนำมาสร้างคำสำคัญต่อไป

2.1.4.2 การจัดเก็บสารสนเทศ

กระบวนการจัดเก็บสารสนเทศ [5] จะทำการประมวลผลข้อความในคลังเก็บเอกสาร เพื่อนำคำสำคัญของเอกสารมาจัดทำคำสำคัญและมีการกำหนดค่าน้ำหนักคำให้แต่ละคำสำคัญของแต่ละเอกสารเหล่านั้นก่อนการจัดเก็บไว้ในไฟล์คำสำคัญ ในงานวิจัยนี้จะเก็บอยู่ในรูปแบบเอกซ์เอ็มแอล

2.1.4.2.1 การทำดัชนีคำสำคัญ

การทำดัชนีคำสำคัญ มีขั้นตอนในการสกัดคำสำคัญจากเอกสารต่าง ๆ ดังแสดงในภาพที่ 2.2

ภาพที่ 2.2 ขั้นตอนการสร้างดัชนีคำสำคัญ

ในขั้นตอนการสกัดคำสำคัญจากเอกสาร (Document) ที่ต้องการจัดเก็บนั้น มีขั้นตอนดังต่อไปนี้

1. วิเคราะห์คำศัพท์ (Lexical Analysis) เป็นกระบวนการในการเปลี่ยนจากสายอักขระ (Strings) ให้เป็นคำโดยการพิจารณาช่องว่าง การขึ้นบรรทัดใหม่ ตัวพิมพ์ใหญ่ และเครื่องหมายต่าง ๆ เช่น เครื่องหมายวรรคตอน เครื่องหมายมหัพภาค ฯลฯ เป็นต้น เพื่อให้ได้คำมาวิเคราะห์ในขั้นตอนต่อไป
2. ตัดคำหยุด (Elimination of Stop Words) คำหยุดคือคำที่ไม่มีความสำคัญเชิงความหมาย และไม่มีผลในการจำแนกความคล้ายกันของเอกสาร เช่น in, on, of, at, which, that , a, an, the เป็นต้น
3. จัดกลุ่มคำนาม (Noun Grouping) เป็นการนำคำที่เมื่อรวมกันแล้ว จะทำให้ได้ความหมายที่เฉพาะเจาะจงมากขึ้น เช่น นำคำว่า system ซึ่งแปลว่า ระบบ มารวมกับคำว่า analyst ซึ่งแปลว่าระบบ จะได้คำว่า system analyst ซึ่งแปลว่า นักวิเคราะห์ระบบ เป็นต้น
4. หารากศัพท์ (Stemming) คือการทำคำที่ยังไม่เป็นรากศัพท์ให้อยู่ในรูปรากศัพท์ เช่น
   1) คำศัพท์ที่อยู่ในรูปพหูพจน์ (Plural) เช่น Risks เปลี่ยนเป็น Risk เป็นต้น
   2) คำศัพท์ที่อยู่ในรูปอดีต (Past Form) เช่น Approved เปลี่ยนเป็น Approve เป็นต้น
   3) คำศัพท์ที่อยู่ในรูปกำลังกระทำ (Participle Form) เช่น Monitoring เปลี่ยนเป็น Monitor เป็นต้น
5. ตรวจสอบคำศัพท์ควบคุม (Controlled Vocabulary Checking) เป็นการสกัดคำสำคัญโดยจะมีการเก็บคำศัพท์ที่สำคัญสำหรับขั้นตอนการทำคำสำคัญไว้เป็นคำศัพท์ควบคุม หากสกัดได้คำใดที่ปรากฏอยู่ในคำศัพท์ควบคุม คำนั้นจะถูกเลือกมาทำคำสำคัญ เช่น ในไฟล์เก็บคำศัพท์ควบคุมมีคำว่า Audit Planning เมื่อสกัดได้คำว่า Audit Planning ก็จะนำคำนี้มาทำคำสำคัญ (Taxonomy Keywords) ต่อไป

2.1.4.2.2 การหาค่าน้ำหนักคำ (Term Weighting)

ขั้นตอนนี้จะนำคำสำคัญจากขั้นตอนที่ 2.1.4.2.1 มาทำการหาค่าน้ำหนักคำโดยใช้ค่าส่วนกลับความถี่ของเอกสาร (Inverted Document Frequency : IDF) และค่าความถี่ของคำ (Term Frequency : TF) ซึ่งสามารถคำนวณได้จากสมการที่ 2.1 และ 2.2 ตามลำดับ

$$idf(i) = \log_2 \frac{N}{n_i} \qquad (2.1)$$

เมื่อ $idf(i)$ คือ ค่าส่วนกลับความถี่ของเอกสารของเทอม i

N คือ จำนวนเอกสารทั้งหมดที่เก็บอยู่ในฐานข้อมูล

n_i คือ จำนวนเอกสารที่เทอม i ปรากฏ

$$tf(i,j) = \begin{cases} 1+\log_2 f_{i,j} & iff_{i,j} > 0 \\ 0 & otherwise \end{cases} \qquad (2.2)$$

เมื่อ $tf(i,j)$ คือ ค่าความถี่ที่ถูกปรับให้อยู่ในค่าประมาณเดียวกันกับค่าส่วนกลับความถี่ของเอกสาร

$f_{i,j}$ คือ จำนวนครั้งของเทอม i ที่ปรากฏในเอกสาร j

เมื่อได้ค่าส่วนกลับความถี่ของเอกสารและค่าความถี่ของคำแล้ว สามารถคำนวณหาค่าน้ำหนักคำได้จากสมการที่ 2.3

$$w(i,j) = tf(i,j) \cdot idf(i) \qquad (2.3)$$

เมื่อ $w(i,j)$ คือ ค่าน้ำหนักคำของเทอม i ในเอกสาร j

ค่าน้ำหนักคำถูกใช้ต่อไปในการจำแนกเอกสาร ถ้าเทอม i มีความถี่ในเอกสาร j สูงจะทำให้ค่าน้ำหนักคำสูงขึ้น อย่างไรก็ตาม ถ้าเอกสารส่วนมากในคอลเลคชันบรรจุเทอม i ค่าน้ำหนักคำจะลดลงตามค่าส่วนกลับความถี่ของเอกสาร เนื่องจากค่าส่วนกลับความถี่ของเอกสารจะลดลงถ้าเทอม i ปรากฏอยู่ในหลายเอกสารและจะสูงขึ้นถ้าเทอม i ปรากฏในไม่กี่เอกสาร

2.1.5 การจำแนกข้อความ

การจำแนกข้อความ (Text Classification) [5] เป็นกระบวนการในการจำแนกสารสนเทศออกเป็นกลุ่มหรือประเภทต่าง ๆ โดยงานวิจัยนี้ใช้การจำแนกข้อความอย่างง่าย (Naïve Text Classification) เพื่อจำแนกความสอดคล้องด้านความมั่นคงของข้อความในหน้าเว็บผู้ให้บริการคลาวด์ตามเมตริกซ์ควบคุมคลาวด์

2.1.5.1 การจำแนกข้อความอย่างง่าย

การจำแนกข้อความอย่างง่าย [5] เป็นอัลกอริทึมในการจำแนกข้อมูลจากกลุ่มข้อมูลที่มีการแบ่งกลุ่มเอาไว้อย่างชัดเจน โดยจะสร้างเอกสารที่เป็นตัวแทนแต่ละกลุ่ม จากนั้นนำเอกสารที่ต้องการจัดกลุ่มเข้ามาเทียบว่าเป็นเอกสารในกลุ่มใด สามารถคำนวณได้จากขั้นตอนต่อไปนี้

1) ให้ $\vec{d}_j$ เป็นตัวแทนเอกสารแต่ละกลุ่มถูกแสดงด้วยเวกเตอร์ $\vec{d}_j$ ดังสมการที่ 2.4

$$\vec{d}_j = (w_{1,j}, w_{2,j}, ..., w_{t,j}) \quad (2.4)$$

เมื่อ $w_{i,j}$ คือ ค่าน้ำหนักของเทอม k_i ในเอกสาร d_j ซึ่งหาได้จากสมการที่ 2.3

t คือ จำนวนของคำศัพท์

2) ให้ $\vec{p}_j$ เป็นตัวแทนเอกสารที่ต้องการจำแนกดังสมการที่ 2.5

$$\vec{p} = (w_{1,p}, w_{2,p}, ..., w_{t,p}) \quad (2.5)$$

เมื่อ $w_{i,p}$ คือ ค่าน้ำหนักของเทอม k_i ในเอกสาร $\vec{p}$ ซึ่งหาได้จากสมการที่ 2.3

t คือ จำนวนของคำศัพท์

3) ค่าความสอดคล้องระหว่างเอกสาร $\vec{d}_j$ กับเอกสาร $\vec{p}$ คำนวณได้ดังสมการที่ 2.6 นั่นคือ ถ้าค่าความสอดคล้องมีค่ามากแสดงว่าเอกสารมีความคล้ายกัน

$$sim(d_j, p) = \frac{\vec{d}_j \bullet \vec{p}}{|\vec{d}_j| \times |\vec{p}|} = \frac{\sum_{i=1}^{t} w_{i,j} \times w_{i,p}}{\sqrt{\sum_{i=1}^{t} w_{i,j}^2} \times \sqrt{\sum_{i=1}^{t} w_{i,p}^2}} \quad (2.6)$$

เมื่อ $sim(d_j, p)$ คือ ค่าความคล้ายของเอกสาร $\vec{d}_j$ กับเอกสาร $\vec{p}$ อยู่ใน [0,1]

d_j คือ เอกสารแต่ละกลุ่ม

p คือ เอกสารที่ต้องการจำแนก

2.1.6 การวัดประสิทธิภาพการจำแนก

ในการวัดประสิทธิภาพของวิธีที่เสนอในการจำแนกความสอดคล้องด้านความมั่นคงของผู้ให้บริการคลาวด์ว่ามีความถูกต้อง ผู้วิจัยจะประเมินเทียบกับผลการจำแนกด้วยมือ ผู้วิจัยจะใช้สหสัมพันธ์ของเพียร์สัน (The Pearson's Correlation) ในการหาค่าความสัมพันธ์ระหว่างตัวแปรสองตัวแปร ซึ่งค่าที่ได้เรียกว่าสัมประสิทธิ์สหสัมพันธ ค่าปกติจะอยู่ระหวาง -1 ถึง 1 โดยค่า -1 หมายถึงตัวแปรทั้งสองมีความสัมพันธ์เชิงเส้นแบบผกผันกัน ค่า 1 หมายถึงตัวแปรทั้งสองมีความสัมพันธ์เชิงเส้นแบบตามกันอย่างสมบูรณ์ และค่า 0 หมายถึงตัวแปรทั้งสองไม่สัมพันธ์เชิงเส้นกัน สามารถคำนวณได้ดังสมการที่ 2.7

$$r = \frac{n\sum_{i=1}^{n} x_i y_i - \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} y_i\right)}{\sqrt{\left(n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2\right)\left(n\sum_{i=1}^{n} y_i^2 - \left(\sum_{i=1}^{n} y_i\right)^2\right)}} \qquad (2.7)$$

เมื่อ r คือ ค่าสัมประสิทธิ์สหสัมพันธ์

n คือ จำนวนคู่ผลลัพธ์การจำแนก

x_i คือ ผลลัพธ์จากการจำแนกด้วยวิธีที่เสนอของคู่ที่ i

y_i คือ ผลลัพธ์จากการจำแนกด้วยมือของคู่ที่ i

การทดสอบว่าค่าสหสัมพันธ์มีนัยสำคัญทางสถิติหรือไม่ ทำโดยตั้งสมมติฐาน

H_0: x และ y ไม่มีความสัมพันธ์เชิงเส้นกัน

H_1: x และ y มีความสัมพันธ์เชิงเส้นกัน

จากนั้นนำค่า r ที่คำนวณได้ไปเทียบกับค่าวิกฤต r_{xy} จากตารางค่าวิกฤต (Critical Value) ของเพียร์สันโดยใช้ค่าองศาอิสระ (Degree of Freedom) df = n-2 ที่ระดับนัยสำคัญ (Significance Level) α โดยหากค่า r ที่คำนวณได้มีค่ามากกว่าหรือเท่ากับ ค่าวิกฤต r_{xy} จะปฏิเสธ H_0 และยอมรับ H_1

2.1.7 ออนโทโลจี

ออนโทโลจี (Ontology) [6] คือ ข้อกำหนดเกี่ยวกับแนวความคิด (Concepts) เป็นการบรรยายแนวความคิดของโดเมนหรือขอบเขตความสนใจใด ๆ ในรูปของสิ่งต่าง ๆ ที่อยู่ภายในโดเมนและความสัมพันธ์ ระหว่างสิ่งเหล่านั้น ซึ่งสามารถแสดงออกมา ในรูปของระบบสัญลักษณ์ (Notation)

ตัวอย่างเช่น คลาส (Class) อินสแตนซ์ (Instance) ความสัมพันธ์ (Relationship) คุณสมบัติ (Property) และกฎ (Rule) โดยใช้ภาษาสำหรับแสดงความรู้ (Knowledge Representation Language) ที่ใช้คำศัพท์มาเชื่อมต่อกัน เป็นประโยคเพื่อบรรยายถึงสิ่งของในแง่มุมต่าง ๆ ทั้งนี้การใช้ระบบสัญลักษณ์จะช่วยสื่อความหมาย (Semantics) ให้ซอฟต์แวร์และเครื่องมือเข้าใจ และสามารถนำไปใช้ประโยชน์ได้ นอกจากนี้คำจำกัดความของออนโทโลจี หมายถึง การอธิบายความสัมพันธ์โครงสร้างความรู้ให้อยู่ในรูปแบบลำดับชั้นเชิงวัตถุ (Hierarchical Data Structure) เพื่ออธิบายขอบเขตขององค์ความรู้ที่สนใจ

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง

งานวิจัยที่เกี่ยวข้องกับการพิจารณาความสามารถของผู้ให้บริการคลาวด์ในการให้บริการที่มีความมั่นคง มีดังนี้

2.2.1 งานวิจัยของ Wayne A. Pauley [7] นำเสนอการประเมินความโปร่งใสของผู้ให้บริการคลาวด์ในรูปแบบ บัตรลงคะแนน (Scorecard) ซึ่งจะประเมิน 1) ความมั่นคง 2) ความเป็นส่วนตัว 3) ความสามารถในการตรวจสอบได้ และ 4) ข้อตกลงในการให้บริการ บนแนวความคิดที่ว่า ความพร้อมของข้อมูลที่เกี่ยวข้องกับการประเมินทั้งสี่ด้านดังกล่าว ทำให้เกิดความโปร่งใสและเกิดความสามารถในการนำข้อมูลมาประเมินความเสี่ยงได้ Pauley ได้เสนอรูปแบบการประเมินผู้ให้บริการคลาวด์ในลักษณะของบัตรลงคะแนนบนเว็บไซต์ ทั้งนี้เพื่อลดการใช้คนในการทำการประเมิน จากนั้นผู้วิจัยจะเก็บรวบรวมข้อมูลจากผู้ให้บริการคลาวด์รายต่าง ๆ เพื่อนำมาตอบคำถามที่อยู่ในบัตรลงคะแนน โดยลักษณะของคำถามจะเป็นคำถามที่ตอบว่า “ใช่” หรือ “ไม่ใช่” ถ้าคำตอบคือ “ใช่” คะแนนของคำถามเป็น 1 คะแนน แต่ถ้าคำตอบคือ “ไม่ใช่” คะแนนของคำถามจะคิดเป็น 0 คะแนน และคำถามที่สร้างขึ้นจะอ้างอิงตามมาตรฐานขององค์กรความมั่นคงของคลาวด์ NIST และองค์กรความมั่นคงด้านเครือข่ายและข้อมูลของยุโรป (European Network and Information Security Agency: ENISA) โดยกระบวนการในการประเมินแบ่งเป็น 3 ขั้นตอน ได้แก่

1) ขั้นตอนก่อนการประเมิน (Pre-assessment) ในขั้นตอนนี้ผู้ใช้บริการคลาวด์จะถามคำถามชี้นำประเภท ลักษณะการให้บริการคลาวด์ ลักษณะการใช้งานคลาวด์ หรือผู้ให้บริการคลาวด์เป็นองค์กรเพื่อแสวงผลกำไรหรือไม่ คำถามเหล่านี้จะสามารถคัดกรองผู้ให้บริการคลาวด์ได้ในเบื้องต้น ว่าลักษณะของผู้ให้บริการคลาวด์เหมาะสมกับลักษณะทางธุรกิจของผู้ใช้บริการคลาวด์หรือไม่

2) ขั้นตอนการลงรายละเอียดการประเมิน (Detailed Assessment) ในขั้นตอนนี้จะเป็นการสำรวจผู้ให้บริการคลาวด์แต่ละรายจากเว็บไซต์ของผู้ให้บริการคลาวด์เองเพื่อเก็บรวบรวมข้อมูลทั้ง 4 ด้าน ได้แก่

- ข้อมูลด้านความมั่นคง

ข้อมูลที่เก็บรวบรวมเพื่อนำมาประเมินในด้านความมั่นคง ตัวอย่างเช่น ผู้ให้บริการมีการทำตามมาตรฐานด้านความมั่นคง เช่น COBIT, ISO27000 หรือ NIST หรือไม่

- ข้อมูลด้านความเป็นส่วนตัว

ข้อมูลที่เก็บรวบรวมเพื่อนำมาประเมินในด้านความเป็นส่วนตัว ตัวอย่างเช่น ผู้ให้บริการมีนโยบายการรักษาความเป็นส่วนตัวของผู้ใช้บริการหรือไม่ หรือถ้าผู้ให้บริการคลาวด์มีการเรียกใช้บริการจากผู้ให้บริการรายอื่น จะมีข้อตกลงร่วมกันเกี่ยวกับนโยบายความเป็นส่วนตัวหรือไม่

- ความสามารถในการตรวจสอบได้

ข้อมูลที่เก็บรวบรวมเพื่อนำมาประเมินความสามารถในการตรวจสอบได้ ตัวอย่างเช่น ผู้ให้บริการคลาวด์มีการทำตามมาตรฐานด้านความสามารถในการตรวจสอบได้ เช่น ISACA หรือไม่

- ข้อตกลงในการให้บริการ

ข้อมูลที่เก็บรวบรวมเพื่อนำมาประเมินในด้านข้อตกลงในการให้บริการ ตัวอย่างเช่น ผู้ให้บริการมีการนำเสนอข้อตกลงในการให้บริการหรือไม่ และข้อตกลงนี้มีการประยุกต์ใช้ได้กับทุกบริการของผู้ให้บริการคลาวด์หรือไม่

3) ขั้นตอนหลังการประเมิน (Post-assessment) ในขั้นตอนนี้จะเป็นการเปรียบเทียบข้อมูลที่รวบรวมได้กับนโยบายหรือมาตรฐานที่จัดทำขึ้นภายในองค์กร เพื่อดูว่าผู้ให้บริการคลาวด์ ให้ข้อมูลที่เพียงพอกับนโยบายหรือมาตรฐานขององค์กรหรือไม่

ผลการประเมินผู้ให้บริการคลาวด์แต่ละราย จะใช้วิธีการนับคะแนนจากคำถามแต่ละข้อและพิจารณาจากผลรวมคะแนน รวมทั้งเปรียบเทียบคะแนนในด้านต่าง ๆ ทั้งสี่ด้านของผู้ให้บริการคลาวด์แต่ละราย

ถึงแม้ว่าแนวความคิดของงานวิจัยของ Pauley จะเป็นไปเพื่อลดเวลาและลดการใช้คนในการประเมิน แต่ขั้นตอนในการรวบรวมข้อมูลซึ่งต้องอาศัยผู้ใช้บริการคลาวด์หรือองค์กรที่สามในการรวบรวมข้อมูลจากผู้ให้บริการคลาวด์ก็เป็นขั้นตอนที่ต้องใช้คนและใช้เวลา

2.2.2 บทความของ Bret Michael [8] และงานวิจัยของ Sun Microsystems, Inc. [9] ให้ความสำคัญกับประเด็นความน่าเชื่อถือและความโปร่งใสของคลาวด์ โดย Bret Michael ตั้งคำถามถึงปริมาณข้อมูลที่ใช้ในการประเมินความโปร่งใส ว่าต้องมีข้อมูลเท่าไรถึงจะเพียงพอ และมุ่งเน้นให้ผู้ให้บริการคลาวด์ให้ความสำคัญกับการสร้างความน่าเชื่อถือแก่ผู้ใช้บริการคลาวด์

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

2.2.3 งานวิจัยของ Catherine Everett [10] ได้ตั้งประเด็นเกี่ยวกับการตั้งคำถามที่นำไปสู่การประเมินความมั่นคง โดยกล่าวว่า หากผู้ใช้บริการคลาวด์ไม่สามารถตั้งคำถามต่อผู้ให้บริการคลาวด์ได้ว่าคาดหวังความมั่นคงจากสิ่งใดบ้าง (เป็นคำถามที่สะท้อนให้เห็นว่าผู้ใช้บริการคลาวด์มีลักษณะองค์กรแบบใด และต้องการการใช้งานคลาวด์แบบใด) จะถือเป็นความเสี่ยงในการใช้บริการ

2.2.4 งานวิจัยของ Burton S. Kaliski Jr. และ Wayne Pauley [11] ได้นำเสนอบริการการประเมินความเสี่ยง (Risk Assessment as a Service) โดยมีวัตถุประสงค์เพื่อให้องค์กรนำผลการประเมินความเสี่ยงมาใช้ในการตัดสินใจว่าจะประยุกต์ใช้ทรัพยากรใหม่ที่ยังไม่เคยใช้บริการมาก่อนอย่างไร เพื่อให้ทรัพยากรเหล่านั้นสามารถปกป้องสินทรัพย์ที่มีความสำคัญขององค์กรได้โดยการประเมินความเสี่ยงประกอบด้วยการประเมินความมั่นคง การตรวจสอบและการประเมินผลจากองค์กรภายนอก และการประเมินความเป็นส่วนตัว งานวิจัยยังได้ให้เหตุผลในการประเมินความเสี่ยงของการใช้บริการคลาวด์ว่า การบริการคลาวด์เปรียบเสมือนการทำ

การค้าทางอิเล็กทรอนิกส์ (E-Commerce) ซึ่งประเด็นความมั่นคงและความเป็นส่วนตัวในการทำการค้าทางอิเล็กทรอนิกส์ถือเป็นเรื่องสำคัญเนื่องจากนำมาซึ่งความเชื่อใจและความไว้วางใจของผู้ใช้บริการ เช่นเดียวกันกับการให้บริการคลาวด์ที่ความเชื่อใจของผู้ใช้บริการคลาวด์มีความสำคัญ ดังนั้น ผู้ให้บริการคลาวด์จึงควรมีสิ่งที่แสดงให้เห็นถึงกระบวนการรักษาความมั่นคงและความเป็นส่วนตัวของข้อมูลหรือหลักฐานอ้างอิง เพื่อให้ผู้ใช้บริการคลาวด์ประเมินได้ เช่น Amazon.com ที่ออกประกาศว่าได้ผ่านการตรวจสอบ SAS70 Type 2 ซึ่งเป็นการตรวจสอบว่าองค์กรได้ทำตามวัตถุประสงค์และกิจกรรมด้านความมั่นคงตามที่กำหนดไว้หรือไม่ โดยส่วนใหญ่จะเน้นไปที่เทคโนโลยีสารสนเทศ อย่างไรก็ตาม หลายองค์กรพยายามสร้างมาตรฐานการรักษาความมั่นคงและความเป็นส่วนตัวในการให้บริการคลาวด์ เช่น ซีเอสเอ แต่มาตรฐานที่สร้างขึ้นก็เป็นเพียงคำถามปลายเปิดที่ไม่สามารถวัดความมั่นคงและความเป็นส่วนตัวได้อย่างชัดเจน สำหรับการประเมินผู้ให้บริการคลาวด์ในงานวิจัยของ Burton มองว่า เนื่องจากบริการคลาวด์เป็นบริการที่สามารถจัดเตรียมการใช้งานได้ตามความต้องการของผู้ใช้บริการเอง โดยไม่ต้องมีการปฏิสัมพันธ์กับผู้ให้บริการดังนั้น การประเมินก็ควรเป็นไปในลักษณะเดียวกัน คือ ผู้ใช้บริการคลาวด์สามารถประเมินผู้ให้บริการคลาวด์ได้ตามต้องการ โดยไม่ต้องมีปฏิสัมพันธ์กับผู้ให้บริการคลาวด์ และจากลักษณะการเป็นบริการของคลาวด์ (As a Service) การประเมินจึงควรทำได้แบบเป็นบริการด้วยเช่นเดียวกัน ดังนั้นงานวิจัยจึงเสนอบริการการประเมินความเสี่ยงซึ่งเป็นการประเมินแบบทันทีทันใด (Real Time Assessment) เช่น ผู้ให้บริการคลาวด์ มีการแสดงหลักฐานอ้างอิงตลอดระยะเวลาที่มีการปฏิบัติการ (Run-Time) โดยหลักฐานอ้างอิงอาจเป็นล็อกไฟล์ (Log Files) ที่แสดงให้เห็นว่าผู้ให้บริการมีหลักฐานที่บันทึกข้อมูลที่ผ่านเข้าออกสู่ระบบ นอกจากนี้ Burton ยังให้เหตุผลว่าควรมีการออกแบบการประเมินให้เข้ากับลักษณะการทำงานของคลาวด์ เช่น บริการคลาวด์ที่มีการทำงานร่วมกันระหว่างผู้ให้บริการคลาวด์หลายเจ้า เป็นต้น ถึงแม้ว่าผลสรุปจากงานวิจัยของ Kaliski Jr. และ Pauley จะมีเพียงแนวคิดในการออกแบบการประเมินเท่านั้น แต่แนวคิดในการพยายามทำให้การประเมินเป็นไปแบบทันทีทันใดเป็นสิ่งที่น่าสนใจสำหรับผู้วิจัย

2.2.5 งานวิจัยของ David Tancock และคณะ [12] นำเสนอเครื่องมือที่ใช้วัดความเป็นส่วนตัวของการคำนวณแบบคลาวด์โดยเครื่องมือที่พัฒนาขึ้น จะเป็นการนำเสนอความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความเป็นส่วนตัวที่อาจก่อให้เกิดความเสี่ยงในองค์กร โดยเน้นกลุ่มผู้ใช้งานซึ่งเป็นองค์กรที่ไม่มีความเชี่ยวชาญทางความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความเป็นส่วนตัว เพื่อให้องค์กรวางแนวทางในการป้องกันการเกิดความเสี่ยง โดยวิธีนี้จะทำให้การป้องกันความเสี่ยงด้านความเป็นส่วนตัวถูกนำมาใช้ตั้งแต่ขั้นตอนการเริ่มต้นโครงการ นอกจากนี้ผู้ใช้บริการคลาวด์ยังสามารถนำข้อมูลความเสี่ยงมาวิเคราะห์ในการริเริ่มโครงการต่าง ๆ ว่าเหมาะสมหรือไม่ ส่วน

การออกแบบเครื่องมือ จะมีการออกแบบในลักษณะของแบบสอบถามเพื่อให้ผู้ให้บริการคลาวด์ตอบคำถามเกี่ยวกับนโยบายการรักษาความเป็นส่วนตัวในด้านต่าง ๆ แล้วนำคำตอบมาเก็บบันทึกเป็นฐานความรู้ (Knowledge Base)เพื่อใช้วิเคราะห์ความเสี่ยงด้านความเป็นส่วนตัวต่อไป

2.2.6 งานวิจัยของ Nuntapun Bhensook และ Twittie Senivongse [13] นำเสนอวิธีการประเมินคะแนนความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงของผู้ให้บริการคลาวด์ โดยนำวิธีจีคิวเอ็ม (Goal Question Metric) มาใช้กำหนดหลักฐานที่แสดงให้เห็นถึงนโยบายหรือกระบวนการที่ผู้ให้บริการคลาวด์จัดทำขึ้นเพื่อเป็นวิธีปฏิบัติในการรักษาความมั่นคงของทรัพยากรคลาวด์ที่ให้บริการ ผู้วิจัยนำแนวคิดของวิธีจีคิวเอ็มซึ่งประกอบด้วยการกำหนดเป้าหมาย คำถาม และตัววัด มาประยุกต์ใช้กับเมตริกซ์ควบคุมคลาวด์และคำถามการประเมินตามความคิดเห็นของคนส่วนใหญ่ที่ถูกกำหนดโดยองค์กรความมั่นคงของคลาวด์ ทำให้ผู้วิจัยสามารถวิเคราะห์หาตัววัดซึ่งหมายถึงหลักฐานจำนวน 224 ข้อ ที่แสดงให้เห็นถึงวิธีปฏิบัติด้านความมั่นคงของผู้ให้บริการคลาวด์ ในการให้คะแนนของหลักฐานเพื่อความโปร่งใสและตรวจสอบได้ งานวิจัยได้ออกแบบให้มีผู้ตรวจสอบความมั่นคงของคลาวด์เป็นผู้วิเคราะห์และให้คะแนนหลักฐานความมั่นคงของผู้ให้บริการคลาวด์ ทำให้การทำงานของระบบที่ออกแบบยังไม่เป็นอัตโนมัติ

2.2.7 งานวิจัยของ Lance Hayden และ Ken Stavinoha [14] นำเสนอแนวคิดสำหรับสถาปัตยกรรมความมั่นคงของคลาวด์และวิธีการประยุกต์เพื่อวัดผลความมั่นคงของคลาวด์ โดยกล่าวถึงแนวคิดการวัดความมั่นคงของคลาวด์ที่เสนอโดยสถาบันมาตรฐานและเทคโนโลยีระดับชาติ (NIST) ซึ่งแสดงความเชื่อมโยงระหว่าง 1) แผน (Plan) ซึ่งแสดงความคาดหวังในการทำงาน 2) ตัววัด (Metric) ซึ่งแสดงตัววัดที่ใช้ควบคุมการทำงานให้เป็นไปตามแผน และ 3) มาตรวัด (Measure) ซึ่งแสดงค่าที่วัดได้โดยตรงจากการทำงานและจะสะท้อนถึงค่าตัววัดที่ใช้ แนวคิดนี้คล้ายกับวิธีจีคิวเอ็ม (Goal Question Metric) ซึ่งใช้ในการวัดคุณภาพในทางวิศวกรรมซอฟต์แวร์ งานวิจัยนี้ได้เสนอตัวอย่างนิยามของตัววัดความมั่นคงซึ่งเกี่ยวข้องกับการวัดปริมาณหรือระดับของความใส่ใจ การลงทุน การถูกตรวจสอบ และการทำตามมาตรฐานด้านความมั่นคง แต่ยังเป็นเพียงแนวคิดและไม่ได้อิงตามมาตรฐานความมั่นคงของคลาวด์ของซีเอสเอ

งานวิจัยด้านการประเมินความมั่นคงของผู้ให้บริการคลาวด์สามารถสรุปได้ดังตารางที่ 2.3

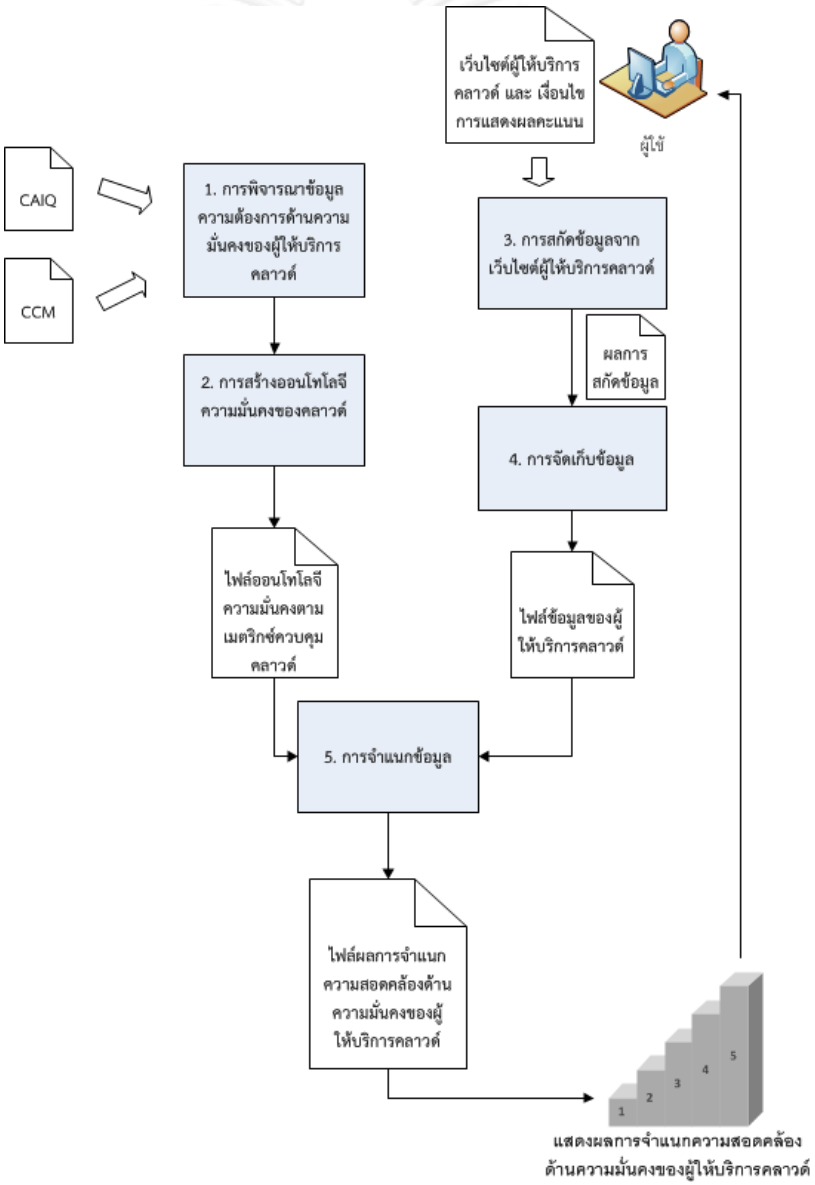
ตารางที่ 2.3 สรุปงานวิจัยด้านการประเมินความมั่นคงของผู้ให้บริการคลาวด์

ผู้วิจัย	ประเด็นในงานวิจัย	แนวคิดของงานวิจัย	ปัญหาของงานวิจัย
Wayne A. Pauley	การประเมินความโปร่งใสของผู้ให้บริการคลาวด์ด้านความมั่นคง ความเป็นส่วนตัว ความสามารถในการตรวจสอบได้ และข้อตกลงในการให้บริการ	บัตรคะแนน (Scorecard) โดยประเมินจากข้อมูลบนเว็บไซต์ของผู้ให้บริการคลาวด์	อาศัยคนในการประเมิน
Burton S.Kaliski Jr. และ Wayne Pauley	1. ความท้าทายในการประเมินการให้บริการคลาวด์ 2. แนวคิดในการประเมินแบบทันทีทันใด	Risk Assessment as a Service	เป็นเพียงแนวคิด ยังไม่มีวิธีการประเมิน
Bret Michael, Sun Microsystems, Inc., Catherine Everett, David Tancock และ คณะ	การประเมินความโปร่งใสของการให้บริการคลาวด์	หลักการพิจารณาความโปร่งใส	เป็นเพียงแนวคิด ยังไม่มีวิธีการประเมิน
Nuntapun Bhensook และ Twittie Senivongse	การประยุกต์จีคิวเอ็มมาใช้ในการกำหนดหลักฐานเพื่อคำนวณคะแนนการปฏิบัติด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์	การประเมินด้านความมั่นคงโดยมีการให้คะแนนหลักฐาน ซึ่งพิจารณาจากคุณภาพและปริมาณของหลักฐาน	การประเมินยังไม่เป็นอัตโนมัติ ยังต้องอาศัยผู้ตรวจสอบในการพิจารณาว่าผู้ให้บริการคลาวด์ดำเนินตามเมตริกซ์ควบคุมคลาวด์ในด้านใดโดยดูจากหลักฐานที่ได้จากผู้ให้บริการ
Lance Hayden และ Ken Stavinoha	สถาปัตยกรรมความมั่นคงของคลาวด์และวิธีการประยุกต์เพื่อวัดผลความมั่นคงของคลาวด์ตามแนวคิดที่เสนอโดยสถาบันมาตรฐานและเทคโนโลยีระดับชาติ (NIST)	การวัดโดยกำหนดแผน ตัววัด มาตรวัด พร้อมตัวอย่างนิยามของตัววัด	เป็นเพียงแนวคิดของวิธีการ ยังไม่มีตัววัดที่ชัดเจน

โดยสรุปจากงานวิจัย แม้ว่าจะสามารถประเมินความมั่นคงของผู้ให้บริการคลาวด์ได้แต่งานวิจัยส่วนใหญ่ยังเป็นการประเมินจากการทำแบบสอบถามเพื่อวัดว่าผู้ให้บริการคลาวด์นั้นมีนโยบาย หรือข้อตกลงทางด้านความมั่นคงอย่างไรบ้าง ซึ่งกระบวนการดังกล่าวอาศัยคนในการควบคุม และ ประเมินผลทำให้เกิดความล่าช้าเนื่องจากข้อมูลทางด้านความมั่นคงมีจำนวนมาก และ ผู้ให้บริการคลาวด์ก็มีจำนวนมาก บางงานวิจัยก็เป็นเพียงแนวคิด ยังไม่มีตัววัดหรือเครื่องมือสนับสนุนที่จะสามารถนำมาประเมินผู้ให้บริการคลาวด์

บทที่ 3
การจำแนกความสอดคล้องด้านความมั่นคงกับเมตริกซ์ควบคุมคลาวด์

ภาพที่ 3.1แสดงภาพรวมของงานวิจัยนี้ ซึ่งตั้งอยู่บนพื้นฐานของความคิดที่ว่า ทำอย่างไรผู้ใช้บริการคลาวด์จะสามารถประเมินผู้ให้บริการคลาวด์ในแง่ของความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคง เพื่อนำมาซึ่งการตัดสินใจเลือกใช้บริการ สำหรับการให้บริการคลาวด์ ความมั่นคงของผู้ให้บริการเป็นปัจจัยที่สำคัญซึ่งนำมาซึ่งความเชื่อถือได้ของผู้ให้บริการ ผู้ใช้บริการคลาวด์จำเป็นต้องตรวจสอบและประเมินความมั่นคงเบื้องต้นของผู้ให้บริการคลาวด์ก่อนตัดสินใจเลือกใช้บริการคลาวด์



ภาพที่ 3.1 แนวคิดของงานวิจัย

งานวิจัยนี้จึงมีวัตถุประสงค์เพื่อนำเสนอวิธีการประเมินคะแนนความมั่นคงของผู้ให้บริการคลาวด์ด้วยวิธีการจำแนกความสอดคล้องด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ด้วยการจำแนกข้อความอย่างง่าย โดยนำข้อมูลความมั่นคงจากหน้าเว็บผู้ให้บริการคลาวด์มาจำแนก ขั้นตอนการดำเนินงานมีดังนี้

3.1 การพิจารณาข้อมูลความต้องการด้านความมั่นคงของผู้ให้บริการคลาวด์

ในขั้นตอนนี้จะเป็นการพิจารณาข้อมูลความต้องการด้านความมั่นคงเพื่อที่จะนำคำศัพท์ไปสร้างออนโทโลจีข้อมูลความมั่นคง โดยพิจารณาจากเอกสารเมตริกซ์ควบคุมคลาวด์เป็นหลักรวมถึงเอกสารมาตรฐานต่างๆที่เอกสารเมตริกซ์ควบคุมคลาวด์อ้างอิงถึง และอาจเสริมด้วยคำศัพท์ที่อยู่ในแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน

3.1.1 เมตริกซ์ควบคุมคลาวด์ [1] ครอบคลุมแนวปฏิบัติด้านความมั่นคง และระบุว่าแนวปฏิบัตินั้นเกี่ยวข้องกับการให้บริการคลาวด์ในลักษณะใดบ้าง ดังตัวอย่างในตารางที่ 3.1

ตารางที่ 3.1 ตัวอย่างเมตริกซ์ควบคุมคลาวด์

Control Domain	CCM V3.0 Control ID	Control Specification	CCM V1.X	COBIT 4.1	CSA Guidance V3.0	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	NERC CIP	NIST SP800-53 R3	PCI DSS v2.0
Application & Interface Security *Application Security*	AIS-01	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	SA-04	AI2.4	Domain 10	1.2.6	45 CFR 164.312(e)(2)(i)	A.11.5.6 A.11.6.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.2 A.12.5.4 A.12.5.5 A.12.6.1 A.15.2.1	CIP-007-3 - R5.1	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	6.5

ตารางที่ 3.1 ตัวอย่างเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain	CCM V3.0 Control ID	Control Specification	CCM V1.X	COBIT 4.1	CSA Guidance V3.0	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	NERC CIP	NIST SP800-53 R3	PCI DSS v2.0
Application & Interface Security *Customer Access Requirements*	AIS-02	Prior to granting customers access to data, assets, and information systems, all identified security, contractual, and regulatory requirements for customer access shall be addressed and remediated.	SA-01		Domain 10	1.2.2 1.2.6 6.2.1 6.2.2		A.6.2.1 A.6.2.2 A.11.1.1		CA-1 CA-2 CA-5 CA-6	

3.1.2 มาตรฐานที่เมตริกซ์ควบคุมคลาวด์อ้างอิงถึงได้แก่ AICPA TS Map, AICPA Trust Service Criteria (SOC 2SM Report), BITS Shared Assessments AUP v5.0, BITS Shared Assessments SIG v6.0, BSI Germany, CCM V1.X, COBIT 4.1, CSA Enterprise Architecture / Trust Cloud Initiative, CSA Guidance V3.0, ENISA IAF, FedRAMP Security Controls (Final Release, Jan 2012) LOW IMPACT LEVEL, FedRAMP Security Controls (Final Release, Jan 2012) MODERATE IMPACT LEVEL, GAPP (Aug 2009), HIPAA / HITECH Act, ISO/IEC 27001-2005, Jericho Forum, NERC CIP, NIST SP800-53 R3, NZISM และ PCI DSS v2.0 ดังตัวอย่างในตารางที่ 3.2

ตารางที่ 3.2 ตัวอย่างมาตรฐาน ISO/IEC 27001-2005

ISO 27001-2005 ISMS Requirements	Yes	No	Partial	N.A.
4 Information Security Mgmt System 4.1 General Requirements For ISMS Is the documented Information Security Mgmt System (ISMS) established, implemented, operated, monitored, reviewed, maintained and improved? Does it address the · Overall business activities? · The risks that it faces? Remarks (if any):				

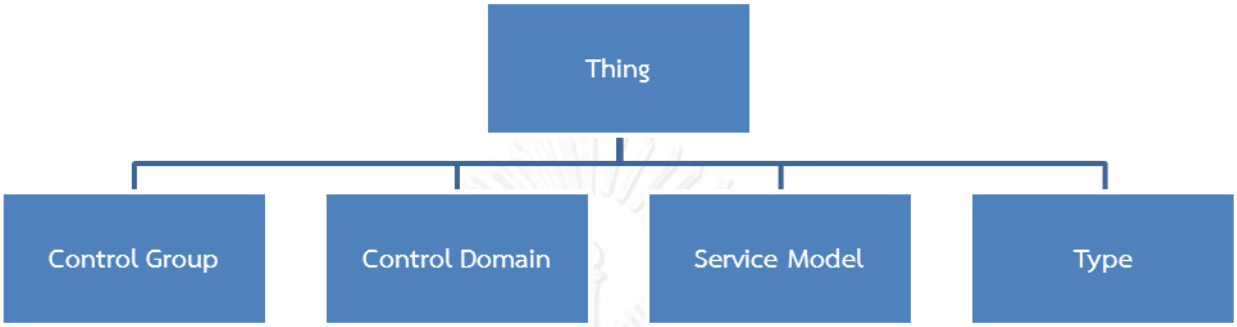
3.1.3 แบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน [2] เป็นรายการคำถามสำหรับตรวจสอบว่ามีการปฏิบัติตามแนวปฏิบัติในเมตริกซ์ควบคุมคลาวด์หรือไม่ ดังตัวอย่างในตารางที่ 3.3

ตารางที่ 3.3 ตัวอย่างแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน

Control Domain	CGID	CID	Control Specification	Consensus Assessment Questions
Application Security	AIS-01	AIS-01.1	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you utilize 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 utilize an automated source-code analysis tool to detect code security defects prior to production?
		AIS-01.3		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?
		AIS-01.4		Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?

3.2 การสร้างออนโทโลจีความมั่นคงของคลาวด์

จากการพิจารณาข้อมูลด้านความมั่นคงของคลาวด์ดังข้างต้น ผู้วิจัยจะนำคำศัพท์ที่ระบุอยู่ในความมั่นคงด้านต่าง ๆ มาสร้างออนโทโลจี โดยมีโครงสร้างดังภาพที่ 3.2 และคำอธิบายในตารางที่ 3.3



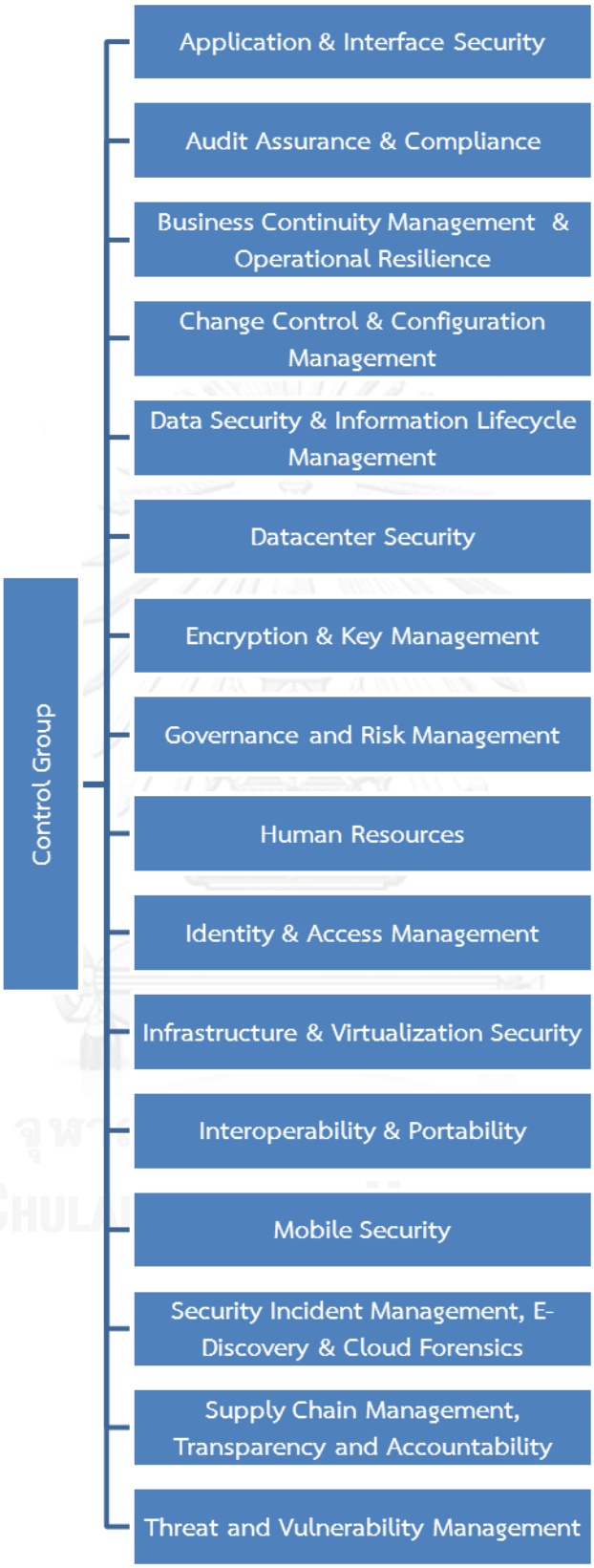
ภาพที่ 3.2 โครงสร้างออนโทโลจีความมั่นคงของคลาวด์

ตารางที่ 3.4 ความหมายของโครงสร้างออนโทโลจีความมั่นคงของคลาวด์

คำศัพท์	ความหมาย
Thing	คำศัพท์ที่จะนำมาสร้างออนโทโลจี
Control Group	แนวปฏิบัติด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์
Control Domain	หมวดย่อยของแนวปฏิบัติด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ซึ่งเป็นเป้าหมายการควบคุมความมั่นคง
Service Model	แนวปฏิบัติเกี่ยวข้องกับการให้บริการคลาวด์ในลักษณะใด
Type	ประเภทของคำ (Activity, Product, Related Concept)

3.2.1 กำหนดแนวปฏิบัติด้านความมั่นคงของคลาวด์

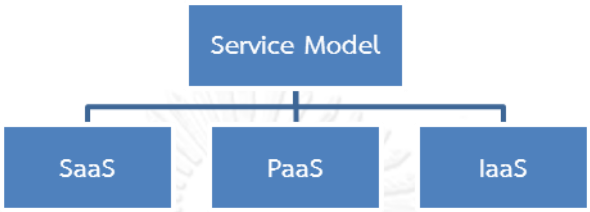
ภาพที่ 3.3 แสดงคำศัพท์ที่เป็นแนวปฏิบัติด้านความมั่นคงของคลาวด์ (Control Group) ซึ่งมีทั้งหมด 16 ด้าน ในแต่ละด้านจะประกอบด้วยคำศัพท์ซึ่งแสดงหมวดย่อยของแนวปฏิบัติด้านนั้น (Control Domain) ผู้วิจัยจะวิเคราะห์คำศัพท์ต่าง ๆ ที่อยู่ในแต่ละด้านในการสร้างออนโทโลจี



ภาพที่ 3.3 แนวปฏิบัติด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์

3.2.2 กำหนดลักษณะของการให้บริการคลาวด์

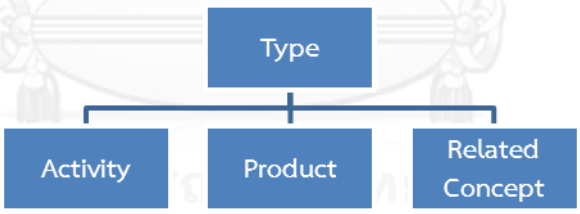
ภาพที่ 3.4 แสดงลักษณะการให้บริการคลาวด์ (Service Model) ซึ่งแนวปฏิบัติด้านความมั่นคงมีความเกี่ยวข้อง แบ่งเป็น 3 ลักษณะได้แก่ 1) การให้บริการซอฟต์แวร์ (SaaS) 2) การให้บริการแพลตฟอร์ม (PaaS) 3) การให้บริการโครงสร้างพื้นฐาน (IaaS)



ภาพที่ 3.4 ลักษณะของการให้บริการคลาวด์

3.2.3 กำหนดประเภทของคำ

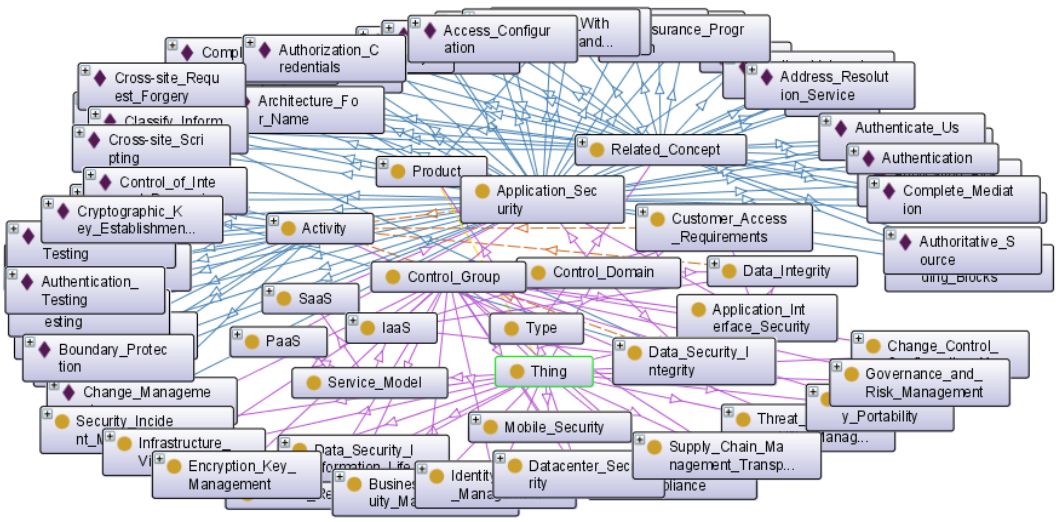
ภาพที่ 3.5 แสดงประเภทของคำศัพท์ที่อยู่ภายใต้แนวปฏิบัติแต่ละด้านซึ่งสามารถแบ่งประเภทได้เป็น 3 ประเภทได้แก่ 1) กิจกรรม (Activity) หมายถึงกิจกรรมที่แนวปฏิบัติด้านนั้นระบุให้กระทำ 2) ผลิตภัณฑ์ (Product) หมายถึงสิ่งที่เป็นผลผลิตจากการดำเนินการตามแนวปฏิบัติด้านนั้น และ 3) คอนเซปต์ที่เกี่ยวข้อง (Related Concept) หมายถึงแนวคิดหรือหลักการที่แนวปฏิบัติด้านนั้นกล่าวถึง แต่ไม่ได้เป็นกิจกรรมและผลิตภัณฑ์



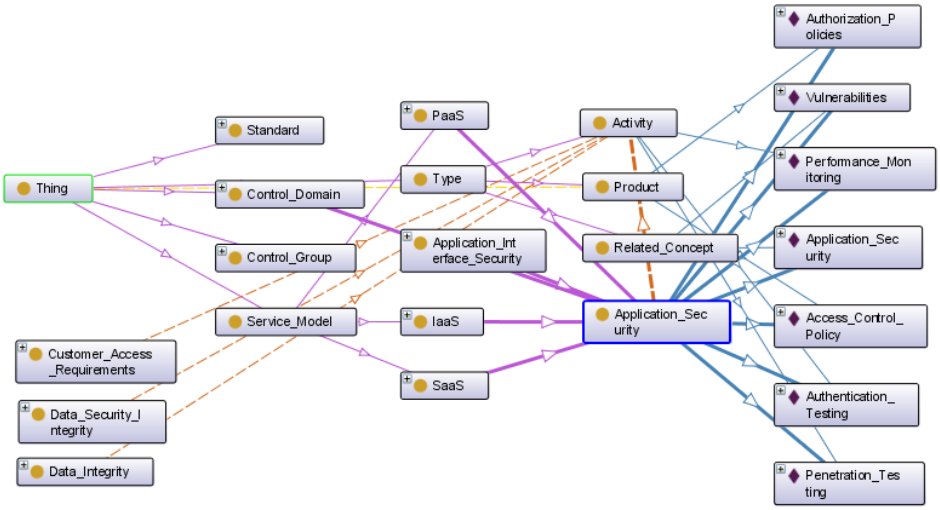
ภาพที่ 3.5 ประเภทของคำ

3.2.4 ตัวอย่างออนโทโลจี

ตัวอย่างภาพรวมของออนโทโลจีความมั่นคงของคลาวด์แสดงในภาพที่ 3.6 ซึ่งประกอบด้วยคำศัพท์ที่เกี่ยวกับ Control Group, Control Domain และ Type ประเภทต่าง ๆ รวม 461 คำ ภาพที่ 3.7 แสดงตัวอย่างบางส่วนของคำศัพท์ที่เกี่ยวกับ Application Security Control Domain ใน Application & Interface Security Control Group สำหรับคำศัพท์ในออนโทโลจีทั้งหมดแสดงไว้ในภาคผนวก ก



ภาพที่ 3.6 ภาพรวมของออนโทโลจีความมั่นคงของคลาวด์



ภาพที่ 3.7 บางส่วนของคำศัพท์ที่เกี่ยวกับ Application Security Control Domain

3.3 การสกัดข้อมูลจากเว็บไซต์ผู้ให้บริการคลาวด์

การเก็บข้อมูลด้านความมั่นคงของผู้ให้บริการคลาวด์จากเว็บไซต์ จะทำการดาวน์โหลดข้อมูลมาเก็บในรูปแบบไฟล์ HTML แล้วจึงนำมาประมวลผลเพื่อหาคำสำคัญ ในการดาวน์โหลดจะใช้เครื่องมือ HTTrack Website Copier [15] โดยเลือกเก็บเฉพาะข้อมูลที่เป็น HTML ไม่มีการเก็บข้อมูลภาพ เสียง และ ไฟล์แนบอื่น ๆ ดังภาพที่ 3.8

```
<p>Amazon Web Services strives to provide a robust and trustworthy platform for our customers. '
our services for suspected attack. We also understand that security is a partnership between us
application deployment involves testing applications for potential vulnerabilities.</p>

<p>Our <a href="http://aws.amazon.com/aup">Acceptable Use Policy</a> describes permitted and pr
prohibited security violations and network abuse. However, because penetration testing frequent
established a policy for customers to request permission to conduct penetration tests.</p>

<h2>Communicating with AWS</h2>

<h3>Appropriate Use and Your Privacy</h3>

<p>The information you share with AWS as part of this process is kept confidential within AWS.
permission.</p>
```

ภาพที่ 3.8 รูปแบบข้อมูลที่ได้จากการเก็บข้อมูลด้วยเครื่องมือ HTTrack Website Copier

3.4 การจัดเก็บข้อมูล

หลังจากทำการสกัดข้อมูลจากหน้าเว็บแล้ว ระบบจะทำการสร้างดัชนีคำสำคัญโดยใช้ไลบรารีของ The Stanford Natural Language Processing Group [16] ในการตัดคำ กำจัดคำหยุด และหารากศัพท์ คำรากศัพท์ (lemma) จะถูกนำไปเปรียบเทียบกับคำในออนโทโลจี ซึ่งจะถูกประมวลผลโดยการตัดคำ กำจัดคำหยุด และหารากศัพท์ เช่นเดียวกัน แล้วจัดเก็บคำในหน้าเว็บเฉพาะที่ตรงกับคำในออนโทโลจี โดยเก็บอยู่ในรูปแบบของเอกซ์เอ็มแอล (XML) ดังภาพที่ 3.9 ก่อนนำไปดำเนินการจำแนกในขั้นต่อไป ตัวอย่างคำศัพท์ที่สกัดได้จากหน้าเว็บแสดงไว้ในภาคผนวก ข

```
<token id="2">
  <word>vulnerabilities</word>
  <lemma>vulnerability</lemma>
  <CharacterOffsetBegin>10</CharacterOffsetBegin>
  <CharacterOffsetEnd>25</CharacterOffsetEnd>
  <POS>NNS</POS>
  <NER>O</NER>
</token>
```

ภาพที่ 3.9 ตัวอย่างการเก็บข้อมูลในรูปแบบเอกซ์เอ็มแอล

3.5 การจำแนกข้อมูล

ในขั้นตอนนี้จะนำคำสำคัญที่ได้จากหน้าเว็บผู้ให้บริการคลาวด์มาทำการจำแนกตามกลุ่มข้อมูลแนวปฏิบัติด้านความมั่นคงทั้ง 16 ด้านโดยใช้การจำแนกข้อความอย่างง่ายที่อธิบายไว้ในหัวข้อที่ 2.1.5 โดยนำออนโทโลจีที่สร้างในขั้นต้นมาใช้ในการพิจารณาคำสำคัญที่ได้จากหน้าเว็บของผู้

ให้บริการว่า สอดคล้องกับคำศัพท์ในหมวดใดบ้างของออนโทโลจี ตัวอย่างการคำนวณเพื่อจำแนกความสอดคล้องต่อความมั่นคงด้าน Application & Interface Security มีดังต่อไปนี้

1) ตัวอย่างข้อมูลความถี่ของคำศัพท์ที่พบในเอกสารความมั่นคงด้าน Application & Interface Security และเอกสารผู้ให้บริการคลาวด์ Amazon แสดงในตารางที่ 3.5 โดยที่

$f_{i,1}$ คือ ตัวแทนเอกสารความมั่นคงหมวดย่อย Application Security

$f_{i,2}$ คือ ตัวแทนเอกสารความมั่นคงหมวดย่อย Customer Access Requirements

$f_{i,3}$ คือ ตัวแทนเอกสารความมั่นคงหมวดย่อย Data Integrity

$f_{i,4}$ คือ ตัวแทนเอกสารความมั่นคงหมวดย่อย Data Security / Integrity

$f_{i,p}$ คือ ตัวแทนเอกสารผู้ให้บริการคลาวด์ Amazon

ตารางที่ 3.5 ตารางข้อมูลความถี่ของคำศัพท์ที่พบในเอกสารความมั่นคงด้าน Application & Interface Security และผู้ให้บริการคลาวด์ Amazon

คำศัพท์	$f_{i,1}$	$f_{i,2}$	$f_{i,3}$	$f_{i,4}$	$f_{i,p}$
Application Security	1	0	0	0	1
Security Authorization	0	1	0	0	1
Penetration Testing	1	1	1	1	1
Performance Monitoring	1	1	1	1	0
Vulnerabilities	1	0	0	0	1

2) ตัวอย่างการคำนวณน้ำหนักของคำตามสมการที่ 2.3 แสดงในตารางที่ 3.6 โดยที่

$w_{i,1}$ คือ น้ำหนักของคำในเอกสารความมั่นคงหมวดย่อย Application Security

$w_{i,2}$ คือ น้ำหนักของคำในเอกสารความมั่นคงหมวดย่อย Customer Access Requirements

$w_{i,3}$ คือ น้ำหนักของคำในเอกสารความมั่นคงหมวดย่อย Data Integrity

$w_{i,4}$ คือ น้ำหนักของคำในเอกสารความมั่นคงหมวดย่อย Data Security / Integrity

$w_{i,p}$ คือ น้ำหนักของคำในเอกสารผู้ให้บริการคลาวด์ Amazon

ค่า N ในที่นี้เป็น 4 ตามจำนวนหมวดย่อยของความมั่นคงด้าน Application & Interface Security

ตารางที่ 3.6 ตารางน้ำหนักของคำศัพท์ที่พบในเอกสารความมั่นคงด้าน Application & Interface Security และผู้ให้บริการคลาวด์ Amazon

คำศัพท์	$w_{i,1}$	$w_{i,2}$	$w_{i,3}$	$w_{i,4}$	$w_{i,p}$
Application Security	$(1+\log_2 1)\times\log_2 \frac{4}{1}=2$	0	0	0	2
Security Authorization	0	2	0	0	2
Penetration Testing	0	0	0	0	0
Performance Monitoring	0	0	0	0	0
Vulnerabilities	2	0	0	0	2

3) ตัวอย่างการคำนวณค่าความสอดคล้องดังสมการที่ 2.6 แสดงในตารางที่ 3.7 โดยที่

$sim(d_{1,p})$ คือ ค่าความสอดคล้องของเอกสารความมั่นคงหมวดย่อย Application Security กับเอกสารผู้ให้บริการคลาวด์ Amazon

$sim(d_{2,p})$ คือ ค่าความสอดคล้องของเอกสารความมั่นคงหมวด Customer Access Requirements กับเอกสารผู้ให้บริการคลาวด์ Amazon

$sim(d_{3,p})$ คือ ค่าความสอดคล้องของเอกสารความมั่นคงหมวดย่อย Data Integrity กับเอกสารผู้ให้บริการคลาวด์ Amazon

$sim(d_{4,p})$ คือ ค่าความสอดคล้องของเอกสารความมั่นคงหมวดย่อย Data Security / Integrity กับเอกสารผู้ให้บริการคลาวด์ Amazon

ตารางที่ 3.7 ตารางผลการประเมินความสอดคล้องกับความมั่นคงด้าน Application & Interface Security ของผู้ให้บริการคลาวด์ Amazon

ความมั่นคงหมวดย่อย	การคำนวณ	คะแนน
$sim(d_{1,p})$	$(8)/\left(\sqrt{8}\times\sqrt{12}\right)$	0.82
$sim(d_{2,p})$	$\left(\sum_{i=1}^{n} w_{i,2}\times w_{i,p}\right)/\left(\sqrt{\sum_{i=1}^{n} w_{i,2}^2}\times\sqrt{\sum_{i=1}^{n} w_{i,p}^2}\right)$	0.58
$sim(d_{3,p})$	$\left(\sum_{i=1}^{n} w_{i,3}\times w_{i,p}\right)/\left(\sqrt{\sum_{i=1}^{n} w_{i,3}^2}\times\sqrt{\sum_{i=1}^{n} w_{i,p}^2}\right)$	0

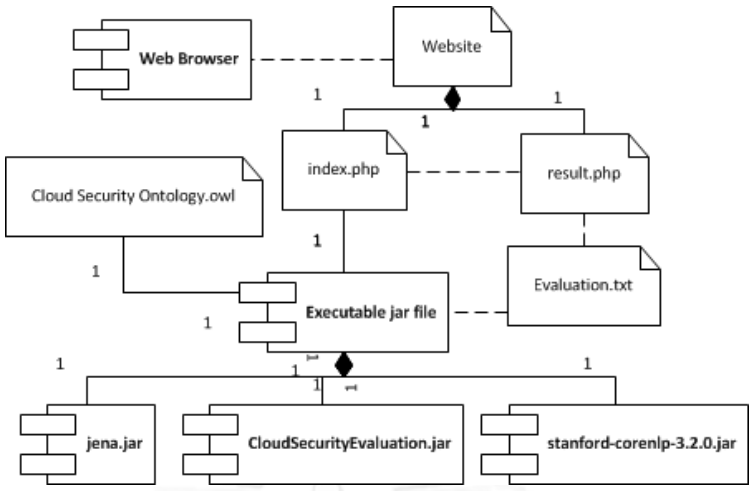
ตารางที่ 3.7 ตารางผลการประเมินความสอดคล้องกับความมั่นคงด้าน Application & Interface Security ของผู้ให้บริการคลาวด์ Amazon (ต่อ)

ความมั่นคงหมวดย่อย	การคำนวณ	คะแนน
$sim(d_{4,p})$	$\left(\sum_{i=1}^{n} w_{i,4} \times w_{i,p}\right) / \left(\sqrt{\sum_{i=1}^{n} w_{i,4}^2} \times \sqrt{\sum_{i=1}^{n} w_{i,p}^2}\right)$	0

จากคะแนนที่ได้ทำให้สามารถทราบเบื้องต้นจากข้อมูลบนหน้าเว็บว่า ผู้ให้บริการคลาวด์ได้เปิดเผยการดำเนินการที่สอดคล้องกับแนวปฏิบัติด้านต่าง ๆ ในเมตริกซ์ควบคุมคลาวด์หรือไม่ และความสอดคล้องที่มี อยู่ในระดับใด จากตัวอย่างข้างต้นพบว่า ผู้ให้บริการคลาวด์ Amazon มีการเปิดเผยข้อมูลการให้บริการที่สอดคล้องกับความมั่นคงด้าน Application & Interface Security ในหมวดย่อย Application Security มากที่สุด ตามด้วยหมวดย่อย Customer Access Requirements แต่ยังไม่แสดงข้อมูลการทำตามหมวดย่อย Data Integrity และ Data Security / Integrity

3.6 การพัฒนาเครื่องมือจำแนกความสอดคล้องด้านความมั่นคง

แนวคิดในการพัฒนาเครื่องมือจำแนกความสอดคล้องด้านความมั่นคงเพื่อสนับสนุนงานวิจัย คือ การพัฒนาเว็บแอปพลิเคชันสำหรับรับข้อมูลผู้ให้บริการคลาวด์มาประมวลผล ทำการจำแนก และแสดงคะแนนความสอดคล้องของผู้ให้บริการคลาวด์ต่อเมตริกซ์ควบคุมคลาวด์ แผนภาพคอมโพเนนต์ (Component Diagram) ของเว็บแอปพลิเคชันแสดงดังภาพที่ 3.10 และคำอธิบายในตารางที่ 3.8 ซึ่งมีโครงสร้างการทำงานเป็นดังภาพที่ 3.11 ส่วนตัวอย่างหน้าจอของเว็บแอปพลิเคชันประกอบด้วยตัวอย่างหน้าจอหลักที่ใช้สำหรับการอัปโหลดไฟล์และเลือกเงื่อนไขต่างๆ แสดงในภาพที่ 3.12 หน้าจอแสดงผลการเปรียบเทียบความสอดคล้องด้านความมั่นคงระหว่างผู้ให้บริการคลาวด์แต่ละรายในรูปแบบกราฟแท่งและตารางคะแนน ในภาพที่ 3.13 และ หน้าจอแสดงผลความสอดคล้องด้านความมั่นคงของผู้ให้บริการคลาวด์แต่ละรายในรูปแบบกราฟวงกลมและตารางคะแนน ในภาพที่ 3.14 โดยมีคำอธิบายหน้าจอแสดงไว้ในตารางที่ 3.9 – 3.11 ตามลำดับ

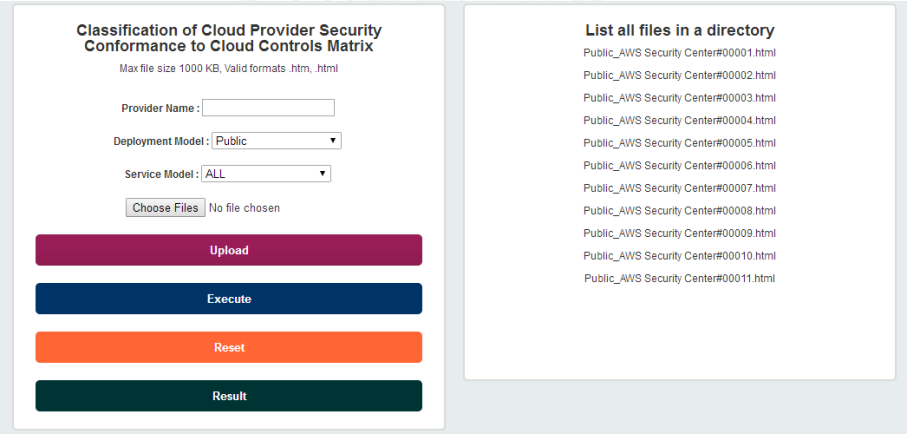


ภาพที่ 3.10 แผนภาพคอมโพเนนต์ของเครื่องมือจำแนกความสอดคล้องด้านความมั่นคง

ตารางที่ 3.8 คำอธิบายแผนภาพคอมโพเนนต์ของเครื่องมือจำแนกความสอดคล้องด้านความมั่นคง

หัวข้อ	คำอธิบาย
Web Browser	โปรแกรมที่ใช้ดูข้อมูลที่อยู่ในเว็บไซต์
Website	เป็นส่วนที่ใช้ติดต่อกับผู้ใช้งานซึ่งประกอบไปด้วยไฟล์ index.php ใช้แสดงหน้าจอหลัก และ Result.php แสดงหน้าจอผลการประเมิน
Executable jar File	เป็นส่วนประมวลผลของระบบซึ่งประกอบไปด้วยไฟล์ดังต่อไปนี้ 1.standford-corenlp-3.2.0.jar ทำหน้าที่ในการประมวลผลคำศัพท์จากหน้าเว็บผู้ให้บริการคลาวด์ และคำศัพท์จากออนโทโลจี 2.jena.jar เป็นขอบข่ายงาน (Framework) ในการติดต่อและจัดการออนโทโลจี 3.CloudSecurity Evaluation.jar เป็นตัวหลักที่ใช้ในการประมวลผล โดยทำหน้าที่อ่านไฟล์ที่ได้รับจากผู้ใช้บริการ เรียกใช้งานไลบราลีและเขียนไฟล์ผลการประเมิน 4.Cloud Security Ontology.owl คือ ไฟล์ออนโทโลจีความมั่นคงของคลาวด์ โดยเมื่อทำการประมวลผลเสร็จจะได้ไฟล์ผลการประเมินคือ Evaluation.txt

ภาพที่ 3.11 โครงสร้างการทำงานของเว็บแอปพลิเคชัน



ภาพที่ 3.12 หน้าจอหลักใช้สำหรับการอัปโหลดไฟล์และเลือกเงื่อนไขต่างๆ

ตารางที่ 3.9 คำอธิบายหน้าจอหลักใช้สำหรับการอัปโหลดไฟล์และเลือกเงื่อนไขต่างๆ

หัวข้อ	คำอธิบาย
Provider Name	ผู้ใช้ระบุชื่อผู้ให้บริการคลาวด์ ซึ่งจะถูกนำไปใช้ในการตั้งชื่อไฟล์ผลลัพธ์ด้วย
Deployment Model	ผู้ใช้ระบุรูปแบบการใช้งานคลาวด์ที่สนใจ ซึ่งประกอบไปด้วย Public, Private, Community และ Hybrid
Service Model	ผู้ใช้ระบุลักษณะการให้บริการที่สนใจ ซึ่งประกอบไปด้วย ALL, SaaS, PaaS, IaaS ในกรณีที่ไม่ต้องการระบุลักษณะการให้บริการ ให้เลือก ALL ซึ่งในการเลือกลักษณะการให้บริการจะมีผลต่อการประเมินผล

ตารางที่ 3.9 คำอธิบายหน้าจอหลักใช้สำหรับการอัปโหลดไฟล์และเลือกเงื่อนไขต่างๆ (ต่อ)

หัวข้อ	คำอธิบาย
Choose Files	ผู้ใช้เลือกไฟล์ที่ต้องการอัปโหลดซึ่งเป็นไฟล์ที่ผู้ใช้บันทึกมาจากหน้าเว็บของผู้ให้บริการคลาวด์ โดยสามารถเลือกได้มากกว่าหนึ่งไฟล์ ขนาดของไฟล์จะต้องไม่เกิน 1000KB และเป็นไฟล์ .htm หรือ .html เท่านั้น
Upload	หลังจากเลือกไฟล์แล้ว ผู้ใช้จะต้องกดปุ่ม Upload เพื่อทำการอัปโหลดไฟล์ โดยจะตรวจสอบว่ามีการระบุชื่อผู้ให้บริการคลาวด์แล้ว
Execute	หลังจากอัปโหลดไฟล์เรียบร้อยแล้ว กดปุ่ม Execute ระบบจะทำการประมวลผลคำศัพท์จากไฟล์ผู้ให้บริการทั้งหมดและนำคำศัพท์ที่ได้ไปเทียบกับคำศัพท์ในออนโทโลจี
Reset	ใช้ลบไฟล์ที่อัปโหลดและไฟล์ที่ถูกประมวลผลแล้วทั้งหมด
Result	ใช้เพื่อดูผลลัพธ์ที่ได้จากการประมวลผล เมื่อคลิกแล้วหน้าจอจะเปลี่ยนไปดังภาพที่ 3.12
List all files in a directory	แสดงรายชื่อไฟล์ที่ถูกอัปโหลดทั้งหมด โดยโครงสร้างของชื่อไฟล์ประกอบไปด้วย รูปแบบการใช้งานผู้ให้บริการคลาวด์ตามด้วยชื่อผู้ให้บริการคลาวด์และหมายเลขเอกสารของผู้ให้บริการคลาวด์ซึ่งระบบจะสร้างขึ้นให้อัตโนมัติ

ภาพที่ 3.13 หน้าจอแสดงผลการเปรียบเทียบความสอดคล้องด้านความมั่นคงระหว่างผู้ให้บริการคลาวด์แต่ละรายในรูปแบบกราฟแท่งและตารางคะแนน

ตารางที่ 3.10 คำอธิบายหน้าจอแสดงผลของผู้ให้บริการคลาวด์แต่ละรายในรูปแบบกราฟแท่งและตารางคะแนน

หัวข้อ	คำอธิบาย
Home	คลิกเพื่อกลับสู่หน้าจอหลัก
Deployment Model	เป็นตัวกรองที่ใช้ในการกรองไฟล์ผลลัพธ์ทั้งหมดโดยมีให้เลือก 4 รายการคือ ALL, Public, Private, Community และ Hybrid กรณีที่เลือก ALL จะแสดงผลลัพธ์การเปรียบเทียบของผู้ให้บริการคลาวด์แต่ละรายในรูปแบบกราฟแท่งและตารางคะแนน
รายการไฟล์	รายการไฟล์ทั้งหมดที่ถูกแสดงเป็นผลการประเมินเปรียบเทียบผู้ให้บริการคลาวด์กับความมั่นคงทั้ง 16 ด้าน โดยภายในไฟล์ประกอบไปด้วยคะแนนประเมินความสอดคล้องตามแนวปฏิบัติด้านความมั่นคง
กราฟแท่ง	เพื่อให้เห็นความแตกต่างของคะแนนระหว่างผู้ให้บริการได้อย่างชัดเจน จึงแสดงในรูปแบบของกราฟแท่งโดยจะแสดงแยกสีตามผู้ให้บริการ
ตาราง	แสดงคะแนนที่คำนวณได้โดยจะมีค่าอยู่ระหว่าง [0-1]

ภาพที่ 3.14 หน้าจอแสดงผลความสอดคล้องด้านความมั่นคงของผู้ให้บริการคลาวด์แต่ละรายในรูปแบบกราฟวงกลมและตารางคะแนน

ตารางที่ 3.11 คำอธิบายหน้าจอแสดงผลของผู้ให้บริการคลาวด์แต่ละรายในรูปแบบกราฟวงกลมและตารางคะแนน

หัวข้อ	คำอธิบาย
Home	คลิกเพื่อกลับสู่หน้าจอหลัก
Deployment Model	เป็นตัวกรองที่ใช้ในการกรองไฟล์ผลลัพธ์ทั้งหมดโดยมีให้เลือก 4 รายการคือ ALL, Public, Private, Community และ Hybrid กรณีที่เลือก Public, Private, Community และ Hybrid จะแสดงผลลัพธ์การเปรียบเทียบของผู้ให้บริการคลาวด์แต่ละรายในรูปแบบกราฟวงกลมและตารางคะแนน
รายการไฟล์	รายการไฟล์ทั้งหมดที่ถูกแสดงเป็นผลการประเมินเปรียบเทียบผู้ให้บริการคลาวด์กับความมั่นคงทั้ง 16 ด้าน โดยภายในไฟล์ประกอบไปด้วยคะแนนประเมินความสอดคล้องตามแนวปฏิบัติด้านความมั่นคง
กราฟวงกลม	แสดงอัตราส่วนของคะแนนผลลัพธ์ที่ได้ว่ามีความสอดคล้องกับความมั่นคงด้านใดบ้างและเป็นกี่เปอร์เซ็นต์
ตาราง	แสดงคะแนนที่คำนวณได้โดยจะมีค่าอยู่ระหว่าง [0-1]

จากโครงสร้างของเว็บแอปพลิเคชันดังภาพที่ 3.11 เครื่องมือจะสามารถทำงานได้ดังต่อไปนี้

1) เลือกไฟล์เอชทีเอ็มแอลของผู้ให้บริการคลาวด์เพื่อนำมาสร้างคำสำคัญได้
2) ระบุลักษณะการให้บริการคลาวด์ว่าเป็น IaaS, PaaS หรือ SaaS เพื่อเป็นเงื่อนไขในการจำแนก เนื่องจากผู้ใช้อาจสนใจการให้บริการคลาวด์เฉพาะบางลักษณะ ซึ่งแนวปฏิบัติด้านความมั่นคงบางด้านจะกำหนดไว้สำหรับการให้บริการคลาวด์บางลักษณะเท่านั้น
3) ระบุลักษณะการใช้งานคลาวด์ว่าเป็น Private, Community, Public หรือ Hybrid เพื่อเป็นเงื่อนไขในการจำแนก เนื่องจากผู้ใช้อาจสนใจการใช้งานคลาวด์เฉพาะบางลักษณะ
4) ระบุแนวปฏิบัติด้านความมั่นคงแต่ละด้านที่ต้องการประเมินได้
5) แสดงผลการจำแนกความสอดคล้องด้านความมั่นคงในรูปแบบของตาราง กราฟวงกลม และกราฟแท่งได้

3.6.1 เครื่องมือที่ใช้ในการพัฒนา

- เอชทีเอ็มแอล จาวาสคริปต์ และ พีเอชพี เป็นภาษาที่ใช้ในการพัฒนาแอปพลิเคชันเพื่อการแสดงผล

- Java(TM) Platform Standard Edition Runtime Environment Version7 ใช้ในการพัฒนาและประมวลผลไฟล์เอกสารและออนโทโลจี โดยทำงานร่วมกับเอชทีเอ็มแอล จาวาสคริปต์ และ พีเอชพี
- Google Chart เป็นเครื่องมือในการสร้างตารางและกราฟวงกลม
- AppServ เวอร์ชัน 2.5.10 เป็นแอพพลิเคชันเซิร์ฟเวอร์

บทที่ 4

การทดสอบและการประเมินผลการวิจัย

ผู้วิจัยได้รวบรวมเว็บไซต์จากผู้ให้บริการคลาวด์ **5** รายเพื่อนำมาทดสอบและประเมินผล ได้แก่ Amazon [17], Google [18] , Salesforce [19], Box [20] และ Windows Azure [21] โดยมีรายละเอียด ดังนี้

1) ผู้ให้บริการคลาวด์ Amazon ให้บริการคลาวด์ทั้งด้าน Infrastructure as a Service เช่น Amazon EC2 [22] ซึ่งเป็นการให้บริการเกี่ยวกับ Virtual Computing Environment และ Platform as a Service เช่น Amazon RDS [23] ซึ่งเป็นการให้บริการเกี่ยวกับ Database Server โดย Amazon EC2 และ Amazon RDS จัดเป็นการใช้งานคลาวด์ทั้งแบบ Public และ Private
2) ผู้ให้บริการคลาวด์ Google ให้บริการคลาวด์ทั้งด้าน Platform as a Service เช่น Google Cloud Platform [24] และ Software as a Service เช่น Google Drive [25] ซึ่งเป็นการให้บริการเกี่ยวกับแอปพลิเคชันสำหรับจัดการเอกสาร โดย Google Cloud Platform และ Google Drive จัดเป็นการใช้งานคลาวด์แบบ Public
3) ผู้ให้บริการคลาวด์ SalesForce ให้บริการคลาวด์ทั้งด้าน Platform as a Service เช่น SalesForce Platform [26] และ Software as a Service เช่น CRM Sales app [27] โดย SalesForce Platform และ CRM Sales app จัดเป็นการใช้งานคลาวด์แบบ Public
4) ผู้ให้บริการคลาวด์ Box ให้บริการคลาวด์ทั้งด้าน Platform as a Service เช่น Box Online File Sharing [28] เป็นการให้บริการการใช้ไฟล์ร่วมกัน และ Software as a Service เช่น แอปพลิเคชัน Box for iPad and iPhone [29] จัดเป็นการใช้งานคลาวด์แบบ Public
5) ผู้ให้บริการคลาวด์ Windows Azure ให้บริการคลาวด์ทั้งด้าน Platform as a Service เช่น Azure Storage, Backup, and Recovery [30] ให้บริการด้านการจัดเก็บข้อมูล และ Software as a Service เช่น Push notifications to millions [31] ให้บริการทางด้านการแจ้งเตือน หรือ ประกาศไปยังโทรศัพท์มือถือทุกแพลตฟอร์ม จัดเป็นการใช้งานคลาวด์แบบ Public

การทดสอบจะเป็นการแสดงและเปรียบเทียบผลคะแนนความสอดคล้องกับเมตริกซ์ควบคุมคลาวด์ของผู้ให้บริการคลาวด์แต่ละราย การทดสอบประกอบด้วย

1) ทดสอบการแสดงผลคะแนนความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงของผู้ให้บริการคลาวด์แต่ละรายโดยไม่มีการระบุเงื่อนไขใด

2) ทดสอบการแสดงผลคะแนนความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงของผู้ให้บริการคลาวด์แต่ละรายโดยระบุความมั่นคงแต่ละด้าน
3) ทดสอบการระบุลักษณะการใช้งานคลาวด์เป็นเงื่อนไข
4) ทดสอบการระบุลักษณะการให้บริการคลาวด์เป็นเงื่อนไข
5) ทดสอบการแสดงผลการเปรียบเทียบคะแนนความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงของผู้ให้บริการแต่ละรายโดยไม่ระบุเงื่อนไข
6) ทดสอบการแสดงผลการเปรียบเทียบคะแนนความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงของผู้ให้บริการแต่ละรายโดยระบุความมั่นคงแต่ละด้าน

ส่วนการประเมินผลการจำแนก จะนำผลการทดสอบจากเครื่องมือมาเปรียบเทียบกับการจำแนกด้วยมือ โดยแบ่งการประเมินผลเป็น

1) ประเมินว่ามีการระบุถึงความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงด้านใดบ้างใน 16 ด้าน
2) ประเมินความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงในแต่ละด้านว่าอยู่ในระดับใด

รายละเอียดการทดสอบและการประเมินผลมีดังนี้

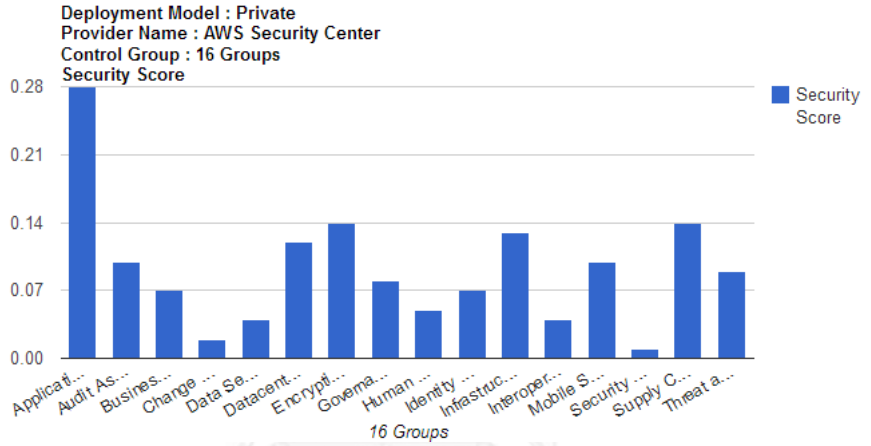
4.1 กรณีทดสอบการแสดงผลคะแนนความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงโดยไม่ระบุเงื่อนไข

Amazon, Google, SalesForce, Box และ Azure มีจำนวนหน้าเว็บที่พูดถึงความมั่นคงและนำมาใช้ทดสอบเป็นจำนวน 11, 1, 1, 2, 5 หน้า ตามลำดับ คะแนนการประเมินของความมั่นคงแต่ละด้าน (ทศนิยม 2 ตำแหน่ง) ของ Amazon, Google, SalesForce, Box และ Azure แสดงดังตารางที่ 4.1-4.5 ตามลำดับ

ระบบจะนำเสนอผลการประเมินคะแนนความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงของผู้ให้บริการคลาวด์แต่ละรายในรูปแบบของกราฟวงกลม เพื่อแสดงให้เห็นถึงอัตราส่วนของคะแนนแต่ละด้าน ดังตัวอย่างกราฟแสดงคะแนนความสอดคล้องในแต่ละด้านของผู้ให้บริการคลาวด์ Amazon ในภาพที่ 4.1 ซึ่งสามารถสรุปได้ว่า ความมั่นคงที่ผู้ให้บริการคลาวด์ Amazon แสดงไว้บนเว็บไซต์มีข้อมูลด้าน Application & Interface Security มากที่สุด รองลงมาเรียงจากมากไปน้อย คือ Supply Chain Management, Transparency, and Accountability, Encryption & Key Management, Infrastructure & Virtualization Security, Datacenter Security, Audit

Assurance & Compliance, Mobile Security, Threat and Vulnerability Management, Governance and Risk Management, Business Continuity Management & Operational Resilience, Identity & Access Management, Human Resources, Data Security & Information Lifecycle Management, Interoperability & Portability, Change Control & Configuration Management และ Security Incident Management, E-Discovery & Cloud Forensics ตามลำดับ

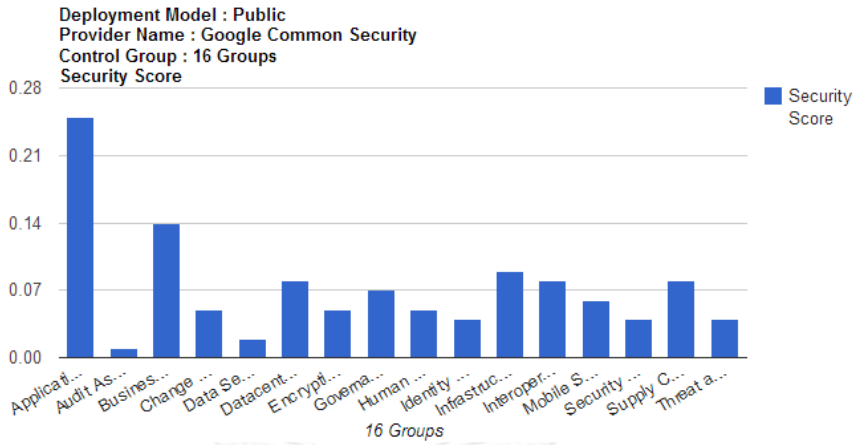
สำหรับกราฟแสดงคะแนนความสอดคล้องของ Google, SalesForce, Box และ Azure แสดงในภาพที่ 4.1-4.5 ตามลำดับ



ภาพที่ 4.1 กราฟแสดงเปอร์เซ็นต์ความสอดคล้องในแต่ละด้านของ Amazon

ตารางที่ 4.1 คะแนนความสอดคล้องในแต่ละด้านของ Amazon

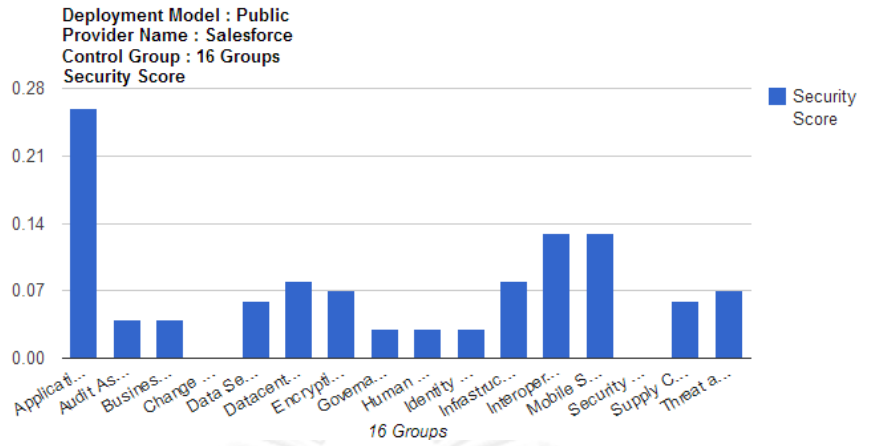
Control Group	Score
Application & Interface Security	0.28
Audit Assurance & Compliance	0.10
Business Continuity Management & Operational Resilience	0.07
Change Control & Configuration Management	0.02
Data Security & Information Lifecycle Management	0.04
Datacenter Security	0.12
Encryption & Key Management	0.14
Governance and Risk Management	0.08
Human Resources	0.05
Identity & Access Management	0.07
Infrastructure & Virtualization Security	0.13
Interoperability & Portability	0.04
Mobile Security	0.10
Security Incident Management, E-Discovery & Cloud Forensics	0.01
Supply Chain Management, Transparency and Accountability	0.14
Threat and Vulnerability Management	0.09



ภาพที่ 4.2 กราฟแสดงเปอร์เซ็นต์ความสอดคล้องในแต่ละด้านของ Google

ตารางที่ 4.2 คะแนนความสอดคล้องในแต่ละด้านของ Google

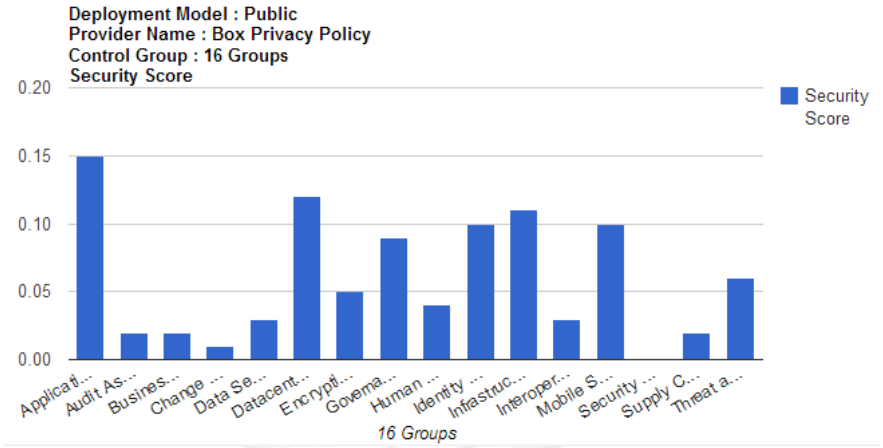
Control Group	Score
Application & Interface Security	0.25
Audit Assurance & Compliance	0.01
Business Continuity Management & Operational Resilience	0.14
Change Control & Configuration Management	0.05
Data Security & Information Lifecycle Management	0.02
Datacenter Security	0.08
Encryption & Key Management	0.05
Governance and Risk Management	0.07
Human Resources	0.05
Identity & Access Management	0.04
Infrastructure & Virtualization Security	0.09
Interoperability & Portability	0.08
Mobile Security	0.05
Security Incident Management, E-Discovery & Cloud Forensics	0.04
Supply Chain Management, Transparency and Accountability	0.08
Threat and Vulnerability Management	0.04



ภาพที่ 4.3 กราฟแสดงเปอร์เซ็นต์ความสอดคล้องในแต่ละด้านของ SalesForce

ตารางที่ 4.3 คะแนนความสอดคล้องในแต่ละด้านของ SalesForce

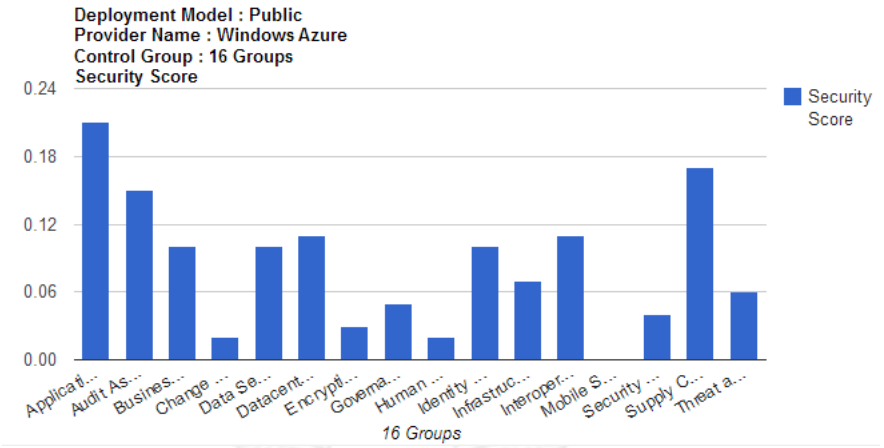
Control Group	Score
Application & Interface Security	0.26
Audit Assurance & Compliance	0.04
Business Continuity Management & Operational Resilience	0.04
Change Control & Configuration Management	0.00
Data Security & Information Lifecycle Management	0.06
Datacenter Security	0.08
Encryption & Key Management	0.07
Governance and Risk Management	0.03
Human Resources	0.03
Identity & Access Management	0.03
Infrastructure & Virtualization Security	0.08
Interoperability & Portability	0.13
Mobile Security	0.13
Security Incident Management, E-Discovery & Cloud Forensics	0
Supply Chain Management, Transparency and Accountability	0.06
Threat and Vulnerability Management	0.07



ภาพที่ 4.4 กราฟแสดงเปอร์เซ็นต์ความสอดคล้องในแต่ละด้านของ Box

ตารางที่ 4.4 คะแนนความสอดคล้องในแต่ละด้านของ Box

Control Group	Score
Application & Interface Security	0.15
Audit Assurance & Compliance	0.02
Business Continuity Management & Operational Resilience	0.02
Change Control & Configuration Management	0.01
Data Security & Information Lifecycle Management	0.03
Datacenter Security	0.12
Encryption & Key Management	0.05
Governance and Risk Management	0.09
Human Resources	0.04
Identity & Access Management	0.10
Infrastructure & Virtualization Security	0.11
Interoperability & Portability	0.03
Mobile Security	0.10
Security Incident Management, E-Discovery & Cloud Forensics	0.00
Supply Chain Management, Transparency and Accountability	0.02
Threat and Vulnerability Management	0.06



ภาพที่ 4.5 กราฟแสดงเปอร์เซ็นต์ความสอดคล้องในแต่ละด้านของ Azure

ตารางที่ 4.5 คะแนนความสอดคล้องในแต่ละด้านของ Azure

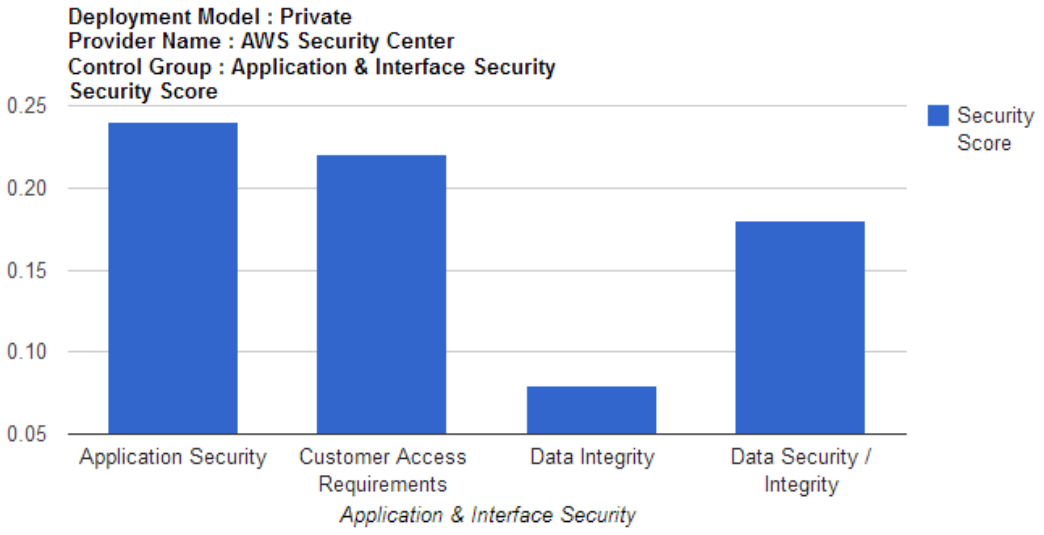
Control Group	Score
Application & Interface Security	0.21
Audit Assurance & Compliance	0.15
Business Continuity Management & Operational Resilience	0.10
Change Control & Configuration Management	0.02
Data Security & Information Lifecycle Management	0.10
Datacenter Security	0.11
Encryption & Key Management	0.03
Governance and Risk Management	0.05
Human Resources	0.02
Identity & Access Management	0.10
Infrastructure & Virtualization Security	0.07
Interoperability & Portability	0.11
Mobile Security	0.00
Security Incident Management, E-Discovery & Cloud Forensics	0.04
Supply Chain Management, Transparency and Accountability	0.17
Threat and Vulnerability Management	0.06

4.2 กรณีทดสอบการแสดงผลคะแนนความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงโดยระบุความมั่นคงแต่ละด้าน

จากทดสอบการประเมินคะแนนความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงในหัวข้อที่ 4.1 จะได้เห็นถึงภาพรวมคะแนนความสอดคล้องทั้ง 16 ด้านของผู้ให้บริการแต่ละราย ในกรณีทดสอบนี้ จะเพิ่มเงื่อนไขในการทดสอบคือระบุด้านความมั่นคง เพื่อให้เห็นรายละเอียดว่ามีคะแนนหมวดย่อยของแนวปฏิบัติด้านความมั่นคงแต่ละด้านเป็นเท่าไรบ้าง ในที่นี้จะแสดงตัวอย่างความมั่นคงด้าน Application & Interface Security โดยผลคะแนนของผู้ให้บริการคลาวด์ Amazon, Google, SalesForce, Box และ Azure จะแสดงในตารางที่ 4.6-4.10 ตามลำดับ

ระบบจะนำเสนอผลการประเมินคะแนนความสอดคล้องของผู้ให้บริการคลาวด์แต่ละรายในความมั่นคงด้าน Application & Interface Security ในรูปแบบของกราฟวงกลม เพื่อแสดงให้เห็นถึงอัตราส่วนของคะแนนแต่ละหมวดย่อยของแนวปฏิบัติด้านความมั่นคง ดังตัวอย่างกราฟแสดงคะแนนความสอดคล้องในแต่ละหมวดย่อยของผู้ให้บริการคลาวด์ Amazon ในภาพที่ 4.6 ซึ่งสามารถสรุปได้ว่า ข้อมูลความมั่นคงที่ผู้ให้บริการคลาวด์ Amazon แสดงไว้บนเว็บไซต์ในด้าน Application & Interface Security มีข้อมูลหมวดย่อยของแนวปฏิบัติด้านความมั่นคงด้าน Application Security มากที่สุด และมีด้านอื่นๆเรียงลำดับมากไปน้อยคือ Customer Access Requirements, Data Security / Integrity และ Data Integrity

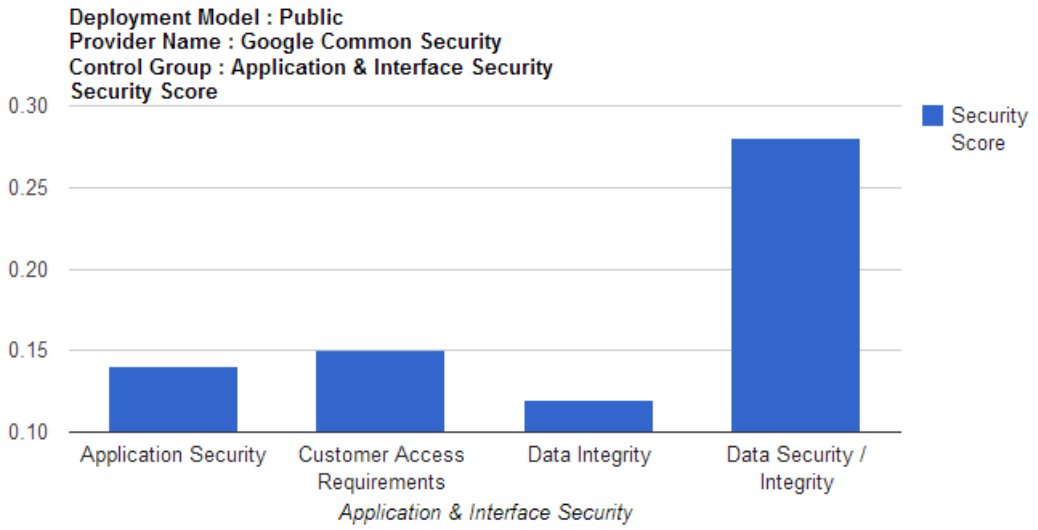
สำหรับกราฟแสดงความสอดคล้องด้าน Application & Interface Security ของผู้ให้บริการคลาวด์ Google, SalesForce, Box และ Azure แสดงในภาพที่ 4.6-4.10 ตามลำดับ



ภาพที่ 4.6 กราฟแสดงเปอร์เซ็นต์ความสอดคล้องในด้าน Application & Interface Security ของ Amazon

ตารางที่ 4.6 คะแนนความสอดคล้องในด้าน Application & Interface Security ของ Amazon

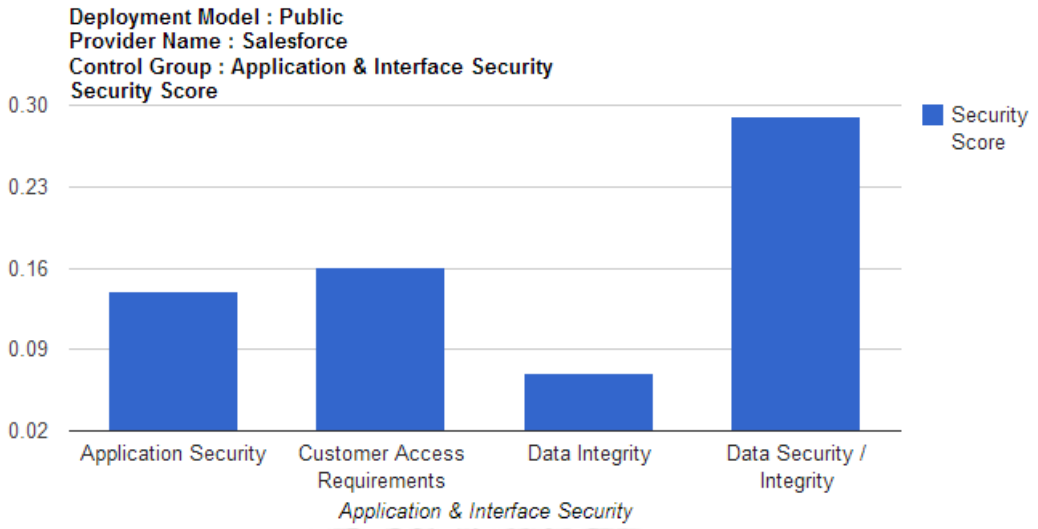
Control Domain	Score
Application Security	0.24
Customer Access Requirements	0.22
Data Integrity	0.08
Data Security / Integrity	0.18



ภาพที่ 4.7 กราฟแสดงเปอร์เซ็นต์ความสอดคล้องในด้าน Application & Interface Security ของ Google

ตารางที่ 4.7 คะแนนความสอดคล้องในด้าน Application & Interface Security ของ Google

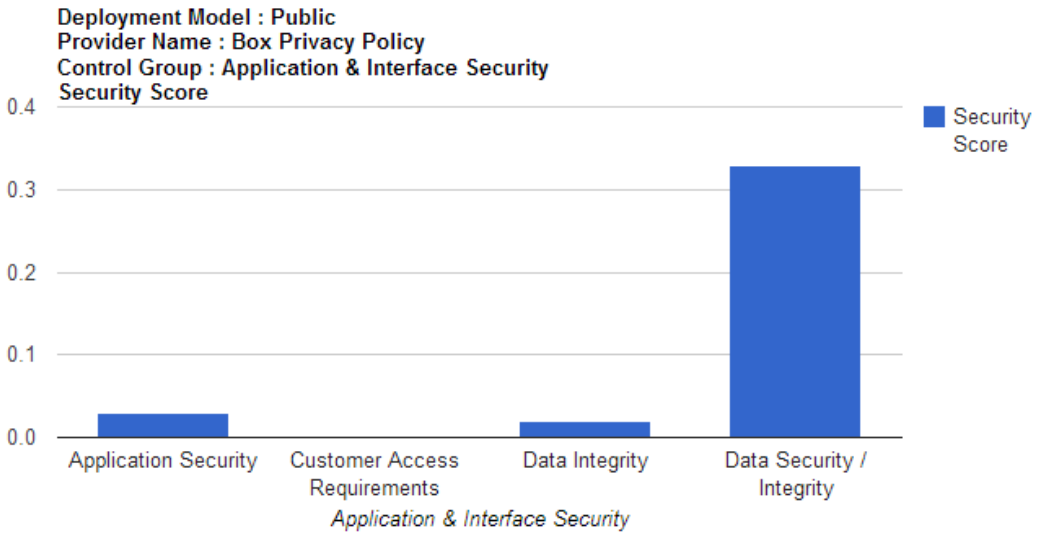
Control Domain	Score
Application Security	0.14
Customer Access Requirements	0.15
Data Integrity	0.12
Data Security / Integrity	0.28



ภาพที่ 4.8 กราฟแสดงเปอร์เซ็นต์ความสอดคล้องในด้าน Application & Interface Security ของ Salesforce

ตารางที่ 4.8 คะแนนความสอดคล้องในด้าน Application & Interface Security ของ Salesforce

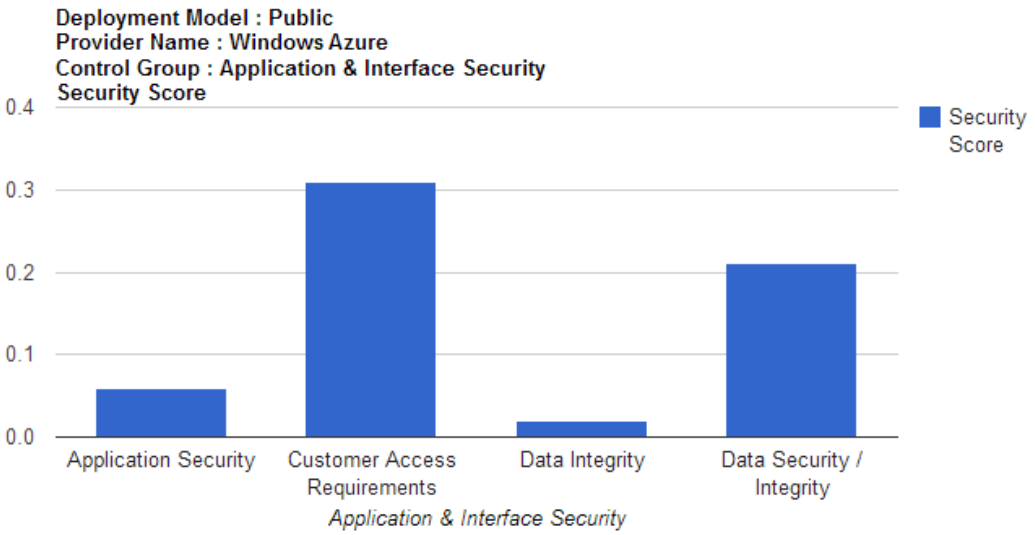
Control Domain	Score
Application Security	0.14
Customer Access Requirements	0.16
Data Integrity	0.07
Data Security / Integrity	0.29



ภาพที่ 4.9 กราฟแสดงเปอร์เซ็นต์ความสอดคล้องในด้าน Application & Interface Security ของ Box

ตารางที่ 4.9 คะแนนความสอดคล้องในด้าน Application & Interface Security ของ Box

Control Domain	Score
Application Security	0.03
Customer Access Requirements	0.00
Data Integrity	0.02
Data Security / Integrity	0.33



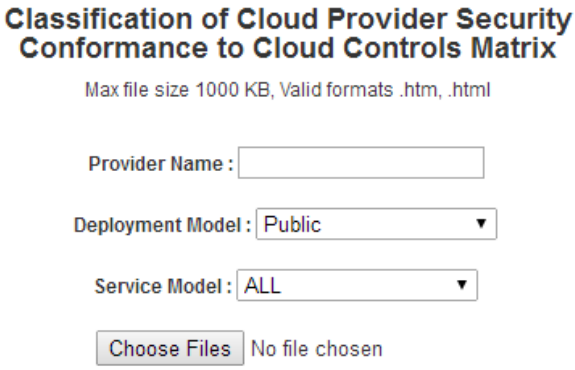
ภาพที่ 4.10 กราฟแสดงเปอร์เซ็นต์ความสอดคล้องในด้าน Application & Interface Security ของ Azure

ตารางที่ 4.10 คะแนนความสอดคล้องในด้าน Application & Interface Security ของ Azure

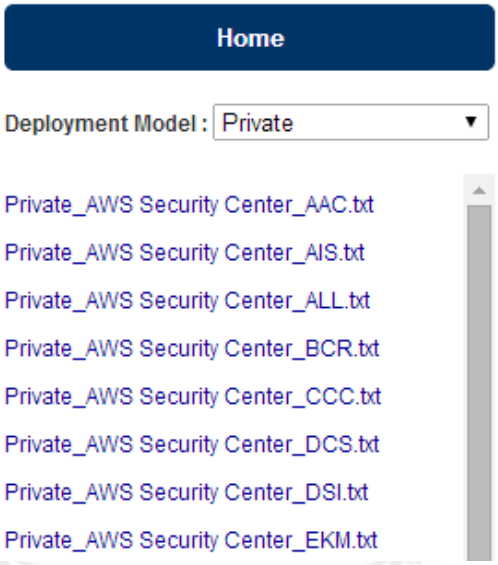
Control Domain	Score
Application Security	0.06
Customer Access Requirements	0.31
Data Integrity	0.02
Data Security / Integrity	0.21

4.3 กรณีทดสอบการระบุลักษณะการใช้งานคลาวด์เป็นเงื่อนไข

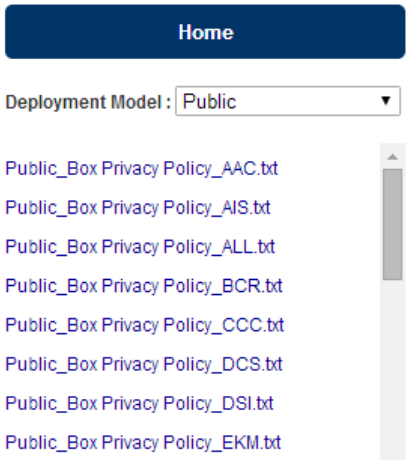
การระบุลักษณะการใช้งานคลาวด์เป็นเงื่อนไข จะถูกระบุโดยผู้ใช้ตั้งแต่ตอนอัปโหลดไฟล์ผู้ให้บริการดังตัวอย่างในภาพที่ 4.11 เพื่อเป็นการระบุว่าผู้ให้บริการคลาวด์รายนั้นมีบริการให้ใช้งานในลักษณะใด ในตอนแสดงผลโปรแกรมจะช่วยกรองเฉพาะผู้ให้บริการคลาวด์ที่มีลักษณะการใช้งานคลาวด์ตามที่ผู้ใช้สนใจเท่านั้น ดังตัวอย่างในภาพที่ 4.12 แสดงการเลือกกรองเฉพาะการใช้งานแบบ Private และ ภาพที่ 4.13 แสดงการเลือกกรองเฉพาะการใช้งานแบบ Public



ภาพที่ 4.11 หน้าจอการอัปโหลดไฟล์พร้อมระบุเงื่อนไขต่างๆ



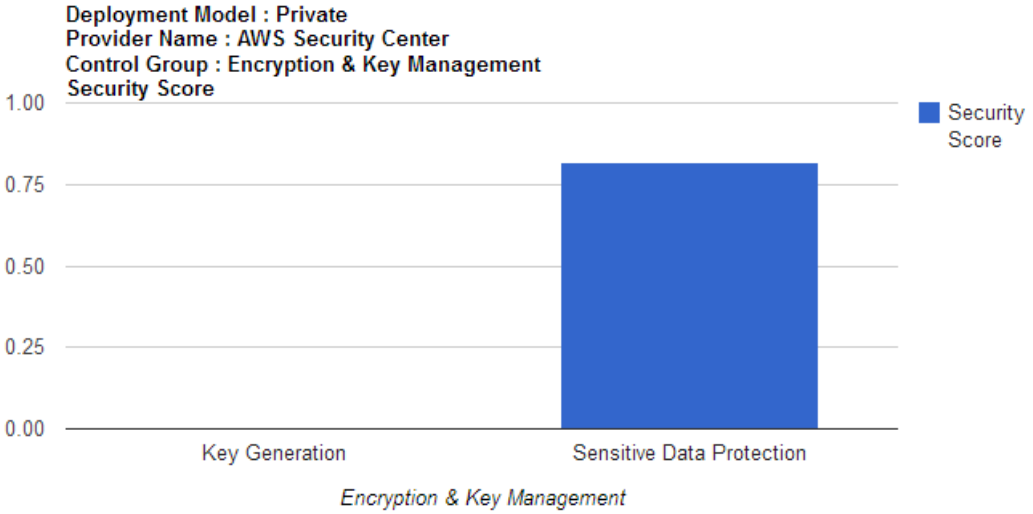
ภาพที่ 4.12 ตัวอย่างผลการเลือกเงื่อนไขการใช้งานแบบ Private



ภาพที่ 4.13 ตัวอย่างผลการเลือกเงื่อนไขการใช้งานแบบ Public

4.4 กรณีทดสอบการระบุลักษณะการให้บริการคลาวด์เป็นเงื่อนไข

การระบุลักษณะการให้บริการคลาวด์เป็นเงื่อนไข จะถูกระบุโดยผู้ใช้ตั้งแต่ตอนอัปโหลดไฟล์ผู้ให้บริการดังตัวอย่างในภาพที่ 4.11 โดยที่เมื่อกดประมวลผลแล้วระบบจะประมวลผลออกมาเฉพาะหมวดหมู่ด้านความมั่นคงที่เกี่ยวข้องกับประเภทการให้บริการคลาวด์ที่ผู้ใช้เลือกเท่านั้น เช่น หากผู้ใช้เลือก Platform as a Service ในส่วนของแนวปฏิบัติด้านความมั่นคงด้าน Encryption & Key Management จะมีหมวดย่อยที่มีความเกี่ยวข้องกับ Platform as a Service เพียงสองหมวดย่อย คือ Key Generation และ Sensitive Data Protection ระบบก็จะแสดงผลออกมาเพียงแค่สองหมวดย่อยนี้เท่านั้น ดังคะแนนในภาพที่ 4.14 และตารางที่ 4.11



ภาพที่ 4.14 ตัวอย่างคะแนนความสอดคล้องด้าน Encryption & Key Management ของ Amazon โดยมีการให้บริการแบบ Platform as a Service เป็นเงื่อนไข

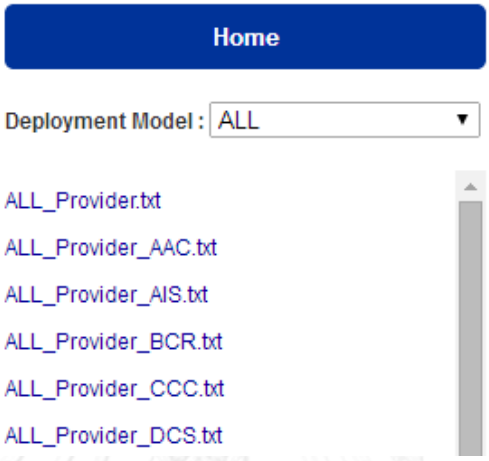
ตารางที่ 4.11 คะแนนความสอดคล้องในด้าน Encryption & Key Management ของ Amazon โดยมีการให้บริการแบบ Platform as a Service เป็นเงื่อนไข

Control Domain	Score
Key Generation	0.0
Sensitive Data Protection	0.82

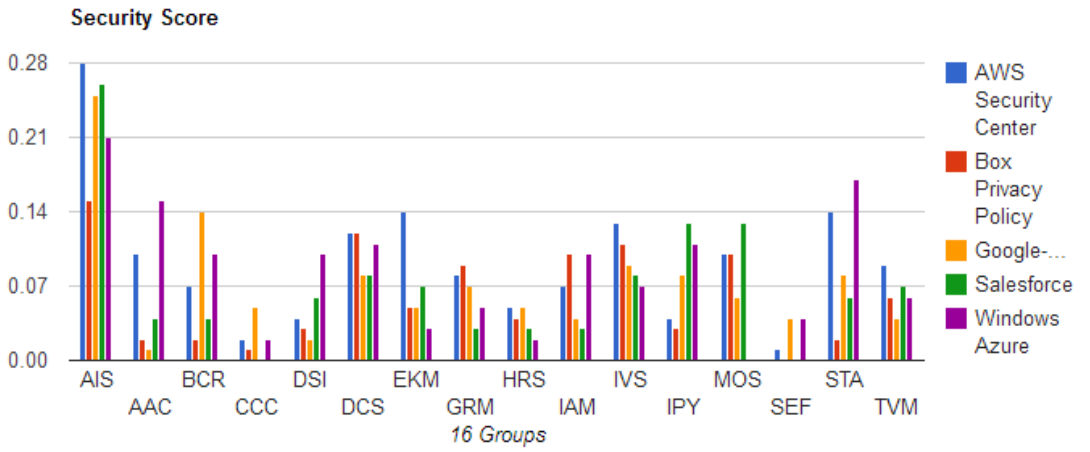
4.5 กรณีทดสอบการแสดงผลการเปรียบเทียบคะแนนความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงโดยไม่ระบุเงื่อนไข

ในการเปรียบเทียบคะแนนความสอดคล้องของผู้ให้บริการทั้งหมดต่อแนวปฏิบัติด้านความมั่นคงทั้ง 16 ด้าน ผู้ใช้เลือก Deployment Model เป็น ALL ระบบจะแสดงผลไฟล์ที่เปรียบเทียบผู้

ให้บริการแต่ละรายตามแนวปฏิบัติด้านความมั่นคงทั้ง 16 ด้าน และสามารถเลือกที่ไฟล์ ALL Provider.txt เพื่อแสดงการเปรียบเทียบทั้งหมดตามภาพที่ 4.15 ผลลัพธ์ที่ได้จะเป็นกราฟแท่งดังภาพที่ 4.16 ซึ่งช่วยให้ผู้ใช้บริการคลาวด์เห็นความแตกต่างของคะแนนความสอดคล้องของผู้ให้บริการคลาวด์แต่ละรายอย่างชัดเจน และได้ตารางคะแนนตามตารางที่ 4.12



ภาพที่ 4.15 ตัวอย่างแถบเมนูสำหรับเลือกไฟล์เพื่อมาแสดงผล



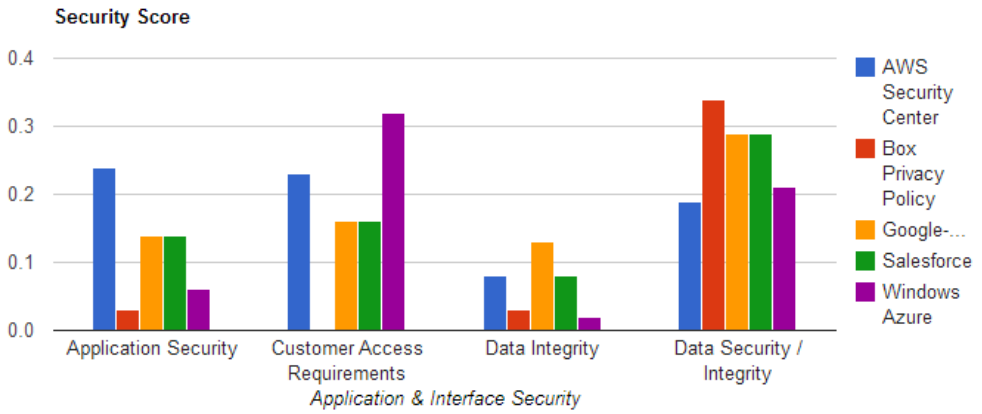
ภาพที่ 4.16 กราฟแสดงการเปรียบเทียบคะแนนความสอดคล้องในแต่ละด้านความมั่นคงของผู้ให้บริการคลาวด์ทั้ง 5 ราย

ตารางที่ 4.12 ผลลัพธ์การประเมินความสอดคล้องในแต่ละด้านความมั่นคงของผู้ให้บริการคลาวด์ทั้ง 5 ราย

Control Group	Amazon	Google	Salesforce	Box	Azure
1.Application & Interface Security (AIS)	0.28	0.25	0.26	0.15	0.22
2.Audit Assurance & Compliance (AAC)	0.10	0.01	0.04	0.02	0.15
3.Business Continuity Management & Operational Resilience (BCR)	0.07	0.14	0.04	0.02	0.09
4.Change Control & Configuration Management (CCC)	0.02	0.05	0.004	0.01	0.02
5.Data Security & Information Lifecycle Management (DSI)	0.04	0.02	0.06	0.03	0.10
6.Datacenter Security (DCS)	0.12	0.08	0.08	0.12	0.11
7.Encryption & Key Management (EKM)	0.14	0.05	0.07	0.05	0.03
8.Governance and Risk Management (GRM)	0.08	0.07	0.03	0.09	0.05
9.Human Resources (HRS)	0.05	0.05	0.03	0.04	0.02
10.Identity & Access Management (IAM)	0.07	0.04	0.03	0.10	0.10
11.Infrastructure & Virtualization Security (IVS)	0.13	0.09	0.08	0.11	0.07
12.Interoperability & Portability (IPY)	0.04	0.08	0.13	0.03	0.11
13.Mobile Security (MOS)	0.10	0.06	0.13	0.10	0.00
14.Security Incident Management, E-Discovery & Cloud Forensics (SEF)	0.01	0.04	0.00	0.00	0.04
15.Supply Chain Management, Transparency and Accountability (STA)	0.14	0.08	0.06	0.02	0.17
16.Threat and Vulnerability Management (TVM)	0.09	0.04	0.07	0.06	0.06

4.6 กรณีทดสอบการแสดงผลการเปรียบเทียบคะแนนความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงโดยระบุความมั่นคงแต่ละด้าน

ในการเปรียบเทียบคะแนนความสอดคล้องของผู้ให้บริการทั้งหมดต่อแนวปฏิบัติด้านความมั่นคงแต่ละด้าน ผู้ใช้สามารถเลือกไฟล์ที่แถบเมนูได้ตามตัวอย่างในภาพที่ 4.15 จากตัวอย่างสามารถเลือกดูในหมวดของ Application & Interface Security ได้ที่ไฟล์ชื่อ ALL Provider AIS.txt ผลลัพธ์ที่ได้จะเป็นกราฟแท่งดังภาพที่ 4.17 ซึ่งช่วยให้ผู้ใช้บริการคลาวด์เห็นความแตกต่างของคะแนนความสอดคล้องของผู้ให้บริการคลาวด์แต่ละรายอย่างชัดเจน และได้ตารางคะแนนตามตารางที่ 4.13



ภาพที่ 4.17 กราฟแสดงการเปรียบเทียบคะแนนความสอดคล้องในด้าน Application & Interface Security ของผู้ให้บริการคลาวด์ทั้ง 5 ราย

ตารางที่ 4.13 ผลลัพธ์การประเมินความสอดคล้องในด้าน Application & Interface Security ของผู้ให้บริการคลาวด์ทั้ง 5 ราย

Control Domain	Amazon	Google	Salesforce	Box	Azure
Application Security	0.24	0.14	0.14	0.03	0.06
Customer Access Requirements	0.23	0.16	0.16	0.00	0.32
Data Integrity	0.08	0.13	0.08	0.03	0.02
Data Security / Integrity	0.19	0.29	0.29	0.34	0.21

4.7 การประเมินผลการจำแนกโดยวิธีสหสัมพันธ์ของเพียร์สัน

ในการประเมินความถูกต้องของการจำแนกหน้าเว็บผู้ให้บริการคลาวด์ จะใช้วิธีสหสัมพันธ์ของเพียร์สัน เพื่อวัดความสามารถของระบบการจำแนกความสอดคล้องด้านความมั่นคงของผู้ให้บริการคลาวด์โดยเปรียบเทียบกับผลการจำแนกด้วยมือโดยผู้วิจัย การประเมินมีสองลักษณะดังนี้

4.7.1 การประเมินความสอดคล้องในแต่ละด้านความมั่นคง

การประเมินนี้จะประเมินความถูกต้องของการจำแนกความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงในแต่ละด้านของผู้ให้บริการคลาวด์ทั้ง 5 ราย คะแนนความสอดคล้องที่ประเมินได้จากระบบแสดงไว้แล้วในตารางที่ 4.12 ข้างต้น จากตารางดังกล่าว หากผู้ให้บริการมีคะแนนจากการจำแนกมากกว่า 0 ในด้านใด จะถือว่ามีความสอดคล้องในด้านนั้น (ได้ค่า 1) แต่หากมีคะแนนจากการจำแนกเป็น 0 ในด้านใด จะถือว่าไม่มีความสอดคล้องด้านนั้น (ได้ค่า 0) ดังนั้นจะสามารถแปลงผลการประเมินคะแนนจากระบบในตารางที่ 4.12 ได้ดังตารางที่ 4.14 (คอลัมน์ M) ส่วนการจำแนกด้วยมือจากข้อมูลบนหน้าเว็บของผู้ให้บริการจะเป็นไปในทำนองเดียวกัน กล่าวคือ ถ้าข้อมูลหน้าเว็บมีการพูดถึงความมั่นคงในด้านใด ผู้วิจัยจะให้ค่าความสอดคล้องเป็น 1 แต่หากไม่มีการพูดถึงความมั่นคงด้านใดจะให้ค่าความสอดคล้องเป็น 0 ดังผลการจำแนกในตารางที่ 4.14 (คอลัมน์ W)

ตารางที่ 4.14 ผลการจำแนกด้วยระบบกับผลการจำแนกด้วยมือสำหรับการประเมินความสอดคล้องในแต่ละด้าน

Control Group	Amazon		Google		Salesforce		Box		Azure	
	M	W	M	W	M	W	M	W	M	W
1.Application & Interface Security (AIS)	1	1	1	1	1	1	1	1	1	1
2.Audit Assurance & Compliance (AAC)	1	1	1	1	1	1	1	1	1	1
3.Business Continuity Management & Operational Resilience (BCR)	1	1	1	1	1	1	1	1	1	1
4.Change Control & Configuration Management (CCC)	1	1	1	1	1	1	1	1	1	1
5.Data Security & Information Lifecycle Management (DSI)	1	1	1	1	1	1	1	1	1	1

ตารางที่ 4.14 ผลการจำแนกด้วยระบบกับผลการจำแนกด้วยมือสำหรับการประเมินความสอดคล้องในแต่ละด้าน (ต่อ)

Control Group	Amazon		Google		Salesforce		Box		Azure	
	M	W	M	W	M	W	M	W	M	W
6.Datacenter Security (DCS)	1	1	1	1	1	1	1	1	1	1
7.Encryption & Key Management (EKM)	1	1	1	1	1	1	1	1	1	1
8.Governance and Risk Management (GRM)	1	1	0	0	0	0	1	1	1	1
9.Human Resources (HRS)	1	1	1	1	1	1	1	1	1	1
10.Identity & Access Management (IAM)	1	1	1	1	1	1	1	1	1	1
11.Infrastructure & Virtualization Security (IVS)	1	1	1	1	1	1	1	1	1	1
12.Interoperability & Portability (IPY)	1	1	1	1	1	1	1	1	1	1
14.Security Incident Management, E-Discovery & Cloud Forensics (SEF)	1	1	1	1	0	1	0	0	1	1
15.Supply Chain Management, Transparency and Accountability (STA)	1	1	1	1	1	1	1	1	1	1
16.Threat and Vulnerability Management (TVM)	1	1	1	1	1	1	1	1	1	1

จากนั้นนำข้อมูลผลการจำแนกทุกคู่ (80 คู่) มาตรวจสอบว่า ผลการจำแนกโดยระบบสอดคล้องกับผลการจำแนกด้วยมือเพียงใดโดยใช้วิธีสหสัมพันธ์ของเพียร์สันดังที่กล่าวไว้ในหัวข้อที่ 2.1.6 จากการคำนวณ ได้ค่าสัมประสิทธิ์สหสัมพันธ์ของเพียร์สัน r = 0.74 ซึ่งเมื่อเปรียบเทียบกับค่าวิกฤต r = 0.303 ในตารางค่าวิกฤตของเพียร์สันที่ระดับนัยสำคัญ α = 0.01 และองศาอิสระ df = n-2 = 78 โดยที่ n คือจำนวนคู่ที่นำมาเปรียบเทียบ แล้วพบว่าค่า r ที่คำนวณได้มีค่ามากกว่าค่าวิกฤต ดังนั้นจึงสรุปว่าผลการจำแนกโดยระบบจึงมีความสัมพันธ์สอดคล้องกับผลการจำแนกด้วยมือ อย่างมีนัยสำคัญที่ระดับความเชื่อมั่น 99%

4.7.2 การประเมินระดับความสอดคล้อง

การประเมินนี้จะประเมินความถูกต้องของระดับความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงของผู้ให้บริการคลาวด์ทั้ง 5 ราย ซึ่งเป็นผลมาจากการจำแนก โดยพิจารณาความมั่นคงด้าน Application & Interface Security ในการประเมิน คะแนนความสอดคล้องด้าน Application & Interface Security ของ Amazon, Google, Salesforce, Box และ Azure ที่คำนวณได้จากระบบแสดงไว้แล้วในตารางที่ 4.6-4.10 ข้างต้น และเนื่องจากผลการจำแนกโดยระบบสามารถให้ค่าความสอดคล้องอย่างละเอียดในระดับทศนิยม แต่ในการจำแนกด้วยมือทำเช่นนั้นได้ยาก ดังนั้นผู้วิจัยจึงใช้การพิจารณาข้อมูลหน้าเว็บแล้วจำแนกว่าผู้ให้บริการมีความสอดคล้องมากน้อยเพียงใดเป็น 3 ระดับ คือ 1-3 จากนั้นทำการแปลงคะแนนที่ได้จากระบบให้เป็น 3 ระดับ เช่นกัน ซึ่งเกณฑ์ในการให้คะแนนแสดงในตารางที่ 4.15 ผู้วิจัยกำหนดช่วงเปอร์เซ็นต์สำหรับการแปลงคะแนนที่ได้จากระบบดังในตารางแทนการแบ่งช่วงเปอร์เซ็นต์เท่า ๆ กัน ทั้งนี้เนื่องจากจากการสังเกตข้อมูลบนหน้าเว็บ พบว่าผู้ให้บริการอาจพูดถึงการปฏิบัติในด้านความมั่นคงแต่ใช้คำศัพท์หรือข้อความที่แตกต่างจากคำศัพท์ในออนโทโลจี จึงอาจทำให้คะแนนที่ได้จากระบบไม่สูงนัก จากเกณฑ์ดังกล่าวนี้จะทำให้ได้ผลการจำแนกความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงดังตารางที่ 4.16 โดยคอลัมน์ M คือคะแนนจากการจำแนกโดยระบบ และ คอลัมน์ W คือคะแนนจากการจำแนกด้วยมือ

ตารางที่ 4.15 หลักเกณฑ์การให้คะแนนจากการจำแนกด้วยมือและการแปลงคะแนนที่ได้จากระบบ

คะแนนจากการจำแนกด้วยมือ	**หลักเกณฑ์ในการให้คะแนนสำหรับการจำแนกด้วยมือ**	**คะแนนจากการจำแนกโดยระบบ (%)**
3 = มาก	ผู้ให้บริการมีการพูดถึงความมั่นคงตามเมตริกซ์ควบคุมคลาวด์อย่างชัดเจนและส่วนมากมีการอ้างอิงหลักฐานเกี่ยวกับกิจกรรมหรือผลิตภัณฑ์มายืนยันอย่างชัดเจน	51-100
2 = ปานกลาง	ผู้ให้บริการมีการพูดถึงความมั่นคงตามเมตริกซ์ควบคุมคลาวด์พอควรและมีการอ้างอิงหลักฐานเกี่ยวกับกิจกรรมหรือผลิตภัณฑ์มายืนยันบ้างบางส่วน	21-50
1 = น้อย	ผู้ให้บริการมีการพูดถึงความมั่นคงตามเมตริกซ์ควบคุมคลาวด์เพียงเล็กน้อยและไม่มีหลักฐานเกี่ยวกับกิจกรรมหรือผลิตภัณฑ์มายืนยัน หรือมีเพียงเล็กน้อย	0-20

ตารางที่ 4.16 ผลการจำแนกด้วยระบบกับผลการจำแนกด้วยมือสำหรับการประเมินระดับความสอดคล้อง

Control Domain	Amazon		Google		Salesforce		Box		Azure	
	M	W	M	W	M	W	M	W	M	W
1.Application Security	2	2	1	2	1	1	1	1	1	1
2.Customer Access Requirements	2	1	1	1	1	1	1	1	2	2
3.Data Integrity	1	1	1	1	1	1	1	1	1	1
4.Data Security /Integrity	1	2	2	2	2	2	2	2	2	2

จากนั้นนำข้อมูลผลการจำแนกทุกคู่ (20 คู่) มาตรวจสอบว่า ผลการจำแนกโดยระบบสอดคล้องกับผลการจำแนกด้วยมือเพียงใดโดยใช้วิธีสหสัมพันธ์ของเพียร์สันดังที่กล่าวไว้ในหัวข้อที่ 2.1.6 จากการคำนวณ ได้ค่าสัมประสิทธ์สหสัมพันธ์ของเพียร์สัน r = 0.68 ซึ่งเมื่อเปรียบเทียบกับค่าวิกฤต r = 0.561 ในตารางค่าวิกฤตของเพียร์สันที่ระดับนัยสำคัญ α = 0.01 และองศาอิสระ df = n-2 = 18 โดยที่ n คือจำนวนคู่ที่นำมาเปรียบเทียบ แล้วพบว่าค่า r ที่คำนวณได้มีค่ามากกว่าค่าวิกฤต ดังนั้นจึงสรุปว่าผลการจำแนกโดยระบบจึงมีความสัมพันธ์สอดคล้องกับผลการจำแนกด้วยมืออย่างมีนัยสำคัญที่ระดับความเชื่อมั่น 99%

บทที่ 5
สรุปผลการวิจัย

5.1 สรุปผลการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อกำหนดวิธีการจำแนกความสอดคล้องด้านความมั่นคงของผู้ให้บริการคลาวด์เพื่อใช้ประเมินระดับความมั่นคงของการให้บริการจากข้อมูลที่เปิดเผยบนหน้าเว็บ รวมทั้งพัฒนาเครื่องมือสนับสนุนสำหรับให้ผู้ใช้บริการคลาวด์ใช้ในการประเมินเพื่อประกอบการพิจารณาเลือกผู้ให้บริการคลาวด์ โดยพิจารณาจากแนวปฏิบัติด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ ซึ่งกำหนดความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงที่ผู้ให้บริการคลาวด์จำเป็นต้องดำเนินการไว้ 16 ด้าน โดยประกอบไปด้วยหมวดย่อย 136 หมวด [1] ผู้วิจัยได้สร้างออนโทโลจีความมั่นคงโดยศึกษาจากเมตริกซ์ควบคุมคลาวด์ แบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน และมาตรฐานต่าง ๆ ที่เมตริกซ์ควบคุมคลาวด์อ้างอิงถึง ออนโทโลจีความมั่นคงที่ได้ประกอบด้วยคำศัพท์ทั้งหมด 461 คำ ซึ่งเกี่ยวข้องกับกิจกรรมที่ผู้ให้บริการคลาวด์ควรดำเนินการ หรือผลิตภัณฑ์ที่ได้จากการดำเนินการนั้น รวมไปถึงแนวคิดหรือหลักการที่เมตริกซ์ควบคุมคลาวด์กล่าวถึงไว้ ผู้วิจัยได้พัฒนาเว็บแอปพลิเคชันที่สามารถนำมาใช้ในการพิจารณาคำศัพท์ที่สกัดมาจากหน้าเว็บของผู้ให้บริการคลาวด์ แล้วนำคำศัพท์ที่ได้มาจำแนกโดยใช้วิธีการจำแนกข้อความอย่างง่าย เพื่อประเมินว่าผู้ให้บริการคลาวด์มีความสอดคล้องกับความต้องการด้านความมั่นคงตามที่ระบุในเมตริกซ์ควบคุมคลาวด์ในด้านใดบ้างและในระดับใด ผู้ใช้บริการสามารถระบุเงื่อนไขในการจำแนกและการแสดงผลคะแนนความสอดคล้องกับเมตริกซ์ควบคุมคลาวด์โดยรวม หรือแสดงผลคะแนนความสอดคล้องตามหมวดย่อย สามารถระบุลักษณะการใช้งานคลาวด์และลักษณะการให้บริการคลาวด์ที่สนใจ รวมไปถึงสามารถเปรียบเทียบความสอดคล้องกับเมตริกซ์ควบคุมคลาวด์ของผู้ให้บริการคลาวด์หลาย ๆ รายที่สนใจได้ จากการประเมินผลการจำแนกเปรียบเทียบกับการจำแนกด้วยมือได้ผลเป็นที่น่าพอใจ โดยการจำแนกด้วยวิธีที่เสนอมีความสัมพันธ์เชิงเส้นแบบตามกันหรือมีความสอดคล้องกับการจำแนกด้วยมือ

5.2 ปัญหาและข้อจำกัด

ปัญหาและข้อจำกัดของงานวิจัยนี้มีดังนี้

1) การวิเคราะห์คำศัพท์เพื่อนำมาสร้างออนโทโลจีความมั่นคงทำได้ค่อนข้างยาก เนื่องจากเมตริกซ์ควบคุมคลาวด์และแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกันเป็นเอกสารที่มีเนื้อหาทางเทคนิคเชิงลึก และเชื่อมโยงไปยังเอกสารมาตรฐานอื่นอีกเป็นจำนวนมาก การแยกประเภทว่าคำศัพท์ใดควรเป็นกิจกรรมหรือผลิตภัณฑ์ก็ทำได้ยากเช่นกัน ออนโทโลจีความมั่นคงที่ผู้วิจัยเสนอจึงยังเป็นเพียงกลุ่มของคำศัพท์และวลีที่สกัดมาเบื้องต้นจากเนื้อหาเอกสารดังกล่าว ซึ่งเพียงพอสำหรับใช้กับวิธีการจำแนกข้อความ

อย่างง่าย แต่ออนโทโลจียังไม่ได้อยู่ในรูปโครงสร้างขององค์ความรู้เกี่ยวกับแนวปฏิบัติด้านความมั่นคง ซึ่งแสดงคอนเซปต์สำคัญและความสัมพันธ์ระหว่างคอนเซปต์อย่างเต็มรูปแบบ

2) ผู้ให้บริการใช้คำศัพท์ในการอธิบายด้านความมั่นคงซึ่งอาจไม่ครอบคลุมและไม่ตรงกับคำศัพท์เทคนิคในเมตริกซ์ควบคุมคลาวด์ ทั้งนี้อาจเป็นเพราะต้องการสื่อสารกับผู้ใช้บริการให้เข้าใจได้ง่าย นอกจากนี้การวิเคราะห์หน้าเว็บยังไม่ได้พิจารณาความหมายของข้อความ แต่พิจารณาที่การปรากฏของคำศัพท์ในออนโทโลจี ดังนั้นหากข้อความระบุคำศัพท์อื่นที่มีความหมายเดียวกับคำในออนโทโลจี การวิเคราะห์จะไม่สามารถตรวจพบได้ หรือในทางตรงกันข้าม หากมีการระบุเนื้อหาในเชิงปฏิเสธการทำกิจกรรมหรือการมีผลิตภัณฑ์ใด ๆ ตามออนโทโลจี การวิเคราะห์จะผิดพลาดได้เนื่องจากตรวจพบคำศัพท์ที่ตรงกับออนโทโลจี

3) คะแนนการจำแนกที่ได้ช่วยให้เห็นภาพรวมในเบื้องต้นของความสอดคล้องตามแนวปฏิบัติด้านความมั่นคงในด้านต่าง ๆ ของผู้ให้บริการคลาวด์ แต่ยังไม่สามารถถือเป็นคะแนนความมั่นคงในด้านต่าง ๆ ได้เต็มที่ เนื่องจากผลการจำแนกขึ้นอยู่กับปริมาณการเปิดเผยข้อมูลบนหน้าเว็บและความถูกต้องของข้อมูล ซึ่งอาจไม่ครบถ้วน ไม่ชัดเจน ไม่ทันสมัย รวมทั้งข้อมูลอาจเป็นเพียงคำโฆษณา คะแนนที่ได้จึงเป็นเพียงข้อมูลที่สะท้อนถึงระดับการเปิดเผยข้อมูลที่สอดคล้องกับเมตริกซ์ควบคลุมคลาวด์ เพื่อช่วยประกอบการพิจารณาเลือกใช้บริการ แต่ยังไม่สามารถทดแทนผลการประเมินความมั่นคงโดยผู้ตรวจสอบด้านความมั่นคง (Security Auditor) หรือผลการประเมินจากการทดสอบการทำงานจริงของบริการคลาวด์

4) ถึงแม้การประเมินวิธีการจำแนกเมื่อเทียบกับการจำแนกด้วยมือจะได้ผลเป็นที่น่าพอใจ แต่เนื่องจากการจำแนกด้วยมือทำโดยผู้วิจัย ซึ่งมีประสบการณ์เกี่ยวกับเมตริกซ์ควบคุมคลาวด์ประมาณ 1 ปี ผลการประเมินจึงอาจมีความคลาดเคลื่อน

5) การอัพโหลดไฟล์ผู้ให้บริการคลาวด์ยังไม่มีการตรวจสอบความซ้ำซ้อนของไฟล์ซึ่งถ้ามีการอัพโหลดไฟล์ซ้ำจะทำให้การประมวลผลใช้เวลานานขึ้นแต่จะไม่มีผลกับการคำนวณคะแนน

6) การประมวลผลไฟล์ผู้ให้บริการคลาวด์จะประมวลผลไฟล์ทุกไฟล์ของผู้ให้บริการคลาวด์ทุกรายที่มีการอัพโหลดไว้แล้วในระบบ ในกรณีที่มีการอัพโหลดไฟล์ผู้ให้บริการคลาวด์เพิ่มเติม ระบบจะทำการประมวลผลไฟล์ผู้ให้บริการคลาวด์ใหม่ทั้งหมด รวมทั้งไฟล์ที่เคยอัพโหลดไว้ในระบบแล้ว

5.3 แนวทางการวิจัยต่อไป

แนวทางในการพัฒนางานวิจัยนี้ต่อมีดังนี้

1) พัฒนาออนโทโลจีความมั่นคงให้เป็นโครงสร้างขององค์ความรู้เกี่ยวกับแนวปฏิบัติด้านความมั่นคงที่สมบูรณ์ และอาจเพิ่มคำศัพท์ในออนโทโลจีโดยการอ้างอิงออนโทโลจีด้านความมั่นคงอื่น ๆ เพื่อเพิ่มคำที่สามารถพิจารณาหน้าเว็บผู้ให้บริการได้ถูกต้องและครบถ้วนมากยิ่งขึ้น เช่น ในงานวิจัยของ Bill Tsoumas และ Dimitris Gritzalis [32] ได้พูดถึงออนโทโลจีด้านความมั่นคง ซึ่งสามารถนำมาเป็นส่วนเสริมในการเพิ่มประสิทธิภาพของออนโทโลจีได้ ตัวอย่างเช่น คำว่า Risk Assessment จะถูกเสริมด้วยคำว่า Threat Agent ซึ่งเป็นคำที่มีความหมายถึงสาเหตุการเกิดความเสี่ยง รวมถึงออนโทโลจีด้านความมั่นคงของงานวิจัยอื่น ๆ ซึ่งถูกรวบรวมไว้ในงานวิจัยของ Carlos Blanco [33] นอกจากนี้ควรมีการประเมินออนโทโลจีที่ได้โดยผู้เชี่ยวชาญด้านความมั่นคงของคลาวด์เพื่อนำออนโทโลจีมาใช้ปรับปรุงการจำแนกหรือนำไปใช้งานในลักษณะอื่นต่อไปได้

2) ปรับปรุงวิธีการจำแนกให้มีประสิทธิภาพมากขึ้น เช่น การให้ค่าน้ำหนักของคำศัพท์แตกต่างกันในการเปรียบเทียบความเหมือนของคำศัพท์ โดยคำประเภทกิจกรรมและผลิตภัณฑ์ ควรมีน้ำหนักมากกว่าคำที่เป็นประเภทคอนเซปต์ที่เกี่ยวข้อง เพราะกิจกรรมและผลิตภัณฑ์ ถือเป็นหลักฐานยืนยันความสอดคล้องได้ดีกว่า หรือปรับปรุงวิธีการโดยใช้การวิเคราะห์ความหมายของข้อความที่อยู่บนหน้าเว็บร่วมด้วยเมื่อทำการเปรียบเทียบกับคำในออนโทโลจี เช่น พิจารณาคำที่มีความหมายเชิงปฏิเสธ คำที่มีความหมายเหมือนกัน หรือเปลี่ยนจากการใช้วิธีการจำแนกข้อความอย่างง่ายมาเป็นวิธีการจำแนกที่ต้องอาศัยการเรียนรู้ ซึ่งเป็นวิธีการที่ซับซ้อนกว่าแต่มีประสิทธิภาพดีกว่า

3) ปรับปรุงโปรแกรมสนับสนุนงานวิจัยโดยเพิ่มการตรวจสอบความซ้ำซ้อนของไฟล์ โดยการเก็บชื่อไฟล์ต้นฉบับจากหน้าเว็บที่เคยอัพโหลดมาแล้ว เพื่อนำมาเปรียบเทียบกับชื่อไฟล์ที่จะอัพโหลดใหม่ โดยอาจจะพิจารณาพร้อมกับขนาดของไฟล์ ซึ่งจะทำให้ลดเวลาที่ใช้ในการประมวลผลลงได้ นอกจากนี้ควรเพิ่มประสิทธิภาพการประมวลผลไฟล์โดยสามารถเลือกเฉพาะไฟล์ที่ต้องการประมวลผลใหม่ ซึ่งอาจจะเป็นไฟล์ของผู้ให้บริการรายใหม่ ไฟล์ที่มีการแก้ไข หรือไฟล์ที่มีการอัพเดตข้อมูล

รายการอ้างอิง

1. Cloud Security Alliance. *Cloud Controls Matrix*. 2013 [cited 2013 August]; Available from: https://cloudsecurityalliance.org/research/ccm.
2. Cloud Security Alliance. *Consensus Assessments Initiative Questionnaire*. 2013 [cited 2013 August]; Available from: https://cloudsecurityalliance.org/research/cai
3. NIST, *T. Guidelines on Security and Privacy in Public Cloud Computing*, in *NIST Special Publication 800-144*. 2011, Wayne Jansen, Timothy Grance.
4. Walker, G. *Cloud Computing Fundamentals* 2010 [cited 2013 August]; Available from: https://www.ibm.com/developerworks/cloud/library/cl-cloudintro/index.html.
5. Baeza-Yates, R. and B. Ribeiro-Neto, *Modern Information Retrieval*. Second edition, ed. A. Wesley. 2011, ACM Press.
6. Gruber, T. *Ontology (Computer Science) definition in Encyclopedia of Database Systems* 2009 [cited 2013 August]; Available from: http://tomgruber.org/writing/ontology-definition-2007.htm.
7. Pauley, W.A., *Cloud Provider Transparency: An Empirical Evaluation*, in *IEEE Security & Privacy*. 2010, IEEE. p. 32-39.
8. Michael, B., *In Clouds Shall We Trust.* IEEE Security & Privacy, 2009. **7**(5): p. 1.
9. Sun Microsystems, *Building Customer Trust in Cloud Computing with Transparent Security*, in *White Paper, Sun Microsystems, Inc.* 2009.
10. Everett, C., *Cloud Computing – A Question of Trust.* Computer Fraud & Security, 2009: p. 3.
11. Kaliski, B.S.J. and W. Pauley, *Toward Risk Assessment as a Service in Cloud Environments*, in *Proceedings of 2nd USENIX Conference on Hot Topics in Cloud Computing (HotCloud'10)*. 2010. p. 7.
12. Tancock, D., S. Pearson, and Charlesworth, *A Privacy Impact Assessment Tool for Cloud Computing*, in *Proceedings of 2nd IEEE International Conference on Cloud Computing Technology and Science*. 2010. p. 10.
13. Bhensook, N. and T. Senivongse, *An Assessment of Security Requirements Compliance of Cloud Providers*, in *4th IEEE International Conference on Cloud Computing Technology and Science*. 2012: Taipei, Taiwan p. 520 - 525.
14. Hayden, L. and K. Stavinoha, *Measuring Cloud Security.* ISSA Journal, 2013: p. 7.
15. HTTrack. *HTTrack Website Copier* 2013 [cited 2013 August]; Available from: http://www.httrack.com/page/2/en/index.html.

16. The Stanford Natural Language Processing Group. *Supported software distributions* 2013 [cited 2013 September]; Available from: http://nlp.stanford.edu/software/index.shtml.
17. Amazon Web Serices. *AWS Security Center*. 2013 [cited 2014 April]; Available from: http://aws.amazon.com/security/.
18. Google. *Google's Approach to IT Security*. 2013 [cited 2014 April]; Available from: https://cloud.google.com/files/Google-CommonSecurity-WhitePaper-v1.4.pdf.
19. Salesforce.com, *Secure, private, and trustworthy: enterprise cloud computing with Force.com.* 2013.
20. Box.com. *BOX PRIVACY POLICY*. 2012 [cited 2013 August]; Available from: http://box.com/static/html/privacy.html.
21. Microsoft Azure. *Microsoft Azure Trust Center*. 2014 [cited 2014 April]; Available from: http://azure.microsoft.com/en-us/support/trust-center/security/.
22. Services, A.W. *mazon Elastic Compute Cloud (Amazon EC2)*. 2014 [cited 2014 April]; Available from: http://aws.amazon.com/ec2/
23. Services, A.W., *Amazon Relational Database Service (Amazon RDS)*. 2014.
24. Google. *Google Cloud Platform*. 2014 [cited 2014 April]; Available from: https://cloud.google.com/
25. Google. *Google Drive*. 2014 [cited 2014 April]; Available from: https://drive.google.com/.
26. Salesforce.com. *The Salesforce1 Platform*. 2014 [cited 2014 April]; Available from: http://www.salesforce.com/platform/overview/
27. Salesforce.com. *Sales Cloud*. 2014 [cited 2014 April]; Available from: http://www.salesforce.com/sales-cloud/resources/.
28. Box.com, *Box Online File Sharing.* 2014.
29. Box.com, *Box for iPad and iPhone.* 2014.
30. Microsoft Azure. *Storage, Backup, and Recovery*. 2014 [cited 2014 April]; Available from: http://azure.microsoft.com/en-us/solutions/storage-backup-recovery/.
31. Windows Azure. *Mobile Apps on Azure*. 2014 [cited 2014 April]; Available from: http://azure.microsoft.com/en-us/solutions/mobile/.
32. TSOUMAS, B. and GRITZALIS, *Towards an Ontology-based Security Management*, in *the 20th International Conference on Advanced Information Networking and Applications (AINA'06)*. 2006.
33. Blanco1, C., et al., *A Systematic Review and Comparison of Security Ontologies*. 2008.

ภาคผนวก

ภาคผนวก ก. คำศัพท์ในออนโทโลจี

ตารางที่ ก.1 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Application & Interface Security

คำศัพท์		
Related Concept	Activity	Product
Access By Individuals	Access Control Procedures	Access Control Policy
Access Configuration	Access Management	Authorization Policies
Access Control	Ajax Testing	Communications Protection Policy
Accuracy Completeness Personal Information	Authentication Testing	Compliance With Security Policies
Accuracy of Personal Information	Authorization Testing	Compliance With Security Standards
Address Resolution Service	Boundary Protection	Consistency Privacy Policies
Addressing Security	Business Logic Testing	Information Exchange Policies
Anonymized	Change Detection	Plan of Action
Application Availability	Change Management	Provision Of Access Policies
Application Partitioning	Code Review	Provisioning For Name
Application Security	Configuration Management Testing	Public Key Infrastructure Certificates
Application Security Architecture	Consistency Privacy Procedures	Security Protocols
Architecture For Name	Control of Internal Processing	System Protection Policy
Assurance Program	Cryptographic Key Establishment And Management	
Audit Files	Data Protection	
Authenticate Users	Data Validation Testing	
Authentication	Denial Of Service Protection	
Authoritative Source	Denial Of Service Testing	
Authorization	Error Handling	
Authorization Credentials	File Integrity Monitoring	
Authorized Access Permissions	Improper Access Control	
Buffer Overflow	Improper Error Handling	
Business Requirements	Information Exchange Pocedures	
CCM	Information System Monitoring	
Classify Information	Infrastructure Management	
COBIT	Integrity Controls	
Coding Vulnerabilities	Interoperability Testing	
Collection Third Parties	Log Monitoring	

ตารางที่ ก.1 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Application & Interface Security (ต่อ)

คำศัพท์		
Related Concept	Activity	Product
Communication Third Parties	Logical Access Controls	
Complete Mediation	Malicious Code Protection	
Completeness of Personal Information	Management Assesses	
Compliance Building Blocks	Management Interfaces	
Compliance Risk	Management Of Applications	
Configuration And Parameter Files	Management Of Databases	
Connection Time	Management Of Information Repositories	
Control of Technical Vulnerabilities	Management Of Infrastructures	
Critical Cyber Asset information	Management Of Mobile Computing	
Cross-site Request Forgery	Management Of Procedures	
Cross-site Scripting	Management Of Product And Services	
Cryptographic Controls	Management Of Systems	
Cryptography	Management Of Websites	
CSA	Monitoring Applications	
Customer Access Requirements	Monitoring For Compromise	
Cyber Security	Monitoring For Malicious Use	
Data Classification	Monitoring For Policy Violations	
Data Integrity	Network Connection Control	
Data Security	Open Design	
Denial Of Service	Outsourced Software Development	
Directory Traversal	Penetration Testing	
Disclosure Personal Information	Performance Monitoring	
Disk Encryption	Physical Access Controls	
Economy Of Mechanism	Privacy of Personal Information	
Elevation Of privilege	Privacy Policies	
Encrypt	Protection Of Personal Information	
Entitlement	Public Access Protections	
Exchange Sensitive Data	Regression Testing	
Fail Safe	Security Management Controls	
FedRAMP	Security Testing	
Flaw Remediation	Session Management Testing	
GAPP	Software Development Processes	
HIPAA	Systems Management	
Identification of Risks	Systems Security Management	
Identity	Technical Review	
Implementation Specification	Web Service Testing	
Individual’s Identity		
Information Access Restriction		
Information Architecture		

ตารางที่ ก.1 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Application & Interface Security (ต่อ)

คำศัพท์		
Related Concept	Activity	Product
Information Disclosure		
Information Flow Enforcement		
Information In Shared Resources		
Information Input Restrictions		
Information Input Validation		
Information Leakage		
Information Security Architecture		
Information Security Program		
Injection Flaws		
Input Data Validation		
Insecure Communications		
Insecure Cryptographic Storage		
Integrity		
IPSEC		
ISO 27001		
Isolation Failure		
Lack of Control		
Lack Of Manageability		
Lack Of Visibility		
Least Common Mechanism		
Least Privilege		
Log Files		
Loss Of Governance		
Message Integrity		
Milestones		
Misuse of Personal Information		
Mobile Code		
NERC		
Network Disconnect		
NIST		

ตารางที่ ก.1 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Application & Interface Security (ต่อ)

คำศัพท์		
Related Concept	Activity	Product
Online Transactions		
Output Data Validation		
PCI		
Personal Information		
Prevent Cryptographic Flaws		
Properly Encrypt All Authenticated		
Public Facing Devices		
Public Facing Systems		
Publicly Available Information		
Quantitative Improvement		
Removal of custom application accounts		
Repudiation		
Resource Priority		
Review Of Custom Code		
Risk Tolerance		
Risks And Solutions		
Sanitize Input		
SDLC Security Technology Features		
SDLC Security Technology Tools		
Secure Coding Guidelines		
Secure Coding Techniques		
Security Assessment		
Security Authorization		
Security Functionality Verification		
Segregation of Duties		
Sensitive Communications		
Session Authenticity		
Software and Information Integrity		
Spoofing		
SQL Injection		
SSH		
System Executables		
Systems Security Management		
Tampering		
Technical Vulnerabilities		
Transmission Confidentiality		
Transmission integrity		
Transmission of Security Attributes		
Transmitted Personal Information		
Truncate Input Strings		

ตารางที่ ก.1 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Application & Interface Security (ต่อ)

คำศัพท์		
Related Concept	Activity	Product
Trusted Path		
Two-factor Authentication		
Validate Buffer Boundaries		
VPN		
Vulnerabilities		
Vulnerability Identification		
Weakest Link		

ตารางที่ ก.2 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Audit Assurance & Compliance

คำศัพท์		
Related Concept	Activity	Product
Assurance Internal Control	Audit Management	Audit Planning
Audit controls	Breach Management	Consistency Privacy Policies
CCM	Compliance Management	Control Framework
COBIT	Compliance Review	Maintenance of a Risk Action Plan
Collection Limited Identified Purpose	Enterprise Risk Management	Maintenance Risk Action plan
Consent	Independent Audits	
Consistency Commitments	Infrastructure Management	
Contractual Compliance Requirements	Internal ISMS Audits	
Cooperate Governance	Management Commitment	
Governance	Monitor ISMS	
Identification External Legal	Monitoring	
Information System Regulatory Mapping	Monitoring Of A Risk Action Plan	
Organizational Objectives	Monitoring Of Internal Control Framework	
Personal Information	Monitoring Risk Action Plan	
Regulations	Ongoing Monitoring	
Regulatory	Privacy Incident	
Risk Assessment	Privacy Policies Procedures	
Risk Response	Procedures Laws	
Surveillance	Review ISMS	
	Security Testing	
	Supervisory Review	
	Systems Management	
	Testing Security Safeguards	

ตารางที่ ก.3 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Business Continuity Management & Operational Resilience

คำศัพท์		
Related Concept	Activity	Product
Business Continuity	Business Continuity Testing	Business Continuity Planning
CCM	Equipment Maintenance	IT Continuity Framework
COBIT	Information Management	IT Continuity Plans
Communication Individuals	Infrastructure Maintenance	Retention Policy
Data Center Operations	Infrastructure Management	Risk Management Framework
Data Security	Logical Access Controls	Testing IT Continuity Plan
Destruction	Management Commitment	
Disaster Recovery	Management Program	
Disposal	Operations Procedures	
Environmental Risks	Physical Access Controls	
Environmental Safeguards	Privacy Policies	
Equipment Location	Security Requirements Data Management	
Equipment Power Failures	Systems Management	
Establishing a Physical Security Function	Testing Security Safeguards	
Establishment Risk Context		
Human Resources Physical Security		
Impact Analysis		
Information Governance		
Information Security Program		
Instructions		
Manage Configuration		
Offsite Backup Storage		
Personal Information Portable Media		
Power Telecommunications		
Redaction Personal Information		
Retention Personal Information		
Traditional Security		
Transmitted Personal Information		

ตารางที่ ก.4 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Change Control & Configuration Management

คำศัพท์		
Related Concept	Activity	Product
Accuracy Completeness Personal Information	Change Standards Procedures	Quality Management System
Acquire Application Software	Infrastructure Management	
Audit controls	Logical Access Controls	
CCM	Outsourced Development	
COBIT	Privacy Policies	
Communication Individuals	Quality Testing	
Consent	Systems Management	
Maintain Application Software	Testing of Changes	
New Development Acquisition		
Production Changes		
Relevance Personal Information		
Unauthorized Software Installations		

ตารางที่ ก.5 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Data Security & Information Lifecycle Management

คำศัพท์		
Related Concept	Activity	Product
Access Individuals Personal Information	Privacy Policies	Accountability Policies
CCM	Infrastructure Management	Handling Labeling Security Policy
Classification	Management IT Security	
COBIT	Security Requirements Data Management	
Collection Third Parties	Information Management	
Communication Individuals	Protection Personal Information	
Communication Third Parties	Logical Access Controls	
Consent	Systems Management	
Cooperate Governance	Enterprise Risk Management	
Data Classification Scheme		
Data Flow		
Data Inventory		
Data Security		
Destruction		
Disclosure Personal Information		
Disposal		
eCommerce Transactions		
Exchange Sensitive Data		
Governance		
Information Governance		
Information Leakage		
Information Security Program		
Network Security		
Non Production Data		
Ownership Stewardship		
Personal Information Collected		
Personal Information Identification		
Personal Information Portable Media		
Redaction Personal Information		
Secure Disposal		
Transmitted Personal Information		

ตารางที่ ก.6 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Datacenter Security

คำศัพท์		
Related Concept	Activity	Product
Access Configuration	Access Management	Provision Of Access Policies
Application Security Architecture	Asset Management	
Assurance Program	Business Logic Testing	
Authentication	Code Review	
CCM	Configuration Management Testing	
COBIT	Data Protection	
Complete Mediation	Data Validation Testing	
Compliance Building Blocks	Denial Of Service Testing	
Compliance Risk	Log Monitoring	
Controlled Access Points	Logical Access Controls	
Data Center Operations	Management Interfaces	
Denial Of Service	Monitoring Applications	
Economy Of Mechanism	Monitoring For Compromise	
Elevation Of privilege	Open Design	
Entitlement	Penetration Testing	
Equipment Identification	Performance Monitoring	
Fail Safe	Protection Security Technology	
Identity	Security Testing	
Information Disclosure		
Information Security Program		
Interoperability		
Isolation Failure		
Lack of Control		
Lack Of Manageability		
Lack Of Visibility		
Least Common Mechanism		
Least Privilege		
Loss Of Governance		
Off-Site Authorization		
Off-Site Equipment		
Personal Information Portable Media		
Physical Access		
Physical Security Measures		
Portability		
Quantitative Improvement		
Repudiation		
Risks And Solutions		
SDLC Security Technology Features		
SDLC Security Technology Tools		

ตารางที่ ก.6 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Datacenter Security (ต่อ)

คำศัพท์		
Related Concept	Activity	Product
Secure Area Authorization		
Segregation of Duties		
Spoofing		
Tampering		
Transmitted Personal Information		
Unauthorized Persons Entry		
User Access		
Weakest Link		

ตารางที่ ก.7 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Encryption & Key Management

คำศัพท์		
Related Concept	Activity	Product
CCM	Cryptographic Key Management	
COBIT	Encryption Key Management	
Communication Individuals	Key Management	
Cooperate Governance	Enterprise Risk Management	
Encrypt		
Entitlement		
Exchange Sensitive Data		
Governance		
Information Security Program		
Network Security		
Transmitted Personal Information		

ตารางที่ ก.8 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Governance and Risk Management

คำศัพท์		
Related Concept	Activity	Product
Baseline Requirements	Audit Management	Accountability Policies
CCM	Compliance Management	Consistency Privacy Policies
COBIT	Compliance Review	IT Security Plan
Communication Individuals	Consistency Privacy Procedures	Maintenance Risk Action plan
Consistency Commitments	Detailed Design	Policy Change Impacts
Contracts	Employee Job Performance Evaluation	Policy Enforcement
Cooperate Governance	Enterprise Risk Management	Policy Reviews
Electronic Discovery	High Level Design	Risk Management Framework
Establishment Risk Context	Identity Management	
Forensic Accountability	Infrastructure Maintenance	
Governance	Infrastructure Management	
Incident Response	Management Commitment	
Information Security Program	Management Involvement	
Instances of Noncompliance	Management IT Security	
Legal Issues	Management Oversight	
Risk Acceptance	Management Program	
Risk Assessment	Management Support	
Risk Mitigation	Monitor ISMS	
Risk Response	Monitoring	
Surveillance	Monitoring Risk Action Plan	
	Privacy Policies	
	Protection Security Technology	
	Review Approval	
	Review ISMS	
	Security Requirements Data Management	
	Security Testing	
	Supplier Risk Management	
	Systems Management	
	Testing Security Safeguards	
	User Account Management	

ตารางที่ ก.9 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Human Resources

คำศัพท์		
Related Concept	Activity	Product
Asset Returns	Management IT Security	Employment Agreements
Background Screening	Protection Personal Information	Non-Disclosure Agreements
Benchmarking	Identity Management	
CCM	Privacy Policies Procedures	
COBIT	Privacy Policies	
Consent	Physical Access Controls	
Consistency Commitments	Privacy Awareness Training	
Contracts	Management Commitment	
Cooperate Governance	Logical Access Controls	
Destruction	Ongoing Monitoring	
Disposal	Systems Management	
Electronic Discovery	Personnel Training	
Employment Termination	Monitoring	
Establishment Roles Responsibilities	Enterprise Risk Management	
Exchange Sensitive Data	Mobile Device Management	
Governance		
Identification Supplier Relationships		
Industry Knowledge		
Information Security Program		
Job Change Termination		
Legal Issues		
Personal Information Portable Media		
Personnel Clearance Procedures		
Redaction Personal Information		
Roles Responsibilities		
Surveillance		
Training Awareness		
User Responsibility		
Workspace		

ตารางที่ ก.10 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Identity & Access Management

คำศัพท์		
Related Concept	Activity	Product
Access Configuration	Access Management	Provision Management
Access Individuals Personal Information	Ajax Testing	Provision Of Access Policies
Application Security Architecture	Audit Management	User ID Credentials
Assurance Program	Authentication Testing	
Audit controls	Authorization Testing	
Audit Tools Access	Business Logic Testing	
Authentication	Code Review	
Benchmarking	Compliance Management	
CCM	Configuration Management Testing	
COBIT	Data Protection	
Communication Individuals	Data Validation Testing	
Communication Third Parties	Denial Of Service Testing	
Complete Mediation	Enterprise Risk Management	
Compliance Building Blocks	Identity Management	
Compliance Risk	Infrastructure Management	
Configuration Ports Access	Interoperability Testing	
Cooperate Governance	Log Monitoring	
Credential Lifecycle	Logical Access Controls	
Denial Of Service	Management Interfaces	
Diagnostic	Monitoring Applications	
Disclosure Personal Information	Monitoring For Compromise	
Economy Of Mechanism	Monitoring For Malicious Use	
Elevation Of privilege	Monitoring For Policy Violations	
Entitlement	Open Design	
Fail Safe	Penetration Testing	
Governance	Performance Monitoring	
Identity	Privacy Policies	
Industry Knowledge	Protection Personal Information	
Information Disclosure	Protection Security Technology	
Information Security Program	Security Testing	
Isolation Failure	Session Management Testing	
Lack of Control	Supplier Risk Management	
Lack Of Manageability	Systems Management	
Lack Of Visibility	Testing Security Safeguards	
Least Common Mechanism	User Access Reviews	
Least Privilege	User Account Management	
Loss Of Governance	Web Service Testing	
Misuse Personal Information Third Party		
New Purposes Uses		

ตารางที่ ก.10 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Identity & Access Management (ต่อ)

คำศัพท์		
Related Concept	Activity	Product
Quantitative Improvement		
Repudiation		
Restriction Authorization		
Risks And Solutions		
SDLC Security Technology Features		
SDLC Security Technology Tools		
Segregation of Duties		
Source Code Access Restriction		
Spoofing		
Tampering		
Third Party Access		
Trusted Sources		
User Access Authorization		
User Access Revocation		
Utility Programs Access		
Weakest Link		

ตารางที่ ก.11 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Infrastructure & Virtualization Security

คำศัพท์		
Related Concept	Activity	Product
Access Configuration	Access Management	Architectural Framework
Application Security Architecture	Ajax Testing	Information System Documentation
Assurance Program	Authentication Testing	Provision Of Access Policies
Audit Logging	Authorization Testing	
Authentication	Business Logic Testing	
Base Controls	Change Detection	
Business Continuity	Code Review	
CCM	Configuration Management Testing	
Clock Synchronization	Cryptographic Key Management	
COBIT	Data Protection	
Complete Mediation	Data Validation Testing	
Compliance Building Blocks	Denial Of Service Testing	
Compliance Risk	Identification Maintenance Configuration Items	
Denial Of Service	Infrastructure Management	
Disaster Recovery	Interoperability Testing	
Economy Of Mechanism	Log Monitoring	
Elevation Of privilege	Logical Access Controls	
Entitlement	Management Interfaces	
Establishing a Physical Security Function	Monitoring	
Fail Safe	Monitoring Applications	
Human Resources Physical Security	Monitoring For Compromise	
Hypervisor Hardening	Monitoring For Malicious Use	
Identity	Monitoring For Policy Violations	
Information Disclosure	Open Design	
Information Security Program	Penetration Testing	
Intrusion Detection	Performance Monitoring	
Isolation Failure	Protection Security Technology	
Lack of Control	Security Testing	
Lack Of Manageability	Session Management Testing	
Lack Of Visibility	Systems Management	
Least Common Mechanism	vMotion Data Protection	
Least Privilege	Vulnerability Management	
Loss Of Governance	Web Service Testing	
Manage Performance Capacity		
Network Security		
Non-Production Environments		
OS Hardening		

ตารางที่ ก.11 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Infrastructure & Virtualization Security (ต่อ)

คำศัพท์		
Related Concept	Activity	Product
Production Environments		
Quantitative Improvement		
Repudiation		
Risk Assessment		
Risks And Solutions		
SDLC Security Technology Features		
SDLC Security Technology Tools		
Security Incident Definition		
Segmentation		
Segregation of Duties		
Spoofing		
Surveillance		
Tampering		
Traditional Security		
Transmitted Personal Information		
Virtualization		
VM Security		
VMM Security		
Weakest Link		
Wireless Security		

ตารางที่ ข.12 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Interoperability & Portability

คำศัพท์		
Related Concept	Activity	Product
Contracts		
Data Request		
Electronic Discovery		
Interoperability		
Legal Issues		
Portability		
Standardized Network Protocols		
Virtualization		

ตารางที่ ก.13 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Mobile Security

คำศัพท์		
Related Concept	Activity	Product
Anti-Malware	Device Management	
Application Stores		
Approved Applications		
Approved Software BYOD		
Cloud Based Services		
Compatibility		
Device Eligibility		
Device Inventory		
Encrypt		
Jailbreaking		
Lockout Screen		
Passwords		
Remote Wipe		
Rooting		
Security Patches		
Training Awareness		

ตารางที่ ก.14 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Security Incident Management, E-Discovery & Cloud Forensics

คำศัพท์		
Related Concept	Activity	Product
CCM	Audit Management	Incident Reporting
Communication Individuals	Authority Maintenance	Maintenance Risk Action plan
Communication Third Parties	Breach Management	
Contractual Compliance Requirements	Complaint Process	
Cooperate Governance	Compliance Management	
Governance	Contact Maintenance	
Identification External Legal	Dispute Process	
Incident Response Metrics	Enterprise Risk Management	
Instances of Noncompliance	Incident Management	
Misuse Personal Information Third Party	Incident Response Legal Preparation	
Offsite Backup Storage	Inquiry Process	
Regulatory	Monitoring Risk Action Plan	
Risk Assessment	Privacy Awareness Training	
Security Incident Definition	Privacy Incident	
	Protection Personal Information	

ตารางที่ ก.15 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Supply Chain Management, Transparency and Accountability

คำศัพท์		
Related Concept	Activity	Product
CCM	Audit Management	Incident Reporting
Collection Third Parties	Compliance Management	Consistency Privacy Policies
Consistency Commitments	Compliance Review	Supply Chain Agreements
Contracts	Consistency Privacy Procedures	
Cooperate Governance	Enterprise Risk Management	
Data Integrity	Internal Control Third Parties	
Data Quality	Logical Access Controls	
Electronic Discovery	Supplier Performance Monitoring	
Exchange Sensitive Data	Supply Chain Governance Reviews	
Governance		
Identification Supplier Relationships		
Infrastructure Services		
Instances of Noncompliance		
Misuse Personal Information Third Party		
Network Security		
Network Services		
Provider Internal Assessments		
Supply Chain Metrics		
Third Party Assessment		
Third Party Audits		
Transmitted Personal Information		

ตารางที่ ก.16 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Threat and Vulnerability Management

คำศัพท์		
Related Concept	Activity	Product
Access Configuration	Access Management	Provision Of Access Policies
Anti-Virus	Ajax Testing	
Application Security Architecture	Authentication Testing	
Assurance Program	Authorization Testing	
Authentication	Business Logic Testing	
CCM	Change Standards Procedures	
Complete Mediation	Code Review	
Compliance Building Blocks	Configuration Management Testing	
Compliance Risk	Data Protection	
Cooperate Governance	Data Validation Testing	
Denial Of Service	Denial Of Service Testing	
Detection Correction	Enterprise Risk Management	
Economy Of Mechanism	Infrastructure Maintenance	
Elevation Of privilege	Infrastructure Management	
Entitlement	Interoperability Testing	
Fail Safe	Log Monitoring	
Governance	Logical Access Controls	
Identity	Malicious Software Prevention	
Information Disclosure	Management Interfaces	
Isolation Failure	Monitoring Applications	
Lack of Control	Monitoring For Compromise	
Lack Of Manageability	Monitoring For Malicious Use	
Lack Of Visibility	Monitoring For Policy Violations	
Least Common Mechanism	Open Design	
Least Privilege	Patch Management	
Loss Of Governance	Penetration Testing	
Malicious Software	Performance Monitoring	
Mobile Code	Security Testing	
Quantitative Improvement	Session Management Testing	
Repudiation	Systems Management	
Risks And Solutions	Testing Security Safeguards	
SDLC Security Technology Features	Web Service Testing	
SDLC Security Technology Tools		
Segregation of Duties		
Spoofing		
Tampering		
Vulnerabilities		
Weakest Link		

ภาคผนวก ข. คำศัพท์จากหน้าเว็บผู้ให้บริการ

ตารางที่ ข.1 คำศัพท์ของผู้ให้บริการคลาวด์ Amazon ที่ถูกสกัดออกมา

คำศัพท์	
application security	key management
application stores	least privilege
audit controls	management program
audit logging	monitoring applications
audit management	network security
authentication	passwords
authorization	pci
authorization testing	penetration testing
coding vulnerabilities	personal information
compliance management	physical access controls
compliance risk	portability
compliance with security standards	risk response
csa	security assessment
data protection	security authorization
data security	security management controls
denial of service	surveillance
denial of service protection	systems management
disaster recovery	systems security management
encrypt	third party assessment
fedramp	third party audits
hipaa	user access
identity	vulnerabilities
incident response	vulnerability management
independent audits	workspace
information architecture	
information management	
information security architecture	

ตารางที่ ข.2 คำศัพท์ของผู้ให้บริการคลาวด์ Google ที่ถูกสกัดออกมา

คำศัพท์	
access control	integrity
addressing security	it continuity plans
application security	least privilege
asset management	log files
authentication	maintain application software
authorization	management of infrastructures
authorization policies	management of procedures
business continuity	management of systems
cryptography	monitoring
data center operations	network security
data integrity	network services
data request	nist
data security	passwords
disaster recovery	physical access controls
employment agreements	policy reviews
encrypt	security protocols
environmental risks	software development processes
incident management	systems management
incident response	systems security management
information security program	third party access
information system monitoring	vulnerabilities
infrastructure management	vulnerability management

ตารางที่ ข.3 คำศัพท์ของผู้ให้บริการคลาวด์ Salesforce ที่ถูกสกัดออกมา

คำศัพท์	
access control	iso 27001
addressing security	least privilege
application security	log files
authentication	monitoring
authorization	network security
coding vulnerabilities	nist
connection time	passwords
contracts	personal information
data integrity	privacy of personal information
data request	privacy policies
data security	rooting
encrypt	security assessment
governance	security testing
identity	segregation of duties
information governance	user access
integrity	vulnerabilities
intrusion detection	

ตารางที่ ข.4 คำศัพท์ของผู้ให้บริการคลาวด์ Box ที่ถูกสกัดออกมา

คำศัพท์	
access control	nist
authentication	passwords
communication to third parties	penetration testing
contracts	policy reviews
data protection	privacy of personal information
data security	privacy policies
encrypt	protection of personal information
hipaa	security testing
identity	systems management
information disclosure	third party access
intrusion detection	user access
monitoring	

ตารางที่ ข.5 คำศัพท์ของผู้ให้บริการคลาวด์ Azure ที่ถูกสกัดออกมา

คำศัพท์	
access control	identity
access management	independent audits
application security	information management
assurance program	information security program
audit controls	infrastructure services
authentication	iso 27001
authorization	management program
business continuity	monitoring
ccm	network security
compliance management	network services
compliance risk	nist
contracts	pci
control framework	penetration testing
csa	personal information
customer access requirements	provision management
data center operations	regulatory
data flow	security assessment
data protection	security authorization
data request	security testing
data security	third party audits
fedramp	user access
hipaa	

ประวัติผู้เขียนวิทยานิพนธ์

นายณัฐพงศ์ ภุมวารพฤษภ์ เกิดเมื่อวันที่ 10 พฤษภาคม พ.ศ. 2532 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาระดับปริญญาวิทยาศาสตรบัณฑิต สาขาศาสตร์คอมพิวเตอร์ จากคณะวิทยาศาสตร์ มหาวิทยาลัยธรรมศาสตร์ และได้เข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมซอฟต์แวร์ ณ ภาควิชาคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัยในปีการศึกษา 2555