การประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของบริการจัดเก็บข้อมูลบนคลาวด์

นายชัชวาลย์ คำหวาน

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2558

Risk of Privacy Loss Assessment of Cloud Storage Services

Mr. Chatchawan Kamwan

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Computer Science

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2015

หัวข้อวิทยานิพนธ์	การประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของบริการจัดเก็บข้อมูลบนคลาวด์
โดย	นายชัชวาลย์ คำหวาน
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร. ทวิตีย์ เสนีวงศ์ ณ อยุธยา

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร. บัณฑิต เอื้ออาภรณ์)

คณะกรรมการสอบวิทยานิพนธ์

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

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

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

ชัชวาลย์ คำหวาน : การประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของบริการจัดเก็บข้อมูลบนคลาวด์ (Risk of Privacy Loss Assessment of Cloud Storage Services) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: รศ. ดร. ทวิตีย์ เสนีวงศ์ ณ อยุธยา, 85 หน้า.

บริการจัดเก็บข้อมูลบนคลาวด์มีคุณลักษณะที่เหมาะกับการใช้งานทั้งในรูปแบบส่วนบุคคลและองค์กร เนื่องจากข้อมูลของผู้ใช้บริการสามารถจัดเก็บร่วมกันบนหน่วยเก็บข้อมูลของผู้ให้บริการคลาวด์ โดยที่ผู้ใช้บริการสามารถเข้าถึงและจัดการข้อมูลได้ทุกที่โดยผ่านการเชื่อมต่อทางอินเทอร์เน็ต แม้กระนั้นก็ตามการป้องกันความเป็นส่วนตัวของข้อมูลเป็นอีกหนึ่งประเด็นที่เป็นปัญหาเนื่องจากในขณะเลือกผู้ให้บริการคลาวด์ ผู้ใช้บริการมักมีความกังวลว่าผู้ให้บริการมีการจัดการข้อมูลส่วนบุคคลอย่างไร เพื่อช่วยผู้ใช้บริการในการเลือกบริการจัดเก็บข้อมูล วิทยานิพนธ์นี้เสนอวิธีการประเมินความเสี่ยงในด้านการสูญเสียความเป็นส่วนตัวเมื่อข้อมูลของผู้ใช้บริการถูกจัดเก็บไว้กับผู้ให้บริการบนคลาวด์ ความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวจะพิจารณาจากสองแง่มุม แง่มุมแรกคือความอ่อนไหวของข้อมูลส่วนบุคคลที่ต้องการจัดเก็บบนคลาวด์และความอ่อนไหวของข้อมูลส่วนบุคคลของผู้ใช้บริการที่ถูกร้องขอโดยผู้ให้บริการเมื่อลงทะเบียนเข้าใช้งานจะมีส่วนทำให้เกิดความเสี่ยง แง่มุมที่สองคือการขาดความโปร่งใสในด้านการควบคุมความเป็นส่วนตัวสามารถถือเป็นปัจจัยเสี่ยงได้ หากผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์ไม่สามารถแสดงให้เห็นได้อย่างเพียงพอว่ามีการปฏิบัติตามหลักการด้านความเป็นส่วนตัวต่าง ๆ ที่จำเป็น วิธีที่เสนอจะช่วยให้ผู้ใช้บริการสามารถประเมินระดับความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์รายต่าง ๆ ได้ ผู้วิจัยได้นำเสนอการประยุกต์วิธีการดังกล่าวกับกรณีศึกษาขององค์กรแห่งหนึ่งซึ่งต้องการเลือกผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์เพื่อจัดเก็บข้อมูลองค์กร

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

ปีการศึกษา 2558

5670913421 : MAJOR COMPUTER SCIENCE
KEYWORDS:

CHATCHAWAN KAMWAN: Risk of Privacy Loss Assessment of Cloud Storage Services. ADVISOR: ASSOC. PROF. TWITTIE SENIVONGSE, Ph.D., 85 pp.

Cloud storage services have promising characteristics for personal and corporate use as consumers' data can be stored on shared pools of storage hosted by cloud providers, while consumers can access and manage their data anywhere via an Internet connection. Nevertheless, protection of data privacy is one of the major issues, and at the time of storage service selection, prospective consumers are concerned with how the cloud storage providers handle their personal data. To help a consumer with storage service selection, this thesis proposes a methodology to assess the risk of privacy loss when consumer data are stored with a particular cloud storage service. The risk of privacy loss is viewed from two aspects. First, sensitivity of the personal data to be stored in the cloud and sensitivity of consumers' personal data requested at the time of service registration can contribute to the risk. Second, lack of privacy control transparency can be a risk factor if the cloud storage provider inadequately show the necessary privacy principles that are practiced. The proposed methodology can assist the consumers when determining the risk levels of privacy loss of different cloud storage services. We present the application of the methodology to a case of an organization selecting a cloud storage service to host its corporate data.

Department: Computer Engineering Student's Signature .....
Field of Study: Computer Science Advisor's Signature .....
Academic Year: 2015

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลงด้วยความกรุณาอย่างสูงของ รองศาสตรจารย์ ดร. ทวิตีย์ เสนีวงศ์ ณ อยุธยา อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่กรุณาให้คำปรึกษา แนะนำแนวทางการวิจัย ตรวจทานงานวิจัย และแนะแนวทางการแก้ไขปัญหาจากงานวิจัย ตลอดจนมีความมีเมตตาในการให้ความรู้ที่เป็นประโยชน์ในการทำงานวิจัย ทำให้งานวิจัยสำเร็จลุล่วงไปด้วยดี ขอขอบพระคุณอาจารย์เป็นอย่างสูง ณ ที่นี้

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

ขอขอบพระคุณอาจารย์ทุกท่านที่ให้ความรู้ สั่งสอน และให้คำแนะนำที่เป็นประโยชน์จนสามารถนำมาใช้ในการทำวิทยานิพนธ์ได้

ขอขอบพระคุณบิดาและมารดาที่ให้โอกาส กำลังใจในการเรียน สั่งสอน และสนับสนุนให้ข้าพเจ้าหลาย ๆ ด้าน จนข้าพเจ้าประสบผลสำเร็จ

ขอบคุณเพื่อนนิสิตวิทยาศาสตร์คอมพิวเตอร์ วิศวกรรมซอฟต์แวร์ และวิศวกรรมคอมพิวเตอร์ ที่คอยช่วยเหลือในหลาย ๆ เรื่องเช่นข่าวสารมหาวิทยาลัย แหล่งข้อมูลงานประชุมวิชาการ เป็นต้น

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ง

บทคัดย่อภาษาอังกฤษ ..... จ

กิตติกรรมประกาศ ..... ฉ

สารบัญ ..... ช

สารบัญตาราง ..... ญ

สารบัญรูปภาพ ..... ฐ

บทที่ 1 1

บทนำ 1

1.1 ความเป็นมาและความสำคัญของปัญหา 1

1.2 วัตถุประสงค์งานวิจัย 3

1.3 ขอบเขตการวิจัย 3

1.4 ขั้นตอนการวิจัย 4

1.5 ประโยชน์ที่คาดว่าจะได้รับ 4

1.6 ผลงานตีพิมพ์ 4

บทที่ 2 5

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง 5

2.1 แนวคิดและทฤษฎี 5

2.1.1 บริการจัดเก็บข้อมูลบนคลาวด์ 5

2.1.2 ความอ่อนไหวของข้อมูล 5

2.1.3 ความเป็นส่วนตัว 7

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง 10

บทที่ 3 16

หน้า

การประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของบริการจัดเก็บข้อมูลบนคลาวด์ 16
3.1 การประเมินระดับความอ่อนไหวของข้อมูลผู้ใช้บริการ 16
3.1.1 การประเมินระดับความอ่อนไหวของข้อมูลที่ผู้ใช้บริการเอาไปจัดเก็บบนคลาวด์..... 17
3.1.2 การประเมินระดับความอ่อนไหวของข้อมูลส่วนบุคคลที่ผู้ให้บริการร้องขอจากผู้ใช้บริการในการเข้าใช้ 24
3.1.3 การประเมินระดับความอ่อนไหวของข้อมูลผู้ใช้บริการ..... 28
3.2 การประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการ 29
3.3 การประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว 40
3.4 การทวนสอบวิธีการประเมิน 41
3.5 การพัฒนาระบบสนับสนุนการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของการใช้บริการจัดเก็บข้อมูลบนคลาวด์..... 43
บทที่ 4 53
การทดสอบและการประเมินผลการวิจัย 53
4.1 การทดลองการประเมินระดับความอ่อนไหวของข้อมูลผู้ใช้บริการ 53
4.2 การทดลองการประเมินระดับความอ่อนไหวของข้อมูลส่วนบุคคลที่ผู้ให้บริการร้องขอจากผู้ใช้บริการในการเข้าใช้..... 56
4.3 การทดลองการประเมินระดับความอ่อนไหวของข้อมูลผู้ใช้บริการ 60
4.4 การทดลองการประเมินความโปร่งใสในด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการ 61
4.5 การทดลองการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว 62
4.6 การวิเคราะห์ค่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว 63
4.7 การทดสอบความสัมพันธ์เชิงสถิติระหว่างความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวกับการไม่ปฏิบัติตามแนวปฏิบัติด้านความมั่นคง 66
บทที่ 5 69
สรุปผลการวิจัย 69

หน้า

5.1 สรุปผลการวิจัย 69
5.2 ปัญหาและข้อจำกัด 69
5.3 ข้อควรระวัง 70
5.4 แนวทางการวิจัยต่อไป 70
รายการอ้างอิง 71
ภาคผนวก ก 74
ข้อมูลสำหรับการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัว 74
ภาคผนวก ข 84
การปฏิบัติตามและไม่ปฏิบัติตามแนวปฏิบัติด้านความมั่นคง CCM 84
ประวัติผู้เขียนวิทยานิพนธ์ 85

สารบัญตาราง

หน้า

ตารางที่ 3.1 ระดับผลกระทบต่อองค์กรและระดับความอ่อนไหวของข้อมูลแต่ละประเภท (ขยายจาก [6])..... 18
ตารางที่ 3.1 ระดับผลกระทบต่อองค์กรและระดับความอ่อนไหวของข้อมูลแต่ละประเภท (ขยายจาก [6]) (ต่อ)..... 19
ตารางที่ 3.1 ระดับผลกระทบต่อองค์กรและระดับความอ่อนไหวของข้อมูลแต่ละประเภท (ขยายจาก [6]) (ต่อ)..... 20
ตารางที่ 3.1 ระดับผลกระทบต่อองค์กรและระดับความอ่อนไหวของข้อมูลแต่ละประเภท (ขยายจาก [6]) (ต่อ)..... 21
ตารางที่ 3.1 ระดับผลกระทบต่อองค์กรและระดับความอ่อนไหวของข้อมูลแต่ละประเภท (ขยายจาก [6]) (ต่อ)..... 22
ตารางที่ 3.1 ระดับผลกระทบต่อองค์กรและระดับความอ่อนไหวของข้อมูลแต่ละประเภท (ขยายจาก [6]) (ต่อ)..... 23
ตารางที่ 3.2 *ตัวอย่าง Cross Table ของ Microsoft Azure* 25
ตารางที่ 3.3 ตัวอย่างค่าความอ่อนไหวของข้อมูลที่ผู้ให้บริการ Microsoft Azure ร้องขอเพื่อเข้าใช้บริการ..... 28
ตารางที่ 3.4 Cloud Privacy Control Questionnaire (CPCQ)..... 30
ตารางที่ 3.4 Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)..... 31
ตารางที่ 3.4 Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)..... 32
ตารางที่ 3.4 Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)..... 33
ตารางที่ 3.4 Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)..... 34
ตารางที่ 3.4 Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)..... 35
ตารางที่ 3.4 Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)..... 36
ตารางที่ 3.4 Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)..... 37
ตารางที่ 3.4 Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)..... 38
ตารางที่ 4.1 คะแนนความอ่อนไหวของข้อมูลที่จะนำขึ้นไปเก็บบนคลาวด์แยกตามแผนก..... 54
ตารางที่ 4.2 Cross Table ของ Dropbox Business..... 56

หน้า

ตารางที่ 4.3 ค่าความอ่อนไหวของข้อมูลของ Dropbox Business.....57
ตารางที่ 4.4 Cross Table ของ Citrix ShareFile.....57
ตารางที่ 4.5 ค่าความอ่อนไหวของข้อมูลของ Citrix ShareFile.....58
ตารางที่ 4.6 Cross Table ของ Verizon Enterprise Solution.....58
ตารางที่ 4.7 ค่าความอ่อนไหวของข้อมูลของ Verizon Enterprise Solution.....59
ตารางที่ 4.8 Cross Table ของ SoftLayer.....59
ตารางที่ 4.9 คะแนนความอ่อนไหวของข้อมูลที่ผู้ให้บริการร้องขอแยกตามผู้ให้บริการ.....60
ตารางที่ 4.10 คะแนนความอ่อนไหวของข้อมูลที่ผู้ให้บริการร้องขอแยกตามผู้ให้บริการ.....60
ตารางที่ 4.11 สรุปค่าความอ่อนไหวของข้อมูลของผู้ใช้บริการ จากตัวอย่างการทดลอง 5 แผนกและ 5 ผู้ให้บริการคลาวด์.....61
ตารางที่ 4.12 คะแนนความโปร่งใสและคะแนนความเสี่ยงด้านการจัดการความเป็นส่วนตัวของผู้ให้บริการแยกตามผู้ให้บริการ.....61
ตารางที่ 4.13 คะแนนความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของผู้ให้บริการคลาวด์แยกตามผู้ให้บริการ.....62
ตารางที่ 4.14 ค่าคะแนนที่ใช้ในการวิเคราะห์.....63
ตารางที่ 4.15 ค่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวที่เป็นไปได้.....64
ตารางที่ 4.15 ค่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวที่เป็นไปได้ (ต่อ).....65
ตารางที่ 4.16 ตารางสำหรับหาค่าสหสัมพันธ์ของความเกี่ยวข้องระหว่างการทำตาม CCM และความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์.....67
ตารางที่ ก2.1 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Microsoft Azure.....74
ตารางที่ ก2.1 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Microsoft Azure (ต่อ).....75
ตารางที่ ก2.1 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Microsoft Azure (ต่อ).....76
ตารางที่ ก2.2 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Dropbox Business.....76

หน้า

ตารางที่ ก2.2 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Dropbox Business (ต่อ).....77
ตารางที่ ก2.2 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Dropbox Business (ต่อ).....78
ตารางที่ ก2.3 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Citrix ShareFile.....78
ตารางที่ ก2.3 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Citrix ShareFile (ต่อ).....79
ตารางที่ ก2.3 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Citrix ShareFile (ต่อ).....80
ตารางที่ ก2.4 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Verizon Business Solution.....80
ตารางที่ ก2.4 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Verizon Business Solution (ต่อ).....81
ตารางที่ ก2.4 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Verizon Business Solution (ต่อ).....82
ตารางที่ ก2.5 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ SolfLayer.....82
ตารางที่ ก2.5 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ SolfLayer (ต่อ).....83
ตารางที่ ข.1.1 การปฏิบัติตามและไม่ปฏิบัติตามแนวปฏิบัติด้านความมั่นคง CCM.....84

สารบัญรูปภาพ

หน้า

ภาพที่ 3.1 ภาพรวมการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว.....16
ภาพที่ 3.2 ระบบการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์.....44
ภาพที่ 3.3 หน้าหลักของโปรแกรมประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์.....46
ภาพที่ 3.4 หน้าการประเมินค่าความอ่อนไหวของข้อมูลที่จะนำไปจัดเก็บบนคลาวด์ส่วนแรก.....47
ภาพที่ 3.5 หน้าการประเมินค่าความอ่อนไหวของข้อมูลที่จะนำไปจัดเก็บบนคลาวด์ส่วนที่สอง.....48
ภาพที่ 3.6 หน้าการประเมินความอ่อนไหวของข้อมูลที่ถูกร้องขอโดยผู้ให้บริการเพื่อเข้าใช้บริการ.....49
ภาพที่ 3.7 หน้าส่วนการประเมินความโปร่งใสด้านการจัดการความเป็นส่วนตัวของผู้ให้บริการส่วนแรก.....50
ภาพที่ 3.8 หน้าส่วนการประเมินความโปร่งใสด้านการจัดการความเป็นส่วนตัวของผู้ให้บริการส่วนที่สอง.....50
ภาพที่ 3.9 หน้าส่วนการประเมินความโปร่งใสด้านการจัดการความเป็นส่วนตัวของผู้ให้บริการส่วนที่สาม.....51
ภาพที่ 3.10 หน้าหลักแสดงผลการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์.....52
ภาพที่ 4.1 กราฟแสดงความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์โดยแยกตามแผนกข้อมูลและแยกตามผู้ให้บริการ.....62

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การประมวลผลแบบคลาวด์ [1] เป็นเทคโนโลยีการใช้งานทรัพยากรคอมพิวเตอร์ต่าง ๆ เช่น การประมวลผล การจัดเก็บข้อมูล ระบบปฏิบัติการ เป็นต้น ผ่านทางอินเทอร์เน็ตที่มีความยืดหยุ่นในการใช้งาน ช่วยประหยัดการลงทุน ใช้ทรัพยากรทางด้านฮาร์ดแวร์น้อยลง ง่ายต่อการจัดการ การให้บริการของการประมวลผลแบบคลาวด์มีหลากหลายรูปแบบแบ่งตามโมเดลการให้บริการ ได้แก่

1. การให้บริการซอฟต์แวร์ (Software as a Service (SaaS)) คือ การให้บริการประมวลผลแอปพลิเคชันบนระบบของผู้ให้บริการ
2. การให้บริการแพลตฟอร์ม (Platform as a Service (PaaS)) คือ การให้บริการประมวลผลที่มีระบบปฏิบัติการและระบบแอปพลิเคชันสนับสนุน
3. การให้บริการโครงสร้างพื้นฐาน (Infrastructure as a Service (IaaS)) คือ การให้บริการเพื่อสนับสนุนการประมวลผลทรัพยากรพื้นฐานของผู้ใช้บริการ
4. การให้บริการด้านการสื่อสาร (Unified Communications as a Service) คือการให้บริการประมวลผลด้านการสื่อสาร เช่น อีเมล การประชุมทางไกล เป็นต้น

หากแบ่งตามโมเดลการปรับใช้งาน ได้แก่

1. คลาวด์แบบส่วนตัว (Private cloud) เป็นการให้บริการคลาวด์โดยผู้ใช้บริการไม่มีการใช้ทรัพยากรใด ๆ ร่วมกับผู้ใช้บริการรายอื่น
2. คลาวด์แบบสาธารณะ (Public cloud) เป็นการให้บริการคลาวด์โดยผู้ใช้บริการมีการใช้ทรัพยากรร่วมกับผู้ใช้บริการคนอื่น ๆ แต่มีการจัดการการเข้าถึงที่ถูกต้องให้ผู้ใช้บริการ
3. คลาวด์แบบผสม (Hybrid cloud) เป็นการให้บริการแบบผสมคือมีทั้งคลาวด์แบบส่วนตัวและคลาวด์แบบสาธารณะ
4. อื่น ๆ คือการให้บริการประมวลผลตามประเภทที่จัดกลุ่มแบบพิเศษ เช่น คลาวด์แบบกลุ่ม (Community Cloud) คลาวด์แบบแบ่งปัน (Distributed Cloud)

บริการจัดเก็บข้อมูลบนคลาวด์ (Cloud Storage) [2] คือการบริหารจัดการ เช่น จัดเก็บ เพิ่ม ลบ โอนย้ายข้อมูลผ่านเครือข่ายอินเทอร์เน็ต โดยผู้ให้บริการจัดสรรพื้นที่สำหรับจัดเก็บข้อมูลและส่วนต่อประสานสำหรับจัดการข้อมูลให้ผู้ใช้บริการ เป็นคลาวด์เทคโนโลยีที่ได้รับความนิยมเพราะสามารถ

เก็บข้อมูลไว้บนคลาวด์ สามารถเชื่อมต่อได้ทุก ๆ ที่ ที่สามารถเชื่อมต่ออินเทอร์เน็ตทำให้สะดวกสบายในการใช้งานโดยไม่ต้องพึ่งพาอุปกรณ์จัดเก็บข้อมูลใด ๆ เลย

การเลือกผู้ให้บริการนั้นควรมีการประเมินผู้ให้บริการในหลาย ๆ ด้านเช่น ความมั่นคงของข้อมูล ความเป็นส่วนตัว การบริการ และอื่น ๆ ว่ามีความเหมาะสมกับการใช้งานโดยผู้ใช้บริการหรือไม่ ความเป็นส่วนตัวของข้อมูล (Data Privacy) เป็นปัจจัยหนึ่งที่มีความสำคัญเพราะมันคือตัวบ่งบอกว่าผู้ให้บริการมีการจัดการรักษาความเป็นส่วนตัวของข้อมูลผู้ใช้บริการอยู่ในระดับใด ผู้ใช้บริการจะให้ความสำคัญกับเรื่องระดับความเป็นส่วนตัวของข้อมูลส่วนบุคคล (Personal Data) เป็นพิเศษเพราะข้อมูลส่วนบุคคลโดยส่วนมากนั้นจะเป็นข้อมูลที่เป็นความลับและเป็นส่วนตัว ดังนั้นความเป็นส่วนตัวของข้อมูลจึงถือว่ามีความสำคัญมากสำหรับการจัดเก็บข้อมูลบนคลาวด์ ผู้วิจัยมีแนวคิดในการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว (Risk of Privacy Loss Assessment) ของผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์ โดยพิจารณาทั้งลักษณะข้อมูลที่จะนำไปจัดเก็บและการจัดการด้านความเป็นส่วนตัวโดยผู้ให้บริการ กล่าวคือการประเมินจะแบ่งเป็นสองส่วนได้แก่

1. การประเมินระดับความอ่อนไหวของข้อมูลผู้ใช้บริการ

   จะทำการประเมินโดยให้ผู้ใช้บริการประเมินระดับความอ่อนไหวของข้อมูล (Data Sensitivity) ของผู้ใช้บริการเอง โดยมีการประเมินสองส่วนคือ

   1.1 ข้อมูลที่ผู้ใช้บริการเอาไปจัดเก็บบนคลาวด์ เช่น ไฟล์รูปภาพ เอกสารทางธุรกิจ ข้อมูลทางการบัญชี เป็นต้น

   1.2 ข้อมูลส่วนบุคคลที่ผู้ให้บริการร้องขอจากผู้ใช้บริการในการเข้าใช้บริการ เช่น ชื่อ ที่อยู่ เลขที่บัตรเครดิต เป็นต้น

2. การประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการ

   ส่วนนี้จะมีการจัดทำชุดคำถามประเมินระดับความโปร่งใสด้านการควบคุมความเป็นส่วนตัว (Privacy Control Transparency) เพื่อประเมินว่าผู้ให้บริการมีการเปิดเผยข้อมูลเกี่ยวกับการควบคุมอยู่ในระดับใด

จากวิธีการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวที่ได้ ผู้ใช้บริการสามารถนำไปใช้พิจารณาในการเลือกผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์ที่เหมาะสมกับข้อมูลที่จะจัดเก็บต่อไป

1.2 วัตถุประสงค์งานวิจัย

1. เพื่อเสนอวิธีการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของการใช้บริการจัดเก็บข้อมูลบนคลาวด์
2. เพื่อพัฒนาเครื่องมือสนับสนุนการประเมิน

1.3 ขอบเขตการวิจัย

1. เสนอวิธีการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของบริการจัดเก็บข้อมูลบนคลาวด์ ซึ่งประเมินจาก
    1.1 ความอ่อนไหวของข้อมูลที่ผู้ใช้บริการนำไปจัดเก็บบนคลาวด์
    1.2 ความอ่อนไหวของข้อมูลที่ผู้ให้บริการร้องขอเพื่อการเปิดใช้บริการ
    1.3 ความโปร่งใสของการควบคุมความเป็นส่วนตัวของผู้ให้บริการคลาวด์
2. การประเมินความอ่อนไหวของข้อมูลที่ผู้ใช้บริการนำไปจัดเก็บบนคลาวด์จะอิงจากผลกระทบต่อองค์กรที่เกิดจากความเสียหายของข้อมูลประเภทต่าง ๆ ซึ่งกำหนดโดยเอกสาร Information Security ของ NIST [13]
3. กำหนดตาราง Cross Table สำหรับใช้ในการประเมินข้อมูลของผู้ใช้บริการที่ผู้ให้บริการร้องขอจากการพิจารณาตัวอย่างผู้ให้บริการ ทั้งนี้ตารางสามารถปรับได้ตามความเหมาะสมของผู้ใช้บริการแต่ละราย
4. ประมวลชุดคำถามในการประเมินการปฏิบัติตามแนวปฏิบัติด้านความเป็นส่วนตัวของผู้ให้บริการ จากเอกสารมาตรฐาน เช่น Privacy Level Agreement [11], Australian Privacy Principle [12], Security and Privacy Controls for Federal Information Systems and Organizations [13]
5. พัฒนาโปรแกรมเครื่องมือสนับสนุนที่ผู้ใช้บริการสามารถระบุประเภทข้อมูลที่จะนำไปจัดเก็บบนคลาวด์ และข้อมูลที่ผู้ให้บริการร้องขอ และสามารถให้คะแนนการปฏิบัติตามการควบคุมความเป็นส่วนตัวของผู้ให้บริการ เครื่องมือจะคำนวณคะแนนความเสี่ยง และแสดงผลได้
6. ทวนสอบวิธีการและทดลองกับองค์กรกรณีศึกษาโดยประเมินผู้ให้บริการอย่างน้อย 5 ราย ซึ่งมีลักษณะแตกต่างกัน เช่น ได้รับการจัดลำดับแตกต่างกันจากเว็บไซต์จัดลำดับผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์ เป็นต้น

1.4 ขั้นตอนการวิจัย

1. ศึกษาทฤษฎีที่เกี่ยวข้องที่ใช้ในการวิจัยเพื่อประเมินความเสี่ยงการสูญเสียด้านความเป็นส่วนตัว
2. กำหนดแนวทางและวิธีการทางการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว
3. ออกแบบและพัฒนาเครื่องมือที่ใช้ในการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว
4. ทำการทวนสอบวิธีการและทดลองกับองค์กรกรณีศึกษา
5. สรุปผลการทดสอบและปรับปรุงวิธีการ
6. จัดทำบทความวิจัยและวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้วิธีการประเมินความเสี่ยงในด้านการสูญเสียความเป็นส่วนตัวของการใช้บริการจัดเก็บข้อมูลบนคลาวด์และเครื่องมือสนับสนุน
2. ผู้ใช้บริการสามารถปรับใช้วิธีการประเมินได้ตามความเหมาะสมในการเปรียบเทียบเพื่อเลือกผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์มาใช้งาน
3. ผู้ให้บริการสามารถใช้วิธีการและเครื่องมือในการประเมินตนเองเพื่อนำมาปรับปรุงนโยบายความเป็นส่วนตัวของระบบผู้ให้บริการได้

1.6 ผลงานตีพิมพ์

เรื่อง Risk of Privacy Loss Assessment of Cloud Storage Services โดย Chatchawan KAMWAN, Twittie SENIVONGSE ในการประชุมวิชาการ The 18th International Conference on Advanced Communications Technology (ICACT2016) ซึ่งจัดขึ้น ณ PyeongChang, Korea ระหว่างวันที่ 31 มกราคม ถึง 3 กุมภาพันธ์ 2559

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎี

2.1.1 บริการจัดเก็บข้อมูลบนคลาวด์

บริการจัดเก็บข้อมูลบนคลาวด์ (Cloud Storage) [2] เป็นเทคโนโลยีบริหารจัดการการจัดเก็บและดูแลรักษาข้อมูลผ่านระบบอินเทอร์เน็ต เป็นระบบที่ได้รับความนิยมมากในปัจจุบัน โดยอาศัยเทคโนโลยีการบริหารและจัดการระยะไกลเข้ามาช่วยในการบริการและจัดการข้อมูล ทำให้ง่ายต่อการใช้งาน

ปัจจุบันบริการจัดเก็บข้อมูลบนคลาวด์มีการพัฒนาเทคโนโลยีเพื่อความเหมาะสมกับการใช้งานที่หลากหลายมากขึ้นเช่น การจัดเก็บข้อมูลที่เป็นฐานข้อมูล การจัดเก็บข้อมูลที่เป็นเฉพาะด้าน เป็นต้น การประมวลผลแบบคลาวด์จะอำนวยความสะดวกในเรื่องการบริหารและจัดการฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ในการจัดเก็บข้อมูล

2.1.2 ความอ่อนไหวของข้อมูล

ความอ่อนไหวของข้อมูล (Data Sensitivity) [3, 4] หมายถึงความสำคัญและผลกระทบที่เกิดขึ้นหากข้อมูลได้รับการเปิดเผยอย่างไม่เหมาะสม เกิดความเสียหาย หรือสูญหาย ข้อมูลเหล่านั้นจะเป็นข้อมูลส่วนบุคคลหรือข้อมูลที่มีกรรมสิทธิ์ ซึ่งควรได้รับการปกป้องโดยใช้กฎหมายและจริยธรรมมาช่วย

การจำแนกประเภทข้อมูลตามระดับความอ่อนไหวสามารถแบ่งออกได้ 3 ระดับ [5]

- ต่ำ (Low) คือข้อมูลที่สามารถเปิดเผยได้ เมื่อเกิดความเสียหายหรือการสูญหายของข้อมูลแล้วมีผลกระทบกับเจ้าของข้อมูลน้อยมากหรือแทบไม่มีผลกระทบเลย เช่น เอกสารต่าง ๆ ที่สามารถเปิดเผยต่อสาธารณะได้
- ปานกลาง (Medium) คือข้อมูลที่ใช้แค่ภายในองค์กรเท่านั้น เมื่อเกิดความเสียหายหรือการสูญหายของข้อมูลแล้วมีผลกระทบกับเจ้าของข้อมูลในระดับปานกลาง เช่น เอกสารที่ใช้ภายในองค์กร อีเมล
- สูง (High) คือข้อมูลที่ใช้แค่ภายในองค์กรเท่านั้น และเป็นข้อมูลที่เป็นความลับ เมื่อเกิดความเสียหายหรือการสูญหายของข้อมูลแล้วมีผลกระทบกับเจ้าของข้อมูลในระดับสูง เช่น ข้อมูลทางการเงิน เอกสารทางธุรกิจ ข้อมูลทางกฎหมาย ข้อมูลส่วนบุคคลของพนักงาน

National Institute of Standards and Technology (NIST) ได้กำหนดระดับผลกระทบที่จะเกิดต่อองค์กรภาครัฐ [6] หากข้อมูลขององค์กรได้รับการเปิดเผย เสียหาย หรือสูญหาย โดยกำหนดกลุ่มข้อมูลในด้านการจัดการและการสนับสนุนธุรกิจและสารสนเทศขององค์กรไว้สองกลุ่มคือ

1. Services Delivery Support Information

แบ่งย่อยตามกลุ่มข้อมูลสนับสนุนการบริการ ได้ทั้งหมด 8 กลุ่มดังนี้

1. Controls and Oversight
2. Regulatory Development
3. Planning & Budgeting
4. Internal Risk Management & Mitigation
5. Revenue Collection
6. Public Affairs
7. Legislative Relations
8. General Government

2. Government Resource Management Information

แบ่งย่อยตามกลุ่มข้อมูลการจัดการทรัพยากรภาครัฐได้ 5 กลุ่มดังนี้

1. Administrative Management
2. Financial Management
3. Human Resource Management
4. Supply Chain Management
5. Information & Technology Management

NIST กำหนดระดับผลกระทบที่จะเกิดต่อองค์กรหากข้อมูลในกลุ่มต่าง ๆ ข้างต้นสูญเสียองค์ประกอบด้านความมั่นคง (Security) 3 องค์ประกอบ ได้แก่ การรักษาความลับ (Confidentiality) บูรณภาพ (Integrity) และสภาพพร้อมใช้งาน (Availability) ระดับผลกระทบจากการสูญเสียแต่ละองค์ประกอบแบ่งออกเป็น 3 ระดับคือ [8, 9]

1. ต่ำ (Low) ถ้าเกิดความสูญเสียต่อข้อมูลไม่ว่าจะเป็นการเปิดเผย สูญหาย หรือเสียหาย จะเกิดผลกระทบในวงจำกัดต่อเจ้าของข้อมูลหรือองค์กร
2. ปานกลาง (Moderate) ถ้าเกิดความสูญเสียต่อข้อมูลไม่ว่าจะเป็นการเปิดเผย สูญหาย หรือเสียหาย จะเกิดผลกระทบในระดับที่ร้ายแรงต่อเจ้าของข้อมูลหรือองค์กร

3. สูง (High) คือถ้าเกิดความสูญเสียต่อข้อมูลไม่ว่าจะเป็นการเปิดเผย สูญหาย หรือเสียหาย จะเกิดผลกระทบในระดับรุนแรงหรือหายนะต่อเจ้าของข้อมูลหรือองค์กร

เนื่องจากความอ่อนไหวของข้อมูลเกี่ยวเนื่องกับผลกระทบของข้อมูลต่อองค์กร ระดับความอ่อนไหวของข้อมูลจึงสามารถพิจารณาได้จากระดับผลกระทบเมื่อเกิดการสูญเสียองค์ประกอบด้านความมั่นคงโดยใช้หลักการ High Water Mark [7] เช่น หากข้อมูลมีระดับผลกระทบจากการสูญเสียการรักษาความลับในระดับต่ำ มีระดับผลกระทบจากการสูญเสียบูรณภาพในระดับปานกลาง และมีระดับผลกระทบจากการสูญเสียสภาพพร้อมใช้งานในระดับสูง ดังนั้นความอ่อนไหวของข้อมูลนี้จะถือว่าอยู่ในระดับสูง นอกจากนี้ NIST ยังกำหนดไว้ว่า สำหรับบางกลุ่มข้อมูล ระดับผลกระทบจากการสูญเสียองค์ประกอบด้านความมั่นคงสามารถปรับระดับขึ้นลงได้จากที่กำหนดไว้หากมีปัจจัยบางอย่างเกิดขึ้น ตัวอย่างเช่น หากข้อมูล IT Infrastructure Maintenance มีระดับผลกระทบจากการสูญเสียการรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน อยู่ในระดับต่ำทั้งหมด ดังนั้นข้อมูลนี้จะมีระดับความอ่อนไหวต่ำ แต่หากการเข้าถึงข้อมูลมีความจำเป็นเพื่อตอบสนองงานวิกฤตหรือเหตุฉุกเฉินที่เกี่ยวข้องกับความปลอดภัยของสาธารณะ เช่น Air Traffic Control ผลกระทบต่อองค์กรซึ่งเกิดจากการสูญเสียสภาพพร้อมใช้งานและทำให้ไม่สามารถเข้าถึงข้อมูลได้จะเปลี่ยนเป็นระดับสูง ซึ่งจะทำให้ระดับความอ่อนไหวของข้อมูลนี้เปลี่ยนไปเป็นระดับสูงด้วย

2.1.3 ความเป็นส่วนตัว

ความเป็นส่วนตัว (Privacy) [10] เกี่ยวข้องกับการควบคุมและป้องกันการเข้าถึงการใช้งานข้อมูลที่ไม่ถูกต้อง รวมไปถึงการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตหรือไม่ถูกต้อง การควบคุมความเป็นส่วนตัวของข้อมูลจะต้องกระทำโดยเจ้าของข้อมูลเองหรือได้รับการยินยอมจากเจ้าของข้อมูล เพื่อสามารถกำหนดความเป็นส่วนตัวของข้อมูลได้อย่างถูกต้องและเหมาะสมในการเข้าถึงข้อมูลนั้น ๆ แนวปฏิบัติด้านความเป็นส่วนตัวมีตัวอย่างดังต่อไปนี้

2.1.3.1 Privacy Level Agreement (PLA) [11] เป็นแนวปฏิบัติสำหรับให้บริการคลาวด์ในกลุ่มประเทศอียูในการบริหารและจัดการความเป็นส่วนตัวบนคลาวด์ กำหนดขึ้นโดย Cloud Security Alliance (CSA) โดยมีทั้งหมด 16 ข้อดังนี้

1. Identity of the CSP (and of representative in the EU as applicable), its role, and the contact information of the data protection officer and the information security officer
2. Categories of personal data that the customer is prohibited from sending to or processing in the cloud

3. Ways in which the data will be processed
4. Data transfer
5. Data security measures
6. Monitoring
7. Third-party audits
8. Personal data breach notification
9. Data portability, migration, and transfer back assistance
10. Data retention, restitution and deletion
11. Accountability
12. Law enforcement access
13. Cooperation
14. Complaint; dispute resolution
15. Remedies
16. CSP insurance policy

แนวปฏิบัติ 16 ข้อนี้สามารถนำไปใช้ในการจัดการรักษาความเป็นส่วนตัวโดยปรับแต่งให้เหมาะสมกับผู้ให้บริการแต่ละรายได้ เพื่อให้เกิดมาตรฐานที่เหมาะสมสำหรับการจัดการความเป็นส่วนตัวของข้อมูลสำหรับผู้ใช้บริการ

2.1.3.2 Australian Privacy Principle (APP) [12] หลักความเป็นส่วนตัวของประเทศออสเตรเลียถูกกำหนดขึ้นโดย Office of the Australian Information Commissioner เป็นหลักความเป็นส่วนตัวที่เป็นกฎหมายขั้นพื้นฐานในการจัดการความเป็นส่วนตัวของผู้ให้บริการคลาวด์ โดยจะมีการบังคับใช้ในประเทศออสเตรเลีย มีทั้งหมด 13 ข้อดังนี้

1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use or disclosure of personal information
7. Direct marketing

8. Cross-border disclosure of personal information
9. Adoption, use or disclosure of government related identifiers
10. Quality of personal information
11. Security of personal information
12. Access to personal information
13. Correction of personal information

2.1.3.3 Security and Privacy Controls for Federal Information Systems and Organizations [13] เป็นข้อกำหนดทางด้านความมั่นคงและความเป็นส่วนตัวที่ใช้ในหน่วยงานภาครัฐของรัฐบาลสหรัฐอเมริกา จัดทำโดย NIST ส่วนที่นำมาแสดงเป็นข้อกำหนดทางด้านความเป็นส่วนตัว มีทั้งหมด 8 หมวดดังนี้

AP Authority and Purpose

AP-1 Authority to Collect

AP-2 Purpose Specification

AR Accountability, Audit, and Risk Management

AR-1 Governance and Privacy Program

AR-2 Privacy Impact and Risk Assessment

AR-3 Privacy Requirements for Contractors and Service Providers

AR-4 Privacy Monitoring and Auditing

AR-5 Privacy Awareness and Training

AR-6 Privacy Reporting

AR-7 Privacy-Enhanced System Design and Development

AR-8 Accounting of Disclosures

DI Data Quality and Integrity

DI-1 Data Quality

DI-2 Data Integrity and Data Integrity Board

DM Data Minimization and Retention

DM-1 Minimization of Personally Identifiable Information

DM-2 Data Retention and Disposal

DM-3 Minimization of PII Used in Testing, Training, and Research

IP Individual Participation and Redress

IP-1 Consent

IP-2 Individual Access

IP-3 Redress

IP-4 Complaint Management

SE Security

SE-1 Inventory of Personally Identifiable Information

SE-2 Privacy Incident Response

TR Transparency

TR-1 Privacy Notice

TR-2 System of Records Notices and Privacy Act Statements

TR-3 Dissemination of Privacy Program Information

UL Use Limitation

UL-1 Internal Use

UL-2 Information Sharing with Third Parties

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง

2.2.1 การประเมินความอ่อนไหว

Injoo Jang และ Hyeong Seon Yoo [14] ได้เสนอวิธีการประเมินค่าความอ่อนไหวของข้อมูลส่วนบุคคล และ Punyaphat Chaiwongsa และ Twittie Senivongse [15] ได้ประยุกต์วิธีการไปใช้กับการประเมินค่าความอ่อนไหวของข้อมูลส่วนบุคคลที่แลกเปลี่ยนกับเว็บเซอร์วิช หลักการประเมินเริ่มจากจำแนกข้อมูลส่วนบุคคลออกตามประเภทหรือคอนเซปต์ ซึ่งมีทั้งหมด 7 กลุ่มเช่น Basic เป็นข้อมูลพื้นฐานทั่วไป, Career เป็นข้อมูลที่เกี่ยวข้องเกี่ยวกับการทำงาน, Health เป็นข้อมูลด้านสุขภาพ เป็นต้น หลังจากนั้นนำข้อมูลที่สนใจหรือแอตทริบิวต์มาทำการคำนวณหาค่าระดับความอ่อนไหวของข้อมูล โดยจะพิจารณาจากปัจจัยทั้ง 4 ข้อดังนี้

1. ระดับความเชื่อมโยง (Degree of Conjunction) คือการตรวจสอบว่าข้อมูลส่วนบุคคลที่สนใจ สามารถจัดอยู่ในคอนเซปต์ใดบ้าง นั่นคือสามารถเชื่อมโยงคอนเซปต์ใดเข้าด้วยกันได้บ้าง
2. หลักเอกลักษณ์ (Principle of Identity) คือการตรวจสอบว่าข้อมูลที่สนใจนั้นเป็นข้อมูลเอกลักษณ์หรือไม่
3. หลักความเป็นส่วนตัว (Principle of Privacy) เป็นการระบุว่าข้อมูลที่สนใจ ถือเป็นข้อมูลส่วนตัวที่ไม่ต้องการให้ผู้อื่นรู้หรือไม่
4. ค่าการอนุมาน (Value of Analogism) เป็นการระบุว่าข้อมูลที่สนใจนำไปสู่การเปิดเผยข้อมูลอื่น ๆ หรือไม่

ดังนั้นเมื่อหาค่าของระดับความเชื่อมโยง หลักเอกลักษณ์ หลักความเป็นส่วนตัว และค่าการอนุมาน ทั้งสี่องค์ประกอบสามารถประเมินความอ่อนไหวของข้อมูลที่สนใจได้ ผู้วิจัยมีแนวคิดในการนำหลักการนี้มาใช้ประเมินความอ่อนไหวของข้อมูลที่ผู้ให้บริการร้องขอจากผู้ใช้บริการ

2.2.2 แนวทางการออกแบบการจัดการความเป็นส่วนตัวสำหรับผู้ใช้บริการคลาวด์

Siani Pearson [16] ได้นำเสนอแนวทางสำหรับจัดการความเป็นส่วนตัว เมื่อมีการออกแบบระบบคลาวด์ โดยมีการกำหนดความต้องการหลักของความเป็นส่วนตัว (Key Privacy Requirements) เอาไว้คือ

1. การแจ้งเตือน ความเปิดเผย และความโปร่งใส (Notice, openness and transparency) ต้องมีการแจ้งเมื่อมีการกระทำการใด ๆ ที่เกี่ยวข้องกับข้อมูลของผู้ใช้บริการ รวมทั้งถ้ามีการเข้าถึงข้อมูลที่ไม่ถูกต้อง การสูญหาย ถูกโจมตี มีการเปลี่ยนแปลงข้อมูลของผู้ใช้บริการ เพื่อความเปิดเผยและโปร่งใส
2. ทางเลือก ความยินยอม และการควบคุม (Choice, consent and control) ผู้ใช้บริการจะต้องสามารถเลือกได้ว่าจะให้เก็บรวบรวมข้อมูลหรือไม่ ในการรวบรวมและเก็บข้อมูล การใช้ และการเปิดเผยข้อมูลต้องได้รับความยินยอมจากผู้ที่ข้อมูลนั้นกล่าวถึง
3. ขอบเขต/การทำให้น้อยที่สุด (Scope/minimization) การเก็บรวบรวมข้อมูลควรมีน้อยที่สุด ทำเท่าที่จำเป็นต้องใช้งาน

4. การเข้าถึงและความถูกต้อง (Access and accuracy) ผู้ใช้บริการจะต้องสามารถเข้าถึงข้อมูลส่วนบุคคล เพื่อดูได้ว่าข้อมูลมีอะไรเก็บอยู่บ้างและถูกต้องหรือไม่ การจัดเก็บต้องรักษาความถูกต้องของข้อมูล
5. การป้องกันรักษาความมั่นคง (Security safeguards) การป้องกันจะป้องกันไม่ให้มีการเข้าถึง เปิดเผย คัดลอก ใช้งาน หรือเปลี่ยนแปลงข้อมูลส่วนบุคคลโดยผู้ที่ไม่มีสิทธิ์
6. (การท้าทาย) การปฏิบัติตาม ((Challenging) compliance) ผู้ใช้บริการต้องสามารถท้าทายกระบวนการทางด้านความเป็นส่วนตัว ธุรกรรมต่าง ๆ ต้องทำตามกฎหมายความเป็นส่วนตัว เช่น กฎหมายการส่งข้อมูลข้ามเขตแดน
7. วัตถุประสงค์ (Purpose) ข้อมูลส่วนบุคคลหรือข้อมูลของผู้ใช้บริการที่มีการเก็บรวบรวม ควรมีการระบุวัตถุประสงค์ของการเก็บรวบรวมและการใช้ข้อมูลร่วมให้ชัดเจน และแจ้งผู้ที่ข้อมูลนั้นกล่าวถึงก่อนทำการรวบรวม
8. การจำกัดการใช้งาน - การเปิดเผยข้อมูลและการเก็บรักษา (Limiting use – disclosure and retention) ข้อมูลสามารถนำมาใช้หรือเปิดเผยได้เฉพาะตามวัตถุประสงค์สำหรับการเก็บรวบรวม และควรจะเปิดเผยเฉพาะผู้ที่มีสิทธิ์ทราบ ข้อมูลส่วนบุคคลควรทำให้เป็นนิรนามและเก็บรักษาไว้นานเท่าที่จำเป็น
9. ความรับผิดชอบ (Accountability) องค์กรจะต้องแต่งตั้งผู้ควบคุมนโยบายความเป็นส่วนตัวและการปฏิบัติตามจริง ต้องมีระบบการตรวจสอบเพื่อเฝ้าสังเกตการเข้าถึงและการแก้ไขข้อมูล

หลังจากนั้นงานวิจัยได้เสนอแนวทางการออกแบบการให้บริการ โดยให้ทำการประเมินผลกระทบจากการทำงานต่อความเป็นส่วนตัวในแต่ละเฟสของการพัฒนาบริการ ใช้เทคโนโลยีหรือเครื่องมือช่วยจัดการความเป็นส่วนตัว และให้ผู้ให้บริการจัดเก็บข้อมูลเท่าที่จำเป็น อนุญาตให้ผู้ใช้บริการสามารถควบคุมข้อมูล และพัฒนาบริการให้มีปฏิสัมพันธ์กับผู้ใช้บริการในเรื่องความเป็นส่วนตัว แนวทางที่เสนอในงานวิจัยนี้สามารถช่วยในการกำหนดแบบประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการ

2.2.3 ความเป็นส่วนตัวและความมั่นคงของคลาวด์

Saleem-ullah Lar, Xiaofeng Liao and Syed Ali Abbas [17] กล่าวถึงกลไกด้านความมั่นคงและความเป็นส่วนตัวที่ผู้ให้บริการพึงปฏิบัติมีดังนี้

1. การป้องกันการทำงานร่วมกัน ต้องมีนโยบายการควบคุมการเข้าถึง ต้องป้องกันการเข้าถึงข้อมูลหรือการแทรกแซงการทำงานของผู้ใช้บริการรายหนึ่งโดยผู้ใช้บริการรายอื่น
2. การจัดการด้านความไว้วางใจ ต้องมีกรอบงานในการสร้างความไว้วางใจ เช่น การเข้ารหัส การจัดการคีย์
3. การจัดการด้านเอกลักษณ์ ต้องมีระบบจัดการที่สามารถให้ผู้ใช้บริการควบคุมข้อมูลเกี่ยวกับเอกลักษณ์ดิจิทัล (Digital Identity) ของตน สามาถใช้เอกลักษณ์ดิจิทัลในการเข้าถึงบริการจากที่ใดก็ได้ หรือในบางกรณีสามารถกำหนดชื่อเทียมให้ผู้ใช้บริการได้เพื่อป้องกันความเป็นส่วนตัว
4. ความมั่นคงและความเป็นส่วนตัวแบบใช้ข้อมูลเป็นศูนย์กลาง เจ้าของข้อมูลต้องสามารถควบคุมได้ว่าใครสามารถเข้าถึงข้อมูลได้และทำอะไรได้บ้าง ต้องคำนึงถึงกฎหมายเมื่อมีการเคลื่อนย้ายข้อมูล มีการเฝ้าสังเกต ตรวจจับ และตอบสนองปัญหาที่เกิดขึ้น

แนวทางที่เสนอในงานวิจัยนี้สามารถช่วยในการกำหนดแบบประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการ

2.2.4 เครื่องมือในการประเมินผลกระทบด้านความเป็นส่วนตัวสำหรับคลาวด์

David Tancock, Siani Pearson และ Andrew Charlesworth [18] ได้นำเสนอเครื่องมือเพื่อช่วยองค์กรในการประเมินโครงการที่กำลังจะพัฒนาว่าจะมีผลกระทบด้านความเป็นส่วนตัวอย่างไรบ้างเมื่อดำเนินโครงการบนคลาวด์ ซึ่งเปรียบได้กับเครื่องมือประเมินความเสี่ยงหรือภัยคุกคามด้านความเป็นส่วนตัว เครื่องมือจะมีฐานความรู้ซึ่งผู้เชี่ยวชาญด้านความเป็นส่วนตัวทำการบันทึกข้อมูลกฎหมายความเป็นส่วนตัวและการป้องกันข้อมูลในรูปของกฎไว้ ส่วนองค์กรจะให้ข้อมูลเกี่ยวกับโปรไฟล์ของโครงการและตอบคำถามการประเมินความเสี่ยง จากนั้นเครื่องมือจะประเมินความเสี่ยงในประเด็นต่าง ๆ ด้านความเป็นส่วนตัว พร้อมทั้งออกรายงานว่ามีความเสี่ยงในประเด็นใดบ้าง อย่างไรก็ตามงานวิจัยนี้กล่าวถึงเพียงแนวคิดการออกแบบเครื่องมือ แต่ยังไม่มีรายละเอียดของการออกแบบและการพัฒนา รวมทั้งไม่มีรายละเอียดของคำถามที่ใช้ประเมินและผลการประเมินไม่ได้อยู่ในรูปค่าคะแนนความเสี่ยง

2.2.5 ประเด็นความเป็นส่วนตัว ความมั่นคง และความไว้วางใจที่เกิดจากคลาวด์

Siani Pearson และ Azzedine Benameur [19] นำเสนอปัจจัยที่มีผลกระทบต่อความเป็นส่วนตัว ความมั่นคง และความไว้วางใจ และกล่าวถึงวิธีการจัดการดังนี้

1. วิธีการจัดการข้อมูล ต้องมีการจำแนกประเภทข้อมูลที่จะส่งให้ผู้ให้บริการก่อนว่าเป็นความลับหรือไม่ และพยายามจำกัดการเคลื่อนย้ายข้อมูลไปยังผู้ให้บริการให้เป็นเพียงข้อมูลที่ไม่เป็นความลับ ในการทำสัญญาการใช้บริการ ให้ระบุวิธีการป้องกันข้อมูล สถานที่จัดเก็บ มีการแจ้งเมื่อเปลี่ยนสถานที่ ผู้ให้บริการต้องทำตามกฎหมาย มีการระบุความเป็นเจ้าของข้อมูลให้ชัดเจน และจะดำเนินการอย่างไรกับข้อมูลเมื่อสิ้นสุดสัญญา เมื่อข้อมูลหายหรือถูกลบ หรือจะยังคงเก็บข้อมูลอยู่ในกรณีใดบ้าง
2. การบรรเทาความมั่นคง ข้อมูลที่มีการเคลื่อนย้ายหรือข้อมูลที่ต้องการเพียงการจัดเก็บธรรมดาจะมีการเข้ารหัส แต่สำหรับข้อมูลที่จัดเก็บแล้วต้องมีการทำดัชนีเพื่อใช้ค้นหาการเข้ารหัสจะทำให้ไม่สามารถทำเช่นนั้นได้เพราะการประมวลผลข้อมูลที่เข้ารหัสยังทำได้ไม่มีประสิทธิภาพบนคลาวด์ จึงต้องหาจุดสมดุลระหว่างประสิทธิภาพในการใช้งานกับความมั่นคง
3. การออกแบบความเป็นส่วนตัว ต้องมีการออกแบบการให้บริการคลาวด์ที่คำนึงถึงความเป็นส่วนตัว ต้องให้ผู้ใช้บริการยังคงสามารถควบคุมการจัดการข้อมูลของตนที่อยู่บนคลาวด์ได้ มีการป้องกันผู้ให้บริการหาประโยชน์จากข้อมูลของผู้ใช้บริการที่จัดเก็บบนคลาวด์ คำนึงถึงการเคลื่อนย้ายข้อมูลข้ามเขตแดน จัดการการรับช่วงต่อให้บริการ
4. ความเป็นมาตรฐาน ต้องมีการพัฒนามาตรฐานสำหรับคลาวด์เรื่องกรอบงานความไว้วางใจ การรับประกัน และการตรวจสอบ
5. ความรับผิดชอบ ต้องมีการกำหนดผู้รับผิดชอบในกรณีข้อมูลสูญหาย สูญเสีย หรือมีการละเมิดความเป็นส่วนตัว ต้องอาศัยวิธีการตรวจสอบบันทึกการเคลื่อนย้ายและการใช้บริการจากการรับช่วงเพื่อให้ระบุผู้รับผิดชอบได้
6. การผสมผสานการดำเนินการกับการบังคับใช้ ควรที่จะมีการสอดประสานของการบังคับการใช้นโยบายไปยังทุกส่วนของการให้และใช้บริการคลาวด์ มีเครื่องมือช่วยในการตัดสินใจและการประเมินความเสี่ยงด้านความเป็นส่วนตัวจากการใช้คลาวด์ ความงานในส่วนที่มีผลกระทบต่อความมั่นคงของระบบ เช่นเมื่อทำสัญญาในการใช้งานระบบ เป็นต้น
7. กลไกการเพิ่มความไว้วางใจ วิธีการทางสังคมเป็นพฤติกรรมที่ช่วยการเพิ่มความไว้วางใจ เช่น การออกเอกสารรับประกัน แบรนด์ ชื่อเสียง พฤติกรรมในอดีต
8. การรวมโซลูชั่น การรวมวิธีการหรือแนวทางที่หลากหลายเพื่อช่วยให้จัดการได้ดีขึ้น
9. การปรับวิธีการจัดการให้เข้ากับบริบทหรือความต้องการด้านความเป็นส่วนตัว ความมั่นคง

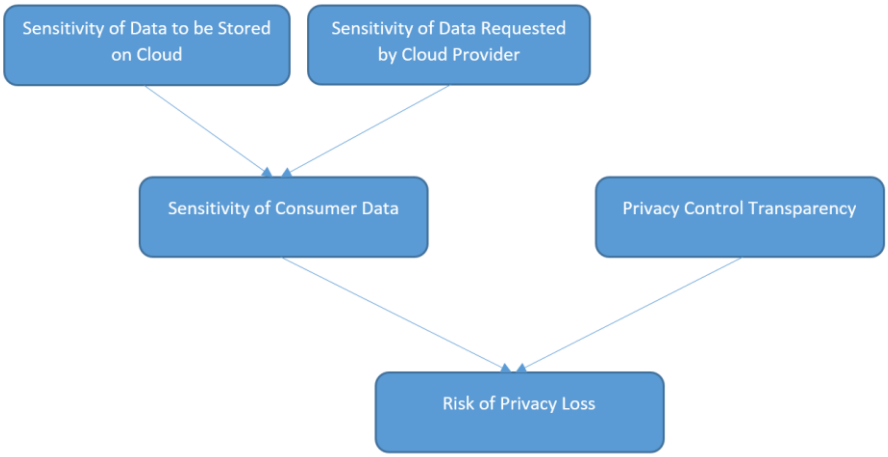
แนวทางที่เสนอในงานวิจัยนี้สามารถช่วยในการกำหนดแบบประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการ

บทที่ 3

การประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของบริการจัดเก็บข้อมูลบนคลาวด์

เมื่อองค์กรมีข้อมูลที่ต้องการนำไปจัดเก็บบนคลาวด์ มักจะมีความกังวลเกี่ยวกับความเป็นส่วนตัวของข้อมูล ดังนั้นจึงเกิดแนวคิดในการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว (Risk of Privacy Loss Assessment) ของข้อมูลที่จะนำไปจัดเก็บบนคลาวด์

การประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวมีการดำเนินการประเมินสองส่วนคือ การประเมินระดับความอ่อนไหวของข้อมูลผู้ใช้บริการ และการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการ ดังภาพรวมในภาพที่ 3.1 โดยการประเมินมีรายละเอียดดังนี้



ภาพที่ 3.1 *ภาพรวมการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว*

3.1 การประเมินระดับความอ่อนไหวของข้อมูลผู้ใช้บริการ

ข้อมูลผู้ใช้บริการที่พิจารณาประกอบด้วย ข้อมูลที่ผู้ใช้บริการเอาไปจัดเก็บบนคลาวด์ และข้อมูลส่วนบุคคลที่ผู้ให้บริการร้องขอจากผู้ใช้บริการในการเข้าใช้ วิธีการประเมินมีดังนี้

3.1.1 การประเมินระดับความอ่อนไหวของข้อมูลที่ผู้ใช้บริการเอาไปจัดเก็บบนคลาวด์

การประเมินค่าความอ่อนไหวของข้อมูลที่ผู้ใช้บริการนำไปจัดเก็บบนคลาวด์ จะประเมินตามกลุ่มข้อมูลในด้านการจัดการและการสนับสนุนธุรกิจและสารสนเทศขององค์กรซึ่ง NIST แบ่งไว้สองกลุ่ม [6] คือกลุ่ม Service Delivery Support Information (SDSI) ซึ่งแบ่งเป็นประเภทข้อมูล 8 ประเภท และกลุ่ม Government Resources Management Information (GRMI) ซึ่งแบ่งเป็นประเภทข้อมูลได้ 5 ประเภท แต่ละประเภทมีการแบ่งประเภทย่อยลงไปอีกรวม 77 ประเภท NIST ได้กำหนดระดับผลกระทบที่จะเกิดขึ้นต่อองค์กรหากข้อมูลแต่ละประเภทสูญเสียการรักษาความลับ (Loss of Confidentiality) สูญเสียบูรณภาพ (Loss of Integrity) และสูญเสียสภาพพร้อมใช้งาน (Loss of Availability) โดยแบ่งเป็น 3 ระดับ ดังตารางที่ 3.1 คือ

1. High ประเภทข้อมูลมีค่าระดับผลกระทบต่อองค์กรอยู่ในระดับสูง
2. Moderate ประเภทข้อมูลมีค่าระดับผลกระทบต่อองค์กรอยู่ในระดับปานกลาง
3. Low ประเภทข้อมูลมีค่าระดับผลกระทบต่อองค์กรอยู่ในระดับต่ำ
4. N/A ประเภทข้อมูลไม่มีการประเมินค่าผลกระทบ

NIST ระบุไว้ว่าในกรณีที่มีปัจจัยบางอย่างเกิดขึ้นจะทำให้ระดับผลกระทบที่เป็นสีเทาปรับขึ้นได้ แต่ระดับผลกระทบที่เป็นสีดำจะไม่สามารถปรับขึ้นได้ จากนิยามของความอ่อนไหวดังหัวข้อที่ 2.1.2 ซึ่งเกี่ยวข้องกับระดับผลกระทบที่เกิดขึ้นหากข้อมูลได้รับการเปิดเผยอย่างไม่เหมาะสม เกิดความเสียหาย หรือสูญหาย ผู้วิจัยจึงนิยามระดับความอ่อนไหวของข้อมูลแต่ละประเภทที่ NIST กำหนดไว้ ตามระดับผลกระทบที่เกิดจากการสูญเสียการรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน โดยใช้หลักการ High Water Mark กล่าวคือใช้ค่าระดับผลกระทบสูงสุดจากการสูญเสียองค์ประกอบด้านความมั่นคงทั้งสามประเภทแทนค่าความอ่อนไหว ดังตารางที่ 3.1 ดังนั้นหากมีปัจจัยบางอย่างเกิดขึ้นและทำให้ระดับผลกระทบจากการสูญเสียองค์ประกอบด้านความมั่นคงทั้งสามซึ่งเป็นสีเทามีการปรับขึ้น ก็จะทำให้ระดับความอ่อนไหวของข้อมูลประเภทนั้น ๆ ซึ่งกำหนดโดยใช้หลักการ High Water Mark มีการปรับตามไปด้วย

ตารางที่ 3.1 *ระดับผลกระทบต่อองค์กรและระดับความอ่อนไหวของข้อมูลแต่ละประเภท (ขยายจาก [6])*

No.	Information Type	Loss-of-Confidentiality Impact	Loss-of-Integrity Impact	Loss-of-Availability Impact	Sensitivity (Derived by this Research)
SDSI(C2.1)	**Controls and Oversight**				
	Corrective Action (Policy/Regulation)	Low	**Low**	**Low**	Low
	Program Evaluation	Low	**Low**	**Low**	Low
	Program Monitoring	Low	Low	Low	Low
SDSI(C2.2)	**Regulatory Development**				
	Policy & Guidance Development	Low	Low	**Low**	Low
	Public Comment Tracking	**Low**	**Low**	**Low**	**Low**
	Regulatory Creation	Low	Low	**Low**	Low
	Rule Publication	**Low**	**Low**	**Low**	**Low**
SDSI(C2.3)	**Planning & Budgeting**				
	Budget Formulation	Low	Low	**Low**	Low
	Capital Planning	Low	Low	**Low**	Low
	Enterprise Architecture	Low	Low	**Low**	Low
	Strategic Planning	Low	Low	**Low**	Low
	Budget Execution	Low	Low	**Low**	Low
	Workforce Planning	Low	Low	**Low**	Low
	Management Improvement	Low	Low	**Low**	Low
	Budgeting & Performance Integration	Low	Low	**Low**	Low
	Tax & Fiscal Policy	Low	Low	**Low**	Low

ตารางที่ 3.1 *ระดับผลกระทบต่อองค์กรและระดับความอ่อนไหวของข้อมูลแต่ละประเภท (ขยายจาก [6]) (ต่อ)*

No.	Information Type	Loss-of-Confidentiality Impact	Loss-of-Integrity Impact	Loss-of-Availability Impact	Sensitivity (Derived by this Research)
SDSI(C2.4)	**Internal Risk Management & Mitigation**				
	Contingency Planning	Moderate	**Moderate**	Moderate	Moderate
	Continuity of Operations	Moderate	**Moderate**	Moderate	Moderate
	Service Recovery	Low	**Low**	Low	Low
SDSI(C2.5)	**Revenue Collection**				
	Debt Collection	Moderate	Low	**Low**	Moderate
	User Fee Collection	**Low**	Low	**Moderate**	Moderate
	Federal Asset Sales	Low	**Moderate**	**Low**	Moderate
SDSI(C2.6)	**Public Affairs**				
	Customer Services	Low	Low	Low	Low
	Official Information Dissemination	**Low**	Low	Low	Low
	Product Outreach	**Low**	Low	**Low**	Low
	Public Relations	Low	Low	**Low**	Low
SDSI(C2.7)	**Legislative Relations**				
	Legislation Tracking	Low	**Low**	**Low**	Low
	Legislation Testimony	Low	**Low**	Low	Low
	Proposal Development	Moderate	**Low**	Low	Moderate
	Congressional Liason Operations	Moderate	**Low**	Low	Moderate
SDSI(C2.8)	**General Management**				
	Central Fiscal Operations	Moderate	**Low**	**Low**	Moderate

ตารางที่ 3.1 *ระดับผลกระทบต่อองค์กรและระดับความอ่อนไหวของข้อมูลแต่ละประเภท (ขยายจาก [6]) (ต่อ)*

No.	Information Type	Loss-of-Confidentiality Impact	Loss-of-Integrity Impact	Loss-of-Availability Impact	Sensitivity (Derived by this Research)
	Legislative Functions	Low	Low	Low	Low
	Executive Functions	Low	Low	Low	Low
	Central Property Management	Low	Low	Low	Low
	Central Personnel Management	Low	Low	Low	Low
	Taxation Management	Moderate	Low	Low	Moderate
	Central Records & Statistics Management	Moderate	Low	Low	Moderate
	Income Information	Moderate	Moderate	Moderate	Moderate
	Personal Identity and Authentication	Moderate	Moderate	Moderate	Moderate
	Entitlement Event Information	Moderate	Moderate	Moderate	Moderate
	Representative Payee Information	Moderate	Moderate	Moderate	Moderate
	General Information	Low	Low	Low	Low
GRMI(C3.1)	**Administrative Management**				
	Facilities, Fleet, and Equipment Management	Low	Low	Low	Low
	Help Desk Services	Low	Low	Low	Low
	Security Management	Moderate	Moderate	Low	Moderate

ตารางที่ 3.1 *ระดับผลกระทบต่อองค์กรและระดับความอ่อนไหวของข้อมูลแต่ละประเภท (ขยายจาก [6]) (ต่อ)*

No.	Information Type	Loss-of-Confidentiality Impact	Loss-of-Integrity Impact	Loss-of-Availability Impact	Sensitivity (Derived by this Research)
	Travel	Low	Low	Low	Low
	Workplace Policy Development & Management	Low	Low	Low	Low
GRMI(C3.2)	**Financial Management**				
	Accounting	Low	Low	Low	Low
	Funds Control	Low	Moderate	Low	Moderate
	Payments	Moderate	Moderate	Low	Moderate
	Collections and Receivables	Low	Moderate	Low	Moderate
	Asset and Liability Management	Low	Moderate	Low	Moderate
	Reporting and Information	Low	Moderate	Low	Moderate
	Cost Accounting/ Performance Measurement	Low	Moderate	Low	Moderate
GRMI(C3.3)	**Human Resource Management**				
	HR Strategy	Low	Low	Low	Low
	Staff Acquisition	Low	Low	Low	Low
	Organization & Position Mgmt	Low	Low	Low	Low
	Compensation Management	Low	Low	Low	Low
	Benefits Management	Low	Low	Low	Low

ตารางที่ 3.1 *ระดับผลกระทบต่อองค์กรและระดับความอ่อนไหวของข้อมูลแต่ละประเภท (ขยายจาก [6]) (ต่อ)*

No.	Information Type	Loss-of-Confidentiality Impact	Loss-of-Integrity Impact	Loss-of-Availability Impact	Sensitivity (Derived by this Research)
	Employee Performance Mgmt	Low	Low	Low	Low
	Employee Relations	Low	Low	Low	Low
	Labor Relations	Low	Low	Low	Low
	Separation Management	Low	Low	Low	Low
	Human Resources Development	Low	Low	Low	Low
GRMI(C3.4)	**Supply Chain Management**				
	Goods Acquisition	Low	Low	Low	Low
	Inventory Control	Low	Low	Low	Low
	Logistics Management	Low	Low	Low	Low
	Services Acquisition	Low	Low	Low	Low
GRMI(C3.5)	**Information & Technology Management**				
	System Development	Low	Moderate	Low	Moderate
	Lifecycle/Change Management	Low	Moderate	Low	Moderate
	System Maintenance	Low	Moderate	Low	Moderate
	IT Infrastructure Maintenance	Low	Low	Low	Low
	Information Security	Low	Moderate	Low	Moderate
	Record Retention	Low	Low	Low	Low
	Information Management	Low	Moderate	Low	Moderate

ตารางที่ 3.1 *ระดับผลกระทบต่อองค์กรและระดับความอ่อนไหวของข้อมูลแต่ละประเภท (ขยายจาก [6]) (ต่อ)*

No.	Information Type	Loss-of-Confidentiality Impact	Loss-of-Integrity Impact	Loss-of-Availability Impact	Sensitivity (Derived by this Research)
	System and Network Monitoring	Moderate	Moderate	Low	Moderate
	Information Sharing	N/A	N/A	N/A	N/A

จากข้อมูลประเภทต่าง ๆ ที่องค์กรจะนำไปจัดเก็บบนคลาวด์ สามารถคำนวณระดับความอ่อนไหวของข้อมูลที่จะจัดเก็บ S_{Stored} ได้จากระดับความอ่อนไหวของข้อมูลแต่ละประเภทโดยใช้หลักการ High Water Mark เช่นกัน ดัง (1)

$$S_{Stored} = \begin{cases} 1 & if\ highest\ sensitivity\ level\ of\ stored\ information\ types\ is\ H \\ 0.67 & if\ highest\ sensitivity\ level\ of\ stored\ information\ types\ is\ M \\ 0.33 & if\ highest\ sensitivity\ level\ of\ stored\ information\ types\ is\ L \\ 0 & if\ highest\ sensitivity\ level\ of\ stored\ information\ types\ is\ N/A. \end{cases} \quad (1)$$

โดยที่ S_{Stored} = Sensitivity level of data to be stored on cloud

เมื่อผู้ใช้บริการต้องการจัดเก็บข้อมูลใด ๆ บนคลาวด์ ผู้ใช้บริการจะทำการตรวจระดับค่าความอ่อนไหวของข้อมูลแต่ละประเภทตามประเภทข้อมูลของ NIST ตามตารางที่ 3.1 หลังจากนั้นจะใช้วิธีการ High Water Mark ในการกำหนดรระดับความอ่อนไหวของข้อมูลที่จะจัดเก็บ ดังตัวอย่างต่อไปนี้

ตัวอย่าง องค์กรกรณีศึกษาบริษัทโฆษณาแห่งหนึ่งต้องการนำข้อมูลไปจัดเก็บบนคลาวด์ โดยมีข้อมูลที่จะนำขึ้นไปจัดเก็บ ดังนี้

แผนกบัญชีขององค์กรต้องการจัดเก็บข้อมูลของแผนกบนคลาวด์โดยทางแผนกพิจารณาข้อมูล Government Resources Management Information (GRMI) ส่วน Financial Management ซึ่งมี 7 ประเภทข้อมูลย่อย โดยที่แผนกบัญชีต้องการจัดเก็บข้อมูลทั้ง 7 ประเภทย่อยบนคลาวด์ ดังนั้นสามารถกำหนดค่าความอ่อนไหวของข้อมูลแผนกบัญชีได้ดังนี้

Accounting มีระดับความอ่อนไหวเป็น Low

Funds Control มีระดับความอ่อนไหวเป็น Moderate

Payments มีระดับความอ่อนไหวเป็น Moderate

Collections and Receivables มีระดับความอ่อนไหวเป็น Moderate

Asset and Liability Management มีระดับความอ่อนไหวเป็น Moderate

Reporting and Information มีระดับความอ่อนไหวเป็น Moderate

Cost Accounting/ Performance Measurement มีระดับความอ่อนไหวเป็น Moderate

ดังนั้นโดยวิธี High Water Mark ระดับความอ่อนไหวสูงสุดของข้อมูลทั้ง 7 ประเภทจะเป็น Moderate และจาก (1) จะได้ระดับความอ่อนไหวของข้อมูลที่จะจัดเก็บบนคลาวด์เป็น

$$S_{Stored} = 0.6667$$

3.1.2 การประเมินระดับความอ่อนไหวของข้อมูลส่วนบุคคลที่ผู้ให้บริการร้องขอจากผู้ใช้บริการในการเข้าใช้

การประเมินส่วนนี้คือการประเมินจากการที่ผู้ให้บริการร้องขอข้อมูลจากผู้ใช้บริการ เมื่อต้องการจะนำข้อมูลไปจัดเก็บบนคลาวด์ โดยจะตรวจสอบว่าผู้ให้บริการมีการร้องขอข้อมูลส่วนบุคคลอะไรบ้างจากผู้ใช้บริการ และข้อมูลเหล่านั้นมีความอ่อนไหวระดับใด ผู้วิจัยใช้แนวทางการประเมินระดับความอ่อนไหวของข้อมูลจากงานวิจัย [14] [15] โดยผู้ใช้บริการจะสำรวจข้อมูลที่ถูกร้องขอโดยผู้ให้บริการ เพื่อนำมาออกแบบ Cross Table สำหรับใช้คำนวณระดับความอ่อนไหวดังตัวอย่าง Cross Table ในตารางที่ 3.2 เป็น Cross Table ของ Microsoft Azure ที่ผู้ใช้บริการกำหนด ซึ่งประกอบไปด้วยคอนเซปต์ 4 กลุ่ม และแอตทริบิวต์ ซึ่งคือข้อมูลที่ผู้ให้บริการร้องขอ โดยที่แอตทริบิวต์จะถูกจัดอยู่ในคอนเซปต์ต่าง ๆ โดยตาราง Cross Table สามารถปรับได้ตามความเหมาะสมสำหรับผู้ใช้บริการแต่ละราย และขึ้นอยู่กับจำนวนของข้อมูลส่วนบุคคลที่ผู้ให้บริการร้องขอ

ตารางที่ 3.2 *ตัวอย่าง Cross Table ของ Microsoft Azure*

Concept/Attribute	First Name	Last Name	Company Name	Email	Work Phone	Mobile Phone	Credit Card Number	Security Code	Expiration Date
Basic	X	X	X	X	X	X			
Privat						X	X	X	
Identity		X	X				X		
Finance	X	X	X		X	X	X	X	X

องค์ประกอบของการคำนวณระดับความอ่อนไหวของข้อมูลส่วนบุคคลประกอบด้วย 4 องค์ประกอบ ได้แก่ ระดับความเชื่อมโยง หลักเอกลักษณ์ หลักความเป็นส่วนตัว และค่าการอนุมาน โดยมีรายละเอียดดังนี้

1. ระดับความเชื่อมโยง (Degree of Conjunction) เป็นค่าที่บ่งบอกว่าแอตทริบิวต์ d จัดอยู่ในคอนเซปต์ใดบ้าง กล่าวคือ d สามารถเชื่อมโยงคอนเซปต์ใดเข้าด้วยกันได้บ้าง สามารถคำนวณได้จาก

$$D_C(d) = \frac{Number\ of\ concepts\ to\ which\ d\ belongs}{Total\ number\ of\ concepts} \quad (2)$$

เช่น ข้อมูล First Name อยู่ในคอนเซปต์ Basic และ Finance ดังนั้น D_C(First Name) = 2/4 = 0.5

2. หลักเอกลักษณ์ (Principle of Identity) เป็นการระบุว่าแอตทริบิวต์ d เป็นแอตทริบิวต์เอกลักษณ์ของคอนเซปต์ที่ d เป็นสมาชิกอยู่ กล่าวคือ เป็นคีย์ที่ใช้ในการเข้าถึงแอตทริบิวต์อื่น ๆ ในคอนเซปต์ต่าง ๆ สามารถคำนวณได้จาก

$$I_A(d) = \begin{cases} 0, & if\ d\ is\ not\ identity\ attribute \\ \frac{Number\ of\ attributes\ in\ the\ concepts}{Total\ number\ of\ attributes}, & if\ d\ is\ identity\ attribute\ for\ the\ concepts \end{cases} \quad (3)$$

เช่น Company Name เป็นแอตทริบิวต์เอกลักษณ์ของคอนเซปต์ Basic และ Finance มีแอตทริบิวต์ในทั้งสองคอนเซปต์รวม 9 แอตทริบิวต์ ซึ่งก็คือจำนวนแอตทริบิวต์ทั้งหมด ดังนั้น I_A(Company Name) = 9/9 แต่สำหรับแอตทริบิวต์ First Name ซึ่งไม่ได้อยู่ในคอนเซปต์ Identity จะมีค่าหลักเอกลักษณ์เป็น 0

3. หลักความเป็นส่วนตัว (Principle of Privacy) เป็นการระบุว่าแอตทริบิวต์ d เป็นข้อมูลที่เป็นส่วนตัว ซึ่งแต่ละผู้ใช้บริการอาจมีความเห็นว่า d เป็นข้อมูลที่เป็นส่วนตัวหรือไม่เป็นส่วนตัวแตกต่างกันได้ และสามารถปรับ Cross Table ให้ d อยู่หรือไม่อยู่ในคอนเซปต์ Private ได้ตามความเหมาะสม สามารถคำนวณได้โดย

$$P_A(d) = \begin{cases} 0, & if\ d\ does\ not\ belong\ to\ the\ Private\ concept \\ 1, & if\ d\ belongs\ to\ the\ Private\ concept \end{cases} \quad (4)$$

เช่น Credit Card Number เป็นข้อมูลที่เป็นส่วนตัว ดังนั้น P_A(Credit Card Number) มีค่าเท่ากับ 1 แต่ Company Name มีค่า P_A(Company Name) เท่ากับ 0

4. ค่าการอนุมาน (Value of Analogism) เป็นการระบุว่าแอตทริบิวต์ d สามารถใช้บ่งบอกถึงแอตทริบิวต์อื่น ๆ ได้หรือไม่ สามารถคำนวณได้จาก

$$A_A(d) = \begin{cases} 0, & if\ d\ cannot\ derive\ other\ attributes \\ 1, & if\ d\ can\ derive\ other\ attributes \end{cases} \quad (5)$$

เช่น Email สามารถเชื่อมโยงหรือบ่งบอกไปถึง Last Name หรือ Company Name ได้ ดังนั้น A_A(Email) มีค่าเท่ากับ 1 แต่ข้อมูล Expiration Date ไม่สามารถเชื่อมโยงหรือบ่งบอกไปยังแอตทริบิวต์อื่น ๆ ได้ ดังนั้น A_A(Expiration Date) มีค่าเท่ากับ 0 นั่นเอง

เมื่อหาค่าระดับความเชื่อมโยง หลักเอกลักษณ์ หลักความเป็นส่วนตัว และค่าการอนุมานได้แล้วค่าระดับความอ่อนไหวของแต่ละแอตทริบิวต์จะคำนวณได้จาก

$$S(d) = D_C(d) + I_A(d) + P_A(d) + A_A(d) \quad (6)$$

ค่าระดับความอ่อนไหวของข้อมูลทั้งหมดที่ผู้ให้บริการร้องขอ $S_{Requested}$ สามารถคำนวณได้จาก

$$S_{Requested} = \frac{\sum_{i=1}^{k} S(d_i)}{4k} \quad (7)$$

โดยที่ $S_{Requested}$ = Sensitivity level of personal data requested by cloud provider, $S_{Requested}$ is in (0-1]

k = Number of personal data attributes requested by cloud provider

ในการประเมินค่าความอ่อนไหวของข้อมูลที่ผู้ให้บริการรายหนึ่ง ๆ ร้องขอในการเข้าใช้บริการ ผู้ใช้บริการจะต้องพิจารณาว่าผู้ให้บริการรายนั้นร้องขอข้อมูลอะไรบ้าง แล้วนำมาสร้าง Cross Table สำหรับผู้ให้บริการรายนั้น โดยกำหนดกลุ่มคอนเซปต์และแอตทริบิวต์ในแต่ละคอนเซปต์ ดังนั้นหากผู้ใช้บริการต้องการพิจารณาผู้ให้บริการคลาวด์หลายราย ผู้ให้บริการคลาวด์แต่ละรายจะมี Cross Table ที่แตกต่างกันได้เนื่องจากมีการร้องขอข้อมูลที่แตกต่างกัน รวมทั้งผู้ใช้บริการต่างรายกันสามารถกำหนด Cross Table ที่แตกต่างกันให้กับผู้ให้บริการคลาวด์รายเดียวกันได้

ตัวอย่างกรณีศึกษาบริษัทโฆษณากำหนด Cross Table ให้กับ Microsoft Azure ดังตารางที่ 3.2 ข้างต้น ค่าความอ่อนไหวของข้อมูลที่ผู้ให้บริการรายนี้ร้องขอ $S_{Requested}$ ซึ่งคำนวณโดย (7) ได้ผลดังตารางที่ 3.3

ตารางที่ 3.3 *ตัวอย่างค่าความอ่อนไหวของข้อมูลที่ผู้ให้บริการ Microsoft Azure ร้องขอเพื่อเข้าใช้บริการ*

Attribute	$D_c(d)$	$I_A(d)$	$P_A(d)$	$A_A(d)$	$S(d)$
First Name	2/4	0	0	0	0.5000
Last Name	3/4	9/9	0	0	1.7500
Company Name	3/4	9/9	0	0	1.7500
Email	1/4	0	0	1	1.2500
Work Phone	2/4	0	0	0	0.5000
Mobile Phone	3/4	0	1	0	1.7500
Credit Card Number	3/4	8/9	1	0	2.6389
Security Code	2/4	0	1	0	1.5000
Expiration Date	1/4	0	0	0	0.2500
Total					11.8889
					$S_{Requested}$ = 11.8889 / (4 * 9) = 0.3302

3.1.3 การประเมินระดับความอ่อนไหวของข้อมูลผู้ใช้บริการ

การประเมินระดับความอ่อนไหวของข้อมูลของผู้ใช้บริการจะคำนวณจากระดับความอ่อนไหวของข้อมูลที่จะจัดเก็บและข้อมูลที่ผู้ให้บริการร้องขอดังข้างต้น โดยที่ผู้ใช้บริการสามารถกำหนดค่าน้ำหนักเพื่อให้ความสำคัญแก่ข้อมูลทั้งสองส่วนแตกต่างกันได้ ดังสมการ

$$S_{Data} = (W_{Stored} * S_{Stored}) + (W_{Requested} * S_{Requested}) \quad (8)$$

โดยที่ S_{Data} = Sensitivity level of consumer data, S_{Data} is in (0,1]

W_{Stored} = Weight given to data to be stored on cloud

S_{Stored} = Sensitivity level of data to be stored on cloud from (1)

$W_{Requested}$ = Weight given to personal data requested by cloud provider

$S_{Requested}$ = Sensitivity level of personal data requested by cloud provider from (7)

และ $W_{Stored} + W_{Requested} = 1$

การให้ค่าน้ำหนัก W_{Stored} และ $W_{Requested}$ จะให้ตามสำคัญของข้อมูลที่จะนำขึ้นไปจัดเก็บบนคลาวด์และข้อมูลที่ผู้ให้บริการร้องขอ ตามที่ผู้ใช้บริการเห็นสมควร เช่น หากผู้ใช้บริการให้ความสำคัญกับปริมาณข้อมูลและเห็นว่าข้อมูลที่จะนำขึ้นไปจัดเก็บบนคลาวด์มีปริมาณมากและมีหลากหลายประเภท ในขณะที่ผู้ให้บริการร้องขอข้อมูลปริมาณน้อยและข้อมูลส่วนใหญ่ที่ผู้ให้บริการร้องขอเป็นข้อมูลที่เผยแพร่โดยทั่วไปอยู่แล้ว ผู้ใช้บริการจะกำหนดค่า W_{Stored} มากกว่า $W_{Requested}$ แต่ในทางตรงกันข้ามหากผู้ใช้บริการเห็นว่าข้อมูลที่ผู้ให้บริการร้องขอมีความสำคัญมากกว่าเนื่องจากเป็นข้อมูลเกี่ยวกับการเงิน ในขณะที่ข้อมูลที่จัดเก็บเป็นข้อมูลที่ไม่มีความสำคัญมากถึงแม้จะมีปริมาณมากก็ตาม ผู้ใช้บริการสามารถกำหนดค่า $W_{Requested}$ ให้มากกว่า W_{Stored} ในกรณีที่ผู้ใช้บริการเห็นว่าข้อมูลทั้งสองส่วนมีความสำคัญพอ ๆ กันก็จะกำหนดให้ $W_{Requested}$ เท่ากับ W_{Stored}

ตัวอย่าง จากการคำนวณค่าความอ่อนไหวของข้อมูลแผนกบัญชีขององค์กรกรณีศึกษาที่ต้องการนำขึ้นไปจัดเก็บบนคลาวด์ S_{Stored} = 0.6667 และค่าความอ่อนไหวของข้อมูลที่ผู้ให้บริการร้องขอเพื่อเข้าใช้บริการ $S_{Requested}$ = 0.3133 หากองค์กรให้ความสำคัญกับข้อมูลที่จะจัดเก็บบนคลาวด์มากกว่าข้อมูลที่ผู้ให้บริการร้องขอและมีการกำหนดค่า W_{Stored} = 0.8 และค่า $W_{Requested}$ = 0.2 แล้วสามารถคำนวณค่าความอ่อนไหวของข้อมูลผู้ใช้บริการได้จาก (8) ดังนี้

$$S_{Data} = (0.8 * 0.6667) + (0.2 * 0.3302)$$
$$= 0.5994$$

3.2 การประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการ

ความโปร่งใสด้านการควบคุมความเป็นส่วนตัว (Privacy Control Transparency) ของผู้ให้บริการจะประเมินจากข้อมูลของผู้ให้บริการที่เผยแพร่ไว้ โดยพิจารณาจากแนวปฏิบัติของ Privacy Level Agreement [11], Australian Privacy Principle [12] และ Security and Privacy Controls for Federal Information Systems and Organizations [13] โดยเมื่อได้ประมวลแนวปฏิบัติด้านความเป็นส่วนตัวแล้ว ผู้วิจัยได้จัดทำคำถามสำหรับประเมินค่าความโปร่งใสด้านการควบคุมความเป็นส่วนตัว (Cloud Privacy Control Questionnaire (CPCQ)) ในแต่ละหัวข้อซึ่งอ้างอิงจากแนวปฏิบัติใน [11, 12, 13] สำหรับให้ผู้ใช้บริการนำไปใช้ในการประเมินผู้ให้บริการคลาวด์ดังตารางที่ 3.4

ตารางที่ 3.4 *Cloud Privacy Control Questionnaire (CPCQ)*

Code	**Cloud Privacy Control**	**Cloud Privacy Control Questionnaire**	**PLA [11]**	**APP [12]**	**Privacy Control [13]**
CPC1	Identity of the CSP (and of Representative, as applicable), its role, and the contact information for the data protection officer and information security officer	1. Does the provider specify its name, its representative, and address?	PLA1		
		2. Does the provider specify its role in processing of consumer data (i.e. controller, joint-controller, processor or subprocessor)?			
		3. Does the provider specify contact information of the person in charge of data protection matters (e.g. Data Protection Officer, Information Security Officer)?			
CPC2	Categories of personal data that the customer is prohibited from sending to or processing in the cloud	1. Does the provider clearly specify which data categories are uploadable or prohibited from uploading to cloud?	PLA2	APP1, APP4, APP12	
CPC3	Ways in which the data will be processed	1. Does the provider specify locations of data centers where consumer data may be processed (e.g. collected, stored, used, disseminated, changed, and erased)?	PLA3	APP2, APP3, APP5, APP6, APP9, APP10, APP13	AP-1,AP-2, DI-1, DM-1, DM-3, IP-1, IP-3, SE-1, UL-1

ตารางที่ 3.4 *Cloud Privacy Control Questionnaire (CPCQ)*

Code	Cloud Privacy Control	Cloud Privacy Control Questionnaire	PLA [11]	APP [12]	Privacy Control [13]
		2. Does the provider specify how consumer data will be processed to provide agreed service (i.e. storage)?			
		3. Does the provider specify how consumer data will be processed on consumer's request (e.g. report preparation and production)?			
		4. Does the provider specify how consumer data will be processed on provider's initiative (e.g. backup, recovery, monitoring)?			
		5. Does the provider clearly identify whether the service involves subcontractor, and if so, identify chain of accountability in data protection, and procedure to change and objection to change of subcontractor?			
		6. Does the provider clearly identify consumer data that will be shared with subcontractor, other third-parties, or other services the provider may offer?			
		7. Does the provider indicate whether the service requires installation of software on consumer's system, and if so, its implication on data protection and security?			

ตารางที่ 3.4 *Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)*

Code	**Cloud Privacy Control**	**Cloud Privacy Control Questionnaire**	**PLA [11]**	**APP [12]**	**Privacy Control [13]**
CPC4	Data transfer	1. Does the provider indicate whether consumer data will be transferred, backed up, and recovered across borders in regular operations or emergency?	PLA4	APP1, APP5, APP8	
		2. Does the provider clearly identify applicable laws to which the transfer is restricted?			
CPC5	Data security measures	1. Does the provider describe the processes and measures to ensure availability (e.g. backup network links, redundant storage, data backup and restore)?	PLA5	APP1, APP2, APP11, APP12	AR-2, DI-2, DM-1, IP-1, IP-2, TR-1, UL-1
		2. Does the provider describe the processes and measure to ensure data integrity (e.g. data alteration detection by cryptographic mechanism, signature)?			
		3. Does the provider describe the processes and measures to ensure data confidentiality (e.g. encryption of in-transit and at-rest data, strong authentication, authorization mechanism, access control on employees and/or subcontractors)?			

ตารางที่ 3.4 *Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)*

Code	Cloud Privacy Control	Cloud Privacy Control Questionnaire	PLA [11]	APP [12]	Privacy Control [13]
		4. Does the provider describe how isolation in operating environment is provided (e.g. access management on least privilege principle, hardening of hypervisors management of shared resources on virtual machines)?			
		5. Does the provider describe how intervenability is enabled to allow data subjects the rights of data access, rectification, erasure, blocking, and objection when proper security measures are absent?			
		6. Does the provider specify which security controls frameworks are in use (e.g. ISO/IEC 27002, CSA CCM, ENISA Information Assurance Framework) and which controls are implemented?			
CPC6	Monitoring	1. Does the provider specify whether the consumer can monitor or audit, on an ongoing basis, to see if privacy and security measure are met, and if so, how (e.g. reporting, audit)?	PLA6		AR-2, AR-4, AR-6, AR-8, IP-1, IP-3, TR-2

ตารางที่ 3.4 *Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)*

Code	**Cloud Privacy Control**	**Cloud Privacy Control Questionnaire**	**PLA [11]**	**APP [12]**	**Privacy Control [13]**
CPC7	Third-party audits	1. Does the provider specify whether and what third-party audit reports will be provided to the consumer?	PLA7		AR-4, AR-6
		2. Does the provider specify regular update frequency for third-party audit reports?			
		3. Does the provider allow the consumer to choose or participate in choosing the third-party auditor?			
CPC8	Personal data breach notification	1. Does the provider specify whether and how the consumer will be informed of security breach (e.g. accidental or unlawful destruction, loss, alteration, unauthorized access) in consumer data?	PLA8	APP1, APP5	IP-1, SE-2, TR-1
CPC9	Data portability, migration, and transfer-back assistance	1. Does the provider specify the supported formats, preservation of logical relations, and costs for porting consumer data?	PLA9		
		2. Does the provider describe whether, how, and at what cost it will assist the consumer in migrating consumer data to another provider or transfer back to consumer's in-house IT environment?			

ตารางที่ 3.4 *Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)*

Code	**Cloud Privacy Control**	**Cloud Privacy Control Questionnaire**	**PLA [11]**	**APP [12]**	**Privacy Control [13]**
CPC10	Data retention, restitution, and deletion	1. Does the provider indicate for how long consumer data will be retained?	PLA10	APP11	DM-2, IP-1
		2. Does the provider indicate the methods to delete consumer data after the consumer has deleted, after the end of service, or as soon as their retention is not necessary any more (e.g. every redundant instance of consumer data and its previous versions, temporary files, and file fragment are to be deleted)?			
		3. Does the provider indicate whether and for how long consumer data may be retained, and how they are handled, after the consumer has deleted or after the end of service in order to satisfy legal requirements (e.g. tax regulations)?			
		4. Does the provider indicate whether and how the consumer can request the provider to comply with specify laws and regulations on data retention?			

ตารางที่ 3.4 *Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)*

Code	**Cloud Privacy Control**	**Cloud Privacy Control Questionnaire**	**PLA [11]**	**APP [12]**	**Privacy Control [13]**
CPC11	Accountability	1. Does the provider describe policies and procedures that demonstrate accountability (e.g. documenting all processing operations, provider monitoring and logging)?	PLA11	APP	AR-1, AR-7, AR-8, DI-1, IP-3, SE-1, SE-2, TR-2, TR-3
		2. Does the provider identify third-party audit certificates that indicate their data protection controls compliance with recognized standards (e.g. ISO 27001, SOC2 attestation, CSA STAR)?			
CPC12	Cooperation	1. Does the provider specify how it will cooperate with the consumer to ensure data protection compliance?	PLA12	APP2, APP9, APP13	AR-3, IP-3, UL-2
		2. Does the provider describe how it will provide information that demonstrates data protection compliance to the consumer and supervisory authorities?			

ตารางที่ 3.4 *Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)*

Code	**Cloud Privacy Control**	**Cloud Privacy Control Questionnaire**	**PLA [11]**	**APP [12]**	**Privacy Control [13]**
CPC13	Law enforcement access	1. Does the provider describe the process to respond to requests for disclosure of consumer data by law enforcement authorities?	PLA13	APP9, APP12	
		2. Does the provider indicate that notification will be sent to the consumer in the course of disclosure of consumer data to law enforcement authorities, unless otherwise prohibited (e.g. under criminal law to preserve confidentiality of law enforcement investigation)?			
CPC14	Remedies	1. Does the provider indicate what remedies are available to the consumer on contractual obligation breaches by itself or by subcontractor (e.g. compensation, service credits, financial penalties, ability to sue)?	PLA14	APP1	AR-3, IP-13
CPC15	Complaint and dispute resolution	1. Does the provider provide contract detail of the person who will receive questions and complaints?	PLA15		IP-4
		2. Does the provider provide contact details of the third-party that may assist in resolution of dispute with the provider (e.g. a data protection authority)?			

ตารางที่ 3.4 *Cloud Privacy Control Questionnaire (CPCQ) (ต่อ)*

Code	**Cloud Privacy Control**	**Cloud Privacy Control Questionnaire**	**PLA [11]**	**APP [12]**	**Privacy Control [13]**
CPC16	CSP insurance policy	1. Does the provider describe its cyber-insurance policy regarding data protection and security breaches?	PLA16		
CPC17	Intended use of service	1. Does the provider indicate that consumer data will not be processed in a way that is not intended by the use of service, e.g., no transfer of data for marketing purpose?		APP7	
CPC18	Dissemination of Privacy Program Information	1. Does the provider make its privacy program information available and easily accessible?			TR-3

จากตาราง ผู้ใช้บริการคลาวด์จะทำการประเมินผู้ให้บริการจากคำถามโดยพิจารณาข้อมูลที่ผู้ให้บริการเผยแพร่อยู่ เช่น บนหน้าเว็บของผู้ให้บริการ ข้อตกลงการใช้งาน (Term of use) และนโยบายความเป็นส่วนตัว (Privacy Policy) จากนั้นจะให้คะแนนตามข้อคำถามของ Cloud Privacy Control Questionnaire โดยเกณฑ์การให้คะแนนมีดังนี้

1. หากผู้ให้บริการกล่าวถึงการทำตามคำถาม จะได้ 1 คะแนนในข้อนั้น
2. หากผู้ให้บริการมีหลักฐานซึ่งแสดงว่าเป็นไปตามข้อคำถาม เช่น มีรายละเอียดของข้อมูลอย่างชัดเจน มีการปฏิบัติตามมาตรฐานสากล มาตรฐานอุตสาหกรรม หรือกฎหมาย มีใบรับรอง (Certificate) หรือรายงานแสดงการปฏิบัติตาม เป็นต้น จะได้คะแนนเพิ่มอีก 1 คะแนน ในข้อคำถามนั้น

เมื่อมีการให้คะแนนตามข้อคำถามทั้งหมดแล้ว ผู้ใช้บริการสามารถคำนวณคะแนนความโปร่งใสด้านการควบคุมความเป็นส่วนตัวได้จาก

$$T_{Provider} = \left(\frac{\sum_{i=1}^{n}(c_i + e_i)}{2n}\right) \quad (9)$$

โดยที่ $T_{Provider}$ = Privacy control transparency level of provider

n = Number of privacy control questions, n = 42

c_i = Compliance score for privacy control question i, 1 = Compliance and 0 = Non-Compliance

e_i = Evidence score for privacy control question i, 1= Evidence present and 0 = No evidence or non-compliance

ตัวอย่าง องค์กรกรณีศึกษาบริษัทโฆษณาทำการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวของ Microsoft Azure ตามข้อคำถามต่าง ๆ เช่น

CPC1.1 Does the provider specify its name, its representative, and address?

องค์กรทำการตรวจสอบบนเว็บไซต์ Microsoft Azure : https://azure.microsoft.com/en-us/overview/contact-us/ มีการแสดงที่อยู่ ข้อมูลการติดต่อ ฝ่ายต่าง ๆ ที่สามารถติดต่อได้ ตัวแทนในประเทศไทย ดังนั้นคะแนนส่วนทำตามข้อคำถามได้ 1 คะแนนและได้คะแนนส่วนหลักฐานอีก 1 คะแนนเพราะข้อมูลปรากฏบนเว็บไซต์อย่างชัดเจน

CPC1.2 Does the provider specify its role in processing of consumer data (i.e. controller, joint-controller, processor or subprocessor)?

องค์กรตรวจสอบข้อมูลส่วน Privacy Statement : http://www.microsoft.com/en-us/privacystatement/default.aspx มีการระบุถึงบทบาทการเป็น Data Controller ของ Microsoft และระบุการมี affiliates, subsidiaries และผู้ให้บริการที่ Microsoft ไปใช้บริการ ดังนั้นคะแนนส่วนทำตามข้อคำถามได้ 1 คะแนนและได้คะแนนส่วนหลักฐานอีก 1 คะแนนเพราะข้อมูลปรากฏบนเว็บไซต์อย่างชัดเจน

CPC1.3 Does the provider specify contact information of the person in charge of data protection matters (e.g. Data Protection Officer, Information Security Officer)?

องค์กรตรวจสอบข้อมูลส่วน Privacy Statement : http://www.microsoft.com/en-us/privacystatement/default.aspx มีการระบุช่องทางในการติดต่อ Chief Privacy Officer ดังนั้นคะแนนส่วนทำตามข้อคำถามได้ 1 คะแนนและได้คะแนนส่วนหลักฐานอีก 1 คะแนนเพราะมีหน้าฟอร์มสำหรับการส่งคำถามเพื่อติดต่อปรากฏบนเว็บไซต์อย่างชัดเจน

จากการประเมิน องค์กรพบว่า Microsoft Azure ปฏิบัติตาม CPCQ 37 ข้อ และมีหลักฐานแสดง 32 ข้อสามารถหา $T_{Provider}$ ได้จาก (9)

$$T_{Provider} = (37 + 32) / (2 * 42)$$
$$= 0.8214$$

3.3 การประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว

การประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว (Risk of Privacy Loss) ของการใช้บริการจัดเก็บข้อมูลบนคลาวด์ ใช้แนวคิดจากการประเมินดัชนีความเสี่ยง (Risk Index) [21] ซึ่งคำนวณได้จาก

Risk Index = Impact of risk event x Probability of occurrence (10)

โดยที่ Impact of risk event คือผลกระทบจากการเกิดเหตุการณ์ที่เป็นความเสี่ยง และ
Probability of occurrence คือความน่าจะเป็นของการเกิดเหตุการณ์ที่เป็นความเสี่ยง

ในงานวิจัยนี้เหตุการณ์ที่เป็นความเสี่ยงหมายถึงการสูญเสียความเป็นส่วนตัว ผู้วิจัยใช้แนวคิดที่ว่าผลกระทบที่เกิดจากการสูญเสียความเป็นส่วนตัวประเมินได้จากระดับความอ่อนไหวของข้อมูลผู้ใช้บริการ และความน่าจะเป็นหรือโอกาสที่จะเกิดการสูญเสียความเป็นส่วนตัวนั้นเกิดจากความไม่โปร่งใสด้านการควบคุมความเป็นส่วนตัว ซึ่งจะสะท้อนถึงการควบคุมความเป็นส่วนตัวที่ไม่ดี ดังนั้นการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของการใช้บริการจัดเก็บข้อมูลบนคลาวด์ จึงคำนวณได้จาก

$$R_{Privacy} = (1-T_{Provider})*S_{Data} \quad (11)$$

โดยที่ $R_{Privacy}$ = Privacy risk of using cloud storage of provider, $R_{Privacy}$ is in [0,1]
$T_{Provider}$ = Privacy control transparency level of provider from (9)
S_{Data} = Sensitivity level of consumer data from (8)

ในการใช้งาน เนื่องจากค่า $R_{Privacy}$ อยู่ในช่วงตั้งแต่ 0 – 1 ผู้วิจัยได้จัดระดับช่วงค่าความเสี่ยงเป็น 5 ระดับเพื่อเป็นทางเลือกให้กับผู้ใช้บริการในการแปลความหมายค่าความเสี่ยง ดังนี้

ค่า $R_{Privacy}$ [0, 0.2] ถือเป็นความเสี่ยงระดับต่ำ

ค่า $R_{Privacy}$ (0.2, 0.4] ถือเป็นความเสี่ยงระดับค่อนข้างต่ำ

ค่า $R_{Privacy}$ (0.4, 0.6] ถือเป็นความเสี่ยงระดับปานกลาง

ค่า $R_{Privacy}$ (0.6, 0.8] ถือเป็นความเสี่ยงระดับค่อนข้างสูง

ค่า $R_{Privacy}$ (0.8, 1] ถือเป็นความเสี่ยงระดับสูง

ตัวอย่าง

องค์กรกรณีศึกษาทำการคำนวณค่าความเสี่ยงของการสูญเสียความเป็นส่วนตัวของข้อมูลแผนกบัญชีที่ต้องการนำไปจัดเก็บบน Microsoft Azure โดย (11) ได้ผลดังนี้

$$R_{Privacy}\text{ (Microsoft Azure)} = (1\text{-}T_{Provider}\text{(Microsoft Azure)})*S_{Data}\text{ (FN)}$$
$$= (1 - 0.8214) * 0.5994$$
$$= 0.1786 * 0.5994$$
$$= 0.1071$$

ดังนั้นค่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวขององค์กรกรณีศึกษาเมื่อต้องการนำข้อมูลขึ้นไปจัดเก็บบน Microsoft Azure ถือว่าอยู่ในระดับต่ำ

3.4 การทวนสอบวิธีการประเมิน

การทวนสอบวิธีการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวสำหรับบริการจัดเก็บข้อมูลบนคลาวด์มีสามด้านคือ ด้านการประเมินความอ่อนไหวของข้อมูลผู้ใช้บริการที่จัดเก็บ ด้านการประเมินความอ่อนไหวของข้อมูลที่ผู้ให้บริการร้องขอ และด้านการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัว โดยมีรายละเอียดดังนี้

1. การทวนสอบวิธีการประเมินความอ่อนไหวของข้อมูลผู้ใช้บริการที่จัดเก็บ

ในเบื้องต้นผู้วิจัยมีแนวคิดในการประเมินความอ่อนไหวของข้อมูลที่จะนำขึ้นไปจัดเก็บบนคลาวด์ S_{Stored} ในสองแนวทางคือ

1.1 กำหนดค่าความอ่อนไหวของข้อมูลทั้งหมดที่จะนำขึ้นไปจัดเก็บบนคลาวด์โดยใช้ค่าความอ่อนไหวของประเภทข้อมูลที่จะจัดเก็บซึ่งมีค่าสูงสุดตามหลักการ High Water Mark แทน

ค่าความอ่อนไหวของข้อมูลทั้งหมดที่จะจัดเก็บบนคลาวด์ ดังที่ได้อธิบายไว้แล้วในหัวข้อที่ 3.1.1 ซึ่งจากตัวอย่างการจัดเก็บข้อมูลของแผนกบัญชีขององค์กรกรณีศึกษาจะได้ค่าความอ่อนไหวเป็น 0.6667

1.2 คำนวณค่าความอ่อนไหวของข้อมูลทั้งหมดที่จะนำขึ้นไปจัดเก็บบนคลาวด์โดยการพิจารณาจากค่าความอ่อนไหวของแต่ละประเภทข้อมูลที่จะจัดเก็บ โดยแทนค่าความอ่อนไหว High, Moderate, Low และ N/A ด้วยคะแนนเท่ากับ 3, 2, 1 และ 0 ตามลำดับแล้วทำการนอร์มัลไลซ์ค่า จากนั้นนำไปหาค่าเฉลี่ยเพื่อให้ได้ค่าความอ่อนไหวของข้อมูลทั้งหมด ตัวอย่างเช่น ในการจัดเก็บข้อมูลของแผนกบัญชีขององค์กรกรณีศึกษาทั้ง 7 ประเภทข้อมูลในกลุ่ม Financial Management ซึ่งแต่ละประเภทข้อมูลมีค่าความอ่อนไหวเป็น Low, Moderate, Moderate, Moderate, Moderate, Moderate และ Moderate ผู้วิจัยจะแทนค่าความอ่อนไหวของทั้ง 7 ประเภทข้อมูลเป็น 1, 2, 2, 2, 2, 2 และ 2 ซึ่งจะได้ค่าที่นอร์มัลไลซ์แล้วคือ 1/3, 2/3, 2/3, 2/3, 2/3, 2/3 และ 2/3 จากนั้นคำนวณค่าเฉลี่ยของค่าเหล่านี้เพื่อให้ได้เป็นค่าความอ่อนไหวของข้อมูลที่จะจัดเก็บ เท่ากับ 0.619

จากทั้งสองแนวทาง ผู้วิจัยเลือกแนวทางในข้อที่ 1.1 เนื่องจากผู้ใช้บริการจัดเก็บข้อมูลหลายประเภทร่วมกัน ดังนั้นผลกระทบต่อองค์กรจากความอ่อนไหวของข้อมูลประเภทหนึ่งอาจจะส่งผลต่อข้อมูลประเภทอื่นที่จัดเก็บร่วมกันได้ ผู้ใช้บริการจึงน่าจะคาดหวังให้ผู้ให้บริการสามารถดูแลและจัดการข้อมูลโดยเฉพาะประเภทที่มีความอ่อนไหวสูงได้ ผู้วิจัยจึงเห็นว่าค่าความอ่อนไหวของข้อมูลทั้งหมดที่จะนำขึ้นไปจัดเก็บบนคลาวด์ควรใช้ค่าความอ่อนไหวสูงสุดของข้อมูลประเภทต่าง ๆ ที่จะจัดเก็บเป็นตัวแทนค่าความอ่อนไหวของข้อมูลทั้งหมด การแทนค่าความอ่อนไหวของข้อมูลทั้งหมดด้วยค่าเฉลี่ยตามแนวทางที่ 1.2 จะทำให้ข้อมูลบางประเภทซึ่งมีค่าความอ่อนไหวสูงกว่าค่าเฉลี่ยอาจไม่ได้รับการดูแลจัดการที่ดีพอ

2. การทวนสอบวิธีการประเมินความอ่อนไหวของข้อมูลที่ผู้ให้บริการร้องขอ

ในการประเมินความอ่อนไหวของข้อมูลที่ผู้ให้บริการร้องขอ $S_{Requested}$ โดยอิงจาก Cross Table ที่ผู้ใช้บริการสร้างขึ้นสำหรับผู้ให้บริการแต่ละราย มีการคำนวณจากข้อมูลส่วนบุคคลเฉพาะที่ผู้ให้บริการแต่ละรายร้องขอ และมีการนอร์มัลไลซ์ค่าความอ่อนไหวของแต่ละแอตทริบิวต์ S(d) ก่อนนำมาหาค่าเฉลี่ยให้ได้เป็นค่าความอ่อนไหวของข้อมูล $S_{Requested}$ ที่ผู้ให้บริการแต่ละรายร้องขอ ดังนั้นค่า $S_{Requested}$ ที่ได้จะไม่ขึ้นกับจำนวนข้อมูล

แอตทริบิวต์ที่ถูกร้องขอและผู้ใช้บริการสามารถเปรียบเทียบค่า $S_{Requested}$ ของผู้ให้บริการรายต่าง ๆ ซึ่งสร้างจาก Cross Table ที่ต่างกันได้

3. การทวนสอบวิธีการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัว

ผู้วิจัยกำหนดแบบสอบถาม CPCQ โดยอิงจากเอกสาร Privacy Level Agreement (PLA) เป็นหลัก ซึ่ง PLA เป็นเอกสารแนวปฏิบัติด้านการควบคุมความเป็นส่วนตัวของบริการคลาวด์โดยตรง และกำหนดโดยองค์กร Cloud Security Alliance ซึ่งเป็นองค์กรที่กำหนดแนวปฏิบัติที่เกี่ยวข้องกับบริการคลาวด์โดยตรง ข้อคำถามจะครอบคลุมเนื้อหาทั้งหมดที่สรุปได้จาก PLA นอกจากนี้ผู้วิจัยได้ทวนสอบเนื้อหาใน PLA กับหลักการด้านความเป็นส่วนตัวอื่น ๆ ได้แก่ Australian Privacy Principles (APP) ซึ่งเป็นหลักปฏิบัติของบริการคลาวด์ในออสเตรเลียซึ่งกำหนดโดยรัฐบาลออสเตรเลีย และ Security and Privacy Controls ของ NIST ซึ่งกล่าวถึงการควบคุมความมั่นคงและความเป็นส่วนตัวของระบบสารสนเทศโดยทั่วไปรวมทั้งระบบคลาวด์ด้วย โดยพบว่าเนื้อหาของ PLA, APP และ Security and Privacy Controls มีความคล้ายคลึงกัน แต่มีเพียงบางประเด็นที่ APP และ Security and Privacy Controls กล่าวถึง ผู้วิจัยจึงนำมากำหนดเป็นข้อคำถามเพิ่มเติมใน CPCQ การทวนสอบความสอดคล้องกันของ PLA, APP และ Security and Privacy Controls แสดงไว้แล้วในตารางที่ 3.4

3.5 การพัฒนาระบบสนับสนุนการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของการใช้บริการจัดเก็บข้อมูลบนคลาวด์

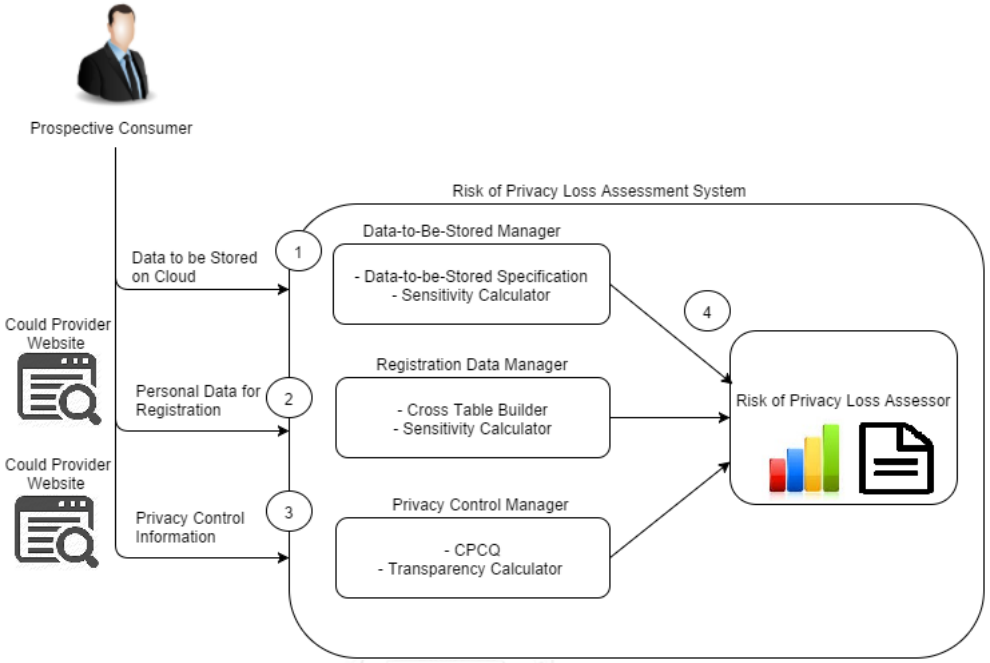
การพัฒนาระบบสนับสนุนการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวมีการพัฒนาแบบ Windows Application โดยภาษาที่ใช้ในการพัฒนาคือ VB.Net โดยระบบสามารถสนับสนุนผู้ใช้บริการในการประเมินทั้ง 3 ส่วนคือ

1. การประเมินค่าความอ่อนไหวของข้อมูลที่จะนำไปจัดเก็บบนคลาวด์
2. การประเมินค่าความอ่อนไหวของข้อมูลที่ผู้ให้บริการร้องขอเพื่อเข้าใช้บริการ
3. การประเมินความโปร่งใสในด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการคลาวด์

3.5.1 ส่วนประกอบของระบบ

ระบบจะสนับสนุนผู้ใช้บริการที่ต้องการนำข้อมูล 1 ชุดซึ่งอาจประกอบด้วยข้อมูลหลายประเภทไปจัดเก็บบนคลาวด์กับผู้ให้บริการ 1 ราย ภาพรวมของระบบเป็นดังภาพที่ 3.2

ส่วนประกอบหลักของระบบประกอบด้วย 4 ส่วนคือ Data-to-be-Stored Manager, Registration Data Manager, Privacy Control Manager และRisk of Privacy Loss Assessor แต่ละส่วนมีการทำงานดังต่อไปนี้



ภาพที่ 3.2 *ระบบการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์*

Data-to-be-Stored Manager รับข้อมูลประเภทต่าง ๆ ที่จะถูกจัดเก็บบนคลาวด์จากผู้ใช้บริการผ่านส่วน Data-to-be-Stored Specification และคำนวณค่าความอ่อนไหวของข้อมูลที่จัดเก็บโดยส่วน Sensitivity Calculator

Registration Data Manager รับข้อมูลส่วนบุคคลที่ผู้ให้บริการร้องขอในการลงทะเบียนเข้าใช้งาน ซึ่งผู้ใช้บริการได้สำรวจจากเว็บไซต์ผู้ให้บริการ เพื่อนำมาสร้าง Cross Table โดยส่วน Cross Table Builder จากนั้นทำการคำนวณค่าความอ่อนไหวของข้อมูลที่ผู้ให้บริการร้องขอโดยส่วน Sensitivity Calculator

Privacy Control Manager รับข้อมูลการประเมินด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการ ซึ่งผู้ใช้บริการได้สำรวจจากเว็บไซต์ผู้ให้บริการ ผ่านแบบประเมิน CPCQ จากนั้นทำการคำนวณค่าความโปร่งใสด้านการควบคุมความเป็นส่วนตัวโดยส่วน Transparency Calculator

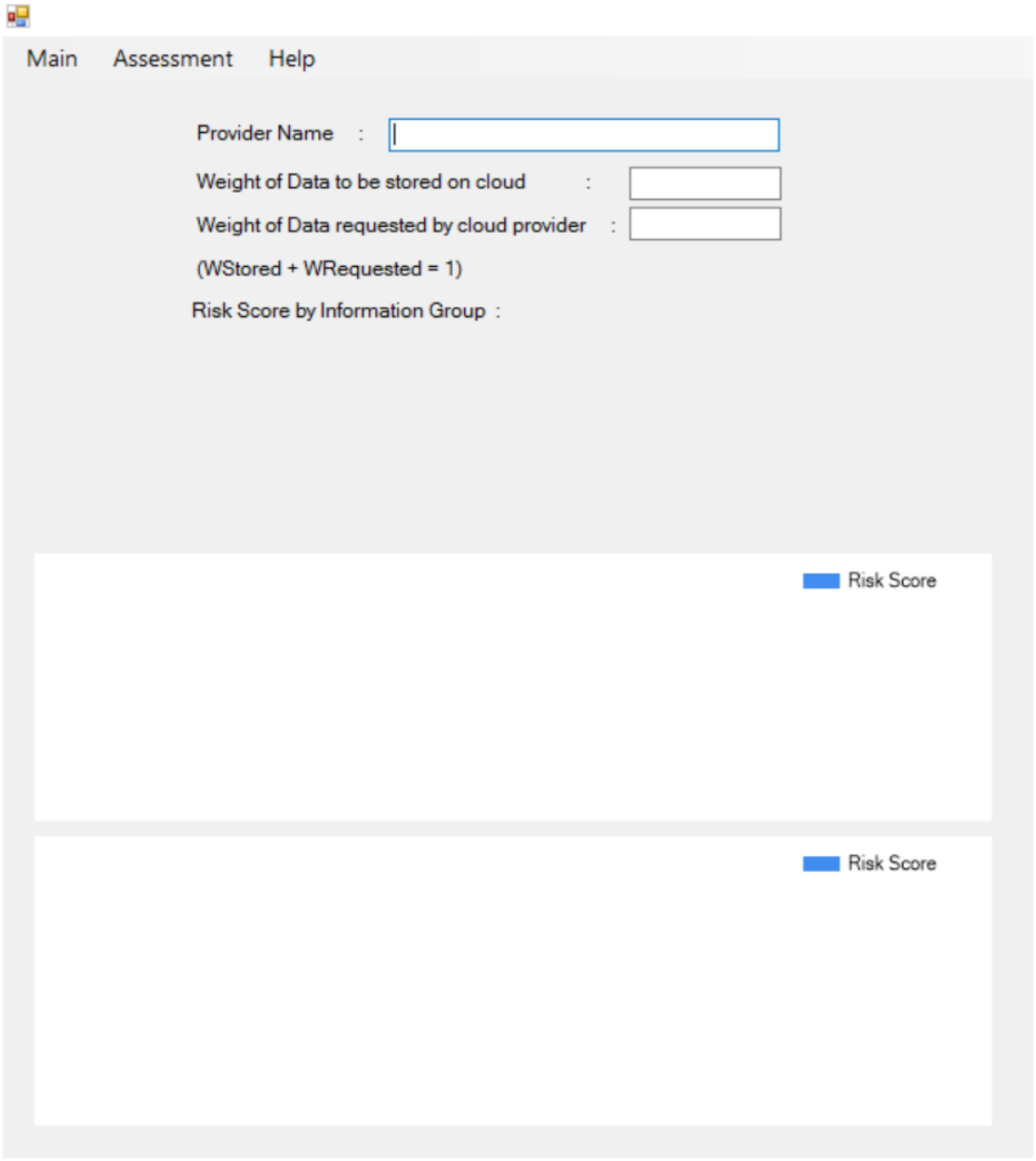
Risk of Privacy Loss Assessor รับค่าความอ่อนไหวของข้อมูลที่จัดเก็บและข้อมูลที่ผู้ให้บริการร้องขอ และค่าความโปร่งใสด้านการควบคุมความเป็นส่วนตัวจากส่วนประกอบทั้งสาม

ส่วนข้างต้น เพื่อนำมาคำนวณค่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของผู้ให้บริการ และแสดงผลการประเมินเป็นกราฟของระดับความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของประเภทข้อมูลในกลุ่มต่าง ๆ หากจะจัดเก็บกับผู้ให้บริการรายนี้

3.5.2 ส่วนต่อประสานผู้ใช้ของระบบ

หน้าจอส่วนต่อประสานของผู้ใช้ระบบประกอบด้วยหน้าจอหลัก หน้าจอการประเมินความอ่อนไหวของข้อมูลที่จะนำขึ้นไปจัดเก็บบนคลาวด์ หน้าจอการประเมินความอ่อนไหวของข้อมูลที่ผู้ให้บริการร้องขอ และหน้าจอการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการคลาวด์

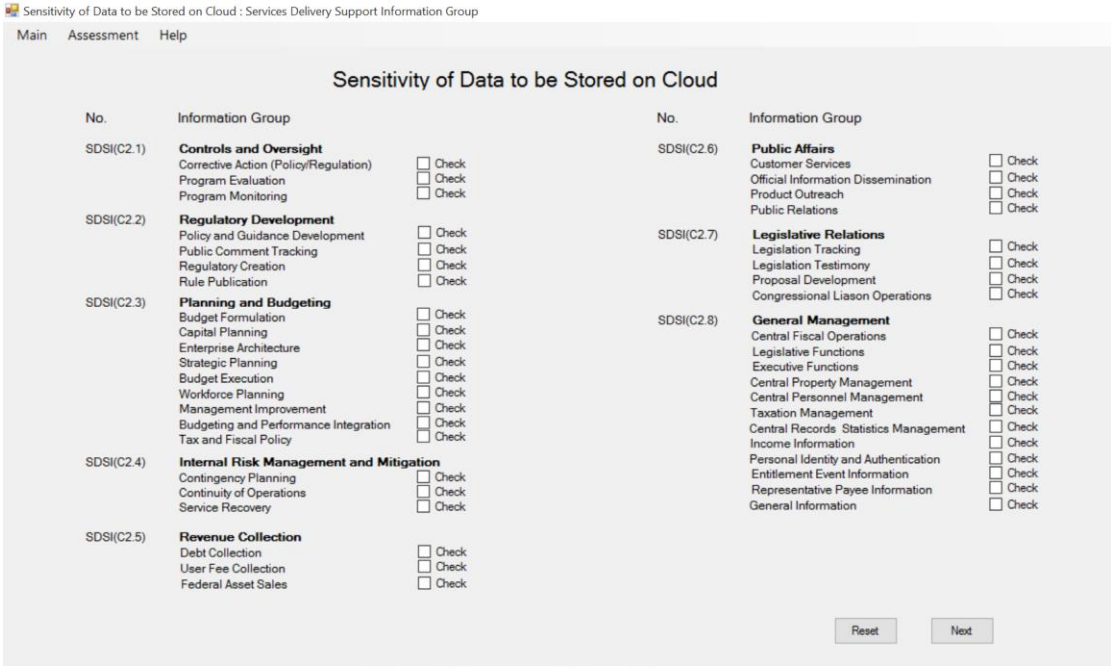
1. หน้าจอหลัก ประกอบด้วยเมนู Main สำหรับการทำการคำนวณค่าความเสี่ยงและแสดงผล เมนู Assessment สำหรับการระบุข้อมูลต่าง ๆ เพื่อใช้ในการประเมิน เมนู Help สำหรับอธิบายขั้นตอนการประเมิน และมีพื้นที่ส่วนล่างในการแสดงคะแนนและกราฟการประเมิน ดังภาพที่ 3.3



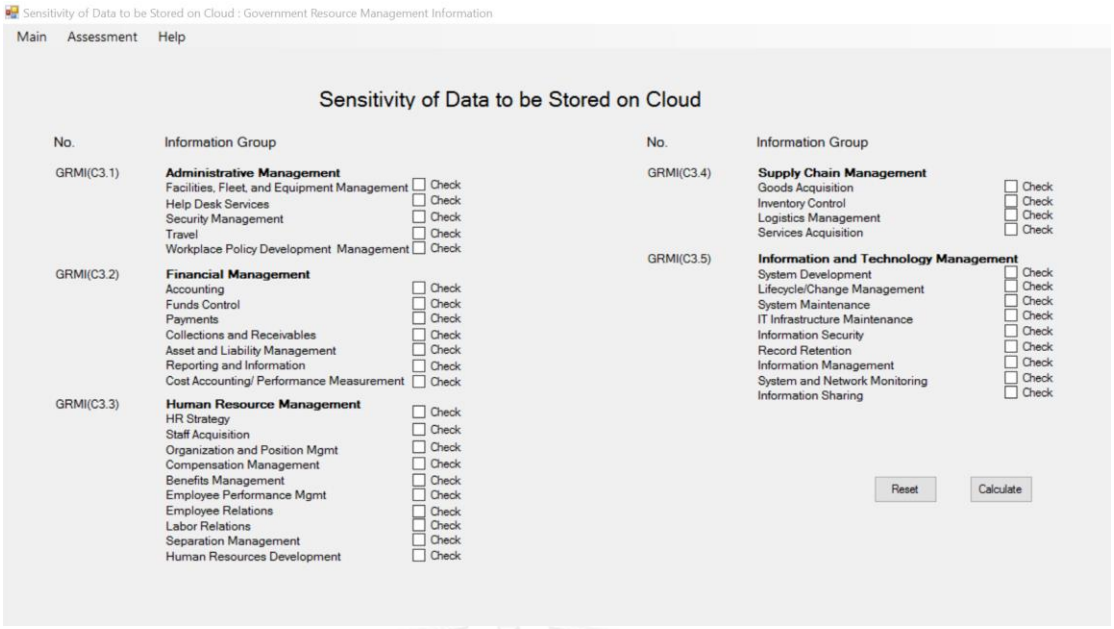
ภาพที่ 3.3 *หน้าจอหลักของระบบประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์*

2. หน้าจอการประเมินความอ่อนไหวของข้อมูลที่จะนำขึ้นไปจัดเก็บบนคลาวด์ โดยจะแบ่งเป็นสองส่วนตามกลุ่มข้อมูลคือ Service Delivery Support Information และ Government Resources Management Information

วิธีการใช้งานคือทำการเลือกลุ่มข้อมูลที่จะนำขึ้นไปจัดเก็บบนคลาวด์โดยหน้าแรกจะแสดงกลุ่มข้อมูล Service Delivery Support Information ดังภาพที่ 3.4 และหน้าที่สองจะแสดงกลุ่มข้อมูล Government Resources Management Information ดังภาพที่ 3.5 เมื่อสิ้นสุดการเลือกข้อมูลในหน้าที่สองให้กด Calculate ระบบจะคำนวณค่าความอ่อนไหวของข้อมูลที่จะนำขึ้นไปจัดเก็บบนคลาวด์



ภาพที่ 3.4 *หน้าจอการประเมินค่าความอ่อนไหวของข้อมูลที่จะนำไปจัดเก็บบนคลาวด์ส่วนแรก*

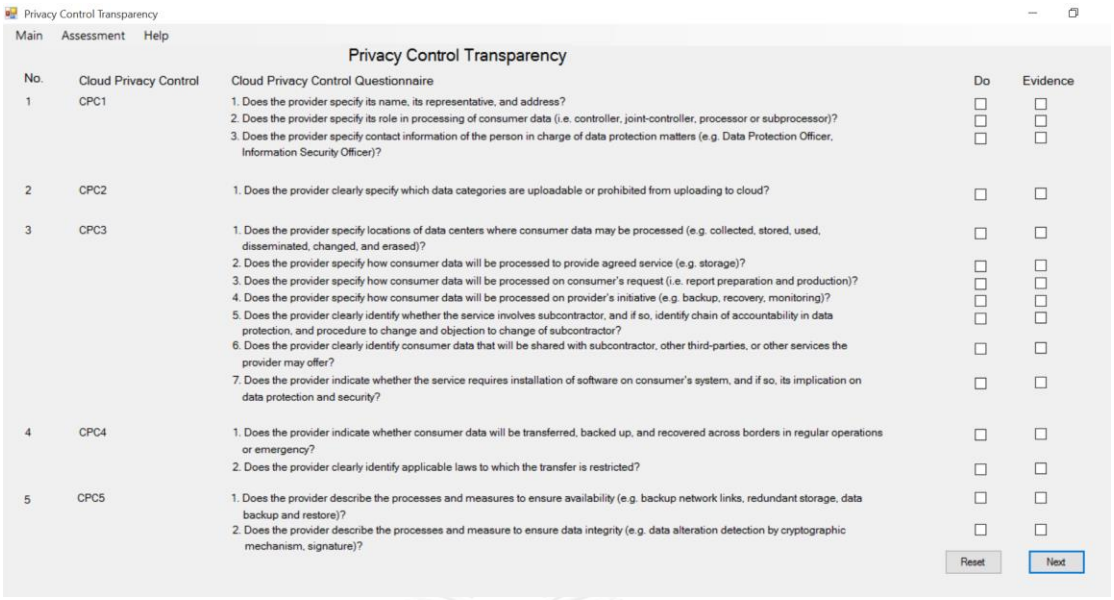


ภาพที่ 3.5 *หน้าจอการประเมินค่าความอ่อนไหวของข้อมูลที่จะนำไปจัดเก็บบนคลาวด์ส่วนที่สอง*

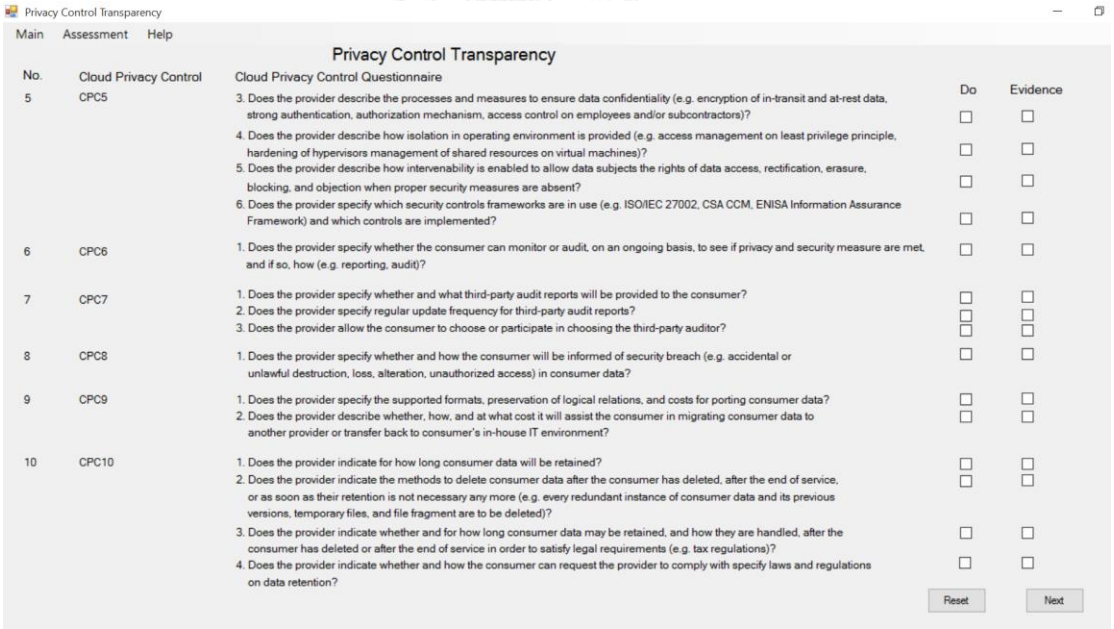
3. หน้าจอการประเมินความอ่อนไหวของข้อมูลที่ถูกร้องขอโดยผู้ให้บริการเพื่อเข้าใช้บริการ ส่วนนี้เป็นการประเมินความอ่อนไหวของข้อมูลที่ผู้ให้บริการร้องขอ วิธีการทำงานคือผู้ใช้บริการจะกรอกแอตทริบิวต์ข้อมูลที่ผู้ให้บริการร้องขอลงไปในระบบ และระบุว่าแอตทริบิวต์อยู่ในคอนเซปต์ใดบ้างและมีลักษณะใดจากรายการที่ให้มาได้แก่ Basic, Private, Identity, Finance และ Derive other data (เลือกได้หลายรายการ) ดังภาพที่ 3.6 เสร็จแล้วทำการกด Add ข้อมูลเข้าระบบ เมื่อระบุแอตทริบิวต์ที่ผู้ให้บริการร้องขอครบแล้วให้กด Calculate ระบบจะคำนวณค่าความอ่อนไหวของข้อมูลที่ถูกร้องขอโดยผู้ให้บริการเพื่อเข้าใช้บริการ

ภาพที่ 3.6 *หน้าการประเมินความอ่อนไหวของข้อมูลที่ถูกร้องขอโดยผู้ให้บริการเพื่อเข้าใช้บริการ*

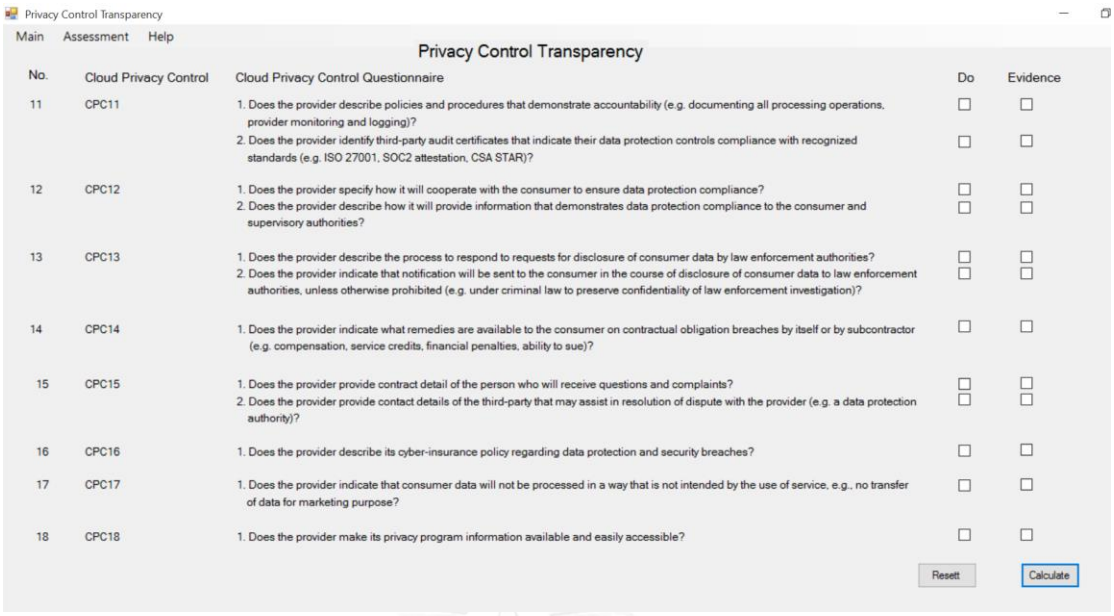
4. หน้าจอการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการจะแสดงข้อคำถามตามแบบประเมิน CPCQ จำนวนทั้งหมด 42 ข้อ แบ่งออกเป็น 3 หน้าจอดังภาพที่ 3.7 – 3.9 เพื่อให้ผู้ใช้บริการประเมินโดยตรวจสอบข้อมูล Term of use และ Privacy Policy ที่เผยแพร่บนหน้าเว็บไซต์ของผู้ให้บริการแล้วนำมาตอบคำถามในระบบ



ภาพที่ 3.7 *หน้าจอส่วนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการ ส่วนแรก*

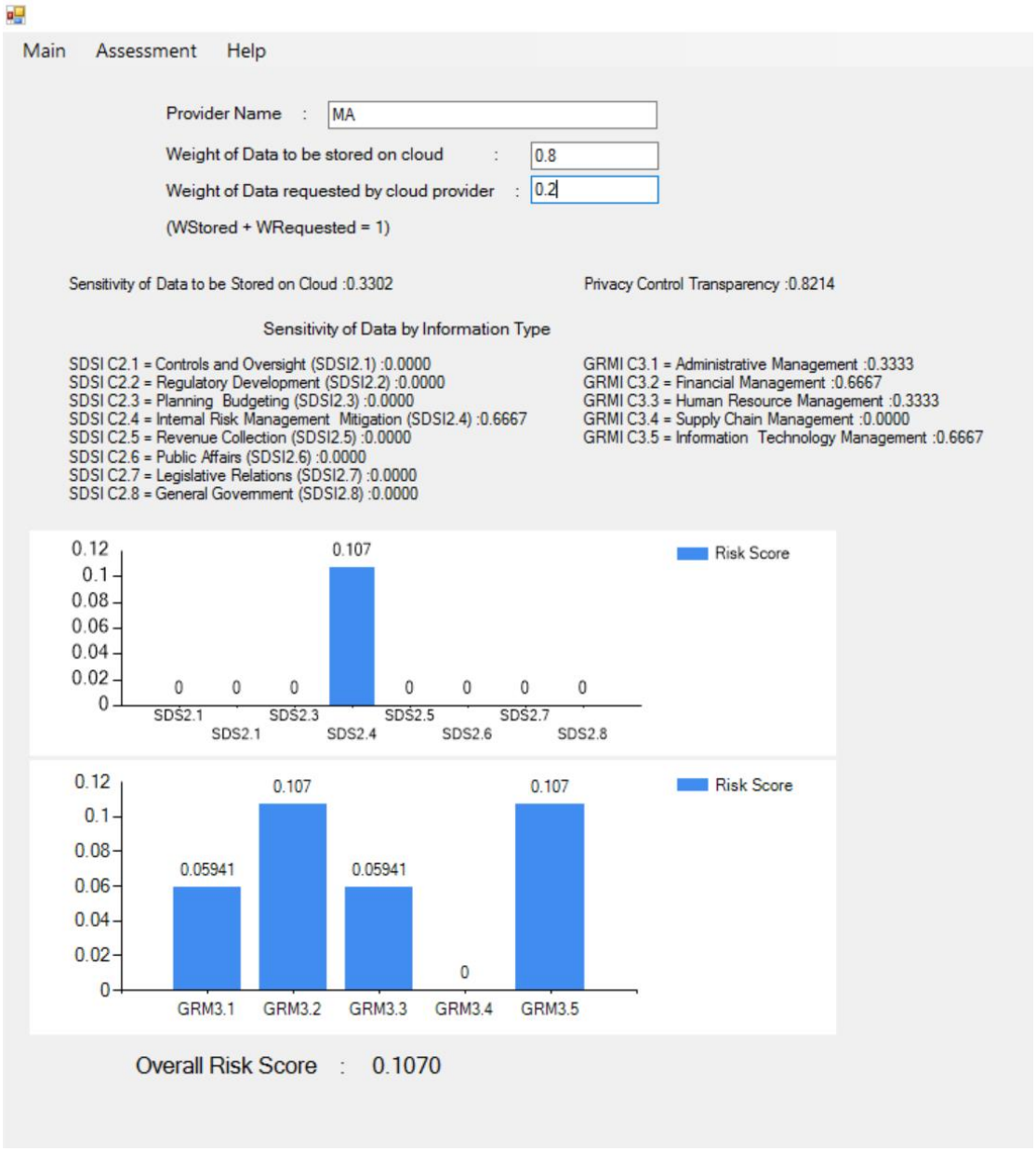


ภาพที่ 3.8 *หน้าจอส่วนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการ ส่วนที่สอง*



ภาพที่ 3.9 *หน้าจอส่วนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการ ส่วนที่สาม*

5. หน้าจอการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวสำหรับบริการจัดเก็บข้อมูลบนคลาวด์ ส่วนนี้เป็นส่วนสุดท้ายของการประเมินจะปรากฏที่หน้าจอหลัก โดยระบบจะให้ผู้ใช้บริการระบุข้อมูล ชื่อผู้ให้บริการ ค่าน้ำหนักของข้อมูลที่จะนำขึ้นไปจัดเก็บบนคลาวด์ และค่าน้ำหนักของข้อมูลที่ผู้ให้บริการร้องขอ ดังภาพที่ 3.10 ระบบจะทำการแสดงผลการประเมินออกมาเป็นกราฟเปรียบเทียบระดับความเสี่ยงของการสูญเสียความเป็นส่วนตัวของข้อมูลแยกตามประเภทข้อมูล และระดับความเสี่ยงรวม เมื่อนำข้อมูลไปจัดเก็บกับผู้ให้บริการคลาวด์ตามที่ระบุ



ภาพที่ 3.10 *หน้าจอหลักแสดงผลการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์*

บทที่ 4

การทดสอบและการประเมินผลการวิจัย

ในการทดลองประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวสำหรับบริการจัดเก็บข้อมูลบนคลาวด์ ผู้วิจัยใช้ข้อมูลขององค์กรกรณีศึกษาบริษัทโฆษณาแห่งหนึ่ง ซึ่งมีความสนใจจะนำข้อมูลของแผนกต่าง ๆ 5 แผนกได้แก่ แผนกบัญชี แผนกทรัพยากรบุคคล แผนกไอที แผนกจัดการด้านความเสี่ยง และ แผนกแอดมิน ไปจัดเก็บบนคลาวด์

ในการเลือกผู้ให้บริการคลาวด์มาทดลอง ผู้วิจัยรวบรวมข้อมูลผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์ 13 ราย ที่ได้เผยแพร่แบบประเมินตนเองทางด้านการควบคุมความมั่นคง (Security) ตามแนวปฏิบัติด้านความมั่นคง Cloud Control Matrix (CCM) ที่กำหนดโดย Cloud Security Alliance (CSA) ผู้ให้บริการแต่ละรายจะประเมินตนเองโดยตอบคำถามแต่ละข้อว่าได้ปฏิบัติตามแนวปฏิบัติด้านความมั่นคงหรือไม่ (ตอบว่าใช่หรือไม่ใช่) และเผยแพร่ไว้บนเว็บไซต์ CSA Security, Trust & Assurance Registry (STAR) [20] ผู้วิจัยจึงได้คำนวณผลรวมคะแนนการปฏิบัติตาม (ตอบว่าใช่) เพื่อเป็นคะแนนด้านความมั่นคงของผู้ให้บริการ จากนั้นเลือกผู้ให้บริการ 5 ราย ที่ได้คะแนนด้านการปฏิบัติตามความมั่นคงที่แตกต่างกันในลำดับที่ 1, 4, 7, 10 และ13 ได้แก่ Microsoft Azure (ลำดับที่ 1) Dropbox Business (ลำดับที่ 4) Citrix ShareFile (ลำดับที่ 7) Verizon Enterprise Solution (ลำดับที่ 10) และ SoftLayer (ลำดับที่ 13) มาทำการทดลอง รายละเอียดของคะแนนการปฏิบัติตามแนวปฏิบัติด้านความมั่นคงสามารถดูได้จากภาคผนวก ข

4.1 การทดลองการประเมินระดับความอ่อนไหวของข้อมูลผู้ใช้บริการ

ผู้วิจัยได้รวบรวมข้อมูลแผนกต่าง ๆ ขององค์กรกรณีศึกษามาทำการประเมิน 5 แผนกเพื่อคำนวณค่าความอ่อนไหวของข้อมูลที่จะนำขึ้นไปจัดเก็บบนคลาวด์ S_{Stored} ดังนี้

4.1.1 แผนกบัญชี (FN)

แผนกบัญชีต้องการจัดเก็บข้อมูล 7 ประเภท ในกลุ่ม Financial Management ซึ่งมีการคำนวณค่าความอ่อนไหวแสดงไว้แล้วในหัวข้อที่ 3.1.1 และได้ค่าความอ่อนไหวของข้อมูลที่จะนำขึ้นไปจัดเก็บบนคลาวด์เป็น

$$S_{Stored} = 0.6667$$

4.1.2 แผนกทรัพยากรบุคคล (HR)

แผนกทรัพยากรบุคคลขององค์กรกรณีศึกษาต้องการจัดเก็บข้อมูลในกลุ่ม Government Resources Management Information (GRMI) ประเภท Human Resource Management เป็นจำนวน 6 ประเภทข้อมูล ดังนี้

1. Staff Acquisition มีระดับความอ่อนไหวเท่ากับ Low
2. Organization & Position Mgmt. มีระดับความอ่อนไหวเท่ากับ Low
3. Employee Performance Mgmt. มีระดับความอ่อนไหวเท่ากับ Low
4. Employee Relations มีระดับความอ่อนไหวเท่ากับ Low
5. Labor Relations มีระดับความอ่อนไหวเท่ากับ Low
6. Human Resources Development มีระดับความอ่อนไหวเท่ากับ Low

สามารถกำหนดค่าความอ่อนไหวโดย (1) ได้เป็น

$$S_{Stored} = 0.3333$$

4.1.3 แผนกเทคโนโลยีสารสนเทศ (IT)

แผนกเทคโนโลยีสารสนเทศขององค์กรกรณีศึกษาต้องการจัดเก็บข้อมูลในกลุ่ม Government Resources Management Information (GRMI) ประเภท Information & Technology Management เป็นจำนวน 4 ประเภทข้อมูล ดังนี้

1. System Maintenance มีระดับความอ่อนไหวเท่ากับ Moderate
2. Record Retention มีระดับความอ่อนไหวเท่ากับ Low
3. Information Management มีระดับความอ่อนไหวเท่ากับ Moderate
4. System and Network Monitoring มีระดับความอ่อนไหวเท่ากับ Moderate

สามารถกำหนดค่าความอ่อนไหวโดย (1) ได้เป็น

$$S_{Stored} = 0.6667$$

4.1.4 แผนกการบริหารจัดการความเสี่ยง (RM)

แผนกการบริหารจัดการด้านความเสี่ยงขององค์กรกรณีศึกษาต้องการจัดเก็บข้อมูลในกลุ่ม Service Delivery Support Information (SDSI) ประเภท Internal Risk Management & Mitigation เป็นจำนวน 3 ประเภทข้อมูล ดังนี้

1. Contingency Planning มีระดับความอ่อนไหวเท่ากับ Moderate
2. Continuity of Operations มีระดับความอ่อนไหวเท่ากับ Moderate
3. Service Recovery มีระดับความอ่อนไหวเท่ากับ Low

สามารถกำหนดค่าความอ่อนไหวโดย (1) ได้เป็น

$$S_{Stored} = 0.6667$$

4.1.5 แผนกแอดมิน (AD)

แผนกแอดมินขององค์กรกรณีศึกษาต้องการจัดเก็บข้อมูลในกลุ่ม Government Resources Management Information (GRMI) ประเภท Administrative Management เป็นจำนวน 4 ประเภทข้อมูล ดังนี้

1. Facilities, Fleet, and Equipment Management มีระดับความอ่อนไหวเท่ากับ Low
2. Help Desk Services มีระดับความอ่อนไหวเท่ากับ Low
3. Travel มีระดับความอ่อนไหวเท่ากับ Low
4. Workplace Policy Development & Management มีระดับความอ่อนไหวเท่ากับ Low

สามารถกำหนดค่าความอ่อนไหวโดย (1) ได้เป็น

$$S_{Stored} = 0.3333$$

สรุปคะแนนความอ่อนไหวของข้อมูลที่จะจัดเก็บของ 5 แผนกได้ดังตารางที่ 4.1

ตารางที่ 4.1 *คะแนนความอ่อนไหวของข้อมูลที่จะนำขึ้นไปเก็บบนคลาวด์แยกตามแผนก*

Dept.	**Sensitivity of data to be stored on cloud (S_{Stored})**
FN	0.6667
HR	0.3333
IT	0.6667
RM	0.6667
AD	0.3333

4.2 การทดลองการประเมินระดับความอ่อนไหวของข้อมูลส่วนบุคคลที่ผู้ให้บริการร้องขอจากผู้ใช้บริการในการเข้าใช้

ผู้วิจัยสำรวจข้อมูลส่วนบุคคลที่ผู้ให้บริการร้องขอจากเว็บไซต์ผู้ให้บริการ 5 ราย ได้แก่ Microsoft Azure, Dropbox Business, Citrix ShareFile, Verizon Enterprise Solution และ SoftLayer เพื่อนำมาสร้าง Cross Table และคำนวณค่าความอ่อนไหวของข้อมูล

4.2.1 Microsoft Azure

ผู้วิจัยกำหนด Cross Table ของ Microsoft Azure ไว้ดังตารางที่ 3.2 และคำนวณค่า $S_{Requested}$ ไว้ดังตารางที่ 3.3 ในบทที่ 3

4.2.2 Dropbox Business

ผู้วิจัยกำหนด Cross Table ของ Dropbox Business ไว้ดังตารางที่ 4.2 และคำนวณค่า $S_{Requested}$ ไว้ดังตารางที่ 4.3

ตารางที่ 4.2 *Cross Table ของ Dropbox Business*

Concept/Attribute	First Name	Last Name	Team Name	Email	Contact Telephone	Company Size	Number of User	Billing Plan	Credit Card Number	Security Code	Expiration Date	Postal Code	Country
Basic	X	X	X	X	X	X						X	X
Private							X	X	X	X			
Identity		X	X						X				
Finance	X	X	X		X			X	X	X	X	X	X

ตารางที่ 4.3 *ค่าความอ่อนไหวของข้อมูลของ Dropbox Business*

Attribute	$D_c(d)$	$I_A(d)$	$P_A(d)$	$A_A(d)$	$S(d)$
First Name	2/4	0	0	0	0.5000
Last Name	3/4	12/13	0	0	1.6731
Team Name	3/4	12/13	0	0	1.6731
Email	1/4	0	0	1	1.2500
Contact Telephone	2/4	0	0	0	0.5000
Company Size	1/4	0	0	0	0.2500
Number of User	1/4	0	1	0	1.2500
Billing Plan	2/4	0	1	0	1.5000
Credit Card Number	3/4	11/13	1	0	2.5963
Security Code	2/4	0	1	0	1.5000
Expiration Date	1/4	0	0	0	0.2500
Postal Code	2/4	0	0	0	0.5000
Country	2/4	0	0	0	0.5000
					$S_{Requested}$ = 13.9423 / (4*13) = 0.2681

4.2.3 Citrix ShareFile

ผู้วิจัยกำหนด Cross Table ของ Citrix ShareFile ไว้ดังตารางที่ 4.4 และคำนวณค่า $S_{Requested}$ ไว้ดังตารางที่ 4.5

ตารางที่ 4.4 *Cross Table ของ Citrix ShareFile*

Concept/Attribute	**First Name**	**Last Name**	**Email**	**Company Name**	**Phone**	**Company Size**
Basic	X	X	X	X	X	X
Private						
Identity		X		X		
Finance	X	X		X	X	

ตารางที่ 4.5 *ค่าความอ่อนไหวของข้อมูลของ Citrix ShareFile*

Attribute	$D_c(d)$	$I_A(d)$	$P_A(d)$	$A_A(d)$	$S(d)$
First Name	2/4	0	0	0	0.5000
Last Name	3/4	6/6	0	0	1.7500
Email	1/4	0	0	1	1.2500
Company Name	3/4	6/6	0	0	1.7500
Phone	2/4	0	0	0	0.5000
Company Size	1/4	0	0	0	0.2500
					$S_{Requested}$ = 6 / (4*6) = 0.25

4.2.4 Verizon Enterprise Solution

ผู้วิจัยกำหนด Cross Table ของ Verizon Enterprise Solution ไว้ดังตารางที่ 4.6 และคำนวณค่า $S_{Requested}$ ไว้ดังตารางที่ 4.7

ตารางที่ 4.6 *Cross Table ของ Verizon Enterprise Solution*

Concept/Attribute	**First Name**	**Last Name**	**Contact Number**	**Email**	**Address**	**City**	**State**	**Country**	**Zip Code**	**User ID**
Basic	X	X	X	X	X	X	X	X	X	
Private										X
Identity		X								X
Finance	X	X	X		X	X	X	X	X	

ตารางที่ 4.7 *ค่าความอ่อนไหวของข้อมูลของ Verizon Business Solution*

Attribute	$D_c(d)$	$I_A(d)$	$P_A(d)$	$A_A(d)$	$S(d)$
First Name	2/4	0	0	0	0.5000
Last Name	3/4	9/10	0	0	1.6500
Contact Number	1/4	0	0	0	0.5000
Email	1/4	0	0	1	1.2500
Address	2/4	0	0	0	0.5000
City	2/4	0	0	0	0.5000
State	2/4	0	0	0	0.5000
Country	2/4	0	0	0	0.5000
Zip Code	2/4	0	0	0	0.5000
User ID	2/4	1/10	1	0	1.6000
					$S_{Requested}$ = 8 / (4*10) = 0.2

4.2.5 SoftLayer

ผู้วิจัยกำหนด Cross Table ของ SoftLayer ไว้ดังตารางที่ 4.8 และคำนวณค่า $S_{Requested}$ ไว้ดังตารางที่ 4.9

ตารางที่ 4.8 *Cross Table ของ SoftLayer*

Concept/Attribute	First Name	Last Name	Company Name	Work Phone	Address	City	State	Country	Vat ID	Credit Card	Security Code	Expiration Date
Basic	X	X	X	X	X	X	X	X				
Private										X	X	
Identity		X	X						X	X		
Finance	X	X	X	X	X	X	X	X	X	X	X	X

ตารางที่ 4.9 *ค่าความอ่อนไหวของข้อมูลของ SoftLayer*

Attribute	$D_c(d)$	$I_A(d)$	$P_A(d)$	$A_A(d)$	$S(d)$
First Name	2/4	0	0	0	0.5000
Last Name	3/4	12/12	0	0	1.7500
Company Name	3/4	12/12	0	0	1.7500
Work Phone	2/4	0	0	0	0.5000
Address	2/4	0	0	0	0.5000
City	2/4	0	0	0	0.5000
State	2/4	0	0	0	0.5000
Country	2/4	0	0	0	0.5000
Vat ID	2/4	12/12	0	0	1.5000
Credit Card Number	3/4	12/12	1	0	2.7500
Security Code	2/4	0	1	0	1.5000
Expiration Date	1/4	0	0	0	0.2500
					$S_{Requested}$ = 12.50 / (4 * 12) = 0.2604

สรุปคะแนนความอ่อนไหวของข้อมูลที่ผู้ให้บริการ 5 ราย ร้องขอได้ดังตารางที่ 4.10

ตารางที่ 4.10 *คะแนนความอ่อนไหวของข้อมูลที่ผู้ให้บริการร้องขอแยกตามผู้ให้บริการ*

Provider Name	$S_{Requested}$
Microsoft Azure	0.3302
Dropbox Business	0.2681
Citrix Sharefile	0.2500
Verizon Business Solution	0.2000
SoftLayer	0.2604

4.3 การทดลองการประเมินระดับความอ่อนไหวของข้อมูลผู้ใช้บริการ

จากค่า S_{Stored} และ $S_{Requested}$ ที่ได้จากหัวข้อที่ 4.1 และ 4.2 ผู้วิจัยคำนวณหาค่าความอ่อนไหวของข้อมูลผู้ใช้บริการหากมีการจัดเก็บกับผู้ให้บริการทั้ง 5 ราย โดยใช้ (8) โดยที่กำหนดค่าน้ำหนักของข้อมูลที่จะนำไปจัดเก็บบนคลาวด์ (W_{Stored}) เท่ากับ 0.8 และค่าน้ำหนักของข้อมูลที่ผู้ให้บริการร้องขอเพื่อเข้าใช้บริการ ($W_{Requested}$) เท่ากับ 0.2 ได้ผลดังตารางที่ 4.11

ตารางที่ 4.11 *สรุปค่าความอ่อนไหวของข้อมูลของผู้ใช้บริการ จากตัวอย่างการทดลอง 5 แผนกและ 5 ผู้ให้บริการคลาวด์*

Dept. / Cloud Provider	Microsoft Azure	Dropbox Business	Citrix ShareFile	Verizon Business Solution	SoftLayer
FN	0.5994	0.5870	0.5834	0.5734	0.5854
HR	0.3327	0.3203	0.3166	0.3066	0.3187
IT	0.5994	0.5870	0.5834	0.5734	0.5854
RM	0.5994	0.587	0.5834	0.5734	0.5854
AD	0.3327	0.3203	0.3166	0.3066	0.3187
Company Overall	0.5994	0.5870	0.5834	0.5734	0.5854

4.4 การทดลองการประเมินความโปร่งใสในด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการ

ผู้วิจัยสำรวจข้อมูลด้านการควบคุมความเป็นส่วนตัวจาก Privacy Policy และ Term of use จากเว็บไซต์ผู้ให้บริการ 5 ราย และตอบข้อคำถามในแบบประเมิน CPCQ โดยผลการตอบแบบประเมินจะแสดงไว้ในภาคผนวก ก และสรุปคะแนนความโปร่งใสด้านการควบคุมความเป็นส่วนตัวซึ่งคำนวณจาก (9) ได้ผลดังตารางที่ 4.12

ตารางที่ 4.12 *คะแนนความโปร่งใสและคะแนนความเสี่ยงด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการแยกตามผู้ให้บริการ*

Provider Name	Score	$T_{provider}$
Microsoft Azure	69	0.8214
Dropbox Business	62	0.7381
Citrix ShareFile	49	0.5833
Verizon Business Solution	47	0.5595
SoftLayer	42	0.5000

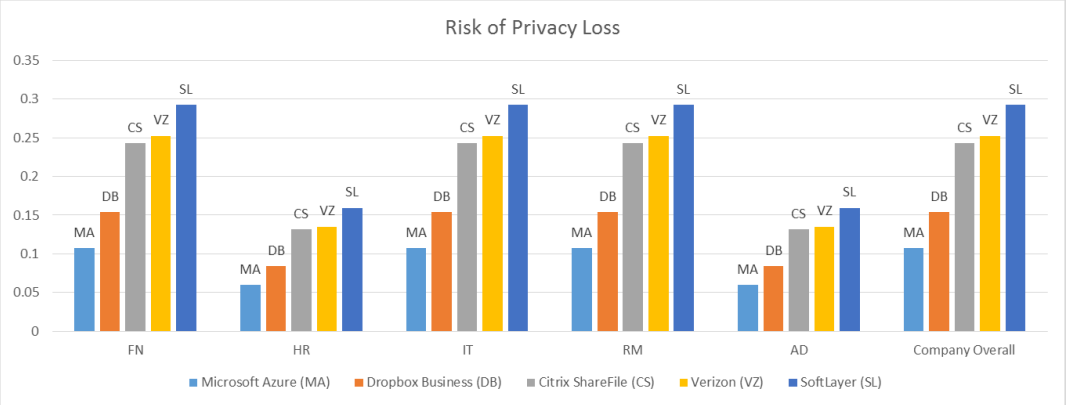
4.5 การทดลองการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว

จากค่า S_{Data} และ $T_{Provider}$ ที่ได้จากข้อที่ 4.3 และ 4.4 ผู้วิจัยคำนวณหาค่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของบริการจัดเก็บข้อมูลบนคลาวด์ $R_{Privacy}$ ได้จาก (11) ดังแสดงในตารางที่ 4.13

ตารางที่ 4.13 *คะแนนความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของผู้ให้บริการคลาวด์แยกตามผู้ให้บริการ*

Provider Name	Microsoft Azure	Dropbox Business	Citrix ShareFile	Verizon Business Solution	SoftLayer
FN	0.1071	0.1537	0.2431	0.2526	0.2927
HR	0.0594	0.0839	0.1319	0.1351	0.1594
IT	0.1071	0.1537	0.2431	0.2526	0.2927
RM	0.1071	0.1537	0.2431	0.2526	0.2927
AD	0.0594	0.0839	0.1319	0.1351	0.1594
Company Overall	0.1071	0.1537	0.2431	0.2526	0.2927

จากคะแนนความเสี่ยงที่ได้สามารถแสดงกราฟเปรียบเทียบได้ดังภาพที่ 4.1



ภาพที่ 4.1 *กราฟแสดงความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์โดยแยกตามแผนกและแยกตามผู้ให้บริการ*

จากกราฟแสดงผลการทดลองแสดงค่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของข้อมูล 5 แผนกกับผู้ให้บริการคลาวด์ 5 ราย แสดงให้เห็นว่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวมีความแตกต่างกันไปตามประเภทข้อมูลและผู้ให้บริการแต่ละราย เช่น ข้อมูลแผนกบัญชีที่จะนำขึ้นไป

จัดเก็บบน Microsoft Azure มีความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวมากกว่าข้อมูลแผนกทรัพยากรบุคคล เพราะข้อมูลของแผนกบัญชีมีค่าความอ่อนไหวของข้อมูลสูงกว่าแผนกทรัพยากรบุคคล ในอีกแง่มุมคือข้อมูลแผนกบัญชีที่ต้องการนำขึ้นไปจัดเก็บบน Microsoft Azure เมื่อเทียบกับ SoftLayer จะมีความเสี่ยงน้อยกว่า เพราะ Microsoft Azure มีการควบคุมด้านความเป็นส่วนตัวที่ดีกว่า

4.6 การวิเคราะห์ค่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว

ผู้วิจัยทำการวิเคราะห์ค่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว เมื่อค่าความอ่อนไหวของข้อมูลผู้ใช้บริการและค่าความโปร่งใสด้านการควบคุมความเป็นส่วนตัวโดยใช้ค่าต่ำสุด ค่ากลาง และค่าสูงสุดที่เป็นไปได้ต่าง ๆ ดังตารางที่ 4.14 โดยที่

ค่าความอ่อนไหวของข้อมูลที่จะนำขึ้นไปจัดเก็บบนคลาวด์ S_{Stored} ใช้ค่าที่เป็นไปได้ทั้งหมดตามสมการ (1) คือ 0, 0.33, 0.67 และ 1

ค่าความอ่อนไหวของข้อมูลส่วนบุคคลที่ผู้ให้บริการร้องขอ $S_{Requested}$ ซึ่งมีค่าที่เป็นไปได้อยู่ในช่วง (0, 1] จะใช้ค่า 0.2, 0.5 และ 1 ในการวิเคราะห์ ทั้งนี้ใช้ค่า 0.2 ซึ่งเป็นค่าต่ำสุดของค่า $S_{Requested}$ จากผู้ให้บริการ 5 ราย ที่ใช้ในการทดลอง ดังตารางที่ 4.10 แทนค่าต่ำสุด

ค่าความโปร่งใสด้านการควบคุมความเป็นส่วนตัว $T_{Provider}$ ซึ่งมีค่าที่เป็นไปได้อยู่ในช่วง [0, 1] จะใช้ค่า 0, 0.5 และ 1 ในการวิเคราะห์

ตารางที่ 4.14 ค่าคะแนนที่ใช้ในการวิเคราะห์

คะแนน	ค่าต่ำสุด	ค่ากลาง		ค่าสูงสุด
S_{Stored}	0	0.33	0.67	1
$S_{Requested}$	0.2	0.5		1
$T_{Provider}$	0	0.5		1

ดังนั้นค่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว $\mathbf{R_{Privacy}}$ ที่เป็นไปได้จากการนำค่าในตารางที่ 4.14 มาคำนวณจะเป็นดังตารางที่ 4.15 เมื่อใช้ค่า W_{Stored} = 0.8 และ $W_{Requested}$ = 0.2

ตารางที่ 4.15 ค่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวที่เป็นไปได้

S_{Stored}	$S_{Requested}$	S_{Data}	$T_{Provider}$	$R_{Privacy}$
0	0.2	0.04	0	0.04
0	0.2	0.04	0.5	0.02
0	0.2	0.04	1	0
0	0.5	0.1	0	0.1
0	0.5	0.1	0.5	0.05
0	0.5	0.1	1	0
0	1	0.2	0	0.2
0	1	0.2	0.5	0.1
0	1	0.2	1	0
0.33	0.2	0.304	0	0.304
0.33	0.2	0.304	0.5	0.152
0.33	0.2	0.304	1	0
0.33	0.5	0.364	0	0.364
0.33	0.5	0.364	0.5	0.182
0.33	0.5	0.364	1	0
0.33	1	0.464	0	0.464
0.33	1	0.464	0.5	0.232
0.33	1	0.464	1	0
0.67	0.2	0.576	0	0.576
0.67	0.2	0.576	0.5	0.288
0.67	0.2	0.576	1	0
0.67	0.5	0.636	0	0.636
0.67	0.5	0.636	0.5	0.318
0.67	0.5	0.636	1	0
0.67	1	0.736	0	0.736
0.67	1	0.736	0.5	0.368
0.67	1	0.736	1	0
1	0.2	0.84	0	0.84
1	0.2	0.84	0.5	0.42
1	0.2	0.84	1	0
1	0.5	0.9	0	0.9

ตารางที่ 4.15 ค่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวที่เป็นไปได้ (ต่อ)

S_{Stored}	$S_{Requested}$	S_{Data}	$T_{Provider}$	$R_{Privacy}$
1	0.5	0.9	0.5	0.45
1	0.5	0.9	1	0
1	1	1	0	1
1	1	1	0.5	0.5
1	1	1	1	0

จากตารางที่ 4.15 ค่าความเสี่ยง $R_{Privacy}$ มีค่าแปรเปลี่ยนไปได้ในช่วง [0, 1] โดยที่

- เมื่อค่า $T_{Provider}$ = 1 จะได้ค่า $R_{Privacy}$ = 0 นั่นคือเมื่อผู้ให้บริการได้คะแนนเต็มด้านความโปร่งใสด้านการควบคุมความเป็นส่วนตัวจากการปฏิบัติตาม CPCQ ทุกข้อ จะถือว่าไม่เกิดความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว ไม่ว่าข้อมูลของผู้ใช้บริการจะมีค่าความอ่อนไหว S_{Data} มากน้อยเพียงใดก็ตาม
- เมื่อค่า $T_{Provider}$ = 0 จะได้ค่า $R_{Privacy}$ = S_{Data} นั่นคือเมื่อผู้ให้บริการได้คะแนนความโปร่งใสด้านการควบคุมความเป็นส่วนตัวเป็น 0 จากการไม่ปฏิบัติตาม CPCQ ข้อใดเลย ปริมาณความเสี่ยงจะขึ้นอยู่กับความอ่อนไหวของข้อมูลผู้ใช้บริการว่ามีมากน้อยเพียงใด
- ค่า $T_{Provider}$ เป็นค่าที่ลดทอนปริมาณความเสี่ยงจากการจัดเก็บข้อมูลผู้ใช้บริการซึ่งมีความอ่อนไหวลงไปได้ ตัวอย่างเช่น ถึงแม้ข้อมูลทั้งหมดที่จะถูกจัดเก็บบนคลาวด์จะมีความอ่อนไหวสูงก็ตาม แต่หากผู้ให้บริการมีการปฏิบัติตาม CPCQ และได้คะแนนความโปร่งใสแม้เพียงครึ่งหนึ่งคือ $T_{Provider}$ = 0.5 จะสามารถลดทอนความเสี่ยงลงไปได้ถึงครึ่งหนึ่ง

จากผลการวิเคราะห์สามารถสรุปได้ว่า ค่าความโปร่งใสด้านการควบคุมความเป็นส่วนตัว $T_{Provider}$ เป็นปัจจัยที่ส่งผลมากต่อระดับความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว $R_{Privacy}$ เนื่องจากผู้วิจัยถือว่าหากผู้ให้บริการปฏิบัติตามแนวปฏิบัติใน CPCQ ซึ่งเป็นแนวปฏิบัติด้านความเป็นส่วนตัวโดยทั่วไปแล้ว จะถือว่ามีการจัดการความเป็นส่วนตัวที่ดีและสามารถรองรับข้อมูลที่จะจัดเก็บได้ทุกระดับความอ่อนไหวเท่าเทียมกัน แต่เมื่อใดที่ผู้ให้บริการขาดความโปร่งใสด้านการควบคุมความเป็นส่วนตัวหรือมีค่า $T_{Provider}$ น้อยแล้วค่าความอ่อนไหวของข้อมูลผู้ใช้บริการจะกลายเป็นปัจจัยที่ส่งผลมากขึ้นต่อระดับความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว

4.7 การทดสอบความสัมพันธ์เชิงสถิติระหว่างความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวกับการไม่ปฏิบัติตามแนวปฏิบัติด้านความมั่นคง

จากการที่ประเด็นด้านความเป็นส่วนตัวและความมั่นคงมักมีความเกี่ยวข้องกันมาก เนื่องจากในการควบคุมความเป็นส่วนตัวจำเป็นต้องใช้การจัดการหรือเทคนิคด้านความมั่นคงเข้ามาช่วย ผู้วิจัยจึงมีแนวคิดในการทดสอบความสัมพันธ์เชิงสถิติว่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวกับการไม่ปฏิบัติตามแนวปฏิบัติด้านความมั่นคง CCM ของผู้ให้บริการมีความสัมพันธ์กันหรือไม่

การทดสอบทำโดยนำคะแนนความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวของ 5 แผนก (ถือเป็นผู้ใช้บริการ 5 ราย) เมื่อจัดเก็บข้อมูลกับผู้ให้บริการรายหนึ่ง ๆ จากตารางที่ 4.13 มาหาค่าเฉลี่ยและทดสอบความสัมพันธ์กับคะแนนการไม่ปฏิบัติตามแนวปฏิบัติด้านความมั่นคง CCM ของผู้ให้บริการรายนั้น ซึ่งคำนวณจากแบบประเมินตนเองของผู้ให้บริการซึ่งเผยแพร่อยู่บนเว็บไซต์ CSA STAR คะแนนการไม่ปฏิบัติตามแนวปฏิบัติด้านความมั่นคง CCM นี้ ผู้วิจัยคำนวณจากผลรวมการไม่ปฏิบัติตามแนวปฏิบัติ (ตอบว่าไม่ใช่) ในแบบประเมินตนเอง แล้วนำมาหาสัดส่วนเมื่อเทียบกับจำนวนคำถามทั้งหมดในแบบประเมินตนเอง เพื่อให้ได้เป็นคะแนนการไม่ปฏิบัติตาม CCM ดังแสดงในตารางที่ 4.14 (รายละเอียดดูได้จากภาคผนวก ข) ผู้วิจัยใช้การวิเคราะห์สหสัมพันธ์อย่างง่าย (Simple Correlation) โดยมีสมมติฐานคือ

H0: ความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวไม่มีความสัมพันธ์ในรูปเชิงเส้นกับการไม่ปฏิบัติตามแนวทางการปฏิบัติด้านความมั่นคง CCM

H1: ความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวมีความสัมพันธ์ในรูปเชิงเส้นเป็นเชิงบวกกับการไม่ปฏิบัติตามแนวทางการปฏิบัติด้านความมั่นคง CCM

ตารางที่ 4.16 *การทดสอบความสัมพันธ์เชิงสถิติระหว่างความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวกับการไม่ปฏิบัติตามแนวปฏิบัติด้านความมั่นคง*

Provider Name	**CCM Noncompliance Score (x)**	**Average Risk of Privacy Loss Score of 5 Dept. (y)**	x^2	y^2	**xy**
Microsoft Azure	0.0107	0.08802	0.0001	0.0077	0.0009
Dropbox Business	0.0576	0.1259	0.0033	0.0158	0.0072
Citrix ShareFile	0.1176	0.1986	0.0138	0.0394	0.0234
Verizon Business Solution	0.1711	0.2056	0.0293	0.0423	0.0352
SoftLayer	0.3529	0.23938	0.1245	0.0573	0.0845
Sum	0.7099	0.8574	0.1711	0.1626	0.1512

การคำนวณค่าสัมประสิทธิ์สหสัมพันธ์ r ทำได้โดยสมการ

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

จากตารางที่ 4.14 คำนวณค่า r ได้เป็น

$$r = \frac{5(0.1512) - (0.7099)(0.8574)}{\sqrt{[5(0.1711) - (0.504)][5(0.1626) - (0.7351)]}}$$

$$r = \frac{0.1473}{0.1654}$$

r = 0.8909

จากค่า r ที่ได้ สรุปได้ว่าความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวมีความสัมพันธ์ในรูปเชิงเส้นเป็นเชิงบวกในระดับสูงกับการไม่ปฏิบัติตามแนวปฏิบัติด้านความมั่นคง CCM เมื่อทดสอบนัยสำคัญทางสถิติ โดยคำนวณค่า t ด้วยสมการ

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

จะได้ว่า $t = 0.8938\sqrt{\frac{5-2}{1-0.8909^2}} = 3.5596$

เมื่อ $\alpha = 0.05$, df = n-2 =3 พบว่า ค่า t=3.5596 ที่คำนวณได้ มากกว่าค่า $t_{0.95, 3}$ ซึ่งเท่ากับ 2.353 ดังนั้น จึงปฏิเสธ H0 และยอมรับ H1 นั่นคือความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวมีความสัมพันธ์ในรูปเชิงเส้นเป็นเชิงบวกกับการไม่ปฏิบัติตามแนวปฏิบัติด้านความมั่นคงอย่างมีนัยสำคัญที่ระดับความเชื่อมั่น 95%

บทที่ 5

สรุปผลการวิจัย

5.1 สรุปผลการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว ในกรณีที่ผู้ใช้บริการต้องการนำข้อมูลขึ้นไปจัดเก็บบนคลาวด์ โดยมีการประเมินความอ่อนไหวของข้อมูลที่จะนำขึ้นไปจัดเก็บและข้อมูลที่ผู้ให้บริการร้องขอเพื่อเข้าใช้งาน และทำการประเมินความโปร่งใสในการควบคุมความเป็นส่วนตัวของผู้ให้บริการ แล้วนำเอาค่าที่ประเมินได้ทั้งสามส่วนมาทำการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว ผู้วิจัยได้พัฒนาระบบสนับสนุนการประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัว ซึ่งสามารถประเมินความเสี่ยงของข้อมูลประเภทต่าง ๆ ของผู้ใช้บริการ หากนำข้อมูลไปจัดเก็บกับผู้ให้บริการรายหนึ่ง ๆ โดยสามารถแสดงผลเป็นค่าคะแนนและแผนภาพกราฟได้

5.2 ปัญหาและข้อจำกัด

ปัญหาและข้อจำกัดของงานวิจัยมีดังนี้

1. การประเมินความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวตามวิธีการที่เสนอ ใช้ข้อมูลการควบคุมความเป็นส่วนตัวของผู้ให้บริการที่มีการเผยแพร่ต่อสาธารณะบนเว็บไซต์ผู้ให้บริการเท่านั้น แต่ข้อมูลที่เผยแพร่ไม่สามารถบ่งบอกได้ว่าผู้ให้บริการมีการจัดการที่ดีในการควบคุมความเป็นส่วนตัวจริงหรือไม่ อยู่ในระดับใด หรือในการให้บริการโดยแท้จริงแล้วมีการละเมิดหลักการด้านความเป็นส่วนตัวหรือไม่ อย่างไรก็ตามผู้ใช้บริการโดยทั่วไปที่ต้องการเลือกผู้ให้บริการคลาวด์มาใช้งานจะสามารถเข้าถึงข้อมูลเฉพาะที่เผยแพร่ต่อสาธารณะเท่านั้น โดยไม่สามารถเข้าถึงข้อมูลเบื้องลึกอื่น ๆ ในการให้บริการจริงของผู้ให้บริการได้ วิธีการประเมินความเสี่ยงที่เสนอจึงนับว่าเป็นประโยชน์ต่อผู้ใช้บริการในการประเมินเบื้องต้น
2. คะแนนความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวสำหรับผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์นั้นเป็นเพียงข้อมูลส่วนหนึ่งที่ใช้ประกอบการตัดสินใจเลือกผู้ให้บริการ ซึ่งในการตัดสินใจเลือกจำเป็นต้องพิจารณาในหลาย ๆ ปัจจัยเช่น ความมั่นคง ราคา บริการสนับสนุน เป็นต้น
3. เครื่องมือสนับสนุนยังมีข้อจำกัดในหลายประเด็นดังนี้

3.1 ระบบสามารถทำการประเมินผู้ให้บริการได้ทีละรายเนื่องจากระบบรองรับการสร้าง Cross Table ทีละ 1 ตาราง

3.2 ในการเปรียบเทียบผู้ให้บริการหลายรายต้องทำการประเมินทีละรายแล้วเก็บผลการไว้ในรูปแบบไฟล์ PDF แล้วนำผลการประเมินของทุกรายมาเปรียบเทียบโดยใช้เครื่องมืออื่น เช่น Excel

3.3 ระบบไม่สามารถแก้ไขข้อมูลที่ผู้ใช้บริการกรอกเพื่อใช้ในการประเมินได้ ผู้ใช้บริการต้องกรอกข้อมูลใหม่หากต้องการแก้ไข

3.4 ระบบไม่สามารถบันทึกข้อมูลที่ผู้ใช้บริการกรอกเพื่อใช้ในการประเมินเก็บไว้ใช้ภายหลังจากการปิดโปรแกรมได้

5.3 ข้อควรระวัง

คะแนนความเสี่ยงด้านการสูญเสียความเป็นส่วนตัวเป็นคะแนนที่ประเมินจากมุมมองของผู้ใช้บริการรายหนึ่ง ๆ ดังนั้นจึงสามารถใช้เปรียบเทียบความเสี่ยงของผู้ให้บริการหลายรายที่จัดเก็บข้อมูลของผู้ใช้บริการรายนั้นหรือใช้เปรียบเทียบความเสี่ยงของการจัดเก็บข้อมูลหลายประเภทของผู้ใช้บริการรายนั้นได้ อย่างไรก็ตามผู้ใช้บริการต่างรายกันที่จัดเก็บข้อมูลประเภทเดียวกันอาจกำหนดค่าความอ่อนไหวให้กับข้อมูลประเภทเดียวกันนั้นแตกต่างกัน, กำหนดค่าน้ำหนักในการคำนวณความอ่อนไหวแตกต่างกัน, กำหนด Cross Table สำหรับผู้ให้บริการรายเดียวกันแตกต่างกัน หรือแม้กระทั่งประเมินความโปร่งใสของผู้ให้บริการรายเดียวกันแตกต่างกันได้ ดังนั้นทำให้ผู้ใช้บริการต่างรายกันอาจได้ผลการคำนวณคะแนนความเสี่ยงของการจัดเก็บข้อมูลประเภทเดียวกันกับผู้ให้บริการรายเดียวกันที่แตกต่างกันได้ จึงไม่สามารถใช้คะแนนความเสี่ยงที่ประเมินจากมุมมองของผู้ใช้บริการต่างรายกันมาเปรียบเทียบกันได้

5.4 แนวทางการวิจัยต่อไป

แนวทางการวิจัยต่อไปมีดังนี้

1. เนื่องจากข้อมูลที่ผู้ให้บริการแสดงบนเว็บไซต์มีปริมาณมากและมีความซับซ้อน ทำให้การประเมินความโปร่งใสในด้านการควบคุมความเป็นส่วนตัวของผู้ให้บริการจึงมีความยุ่งยาก ควรมีการพัฒนาโปรแกรมที่สามารถรวบรวมข้อมูลบนหน้าเว็บไซต์และสามารถจำแนกหมวดหมู่การปฏิบัติตาม CPCQ ได้อย่างอัตโนมัติ
2. ปรับปรุงเครื่องมือสนับสนุนให้มีความสามารถเพิ่มขึ้นเพื่อแก้ปัญหาข้อจำกัดในข้อ 4 ข้างต้น

รายการอ้างอิง

รายการอ้างอิง

[1] A.Huth and J.Cebula, “The Basics of Cloud Computing”, Carnegie Mellon University, 2011

[2] N. Beagrie, A. Charlesworth, and P. Miller, “Guidance on Cloud Storage and Digital Preservation”, Charles Beagrie Ltd., April 2014.

[3] MIT, “Sensitivity of Data", https://ist.mit.edu/security/data_sensitivity

[4] Microsoft, “Data Classification for Cloud Readiness”, 2014, http://download. microsoft.com/download/0/A/3/0A3BE969-85C5-4DD2-83B6-366AA71D1FE 3/ Data-Classification-for-CloudReadiness.pdf.

[5] DataONE, “Identify Data Sensitivity”, https://www.dataone.org/bestpractices/ identify- data-sensitivity

[6] National Institute of Standard and Technology, “Information Security”, NIST Special Publication 800-60 Volume II, August 2008.

[7] National Institute of Standard and Technology, “Minimum Security Requirements for Federal Information and Information Systems”, FIPS Publication 200, 9 March 2006

[8] National Institute of Standard and Technology, “Standards for Security Categorization of Federal Information and Information Systems”, FIPS Publication 199, February 2004

[9] National Institute of Standard and Technology, “Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories”, NIST Special Publication 800-600, October 2007

[10] ITU, “Privacy in Cloud Computing”, ITU-T Technology Watch Report, March 2012, http://www.itu.int/en/ITU-T/techwatch/Pages/cloudcomputing-privacy.aspx

[11] Cloud Security Alliance, “Privacy Level Agreement”, February 2013, https:// cloudsecurityalliance.org/download/privacy-level-agreement-plaoutline-for-the-sale-of-cloud-service-providers-providing-services-inthe-european-union.

[12] Australian Government, “Australian Privacy Principles”, January 2014, http://www.oaic.gov.au/privacy/privacy-resources/privacy-factsheets/other/privacy-fact-sheet-17-australian-privacy-principles.

[13] National Institute of Standard and Technology, “Security and Privacy Controls for Federal Information Systems and Organizations”, NIST Special Publication 800-53, April 2013.

[14] I. Jang and H.S. Yoo, “Personal information classification for privacy negotiation,” in Procs. 4th Int. Conf. Computer Sciences and Convergence Information Technology, 2009, pp. 1117-1122.

[15] P. Chaiwongsa and T. Senivongse, “Web services privacy measurement based on privacy policy and sensitivity level of personal information,” in Procs. 8th Int. Conf. Computing and Information Technology (IC2IT 2012), May 2012, pp. 77-85.

[16] S. Pearson, “Taking account of privacy when designing cloud computing services,” in CLOUD’09 Procs. ICSE Workshop Software Engineering Challenges of Cloud Computing, September 2009, pp. 44-52.

[17] S.-U. Lar, X. Liao, and S.A. Abbas, “Cloud computing privacy & security: Global issues, challenges, & mechanisms,” in Procs. 6th Int. ICST Conf. Communications and Networking in China (CHINACOM), August 2011, pp. 1240-1245.

[18] D. Tancock, S. Pearson, and A. Charlesworth, “A privacy impact assessment tool for cloud computing,” in Procs. 2nd IEEE Int. Conf. Cloud Computing Technology and Science, November 2010, pp. 667-676.

[19] S. Pearson and A. Benameur, “Privacy, security and trust issues arising from cloud computing,” in Procs. 2nd IEEE Int. Conf. Cloud Computing Technology and Science, November 2010, pp. 693-702.

[20] Cloud Security Alliance (CSA), “Security, Trust & Assurance Registry (STAR)”, https://cloudsecurityalliance.org/star/, 2015

[21] Wikipedia, “Risk Management”, https://en.wikipedia.org/wiki/Risk_management

ภาคผนวก

ภาคผนวก ก

ข้อมูลสำหรับการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัว

ก.1 แหล่งข้อมูลสำหรับการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัว

1. Microsoft Azure

   https://azure.microsoft.com/

   https://azure.microsoft.com/en-us/overview/contact-us/

   https://azure.microsoft.com/en-us/support/trust-center/privacy/

2. Dropbox Business

   https://www.dropbox.com/business/contact

   https://www.dropbox.com/privacy

   https://www.dropbox.com/business/trust/security

3. Citrix ShareFile

   https://www.citrix.com/products/sharefile/overview.html

   https://www.citrix.com/about/legal.html

4. Verizon Enterprise Solution

   http://www.verizonenterprise.com/

   http://www.verizon.com/about/privacy/

   http://www.verizonenterprise.com/us/publications/

5. SoftLayer

   http://www.softlayer.com/

   http://www.softlayer.com/privacy-agreement

ก.2 คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ

ตารางที่ ก2.1 *คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Microsoft Azure*

CPCQ Code	Compliance	Evidence
CPCQ1.1	1	1
CPCQ1.2	1	1

ตารางที่ ก2.1 *คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Microsoft Azure (ต่อ)*

CPCQ Code	Compliance	Evidence
CPCQ1.3	1	1
CPCQ2.1	1	0
CPCQ3.1	1	1
CPCQ3.2	1	0
CPCQ3.3	1	1
CPCQ3.4	1	1
CPCQ3.5	1	1
CPCQ3.6	1	1
CPCQ3.7	1	1
CPCQ4.1	1	1
CPCQ4.2	1	1
CPCQ5.1	1	0
CPCQ5.2	1	1
CPCQ5.3	1	1
CPCQ5.4	1	1
CPCQ5.5	1	1
CPCQ5.6	1	1
CPCQ6.1	1	1
CPCQ7.1	1	1
CPCQ7.2	1	1
CPCQ7.3	1	1
CPCQ8.1	1	1
CPCQ9.1	0	0
CPCQ9.2	0	0
CPCQ10.1	1	1
CPCQ10.2	1	1
CPCQ10.3	0	0

ตารางที่ ก2.1 *คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Microsoft Azure (ต่อ)*

CPCQ Code	Compliance	Evidence
CPCQ10.4	1	1
CPCQ11.1	1	1
CPCQ11.2	1	1
CPCQ12.1	1	1
CPCQ12.2	1	0
CPCQ13.1	1	1
CPCQ13.2	1	1
CPCQ14.1	1	1
CPCQ15.1	1	1
CPCQ15.2	1	1
CPCQ16.1	0	0
CPCQ17.1	1	1
CPCQ18.1	1	1
Total Score	38	31
$T_{Provider}$	0.8214	

ตารางที่ ก2.2 *คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Dropbox Business*

CPCQ Code	Compliance	Evidence
CPCQ1.1	1	1
CPCQ1.2	1	1
CPCQ1.3	1	1
CPCQ2.1	1	1
CPCQ3.1	1	0
CPCQ3.2	1	1
CPCQ3.3	1	1
CPCQ3.4	1	0

ตารางที่ ก2.2 *คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Dropbox Business (ต่อ)*

CPCQ Code	Compliance	Evidence
CPCQ3.5	1	0
CPCQ3.6	1	0
CPCQ3.7	1	1
CPCQ4.1	1	1
CPCQ4.2	1	1
CPCQ5.1	1	0
CPCQ5.2	1	1
CPCQ5.3	1	1
CPCQ5.4	1	0
CPCQ5.5	1	1
CPCQ5.6	1	1
CPCQ6.1	1	1
CPCQ7.1	1	1
CPCQ7.2	0	0
CPCQ7.3	0	0
CPCQ8.1	1	1
CPCQ9.1	0	0
CPCQ9.2	0	0
CPCQ10.1	1	1
CPCQ10.2	1	1
CPCQ10.3	1	1
CPCQ10.4	1	1
CPCQ11.1	1	0
CPCQ11.2	1	1
CPCQ12.1	0	0
CPCQ12.2	1	1

ตารางที่ ก2.2 *คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Dropbox Business (ต่อ)*

CPCQ Code	**Compliance**	**Evidence**
CPCQ13.1	1	0
CPCQ13.2	1	1
CPCQ14.1	1	1
CPCQ15.1	1	1
CPCQ15.2	1	1
CPCQ16.1	0	0
CPCQ17.1	0	0
CPCQ18.1	1	1
Total Score	35	27
$T_{Provider}$	0.7381	

ตารางที่ ก2.3 *คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ* Citrix ShareFile

CPCQ Code	**Compliance**	**Evidence**
CPCQ1.1	1	1
CPCQ1.2	1	1
CPCQ1.3	1	1
CPCQ2.1	0	0
CPCQ3.1	1	1
CPCQ3.2	1	1
CPCQ3.3	1	0
CPCQ3.4	1	0
CPCQ3.5	1	0
CPCQ3.6	1	0
CPCQ3.7	1	1
CPCQ4.1	1	1

ตารางที่ ก2.3 *คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ* Citrix ShareFile

CPCQ Code	Compliance	Evidence
CPCQ4.2	1	1
CPCQ5.1	1	0
CPCQ5.2	1	0
CPCQ5.3	1	0
CPCQ5.4	1	0
CPCQ5.5	1	1
CPCQ5.6	1	1
CPCQ6.1	1	0
CPCQ7.1	0	0
CPCQ7.2	0	0
CPCQ7.3	0	0
CPCQ8.1	1	0
CPCQ9.1	0	0
CPCQ9.2	0	0
CPCQ10.1	0	0
CPCQ10.2	1	1
CPCQ10.3	1	1
CPCQ10.4	1	1
CPCQ11.1	1	0
CPCQ11.2	1	0
CPCQ12.1	1	0
CPCQ12.2	1	0
CPCQ13.1	1	0
CPCQ13.2	1	0
CPCQ14.1	1	0
CPCQ15.1	1	1

ตารางที่ ก2.3 *คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ* Citrix ShareFile

CPCQ Code	**Compliance**	**Evidence**
CPCQ15.2	0	0
CPCQ16.1	0	0
CPCQ17.1	0	0
CPCQ18.1	1	1
Total Score	33	16
$T_{Provider}$		0.5833

ตารางที่ ก2.4 *คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Verizon Business Solution*

CPCQ Code	**Compliance**	**Evidence**
CPCQ1.1	1	1
CPCQ1.2	1	1
CPCQ1.3	1	1
CPCQ2.1	1	0
CPCQ3.1	1	0
CPCQ3.2	1	0
CPCQ3.3	1	0
CPCQ3.4	0	0
CPCQ3.5	1	1
CPCQ3.6	1	1
CPCQ3.7	1	1
CPCQ4.1	1	0
CPCQ4.2	1	0
CPCQ5.1	0	0
CPCQ5.2	1	0
CPCQ5.3	1	0

ตารางที่ ก2.4 *คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Verizon Business Solution (ต่อ)*

CPCQ Code	Compliance	Evidence
CPCQ5.4	1	1
CPCQ5.5	1	0
CPCQ5.6	1	1
CPCQ6.1	1	1
CPCQ7.1	0	0
CPCQ7.2	0	0
CPCQ7.3	0	0
CPCQ8.1	0	0
CPCQ9.1	0	0
CPCQ9.2	0	0
CPCQ10.1	1	1
CPCQ10.2	1	0
CPCQ10.3	1	1
CPCQ10.4	1	1
CPCQ11.1	1	0
CPCQ11.2	1	0
CPCQ12.1	1	1
CPCQ12.2	1	0
CPCQ13.1	1	0
CPCQ13.2	1	0
CPCQ14.1	1	1
CPCQ15.1	1	1
CPCQ15.2	1	1
CPCQ16.1	0	0
CPCQ17.1	0	0

ตารางที่ ก2.4 *คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ Verizon Business Solution (ต่อ)*

CPCQ Code	Compliance	Evidence
CPCQ18.1	1	1
Total Score	30	17
$T_{Provider}$		0.5595

ตารางที่ ก2.5 *คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ SoftLayer*

CPCQ Code	Compliance	Evidence
CPCQ1.1	1	1
CPCQ1.2	1	1
CPCQ1.3	1	1
CPCQ2.1	0	0
CPCQ3.1	1	1
CPCQ3.2	1	1
CPCQ3.3	1	1
CPCQ3.4	1	1
CPCQ3.5	1	0
CPCQ3.6	1	0
CPCQ3.7	1	0
CPCQ4.1	1	0
CPCQ4.2	1	1
CPCQ5.1	0	0
CPCQ5.2	1	0
CPCQ5.3	1	0
CPCQ5.4	1	01
CPCQ5.5	1	0
CPCQ5.6	1	1
CPCQ6.1	1	0

ตารางที่ ก2.5 *คะแนนการประเมินความโปร่งใสด้านการควบคุมความเป็นส่วนตัวตาม CPCQ ของ SoftLayer (ต่อ)*

CPCQ7.1	0	0
CPCQ7.2	0	0
CPCQ7.3	0	0
CPCQ8.1	1	1
CPCQ9.1	0	0
CPCQ9.2	0	0
CPCQ10.1	1	1
CPCQ10.2	1	1
CPCQ10.3	1	1
CPCQ10.4	1	0
CPCQ11.1	0	0
CPCQ11.2	0	0
CPCQ12.1	0	0
CPCQ12.2	0	0
CPCQ13.1	0	0
CPCQ13.2	0	0
CPCQ14.1	1	1
CPCQ15.1	1	1
CPCQ15.2	1	0
CPCQ16.1	0	0
CPCQ17.1	1	1
CPCQ18.1	1	1
Total Score	27	15
$T_{Provider}$	0.5	

ภาคผนวก ข

การปฏิบัติตามและไม่ปฏิบัติตามแนวปฏิบัติด้านความมั่นคง CCM

ตารางที่ ข.1.1 *การปฏิบัติตามและไม่ปฏิบัติตามแนวปฏิบัติด้านความมั่นคง CCM*

Provider	CCM Ver.	จำนวนข้อคำถามทั้งหมด	ตอบว่าใช่	ตอบว่าไม่ใช่	ไม่มีบริการ (N/A)	Compliance Score	Noncompliance Score
Microsoft Azuer	1.1	187	185	2	0	0.9893	0.0107
Dropbox Business	3.1	295	275	17	3	0.9322	0.0576
Citrix ShareFile	1.1	187	165	22	0	0.8824	0.1176
Verizon Business Solution	1.1	187	145	32	10	0.7754	0.1711
SoftLayer	1.1	187	115	66	6	0.615	0.3529

ประวัติผู้เขียนวิทยานิพนธ์

นายชัชวาลย์ คำหวาน เกิดเมื่อวันที่ 12 พฤศจิกายน พ.ศ. 2524 ที่จังหวัดขอนแก่น สำเร็จการศึกษาระดับปริญาบัณฑิต สาขาเทคโนโลยีสารสนเทศ คณะคอมพิวเตอร์และเทคโนโลยีสารสนเทศ จากมหาวิทยาลัยภาคตะวันออกเฉียงเหนือ และได้ศึกษาต่อหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ คณะคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัยในปีการศึกษา 2556