Cloud Computing Practice

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

พฤศจิกายน 2562

สารบัญ

1. หลักการและเหตุผล

ในปัจจุบันมีการประยุกต์ใช้งานเทคโนโลยีสารสนเทศเป็นส่วนหนึ่งในการสนับสนุนและดำเนินกิจกรรมสำคัญในการขับเคลื่อนธุรกิจในตลาดทุน หนึ่งในเทคโนโลยีที่มีการประยุกต์ใช้อย่างกว้างขวาง คือ การใช้บริการระบบประมวลผลร่วมกันผ่านเครือข่ายตามความต้องการของผู้ใช้งาน (Cloud Computing) ทั้งเพื่อเพิ่มขีดความสามารถในการประมวลผลและเพื่อเพิ่มประสิทธิภาพและประสิทธิผลในการบริหารจัดการต้นทุนด้านเทคโนโลยีอย่างมีนัยสำคัญ การประยุกต์ใช้งาน Cloud Computing เป็นรูปแบบการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อบริหารจัดการความต้องการทรัพยากรในการประมวลผลตามความต้องการของผู้ใช้งาน ซึ่งอาจมีการกำหนดขอบเขตการใช้งานทรัพยากรการประมวลผลดังกล่าวอย่างเฉพาะเจาะจงสำหรับผู้หนึ่งผู้ใด หรืออาจมีการใช้งานร่วมกันของกลุ่มผู้ใช้งานและนิติบุคคลเพื่อประสิทธิภาพในการใช้บริหารจัดการทรัพยากรและต้นทุนอย่างเหมาะสม การใช้งานทรัพยากรร่วมกันบนเครือข่ายส่งผลให้เกิดความซับซ้อนด้านเทคโนโลยี รวมถึงความเสี่ยงอันอาจจะเกิดขึ้นต่อสารสนเทศที่ถูกจัดเก็บอยู่บนเครือข่ายที่มีการบริหารจัดการโดยบุคคลภายนอก หรือผู้ให้บริการ Cloud Computing

เพื่อให้ผู้ประกอบธุรกิจในตลาดทุนมีความสามารถในการบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ ในขณะเดียวกันสามารถคงขีดความสามารถในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศอันเป็นส่วนสำคัญในการรักษาเสถียรภาพของตลาดทุน สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน”) จึงมีการออกหลักเกณฑ์ว่าด้วยการจัดให้มีระบบเทคโนโลยีสารสนเทศและแนวปฏิบัติที่เกี่ยวข้องที่มีข้อกำหนดและหลักเกณฑ์ในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการใช้งาน Cloud Computing คู่มือฉบับนี้จัดทำขึ้นเพื่อเป็นแนวทางให้ผู้ประกอบธุรกิจในการทำความเข้าใจความเสี่ยงอันอาจจะเกิดขึ้น พร้อมจัดทำแนวทางการบริหารความเสี่ยงและการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ ในการใช้งานระบบ Cloud Computing ได้อย่างมีประสิทธิภาพและประสิทธิผล

1.1 <u>วัตถุประสงค์</u>

แนวทางการกำกับดูแลและบริหารจัดการ Cloud Computing ได้จัดทำขึ้นเพื่อให้ผู้ประกอบธุรกิจใช้เป็นแนวทางในการกำกับดูแลและบริหารความปลอดภัยจากการใช้งาน Cloud Computing ได้แก่

- กิจกรรมทางด้านสารสนเทศมีความสอดคล้องกับวัตถุประสงค์ขององค์กร (Value Delivery)
- มีการจัดการความเสี่ยงอย่างเหมาะสม (Risk Optimization)
- มีการจัดการทรัพยากรทางด้านสารสนเทศเพื่อให้ได้ประโยชน์สูงสุด (Resource Optimization)
- มีการจัดการด้านความมั่นคงปลอดภัยสารสนเทศ Cloud Computing

1.2 การจัดทำแนวทางการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ Cloud Computing ของ ก.ล.ต.

สำนักงานได้กำหนดแนวทางการกำกับดูแลและบริหารจัดการการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์ตามความต้องการของผู้ใช้งาน หรือ Cloud Computing โดยอ้างอิงกรอบมาตรฐานด้านการบริหารจัดการอันเป็นสากล[1] ที่ครอบคลุมกระบวนการสำคัญตั้งแต่การกำหนดกรอบการกำกับดูแลการใช้งาน Cloud Computing การกำหนดแนวทางเชิงกลยุทธ์ในการใช้งาน การกำกับผู้ให้บริการ ตลอดจนการยกเลิกหรือสิ้นสุดการใช้งาน ซึ่งเป็นวงจรการบริหารจัดการ Cloud Computing ดังที่แสดงในแผนภาพที่ 1

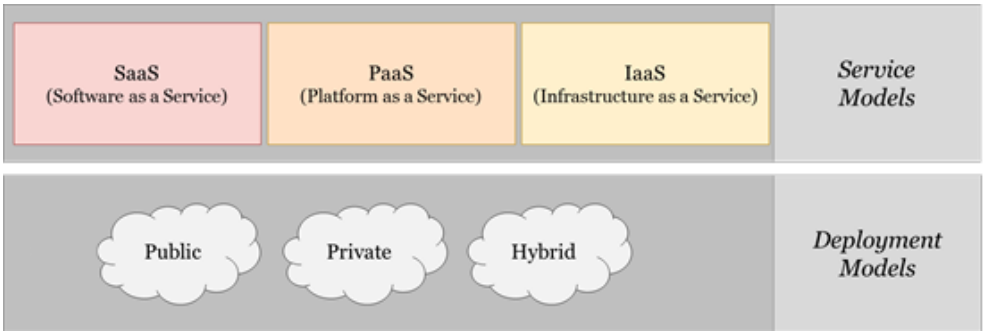
แผนภาพที่ 1 – วงจรการบริหารจัดการการใช้งาน Cloud Computing

[1]ISO/IEC 27017-2015 : Code of practice for information security controls based on ISO/IEC 27002 for cloud services
NIST: National Institute of Standards and Technology : Guidelines on Security and Privacy in Public Cloud Computing
SANS: Cloud Security Framework Audit Methods
ISACA: IS Audit/Assurance Program – Cloud Computing,
CSA: Cloud Security Alliance (https://cloudsecurityalliance.org)

1.3 บทนิยาม

ผู้ประกอบธุรกิจ	หมายถึง	ผู้ประกอบธุรกิจภายใต้การกำกับดูแลของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ที่ได้รับใบอนุญาตประกอบธุรกิจหลักทรัพย์ หรือธุรกิจสัญญาซื้อขายล่วงหน้าตามที่ระบุไว้ในหลักเกณฑ์ว่าด้วยการจัดให้มีระบบเทคโนโลยีสารสนเทศ
ทรัพย์สินสารสนเทศ	หมายถึง	1. ทรัพย์สินสารสนเทศประเภทระบบ ซึ่งได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และ ระบบสารสนเทศ 2. ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ซึ่งได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และ อุปกรณ์อื่นใด 3. ทรัพย์สินสารสนเทศประเภทข้อมูล ซึ่งได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และ ข้อมูลคอมพิวเตอร์
ทรัพย์สินสารสนเทศที่มีความสำคัญ	หมายถึง	ทรัพย์สินสารสนเทศที่เกี่ยวข้อง หรือจำเป็นต้องใช้ประกอบกับงานที่มีความสำคัญตามประกาศสำนักงาน
ระบบสารสนเทศที่มีความสำคัญ	หมายถึง	ระบบสารสนเทศที่รองรับการปฏิบัติงานที่สำคัญ เช่น ระบบซื้อขาย ระบบปฏิบัติการ back office และระบบจัดการลงทุน เป็นต้น
ผู้ใช้งาน	หมายถึง	พนักงานของผู้ประกอบธุรกิจและบุคลากรภายนอกที่มีการปฏิบัติงานโดยมีการเข้าถึงข้อมูลลับหรือระบบงานสำคัญภายในองค์กรโดยไม่รวมถึงลูกค้า
Cloud Computing	หมายถึง	รูปแบบการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อการประมวลผลตามความต้องการของผู้ใช้งาน[2]

[2] NIST: The NIST Definition of Cloud Computing



แผนภาพที่ 2 – ประเภทและรูปแบบการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่าย

ประเภทของ Cloud Computing (Service Models)

1) Software-as-a-Service (SaaS)	หมายถึง	บริการด้านแอปพลิเคชันที่ทำงานบนโครงสร้างพื้นฐานระบบ Cloud Computing ซึ่งผู้ใช้บริการสามารถเข้าใช้งานแอปพลิเคชันผ่านเครือข่ายผ่านโปรแกรมบนอุปกรณ์ของผู้ใช้บริการ เช่น เว็บเบราว์เซอร์ แอปพลิเคชันบนมือถือ เป็นต้น โดยผู้ให้บริการทำหน้าที่บริหารจัดการโครงสร้างพื้นฐานระบบคลาวด์ ซึ่งครอบคลุมถึง ความปลอดภัยทางกายภาพระบบปฏิบัติการ ระบบเครือข่าย ระบบจัดเก็บข้อมูล รวมถึงค่าพื้นฐานของแอปพลิเคชัน
2) Platform-as-a-Service (PaaS)	หมายถึง	บริการด้านแฟลตฟอร์มที่ทำงานบนโครงสร้างพื้นฐานระบบคลาวด์ ซึ่งผู้ใช้บริการสามารถเข้าแฟลตฟอร์มในการพัฒนาแอปพลิชั่น โดยผู้ให้บริการทำหน้าที่บริหารจัดการโครงสร้างพื้นฐานระบบคลาวด์ ซึ่งครอบคลุมถึง ความปลอดภัยทางกายภาพระบบปฏิบัติการ ระบบเครือข่าย และระบบให้บริการ เช่น เว็บเซอร์วิส ระบบจัดการฐานข้อมูล เป็นต้น อย่างไรก็ตาม การควบคุมที่เกี่ยวกับการบริหารจัดการแอปพลิเคชัน เช่น การแก้ไขเปลี่ยนแปลงโปรแกรม ผู้ใช้บริการจะเป็นผู้ดำเนินการ
3) Infrastructure-as-a-Service (IaaS)	หมายถึง	บริการด้านโครงสร้างพื้นฐานระบบคลาวด์ที่มีการใช้งานทรัพยากรทางด้านระบบสารสนเทศร่วมกัน เช่น ระบบปฏิบัติการ ระบบเครือข่าย หรือระบบจัดเก็บข้อมูล โดยทางผู้ให้บริการทำหน้าที่ดูแลทางกายภาพ และทรัพยากรสารสนเทศที่ใช้ในการสนับสนุนการทำงานของโครงสร้างพื้นฐานระบบคลาวด์

รูปแบบของการนำไปใช้งาน (Deployment Models)

1) Public Cloud	หมายถึง	โครงสร้างพื้นฐานระบบคลาวด์ที่เปิดให้ใช้งานผ่านเครือข่ายสาธารณะ
2) Private Cloud	หมายถึง	โครงสร้างพื้นฐานระบบคลาวด์ที่จัดเตรียมไว้สำหรับการใช้งานโดยหน่วยงานภายในองค์กรเดียวกัน
3) Hybrid Cloud	หมายถึง	โครงสร้างพื้นฐานระบบคลาวด์ที่ประกอบด้วยโครงสร้างพื้นฐานระบบคลาวด์ที่แตกต่างกันตั้งแต่สองรูปแบบขึ้นไป (Public และ Private)

1. แนวทางการกำกับดูแลและบริหารจัดการการใช้บริการ Cloud Computing

2.1 การกำกับดูแลและบริหารจัดการการใช้บริการ Cloud Computing (Governance of Cloud Computing Services)

วัตถุประสงค์

ปัจจุบันเทคโนโลยี Cloud Computing เข้ามามีบทบาทสำคัญในการขับเคลื่อนธุรกิจ เพื่อช่วยผู้ประกอบการในการบริหารจัดการเทคโนโลยีได้อย่างรวดเร็ว รวมถึงการบริหารต้นทุนที่มีประสิทธิภาพและประสิทธิผล อย่างไรก็ตามการใช้งานระบบ Cloud Computing ที่มีการบริหารจัดการโดยผู้ให้บริการภายนอก และลักษณะการใช้งานสภาพแวดล้อมการประมวลผลร่วมกันของผู้ใช้บริการ รวมถึงการเชื่อมโยงและเข้าถึงผ่านเครือข่ายสาธารณะยังก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์ อันอาจจะส่งผลกระทบต่อการดำเนินงานของผู้ประกอบธุรกิจ ผู้ลงทุน และความเชื่อมั่นต่อตลาดทุนโดยรวมได้ ผู้บริหารระดับสูงจึงต้องมีบทบาทสำคัญในการบริหารจัดการเชิงกลยุทธ์ในการนำเทคโนโลยี Cloud Computing มาใช้ในการประกอบธุรกิจ รวมถึงการกำหนดนโยบายใช้งานเพื่อให้มั่นใจว่าการนำเทคโนโลยี Cloud Computing มาใช้ในการประกอบธุรกิจ ช่วยให้ผู้ประกอบธุรกิจสามารถบรรลุเป้าหมายได้ตามที่กำหนดไว้ โดยมีการใช้ทรัพยากรและมีการบริหารจัดการความเสี่ยงอย่างเหมาะสม

คู่มือฉบับนี้จัดทำขึ้นเพื่อเป็นแนวทางให้ผู้ประกอบธุรกิจในการประยุกต์ใช้งานระบบ Cloud Computing ด้านการกำกับและบริหารจัดการการใช้บริการ Cloud Computing ทั้งนี้ผู้ประกอบธุรกิจควรกำหนดนโยบายการใช้งานระบบ Cloud Computing ไว้อย่างเป็นลายลักษณ์อักษร เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy) จากการใช้บริการที่ครอบคลุมถึงวิธีการคัดเลือกและประเมินผู้ให้บริการ การทบทวนคุณสมบัติของผู้ให้บริการ ข้อกำหนดเกี่ยวกับการใช้บริการและการตรวจสอบบันทึกหลักฐานต่างๆ ที่อาจจะส่งผลกระทบต่อการใช้บริการโดยมีแนวทางดังต่อไปนี้

แนวทางปฏิบัติที่ควรพิจารณา

เพื่อให้การใช้งาน Cloud Computing เป็นไปอย่างมีประสิทธิภาพและประสิทธิผลและยังคงไว้ซึ่งความสามารถในการบริหารความเสี่ยงทางเทคโนโลยีสารสนเทศตลอดจนความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ ผู้ประกอบธุรกิจควรกำหนดนโยบายและกรอบการบริหารจัดการการใช้งานระบบ Cloud Computing ที่ชัดเจน ประกอบด้วย

- กำหนดกลยุทธ์ที่ชัดเจนในการใช้งานระบบ Cloud Computing เช่น เหตุผลและความจำเป็นทางธุรกิจ ประโยชน์และต้นทุน การดำเนินการตามกฎหมายและข้อบังคับทั้งภายในและภายนอกประเทศ ความเสี่ยงและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ การจัดการด้านทรัพยากรบุคคลและองค์ความรู้ เป็นต้น
- จัดทำนโยบายการใช้งาน Cloud Computing อย่างเป็นลายลักษณ์อักษร โดยนโยบายดังกล่าวควรได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจ ทั้งนี้นโยบายฯควรประกอบไปด้วยหัวข้อสำคัญครอบคลุมเรื่องดังต่อไปนี้
    - การกำหนดประเภทงานที่จะใช้บริการ
    - ประเภทของการใช้งานระบบ Cloud Computing ที่สามารถใช้งานได้ เช่น Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), และ/หรือ Infrastructure-as-a-Service (IaaS) และรูปแบบของการใช้บริการ เช่น Private, Public, และ/หรือ Hybrid
    - ประเภทของข้อมูล รวมถึงมาตรการและวิธีปฏิบัติในการรักษาความปลอดภัยของข้อมูลแต่ละประเภทตามชั้นความลับของข้อมูล

- การประเมินความเสี่ยงและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยทางไซเบอร์จากการใช้งาน Cloud Computing
- การประเมินและการคัดเลือกผู้ให้บริการ
- การจัดทำสัญญาและข้อตกลงการให้บริการ
- การติดตามและการกำกับดูแลด้านประสิทธิภาพและการปฏิบัติตามข้อตกลงการให้บริการ
- การติดตามและการรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นจากการให้บริการอย่างสม่ำเสมอ
- การตรวจสอบโดยผู้ตรวจสอบที่เป็นอิสระ
- บทบาทหน้าที่ความรับผิดชอบของเจ้าหน้าที่ผู้เกี่ยวข้อง

ทั้งนี้ การจัดทำนโยบายการใช้งาน Cloud Computing ดังกล่าว ควรพิจารณาถึงเรื่องสำคัญเพื่อกำหนดนโยบายและมาตรการควบคุมที่เหมาะสมประกอบไปด้วยเรื่องดังต่อไปนี้

- ข้อมูลที่มีการจัดเก็บบนระบบ Cloud Computing ที่อาจมีการเข้าถึงและบริหารจัดการโดยผู้ให้บริการ
- ประเภทของสินทรัพย์สารสนเทศ (assets) ที่มีการประมวลผล และบริหารจัดการบนสภาพแวดล้อมระบบ Cloud Computing เช่น ข้อมูลสารสนเทศ ระบบงาน เป็นต้น
- การประมวลผลบนระบบเสมือนที่อาจมีผู้ใช้งานร่วมกันอยู่ภายใต้สภาพแวดล้อมเดียวกัน (Multi-tenant)
- กลุ่มผู้ใช้งานระบบงานหรือบริการบน Cloud Computing และลักษณะการใช้งานหรือบริการ
- การบริหารจัดการกลุ่มผู้ดูแลระบบ (Cloud Service Administrator) ที่มีสิทธิการเข้าถึงและใช้งานระดับสูง (Privileged Access)
- พื้นที่และประเทศที่ผู้ให้บริการ Cloud Computing จัดเก็บข้อมูลและประมวลผล รวมถึงการจัดเก็บข้อมูลแบบชั่วคราว

- จัดให้มีการสื่อสารนโยบายการใช้งาน Cloud Computing ไปยังพนักงานและเจ้าหน้าที่ที่เกี่ยวข้อง เช่น พนักงานและผู้บริหารหน่วยงานทางธุรกิจ (Business unit) ผู้ดูแลระบบ (Administrator) ผู้พัฒนาระบบและผู้พัฒนาระบบการเชื่อมโยง (Developer & Integrator) ผู้ใช้งาน รวมถึงพนักงานและเจ้าหน้าที่ที่เกี่ยวข้อง ให้ตระหนักถึงความมั่นคงปลอดภัยจากการใช้บริการ Cloud Computing ได้แก่
  - มาตรฐานและขั้นตอนการปฏิบัติงานในการใช้บริการ Cloud Computing
  - ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศจากการใช้งาน Cloud Computing และแนวทางการจัดการความเสี่ยง
  - ความเสี่ยงด้านระบบงาน และเครือข่ายจากการใช้งาน Cloud Computing
  - ข้อกำหนดทางกฎหมายที่เกี่ยวข้อง
- จัดเตรียมและพัฒนาองค์ความรู้ด้านการบริหารจัดการ Cloud Computing ให้แก่ผู้ดูแลระบบ (Administrator) และบุคลากรที่เกี่ยวข้องอย่างเพียงพอ เช่น การประเมินความเสี่ยงและการบริหารจัดการความเสี่ยงจากการใช้งานระบบ Cloud Computing กรอบการกำกับดูแลด้านความมั่นคงปลอดภัยระบบ Cloud Computing (Cloud Security Framework) กรอบการกำกับดูแลข้อมูล (Data Governance) เพื่อการรักษาความปลอดภัยและการบริหารจัดการข้อมูลที่จัดเก็บอยู่บนระบบ Cloud Computing เครื่องมือและกรรมวิธีการในการรักษาความปลอดภัยของข้อมูล เช่น การเข้ารหัสโทเคนข้อมูล (Data Tokenization) การลบการเชื่อมโยงถึงบุคคลได้หรือการลบอัตลักษณ์บุคคลออกไปจากฐานข้อมูล (Data anonymization หรือ de-identification) เป็นต้น
- ทบทวนนโยบายการใช้ Cloud Computing อย่างน้อยปีละ 1 ครั้ง

- สอบทานและปรับปรุงแนวทางการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้ครอบคลุมความเสี่ยงจากการใช้บริการ Cloud Computing ทั้งในเรื่องของการระบุความเสี่ยง การประเมินความเสี่ยง การควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และการกำหนดผู้รับผิดชอบต่อความเสี่ยง โดยพิจารณาถึงความเสี่ยงด้านต่าง ๆ ดังต่อไปนี้
    - ความเสี่ยงด้านกลยุทธ์ เช่น ความเสี่ยงจากการพึ่งพิงผู้ให้บริการภายนอกและความสามารถในการเปลี่ยนแปลงผู้ให้บริการ (vendor locked-in)
    - ความเสี่ยงด้านปฏิบัติการ เช่น ระบบประมวลผลผิดพลาดจากระบบให้บริการหรือบุคลากรผู้ให้บริการ การใช้งานเทคโนโลยีร่วมกัน (Share technology risk) การละเมิดข้อกำหนดและข้อตกลงการใช้งาน Cloud Computing หรือความเสี่ยงจากการไม่สามารถเข้าถึงข้อมูลหรือการจำกัดการเข้าถึงของข้อมูลจากผู้ให้บริการ
    - ความเสี่ยงด้านกฎหมาย เช่น การไม่ปฏิบัติตามกฎหมาย หลักเกณฑ์และข้อกำหนดของทางการ ทั้งภายในประเทศและต่างประเทศ
    - ความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น การเรียกใช้โปรแกรม (APIs) หรือช่องทางบริหารจัดการที่ไม่ปลอดภัย
    - ความเสี่ยงด้านข้อมูลส่วนบุคคล (data privacy) และการรักษาความปลอดภัยของข้อมูล (data security)
    - ความเสี่ยงจากการใช้ผู้ให้บริการภายนอกที่มีการใช้ผู้ให้บริการภายนอกอื่นรับช่วงจัดการงาน (sub-contract)
- รายงานผลการประเมินความเสี่ยงและแนวทางการบริหารความเสี่ยงจากการใช้บริการ Cloud Computing ให้แก่คณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการที่ได้รับมอบหมาย

ถึงแม้ว่ากิจกรรมการบริหารงานด้านสารสนเทศของการใช้บริการ (Cloud Computing) นั้นจะมีการดำเนินงานโดยบริษัทผู้ให้บริการ หรือ Cloud Service Provider (CSP) แต่อย่างไรก็ตาม ผู้ประกอบธุรกิจยังคงมีภาระหน้าที่และความรับผิดชอบต่อกิจกรรมการบริหารงานด้านสารสนเทศนั้น ๆ รวมถึงมีหน้าที่ในการดำเนินกิจกรรมการควบคุมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่อยู่นอกเหนือข้อตกลงการให้บริการ และรูปแบบของการใช้งาน Cloud Computing (Deployment Model) ดังแสดงในตารางที่ 1 – ตัวอย่างบทบาทหน้าที่ของผู้ที่เกี่ยวข้องสำหรับรูปแบบการให้บริการ Cloud Computing ดังนั้น ผู้ประกอบธุรกิจจึงจำเป็นต้องประเมินและจัดให้มีการควบคุมการใช้งานระบบประมวลผลในส่วนที่รับผิดชอบโดยผู้ประกอบธุรกิจให้สอดคล้องกับความเสี่ยง และเป็นไปตามที่ระบุไว้ในหลักเกณฑ์ว่าด้วยการจัดให้มีระบบเทคโนโลยีสารสนเทศและแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ กิจกรรมด้านเทคโนโลยีสารสนเทศที่อยู่ภายใต้ความรับผิดชอบของผู้ให้บริการ Cloud Computing ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมและติดตามผลการดำเนินงานโดยผู้ให้บริการให้เป็นไปตามข้อตกลงการให้บริการ และสอดคล้องกับมาตรฐานอันเป็นที่ยอมรับในสากล เช่น การใช้รายงานการตรวจสอบโดยผู้ตรวจสอบที่เป็นอิสระ ที่มีหัวข้อและขอบเขตการตรวจสอบที่สอดคล้องกับขอบเขตการดำเนินงานและภาระหน้าที่ความรับผิดชอบของผู้ให้บริการ และสอดคล้องกับหลักเกณฑ์ว่าด้วยการจัดให้มีระบบเทคโนโลยีสารสนเทศและแนวปฏิบัติที่เกี่ยวข้องของสำนักงาน

ตารางที่ 1 – ตัวอย่างบทบาทหน้าที่ของผู้ที่เกี่ยวข้องสำหรับรูปแบบการให้บริการ Cloud Computing แต่ละรูปแบบ

กิจกรรมด้านการบริหารเทคโนโลยีสารสนเทศ	รูปแบบการให้บริการ (service model)		
	IaaS	PaaS	SaaS
Data	ผู้ประกอบธุรกิจ	ผู้ประกอบธุรกิจ	CSP
Interfaces (APIs, GUIs)	ผู้ประกอบธุรกิจ	ผู้ประกอบธุรกิจ	CSP
Applications	ผู้ประกอบธุรกิจ	ผู้ประกอบธุรกิจ	CSP
Solution Stack (Programming languages)	ผู้ประกอบธุรกิจ	ผู้ประกอบธุรกิจ	CSP
Operating Systems (OS)	ผู้ประกอบธุรกิจ	CSP	CSP
Virtual Machines	ผู้ประกอบธุรกิจ	CSP	CSP
Virtual network infrastructure	ผู้ประกอบธุรกิจ	CSP	CSP
Hypervisors	CSP	CSP	CSP
Processing and Memory	CSP	CSP	CSP
Data Storage (hard drives, removable disks, backups, etc.)	CSP	CSP	CSP
Network (interfaces and devices, communications infrastructure)	CSP	CSP	CSP
Physical facilities / data centers	CSP	CSP	CSP

2.2 <u>การบริหารจัดการผู้ให้บริการ Cloud Computing (Cloud Service Provider Management)</u>

วัตถุประสงค์

Cloud Computing เป็นระบบให้บริการที่มีการบริหารจัดการโดยผู้ให้บริการภายนอก ผู้ประกอบธุรกิจจึงควรมีแนวทางการจัดการให้สอดคล้องเหมาะสมในแต่ละขั้นตอนตั้งแต่การประเมินและคัดเลือกผู้ให้บริการ (Due Diligence) การทำสัญญาและข้อตกลงการให้บริการ (Engage) การใช้งาน (Operate) และการติดตามการให้บริการ (Monitor) โดยมีแนวทางการดำเนินงานในแต่ละขั้นตอน ดังนี้

2.2.1 การประเมินและคัดเลือกผู้ให้บริการ (Due Diligence)

แนวทางปฏิบัติที่ควรพิจารณา

- ผู้ประกอบธุรกิจควรกำหนดกระบวนการและหลักเกณฑ์ในการคัดเลือกผู้ให้บริการ Cloud Computing ที่ชัดเจน และมีการตรวจสอบความพร้อมและพิจารณาความเหมาะสมของผู้ให้บริการเพื่อให้มั่นใจว่าผู้ให้บริการสามารถให้บริการได้อย่างต่อเนื่อง โดยคำนึงถึงปัจจัยสำคัญ ได้แก่ ความรู้ความสามารถ ประสบการณ์ ความสามารถทางการเงินที่สามารถในการให้บริการอย่างต่อเนื่อง
- ประเมินมาตรฐานด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ได้แก่ การรักษาความลับข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูลและระบบสารสนเทศ (Integrity) และ ความต่อเนื่องของการให้บริการ (Availability) เช่น ผลการประเมินมาตรฐานความปลอดภัยที่เป็นที่ยอมรับในสากล ได้แก่ ISO27001, ISO27017, PCI/DSS, TIA เป็นต้น

- ประเมินผลรายงานการตรวจสอบโดยผู้ตรวจสอบที่เป็นอิสระ ด้านมาตรฐานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น System and Organisation Control (SOC) Report โดยพิจารณาถึงขอบเขตการตรวจสอบ ระยะเวลาที่ครอบคลุมในรายงานการตรวจสอบ ผลการตรวจสอบและประเด็นสำคัญในผลการตรวจสอบ ความสามารถและความน่าเชื่อถือของผู้ตรวจสอบ เป็นต้น ทั้งนี้ ผู้ประกอบธุรกิจควรพิจารณาถึงรายละเอียดประกอบในรายงานการตรวจสอบได้แก่
    - ขอบเขตการตรวจสอบสอดคล้องกับมาตรการรักษาความปลอดภัยที่อยู่ในความรับผิดชอบของผู้ให้บริการ
    - ขอบเขตการตรวจสอบสอดคล้องกับมาตรฐานและข้อกำหนดที่เป็นที่ยอมรับในสากล และสอดคล้องกับหลักเกณฑ์ว่าด้วยการจัดให้มีระบบเทคโนโลยีสารสนเทศและแนวปฏิบัติที่เกี่ยวข้อง
- ประเมินความสอดคล้องกันของแนวทางการรักษาความต่อเนื่องของการให้บริการของผู้ให้บริการระบบ Cloud Computing และผลการประเมินผลกระทบทางธุรกิจ (Business Impact Analysis) ของระบบงานที่จะมีการใช้บริการบนระบบ Cloud Computing อันประกอบไปด้วย ระยะเวลาการหยุดชะงักของระบบให้บริการที่ยอมรับได้ (Maximum Tolerable Downtime: MTD) ระยะเวลาที่ยอมรับได้ในการกู้คืนระบบงานและข้อมูล (Recovery Time Objective: RTO) และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery Point Objective: RPO)
- ประเมินความเสี่ยงและแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และความต่อเนื่องในการให้บริการในกรณีที่ผลการประเมินผู้ให้บริการไม่เป็นไปตามข้อกำหนดหรือมาตรฐานความปลอดภัยที่กำหนดไว้

2.2.2 การทำสัญญาและข้อตกลงการให้บริการ (*Engage)*

ในการจัดทำสัญญาและข้อตกลงการให้บริการ ผู้ประกอบธุรกิจต้องจัดให้มีเงื่อนไขและมาตรการเพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อการประมวลผลตามความต้องการของผู้ใช้งาน ที่ครอบคลุมเงื่อนไขสำคัญอย่างน้อย ดังนี้

ก. ข้อตกลงร่วมกันระหว่างผู้ให้บริการและผู้ใช้บริการซึ่งมีรายละเอียดในเรื่องดังต่อไปนี้เป็นอย่างน้อย
    1. หน้าที่และความรับผิดชอบของผู้ให้บริการ รวมถึงความรับผิดชอบต่อผู้ประกอบธุรกิจในกรณีที่ผู้ให้บริการไม่สามารถปฏิบัติตามข้อตกลงได้
    2. ขั้นตอนการปฏิบัติงานที่เป็นไปตามมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากล
    3. มาตรการรักษาความมั่นคงปลอดภัย การควบคุมการเข้าถึง และการเปิดเผยข้อมูลสารสนเทศ
    4. การตรวจสอบการปฏิบัติงานจากผู้ตรวจสอบที่เป็นอิสระ
    5. เงื่อนไขในกรณีที่ผู้ให้บริการจะให้ผู้ให้บริการรายอื่นรับดำเนินการช่วง (Subcontract of the cloud provider) และข้อกำหนดความรับผิดต่อความเสียหายที่อาจเกิดขึ้นจากการดำเนินงานของผู้ให้บริการรายอื่น

ข. คุณสมบัติด้านความปลอดภัยของผู้ให้บริการรายอื่นที่รับดำเนินการช่วงซึ่งเทียบเท่ากับผู้ให้บริการ หรือ เป็นไปตามมาตรฐานสากล

ค. การติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการ

ง. ขั้นตอนการโอนย้ายข้อมูลไปยังผู้ให้บริการรายใหม่ ในกรณีที่มีการเปลี่ยนตัวผู้ให้บริการ

แนวทางปฏิบัติที่ควรพิจารณา

- ผู้ประกอบธุรกิจควรจัดทำสัญญาการใช้บริการจากผู้ให้บริการอย่างเป็นลายลักษณ์อักษร และมีการจัดทำข้อตกลงการให้บริการ (Service Level Agreement) อย่างชัดเจนครอบคลุมประเด็นที่เกี่ยวข้องดังต่อไปนี้
    - ขอบเขตการให้บริการ ประเภท และเงื่อนไขการให้บริการ
    - เงื่อนไขความเป็นเจ้าของข้อมูลของผู้ใช้บริการ สิทธิการใช้และลิขสิทธิ์ที่เกี่ยวข้อง โดยผู้ใช้บริการควรเป็นเจ้าของสิทธิในข้อมูล
    - ข้อกำหนดด้านเงื่อนไขความรับผิดชอบในกรณีที่ผู้ให้บริการไม่สามารถให้บริการตามที่กำหนดในข้อตกลง ทั้งนี้ ผู้ประกอบธุรกิจควรพิจารณาถึงเงื่อนไขการประเมินความเสียหาย รวมถึงข้อจำกัดในกรณีมีเงื่อนไขการจำกัดความรับผิดในสัญญาระหว่างผู้ใช้บริการและผู้ให้บริการ
    - ข้อกำหนดด้านการเข้าถึงข้อมูลของผู้ให้บริการ ประกอบด้วยสิทธิการเข้าถึงและเงื่อนไขการเปิดเผยข้อมูลโดยผู้ให้บริการจากความยินยอมของผู้ใช้บริการ หรือการเปิดเผยข้อมูลโดยข้อกำหนดทางกฎหมายของประเทศที่ผู้ให้บริการไปตั้งศูนย์ข้อมูล ทั้งนี้ ต้องมีการแจ้งให้ผู้ใช้บริการรับทราบ
    - ข้อกำหนดด้านการสำรองข้อมูลและการจัดทำแผนสำรองฉุกเฉิน และแผนความต่อเนื่องทางธุรกิจสำหรับการให้บริการ โดยมีเงื่อนไขที่ชัดเจนทางด้าน
        - สถานที่ในการกู้คืนข้อมูล (Location)
        - ระยะเวลากู้คืนระบบให้บริการ (Service Restoration)
        - ระยะเวลากู้คืนข้อมูล (Recovery Time Objective: RTO)
        - ชุดข้อมูลล่าสุดที่กู้คืนได้ (Recovery Point Objective: RPO)

      ทั้งนี้ ในกรณีเป้าหมายด้านการกู้คืนข้อมูลไม่เป็นไปตามผลการประเมินผลกระทบทางธุรกิจของระบบให้บริการที่ใช้งานระบบ Cloud Computing ผู้ประกอบธุรกิจควรดำเนินการประเมินความเสี่ยงและทำการควบคุมเพิ่มเติม
    - ข้อกำหนดและเงื่อนไขการส่งมอบข้อมูลเมื่อมีการยกเลิก หรือสิ้นสุดการใช้บริการ โดยพิจารณาถึง
        - ระยะเวลา และ เงื่อนไขในการส่งมอบข้อมูล
        - รูปแบบ (Format) ของข้อมูล
        - เงื่อนไขและระยะเวลาในการเก็บรักษาข้อมูลของผู้ใช้บริการ และการทำลายข้อมูลอย่างปลอดภัยเมื่อสิ้นสุดระยะเวลาที่กำหนด
    - ข้อกำหนดด้านเงื่อนไขในกรณีที่ผู้ให้บริการจะให้ผู้ให้บริการรายอื่นรับดำเนินการช่วง (Subcontract of the cloud provider) ได้แก่
        - มาตรการรักษาความปลอดภัยที่เทียบเคียงกับผู้ให้บริการ
        - ความรับผิดต่อความเสียหายของผู้ให้บริการที่เกิดขึ้นจากผู้ให้บริการรายอื่น
    - ข้อกำหนดและมาตรการป้องกันการรั่วไหลของข้อมูลที่อาจเกิดขึ้นจากผู้ให้บริการ
    - มาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับความเสี่ยงและขอบเขตการให้บริการ โดยควรพิจารณาถึง
        - มาตรการรักษาความมั่นคงปลอดภัยเครือข่าย
        - การวิเคราะห์ข้อมูลและการเฝ้าระวังการโจมตีทางเครือข่าย

- การบริหารจัดการบัญชีผู้ใช้งานของผู้ให้บริการ และมาตรการรักษาความปลอดภัยที่เกี่ยวข้อง เช่น นโยบายรหัสผ่านและมาตรฐานการเข้ารหัส
- มาตรฐานการเข้ารหัสการสื่อสารข้อมูล
- การติดตามและติดตั้งชุดปรับปรุงซอฟต์แวร์ (Patching)
- การจัดเก็บบันทึกเหตุการณ์ ประเภทของเหตุการณ์ ระยะเวลาการจัดเก็บข้อมูล การป้องกันการแก้ไขเปลี่ยนแปลงข้อมูล และหน้าที่ความรับผิดชอบในการวิเคราะห์เหตุการณ์

- ข้อกำหนดด้านสิทธิในการตรวจสอบ (Rights to Audit) ประกอบไปด้วย
  - เงื่อนไขการตรวจสอบโดยผู้ประกอบธุรกิจหรือผู้ตรวจสอบที่เป็นอิสระประจำปี หรือเมื่อมีเหตุการณ์อันน่าเชื่อว่ามีการดำเนินงานไม่เป็นไปตามมาตรฐานหรือข้อกำหนด หรือเมื่อได้รับการร้องขอโดยเจ้าพนักงานตามที่ตามกฎหมายกำหนด
  - เงื่อนไขการตรวจสอบเมื่อมีการตรวจพบเหตุการณ์อันน่าเชื่อว่ามีการละเมิดมาตรการรักษาความปลอดภัย หรือการรั่วไหลของข้อมูลความลับ
- เงื่อนไขการตรวจสอบและเปิดเผยรายงานผลการตรวจสอบด้านมาตรการรักษาความปลอดภัยและการควบคุมที่เกี่ยวข้องโดยผู้ตรวจสอบที่เป็นอิสระ อย่างน้อยปีละ 1 ครั้ง
- บทบาทหน้าที่ความรับผิดชอบของผู้ประกอบธุรกิจและผู้ให้บริการ ในกิจกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ ซึ่งพิจารณาถึงความรับผิดชอบในกิจกรรมดังต่อไปนี้
  - การป้องกันโปรแกรมไม่พึงประสงค์ (Malware protection)
  - การสำรองข้อมูล
  - การควบคุมด้านเทคโนโลยีการเข้ารหัส
  - การจัดการช่องโหว่ความปลอดภัย (Vulnerability management) และการติดตั้งชุดโปรแกรมแก้ไขข้อบกพร่อง (Patch)
  - การจัดการเหตุการณ์ผิดปกติ (Incident management)
  - การทดสอบด้านความปลอดภัย
  - การตรวจสอบ (Auditing)
  - การจัดเก็บ การตรวจสอบ และการรักษาความปลอดภัยบันทึกเหตุการณ์
  - การจัดเก็บและทำลายข้อมูลเมื่อมีการยกเลิกหรือสิ้นสุดสัญญาให้บริการ
  - กระบวนการการพิสูจน์ตัวตนในการควบคุมการเข้าถึง
- ช่องทางติดต่อและผู้รับผิดชอบด้านปัญหาการใช้งาน และเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการ

2.2.3 การใช้งาน *Cloud Computing (Operate)*

เพื่อให้การปฏิบัติงานทางด้านการใช้บริการ Cloud Computing เป็นไปตามหลักเกณฑ์ว่าด้วยการจัดให้มีระบบเทคโนโลยีสารสนเทศ ผู้ประกอบธุรกิจควรจัดให้มีการบริหารจัดการเทคโนโลยีสารสนเทศอย่างปลอดภัย ตามหลักการทางด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ 3 ประการ อันได้แก่ ความลับ (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และความพร้อมใช้งาน (Availability) ทั้งนี้บทบาทหน้าที่ในการดำเนินมาตรการรักษาความปลอดภัย

ควรพิจารณาตามบทบาทหน้าที่ในกิจกรรมด้านเทคโนโลยีสารสนเทศที่แสดงรายละเอียดใน ตารางที่ 1 – ตัวอย่างบทบาทหน้าที่ของผู้ให้บริการโดยทั่วไป

กรณีกิจกรรมด้านเทคโนโลยีสารสนเทศอยู่ในความรับผิดชอบของผู้ประกอบธุรกิจ ผู้ประกอบธุรกิจมีหน้าที่ในการจัดให้มีมาตรการรักษาความปลอดภัยที่กำหนดในหลักเกณฑ์ว่าด้วยการจัดให้มีระบบเทคโนโลยีสารสนเทศและแนวปฏิบัติที่เกี่ยวข้อง ในกรณีที่กิจกรรมด้านเทคโนโลยีสารสนเทศอยู่ในความรับผิดชอบของผู้ให้บริการ ผู้ประกอบธุรกิจมีหน้าที่ประเมินความเสี่ยง กำกับ และติดตามให้มีการดำเนินมาตรการรักษาความปลอดภัยโดยผู้ให้บริการอย่างครบถ้วน ทั้งนี้ ผู้ประกอบธุรกิจควรพิจารณาการควบคุมเพิ่มเติม หรือมาตรการเสริมด้านความมั่นคงปลอดภัยสำหรับการใช้บริการ Cloud Computing ดังต่อไปนี้

หัวข้อการควบคุม	มาตรการเสริมด้านความปลอดภัย
การจัดโครงสร้างองค์กร (Internal organization)	○ มีการกำหนดบทบาทหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของผู้ประกอบธุรกิจและผู้ให้บริการอย่างชัดเจน ○ มีการกำหนดช่องทางติดต่อและผู้รับผิดชอบด้านปัญหาการใช้งาน และเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการ ○ มีการจัดทำรายชื่อหน่วยงานที่เกี่ยวข้องในการกำกับดูแล (Authorities) และช่องทางติดต่อ ทั้งในส่วนของผู้ประกอบธุรกิจ และผู้ให้บริการครอบคลุมถึงหน่วยงานทั้งภายในประเทศและต่างประเทศที่มีการจัดเก็บข้อมูลและประมวลผลโดยผู้ให้บริการ
การบริหารทรัพย์สินสารสนเทศ (Asset management)	○ มีการจัดทำรายการทรัพย์สินสารสนเทศและข้อมูลรายละเอียดของทรัพย์สินสารสนเทศที่มีการจัดเก็บและประมวลผลอยู่บนระบบ Cloud Computing เป็นส่วนหนึ่งของรายการทรัพย์สิน (Asset Inventory) ภายในกระบวนการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศและกระบวนการที่เกี่ยวข้อง ○ ข้อมูลสารสนเทศและเอกสารที่มีการจัดเก็บบนระบบ Cloud Computing ควรได้รับการจัดชั้นความลับข้อมูลและระบุประเภท (Labelling) ตามนโยบายการจัดชั้นความลับข้อมูล
การควบคุมการเข้าถึง (Access control)	○ มีการกำหนดการควบคุมการเข้าถึงและสิทธิการใช้งานและบริการทางเครือข่ายของระบบให้บริการ Cloud Computing ที่มีการใช้งาน ○ มีการใช้วิธีพิสูจน์ตัวตนอย่างเหมาะสม เช่น การใช้งาน multi-factor authentication สำหรับการเข้าถึงฟังก์ชันการบริหารระบบ (Administrator page) ○ มีการตรวจสอบวิธีและขั้นตอนการส่งมอบรหัสผ่าน (Secret authentication information) ของการใช้งานระบบ Cloud Computing ของผู้ให้บริการอย่างปลอดภัย ○ มีการตรวจสอบความสามารถในการบริหารจัดการและกำหนดสิทธิการเข้าถึงข้อมูลและบริการที่อยู่บน ระบบ Cloud Computing ได้ตามแนวทางและนโยบายการควบคุมการเข้าถึง เช่น การกำหนดสิทธิการเข้าถึงบริการ การกำหนดสิทธิการเข้าถึงฟังก์ชันตามอำนาจหน้าที่ความรับผิดชอบ การกำหนดสิทธิการเข้าถึงข้อมูล เป็นต้น ○ มีการตรวจสอบแนวทางการควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Utility Program) ในการเข้าถึงและบริหารจัดการระบบ Cloud Computing (ถ้ามี)

หัวข้อการควบคุม	มาตรการเสริมด้านความปลอดภัย
การเข้ารหัส (Cryptography)	○ มีการใช้งานเทคโนโลยีการเข้ารหัสที่สอดคล้องกับความเสี่ยงในกระบวนการรับส่งและจัดเก็บข้อมูลบนระบบ Cloud Computing ทั้งในกรณีมีการดำเนินการโดยผู้ประกอบธุรกิจ หรือ ดำเนินการโดยผู้ให้บริการ ○ มีการควบคุมและจัดการกุญแจการเข้ารหัส (Cryptographic key) ที่มีการใช้งานในระบบ Cloud Computing ให้เป็นตามนโยบายและกระบวนการบริหารจัดการกุญแจการเข้ารหัส ○ กรณีการบริหารจัดการกุญแจการเข้ารหัสดำเนินการโดยผู้ให้บริการ ผู้ประกอบธุรกิจควรรวบรวมข้อมูลและแนวทางการจัดการกุญแจการเข้ารหัสที่อยู่ในความดูแลของผู้ให้บริการ ดังต่อไปนี้ ▪ ประเภทของกุญแจการเข้ารหัส ▪ กระบวนการบริหารจัดการกุญแจการเข้ารหัส ได้แก่ การสร้าง การแก้ไขเปลี่ยนแปลง การจัดเก็บ การเข้าถึง การยกเลิกและทำลายกุญแจการเข้ารหัส ○ กรณีการบริหารจัดการกุญแจการเข้ารหัสดำเนินการโดยผู้ประกอบธุรกิจ ผู้ให้บริการไม่ควรได้รับสิทธิการเข้าถึง จัดเก็บ และบริหารจัดการกุญแจการเข้ารหัส
ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)	○ ผู้ประกอบธุรกิจควรสอบทานนโยบายและแนวทางการทำลาย (Dispose) และการนำกลับมาใช้ (Reuse) ของอุปกรณ์หรือทรัพยากรด้านสารสนเทศของผู้ให้บริการ
การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน (Operation security)	○ ผู้ประกอบธุรกิจควรกำหนดแนวทางการบริหารการแก้ไขเปลี่ยนแปลง ที่ครอบคลุมผลกระทบจากการแก้ไขเปลี่ยนแปลงอันอาจจะเกิดขึ้นจากผู้ให้บริการ ○ ผู้ประกอบธุรกิจควรมีการติดตามการแก้ไขเปลี่ยนแปลงใด ๆ อันอาจมีการดำเนินการโดยผู้ให้บริการ รวมถึงการประเมินผลกระทบจากการเปลี่ยนแปลงได้แก่ ▪ ประเภทของการแก้ไขเปลี่ยนแปลง ▪ แผนการดำเนินการ และระยะเวลาการดำเนินการ ▪ รายละเอียดการแก้ไขเปลี่ยนแปลง ▪ การติดตามการแจ้งเตือนการเริ่มดำเนินการและผลการดำเนินการ ○ ในกรณีมีข้อตกลงให้ผู้ให้บริการมีความรับผิดชอบในกิจกรรมการสำรองข้อมูล ผู้ประกอบธุรกิจควรดำเนินการสอบทานขั้นตอนและแนวทางการสำรองข้อมูลที่ดำเนินการโดยผู้ให้บริการให้มีความสอดคล้องกับนโยบายการสำรองข้อมูลของผู้ประกอบธุรกิจ ○ ในกรณีไม่มีข้อตกลงให้ผู้ให้บริการดำเนินการสำรองข้อมูล ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการสำรองข้อมูลอย่างเพียงพอ และสอดคล้องกับนโยบายการสำรองข้อมูล ○ ผู้ประกอบธุรกิจควรกำหนดความต้องการทางด้านการจัดเก็บบันทึกเหตุการณ์ที่เกี่ยวข้องกับระบบให้บริการ Cloud Computing และตรวจสอบการดำเนินการจัดเก็บบันทึกเหตุการณ์ของผู้ให้บริการ

หัวข้อการควบคุม	มาตรการเสริมด้านความปลอดภัย
	○ กรณีกิจกรรมการบริหารจัดการระบบ (Privileged Operation) อยู่ภายใต้ความรับผิดชอบของผู้ประกอบธุรกิจ ผู้ประกอบธุรกิจควรประเมินความเพียงพอของการจัดเก็บบันทึกเหตุการณ์ที่เกี่ยวข้องกับกิจกรรมการบริหารจัดการระบบ และ/หรือประเมินความจำเป็นในการดำเนินมาตรการเพิ่มเติมเพื่อจัดเก็บและรักษาความปลอดภัยบันทึกเหตุการณ์ดังกล่าว ○ ผู้ประกอบธุรกิจควรตรวจสอบแนวทางในการเทียบเวลา (Clock synchronization) ของผู้ให้บริการ ○ ผู้ประกอบธุรกิจควรตรวจสอบและประเมินแนวทางการบริหารจัดการช่องโหว่ และการติดตั้งชุดโปรแกรมแก้ไข (Patch) ของผู้ให้บริการ
ความมั่นคงปลอดภัยของการสื่อสารข้อมูล (Communication security)	○ ผู้ประกอบธุรกิจควรประเมินและกำหนดความต้องการทางด้านการแบ่งแยกเครือข่ายและสภาพแวดล้อมการใช้งาน Cloud (Tenant isolation) ในสภาพแวดล้อมที่มีการใช้งานร่วมกัน (Multi-tenant) และตรวจสอบการดำเนินการของผู้ให้บริการตามข้อตกลงการให้บริการ
การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System acquisition, development and maintenance)	○ ผู้ประกอบธุรกิจควรดำเนินการประเมินความต้องการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ของการใช้งาน Cloud Computing พร้อมทั้งประเมินและตรวจสอบความสามารถของผู้ให้บริการ cloud เป็นส่วนหนึ่งในกิจกรรมการประเมินและคัดเลือกผู้ให้บริการ (Due Diligence) ○ กรณีการใช้งานในรูปแบบ SaaS ผู้ประกอบการควรประเมินและตรวจสอบผู้ให้บริการด้านการจัดให้มีขั้นตอนและแนวทางการพัฒนาระบบอย่างปลอดภัย (Secure development procedure)
การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information security incident management)	○ มีการกำหนดบาทบาทและหน้าที่ความรับผิดชอบในกระบวนการบริหารจัดการเหตุการณ์อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจนระหว่างผู้ประกอบธุรกิจและผู้ให้บริการ ■ ประเภทของเหตุการณ์ที่จะมีการรายงานไปยังผู้ใช้งาน Cloud Computing ■ รายละเอียดข้อมูลและการตอบสนองต่อเหตุการณ์ ■ กรอบระยะเวลาและขั้นตอนในการแจ้งเตือนเหตุการณ์แก่ผู้ใช้บริการ ■ รายละเอียดช่องทางการติดต่อ ผู้ประสานงาน และผู้รับผิดชอบต่อเหตุการณ์ ■ แนวทางการแก้ไขปัญหา ○ มีการกำหนดช่องทางการติดต่อและขั้นตอนในการรายงานเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศที่ตรวจพบโดยผู้ประกอบธุรกิจ ○ มีการรายงานการติดตามและสถานการณ์ดำเนินการแก้ไขปัญหาที่มีการรายงานโดยผู้ประกอบธุรกิจ ○ มีการกำหนดขั้นตอนและเงื่อนไขในการร้องขอหลักฐาน (Digital evidence) หรือข้อมูลที่เกี่ยวข้องอย่างชัดเจน
การปฏิบัติตามกฎเกณฑ์ (Compliance)	○ ผู้ประกอบธุรกิจควรพิจารณาและประเมินข้อกำหนดทางกฎหมายที่ผู้ให้บริการ Cloud Computing อยู่ภายใต้การบังคับใช้ นอกเหนือจากข้อกำหนดทางกฎหมายที่ใช้บังคับผู้ประกอบธุรกิจ

หัวข้อการควบคุม	มาตรการเสริมด้านความปลอดภัย
	○ ผู้ประกอบธุรกิจควรมีมาตรการตรวจสอบด้านสิทธิและเงื่อนไขการใช้งานซอฟต์แวร์ (Software license) ก่อนดำเนินการติดตั้งลงบนระบบ Cloud Computing เพื่อป้องกันความเสี่ยงจากการละเมิดเงื่อนไขการใช้งาน

2.2.4 การติดตามและประเมินผู้ให้บริการ *(Monitor)*

ผู้ประกอบธุรกิจควรจัดให้มีการติดตาม ประเมิน และทบทวนคุณภาพของการให้บริการของผู้ให้บริการ Cloud Computing

แนวทางปฏิบัติที่ควรพิจารณา

- ผู้ประกอบธุรกิจควรกำหนดบทบาทหน้าที่ และความรับผิดชอบของบุคลากรที่ทำหน้าที่ติดตาม ประเมิน และทบทวนการให้บริการอย่างชัดเจน เพื่อให้มั่นใจถึงการปฏิบัติตามสัญญาการให้บริการ และคุณภาพของบริการ ตลอดจนความเสี่ยงอันอาจจะเกิดจากการใช้บริการ
- ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการ ติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการให้เป็นไปตามข้อกำหนดในข้อตกลงระหว่างผู้ให้บริการและผู้ใช้บริการ Cloud (Cloud Service Agreement) ดังนี้
  - ติดตามตรวจสอบประสิทธิภาพของการให้บริการ รวมทั้งมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับข้อกำหนดตามสัญญาต่าง ๆ หรือข้อตกลงในการให้บริการ ประกอบด้วย
    - รายงานการปฏิบัติตามระดับการให้บริการที่จัดเตรียมโดยบริษัทผู้ให้บริการ เช่น ร้อยละของการให้บริการอย่างต่อเนื่อง ระยะเวลาการตอบสนองและแก้ไขปัญหาตามข้อกำหนด การปรับปรุงและติดตั้งชุดโปรแกรมแก้ไขข้อบกพร่อง รายงานผลการสำรองข้อมูล เป็นต้น
    - รายงานการตรวจสอบโดยผู้ตรวจสอบที่เป็นอิสระ โดยพิจารณาถึง
      1. ประเภทของรายงาน เช่น SOC1, SOC2, SOC3
      2. ขอบเขตการตรวจสอบที่ครอบคลุมถึงมาตรการรักษาความปลอดภัยตามข้อตกลงการให้บริการหรือมาตรฐานอ้างอิงที่เกี่ยวข้อง
      3. ขอบเขตระบบที่อยู่ภายใต้การตรวจสอบที่ครอบคลุมระบบให้บริการ
      4. รายละเอียดวิธีการตรวจสอบและผลการตรวจสอบ
      5. ระยะเวลาที่ครอบคลุมภายใต้การตรวจสอบ
      6. ความสามารถและความน่าเชื่อถือของผู้ตรวจสอบ เป็นต้น

      กรณีรายงานการตรวจสอบโดยผู้ตรวจสอบที่เป็นอิสระมีข้อจำกัด เช่น ขอบเขตและวิธีการตรวจสอบไม่ครอบคลุมถึงมาตรการรักษาความปลอดภัย หรือไม่แสดงรายละเอียดการควบคุมและวิธีการตรวจสอบ ผู้ประกอบธุรกิจควรประเมินความเสี่ยง และแนวทางการบริหารจัดการความเสี่ยงในกรณีเกิดความล้มเหลวของการควบคุม หรือมาตรการรักษาความปลอดภัยดังกล่าว
  - ประเมินความเพียงพอของระบบงานของผู้ให้บริการ (Capacity planning) อย่างสม่ำเสมอ
    - กรณีการใช้งานมีลักษณะเป็นการคิดค่าใช้จ่ายตามการใช้งานจริง ผู้ประกอบธุรกิจควรประเมินความถูกต้องของรายงานการใช้งาน รวมถึงการรับประกันต่อความเพียงพอต่อการใช้งาน (Capacity guarantee)

- กรณีการใช้งานมีลักษณะการกำหนดเงื่อนไขการใช้งานและทรัพยากรที่ตายตัว (Fixed capacity) ผู้ประกอบธุรกิจควรประเมินการใช้งาน และประมาณการการใช้งานทรัพยากร เพื่อวางแผนการจัดหาและใช้งานอย่างเหมาะสม

- ทบทวนเงื่อนไขการให้บริการในกรณีที่มีการเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าการให้บริการยังคงสอดคล้องกับการใช้งานและนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ประกอบธุรกิจ รวมทั้งกฎระเบียบที่เกี่ยวข้องกับการทำธุรกรรมด้านการลงทุนในตลาดทุนไทยอย่างสม่ำเสมอ เช่น การถ่ายโอนข้อมูลที่สำคัญระหว่างประเทศ (Cross-Border Data Transfers) แนวปฏิบัติทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เป็นต้น
- ทบทวนคุณสมบัติของผู้ให้บริการอย่างต่อเนื่อง เช่น การตรวจสอบความมั่นคงในฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการปฏิบัติงาน เป็นต้น

2.2.5 การยกเลิกหรือสิ้นสุดการใช้บริการ *(Exit)*

แนวทางปฏิบัติที่ควรพิจารณา

- ผู้ประกอบธุรกิจควรพิจารณาความเสี่ยงที่เกี่ยวข้องในการยกเลิกการใช้บริการระบบประมวลผลร่วมกันผ่านเครือข่ายอย่างรอบด้านเพื่อกำหนดกลยุทธ์และจัดทำแผนการยกเลิกการใช้บริการอย่างเหมาะสม เพื่อป้องกันหรือลดผลกระทบอันอาจจะเกิดขึ้นจากความเสี่ยง เช่น ความเสี่ยงด้านการหยุดชะงักของระบบให้บริการ ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความลับข้อมูล ความเสี่ยงด้านความถูกต้องของระบบประมวลผล เป็นต้น ทั้งนี้ กระบวนการวางแผนในการยกเลิกหรือการสิ้นสุดการใช้บริการประกอบด้วยขั้นตอนหลัก 4 ขั้นตอนดังต่อไปนี้

  <u>ขั้นตอนที่ 1</u> - การประเมินแนวทางการยกเลิกหรือการสิ้นสุดการใช้บริการ (Pre-assessment)

  - ผู้ประกอบธุรกิจควรประเมินความเป็นไปได้ ความเสี่ยง และแนวทางการยกเลิกหรือสิ้นสุดการใช้บริการ โดยพิจารณาถึงเงื่อนไขและข้อกำหนดที่ระบุในสัญญาการใช้บริการ อันได้แก่ เงื่อนไขการยกเลิกการใช้บริการในกรณีต่างๆ เช่น การสิ้นสุดระยะเวลาการใช้บริการ การบอกเลิกการให้หรือใช้บริการ การสิ้นสุดสัญญาการใช้บริการเนื่องจากการละเมิดเงื่อนไขข้อตกลง เป็นต้น
  - ผู้ประกอบธุรกิจควรประเมินเงื่อนไขที่ระบุในสัญญาการใช้บริการที่เกี่ยวข้องในกระบวนการยกเลิกการใช้บริการที่สำคัญ ได้แก่ บทบาทหน้าที่ความรับผิดชอบระหว่างผู้ใช้บริการและผู้ให้บริการในกระบวนการยกเลิกหรือการสิ้นสุดการใช้บริการ ความเป็นเจ้าของข้อมูล เงื่อนไข รูปแบบ และช่องทางการส่งมอบข้อมูล ระยะเวลาในการเก็บรักษาข้อมูล สิทธิและลิขสิทธิ์ที่เกี่ยวข้อง เป็นต้น
  - ผู้ประกอบธุรกิจควรประเมินถึงเงื่อนไขสำคัญ ภาระผูกพันและหน้าที่ของผู้ให้บริการที่ต้องคงอยู่แม้สิ้นสุดสัญญาการใช้บริการ เช่น หน้าที่ความรับผิดชอบของผู้ให้บริการต่อการรักษาความลับข้อมูล สิทธิการใช้และลิขสิทธิ์ที่เกี่ยวข้อง เป็นต้น
  - ผู้ประกอบธุรกิจควรดำเนินการประเมินความเป็นไปได้ของการยกเลิกหรือการสิ้นสุดการใช้บริการ ความเสี่ยงที่เกี่ยวข้องด้านความต่อเนื่องในการให้บริการจากการยกเลิกสัญญาการใช้ระบบ Cloud Computing บริษัทควรกำหนดกลยุทธ์ แนวทางบริหารความเสี่ยง และจัดทำแผนและแนวทางการยกเลิกการใช้บริการ

ขั้นตอนที่ 2 - การวางกลยุทธ์และแผนการยกเลิกการใช้บริการ (Exit strategy/Plan)

- ในกรณีการเปลี่ยนผู้ให้บริการ ผู้ประกอบธุรกิจควรดำเนินการประเมินและคัดเลือกผู้ให้บริการรายใหม่อย่างเหมาะสมตามข้อ 2.2.1
- ผู้ประกอบธุรกิจควรประเมินความเชื่อมโยงและผลกระทบ ทั้งความเชื่อมโยงและผลกระทบทางเทคนิค (Technical Dependency) และความเชื่อมโยงและผลกระทบของบริการและระบบให้บริการ (Service Dependency) ของระบบและการประมวลผลร่วมกันผ่านเครือข่าย
- ผู้ประกอบธุรกิจควรจัดทำแผนการยกเลิกหรือการสิ้นสุดการใช้บริการในรายละเอียด ประกอบไปด้วยขั้นตอนสำคัญ ระยะเวลาการดำเนินการ บุคลากรผู้รับผิดชอบและบทบาทหน้าที่ความรับผิดชอบ ความเชื่อมโยงและผลกระทบของกิจกรรมสำคัญที่เกี่ยวเนื่องกัน (Task Dependency)
- ผู้ประกอบธุรกิจควรดำเนินการทดสอบแผนการยกเลิกหรือการสิ้นสุดการใช้บริการ เพื่อให้มั่นใจถึงความครบถ้วนสมบูรณ์ของขั้นตอนการดำเนินการ และป้องกันความเสี่ยงและผลกระทบอันอาจจะเกิดขึ้นจากการยกเลิกการใช้บริการ ทั้งนี้ การทดสอบดังกล่าวควรครอบคลุมถึงการทดสอบระบบงานที่จัดทำขึ้นเพื่อทดแทนและรองรับการประมวลผล (Functional test) รวมถึงการทดสอบด้านความครบถ้วนถูกต้องของกระบวนการโอนย้ายข้อมูล (Data migration/conversion test)
- ผู้ประกอบธุรกิจควรประเมินความเป็นไปได้ของแผนการยกเลิกหรือการสิ้นสุดการใช้บริการ โดยพิจารณาจากผลการทดสอบแผนการยกเลิกหรือการสิ้นสุดการใช้บริการ พร้อมทั้งจัดทำเงื่อนไขการตัดสินใจ (Decision criteria) และอำนาจการตัดสินใจ ในขั้นตอนและกระบวนการยกเลิกการใช้บริการ
- ผู้ประกอบธุรกิจควรจัดเตรียมแผนสำรองในการรองรับ กรณีเกิดความล้มเหลวในการดำเนินงานตามแผนการยกเลิกหรือการสิ้นสุดการใช้บริการ เพื่อให้ผู้ประกอบธุรกิจยังคงความสามารถในการให้บริการได้อย่างต่อเนื่อง

ขั้นตอนที่ 3 - การยกเลิกการใช้บริการ (Execution)

- การดำเนินการตามแผนการยกเลิกหรือการสิ้นสุดการใช้บริการควรได้รับการอนุมัติโดยผู้มีอำนาจ
- ผู้ประกอบธุรกิจควรสื่อสารแผนและขั้นตอนการปฏิบัติตามแผนการยกเลิกหรือการสิ้นสุดการใช้บริการในรายละเอียดไปยังผู้ที่เกี่ยวข้องเพื่อซักซ้อมทำความเข้าใจ รวมถึงการสื่อสารไปยังผู้ใช้งานและ/หรือผู้ที่อาจได้รับผลกระทบจากการยกเลิกหรือการสิ้นสุดการใช้บริการ
- ผู้ประกอบธุรกิจควรมีขั้นตอนการตรวจสอบการลบข้อมูลและโปรแกรมที่จัดเก็บอยู่บนระบบประมวลผลร่วมกันบนเครือข่าย เพื่อให้มั่นใจถึงการรักษาความลับและความปลอดภัยข้อมูลและโปรแกรมของผู้ประกอบธุรกิจ

ขั้นตอนที่ 4 - การติดตามผลการยกเลิกการใช้บริการ (Follow-up)

- ผู้ประกอบธุรกิจควรมีการบริหารจัดการผู้ให้บริการระบบประมวลผลร่วมกันผ่านเครือข่าย แม้มีการยกเลิกหรือสิ้นสุดการใช้บริการ เพื่อให้มั่นใจถึงการปฏิบัติตามภาระหน้าที่ความรับผิดชอบที่อาจคงอยู่แม้สัญญาการใช้บริการสิ้นสุดลง เช่น ความรับผิดชอบในการบริหารจัดการความลับข้อมูลที่มีการจัดเก็บในระยะเวลาที่กำหนด การแจ้งเตือนและการสื่อสารเมื่อมีเหตุการณ์ละเมิดหรือการรั่วไหลของข้อมูลความลับ เป็นต้น
- ผู้ประกอบธุรกิจควรประเมินความจำเป็นในการจัดทำแผนการยกเลิกหรือสิ้นสุดการใช้บริการสำหรับผู้ให้บริการรายใหม่ไว้ล่วงหน้า โดยอาศัยประสบการณ์จากการดำเนินการตามแผนการยกเลิกการใช้บริการ