สพร./CDV

ธันวาคม 2568

ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน

มาตรฐานฉบับสมบูรณ์จะมีประกาศในราชกิจจานุเบกษา

ร่าง

มาตรฐานรัฐบาลดิจิทัล

ว่าด้วยแนวทางการใช้คลาวด์

Cloud Usage Standard

สำหรับเวียนขอข้อคิดเห็นจากหน่วยงานต่างๆ ที่เกี่ยวข้อง

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

เลขที่ 999 ชั้น 4 สถาบันเพื่อการยุติธรรมแห่งประเทศไทย ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

หมายเลขโทรศัพท์: 0 2612 6000 โทรสาร: 0 2612 6011 0 2612 6012

มาตรฐานรัฐบาลดิจิทัล

Digital Government Standard

มรด. 9-2 : 2568

DGS 9-2 : 2568

ว่าด้วยแนวทางการใช้คลาวด์

Cloud Usage Standard

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักนายกรัฐมนตรี

มาตรฐานรัฐบาลดิจิทัล
ว่าด้วยแนวทางการใช้คลาวด์

มรด. x-x : 256x

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

เลขที่ 999 ชั้น 4 สถาบันเพื่อการยุติธรรมแห่งประเทศไทย

ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

หมายเลขโทรศัพท์: 0 2612 6000 โทรสาร: 0 2612 6011 0 2612 6012

ประกาศโดย

คณะกรรมการพัฒนารัฐบาลดิจิทัล

วันที่ กรุณาเลือกวันที่ประกาศ

ประกาศในราชกิจจานุเบกษา ฉบับ.....(ชื่อฉบับ).....

เล่ม xxx ตอน...(พิเศษ)... xxx x วันที่ xx xxxxxx พ.ศ. xxx

คณะกรรมการพัฒนารัฐบาลดิจิทัล

ตามมาตรา 6 แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

ประธานกรรมการ

นายกรัฐมนตรี ประธานกรรมการ

กรรมการ

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ปลัดสำนักนายกรัฐมนตรี

ปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม

ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ผู้อำนวยการสำนักงบประมาณ

เลขาธิการคณะกรรมการข้าราชการพลเรือน

เลขาธิการคณะกรรมการพัฒนาระบบราชการ

เลขาธิการสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ

กรรมการผู้ทรงคุณวุฒิในคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม

กรรมการผู้ทรงคุณวุฒิในคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

กรรมการผู้ทรงคุณวุฒิในคณะกรรมการข้อมูลข่าวสารของราชการ

กรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

กรรมการผู้ทรงคุณวุฒิในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

กรรมการและเลขานุการ

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ผู้ช่วยเลขานุการ

เจ้าหน้าที่สำนักงานพัฒนารัฐบาลดิจิทัล

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์
ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

ที่ปรึกษา

นางไอรดา เหลืองวิไล	รองผู้อำนวยการ รักษาการแทนผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย

รองประธานกรรมการ

นายอาศิส อัญญะโพธิ์	รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

กรรมการ

นายมารุต บูรณรัช	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวขนิษฐ์ ผาทอง	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายชะลอ อินทพันธุ์	สำนักบริหารการทะเบียน กรมการปกครอง
นางสาวดารารัตน์ โฆษิตพิพัฒน์	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นางสาวพรพิมล อุ่นไพร	สำนักงานคณะกรรมการกฤษฎีกา
นายสันติ สิทธิเลิศพิศาล	สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นายวีระ วีระกุล	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
รองศาสตราจารย์เกริก ภิรมย์โสภา	จุฬาลงกรณ์มหาวิทยาลัย
ศาสตราจารย์ธีรณี อจลากุล	สถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ
ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์	มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานกระบวนการและการดำเนินงานทางดิจิทัล

ที่ปรึกษา

นางไอรดา เหลืองวิไล	รองผู้อำนวยการ รักษาการแทนผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย
นายอาศิส อัญญะโพธิ์	รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ประธานคณะทำงาน

รองศาสตราจารย์เกริก ภิรมย์โสภา	จุฬาลงกรณ์มหาวิทยาลัย

รองประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์กุลวดี ศรีพานิชกุลชัย	จุฬาลงกรณ์มหาวิทยาลัย

คณะทำงาน

นายสิทธิโชค ชัยปัญญา	กรมการปกครอง
นางวัลภา นุตโร	กรมบัญชีกลาง
นางสาวพณิชา เกื้อประจง	กรมพัฒนาธุรกิจการค้า
นายกำชัย จัตตานนท์	กรมศุลกากร
นางจันทร์เจริญ แบร์โรวส์	กรมสรรพากร
นางสาวดารารัตน์ โฆษิตพิพัฒน์	สำนักงานคณะกรรมการพัฒนาระบบราชการ
พ.ต.ต.วรกร ทองสุข	สำนักงานตรวจคนเข้าเมือง
พ.ต.อ.ณัทกฤช พรหมจันทร์	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
นายชาลี วรกุลพิพัฒน์	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวขนิษฐ์ ผาทอง	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายเมธวิน กิติคุณ	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายคฑาวุธ ปาระมี	สมาคมไทยบล็อกเชน
นายอธิบดี ลิมสัมพันธ์สันติ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายอุสรา วิสารทานนท์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยเลขานุการ

นายธีรวัฒน์ โรจนไพฑูรย์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิเคราะห์และจัดทำมาตรฐานรัฐบาลดิจิทัล
ว่าด้วยแนวทางการใช้คลาวด์

นายธีรวัฒน์ โรจนไพฑูรย์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาวพิมพ์ชนก เจ็กภู่	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายณัฐพงศ์ บุบผะศิริ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายธนัตถ์ โอมพรนุวัฒน์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

มาตรฐานรัฐบาลดิจิทัลฉบับนี้ ได้ผ่านการประชาพิจารณ์รับฟังความคิดเห็นเป็นการทั่วไป และนำข้อมูลข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้องมาปรับปรุงมาตรฐานฉบับนี้จนมีความสมบูรณ์ครบถ้วน นอกจากนี้ ยังได้รับการพิจารณากลั่นกรองจากคณะทำงานเทคนิคด้านมาตรฐานกระบวนการและการดำเนินงานทางดิจิทัล และผ่านการพิจารณาเห็นชอบจากคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 เพื่อให้มั่นใจว่ามาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วน และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพสูงสุด

มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0 จัดทำโดยฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สำนักนายกรัฐมนตรี

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เลขที่ 999 ชั้น 4 สถาบันเพื่อการยุติธรรมแห่งประเทศไทย
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
E-mail: sd-g1_division@dga.or.th
Website: www.dga.or.th

คำนำ

ปัจจุบัน เทคโนโลยีคลาวด์ (Cloud Technology) ถือเป็นโครงสร้างพื้นฐานทางดิจิทัลที่มีความสำคัญอย่างยิ่งต่อการขับเคลื่อนการทำงานของภาครัฐ ทั้งในด้านการเพิ่มประสิทธิภาพการปฏิบัติภารกิจและการยกระดับการให้บริการประชาชนให้มีความสะดวก รวดเร็ว และทันสมัย เพื่อให้การนำเทคโนโลยีดิจิทัลมาประยุกต์ใช้เกิดประโยชน์สูงสุดและเป็นไปในทิศทางเดียวกัน คณะกรรมการพัฒนารัฐบาลดิจิทัล จึงได้มีมติมอบหมายให้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร. ดำเนินการจัดทำรายละเอียดมาตรฐานที่เกี่ยวข้อง เพื่อให้หน่วยงานภาครัฐสามารถนำไปปฏิบัติได้อย่างเป็นรูปธรรม

เพื่อให้การขับเคลื่อนนโยบายดังกล่าวเป็นไปอย่างมีประสิทธิภาพ สพร. จึงได้จัดทำ มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการใช้คลาวด์ ฉบับนี้ขึ้น โดยเป็นส่วนหนึ่งของชุดมาตรฐานสำคัญ 2 ฉบับ ได้แก่ 1) แนวทางการใช้คลาวด์ และ 2) แนวทางการกำหนดมาตรฐานบริการผู้ให้บริการคลาวด์

มาตรฐานฉบับนี้ มุ่งหมายให้เป็นกรอบแนวทางปฏิบัติสำหรับหน่วยงานของรัฐในการวางแผน เลือกใช้และบริหารจัดการเทคโนโลยีคลาวด์ ให้เหมาะสมกับระดับชั้นข้อมูลและภารกิจ เพื่อให้เกิดการบูรณาการระบบที่มีเอกภาพ ลดความเสี่ยงด้านความมั่นคงปลอดภัยในการปกป้องข้อมูลสำคัญของรัฐ และเกิดความคุ้มค่าในการบริหารจัดการทรัพยากรโดยรวม โดยเนื้อหาจะครอบคลุมตั้งแต่แนวทางการเลือกรูปแบบบริการ การประเมินความคุ้มค่า มาตรการความมั่นคงปลอดภัย ไปจนถึงการบริหารจัดการสัญญา เพื่อยกระดับบริการภาครัฐให้มีความยืดหยุ่น และมีประสิทธิภาพสูงสุด

สารบัญ

สารบัญตาราง

สารบัญภาพ

มาตรฐานรัฐบาลดิจิทัล
ว่าด้วยแนวทางการใช้คลาวด์

1. บทนำ

1.1. หลักการและความจำเป็น

เพื่อเป็นการยกระดับประสิทธิภาพของการบริหารงาน และการบริการประชาชน รองรับการเปลี่ยนผ่านไปสู่การเป็นรัฐบาลดิจิทัล ปัจจุบันหน่วยงานของรัฐจึงได้นำเทคโนโลยีคลาวด์มาประยุกต์ใช้ ซึ่งก่อให้เกิดประโยชน์ในการลดภาระด้านค่าใช้จ่ายในการจัดหาและบำรุงรักษาโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ อย่างไรก็ตาม ด้วยความแตกต่างของบริบทและลักษณะการดำเนินงานของแต่ละหน่วยงาน อาจนำไปสู่ความท้าทายในการเลือกใช้บริการคลาวด์อย่างมีประสิทธิผล สามารถบูรณาการร่วมกันได้อย่างมีเอกภาพ ลดความเสี่ยงด้านความมั่นคงปลอดภัยและการปกป้องข้อมูลภาครัฐที่สำคัญ เกิดความคุ้มค่าในการบริหารจัดการทรัพยากรโดยรวม ช่วยส่งเสริมการประหยัดค่าใช้จ่ายทั้งในส่วนของโครงสร้างพื้นฐานและการบำรุงรักษาในระยะยาว

1.2. วัตถุประสงค์

มาตรฐานว่าด้วยแนวทางการใช้คลาวด์ ฉบับนี้จัดทำขึ้นเพื่อกำหนดแนวทางให้หน่วยงานของรัฐนำไปปฏิบัติให้สอดคล้องและเหมาะสมกับบริการของหน่วยงาน

1) สนับสนุนการเปลี่ยนผ่านสู่รัฐบาลดิจิทัล (Digital Government Transformation) โดยการประยุกต์ใช้เทคโนโลยีคลาวด์ (Cloud) เพื่อเพิ่มประสิทธิภาพในการดำเนินงาน และการให้บริการประชาชนอย่างมีประสิทธิภาพ และมีความมั่นคงปลอดภัย
1) เพิ่มความคุ้มค่าในการใช้งบประมาณ (Cost Efficiency) ลดค่าใช้จ่ายที่เกี่ยวข้องกับการจัดซื้อและบำรุงรักษาโครงสร้างพื้นฐานทางเทคโนโลยี ใช้ทรัพยากรคลาวด์ร่วมกันระหว่างหน่วยงาน เพื่อประหยัดต้นทุน

1.3. ขอบข่าย

มาตรฐานรัฐบาลดิจิทัลฉบับนี้ ว่าด้วยการกำหนดแนวทางการใช้คลาวด์สำหรับหน่วยงานของรัฐ เพื่อเพิ่มประสิทธิภาพการให้บริการประชาชนอย่างมั่นคงปลอดภัย ประหยัดค่าใช้จ่ายทางด้านโครงสร้างพื้นฐาน และการบำรุงรักษา สร้างความสมดุลระหว่างความปลอดภัย และความคุ้มค่า โดยมีเขตของเนื้อหาโดยสรุปมีดังนี้

1) การเลือกประเภทของคลาวด์ การวิเคราะห์จัดประเภทข้อมูล และเลือกประเภทของคลาวด์ที่มีให้บริการได้อย่างเหมาะสม ได้แก่
    - คลาวด์สาธารณะ (Public Cloud)
    - คลาวด์ส่วนตัว (Private Cloud)
    - คลาวด์แบบกลุ่ม (Community Cloud)
    - คลาวด์แบบผสม (Hybrid Cloud)
    - คลาวด์อธิปไตย (Sovereign Cloud)
    - คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud)
2) การเลือกรูปแบบบริการคลาวด์ (Cloud Services) การพิจารณาเลือกรูปแบบบริการที่เหมาะสมกับลักษณะงาน เช่น
    - IaaS (Infrastructure as a Service) สำหรับงานที่ต้องการควบคุมโครงสร้างพื้นฐาน
    - PaaS (Platform as a Service) สำหรับการพัฒนาและปรับใช้แอปพลิเคชัน
    - SaaS (Software as a Service) สำหรับการใช้งานซอฟต์แวร์สำเร็จรูป
3) การวางแผนดำเนินการย้ายไปใช้บริการคลาวด์ การย้ายระบบงานหรือข้อมูลไปยังคลาวด์ รวมถึงแนวทางในการใช้นวัตกรรมใหม่ และการวางแผนการออกจากระบบคลาวด์
4) การประเมินราคา ประเมินการคิดค่าใช้จ่ายของทรัพยากร เช่น จำนวนแกนประมวลผล (Core) หน่วยความจำ (Memory) พื้นที่จัดเก็บข้อมูล (Storage) รวมถึงค่าธรรมเนียมแฝง เช่น ค่าโอนข้อมูล (Data Transfer Cost) และค่าบริการอื่นเพิ่มเติม
5) การบริหารต้นทุน และการตรวจสอบ ปรับปรุงการใช้งานคลาวด์ แนวคิดการบริหารต้นทุนอย่างมีประสิทธิภาพ โดยติดตาม ตรวจสอบ และปรับปรุงการใช้งานคลาวด์อย่างต่อเนื่อง
6) การดูแลรักษาด้านการสำรองข้อมูลและความมั่นคงปลอดภัย การปฏิบัติตาม มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 รวมถึงการวางแผนและกำหนดมาตรการสำรองข้อมูล (Backup) และกู้คืนข้อมูล (Disaster Recovery)

ทั้งนี้ หน่วยงานของรัฐอาจต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ ที่แตกต่างกัน หรือมีรูปแบบการประยุกต์ใช้ทางเทคโนโลยีเป็นการเฉพาะ ควรปรึกษาผู้เชี่ยวชาญด้านกฎหมาย ด้านการเงินและงบประมาณ และด้านเทคโนโลยีสารสนเทศ ที่เกี่ยวข้องก่อนดำเนินการ

1.4. บทนิยาม

ความหมายของคำศัพท์ที่ใช้ในมาตรฐานรัฐบาลดิจิทัลฉบับนี้ มีดังนี้

การประมวลผลแบบคลาวด์ (Cloud Computing) หรือคลาวด์ (Cloud) หมายความว่า รูปแบบการเข้าถึงทรัพยากร[1]ทางกายภาพหรือเสมือนผ่านเครือข่ายสารสนเทศ ซึ่งสามารถแบ่งปันให้ใช้งานร่วมกันได้ (Shareable) อย่างยืดหยุ่น (Elastic) และปรับขยายได้ (Scalable) โดยรองรับการจัดสรรและบริหารจัดการทรัพยากรด้วยตนเอง (Self-service Provisioning[2]) ตามความต้องการ (On-demand) [2]

บริการคลาวด์ (Cloud Service) หมายความว่า การนำเสนอความสามารถของการประมวลผลแบบคลาวด์รูปแบบใดแบบหนึ่งหรือมากกว่านั้นให้กับผู้ใช้บริการ โดยสามารถเรียกใช้งานผ่านอินเทอร์เฟซที่กำหนดไว้ [2]

คลาวด์สาธารณะ (Public Cloud) หมายความว่า บริการคลาวด์ที่เปิดให้บริการกับผู้ใช้บริการทั่วไป โดยทรัพยากรทั้งหมดอยู่ภายใต้การควบคุมของผู้ให้บริการคลาวด์ [2]

คลาวด์ส่วนตัว (Private Cloud) หมายความว่า บริการคลาวด์ที่ใช้งานโดยผู้ใช้บริการเพียงรายเดียว โดยทรัพยากรทั้งหมดอยู่ภายใต้การควบคุมของผู้ใช้บริการรายนั้น [2]

คลาวด์แบบกลุ่ม (Community Cloud) หมายความว่า บริการคลาวด์ที่ใช้เฉพาะกลุ่มผู้ใช้บริการที่มีความต้องการใช้งานและมีความเกี่ยวข้องกัน ซึ่งทรัพยากรถูกควบคุมโดยสมาชิกในกลุ่ม [2]

คลาวด์แบบผสม (Hybrid Cloud) หมายความว่า การใช้บริการคลาวด์ที่รวมการใช้งานคลาวด์ส่วนตัว (Private Cloud) และคลาวด์สาธารณะ (Public Cloud) เข้าด้วยกัน [2]

คลาวด์อธิปไตย (Sovereign Cloud) หมายความว่า บริการคลาวด์ ภายใต้การควบคุมโดยภาครัฐ และดูแลโดยบุคลากรที่ได้รับอนุญาต และใช้สำหรับให้บริการกับหน่วยงานของรัฐเท่านั้น

คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud - VPC) หมายความว่า บริการคลาวด์สาธารณะ (Public Cloud) ที่มีการเพิ่มมาตรการคุ้มครองข้อมูลมากกว่าการใช้งานคลาวด์สาธารณะทั่วไป โดยมีการแยกการบริหารจัดการทรัพยากรและการใช้งานเฉพาะผู้ใช้บริการแต่ละราย (Isolation)

การให้บริการโครงสร้างพื้นฐาน (Infrastructure as a Service: IaaS) หมายความว่า หมวดหมู่ของบริการคลาวด์ที่ผู้ใช้บริการสามารถกำหนดการใช้งานหน่วยประมวลผล พื้นที่จัดเก็บข้อมูล และเครือข่ายได้เองตามความต้องการ [2]

---

[1] ตัวอย่างของทรัพยากรคอมพิวเตอร์ ได้แก่ คอมพิวเตอร์แม่ข่าย ระบบปฏิบัติการ เครือข่าย ซอฟต์แวร์ แอปพลิเคชัน และอุปกรณ์จัดเก็บข้อมูล

[2] การจัดสรรด้วยตนเอง (Self-service Provisioning) หมายถึง การจัดสรรทรัพยากรที่บริการคลาวด์มอบให้ ซึ่งดำเนินการโดยผู้ใช้บริการคลาวด์ ผ่านระบบอัตโนมัติ

การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS) หมายความว่า หมวดหมู่ของบริการคลาวด์ที่ผู้ใช้บริการสามารถติดตั้ง บริหารจัดการ หรือเรียกใช้แอปพลิเคชันที่ผู้ใช้บริการกำหนดเองด้วยคำสั่ง ภาษา หรือสภาพแวดล้อมที่ผู้ให้บริการรองรับ [2]

การให้บริการซอฟต์แวร์ (Software as a Service: SaaS) หมายความว่า หมวดหมู่ของบริการคลาวด์ที่ผู้ใช้บริการสามารถใช้งานซอฟต์แวร์ที่ผู้ให้บริการจัดเตรียมไว้ได้ [2]

ข้อมูลที่สามารถเปิดเผยได้ (Official Data) หมายความว่า ข้อมูลที่สร้าง ประมวลผล ส่ง หรือรับของหน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้อง ซึ่งอาจก่อให้เกิดความเสียหายได้ไม่เกินความเสียหายในระดับต่ำ หากมีการละเมิดความปลอดภัยจะมีการใช้มาตรฐานการควบคุมที่สามารถคุ้มครองข้อมูลให้มีความปลอดภัยจากการโจมตีในรูปแบบต่างๆ ซึ่งอาจเพิ่มการรับรองมาตรการควบคุม

ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data) หมายความว่า ข้อมูลที่มีความอ่อนไหวสูงหากเปิดเผยอาจก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ หรือเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง ซึ่งส่งผลต่อความมั่นคงของชาติ และ/หรือความสัมพันธ์ระหว่างประเทศ ความมั่นคง/เสถียรภาพทางการเงิน หรือขัดขวางความสามารถในการสืบสวนคดีอาชญากรรมที่ร้ายแรง หรือองค์กร ที่จำเป็นต้องมีมาตรการควบคุมที่เข้มงวด และมีการกำหนดการใช้เครือข่ายที่ปลอดภัยบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัย และมีการปฏิบัติอย่างเหมาะสม ซึ่งรวมถึงการใช้สถาปัตยกรรมแบบ Zero - Trust การเข้ารหัส และการปฏิบัติตามมาตรฐานความปลอดภัยทั้งในระดับชาติและระดับสากลอย่างเคร่งครัด

ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) หมายความว่า ข้อมูลที่มีความอ่อนไหวเป็นพิเศษ หากเปิดเผยอาจเกิดความเสียหายอย่างร้ายแรงที่สุดต่อรัฐ ซึ่งส่งผลความมั่นคงของชาติหรือพันธมิตร และต้องการมาตรการควบคุมความปลอดภัยที่สูงมาก เพื่อป้องกันการละเมิดข้อมูลจากภัยคุกคามทั้งหมด โดยการใช้เครือข่ายบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัยสูง และมีการควบคุมความปลอดภัยอย่างเข้มงวด ซึ่งรวมถึงการใช้สถาปัตยกรรมแบบ Zero-Trust การเข้ารหัส และการปฏิบัติตามมาตรฐานความปลอดภัยทั้งในระดับชาติและระดับสากลอย่างเคร่งครัด

1.5. กฎหมายและแนวทางที่เกี่ยวข้อง

มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการใช้คลาวด์ มีความเกี่ยวข้องกับกฎหมายหรือแนวปฏิบัติ ดังนี้

1) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
2) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
3) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการใช้บริการคลาวด์ พ.ศ. 2562
4) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

5) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

2. แนวทางการเลือกใช้บริการคลาวด์ของหน่วยงานภาครัฐ

2.1. ประเภทของคลาวด์

ประเภทของคลาวด์ตามลักษณะการนำไปใช้ (Cloud Deployment Models) โดยทั่วไป ได้แก่ คลาวด์สาธารณะ คลาวด์ส่วนตัว คลาวด์แบบผสม คลาวด์แบบกลุ่ม คลาวด์ส่วนตัวเสมือน และคลาวด์อธิปไตย ซึ่งมีข้อดีและข้อเสีย แตกต่างกันดังรายละเอียดตามตารางที่ 1 [3]

ตารางที่ 1 ประเภทของคลาวด์

หัวข้อ	คลาวด์สาธารณะ (Public Cloud)	คลาวด์ส่วนตัว (Private Cloud)	คลาวด์แบบผสม (Hybrid Cloud)	คลาวด์แบบกลุ่ม (Community Cloud)	คลาวด์ส่วนตัวเสมือน (VPC)	คลาวด์อธิปไตย (Sovereign Cloud)
ข้อดี	-ไม่ต้องลงทุนโครงสร้างพื้นฐาน - ลดค่าใช้จ่าย และความซับซ้อนในการจัดการบำรุงรักษา (ผู้ให้บริการดำเนินการให้) - ง่ายในการจัดการ (Provisioning)	- สามารถปรับแต่งบริการคลาวด์ได้ทั้งหมด (Fully customizable) - โครงสร้างพื้นฐานและข้อมูลทั้งหมดอยู่ในการควบคุมของหน่วยงานเอง - มีความปลอดภัยสูง (เมื่อดำเนินการได้ตามมาตรฐานที่เกี่ยวข้อง)	- ความยืดหยุ่นด้านการจัดการข้อมูลและความจุ - ความสามารถในการกู้คืนจากความขัดข้องของบริการ	- สามารถแบ่งการใช้จ่ายร่วมกันในกลุ่ม - สามารถปรับแต่งบริการคลาวด์ได้ตามความต้องการของกลุ่ม	-ไม่ต้องลงทุนโครงสร้างพื้นฐาน - มีความเป็นส่วนตัวสูง (Isolation) บนโครงสร้างพื้นฐานคลาวด์สาธารณะ - ความยืดหยุ่น ในการปรับเพิ่ม/ลดทรัพยากร (On-demand) - ลดค่าใช้จ่าย และความซับซ้อนในการจัดการบำรุงรักษา (ผู้ให้บริการดำเนินการให้) - ง่ายในการจัดการ (Provisioning)	- ข้อมูลตั้งอยู่ภายใต้กฎหมายที่เกี่ยวข้องของประเทศ - ป้องกันการเข้าถึงข้อมูล ลดความเสี่ยงในการถูกแทรกแซงของต่างประเทศ - เป็นทางเลือกที่ดีสำหรับหน่วยงานรัฐและธุรกิจที่ต้องการความมั่นคงปลอดภัยสูง
ข้อเสีย	- ผู้ให้บริการต้องได้รับการกำกับดูแลที่ดี - ความล่าช้าในการรับส่งข้อมูลที่อาจเกิดขึ้น	- มีต้นทุนโครงสร้างพื้นฐานสูงเมื่อเทียบกับประเภทอื่น - การใช้ทรัพยากรอาจไม่เต็มประสิทธิภาพ - มีค่าใช้จ่ายด้านดูแลบำรุงรักษาเสมอเมื่อเทียบกับประเภทอื่น	- อาจมีปัญหาด้านความเข้ากันได้ของระบบคลาวด์ - มีความซับซ้อนในการบริหารจัดการ	- การปรับขยายขนาดทรัพยากรอาจมีข้อจำกัด เนื่องจากมีการจัดการร่วมกัน	- แม้จะแยกทรัพยากร แต่โครงสร้างพื้นฐานยังอยู่บน Public Cloud (มีความปลอดภัยสูง แต่ไม่สูงสุดเท่า Private Cloud ที่ดูแลเองทั้งหมด) - ความล่าช้าในการทำงาน อาจเกิดขึ้นได้ขึ้นอยู่กับเสถียรภาพ	- กรณีภาครัฐจัดทำขึ้นเองทั้งหมดจะมีค่าใช้จ่ายในการลงทุนโครงสร้างพื้นฐาน และต้องมีผู้เชี่ยวชาญในการดูแล - ลงทุนระดับของเทคโนโลยีที่นำมาใช้อาจจะไม่เทียบเท่า Public Cloud ขนาดใหญ่ (Hyperscaler)

หัวข้อ	คลาวด์สาธารณะ (Public Cloud)	คลาวด์ส่วนตัว (Private Cloud)	คลาวด์แบบผสม (Hybrid Cloud)	คลาวด์แบบกลุ่ม (Community Cloud)	คลาวด์ส่วนตัวเสมือน (VPC)	คลาวด์อธิปไตย (Sovereign Cloud)
					ของเครือข่ายและผู้ให้บริการ	-อัตราค่าบริการอาจจะสูงกว่า Public Cloud เนื่องจากฐานผู้ใช้อยู่ในวงจำกัด

จากการสรุปข้อดีและข้อเสียของคลาวด์แต่ละประเภท หน่วยงานสามารถพิจารณาเลือกใช้บริการคลาวด์ให้เหมาะสมกับการนำไปใช้ โดยคำนึงถึงปัจจัยหลักที่เกี่ยวข้อง [4-5] ดังต่อไปนี้:

1) ความมั่นคงปลอดภัย (Security) เป็นการพิจารณาระดับการป้องกันข้อมูลและระบบที่เหมาะสม เพื่อป้องกันการโจมตีทางไซเบอร์หรือการเข้าถึงที่ไม่ได้รับอนุญาต

2) ความสามารถในการปรับขยาย (Scalability) และความยืดหยุ่น (Flexibility) เป็นการกำหนดความสามารถในการเพิ่มหรือลดทรัพยากรได้ตามความต้องการของผู้ใช้บริการ หรือมีการเพิ่มหรือลดทรัพยากรแบบอัตโนมัติ (Auto Scaling) ซึ่งสามารถตอบสนองต่อการให้บริการของหน่วยงานได้อย่างมีประสิทธิภาพ

3) ค่าใช้จ่าย (Cost) เป็นการประเมินต้นทุนที่เกี่ยวข้องกับการใช้บริการคลาวด์ ซึ่งรวมถึงค่าใช้จ่ายเริ่มต้นและค่าใช้จ่ายรายเดือน ที่ต้องมีความเหมาะสมกับงบประมาณของหน่วยงาน

4) การบริหารจัดการ (Management) เป็นระดับความซับซ้อนในการตั้งค่า การบำรุงรักษา และการจัดการระบบคลาวด์ที่ต้องมีความเหมาะสมต่อการดำเนินการของหน่วยงาน

5) การปฏิบัติตามกฎหมายที่เกี่ยวข้อง (Regulatory Compliance) เป็นการเลือกประเภทของคลาวด์ที่มีความสอดคล้องกับข้อกำหนดทางกฎหมายที่เกี่ยวข้องกับข้อมูล หรือบริการบนระบบคลาวด์ เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 หรือระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

2.2. แนวทางการเลือกประเภทคลาวด์

แนวทางการเลือกประเภทคลาวด์ถือเป็นจุดเริ่มต้นสำคัญในการตัดสินใจเพื่อดำเนินการปรับเปลี่ยนระบบหรือบริการของหน่วยงานภาครัฐไปสู่ระบบคลาวด์ โดยทั่วไปการพิจารณาจะขึ้นอยู่กับปัจจัยด้านความต้องการของหน่วยงาน ซึ่งปัจจัยหลักที่เกี่ยวข้อง ได้แก่ ความมั่นคงปลอดภัย ความสามารถในการปรับขยาย ความยืดหยุ่น ความซับซ้อนในการบริหารจัดการ และการปฏิบัติตามกฎหมายที่เกี่ยวข้อง

เพื่อให้สอดคล้องกับนโยบายรัฐบาลที่มุ่งเน้นให้หน่วยงานของรัฐพิจารณาเลือกใช้ คลาวด์สาธารณะ (Public Cloud) เป็นลำดับแรก สำหรับโครงการใหม่หรือโครงการที่มีแผนปรับปรุงระบบ เพื่อลดภาระด้านการลงทุนโครงสร้างพื้นฐาน การบำรุงรักษา และการจัดหาบุคลากรผู้เชี่ยวชาญ ในการดำเนินการ หน่วยงาน

จำเป็นต้องเริ่มจากการ จำแนกประเภทข้อมูล (Data Classification) ที่ประสงค์จะนำขึ้นสู่ระบบคลาวด์ โดยอ้างอิงตาม มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและการแบ่งปันข้อมูลภาครัฐ (มสพร. 8-2565) และฉบับแก้ไขเพิ่มเติม ควบคู่กับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลที่เกี่ยวข้อง เมื่อทราบระดับชั้นของข้อมูลแล้ว จึงนำมาพิจารณาเลือกรูปแบบบริการคลาวด์ที่เหมาะสม ดังนี้

กรณีบริการเป็นข้อมูลที่สามารถเปิดเผยได้ (Official Data) ให้เลือกใช้คลาวด์สาธารณะ (Public Cloud) ส่วนบริการที่มีข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data) ให้ใช้คลาวด์สาธารณะ (Public Cloud) ที่มีมาตรการด้านความปลอดภัยสูง เช่น คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud) ทั้งนี้การใช้คลาวด์สาธารณะ (Public Cloud) มีความเหมาะสมเป็นพิเศษ สำหรับข้อมูลตามประเภทข้างต้น เนื่องจากการลงทุนอย่างมีนัยสำคัญของผู้ให้บริการคลาวด์ในโครงสร้างพื้นฐาน การดูแลรักษาความมั่นคงปลอดภัยไซเบอร์รวมถึง การใช้ปัญญาประดิษฐ์ (AI) เพื่อการตรวจจับภัยคุกคามขั้นสูง การเฝ้าระวังติดตามอย่างต่อเนื่อง และความสามารถในการตอบสนองต่อเหตุการณ์อย่างรวดเร็ว โดยบริการคลาวด์เหล่านี้มักมีมาตรฐานความปลอดภัยที่สูงกว่าที่หน่วยงานแต่ละแห่งจะสามารถจัดให้มีได้เอง พร้อมทั้งมีความสามารถในการปรับขยาย (Scalability) และการสนับสนุนการปฏิบัติตามข้อกำหนดด้านมาตรฐานต่างๆ อีกด้วย

การใช้คลาวด์สาธารณะต้องเลือกใช้ถิ่นที่อยู่ของข้อมูลให้มีความเหมาะสม เป็นไปตามกฎหมาย และข้อบังคับด้านอธิปไตยทางข้อมูล (Data Sovereignty) ของประเทศ

กรณีที่บริการเป็นประเภทข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) ให้พิจารณาใช้คลาวด์อธิปไตย (Sovereign Cloud) ซึ่งออกแบบมาเพื่อให้มั่นใจว่า ข้อมูลทั้งหมด (รวมถึง แอปพลิเคชัน และข้อมูลที่อยู่ระหว่างการส่งผ่านเครือข่าย) ถูกจัดเก็บ ประมวลผล และบริหารจัดการ อยู่ภายในประเทศหรือภูมิภาคที่กำหนด และเป็นไปตามกฎหมายและข้อบังคับด้านอธิปไตยทางข้อมูล (Data Sovereignty) ของประเทศอย่างเคร่งครัด และสามารถใช้คลาวด์แบบผสม (Hybrid Cloud) ซึ่งมีการแยกข้อมูลที่ต้องได้รับความคุ้มครองสูงสุดไว้ในคลาวด์ส่วนตัว (Private Cloud)

ตารางที่ 2 แนวทางการจำแนกประเภทข้อมูลเพื่อใช้บริการคลาวด์

ประเภทข้อมูล	คำอธิบาย	ประเภทบริการคลาวด์ที่แนะนำ
Official Data	ข้อมูลที่สร้าง ประมวลผล ส่ง หรือรับของหน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้อง ซึ่งอาจก่อให้เกิดความเสียหายได้ไม่เกินความเสียหายในระดับต่ำ หากมีการละเมิดความปลอดภัยจะมีการใช้มาตรฐานการควบคุมที่สามารถคุ้มครองข้อมูลให้มีความปลอดภัยจากการโจมตีในรูปแบบต่างๆ ซึ่งอาจเพิ่มการรับรองมาตรการควบคุม	Public Cloud

ประเภทข้อมูล	คำอธิบาย	ประเภทบริการคลาวด์ที่แนะนำ
Protected Data	ข้อมูลที่มีความอ่อนไหวสูงหากเปิดเผยอาจก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ หรือเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง ซึ่งส่งผลต่อความมั่นคงของชาติ และ/หรือความสัมพันธ์ระหว่างประเทศ ความมั่นคง/เสถียรภาพทางการเงิน หรือขัดขวางความสามารถในการสืบสวนคดีอาชญากรรมที่ร้ายแรง หรือองค์กร ที่จำเป็นต้องมีมาตรการควบคุมที่เข้มงวด และมีการกำหนดการใช้เครือข่ายที่ปลอดภัยบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัย และมีการปฏิบัติอย่างเหมาะสม ซึ่งรวมถึงการใช้สถาปัตยกรรมแบบ ZERO - TRUST การเข้ารหัส และการปฏิบัติตามมาตรฐานความปลอดภัยทั้งในระดับชาติและระดับสากลอย่างเคร่งครัด	Public Cloud ที่มีมาตรการด้านความปลอดภัยสูง เช่น คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud หรือ VPC)
Highly Protected Data	ข้อมูลที่มีความอ่อนไหวเป็นพิเศษ หากเปิดเผยอาจเกิดความเสียหายอย่างร้ายแรงที่สุดต่อรัฐ ซึ่งส่งผลความมั่นคงของชาติหรือพันธมิตร และต้องการมาตรการควบคุมความปลอดภัยที่สูงมาก เพื่อป้องกันการละเมิดข้อมูลจากภัยคุกคามทั้งหมด โดยการใช้เครือข่ายบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัยสูง และมีการควบคุมความปลอดภัยอย่างเข้มงวด ซึ่งรวมถึงการใช้สถาปัตยกรรมแบบ ZERO-TRUST การเข้ารหัส และการปฏิบัติตามมาตรฐานความปลอดภัย ทั้ง ในระดับชาติและระดับสากลอย่างเคร่งครัด	Sovereign Cloud (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนดผู้ให้บริการ) หรือ Hybrid Cloud (เฉพาะบริการด้านความมั่นคงที่กำหนด)

หมายเหตุ

1. ข้อมูลที่ควรอยู่ในประเทศไทย หมายถึง ข้อมูลที่จัดเก็บอยู่ในสถานะพัก (Data-at-Rest) โดยไม่รวมถึงข้อมูลที่อยู่/ระหว่างการรับส่ง (Data-in-Transit) หรือการประมวล (Data Processing)
2. หากมีการทบทวนปรับเปลี่ยนระดับชั้นความลับของข้อมูล (Re-classification) หรือการยกเลิกชั้นความลับ (De-classification) ในกายหลัง ให้หน่วยงานสามารถปรับเปลี่ยนรูปแบบการใช้บริการคลาวด์ให้สอดคล้องกับสถานะความสำคัญใหม่ของข้อมูลได้
3. Sovereign Cloud (คลาวด์อธิปไตย) หมายถึง บริการคลาวด์ภายใต้การควบคุมโดยภาครัฐและดูแลโดยบุคลากรที่ได้รับอนุญาต และใช้สำหรับให้บริการกับหน่วยงานของรัฐเท่านั้น

2.3. บริการคลาวด์ (Cloud Service)

บริการคลาวด์ หมายถึงการให้บริการทรัพยากรด้านเทคโนโลยีสารสนเทศ เช่น คอมพิวเตอร์แม่ข่าย ที่เก็บข้อมูล ระบบประมวลผล ซอฟต์แวร์ และเครื่องมือพัฒนาระบบโดยผู้ใช้งานสามารถเข้าถึงบริการเหล่านี้ได้โดยไม่ต้องลงทุนในโครงสร้างพื้นฐานเอง บริการคลาวด์ช่วยเพิ่มความสะดวก ยืดหยุ่น และลดต้นทุนในการดำเนินธุรกิจ

2.3.1. คุณสมบัติหลักของบริการคลาวด์

1) ผู้ใช้งานสามารถเข้าถึงทรัพยากรหรือบริการได้อย่างสะดวก และมีความยืดหยุ่นและปรับขนาดได้ (Scalability) ทรัพยากรสามารถปรับเพิ่มหรือลดได้อย่างรวดเร็วตามความต้องการของผู้ใช้
2) การจัดการโดยผู้ให้บริการ (Managed by Providers) ผู้ให้บริการดูแลโครงสร้างพื้นฐานทั้งหมด เช่น การบำรุงรักษาคอมพิวเตอร์แม่ข่าย การสำรองข้อมูล และการรักษาความปลอดภัย
3) การทำงานร่วมกัน (Collaboration) ช่วยให้ทีมงานสามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพบนแพลตฟอร์มเดียวกัน

2.3.2.รูปแบบของบริการคลาวด์ (Types of Cloud Services)

บริการคลาวด์ของผู้ให้บริการมีด้วยกันหลายรูปแบบ โดยทั่วไปจะมี 3 รูปแบบหลัก ได้แก่ การให้บริการโครงสร้างพื้นฐาน (Infrastructure as a Service: IaaS) การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS) และการให้บริการซอฟต์แวร์ (Software as a Service: SaaS) ซึ่งลักษณะการใช้งานที่เหมาะสมของบริการแต่ละรูปแบบ [14]-[16] มีรายละเอียดตามตารางที่ 4 ทั้งนี้ ระบบของหน่วยงานที่ต้องการใช้คลาวด์อาจมีความจำเป็นต้องประยุกต์ใช้บริการคลาวด์ที่หลากหลาย เพื่อตอบสนองความต้องการได้ครบถ้วนตามวัตถุประสงค์

ตารางที่ 3 รูปแบบของบริการ Cloud (IaaS, PaaS และ SaaS)

รูปแบบบริการ	ลักษณะการใช้งานที่เหมาะสม	ตัวอย่างการใช้งานในหน่วยงานภาครัฐ	ข้อควรพิจารณา
การให้บริการโครงสร้างพื้นฐาน (Infrastructure as a Service: IaaS)	- ต้องการควบคุมโครงสร้างพื้นฐานอย่างเต็มรูปแบบ - มีระบบที่ต้องการปรับแต่งเฉพาะ	- ศูนย์ข้อมูลเสมือนที่ต้องการควบคุมระดับโครงสร้างพื้นฐาน - ระบบที่พัฒนาขึ้นเฉพาะไม่มีแพลตฟอร์ม หรือซอฟต์แวร์ของผู้ให้บริการคลาวด์	- ต้องมีบุคลากรที่เชี่ยวชาญการจัดการโครงสร้างพื้นฐาน - ความซับซ้อนในการจัดการระบบความปลอดภัยและการบำรุงรักษา
การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS)	- สำหรับการพัฒนาและปรับใช้แอปพลิเคชัน - ต้องการลดภาระการจัดการโครงสร้างพื้นฐาน - มีนักพัฒนาที่ต้องการดำเนินการเฉพาะการพัฒนา	- แพลตฟอร์มสำหรับพัฒนาแอปพลิเคชันที่สามารถปรับใช้และจัดการแอปพลิเคชันโดยไม่ต้องจัดการเกี่ยวกับโครงสร้างพื้นฐาน - ระบบบริหารจัดการฐานข้อมูล (DBMS)	- การย้ายแพลตฟอร์มไปยังผู้ให้บริการรายอื่นอาจซับซ้อน - ต้องทำความเข้าใจเครื่องมือและข้อจำกัดของแพลตฟอร์ม

รูปแบบบริการ	ลักษณะการใช้งานที่เหมาะสม	ตัวอย่างการใช้งานในหน่วยงานภาครัฐ	ข้อควรพิจารณา
การให้บริการซอฟต์แวร์ (Software as a Service: SaaS)	- สำหรับงานทั่วไปที่ต้องการโซลูชันสำเร็จรูป - ไม่ต้องการการปรับแต่งแอปพลิเคชัน - ลดค่าใช้จ่ายในการพัฒนาและบำรุงรักษาระบบ	- ใช้ระบบจัดการเอกสารและอีเมล เช่น Microsoft 365 หรือ Google Workspace - ระบบ CRM สำหรับการบริหารงานภายในหน่วยงาน - ระบบการอบรมออนไลน์ (e-Learning)	- ความยืดหยุ่นต่ำในการปรับแต่งระบบ - ข้อมูลอาจอยู่บนคลาวด์ของผู้ให้บริการ จึงต้องคำนึงถึงความปลอดภัยและข้อกฎหมาย

จากตารางที่ 3 ซึ่งอธิบายลักษณะของบริการคลาวด์ จะมีแนวทางการเลือกใช้งาน โดยสรุปดังนี้

1) เลือกใช้บริการโครงสร้างพื้นฐาน (Infrastructure as a Service: IaaS)
กรณีต้องการสร้างและควบคุมโครงสร้างพื้นฐาน เช่น เครื่องแม่ข่ายเสมือน (VM) หรือระบบเครือข่ายเสมือน
2) เลือกใช้บริการแพลตฟอร์ม (Platform as a Service: PaaS)
กรณีต้องการพัฒนาและปรับใช้แอปพลิเคชันเฉพาะ เช่น ระบบบริหารจัดการฐานข้อมูล
3) เลือกใช้บริการซอฟต์แวร์ (Software as a Service: SaaS)
กรณีต้องการใช้งานแอปพลิเคชันสำเร็จรูป เช่น อีเมล การจัดการเอกสาร หรือระบบ CRM

ทั้งนี้ควรใช้บริการมาตรฐานที่ผู้ให้บริการจัดเตรียมไว้ ไม่ควรดัดแปลงเป็นการเฉพาะ (Customize) เช่น การติดตั้งระบบบริหารจัดการข้อมูลเองในเครื่องแม่ข่ายเสมือน (VM) ที่อยู่นอกเหนือการให้บริการโดยผู้ให้บริการ เนื่องจากจะไม่ได้รับการดูแลโดยผู้ให้บริการ หรือการปรับปรุงเวอร์ชัน อย่างต่อเนื่อง โดยหน่วยงานควรพิจารณาเลือกรูปแบบบริการคลาวด์ (Cloud Services) ที่เหมาะสมกับงาน และเป็นบริการที่ผ่านหลักเกณฑ์ตามที่คณะกรรมการที่เกี่ยวข้องกำหนด

2.4. ความรับผิดชอบร่วม (Shared Responsibility)

บริการคลาวด์แต่ละรูปแบบมีการกำหนดความรับผิดชอบระหว่างผู้ให้บริการคลาวด์ (Cloud Service Provider - CSP) และผู้ใช้บริการ (Cloud Customer) [17] ซึ่งหน่วยงานจำเป็นต้องทำความเข้าใจและวางแผนการใช้งานโดยเฉพาะเมื่อจำเป็นต้องกำหนดบทบาทหน้าที่ และขั้นตอนการประสานงานทั้งสถานการณ์ปกติและเมื่อพบปัญหา ซึ่งโดยทั่วไปขอบเขตความรับผิดชอบจะกำหนดตามรูปแบบของบริการคลาวด์ (IaaS, PaaS, SaaS) ดังนี้

1) Infrastructure as a Service (IaaS)

- ผู้ให้บริการคลาวด์ (CSP)
  - การจัดการโครงสร้างพื้นฐาน เช่น ฮาร์ดแวร์, เครือข่าย และศูนย์ข้อมูล
  - การรักษาความปลอดภัยทางกายภาพของศูนย์ข้อมูล
  - ระบบเครือข่ายและฮาร์ดแวร์ที่พร้อมใช้งาน
- ผู้ใช้บริการ
  - การติดตั้งและจัดการระบบปฏิบัติการ (OS)
  - การกำหนดค่าความปลอดภัย เช่น Firewall, การเข้ารหัสข้อมูล
  - การจัดการข้อมูลและแอปพลิเคชันที่ใช้งาน
  - การควบคุมการเข้าถึงผู้ใช้งาน

2) Platform as a Service (PaaS)

- ผู้ให้บริการคลาวด์ (CSP)
  - การจัดการโครงสร้างพื้นฐาน
  - ระบบปฏิบัติการ, ฐานข้อมูล และเครื่องมือสำหรับการพัฒนาแอปพลิเคชัน
  - การอัปเดตและดูแลแพลตฟอร์มให้ทำงานได้เสถียร
- ผู้ใช้บริการ
  - การจัดการแอปพลิเคชันที่พัฒนาและปรับใช้บนแพลตฟอร์ม
  - การรักษาความปลอดภัยของข้อมูลที่บันทึกไว้
  - การควบคุมสิทธิ์การเข้าถึงและการจัดการผู้ใช้

3) Software as a Service (SaaS)

- ผู้ให้บริการคลาวด์ (CSP)
  - ดูแลทุกอย่างตั้งแต่โครงสร้างพื้นฐาน, ซอฟต์แวร์, การอัปเดตระบบ และความปลอดภัยของแอปพลิเคชัน
  - รับประกันความพร้อมใช้งานและความเสถียรของซอฟต์แวร์
- ผู้ใช้บริการ
  - การจัดการข้อมูลที่ป้อนเข้าไปในระบบ SaaS
  - การควบคุมการเข้าถึง เช่น การตั้งค่าผู้ใช้งานและรหัสผ่าน
  - การปฏิบัติตามนโยบายความปลอดภัย เช่น การกำหนดสิทธิ์ผู้ใช้

จากรายละเอียดข้างต้นสามารถสรุปตามหัวข้อความรับผิดชอบได้ตามตารางที่ 4 ที่อธิบายขอบเขตความรับผิดชอบระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการ โดยผู้ใช้บริการต้องจัดการความปลอดภัยของข้อมูล

แอปพลิเคชัน และการเข้าถึง ในขณะที่ผู้ให้บริการรับผิดชอบโครงสร้างพื้นฐานและการรักษาความปลอดภัยของระบบที่จัดหาให้ การทำความเข้าใจบทบาทและความรับผิดชอบนี้จะช่วยให้องค์กรใช้งานคลาวด์ได้อย่างปลอดภัยและมีประสิทธิภาพ โดยหน่วยงานควรมีการระบุอย่างชัดเจนในข้อตกลงการให้บริการ

ตารางที่ 4 ตารางเปรียบเทียบความรับผิดชอบในแต่ละรูปแบบการให้บริการคลาวด์

● ผู้ใช้บริการ ○ ผู้ให้บริการ

หัวข้อความรับผิดชอบ	On Premise	IaaS	PaaS	SaaS
การตั้งค่าแอปพลิเคชัน (Application configuration)	ผู้ใช้บริการ ●	ผู้ใช้บริการ ●	ผู้ใช้บริการ ●	ผู้ใช้บริการ ●
การพิสูจน์ตัวตนและเข้าถึงของผู้ใช้ (Identity & access controls)	ผู้ใช้บริการ ●	ผู้ใช้บริการ ●	ผู้ใช้บริการ และ ผู้ให้บริการ ● ○	ผู้ใช้บริการ และ ผู้ให้บริการ ● ○
ข้อมูลของแอปพลิเคชัน (Application data storage)	ผู้ใช้บริการ ●	ผู้ใช้บริการ ●	ผู้ใช้บริการ และ ผู้ให้บริการ ● ○	ผู้ให้บริการ ○
แอปพลิเคชัน (Application)	ผู้ใช้บริการ ●	ผู้ใช้บริการ ●	ผู้ใช้บริการ ●	ผู้ให้บริการ ○
ระบบปฏิบัติการ (Operating system)	ผู้ใช้บริการ ●	ผู้ใช้บริการ ●	ผู้ให้บริการ ○	ผู้ให้บริการ ○
การควบคุมระบบเครือข่าย (Network flow controls)	ผู้ใช้บริการ ●	ผู้ใช้บริการ และ ผู้ให้บริการ ● ○	ผู้ให้บริการ ○	ผู้ให้บริการ ○
โครงสร้างพื้นฐานของเครื่องแม่ข่าย (Host infrastructure)	ผู้ใช้บริการ ●	ผู้ให้บริการ ○	ผู้ให้บริการ ○	ผู้ให้บริการ ○
ความปลอดภัยทางกายภาพ (Physical security)	ผู้ใช้บริการ ●	ผู้ให้บริการ ○	ผู้ให้บริการ ○	ผู้ให้บริการ ○

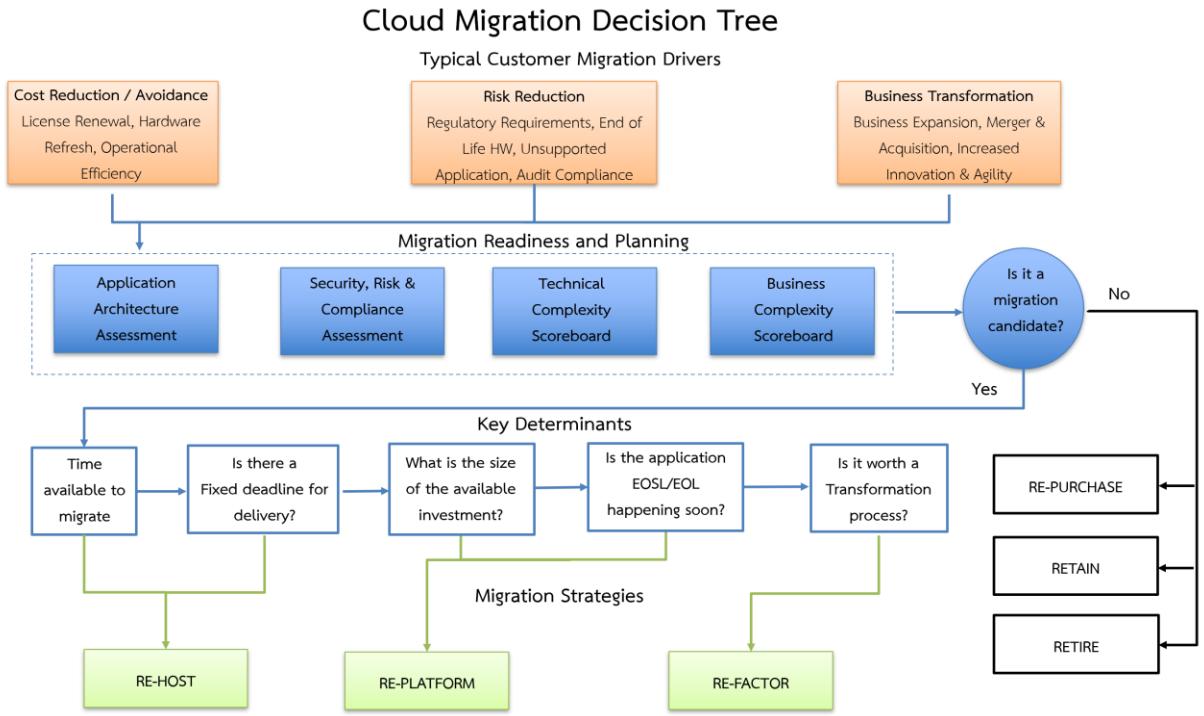
อ้างอิงจาก Cloud security shared responsibility model - NCSC.GOV.UK [17]

2.5. แนวทางการย้ายระบบขึ้นคลาวด์ (Migration)

เมื่อหน่วยงานต้องการย้ายระบบหรือบริการ ซึ่งเดิมจัดทำและใช้งานในรูปแบบเครื่องแม่ข่ายหรือรูปแบบอื่น ๆ ที่มีการติดตั้งภายในองค์กร (On-Premise) ไปสู่ระบบคลาวด์ของผู้ให้บริการจำเป็นต้องเลือกกลยุทธ์ การย้าย ดังตัวอย่างแผนภูมิการตัดสินใจเลือกกลยุทธ์ การย้ายระบบขึ้นคลาวด์ตามภาพที่ 3 ซึ่งโดยทั่วไปสามารถดำเนินการได้ตามแนวทางดังนี้ [18][19]

1) การประเมินความพร้อม (Assessment) ก่อนการย้ายข้อมูลและระบบไปยังระบบคลาวด์ควรประเมินความพร้อมในหลาย ๆ ด้าน ได้แก่
   - การประเมินความเสี่ยง: ระบุความเสี่ยงที่อาจเกิดขึ้นจากการย้ายข้อมูลหรือระบบ เช่น การสูญหายของข้อมูล, ความไม่เข้ากันของระบบ หรือความท้าทายในด้านความปลอดภัย
   - การประเมินค่าใช้จ่าย: คำนวณค่าใช้จ่ายในระยะยาวของการใช้งานระบบคลาวด์เทียบกับการคงระบบเดิมไว้
2) การเลือกรูปแบบการย้าย (Cloud Migration Models) เป็นการพิจารณาเลือกกลยุทธ์ การย้ายระบบไปใช้บริการคลาวด์ ซึ่งสามารถเลือกใช้ตามเงื่อนไข หรือความต้องการที่เหมาะสม เช่น
   - การย้ายระบบเดิมไปยังระบบคลาวด์ (Rehost) โดยไม่ทำการเปลี่ยนแปลงระบบ หรือโปรแกรม
   - การย้ายระบบเดิมพร้อมการปรับปรุงบางส่วนให้รองรับกับเทคโนโลยีคลาวด์ (Re-platform) อาจใช้เทคโนโลยีเทคโนโลยีคอนเทนเนอร์ (Containerization) และการจัดการคอนเทนเนอร์ (Container Orchestration) ซึ่งช่วยเสริม Portability ในการใช้งานบนคลาวด์ เช่น Docker, Kubernetes
   - การย้ายไปยังซอฟต์แวร์หรือบริการใหม่บนคลาวด์ (Repurchase) มักเป็นบริการซอฟต์แวร์ (SaaS)
   - การสร้างระบบใหม่เพื่อให้เหมาะสมกับคลาวด์โดยการออกแบบและพัฒนาใหม่ทั้งหมด (Refactor/Re-architect)
3) การย้ายข้อมูลและการทดสอบ (Migration and Testing) การย้ายข้อมูลไปยัง Public Cloud ควรทำทีละขั้นตอนและมีการทดสอบระบบหลังจากการย้าย ได้แก่
   - การย้ายข้อมูล (Data Migration) เป็นการย้ายแอปพลิเคชัน และข้อมูลของระบบ อาจใช้เครื่องมือที่เหมาะสมในการย้ายข้อมูล เช่น การใช้บริการของผู้ให้บริการคลาวด์ที่ช่วยในการย้ายข้อมูล
   - การทดสอบการทำงาน (System Testing) ควรทดสอบการทำงานของแอปพลิเคชันและข้อมูลหลังจากย้ายไปยังคลาวด์ เพื่อให้แน่ใจว่าระบบยังคงทำงานได้อย่างปกติ
4) การบริหารจัดการหลังการย้าย (Post-migration Management) หลังจากการย้ายเสร็จสิ้น ควรมีการบริหารจัดการและการตรวจสอบอย่างต่อเนื่อง:

- ตรวจสอบ และควบคุมต้นทุน ค่าใช้จ่ายของการใช้งานคลาวด์ให้สอดคล้องตามกรอบงบประมาณ
- ตรวจสอบ และปรับปรุงการทำงานของระบบที่ย้ายไปยังคลาวด์ให้มีประสิทธิภาพเสมอ



ภาพที่ 1 ตัวอย่างแผนภูมิการตัดสินใจเลือกกลยุทธ์การย้ายระบบขึ้นคลาวด์

(อ้างอิงจาก: https://www.leanix.net/en/wiki/tech-transformation/6rs-of-cloud-migration สืบค้นเมื่อวันที่ 13 ธันวาคม 2567)

2.6. แนวทางในการใช้นวัตกรรมใหม่

ผู้ให้บริการคลาวด์มักนำเสนอบริการที่เป็นนวัตกรรมใหม่นอกจากบริการโครงสร้างพื้นฐาน และเครื่องมือสำหรับการพัฒนา (Infrastructure & Development Tools) เช่น บริการเชิงธุรกิจและโปรแกรมประยุกต์ (Business & Application-Oriented Services) ที่มุ่งเน้นการสนับสนุนธุรกิจและการประยุกต์ใช้เทคโนโลยีที่สร้างมูลค่าเพิ่มให้กับองค์กร เพื่อเพิ่มประสิทธิภาพการทำงานโดยไม่ต้องจัดการโครงสร้างพื้นฐานเอง บริการเหล่านี้ส่วนใหญ่มีการคิดค่าใช้จ่ายตามการใช้งานจริง เช่น จำนวนทรัพยากรที่ใช้ หรือปริมาณข้อมูลที่ถูกประมวลผล ตัวอย่างเช่น

1) บริการปัญญาประดิษฐ์ (AI/ML Services) เป็นการนำเทคโนโลยี AI (Artificial Intelligence) ที่สามารถสร้างแบบจำลอง ฝึกสอน ให้ทำงานอย่างใดอย่างหนึ่ง มักเป็นบริการแบบแพลตฟอร์ม (PaaS) คิดค่าใช้จ่ายตามทรัพยากรที่ใช้ เช่น หน่วยประมวลผล (CPU, GPU) และเวลาในการฝึกสอนโมเดล เช่น Amazon Sage Maker หรือ Google AI Platform

2) บริการวิเคราะห์และประมวลผลข้อมูล (Analytics and Data Processing) เช่น ระบบฐานข้อมูลขนาดใหญ่ (Big Data) เช่น AWS EMR, Databricks Hadoop-as-a-Service หรือระบบธุรกิจอัจฉริยะ (Business Intelligence Tools) เช่น Power BI, Tableau Online

3) บริการ IoT (Internet of Things) การใช้คลาวด์ในการเชื่อมต่อและจัดการอุปกรณ์ IoT เช่น เซ็นเซอร์, เครื่องมือวัด, และอุปกรณ์ต่าง ๆ ที่เชื่อมต่อเพื่อติดตามข้อมูลหรือดำเนินการ คิดค่าใช้จ่ายตามจำนวนอุปกรณ์ที่เชื่อมต่อ, ปริมาณข้อมูลที่ส่งผ่าน และเวลาการประมวลผลที่ใช้ เช่น Azure IoT Hub, AWS IoT Core เป็นต้น

2.7. แนวทางการออกจากระบบคลาวด์ (Cloud Exit)

การออกจากระบบคลาวด์ (Cloud Exit) [20][21] คือ การวางแผนล่วงหน้าเพื่อให้การเปลี่ยนผ่านจากระบบคลาวด์ของผู้ให้บริการรายเดิมเป็นไปอย่างราบรื่น โดยมีเป้าหมายเพื่อป้องกันการเกิด “Vendor Lock-In” หรือการพึ่งพาผู้ให้บริการรายเดียวมากเกินไป ซึ่งอาจส่งผลต่อความต่อเนื่องของบริการหรือความปลอดภัยของข้อมูลเมื่อมีการเปลี่ยนแปลงระบบ ประกอบด้วยหลักการสำคัญเบื้องต้น ดังนี้

1) วางแผนตั้งแต่เริ่มต้น ระบุกลยุทธ์การออกจากระบบตั้งแต่ขั้นตอนการวางแผนการย้ายข้อมูลไปยังคลาวด์ โดยการกำหนดข้อกำหนดในสัญญากับผู้ให้บริการคลาวด์ เช่น เงื่อนไขหรือสัญญาที่ระบุการส่งคืนข้อมูล การกำหนดระยะเวลาการเก็บรักษาข้อมูล (Data Retention) การสนับสนุนหลังการยกเลิก ค่าใช้จ่ายที่เกี่ยวข้อง และการเคลื่อนย้ายข้อมูล (Data portability) หรือการที่ผู้ให้บริการคลาวด์กำหนดให้ลูกค้า/ผู้ใช้บริการคลาวด์ ในการถ่ายโอนข้อมูลหรือทรัพยากรดิจิทัล เป็นต้น

2) ป้องกันการพึ่งพาผู้ให้บริการรายเดียว ใช้เทคโนโลยีและมาตรฐานที่เป็นอิสระ เช่น การจัดเก็บข้อมูลในรูปแบบที่สามารถถ่ายโอนข้ามระบบได้ (Interoperability and Portability) ออกแบบสถาปัตยกรรมระบบให้ยืดหยุ่น เช่น ใช้ Multi-cloud หรือ Hybrid Cloud

3) กำหนดข้อมูลและบริการที่ต้องจัดการในกระบวนการออกจากระบบ ระบุข้อมูลและบริการที่ต้องถ่ายโอนหรือกู้คืน ประเมินผลกระทบของการเปลี่ยนแปลง เช่น ความเสี่ยงต่อข้อมูลที่สำคัญหรือการหยุดชะงักของบริการ จัดทำแผนรองรับการออกจากระบบ วางแผนรายละเอียดสำหรับการย้ายข้อมูลและระบบ เช่น การจัดการข้อมูลสำรอง การทดสอบการถ่ายโอนข้อมูล และการตรวจสอบความสมบูรณ์ของข้อมูล กำหนดลำดับความสำคัญของข้อมูล หรือระบบที่ต้องย้ายก่อน เป็นต้น

4) ความปลอดภัยและการปฏิบัติตามข้อกำหนด ดำเนินการให้มั่นใจว่า ข้อมูลถูกลบอย่างปลอดภัยจากระบบเดิม ปฏิบัติตามกฎหมายและข้อกำหนดด้านการคุ้มครองข้อมูล เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เป็นต้น

ทั้งนี้ ขั้นตอนการออกจากระบบคลาวด์โดยสังเขป มีดังนี้

1) การประเมินระบบ ตรวจสอบข้อมูลและระบบทั้งหมดที่อยู่ในคลาวด์ ทำแผนผังการเชื่อมโยงระบบและระบุจุดที่มีความเสี่ยง
2) การเตรียมการจัดเก็บข้อมูลสำรองในสถานที่ที่เชื่อถือได้ พัฒนาเครื่องมือและกระบวนการสำหรับการย้ายข้อมูล เช่น การใช้ API ที่สนับสนุนการถ่ายโอนข้อมูลอัตโนมัติ
3) การดำเนินการย้ายข้อมูลไปยังแพลตฟอร์มใหม่ หรือระบบสำรองทดสอบความสมบูรณ์และความถูกต้องของข้อมูลหลังการถ่ายโอน
4) การตรวจสอบการทำลายข้อมูลในระบบเดิมให้เรียบร้อย ทำรายงานผลการย้ายข้อมูล และข้อเสนอแนะสำหรับกระบวนการในอนาคต

3. แนวทางการประเมินราคา วางแผนงบประมาณ และบริหารการใช้บริการ

เพื่อให้การบริหารจัดการงบประมาณภาครัฐเกิดความคุ้มค่าสูงสุดและลดความซ้ำซ้อนในการลงทุนโครงสร้างพื้นฐาน หน่วยงานภาครัฐพึงพิจารณาเลือกใช้บริการคลาวด์จากหน่วยงานกลาง เช่น บริการจากระบบคลาวด์กลางภาครัฐ (GDCC) เป็นลำดับแรก (First Priority) อย่างไรก็ตาม หากหน่วยงานมีเหตุผลความจำเป็นทางด้านเทคนิคหรือภารกิจเฉพาะที่ต้องดำเนินการจัดหาบริการคลาวด์ด้วยตนเอง ให้ดำเนินการพิจารณาเปรียบเทียบความคุ้มค่าและปฏิบัติตามคำแนะนำดังต่อไปนี้

3.1.1. รูปแบบการคิดค่าบริการจากการใช้บริการคลาวด์

หลักการคิดค่าบริการของผู้ให้บริการคลาวด์โดยทั่วไปมี 2 รูปแบบหลัก ได้แก่ การคิดค่าบริการตามปริมาณการใช้งานจริง (Pay-per-use) และการคิดค่าบริการแบบสมาชิก (Subscription) ทั้งนี้ ผู้ให้บริการคลาวด์อาจมีการประยุกต์ ผสมผสาน และนำเสนอในชื่อเรียกที่ต่างกัน เช่น ค่าบริการแบบจองทรัพยากรล่วงหน้า (Pay-per-Reservation) หรือค่าบริการแบบผสมผสาน (Hybrid Pricing) โดยรูปแบบการคิดค่าบริการคลาวด์ [6]-[13] มีความแตกต่างดังรายละเอียดตามตารางที่ 5

ตารางที่ 5 รูปแบบการคิดค่าบริการจากการใช้บริการคลาวด์

การคิดค่าบริการ	ข้อดี	ข้อเสีย	ลักษณะการใช้งานที่เหมาะสม	ข้อควรพิจารณา
การคิดค่าบริการตามปริมาณการใช้งานจริง (Pay-per-use)	- ประหยัดต้นทุนผู้ใช้งานจ่ายเฉพาะสิ่งที่ใช้จริง - ความยืดหยุ่นรองรับการปรับขนาดทรัพยากรได้อย่างรวดเร็วตามความต้องการ - สามารถตรวจสอบการใช้งานและต้นทุนได้อย่างละเอียด	- ต้นทุนผันแปร หากไม่มีการบริหารจัดการที่ดี ค่าใช้จ่ายอาจเพิ่มขึ้นเกินกว่าที่คาดการณ์ไว้ - ความซับซ้อนในการวางแผนงบประมาณ เนื่องจากค่าใช้จ่ายขึ้นอยู่กับการใช้งานจริง ทำให้การคาดการณ์งบประมาณยากขึ้น	- ธุรกิจที่ต้องการควบคุมต้นทุนในช่วงเริ่มต้น - องค์กรขนาดใหญ่: ใช้สำหรับแผนกหรือโครงการที่ต้องการทรัพยากรคลาวด์เพิ่มขึ้นชั่วคราว	- Pay-per-use เป็นโมเดลการคิดค่าบริการที่ช่วยลดต้นทุนและเพิ่มความยืดหยุ่นในการใช้งานทรัพยากรคลาวด์อย่างไรก็ตาม องค์กรต้องมีการบริหารจัดการการใช้งานอย่างเหมาะสมเพื่อควบคุมต้นทุนและป้องกันค่าใช้จ่ายที่ไม่คาดคิด
การคิดค่าบริการแบบสมาชิก (Fixed Price Contract หรือ Subscription)	- การจัดการงบประมาณ (Budgeting) ช่วยให้สามารถวางแผนและคาดการณ์งบประมาณได้อย่างแม่นยำ - ประสิทธิภาพการใช้งาน (Efficiency) เหมาะสำหรับงานที่มีการใช้งานทรัพยากรคงที่ เช่น การประมวลผลที่ต่อเนื่อง - ความมั่นคงในการให้บริการผู้ให้บริการคลาวด์อาจ	- ความยืดหยุ่นต่ำ หากการใช้งานลดลงหรือเปลี่ยนแปลง ผู้ใช้งานอาจต้องจ่ายเงินสำหรับทรัพยากรที่ไม่ได้ใช้ - ข้อผูกมัดระยะยาว ผู้ใช้งานต้องทำสัญญาล่วงหน้าซึ่งอาจเป็นระยะยาว เช่น 1-3 ปี - ความเสี่ยงด้านการคาดการณ์ผิดพลาด หากการใช้งานไม่ถึงปริมาณที่ตกลงไว้ ผู้ใช้อาจเสีย	- เมื่อทราบปริมาณการใช้งานล่วงหน้า เช่น เครื่องแม่ข่าย ที่ต้องรันอย่างต่อเนื่อง หรือทรัพยากรสำหรับแอปพลิเคชันที่มีผู้ใช้งานคงที่	- ควรประเมินความต้องการและปริมาณการใช้งานอย่างรอบคอบก่อนทำสัญญา เพื่อลดความเสี่ยงจากการใช้งานที่ต่ำกว่าปริมาณที่ตกลงไว้

การคิดค่าบริการ	ข้อดี	ข้อเสีย	ลักษณะการใช้งานที่เหมาะสม	ข้อควรพิจารณา
	รับประกันทรัพยากรที่ถูกจองไว้ให้พร้อมใช้งานเสมอ	ค่าใช้จ่ายโดยเปล่าประโยชน์ - ไม่เหมาะสำหรับความต้องการที่ไม่แน่นอน สำหรับองค์กรที่มีการใช้งานทรัพยากรแบบผันผวนหรือไม่สามารถคาดการณ์ได้		

ทั้งนี้ กรณีที่บริการคลาวด์มีรูปแบบการคิดค่าบริการตามปริมาณการใช้งานจริง (Pay-per-use) ตามจริงให้ผู้ใช้บริการเลือกได้ ต้องพิจารณาเลือกรูปแบบการคิดค่าบริการตามปริมาณการใช้งานจริง (Pay-per-use) เป็นลำดับแรก

3.1.2.การวิเคราะห์ความต้องการทรัพยากร

การวิเคราะห์ความต้องการทรัพยากรและโครงสร้างราคาของคลาวด์ ซึ่งเกี่ยวข้องกับแนวทางการเลือกประเภทคลาวด์ (Cloud Deployment Models) ประเภทของบริการคลาวด์ (Types of Cloud Services) แนวทางการย้ายระบบขึ้นคลาวด์ (Migration) และอื่น ๆ ตาม แนวทางการเลือกใช้บริการคลาวด์ของหน่วยงานภาครัฐ ในข้อ 3 รวมทั้งความต้องการทรัพยากรที่เหมาะสมกับความต้องการของข้อมูลและระบบ [22]

3.1.3. การวิเคราะห์ต้นทุนทางตรงและทางอ้อม [23][24]

ต้นทุนทางตรง (Direct Costs) คือ ค่าบริการซึ่งเกิดจากการใช้บริการคลาวด์ที่สามารถระบุได้โดยตรงและชัดเจน ซึ่งมีหลายกลุ่ม ได้แก่

1) กลุ่มบริการสำหรับการประมวลผล (Compute) เช่น การประเมินค่าบริการการใช้ CPU, RAM, และอื่น ๆ ที่ใช้ในการประมวลผลข้อมูล
2) กลุ่มบริการสำหรับจัดเก็บข้อมูล (Storage) เช่น การประเมินค่าบริการเก็บข้อมูลตามปริมาณข้อมูลที่จัดเก็บและเรียกใช้
3) ค่ากลุ่มบริการสำหรับการเชื่อมต่อเครือข่าย (Networking) เช่น ค่าบริการการรับส่งข้อมูลภายในและนอกระบบคลาวด์ เป็นต้น
4) กลุ่มบริการสำหรับจัดการฐานข้อมูล (Database)
5) กลุ่มบริการสำหรับวิเคราะห์ข้อมูล (Analytics)
6) กลุ่มบริการเครื่องมือสำหรับผู้พัฒนาระบบ (Developer & Management Tools)

7) กลุ่มบริการเครื่องมือความมั่นคงปลอดภัย (Security)
8) กลุ่มบริการการสนับสนุน (Support Plan)
9) กลุ่มบริการอื่น ๆ ที่สามารถระบุได้โดยตรงและชัดเจน

ต้นทุนทางอ้อม หรือ ต้นทุนแฝง (Indirect Costs) คือ ค่าบริการที่เกิดขึ้นจากการดำเนินงานที่ไม่สามารถระบุได้ทันที เช่น ค่าบริการย้ายระบบ (Migration) ค่าบริการติดตามการใช้งาน (Monitoring) ค่าบริการเข้ารหัสข้อมูล หรือค่าบริการอื่นที่อาจเกิดขึ้นซึ่งไม่รวมในบริการสนับสนุน (Support Plan) เป็นต้น

3.1.4. การใช้เครื่องมือประเมินค่าบริการ (Pricing Calculator) ที่มีมาตรฐานการจัดทำเพดานงบประมาณ (Not-To-Exceed Ceiling) [11]

การประเมินราคาสำหรับการจัดซื้อคลาวด์ภาครัฐต้องมีความรัดกุม และครอบคลุมทุกมิติ เพื่อให้มั่นใจว่าบริการที่ได้มีความเหมาะสมและตรงกับความต้องการของหน่วยงาน รวมทั้ง สอดคล้องกับข้อกำหนดด้านความปลอดภัยและงบประมาณ ดังนั้น เพื่อให้การประเมินราคาของการจัดซื้อจัดจ้างระบบคลาวด์ภาครัฐมีประสิทธิภาพ การนำใช้เทคโนโลยี หรือเครื่องมือต่าง ๆ ก็เป็นตัวช่วยที่ควรนำมาพิจารณาด้วยเช่นกัน ซึ่งการใช้เครื่องมือประเมินค่าบริการ (Pricing Calculator) คือ เครื่องมือที่ช่วยผู้ใช้งานสามารถคำนวณต้นทุนหรือค่าใช้จ่ายของบริการคลาวด์ตามปริมาณการใช้งานและการตั้งค่าทรัพยากรที่ต้องการ เครื่องมือนี้มักถูกพัฒนาโดยผู้ให้บริการคลาวด์ เพื่อให้ผู้ใช้งานสามารถประมาณการค่าใช้จ่ายและวางแผนงบประมาณได้อย่างมีประสิทธิภาพ โดยคุณสมบัติของเครื่องมือประเมินค่าบริการ (Pricing Calculator) โดยทั่วไป มีดังนี้

1) การปรับแต่งทรัพยากร (Resource Customization) ผู้ใช้สามารถเลือกทรัพยากร เช่น คอมพิวเตอร์แม่ข่าย (VM), ที่เก็บข้อมูล (Storage), และปริมาณข้อมูลที่รับส่ง (Bandwidth) เพื่อคำนวณค่าใช้จ่ายเฉพาะเจาะจง
2) การเปรียบเทียบตัวเลือก (Cost Comparison) ช่วยให้ผู้รับบริการเปรียบเทียบต้นทุนระหว่างการตั้งค่าต่าง ๆ เพื่อหาทางเลือกที่เหมาะสมที่สุด
3) การแสดงผลที่โปร่งใส (Transparent Breakdown) แสดงรายละเอียดค่าใช้จ่ายในแต่ละส่วน เช่น ค่าประมวลผล, ค่าเก็บข้อมูล, และค่าบริการเสริม
4) รองรับการวางแผนงบประมาณ (Budget Planning) ช่วยผู้ใช้วางแผนการใช้งบประมาณในระยะยาว เช่น การคำนวณค่าใช้จ่ายรายเดือนหรือรายปี

3.1.5. การบริหารและตรวจสอบค่าใช้จ่าย

การบริหารจัดการและตรวจสอบค่าใช้จ่ายสำหรับบริการคลาวด์ เพื่อให้สอดคล้องกับการตั้งงบประมาณแบบยืดหยุ่น (Flexible Budgeting) ของหน่วยงานเป็นสิ่งสำคัญเมื่อต้องการควบคุมต้นทุนและเพิ่มประสิทธิภาพในการใช้งานคลาวด์อย่างเหมาะสม โดยแนวทางและเครื่องมือที่ผู้ให้บริการจัดเตรียมไว้ มีตัวอย่างดังนี้

1) การติดตามการใช้งานแบบเรียลไทม์ (Real-time Monitoring)

2) เปิดใช้งานการแจ้งเตือนเมื่อค่าใช้จ่ายหรือการใช้งานใกล้ถึงขีดจำกัด
3) ใช้ Billing Alerts เพื่อรับการแจ้งเตือนผ่านอีเมลหรือแอปพลิเคชัน
4) การแยกต้นทุนตาม โครงการ หรือแผนก ช่วยให้ทราบว่าแต่ละส่วนใช้งบประมาณเท่าไร
5) การวิเคราะห์ค่าใช้จ่าย (Cost Analysis) วิเคราะห์ต้นทุนที่เกิดขึ้น เพื่อระบุทรัพยากรที่ใช้เกินความจำเป็น เช่น คอมพิวเตอร์แม่ข่ายที่ทำงานนอกเวลาหรือไม่ได้ใช้งานเต็มประสิทธิภาพ

3.2. การบริหารจัดการค่าใช้จ่ายระบบคลาวด์ (Financial Operations, Fin-ops)

แนวทางในการบริหารจัดการค่าใช้จ่ายระบบคลาวด์ [25-26] สามารถใช้เป็นแนวทางเพื่อเพิ่มประสิทธิภาพทางการเงินให้สอดคล้องกับการใช้งานคลาวด์ โดยเน้นการทำงานร่วมกันระหว่างฝ่ายเทคนิค และฝ่ายการเงิน เพื่อให้การตัดสินใจด้านการใช้งบประมาณมีประสิทธิภาพและสอดคล้องกับความเป็นจริงมากยิ่งขึ้น โดยมีหลักการสำคัญ ได้แก่

- การมองเห็นและความโปร่งใสในค่าใช้จ่าย (Visibility and Transparency) ทุกฝ่ายสามารถมองเห็นค่าใช้จ่ายของการใช้คลาวด์ได้อย่างโปร่งใส โดยใช้เครื่องมือรายงานหรือแดชบอร์ด (Dashboard) ที่แสดงค่าใช้จ่ายแบบเรียลไทม์ ซึ่งเป็นประโยชน์ต่อการตัดสินใจและวางแผนควบคุมงบประมาณได้ดียิ่งขึ้น เนื่องจากการทราบข้อมูลค่าใช้จ่ายช่วยให้หน่วยงานสามารถระบุแหล่งที่มาของค่าใช้จ่ายที่ไม่จำเป็นได้ทัน
- การทำงานร่วมกัน (Collaboration) เป็นกระบวนการที่เกี่ยวข้องกับฝ่ายสารสนเทศรับผิดชอบในการจัดการทรัพยากรคลาวด์ ฝ่ายการเงิน ดูแลเรื่องงบประมาณและการวางแผนการใช้จ่าย ดังนั้น การสร้างความเข้าใจร่วมกันจึงเป็นสิ่งสำคัญที่จะช่วยให้ให้องค์กรสามารถบรรลุเป้าหมายร่วมกันได้ เพื่อให้สามารถจัดสรรทรัพยากรได้อย่างเหมาะสม
- การเพิ่มประสิทธิภาพ (Optimization)
    - การลดการใช้ทรัพยากรที่ไม่ได้ใช้งาน เช่น ปิดคอมพิวเตอร์แม่ข่ายที่ไม่ได้ใช้งานในช่วงเวลาที่ไม่จำเป็น
    - การเปลี่ยนไปใช้บริการต้นทุนต่ำกว่า เช่น การเลือกใช้ Spot Instances หรือ Reserved Instances ที่เหมาะสมกับการทำงาน
    - การปรับโครงสร้างสถาปัตยกรรม เช่น การออกแบบระบบให้รองรับ Auto-scaling เพื่อลดต้นทุนในช่วงที่มีความต้องการน้อย
    - การวัดผลและการวางกลยุทธ์ (Measure and Plan)
        - การติดตามผลการใช้งาน โดยใช้ Key Performance Indicators (KPIs) เพื่อวัดความสำเร็จ เช่น การลดต้นทุนหรือเพิ่มประสิทธิภาพการทำงาน
        - การวางแผนล่วงหน้า คือ การวิเคราะห์ข้อมูลเพื่อคาดการณ์แนวโน้มการใช้งานในอนาคตและจัดสรรทรัพยากรให้เหมาะสม

3.3. การประเมินความคุ้มค่าบริการคลาวด์ (Total Cost of Ownership, TCO)

การประเมินความคุ้มค่าบริการคลาวด์ [27] คือ แนวคิดการประเมินค่าใช้จ่ายทั้งหมดที่เกี่ยวข้องการจัดหา การดำเนินงาน และการกำจัดสินทรัพย์หรือระบบตลอดอายุการใช้งาน แนวคิดนี้ช่วยให้องค์กรสามารถประเมินต้นทุนที่แท้จริงของการลงทุน โดยไม่พิจารณาเฉพาะราคาซื้อเริ่มต้นเท่านั้น แต่เป็นการพิจารณาต้นทุนทั้งหมดตั้งแต่การจัดซื้อจนถึงการกำจัด และเป็นวิธีการคิดเกี่ยวกับต้นทุน ประเมินความเหมาะสม วัดและเปรียบเทียบต้นทุนของตัวเลือกซอฟต์แวร์ทั้งหมด ใช้ได้ทั้งกับซอฟต์แวร์โอเพ่นซอร์ส และซอฟต์แวร์ที่มีลิขสิทธิ์

3.4. แนวทางการจัดซื้อจัดจ้างระบบคลาวด์ สำหรับภาครัฐ

การจัดซื้อจัดจ้างระบบคลาวด์สำหรับภาครัฐ ต้องมีความโปร่งใส คุ้มค่า และสอดคล้องกับกฎหมายและนโยบายของรัฐบาล รวมถึงการบริหารพัสดุภาครัฐ เพื่อให้หน่วยงานปฏิบัติได้อย่างถูกต้อง โดยมีขั้นตอน วิธีการเป็นไปตามตามคณะกรรมการที่เกี่ยวข้อง หรือหน่วยงานที่ได้รับมอบหมายหน้าที่ ประกาศกำหนด โดยหน่วยงานควรมีการกำหนดระดับการให้บริการให้เหมาะสมตามประเภท และรูปแบบของบริการคลาวด์ในข้อตกลง หรือสัญญาใช้บริการให้ชัดเจน

3.5. แนวทางในด้านความปลอดภัย

แนวทางในด้านความปลอดภัยการใช้คลาวด์ หน่วยงานสามารถดำเนินการโดยอ้างอิงตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 [28] ซึ่งโดยสรุปเนื้อหาแบ่งออกเป็นแนวทางด้านความปลอดภัยของผู้ให้บริการคลาวด์ (Cloud Service Provider) และผู้ใช้บริการคลาวด์ (Cloud Service Consumer) ซึ่งมีความรับผิดชอบร่วม (Shared Responsibility) โดยมีจุดมุ่งหมายเพื่อปกป้องข้อมูล ระบบและโครงสร้างพื้นฐานของคลาวด์อย่างครบวงจรโดยแบ่งเป็น

1) การกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์
2) การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

3.5.1. การกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

กระบวนการที่มุ่งเน้นการจัดการความเสี่ยงและการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบที่ใช้งานบนคลาวด์ (Cloud Security) เพื่อให้มั่นใจว่าการจัดเก็บ ประมวลผล และถ่ายโอนข้อมูลบนคลาวด์มีความปลอดภัยตามมาตรฐานสากล โดยได้มีการพิจารณา ดำเนินการในรายละเอียดดังต่อไปนี้

1) นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
2) โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ

3) การปฏิบัติตามกฎ ระเบียบ และข้อบังคับ

3.5.2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์ (Cloud Infrastructure Security and Operation)

กระบวนการปกป้องโครงสร้างพื้นฐานของระบบคลาวด์จากภัยคุกคามที่อาจเกิดขึ้นและการจัดการความเสี่ยงที่เกี่ยวข้องกับข้อมูลที่ถูกจัดเก็บและประมวลผลบนคลาวด์ จำเป็นต้องมีแนวทางที่ชัดเจนสำหรับการจัดการความมั่นคงปลอดภัยในหลาย ๆ ด้าน เช่น การควบคุมการเข้าถึง การรักษาความปลอดภัยทางกายภาพ การจัดการกับความเสี่ยงด้านเทคโนโลยี และการประเมินความเสี่ยงที่เกิดจากผู้ให้บริการคลาวด์ โดยได้มีการพิจารณาในรายละเอียดดังต่อไปนี้

1) การปฏิบัติการและรักษาความมั่นคงปลอดภัยด้านองค์กร
2) การควบคุมทางกายภาพและสิ่งแวดล้อม
3) การรักษาความมั่นคงปลอดภัยไซเบอร์
4) การควบคุมด้านเทคโนโลยี

ทั้งนี้ โดยปกติแล้วหน่วยงานควรมีการดำเนินการเรื่อง การจัดการความมั่นคงปลอดภัยข้อมูล (Information Security) ให้สอดคล้องกับมาตรฐานที่เกี่ยวข้อง ให้ครอบคลุมการบริหารจัดการความเสี่ยง การป้องกันภัยคุกคาม และการสร้างความมั่นใจในระบบข้อมูลขององค์กร ซึ่งครอบคลุมการดูแลทรัพย์สินด้านข้อมูล (Information Assets) ขององค์กรจากการเข้าถึงโดยไม่ได้รับอนุญาต การถูกทำลาย หรือการสูญเสีย เน้นการควบคุมพื้นที่และอุปกรณ์ทางกายภาพ รวมถึง สภาพแวดล้อมที่อาจมีผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล

หน่วยงานภาครัฐในฐานะผู้ใช้บริการคลาวด์ควรศึกษารายละเอียดของมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 และปรับปรุงบริการให้สอดคล้องตามข้อกำหนด

3.5.3. มาตรการด้านความปลอดภัยสำหรับการใช้งานคลาวด์สาธารณะ (Public Cloud)

เนื่องจากคลาวด์สาธารณะ (Public Cloud) เป็นบริการคลาวด์ที่เปิดให้บริการกับผู้ใช้บริการทั่วไป โดยที่ทรัพยากรทั้งหมดอยู่ภายใต้การควบคุมของผู้ให้บริการคลาวด์ เพื่อเพิ่มมาตรการควบคุมดูแลความปลอดภัยที่สูงขึ้นหน่วยงานสามารถเลือกใช้งานคลาวด์สาธารณะที่มีการสร้างสภาวะแวดล้อมที่เสมือนเป็นเครือข่ายส่วนตัว หรือที่เรียกว่า Virtual Private Cloud (VPC) ซึ่งให้บริการโดยผู้ให้บริการที่มีความพร้อม เพื่อเพิ่มระดับความมั่นคงปลอดภัย และการควบคุม (Security Measure) โดย VPC จะทำการแบ่งแยกทรัพยากรคลาวด์ของผู้ใช้บริการออกจากผู้ใช้รายอื่นบนโครงสร้างพื้นฐานทางกายภาพเดียวกัน ทำให้หน่วยงานสามารถควบคุมสภาพแวดล้อมเครือข่ายของตนเองได้อย่างสมบูรณ์ ดังนั้น การออกแบบและใช้งาน VPC อย่างเหมาะสมจึงเป็นแนวทางที่สำคัญสำหรับหน่วยงานที่ต้องการยกระดับการควบคุมและความมั่นคงปลอดภัยในการใช้บริการคลาวด์สาธารณะให้ใกล้เคียงกับเครือข่ายส่วนตัวของหน่วยงาน

3.6. การสร้างความตระหนักและการฝึกอบรมเรื่องคลาวด์ (Training)

การสร้างความตระหนักและการฝึกอบรมความมั่นคงปลอดภัยด้านคลาวด์ ถือเป็นการบริหารจัดการความมั่นคงปลอดภัยข้อมูล (Information Security Management System: ISMS) โดยมุ่งเน้นให้พนักงานและบุคลากรในองค์กรมีความตระหนักในความมั่นคงปลอดภัยข้อมูล และมีบทบาทที่ชัดเจนในการป้องกันภัยคุกคามทางไซเบอร์และความเสี่ยงด้านข้อมูล

1) ผู้ใช้บริการคลาวด์ ต้องเพิ่มโปรแกรมสร้างความตระหนักรู้ การศึกษา และการ ฝึกอบรมสำหรับผู้จัดการธุรกิจบริการคลาวด์ ผู้ดูแล ระบบบริการคลาวด์ ผู้ประกอบบริการคลาวด์ และ ผู้ใช้บริการคลาวด์ รวมถึง พนักงานและผู้รับจ้างที่เกี่ยวข้อง
2) ต้องจัดให้มีโปรแกรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษา และการฝึกอบรมเกี่ยวกับบริการคลาวด์แก่ผู้บริหารและผู้จัดการที่กำกับดูแล รวมถึงหน่วยงานธุรกิจ (Business Units)

3.7. แนวทางการจัดการระบบสำรองข้อมูลและกู้คืนข้อมูลบนคลาวด์

แนวทางการจัดการระบบสำรองข้อมูลและกู้คืนข้อมูลบนคลาวด์ จะเน้นการดำเนินการด้านการสำรองข้อมูล (Backup) และ การกู้คืนข้อมูล (Restore) เนื่องจากการบริหารจัดการข้อมูลบนคลาวด์เป็นความรับผิดชอบร่วมกันระหว่าง หน่วยงานเจ้าของข้อมูล และ ผู้ให้บริการคลาวด์ ดังนั้นการสำรองข้อมูล เป็นกิจกรรมที่ต้องมีข้อตกลงร่วมกัน โดยจัดทำตามแนวทางดังนี้

3.7.1.พิจารณาปัจจัยเกี่ยวข้องที่สำคัญ

1) ขอบเขตของการสำรองข้อมูล [22]
   - ระบุข้อมูล ระบบ และแอปพลิเคชันที่ต้องสำรอง
   - จัดหมวดหมู่ข้อมูลตามความสำคัญและความถี่ที่ข้อมูลเปลี่ยนแปลง
2) ประเภทของการสำรองข้อมูล [23][24]
   - Full Back up: การสำรองข้อมูลทั้งหมด (ใช้เวลานานแต่ครอบคลุม)
   - Incremental Backup: สำรองเฉพาะข้อมูลที่เปลี่ยนแปลงตั้งแต่สำรองครั้งล่าสุด (รวดเร็ว แต่ต้องอ้างอิงข้อมูลสำรองก่อนหน้า)
   - Differential Backup: สำรองข้อมูลที่เปลี่ยนแปลงตั้งแต่การสำรองข้อมูลเต็มครั้งล่าสุด (สมดุลระหว่างเวลาและพื้นที่จัดเก็บ)
3) ความถี่ในการสำรองข้อมูล
   - กำหนดตาม Recovery Point Objective (RPO): ระดับการยอมรับข้อมูลที่อาจสูญหายได้
   - ใช้ระบบอัตโนมัติสำหรับการสำรองข้อมูล เช่น รายชั่วโมงหรือรายวัน
4) ตำแหน่งจัดเก็บข้อมูลสำรอง

- ใช้ระบบจัดเก็บข้อมูลสำรองแบบหลายภูมิภาค (Multi-region) เพื่อรองรับการกู้คืนในกรณีฉุกเฉิน
- เลือกระหว่าง Cold Storage (ราคาต่ำสำหรับเก็บข้อมูลระยะยาว) และ Hot Storage (ราคาสูงสำหรับการเข้าถึงข้อมูลได้รวดเร็ว)

5) มาตรการความปลอดภัย
   - เข้ารหัสข้อมูลทั้งระหว่างการส่งผ่านและขณะจัดเก็บ
   - ใช้ระบบควบคุมการเข้าถึงที่ปลอดภัย เช่น Multi-Factor Authentication (MFA)

6) การปฏิบัติตามข้อกำหนด
   - ปฏิบัติตามกฎหมายด้านการคุ้มครองข้อมูล เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, GDPR เป็นต้น
   - ตรวจสอบว่าการจัดเก็บข้อมูลตรงตามข้อกำหนดด้านการตั้งถิ่นฐานของข้อมูลในอุตสาหกรรมที่สำคัญ

3.7.2. แนวปฏิบัติสำหรับการสำรองข้อมูล

1) กำหนดนโยบายชัดเจน
   - ระบุ Recovery Point Objective หรือ RPO (ความถี่ในการสำรองข้อมูล) และ Recovery Time Objective หรือ RTO (ระยะเวลาที่ต้องใช้ในการกู้คืนข้อมูล)

2) เลือกเครื่องมือสำรองข้อมูล
   - เครื่องมือของผู้ให้บริการคลาวด์ เช่น AWS Backup, Azure Backup, Google Cloud Backup
   - เครื่องมือบุคคลที่สาม เช่น Veeam, Acronis, Rubrik

3) ทดสอบการสำรองข้อมูล
   - ทดสอบการกู้คืนข้อมูลเป็นระยะเพื่อยืนยันความสมบูรณ์ของข้อมูลสำรอง
   - ทดสอบหลายสถานการณ์ เช่น การกู้คืนบางส่วนและการกู้คืนทั้งหมด

4) การจัดการเวอร์ชันของข้อมูล
   - เก็บเวอร์ชันสำรองหลายชุดเพื่อลดความเสี่ยงจากการลบข้อมูลโดยไม่ตั้งใจหรือการโจมตีด้วย Ransomware

5) ระบบอัตโนมัติ
   - ใช้ระบบอัตโนมัติเพื่อลดข้อผิดพลาดและเพิ่มความต่อเนื่องในการสำรองข้อมูล

3.7.3. แนวทางสำหรับการกู้คืนข้อมูล

1) วางแผนสถานการณ์การกู้คืน
   - การกู้คืนทั้งหมด: สำหรับกรณีที่ระบบทั้งหมดเสียหาย
   - การกู้คืนบางส่วน: สำหรับการกู้คืนไฟล์ โฟลเดอร์ หรือแอปพลิเคชันเฉพาะ
   - การกู้คืนข้ามภูมิภาคหรือไฮบริด: กู้คืนข้อมูลจากภูมิภาคหรือผู้ให้บริการคลาวด์อื่น

2) กระบวนการกู้คืน
   - ระบุแหล่งข้อมูลสำรอง ค้นหาข้อมูลสำรองโดยใช้ Metadata หรือ Index
   - ตรวจสอบความสมบูรณ์ของข้อมูล ยืนยันว่าไฟล์สำรองสมบูรณ์และไม่มีความเสียหาย
   - ลำดับความสำคัญในการกู้คืน เริ่มจากระบบที่มีความสำคัญต่อธุรกิจมากที่สุด
   - ติดตามและตรวจสอบ ตรวจสอบกระบวนการกู้คืนเพื่อป้องกันข้อผิดพลาด โดยทดสอบ ระบบหลังการกู้คืนเพื่อให้แน่ใจว่าทำงานได้ตามปกติ
3) เครื่องมือและเทคโนโลยีที่แนะนำ
   - โซลูชันของผู้ให้บริการคลาวด์ เช่น AWS Backup, S3 Versioning, EBS Snapshots
   - Azure Backup, Site Recovery Google Cloud
   - โซลูชันผู้พัฒนาอื่น ๆ เช่น Veeam Commvault และ Druva

บรรณานุกรม

[1] พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562. (2562, 22 พฤษภาคม). *ราชกิจจานุเบกษา*, *136*(67 ก), 57-66.

[2] International Organization for Standardization. (2023). *ISO/IEC 22123-1: Information technology — Cloud computing — Part 1: Vocabulary*. International Organization for Standardization. https://www.iso.org/standard/82758.html

[3] Compatibl. (2024). *How to choose the best cloud deployment model for your business*. CompatibL Technologies LLC. https://www.compatibl.com/insights/how-to-choose-the-best-cloud-deployment-model/

[4] Network Interview. (2022). *Public vs private vs hybrid vs community clouds - Types of clouds*. Network Interview. https://networkinterview.com/public-vs-private-vs-hybrid-vs-community-clouds/

[5] Haris, M., & Khan, R. Z. (2018). A systematic review on cloud computing. *International Journal of Computer Sciences and Engineering, 6*(11), 632-639. https://doi.org/10.26438/ijcse/v6i11.632639

[6] Amazon Web Services. (n.d.). *On-demand instances (Pay-per-use) and reserved instances (Committed subscription)*. Amazon Web Services. https://aws.amazon.com/pricing/

[7] Google Cloud Platform. (n.d.). *Committed use discounts and calculation*. Google Cloud Platform. https://cloud.google.com/pricing/

[8] Microsoft Azure. (n.d.). *Pay-as-you-go and reserved instances on Azure*. Microsoft. https://azure.microsoft.com/en-us/pricing/

[9] IBM Cloud. (n.d.). *Pay-as-you-go and subscription-based*. IBM. https://www.ibm.com/cloud/pricing

[10] Oracle Cloud. (n.d.). *Simple and competitive by default*. Oracle. https://www.oracle.com/cloud/pricing/

[11] HashiCorp. (n.d.). *Terraform: Pay-per-use by infrastructure as code*. HashiCorp. https://developer.hashicorp.com/terraform/docs

[12] Gartner. (n.d.). *An analysis report on the advantages and disadvantages of Pay-per-use and Subscription payment models*. Gartner. https://www.gartner.com/peer-insights/home

[13] FinOps Foundation. (n.d.). *Managing and planning cloud expenses in various models*. FinOps Foundation. https://www.finops.org/

[14] National Institute of Standards and Technology. (2011). *Cloud computing service models* (NIST Special Publication 800-145). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[15] Gov.UK. (n.d.). *Using cloud services*. Government Digital Service. https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector

[16] Amazon Web Services. (n.d.). *AWS cloud service models*. Amazon Web Services. https://aws.amazon.com/types-of-cloud-computing/

[17] National Cyber Security Centre. (n.d.). *Cloud security shared responsibility model*. National Cyber Security Centre. https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model

[18] Heptabit. (2024). *How to find the right strategy with cloud migration decision tree*. Heptabit. https://www.heptabit.com/blog/cloud-migration/how-to-find-the-right-strategy-with-cloud-migration-decision-tree

[19] LeanIX. (2024). *6Rs of cloud migration*. LeanIX. https://www.leanix.net/en/wiki/tech-transformation/6rs-of-cloud-migration

[20] Government Digital Service. (n.d.). *Managing technical lock-in in the cloud*. Government Digital Service. https://www.gov.uk/guidance/managing-technical-lock-in-in-the-cloud

[21] Government Digital Service. (n.d.). *Cloud guide for the public sector*. Government Digital Service. https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector#foreword

[22] UK Government. (n.d.). *Government security classifications*. GOV.UK. https://www.gov.uk/government/publications/government-security-classifications

[23] UK Government. (n.d.). *Government adopts 'Cloud First' policy for public sector IT*. GOV.UK. https://www.gov.uk/government/news/government-adopts-cloud-first-policy-for-public-sector-it

[24] Tech Monitor. (n.d.). *Cloud first: UK government urges departments to use public cloud*. Tech Monitor. https://www.techmonitor.ai/digital-economy/government-computing/government-cloud-first-policy-public-sector-guidance-cddo

[25] Amazon Web Services. (n.d.). *FinOps*. Amazon Web Services. https://aws.amazon.com/blogs/

[26] Microsoft. (n.d.). *FinOps*. Microsoft. https://learn.microsoft.com/en-us/azure/cost-management-billing

[27] Government Digital Service. (n.d.). *Total cost of ownership*. Government Digital Service. https://assets.publishing.service.gov.uk/

[28] คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2567). (2567, 11 พฤศจิกายน) *มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์*. ราชกิจจานุเบกษา, 141 (ตอนพิเศษ 306 ง), 32-33.