

สพร./CDV

กรกฎาคม 2568

ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน

มาตรฐานฉบับสมบูรณ์จะมีประกาศในราชกิจจานุเบกษา

ร่าง

มาตรฐานรัฐบาลดิจิทัล

ว่าด้วย[กรณานิเทศน์ชื่อมาตรฐานฯ ภาษาไทย]

สำหรับเสนอคณะกรรมการจัดทำร่างมาตรฐาน

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

ว่าด้วยแนวทางการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก GOVERNMENT CLOUD USAGE GUIDELINE

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักนายกรัฐมนตรี

มาตรฐานรัฐบาลดิจิทัล
ว่าด้วยแนวทางการใช้คลาวด์ตามนโยบาย
การใช้คลาวด์เป็นหลัก

มรด. 9-2 : 2568

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

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์
ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

ที่ปรึกษา

นางไอรดา เหลืองวิไล

รองผู้อำนวยการ

รักษาการแทนผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์

จุฬาลงกรณ์มหาวิทยาลัย

รองประธานกรรมการ

นายอาศิส อัญญะโพธิ์

ผู้ช่วยผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

กรรมการ

นายมารุต บุณรัช

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นางสาวชนิษฐ์ ผาทอง

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

นายเกียรติชัย ชุ่มมงคล

สำนักบริหารการทะเบียน กรมการปกครอง

นางสาวดารารัตน์ โฆษิตพิพัฒน์

สำนักงานคณะกรรมการพัฒนาระบบราชการ

นางสาวพรพิมล อุ่นไพร

สำนักงานคณะกรรมการกฤษฎีกา

นายสันติ สิทธิเลิศพิศาล

สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม

นายวีระ วีระกุล

สภาคิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย

รองศาสตราจารย์เกริก ภิรมย์โสภา

จุฬาลงกรณ์มหาวิทยาลัย

รองศาสตราจารย์ธีรณี อจลากุล

สถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ

ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

กรรมการและเลขานุการ

นางสาวอรุณา เกตุพรหม

ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะกรรมการเทคนิคด้านมาตรฐานกระบวนการและการทำงานทางดิจิทัล ที่ปรึกษา

นางไอรดา เหลืองวิไล

รองผู้อำนวยการ

รักษาการแทนผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์

จุฬาลงกรณ์มหาวิทยาลัย

นายอาศิส อัญญะโพธิ์

ผู้ช่วยผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ประธานคณะกรรมการ

รองศาสตราจารย์เกริก ภริมย์โสภา

จุฬาลงกรณ์มหาวิทยาลัย

รองประธานคณะกรรมการ

ผู้ช่วยศาสตราจารย์กุลวดี ศรีพานิชกุลชัย

จุฬาลงกรณ์มหาวิทยาลัย

คณะกรรมการ

นายสิทธิโชค ชัยปัญญา

กรมการปกครอง

นางวัลภา นุตโร

กรมบัญชีกลาง

นางสาวพนิดา เกื้อประจง

กรมพัฒนาธุรกิจการค้า

นายกำชัย จัดตานนท์

กรมศุลกากร

นางจันทร์เจริญ แบร์โรวส์

กรมสรรพากร

นางสาวดารารัตน์ โฆษิตพิพัฒน์

สำนักงานคณะกรรมการพัฒนาระบบราชการ

พ.ต.ต.วรกร ทองสุข

สำนักงานตรวจคนเข้าเมือง

พ.ต.อ.ณัทฤกษ์ พรหมจันทร์

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ

นายชาติ วรกุลพิพัฒน์

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นางสาวชนิษฐ์ ผาทอง

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

นายเมธวิน กิติคุณ

สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย

นายคฑาทู ปาระมี

สมาคมไทยบล็อกเชน

นายอชิบดี ลิ้มสัมพันธ์สันติ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

นายอุสรวิ วิจารณ์

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะกรรมการและเลขานุการ

นางสาวอุไรฉา เกตุพรหม

ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยเลขานุการ

นายธีรวัฒน์ ไรจน์ไพฑูรย์

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

**วิเคราะห์และจัดทำมาตรฐานรัฐบาลดิจิทัล
ว่าด้วยแนวทางการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก**

นางสาวอุรชฎา เกตุพรหม
นายธีรวัฒน์ โรจนไพฑูรย์
นางสาวพิมพ์ชนก แจ็กภู
นายณัฐพงศ์ บุปผะศิริ
นายธนต์ธ์ โอสมพรนุวัฒน์

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)



มาตรฐานรัฐบาลดิจิทัลฉบับนี้ จัดทำขึ้นเพื่อเป็นข้อเสนอแนะสำหรับหน่วยงานของรัฐตามแนวทางการใช้คลาวด์ เพื่อให้หน่วยงานของรัฐสามารถนำแนวทางที่นำเสนอไปประยุกต์ใช้เพื่อเพิ่มประสิทธิภาพของบริการและบริหารจัดการทรัพยากร โดยใช้เทคโนโลยีคลาวด์ (Cloud Technology) และจัดให้มีการพิจารณาพิจารณาปรับปรุงความคิดเห็นเป็นการทั่วไป และนำข้อมูล ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง มาปรับปรุงมาตรฐานฉบับนี้จนมีความสมบูรณ์ครบถ้วน นอกจากนี้ ยังได้รับการพิจารณากลั่นกรองจากคณะทำงานเทคนิคด้านมาตรฐานกระบวนการและการดำเนินงานทางดิจิทัล และผ่านการพิจารณาเห็นชอบจากคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 เพื่อให้ข้อเสนอแนะเกี่ยวกับมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วน และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

แนวทางการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก เวอร์ชัน 1.0 ฉบับนี้จัดทำโดยฝ่ายมาตรฐานดิจิทัลภาครัฐ 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

มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก จัดทำขึ้นเพื่อสนับสนุนแนวทางการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ตามที่คณะรัฐมนตรีได้แถลงนโยบาย “Go Cloud First” เมื่อวันที่ 11 กันยายน พ.ศ. 2566 ต่อรัฐสภา ซึ่งได้มีการแต่งตั้งคณะกรรมการและคณะอนุกรรมการที่เกี่ยวข้อง โดยมีการกำหนดกรอบแนวทางในการบริหารจัดการคลาวด์ภาครัฐเพื่อใช้เป็นแนวทางการขับเคลื่อนตามนโยบาย และจัดทำรายละเอียดเป็นแนวทางในด้านที่เกี่ยวข้อง จำนวน 3 แนวทาง คือ แนวทางการใช้คลาวด์ แนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ และแนวทางการกำหนดมาตรฐานบริการผู้ให้บริการคลาวด์

มาตรฐานรัฐบาลดิจิทัลฉบับนี้ จัดทำขึ้นเพื่อเป็นข้อเสนอแนะสำหรับหน่วยงานของรัฐตามแนวทางการใช้คลาวด์ เพื่อให้หน่วยงานของรัฐสามารถนำแนวทางที่นำเสนอไปประยุกต์ใช้เพื่อเพิ่มประสิทธิภาพของบริการและบริหารจัดการทรัพยากร โดยใช้เทคโนโลยีคลาวด์ (Cloud Technology) ซึ่งเป็นเครื่องมือสำคัญที่ช่วยสนับสนุนการดำเนินงานของหน่วยงานภาครัฐให้มีความยืดหยุ่น ประหยัดค่าใช้จ่าย และเสริมสร้างศักยภาพในการพัฒนาระบบบริการและโครงสร้างพื้นฐานด้านเทคโนโลยี โดยเนื้อหาในเอกสารจะครอบคลุมแนวทางการเลือกใช้บริการคลาวด์ของหน่วยงานภาครัฐ แนวทางการประเมินราคา แนวทางในด้านความปลอดภัย และด้านอื่นที่เกี่ยวข้อง

สารบัญ

1. บทนำ	1
2. แนวทางการเลือกใช้บริการคลาวด์ของหน่วยงานภาครัฐ	5
3. แนวทางการประเมินราคาและวางแผนงบประมาณ	15
4. แนวทางในด้านความปลอดภัย และด้านอื่นที่เกี่ยวข้อง	20
บรรณานุกรม	24

ร่าง

สารบัญตาราง

ตารางที่ 1 ประเภทของคลาวด์	5
ตารางที่ 2 รูปแบบการคิดค่าบริการจากการใช้บริการคลาวด์.....	7
ตารางที่ 3 รูปแบบของบริการ Cloud (IaaS, PaaS และ SaaS).....	9
ตารางที่ 4 ตารางเปรียบเทียบความรับผิดชอบในแต่ละรูปแบบการให้บริการคลาวด์	11



สารบัญภาพ

ภาพที่ 1 ตัวอย่างแผนภูมิการตัดสินใจเลือกกลยุทธ์ การย้ายระบบขึ้นคลาวด์ อ้างอิงตาม 6Rs..... 13

ร่าง

มาตรฐานรัฐบาลดิจิทัล

ว่าด้วยแนวทางการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก

1. บทนำ

1.1. หลักการและความจำเป็น

ด้วยนโยบายของคณะรัฐมนตรีที่แถลงต่อรัฐสภา เมื่อวันที่ 11 กันยายน 2566 เรื่องการวางรากฐานและโครงสร้างพื้นฐานใหม่เพื่อเพิ่มประสิทธิภาพการให้บริการประชาชนด้วยการนำเทคโนโลยีและระบบดิจิทัลมาใช้อย่างเต็มรูปแบบ ปรับปรุงการทำงานของภาครัฐให้เป็นรัฐบาลดิจิทัลทำให้ประชาชนสามารถรับบริการจากรัฐได้สะดวกมากยิ่งขึ้น รวมทั้งเพิ่มความมั่นคงปลอดภัยด้วยนโยบาย “Go Cloud First” ซึ่งต่อมาเมื่อวันที่ 25 มิถุนายน 2567 คณะรัฐมนตรีมีมติเห็นชอบตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเสนอ ให้แต่งตั้งคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) เพื่อให้การจัดทำแนวทางการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก และให้คณะกรรมการพัฒนารัฐบาลดิจิทัลเป็นผู้ดำเนินการกำหนดรายละเอียดที่เกี่ยวข้องกับนโยบายการใช้คลาวด์ การออกประกาศเพื่อกำหนดหลักเกณฑ์และมาตรฐานประสานงานกับหน่วยงานที่เกี่ยวข้อง พัฒนาระบบบริหารจัดการความต้องการและจัดหาคลาวด์ กำกับดูแลสร้างระบบนิเวศและจัดซื้อจัดจ้าง ตามกรอบนโยบายที่ได้รับอนุมัติจากคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ รวมทั้งกรอบกฎหมายของหน่วยงานรัฐที่เกี่ยวข้องต่อไป ซึ่งคณะกรรมการพัฒนารัฐบาลดิจิทัล ได้มอบหมายให้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) จัดทำแนวทางการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก เพื่อเป็นข้อเสนอแนะสำหรับหน่วยงานภาครัฐตามนโยบายรัฐบาลด้านการใช้คลาวด์เป็นหลัก ที่สนับสนุนการใช้คลาวด์เพื่อเพิ่มประสิทธิภาพการให้บริการประชาชนอย่างมั่นคงปลอดภัย และช่วยประหยัดค่าใช้จ่ายทางด้านโครงสร้างพื้นฐาน และการบำรุงรักษา ซึ่งทำให้เกิดการใช้งบประมาณอย่างมีประสิทธิภาพ ซึ่งมีแนวทางการดำเนินการที่สำคัญ 4 องค์ประกอบ ได้แก่

- 1) การบริหารจัดการความต้องการใช้คลาวด์ (Demand)
- 2) การบริหารจัดการให้มีบริการคลาวด์อย่างเพียงพอ (Supply)
- 3) การบริหารจัดการการใช้งานคลาวด์ของหน่วยงานภาครัฐ (Government Cloud Management)
- 4) ระบบนิเวศการใช้บริการคลาวด์ เพื่อเชื่อมโยงผู้ให้บริการ (Demand) และผู้ให้บริการ (Supply)

ทั้งนี้ เพื่อสนับสนุนหน่วยงานของรัฐในฐานะผู้ให้บริการคลาวด์ ให้มีแนวทางดำเนินการที่สอดคล้องกับนโยบายการใช้คลาวด์เป็นหลักด้านการบริหารจัดการความต้องการใช้คลาวด์ (Demand) จำเป็นต้องจัดทำแนวทางที่ครอบคลุมการเลือกใช้บริการคลาวด์ การประเมินราคา การย้ายไปสู่ระบบคลาวด์ ความมั่นคงปลอดภัย และแนวทางด้านที่เกี่ยวข้อง ภายใต้ มาตรฐานรัฐบาลดิจิทัล

1.2. วัตถุประสงค์

การจัดทำแนวทางการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก เพื่อเป็นข้อเสนอแนะและกรอบแนวทางให้หน่วยงานสามารถนำไปปฏิบัติใช้ให้สอดคล้องและเหมาะสมกับบริการของหน่วยงาน ตามนโยบายการใช้คลาวด์เป็นหลัก

- 1) สนับสนุนการเปลี่ยนผ่านสู่รัฐบาลดิจิทัล (Digital Government Transformation) เพื่อเพิ่มประสิทธิภาพและความทันสมัยของการให้บริการภาครัฐ ส่งเสริมการใช้เทคโนโลยีดิจิทัลในการบริหารจัดการและบริการแก่ประชาชน
- 2) เพิ่มความคุ้มค่าในการใช้งบประมาณ (Cost Efficiency) ลดค่าใช้จ่ายที่เกี่ยวข้องกับการจัดซื้อและบำรุงรักษาโครงสร้างพื้นฐานทางเทคโนโลยี ใช้ทรัพยากรคลาวด์ร่วมกันระหว่างหน่วยงาน เพื่อประหยัดต้นทุน

1.3. ขอบข่าย

มาตรฐานรัฐบาลดิจิทัลฉบับนี้แนะนำเสนอแนวทางการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลักสำหรับหน่วยงานของรัฐ สอดคล้องตามกรอบแนวทางการจัดการระบบคลาวด์ภาครัฐตามนโยบายการใช้คลาวด์เป็นหลัก เพื่อเพิ่มประสิทธิภาพการให้บริการประชาชนอย่างมั่นคงปลอดภัย ประหยัดค่าใช้จ่ายทางด้านโครงสร้างพื้นฐาน และการบำรุงรักษา สร้างความสมดุลระหว่างความปลอดภัย และความคุ้มค่าในการดำเนินงานของภาครัฐ โดยเนื้อหาครอบคลุมแนวทางการปรับเปลี่ยนระบบงาน หรือบริการภาครัฐ ไปสู่ระบบคลาวด์ ซึ่งขอบเขตของเนื้อหาโดยสรุปมีดังนี้

- 1) การเลือกประเภทของคลาวด์ (Cloud Deployment Model) การวิเคราะห์จัดประเภทข้อมูล และเลือกประเภทของคลาวด์ที่มีให้บริการได้อย่างเหมาะสม ได้แก่
 - คลาวด์สาธารณะ (Public Cloud)
 - คลาวด์ส่วนตัว (Private Cloud)
 - คลาวด์แบบกลุ่ม (Community Cloud)
 - คลาวด์แบบผสม (Hybrid 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) การของบประมาณ การเสนอโครงการเพื่อขอรับงบประมาณตามกลไกการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก โดยแยกค่าใช้จ่ายด้านคลาวด์ที่ชัดเจน
- 6) การจัดซื้อจัดจ้าง ปฏิบัติตามระเบียบการจัดซื้อจัดจ้างของภาครัฐ เช่น การประกวดราคา (e-Bidding) หรือการคัดเลือกผู้ให้บริการที่มีมาตรฐาน เพื่อให้ได้บริการที่มีมาตรฐานและปลอดภัย
- 7) การบริหารต้นทุน และการตรวจสอบ ปรับปรุงการใช้งานคลาวด์ แนวคิดการบริหารต้นทุนอย่างมีประสิทธิภาพ โดยติดตาม ตรวจสอบ และปรับปรุงการใช้งานคลาวด์อย่างต่อเนื่อง
- 8) 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 ได้อ้างอิงจากมาตรฐานสากล [2] ประกอบด้วยคำศัพท์ ดังต่อไปนี้

การประมวลผลแบบคลาวด์ (Cloud Computing) หมายความว่า รูปแบบการประมวลผลที่สามารถเข้าถึงทรัพยากรที่ใช้ร่วมกัน¹ ได้อย่างยืดหยุ่น โดยมีการจัดเตรียมทรัพยากร (Self-service Provisioning²) และการบริหารจัดการด้วยตนเองตามความต้องการ (On-demand)

บริการคลาวด์ (Cloud Service) หมายความว่า การนำเสนอความสามารถของการประมวลผลแบบคลาวด์รูปแบบใดแบบหนึ่งหรือมากกว่านั้นให้กับผู้ใช้บริการ โดยสามารถเรียกใช้งานผ่านอินเทอร์เน็ตที่กำหนดไว้

คลาวด์สาธารณะ (Public Cloud) หมายความว่า บริการคลาวด์ที่เปิดให้บริการกับผู้ให้บริการทั่วไป โดยทรัพยากรทั้งหมดอยู่ภายใต้การควบคุมของผู้ให้บริการคลาวด์

¹ ตัวอย่างของทรัพยากร ได้แก่ คอมพิวเตอร์แม่ข่าย ระบบปฏิบัติการ เครือข่าย ซอฟต์แวร์ แอปพลิเคชัน และอุปกรณ์จัดเก็บข้อมูล

² การจัดสรรด้วยตนเอง (Self-service provisioning) หมายถึง การจัดสรรทรัพยากรที่บริการคลาวด์มอบให้ ซึ่งดำเนินการโดยผู้ใช้บริการคลาวด์ ผ่านระบบอัตโนมัติ

คลาวด์ส่วนตัว (Private Cloud) หมายความว่า บริการคลาวด์ที่ใช้งานโดยผู้ให้บริการเพียงรายเดียว โดยทรัพยากรทั้งหมดอยู่ภายใต้การควบคุมของผู้ให้บริการรายนั้น

คลาวด์แบบกลุ่ม (Community Cloud) หมายความว่า บริการคลาวด์ที่ใช้เฉพาะกลุ่มผู้ให้บริการที่มีความต้องการใช้งานและมีความเกี่ยวข้องกัน ซึ่งทรัพยากรถูกควบคุมโดยสมาชิกในกลุ่ม

คลาวด์แบบผสม (Hybrid Cloud) หมายความว่า การใช้คลาวด์ที่รวมการใช้งานคลาวด์ส่วนตัว (Private Cloud) และคลาวด์สาธารณะ (Public Cloud) เข้าด้วยกัน

การให้บริการโครงสร้างพื้นฐาน (Infrastructure as a Service: IaaS) หมายความว่า หมวดหมู่ของบริการคลาวด์ที่ผู้ให้บริการสามารถกำหนดการใช้งานหน่วยประมวลผล พื้นที่จัดเก็บข้อมูล และเครือข่ายได้เองตามความต้องการ

การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS) หมายความว่า หมวดหมู่ของบริการคลาวด์ที่ผู้ให้บริการสามารถติดตั้ง บริหารจัดการ หรือเรียกใช้แอปพลิเคชันที่ผู้ให้บริการกำหนดเองด้วยคำสั่งภาษา หรือสภาพแวดล้อมที่ผู้ให้บริการรองรับ

การให้บริการซอฟต์แวร์ (Software as a Service: SaaS) หมายความว่า หมวดหมู่ของบริการคลาวด์ที่ผู้ให้บริการสามารถใช้งานซอฟต์แวร์ที่ผู้ให้บริการจัดเตรียมไว้ได้

1.5. กฎหมายและแนวทางที่เกี่ยวข้อง

- 1) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
- 1) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- 2) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการให้บริการคลาวด์ พ.ศ. 2562
- 3) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566
- 4) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

2. แนวทางการเลือกใช้บริการคลาวด์ของหน่วยงานภาครัฐ

2.1. ประเภทของคลาวด์ (Cloud Deployment Models)

ประเภทของคลาวด์ตามลักษณะการนำไปใช้ (Cloud Deployment Models) โดยทั่วไปมี 4 ประเภท ได้แก่ คลาวด์สาธารณะ คลาวด์ส่วนตัว คลาวด์แบบผสม และคลาวด์แบบกลุ่มซึ่งมีข้อดีและข้อเสียแตกต่างกันดังรายละเอียดตามตารางที่ 1 [3]

ตารางที่ 1 ประเภทของคลาวด์

หัวข้อ	คลาวด์สาธารณะ (Public Cloud)	คลาวด์ส่วนตัว (Private Cloud)	คลาวด์แบบผสม (Hybrid Cloud)	คลาวด์แบบกลุ่ม (Community Cloud)
ข้อดี	- ไม่มีต้นทุนการลงทุนในโครงสร้างพื้นฐาน - มีค่าใช้จ่ายด้านการดูแลบำรุงรักษาน้อย - ปรับขยายได้อย่างไม่จำกัด	- สามารถปรับแต่งบริการคลาวด์ได้ทั้งหมด (Fully customizable) - โครงสร้างพื้นฐาน และข้อมูลทั้งหมดอยู่ในการควบคุมของหน่วยงานเอง - มีความปลอดภัยสูง (เมื่อดำเนินการได้ตามมาตรฐานที่เกี่ยวข้อง)	- ความยืดหยุ่นด้านการจัดการข้อมูลและความจุ - ความสามารถในการฟื้นตัวจากการหยุดชะงักของบริการ	- สามารถแบ่งภาระค่าใช้จ่ายร่วมกันในกลุ่ม - สามารถปรับแต่งบริการคลาวด์ได้ตามความต้องการของกลุ่ม
ข้อเสีย	- ขาดความสามารถในการปรับแต่งตามต้องการ - ผู้ให้บริการต้องได้รับการกำกับดูแลที่ดี - ความล่าช้าจากอินเทอร์เน็ตที่อาจเกิดขึ้น	- มีต้นทุนโครงสร้างพื้นฐานสูงเมื่อเทียบกับประเภทอื่น - การใช้งานทรัพยากรอาจไม่เต็มประสิทธิภาพ - มีค่าใช้จ่ายด้านการดูแลบำรุงรักษาสูงเมื่อเทียบกับประเภทอื่น	- อาจมีปัญหาด้านความเข้ากันได้ของระบบคลาวด์ - มีความซับซ้อนในการบริหารจัดการ	- การปรับขยายขนาดทรัพยากรอาจมีข้อจำกัดเนื่องจากการต้องบริหารจัดการร่วมกัน

จากสรุปข้อดีและข้อเสียตามประเภทของคลาวด์ หน่วยงานสามารถพิจารณาเลือกใช้บริการคลาวด์ได้เหมาะสมกับการนำไปใช้ ตามปัจจัยที่เกี่ยวข้อง [4-5] ได้แก่

- 1) ความปลอดภัย (Security) ที่มีระดับการป้องกันข้อมูลและระบบจากการโจมตีทางไซเบอร์หรือการเข้าถึงที่ไม่ได้รับอนุญาตที่เหมาะสม
- 2) ความสามารถในการปรับขยาย (Scalability) และ ความยืดหยุ่น (Flexibility) ที่มีความสามารถในการเพิ่มหรือลดทรัพยากรตามความต้องการโดยผู้ให้บริการ หรือการเพิ่มหรือลดทรัพยากรแบบอัตโนมัติ (Auto Scaling) ที่สามารถตอบสนองการให้บริการของหน่วยงานได้
- 3) ค่าใช้จ่าย (Cost) ที่เป็นต้นทุนที่เกี่ยวข้องกับการใช้บริการคลาวด์ รวมถึง ค่าใช้จ่ายเริ่มต้นและค่าใช้จ่ายรายเดือนที่เหมาะสมกับงบประมาณ
- 4) การบริหารจัดการ (Management) ที่มีระดับความซับซ้อนในการตั้งค่าบำรุงรักษา และจัดการระบบคลาวด์เหมาะสมต่อการดำเนินการของหน่วยงาน

2.2. แนวทางการเลือกประเภทคลาวด์ (Cloud Deployment Models)

แนวทางการเลือกประเภทคลาวด์ เป็นจุดเริ่มต้นที่ต้องตัดสินใจในการดำเนินการปรับเปลี่ยนระบบหรือบริการของหน่วยงานไปสู่ระบบคลาวด์ โดยทั่วไปพิจารณาจากปัจจัยด้านความต้องการของหน่วยงาน ความปลอดภัย (Security) ความสามารถในการปรับขยาย (Scalability) ความยืดหยุ่น (Flexibility) ค่าใช้จ่าย (Cost) และการบริหารจัดการ (Management Complexity) ทั้งนี้ ตามนโยบาย Go Cloud First ของรัฐบาลมุ่งเน้นให้หน่วยงานของรัฐพิจารณาเลือกใช้คลาวด์สาธารณะ (Public Cloud) เป็นลำดับแรก สำหรับโครงการใหม่ประจำปีงบประมาณ 2569 หรือโครงการที่มีแผนจะปรับปรุง เพื่อลดภาระของหน่วยงาน ทั้งด้านต้นทุนของโครงสร้างพื้นฐานค่าใช้จ่ายในการบำรุงรักษา และการจัดหาบุคลากรที่มีความเชี่ยวชาญ โดยจำเป็นต้องมีการวิเคราะห์จำแนกประเภทข้อมูล รวมทั้งการกำหนดถิ่นที่อยู่ของข้อมูล ตามมาตรฐานฯ ว่าด้วยแนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก ซึ่งมีการจำแนกประเภทข้อมูลเพื่อใช้คลาวด์ (Cloud Data Classification) ซึ่งมีความจำเป็นต้องเลือกประเภทคลาวด์ให้เหมาะกับระดับชั้นและประเภทข้อมูล โดยการเลือกประเภทคลาวด์ตามกรอบแนวทางการบริหารจัดการระบบคลาวด์ภาครัฐตามนโยบายการใช้คลาวด์เป็นหลักมีแนวทางดังนี้

กรณีให้บริการเป็นข้อมูลสาธารณะ (Public) ข้อมูลใช้ภายใน (Internal) และข้อมูลลับ (Confidential) สามารถเลือกใช้คลาวด์สาธารณะ (Public Cloud) โดยพิจารณาร่วมกับปัจจัยด้านอื่น เช่น ค่าใช้จ่าย (Cost) ความปลอดภัย (Security) การปรับขยาย (Scalability) และความยืดหยุ่น (Flexibility) การเริ่มต้นใช้งาน (Ease of 1st time use) และการควบคุมข้อมูล (Data Control) ทั้งนี้ข้อมูลแต่ละระดับควรมีมาตรการควบคุมความมั่นคงปลอดภัย และการคุ้มครองข้อมูลที่เหมาะสมกับระดับความเสี่ยง

กรณีที่เป็นข้อมูลลับมาก (Secret) ขึ้นไป ให้พิจารณาใช้คลาวด์แบบกลุ่ม (Community Cloud) ซึ่งให้บริการโดยองค์กร หรือบริษัทที่รัฐบาลเป็นเจ้าของทั้งหมดหรือส่วนใหญ่ หรือมีอำนาจควบคุมอย่างมีนัยสำคัญ หรือคลาวด์อธิปไตย (Sovereign Cloud) ซึ่งออกแบบมาเพื่อให้มั่นใจว่า ข้อมูลทั้งหมด (รวมถึง แอปพลิเคชัน และข้อมูลที่อยู่ระหว่างการส่งผ่านเครือข่าย) ถูกจัดเก็บ ประมวลผล และบริหารจัดการอยู่ภายในประเทศหรือภูมิภาคที่กำหนด และเป็นไปตามกฎหมายและข้อบังคับด้านอธิปไตยทางข้อมูล (Data Sovereignty) ของประเทศอย่างเคร่งครัด เพื่อประโยชน์ในการควบคุมและคุ้มครองข้อมูลสำคัญของรัฐ และหากมีเหตุผลความจำเป็นสามารถพิจารณาการใช้คลาวด์ส่วนตัว (Private Cloud) หรือคลาวด์แบบผสม (Hybrid Cloud) ซึ่งมีการแยกข้อมูลที่ต้องได้รับความคุ้มครองสูงสุดไว้ในคลาวด์ส่วนตัว (Private Cloud) โดยหน่วยงานสามารถเสนอเหตุผลความจำเป็นตามกลไกนโยบายการใช้คลาวด์เป็นหลักตามที่คณะกรรมการที่เกี่ยวข้องกำหนด

ทั้งนี้ หน่วยงานควรมีการพิจารณากฎหมายเฉพาะที่เกี่ยวข้องกับข้อมูลที่ต้องการเพิ่มเติม และเลือกใช้ผู้ให้บริการคลาวด์ ที่มีระดับของผู้ให้บริการคลาวด์ที่มีมาตรฐาน (CSP Tier) เหมาะสมกับระดับชั้นของข้อมูล โดยศึกษาเพิ่มเติมได้จาก มาตรฐานฯ ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์

2.3. บริการคลาวด์ (Cloud Service)

บริการคลาวด์ หมายถึง การให้บริการทรัพยากรด้านเทคโนโลยีสารสนเทศ เช่น คอมพิวเตอร์แม่ข่าย, ที่เก็บข้อมูล, ระบบประมวลผล, ซอฟต์แวร์ และเครื่องมือพัฒนาผ่านเครือข่ายอินเทอร์เน็ต ผู้ใช้งานสามารถเข้าถึงบริการเหล่านี้ได้โดยไม่ต้องลงทุนในโครงสร้างพื้นฐานเอง บริการคลาวด์ช่วยเพิ่มความสะดวก ยืดหยุ่น และลดต้นทุนในการดำเนินธุรกิจ

2.3.1. คุณสมบัติหลักของบริการคลาวด์

- 1) การเข้าถึงผ่านอินเทอร์เน็ต (Internet Access) ผู้ใช้งานสามารถเข้าถึงทรัพยากรหรือบริการได้ทุกที่ ทุกเวลา ผ่านการเชื่อมต่ออินเทอร์เน็ต
- 2) ความยืดหยุ่นและปรับขนาดได้ (Scalability) ทรัพยากรสามารถปรับเพิ่มหรือลดได้อย่างรวดเร็วตามความต้องการของผู้ใช้
- 3) การจัดการโดยผู้ให้บริการ (Managed by Providers) ผู้ให้บริการดูแลโครงสร้างพื้นฐานทั้งหมด เช่น การบำรุงรักษาคอมพิวเตอร์แม่ข่าย การสำรองข้อมูล และการรักษาความปลอดภัย
- 4) การทำงานร่วมกัน (Collaboration) ช่วยให้ทีมงานสามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพบนแพลตฟอร์มเดียวกัน

2.3.2. รูปแบบการคิดค่าบริการจากการใช้บริการคลาวด์

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

ตารางที่ 2 รูปแบบการคิดค่าบริการจากการใช้บริการคลาวด์

การคิดค่าบริการ	ข้อดี	ข้อเสีย	ลักษณะการใช้งานที่เหมาะสม	ข้อควรพิจารณา
การคิดค่าบริการตามปริมาณการใช้งานจริง (Pay-per-use)	- ประหยัดต้นทุน ผู้ใช้งานจ่ายเฉพาะสิ่งที่ใช้จริง - ความยืดหยุ่น รองรับการปรับขนาดทรัพยากรได้อย่างรวดเร็วตามความต้องการ - สามารถตรวจสอบการใช้งานและ	- ต้นทุนผันแปร หากไม่มีการบริหารจัดการที่ดี ค่าใช้จ่ายอาจเพิ่มขึ้นเกินกว่าที่คาดการณ์ไว้ - ความซับซ้อนในการวางแผนงบประมาณ เนื่องจากค่าใช้จ่ายขึ้นอยู่กับการใช้งานจริง ทำให้การ	- ธุรกิจที่ต้องการควบคุมต้นทุนในช่วงเริ่มต้น - องค์กรขนาดใหญ่: ใช้สำหรับแผนกหรือโครงการที่ต้องการทรัพยากร	- Pay-per-use เป็นโมเดลการคิดค่าบริการที่ช่วยลดต้นทุนและเพิ่มความยืดหยุ่นในการใช้งานทรัพยากรคลาวด์อย่างไรก็ตาม องค์กร

การคิดค่าบริการ	ข้อดี	ข้อเสีย	ลักษณะการใช้ งานที่เหมาะสม	ข้อควรพิจารณา
	ต้นทุนได้อย่าง ละเอียด	คาดการณ์ งบประมาณยากขึ้น	คลาวด์เพิ่มขึ้น ชั่วคราว	ต้องมีการ บริหารจัดการ การใช้งาน อย่างเหมาะสม เพื่อควบคุม ต้นทุนและ ป้องกัน ค่าใช้จ่ายที่ไม่ คาดคิด
การคิดค่าบริการ แบบสมาชิก (Subscription)	- การจัดการ งบประมาณ (Budgeting) ช่วยให้ สามารถวางแผนและ คาดการณ์ งบประมาณได้อย่าง แม่นยำ - ประสิทธิภาพการใช้ งาน (Efficiency) เหมาะสำหรับงานที่ มีการใช้งาน ทรัพยากรคงที่ เช่น การประมวลผลที่ ต่อเนื่อง - ความมั่นคงในการ ให้บริการผู้ให้บริการ คลาวด์อาจ รับประกันทรัพยากร ที่ถูกจองไว้ให้พร้อม ใช้งานเสมอ	- ความยืดหยุ่นต่ำ หากการใช้งานลดลง หรือเปลี่ยนแปลง ผู้ใช้งานอาจต้อง จ่ายเงินสำหรับ ทรัพยากรที่ไม่ได้ใช้ - ข้อผูกมัดระยะยาว ผู้ใช้งานต้องทำ สัญญาล่วงหน้าซึ่ง อาจเป็นระยะยาว เช่น 1-3 ปี - ความเสี่ยงด้านการ คาดการณ์ผิดพลาด หากการใช้งานไม่ถึง ปริมาณที่ตกลงไว้ ผู้ใช้อาจเสียค่าใช้จ่าย โดยเปล่าประโยชน์ - ไม่เหมาะสำหรับ ความต้องการที่ไม่ แน่นอน สำหรับ องค์กรที่มีการใช้งาน ทรัพยากรแบบผัน ผวนหรือไม่สามารถ คาดการณ์ได้	- เมื่อทราบ ปริมาณการใช้ งานล่วงหน้า เช่น เครื่องแม่ ข่าย ที่ต้องรัน อย่างต่อเนื่อง หรือทรัพยากร สำหรับ แอปพลิเคชันที่ มีผู้ใช้งานคงที่	- ควรประเมิน ความต้องการ และปริมาณ การใช้งาน อย่างรอบคอบ ก่อนทำสัญญา เพื่อลดความ เสี่ยงจากการใช้ งานที่ต่ำกว่า ปริมาณที่ตกลง ไว้

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

2.3.3. 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 3 ทั้งนี้ ระบบของหน่วยงานที่ต้องการใช้คลาวด์อาจมีความจำเป็นต้องประยุกต์ใช้บริการคลาวด์ที่หลากหลายเพื่อตอบสนองความต้องการได้ครบถ้วนตามวัตถุประสงค์

ตารางที่ 3 รูปแบบของบริการ Cloud (IaaS, PaaS และ SaaS)

รูปแบบบริการ	ลักษณะการใช้งานที่เหมาะสม	ตัวอย่างการใช้งานในหน่วยงานภาครัฐ	ข้อควรพิจารณา
การให้บริการโครงสร้างพื้นฐาน (Infrastructure as a Service: IaaS)	- ต้องการควบคุมโครงสร้างพื้นฐานอย่างเต็มรูปแบบ - มีระบบที่ต้องการปรับแต่งเฉพาะ	- ศูนย์ข้อมูลเสมือนที่ต้องการควบคุมระดับโครงสร้างพื้นฐาน - ระบบที่พัฒนาขึ้นเฉพาะ ไม่มีแพลตฟอร์ม หรือซอฟต์แวร์ของผู้ให้บริการคลาวด์	- ต้องมีบุคลากรที่เชี่ยวชาญการจัดการโครงสร้างพื้นฐาน - ความซับซ้อนในการจัดการระบบ ความปลอดภัยและการบำรุงรักษา
การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS)	- สำหรับการพัฒนาและปรับใช้แอปพลิเคชัน - ต้องการลดภาระการจัดการโครงสร้างพื้นฐาน - มีนักพัฒนาที่ต้องการดำเนินการเฉพาะการพัฒนา	- แพลตฟอร์มสำหรับพัฒนาแอปพลิเคชันที่สามารถปรับใช้และจัดการแอปพลิเคชันโดยไม่ต้องจัดการเกี่ยวกับโครงสร้างพื้นฐาน - ระบบบริหารจัดการฐานข้อมูล (DBMS)	- การย้ายแพลตฟอร์มไปยังผู้ให้บริการรายอื่นอาจซับซ้อน - ต้องทำความเข้าใจเครื่องมือและข้อจำกัดของแพลตฟอร์ม
การให้บริการซอฟต์แวร์ (Software as a Service: SaaS)	- สำหรับงานทั่วไปที่ต้องการโซลูชันสำเร็จรูป - ไม่ต้องการการปรับแต่งแอปพลิเคชัน - ลดค่าใช้จ่ายในการพัฒนาและบำรุงรักษาระบบ	- ใช้ระบบจัดการเอกสารและอีเมล เช่น Microsoft 365 หรือ Google Workspace - ระบบ CRM สำหรับการบริหารงานภายในหน่วยงาน - ระบบการอบรมออนไลน์ (e-Learning)	- ความยืดหยุ่นต่ำในการปรับแต่งระบบ - ข้อมูลอาจอยู่บนคลาวด์ของผู้ให้บริการ จึงต้องคำนึงถึงความปลอดภัยและข้อกำหนด

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

นอกจากนี้ กรอบแนวทางการบริหารจัดการระบบคลาวด์ภาครัฐตามนโยบายการใช้คลาวด์เป็นหลัก แนะนำให้ใช้บริการมาตรฐานที่ผู้ให้บริการจัดเตรียมไว้ ไม่ควรดัดแปลงเป็นการเฉพาะ (Customize) เช่น การติดตั้งระบบบริหารจัดการข้อมูลเองในเครื่องแม่ข่ายเสมือน (VM) ที่อยู่นอกเหนือการให้บริการโดยผู้ให้บริการ เนื่องจากจะไม่ได้รับการดูแลโดยผู้ให้บริการ หรือการปรับปรุงเวอร์ชัน อย่างต่อเนื่อง ทั้งนี้ ให้หน่วยงานพิจารณาเลือกรูปแบบบริการคลาวด์ (Cloud Services) ที่เหมาะสมกับงาน และเป็นบริการที่ผ่านหลักเกณฑ์ตามที่คณะกรรมการพัฒนารัฐบาลดิจิทัล หรือหน่วยงานที่ได้รับมอบหมายกำหนด

2.4. ความรับผิดชอบร่วม (Shared Responsibility)

บริการคลาวด์แต่ละรูปแบบมีการกำหนดความรับผิดชอบระหว่างผู้ให้บริการคลาวด์ (Cloud Service Provider - CSP) และผู้ให้บริการ (Cloud Customer) [17] ซึ่งหน่วยงานจำเป็นต้องทำความเข้าใจและวางแผนการใช้งานโดยเฉพาะเมื่อจำเป็นต้องกำหนดบทบาทหน้าที่ และขั้นตอนการประสานงานทั้งสถานการณ์ปกติ และเมื่อพบปัญหา ซึ่งโดยทั่วไปขอบเขตความรับผิดชอบจะกำหนดตามรูปแบบของบริการคลาวด์ (IaaS, PaaS, SaaS) ดังนี้

- 1) Infrastructure as a Service (IaaS)
 - ผู้ให้บริการคลาวด์ (CSP)
 - การจัดการโครงสร้างพื้นฐานพื้นฐาน 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 โดยผู้ให้บริการต้องจัดการความปลอดภัยของข้อมูลแอปพลิเคชัน และการเข้าถึง ในขณะที่ผู้ให้บริการรับผิดชอบโครงสร้างพื้นฐานและการรักษาความปลอดภัยของระบบที่จัดทำให้ การทำความเข้าใจบทบาทและความรับผิดชอบนี้จะช่วยให้องค์กรใช้งานคลาวด์ได้อย่างปลอดภัยและมีประสิทธิภาพ โดยหน่วยงานควรมีการระบุอย่างชัดเจนในข้อตกลงการให้บริการ

ตารางที่ 4 ตารางเปรียบเทียบความรับผิดชอบในแต่ละรูปแบบการให้บริการคลาวด์

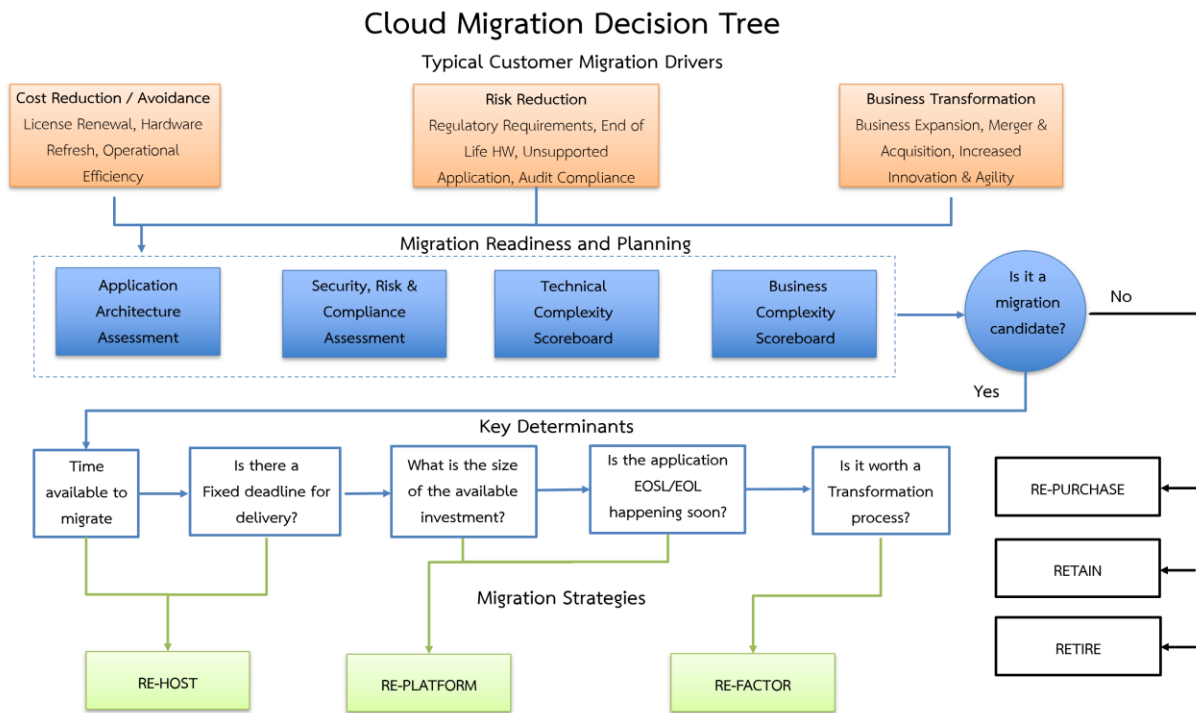
หัวข้อความรับผิดชอบ	On Premise	IaaS	PaaS	SaaS
การตั้งค่าแอปพลิเคชัน (Application configuration)	ผู้ให้บริการ	ผู้ให้บริการ	ผู้ให้บริการ	ผู้ให้บริการ
การพิสูจน์ตัวตนและเข้าถึงของผู้ใช้ (Identity & access controls)	ผู้ให้บริการ	ผู้ให้บริการ	ผู้ให้บริการ และผู้ให้บริการ	ผู้ให้บริการ และผู้ให้บริการ
ข้อมูลของแอปพลิเคชัน (Application data storage)	ผู้ให้บริการ	ผู้ให้บริการ	ผู้ให้บริการ และผู้ให้บริการ	ผู้ให้บริการ
แอปพลิเคชัน (Application)	ผู้ให้บริการ	ผู้ให้บริการ	ผู้ให้บริการ	ผู้ให้บริการ
ระบบปฏิบัติการ (Operating system)	ผู้ให้บริการ	ผู้ให้บริการ	ผู้ให้บริการ	ผู้ให้บริการ
การควบคุมระบบเครือข่าย (Network flow controls)	ผู้ให้บริการ	ผู้ให้บริการ และผู้ให้บริการ	ผู้ให้บริการ	ผู้ให้บริการ
โครงสร้างพื้นฐานของเครื่องแม่ข่าย (Host infrastructure)	ผู้ให้บริการ	ผู้ให้บริการ	ผู้ให้บริการ	ผู้ให้บริการ
ความปลอดภัยทางกายภาพ (Physical security)	ผู้ให้บริการ	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) อาจใช้เทคโนโลยีหลักในการจัดการกับการบรรจุ (Containerization) และการจัดการคอนเทนเนอร์ (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 ตัวอย่างแผนภูมิการตัดสินใจเลือกกลยุทธ์ การย้ายระบบขึ้นคลาวด์ อ้างอิงตาม 6Rs

(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 บริการเหล่านี้ส่วนใหญ่มักมีการคิดค่าใช้จ่ายตามการใช้งานจริง 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 ที่เชื่อมต่อกับอินเทอร์เน็ตเพื่อติดตามข้อมูลหรือดำเนินการ 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 ซึ่งอาจส่งผลกระทบต่อความต่อเนื่องของบริการหรือความปลอดภัยของข้อมูลเมื่อมีการเปลี่ยนแปลงระบบ ประกอบด้วยหลักการสำคัญเบื้องต้น ดังนี้

- 1) วางแผนตั้งแต่เริ่มต้น ระบุกลยุทธ์การออกจากระบบตั้งแต่ขั้นตอนการวางแผนการย้ายข้อมูลไปยังคลาวด์ โดยการกำหนดข้อกำหนดในสัญญากับผู้ให้บริการคลาวด์ เช่น เงื่อนไขหรือสัญญาที่ระบุการส่งคืนข้อมูล การกำหนดระยะเวลาการเก็บรักษาข้อมูล (Data Retention) การสนับสนุนหลังการขาย ค่าใช้จ่ายที่เกี่ยวข้อง และการเคลื่อนย้ายข้อมูล (Data portability) หรือการที่ผู้ให้บริการคลาวด์กำหนดให้ลูกค้า/ผู้ให้บริการคลาวด์ 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. แนวทางการประเมินราคาและวางแผนงบประมาณ

3.1. แนวทางการประเมินราคา

การประเมินราคาและการวางแผนงบประมาณ สำหรับการดำเนินการด้านคลาวด์ของหน่วยงานภาครัฐ มีความสำคัญเป็นอย่างมากเนื่องจากบริการคลาวด์มีรายละเอียดการคิดค่าใช้จ่ายหลายรูปแบบ ตามความต้องการใช้งาน ซึ่งสามารถสรุปแนวทางการประเมินราคาและวางแผนงบประมาณ สำหรับการจัดซื้อจัดจ้างระบบคลาวด์ ภาครัฐ ดังนี้

3.1.1. การวิเคราะห์ความต้องการทรัพยากร

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

3.1.2. การวิเคราะห์ต้นทุนทางตรงและทางอ้อม [23][24]

ต้นทุนทางตรง (Direct Costs) คือ ค่าบริการที่เกิดขึ้นจากการใช้บริการคลาวด์ที่สามารถระบุได้โดยตรงและชัดเจน 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 ค่าบริการ DevOps ค่าบริการติดตามการใช้งาน (Monitoring) ค่าบริการเข้ารหัสข้อมูล หรือค่าบริการอื่น ที่อาจเกิดขึ้น ซึ่งไม่รวมในบริการสนับสนุน (Support Plan) เป็นต้น

3.1.3. 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) ช่วยให้ผู้ใช้บริการเปรียบเทียบต้นทุนระหว่างการจัดตั้งค่าต่าง ๆ เพื่อหาทางเลือกที่เหมาะสมที่สุด
- 3) การแสดงผลที่โปร่งใส (Transparent Breakdown) แสดงรายละเอียดค่าใช้จ่ายในแต่ละส่วน เช่น ค่าประมวลผล, ค่าเก็บข้อมูล, และค่าบริการเสริม
- 4) รองรับการวางแผนงบประมาณ (Budget Planning) ช่วยผู้ใช้งานวางแผนการใช้งบประมาณในระยะยาว เช่น การคำนวณค่าใช้จ่ายรายเดือนหรือรายปี

3.1.4. การบริหารและตรวจสอบค่าใช้จ่าย

การบริหารจัดการและตรวจสอบค่าใช้จ่ายสำหรับบริการคลาวด์ เพื่อให้สอดคล้องกับการตั้งงบประมาณแบบยืดหยุ่น (Flexible Budgeting) ของหน่วยงานเป็นสิ่งสำคัญเมื่อต้องการควบคุมต้นทุนและเพิ่มประสิทธิภาพในการใช้งานคลาวด์อย่างเหมาะสม โดยแนวทางและเครื่องมือที่ผู้ให้บริการจัดเตรียมไว้ มีตัวอย่างดังนี้

- 1) การติดตามการใช้งานแบบเรียลไทม์ (Real-time Monitoring)
- 2) เปิดใช้งานการแจ้งเตือนเมื่อค่าใช้จ่ายหรือการใช้งานใกล้ถึงขีดจำกัด
- 3) ใช้ Billing Alerts เพื่อรับการแจ้งเตือนผ่านอีเมลหรือแอปพลิเคชัน
- 4) การแยกบัญชีหรือ Tag ทรัพยากร (Tagging Resources) ใช้ Tags เพื่อแยกต้นทุนตาม โครงการหรือแผนก ช่วยให้ทราบว่าแต่ละส่วนใช้งบประมาณเท่าไร
- 5) การวิเคราะห์ค่าใช้จ่าย (Cost Analysis) วิเคราะห์ต้นทุนที่เกิดขึ้น เพื่อระบุทรัพยากรที่ใช้เกินความจำเป็น เช่น คอมพิวเตอร์แม่ข่ายที่ทำงานนอกเวลาหรือไม่ได้ใช้งานเต็มประสิทธิภาพ

3.2. การบริหารจัดการค่าใช้จ่ายระบบคลาวด์ (Financial Operations, Fin-ops)

แนวทางในการบริหารจัดการค่าใช้จ่ายระบบคลาวด์ [25-26] สามารถใช้เป็นแนวทางเพื่อเพิ่มประสิทธิภาพทางการเงินให้สอดคล้องกับการใช้งานคลาวด์ โดยเน้นการทำงานร่วมกันระหว่างฝ่ายเทคนิค (เช่น DevOps) และฝ่ายการเงิน (Finance) เพื่อให้การตัดสินใจด้านการใช้งบประมาณมีประสิทธิภาพและสอดคล้องกับความเป็นจริงมากยิ่งขึ้น โดยมีหลักการสำคัญ 4 ข้อ ได้แก่

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

3.3. การประเมินความคุ้มค่าบริการคลาวด์ (Total Cost of Ownership, TCO)

การประเมินความคุ้มค่าบริการคลาวด์ [27] คือ แนวคิดการประเมินค่าใช้จ่ายทั้งหมดที่เกี่ยวข้องกับการจัดหา การดำเนินงาน และการกำจัดสินทรัพย์หรือระบบตลอดอายุการใช้งาน แนวคิดนี้ช่วยให้องค์กรสามารถประเมินต้นทุนที่แท้จริงของการลงทุน โดยไม่พิจารณาเฉพาะราคาซื้อเริ่มต้นเท่านั้น แต่เป็นการพิจารณาต้นทุนทั้งหมดตั้งแต่การจัดซื้อ จนถึงการกำจัด และเป็นวิธีการคิดเกี่ยวกับต้นทุน ประเมินความเหมาะสม วัดและเปรียบเทียบต้นทุนของตัวเลือกซอฟต์แวร์ทั้งหมด ใช้ได้ทั้งกับซอฟต์แวร์โอเพ่นซอร์ส และซอฟต์แวร์ที่มีลิขสิทธิ์

3.4. แนวทางการของงบประมาณโครงการด้านระบบคลาวด์

ตามกรอบแนวทางดำเนินการสำหรับการใช้คลาวด์เป็นหลักเน้นให้หน่วยงานมีการประเมินราคา ค่าใช้จ่าย ด้านคลาวด์ และเสนอโครงการผ่านกลไกตามนโยบายการใช้คลาวด์เป็นหลัก เพื่อให้รัฐบาลทราบความต้องการใช้คลาวด์โดยรวมของประเทศ โดยหน่วยงานของรัฐสามารถศึกษาขั้นตอนวิธีการรวมทั้งเอกสารที่เกี่ยวข้องได้จากเว็บไซต์สนับสนุนการดำเนินการตามนโยบายการใช้คลาวด์เป็นหลัก <https://kb.dga.or.th/cloud/> ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ทั้งนี้กรณีโครงการมีการดำเนินการที่เกี่ยวข้องกับคลาวด์ ควรมีการแยกค่าใช้จ่ายด้านคลาวด์ที่ชัดเจน

ทั้งนี้ หน่วยงานผู้รองรับงบประมาณด้านคลาวด์ควรจัดเตรียมรายละเอียดประกอบการของงบประมาณเบื้องต้น (อ้างอิงตาม แบบฟอร์มใบคำของบประมาณภายใต้แผนงานบูรณาการรัฐบาลดิจิทัล ประจำปีงบประมาณ พ.ศ. 2569 สำหรับหน่วยงานระดับกรมหรือเทียบเท่าดิจิทัล - แนวทางที่ 1.3) ดังนี้

- 1) ข้อมูลรายละเอียดทั่วไปโครงการทั่วไป เช่น ชื่อโครงการ หลักการและเหตุผล วัตถุประสงค์โครงการ
- 2) ประเภทโครงการ ว่าเป็นโครงการระบบ IT ใหม่ หรือ โครงการเดิมที่ต้องมีการซื้อ Server ใหม่เพื่อมาขยายบริการ หรือทดแทนเครื่องที่หมดอายุ หรือ โครงการที่ต้องทำสัญญาเช่าใหม่ เช่าต่อเนื่อง หรือเปลี่ยนสัญญาเช่าบนระบบที่มีการใช้งานในปัจจุบัน หรือ ระบบที่ต้องมีการซื้อ License ของ Software ที่กำลังหมดอายุ เป็นต้น
- 3) แนวทางการดำเนินการสำหรับการใช้คลาวด์เป็นหลัก ว่าเป็นโครงการที่จะขึ้นระบบคลาวด์ หรือโครงการที่มีการพัฒนาการจัดซื้อจัดหาระบบ Application หรือระบบ IT ต่าง ๆ ที่เกี่ยวข้องกับระบบคลาวด์ โดยมีรายละเอียดการดำเนินการว่าเป็นระบบงานที่พัฒนาต้องใช้ระบบคลาวด์ประเภทใดและใช้บริการลักษณะใด (IaaS, PaaS, SaaS)
- 4) รายการงบประมาณที่ใช้ เช่น ค่าเช่าทรัพยากร IaaS (VM, Storage), ค่าใช้จ่าย PaaS (DevOps Tools), ค่าใช้จ่าย SaaS (Office Tools), ค่าอบรมบุคลากร และ ค่าที่ปรึกษาและออกแบบระบบ เป็นต้น
- 5) ประมาณการผู้ใช้งานระบบ เช่น ข้อมูล pageviews (กรณีเป็นเว็บไซต์) ข้อมูล transactions ที่อาจเกิดขึ้น ขนาดของข้อมูล เช่น ข้อมูลที่จัดเก็บเพื่อให้เข้าถึงได้โดยผู้ใช้งาน (contents)
- 6) รายละเอียดรูปแบบโครงสร้างระบบ (กรุณแนบภาพโครงสร้างระบบ)
- 7) รายละเอียดอื่น ๆ ศึกษาได้ตามตัวอย่างแบบฟอร์มใบคำของบประมาณภายใต้แผนงานบูรณาการรัฐบาลดิจิทัล จากเว็บไซต์ <https://kb.dga.or.th/cloud/>

ทั้งนี้ หากหน่วยงานมีความจำเป็นต้องใช้คลาวด์ส่วนตัว (Private Cloud) กับข้อมูลที่ไม่ใช่ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected) ซึ่งไม่สอดคล้องกับแนวทางการจำแนกประเภทข้อมูล และการเลือกใช้บริการคลาวด์ ให้แจ้งต่อ สพร. เพื่อนำเสนอต่อคณะทำงานพิจารณากลับกรองโครงการฯ พร้อมรายละเอียด ดังนี้

- 1) ผลการประเมินระดับชั้นข้อมูล ตามประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เลขที่ ม 1/2565 เรื่อง มสพร. 8-2565 มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นข้อมูลและแบ่งปันข้อมูลภาครัฐ
- 2) ผลการวิเคราะห์ความคุ้มค่า ตลอดอายุการใช้งานของระบบ ตั้งแต่ การลงทุนจัดหาและติดตั้งระบบ การบำรุงรักษา การบริหารจัดการ จนถึงการยุติการใช้งาน
- 3) มาตรฐานและแนวทางการรักษาความมั่นคงปลอดภัย และการบริหารจัดการ คลาวด์ส่วนตัว (Private Cloud) ของหน่วยงาน เช่น ISO27001
- 4) ระดับความพร้อมของเจ้าหน้าที่ด้านเทคนิคของหน่วยงาน

3.5. แนวทางการจัดซื้อจัดจ้างระบบคลาวด์ สำหรับภาครัฐ

การจัดซื้อจัดจ้างระบบคลาวด์สำหรับภาครัฐ ต้องมีความโปร่งใส คุ้มค่า และสอดคล้องกับกฎหมายและนโยบายของรัฐ โดยสามารถศึกษาข้อมูลเพิ่มเติมได้จากพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 [28] ซึ่งเป็นกฎหมายหลักที่กำหนดหลักเกณฑ์และวิธีการจัดซื้อจัดจ้างของหน่วยงานภาครัฐ เพื่อให้การใช้จ่ายงบประมาณเป็นไปอย่างมีประสิทธิภาพและโปร่งใส และ ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 [29] ระเบียบที่ออกตามพระราชบัญญัติฯ ข้างต้น กำหนดรายละเอียดและขั้นตอนการจัดซื้อจัดจ้าง รวมถึงการบริหารพัสดุภาครัฐ เพื่อให้หน่วยงานปฏิบัติได้อย่างถูกต้อง

ทั้งนี้ ตามกรอบแนวทางดำเนินการสำหรับการใช้คลาวด์เป็นหลัก ผู้ประกอบการที่จะจัดซื้อจัดจ้างต้องมีมาตรฐานตามนโยบายการใช้คลาวด์เป็นหลัก เพื่อประโยชน์ในการดำเนินงานให้เป็นไปอย่างมีประสิทธิภาพ และสามารถนำไปปรับใช้ได้จริง

4. แนวทางในด้านความปลอดภัย และด้านอื่นที่เกี่ยวข้อง

4.1. แนวทางในด้านความปลอดภัย

แนวทางในด้านความปลอดภัยการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก หน่วยงานสามารถดำเนินการโดยอ้างอิงตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 [13] ซึ่งสรุปโดยสังเขปเนื้อหาแบ่งออกเป็นแนวทางด้านความปลอดภัยผู้ให้บริการคลาวด์ (Cloud Service Provider) และผู้ใช้บริการคลาวด์ (Cloud Service Consumer) มีความแตกต่างและเชื่อมโยงกันในด้านความรับผิดชอบ และมีจุดมุ่งหมายเพื่อปกป้องข้อมูลระบบและโครงสร้างพื้นฐานของคลาวด์อย่างครบวงจรโดยแบ่งเป็น

- 1) การกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์
- 2) การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

4.1.1.การกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

กระบวนการที่มุ่งเน้นการจัดการความเสี่ยงและการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบที่ใช้งานบนคลาวด์ (Cloud Security) เพื่อให้มั่นใจว่าการจัดเก็บ ประมวลผล และถ่ายโอนข้อมูลบนคลาวด์มีความปลอดภัยตามมาตรฐานสากล โดยได้มีการพิจารณา ดำเนินการในรายละเอียดดังต่อไปนี้

- 1) นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
- 2) โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ
- 3) การปฏิบัติตามกฎ ระเบียบ และข้อบังคับ

4.1.2.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) ขององค์กร เพื่อให้สอดคล้องกับมาตรฐานสากล โดยครอบคลุมการบริหารจัดการความเสี่ยง การป้องกันภัยคุกคาม และการสร้างความมั่นใจในระบบข้อมูลขององค์กร ซึ่งครอบคลุมการดูแลทรัพย์สินด้านข้อมูล (Information Assets) ขององค์กรจากการเข้าถึงโดยไม่ได้รับอนุญาต การถูกทำลาย หรือการสูญเสีย เน้นการควบคุมพื้นที่และอุปกรณ์ทางกายภาพ รวมถึงสภาพแวดล้อมที่อาจมีผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล

มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 กำหนดให้บังคับใช้เมื่อพ้นกำหนดสองปีนับแต่วันที่ประกาศในราชกิจจานุเบกษา หน่วยงานภาครัฐในฐานะผู้ใช้บริการคลาวด์ควรศึกษารายละเอียด และปรับปรุงบริการให้สอดคล้องตามข้อกำหนด

4.1.3. มาตรการด้านความปลอดภัยสำหรับการใช้งานคลาวด์สาธารณะ (Public Cloud)

เนื่องจากคลาวด์สาธารณะ (Public Cloud) เป็นบริการคลาวด์ที่เปิดให้บริการกับผู้ให้บริการทั่วไป โดยที่ทรัพยากรทั้งหมดอยู่ภายใต้การควบคุมของผู้ให้บริการคลาวด์ เพื่อเพิ่มมาตรการควบคุมดูแลความปลอดภัยที่สูงขึ้นหน่วยงานสามารถเลือกใช้งานคลาวด์สาธารณะที่มีการสร้างสถานะแวดล้อมที่เสมือนเป็นเครือข่ายส่วนตัวหรือที่เรียกว่า Virtual Private Cloud (VPC) ³ ซึ่งให้บริการโดยผู้ให้บริการที่มีความพร้อม เพื่อเพิ่มระดับความมั่นคงปลอดภัย และการควบคุม (Security Measure) โดย VPC จะทำการแบ่งแยกทรัพยากรคลาวด์ของผู้ใช้บริการออกจากผู้ใช้อย่างอื่นบนโครงสร้างพื้นฐานทางกายภาพเดียวกัน ทำให้หน่วยงานสามารถควบคุมสภาพแวดล้อมเครือข่ายของตนเองได้อย่างสมบูรณ์ ดังนั้น การออกแบบและใช้งาน VPC อย่างเหมาะสมจึงเป็นแนวทางที่สำคัญสำหรับหน่วยงานที่ต้องการยกระดับการควบคุมและความมั่นคงปลอดภัยในการใช้บริการคลาวด์สาธารณะให้ใกล้เคียงกับเครือข่ายส่วนตัวของหน่วยงาน

4.2. การสร้างความตระหนักและการฝึกอบรมเรื่องคลาวด์ (Training)

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

- 1) ผู้ใช้บริการคลาวด์ ต้องเพิ่มโปรแกรมสร้างความตระหนัก การศึกษา และการฝึกอบรมสำหรับผู้จัดการธุรกิจบริการคลาวด์ ผู้ดูแล ระบบบริการคลาวด์ ผู้ประกอบบริการคลาวด์ และ ผู้ใช้บริการคลาวด์ รวมถึงพนักงานและผู้รับจ้างที่เกี่ยวข้อง
- 2) ต้องจัดให้มีโปรแกรมการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษา และการฝึกอบรมเกี่ยวกับบริการคลาวด์แก่ผู้บริหารและผู้จัดการที่กำกับดูแล รวมถึงหน่วยงานธุรกิจ (Business Units)

4.3. แนวทางการจัดการระบบสำรองข้อมูลและกู้คืนข้อมูลบนคลาวด์

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

³ คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud - VPC) หมายถึง บริการคลาวด์สาธารณะ (Public Cloud) ที่มีการเพิ่มมาตรการคุ้มครองข้อมูลมากกว่าการใช้งานคลาวด์สาธารณะทั่วไป โดยมีการแยกการบริหารจัดการทรัพยากรและการใช้งานเฉพาะผู้ใช้บริการแต่ละราย (Isolation) [16][17]

4.3.1. วิจารณ์ปัจจัยเกี่ยวข้องที่สำคัญ

- 1) ขอบเขตของการสำรองข้อมูล [22]
 - ระบุข้อมูล ระบบ และแอปพลิเคชันที่ต้องสำรอง
 - จัดหมวดหมู่ข้อมูลตามความสำคัญและเวลาที่ข้อมูลเปลี่ยนแปลง
- 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

4.3.2. 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

4.3.3. แนวทางการกู้คืนข้อมูล

- 1) วางแผนสถานการณ์การกู้คืน
 - การกู้คืนทั้งหมด: สำหรับกรณีที่ระบบทั้งหมดเสียหาย
 - การกู้คืนบางส่วน: สำหรับการกู้คืนไฟล์ โฟลเดอร์ หรือแอปพลิเคชันเฉพาะ
 - การกู้คืนข้ามภูมิภาคหรือไฮบริด: กู้คืนข้อมูลจากภูมิภาคหรือผู้ให้บริการคลาวด์อื่น
- 2) กระบวนการกู้คืน
 - ระบุแหล่งข้อมูลสำรอง ค้นหาข้อมูลสำรองโดยใช้ Metadata หรือ Index
 - ตรวจสอบความสมบูรณ์ของข้อมูล ยืนยันว่าไฟล์สำรองสมบูรณ์และไม่มีเสียหาย
 - ลำดับความสำคัญในการกู้คืน เริ่มจากระบบที่มีความสำคัญต่อธุรกิจมากที่สุด
 - ติดตามและตรวจสอบ ตรวจสอบกระบวนการกู้คืนเพื่อป้องกันข้อผิดพลาด โดยทดสอบ ระบบ หลังการกู้คืนเพื่อให้แน่ใจว่าทำงานได้ตามปกติ
- 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] พระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560. (2560, 24 กุมภาพันธ์). ราชกิจจานุเบกษา, 134(24 ก), 13-54.
- [29] ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 (2560, 23 สิงหาคม). ราชกิจจานุเบกษา, 134 (ตอนพิเศษ 210 ก), 1-71.
- [30] คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2567). (2567, 11 พฤศจิกายน) มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์. ราชกิจจานุเบกษา, 141 (ตอนพิเศษ 306 ง), 32-33.
-