สพร./CDV
ธันวาคม 2568

ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน

มาตรฐานฉบับสมบูรณ์จะมีประกาศในราชกิจจานุเบกษา

ร่าง

มาตรฐานรัฐบาลดิจิทัล

ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์

Cloud Service Provider 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-X : 256X

DGS 9-X : 256X

ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์
Cloud Service Provider Standard

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักนายกรัฐมนตรี

มาตรฐานรัฐบาลดิจิทัล
ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์

มรด. 9-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
นายชลอ อินทพันธ์	สำนักบริหารการทะเบียน กรมการปกครอง
นางสาวดารารัตน์ โฆษิตพิพัฒน์	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นางสาวพรพิมล อุ่นไพร	สำนักงานคณะกรรมการกฤษฎีกา
นายสันติ สิทธิเลิศพิศาล	สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นายวีระ วีระกุล	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
รองศาสตราจารย์เกริก ภิรมย์โสภา	ประธานคณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ
ศาสตราจารย์ธีรณี อจลากุล	ประธานคณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการข้อมูลภาครัฐ
ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์	ประธานคณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

ที่ปรึกษา

นางไอรดา เหลืองวิไล	รองผู้อำนวยการ รักษาการแทนผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์	มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

รองประธานคณะทำงาน

นางสาวยศวลัย โชติปทุมวรรณ	มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คณะทำงาน

นายชลอ อินทรพันธุ์	กรมการปกครอง
นางสาวมนทิพา เข่งพิมล	กรมพัฒนาธุรกิจการค้า
นางสาวสำรวย นุ่มศรี	กรมศุลกากร
นางจันทร์เจริญ แบร์โรวส์	กรมสรรพากร
นางศุปกิจ สกลเสาวภาคย์	กรมที่ดิน
นางสาวพิมพ์สราญ บำเพ็ญวิบูลย์กิจ	กรมธนารักษ์
นายชรินทร์ สัจจามั่น	กรมส่งเสริมการปกครองท้องถิ่น
นางสุรีพร พรโสภณวิชญ์	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
นายกิตติ ขุนสนิท	สำนักงานส่งเสริมเศรษฐกิจดิจิทัล
นางสาวอาวีวรรณ อินทกาญจน์	ธนาคารแห่งประเทศไทย
นายสยาม ลววิโรจน์วงศ์	สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยเลขานุการ

นายนพดล แก้วคำ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิเคราะห์และจัดทำมาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล
ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์

นายปราการ ศิริมา สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายณัฐวัฒน์ วรสิทธิ์ตระกูล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายนพดล แก้วคำ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

มาตรฐานรัฐบาลดิจิทัลฉบับนี้ ได้ผ่านการประชาพิจารณ์รับฟังความคิดเห็นเป็นการทั่วไป และนำข้อมูลข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้องมาปรับปรุงมาตรฐานฉบับนี้ จนมีความสมบูรณ์ครบถ้วน นอกจากนี้ มาตรฐานฉบับนี้ยังได้รับการพิจารณากลั่นกรองจากคณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ และผ่านการพิจารณาเห็นชอบจาก คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 เพื่อให้มั่นใจว่ามาตรฐานนี้มีความสมบูรณ์ครบถ้วน และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพสูงสุด

มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ เวอร์ชัน 1.0 ฉบับนี้ จัดทำโดยฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สำนักนายกรัฐมนตรี

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เลขที่ 999 ชั้น 4 สถาบันเพื่อการยุติธรรมแห่งประเทศไทย
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
E-mail: sd-g3_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 มุ่งหมายให้ผู้ให้บริการคลาวด์และผู้ประกอบการที่เกี่ยวข้อง รับทราบถึงหลักเกณฑ์ เงื่อนไข และมาตรฐานต่าง ๆ ที่ต้องปฏิบัติตาม ในการให้บริการคลาวด์แก่หน่วยงานของรัฐ สร้างความรู้ความเข้าใจเกี่ยวกับกระบวนการและกลไกในการประกาศรายชื่อผู้ให้บริการคลาวด์ (shortlist) แก่ข้าราชการ บุคลากรภาครัฐ และผู้มีส่วนเกี่ยวข้อง และนำเสนอข้อมูลเกี่ยวกับมาตรฐาน หลักเกณฑ์ แนวปฏิบัติ และข้อกำหนด ทั้งของไทยและสากล ในด้านการคัดกรองผู้ให้บริการคลาวด์

การดำเนินการตามมาตรฐานนี้จะนำไปสู่การสนับสนุนและส่งเสริมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน การบูรณาการข้อมูลกับหน่วยงานอื่น การเปิดเผยข้อมูลสู่ประชาชน ตลอดจนสนับสนุนการวิเคราะห์ข้อมูลเพื่อนำไปใช้ประโยชน์ในมิติต่าง ๆ ซึ่งจะส่งผลโดยตรงต่อการออกแบบนโยบายการบริหารราชการแผ่นดิน การยกระดับการปฏิบัติงาน และการให้บริการประชาชนอย่างมีประสิทธิภาพและทันสมัย

สารบัญ

สารบัญตาราง

สารบัญภาพ

มาตรฐานรัฐบาลดิจิทัล
ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์

1. บทนำ

1.1 ความเป็นมา

เพื่อเป็นการยกระดับประสิทธิภาพของการบริหารงานและการบริการประชาชน รองรับการเปลี่ยนผ่านไปสู่การเป็นรัฐบาลดิจิทัล ปัจจุบันหน่วยงานของรัฐได้นำเทคโนโลยีคลาวด์มาประยุกต์ใช้เพื่อลดภาระค่าใช้จ่ายและเพิ่มความยืดหยุ่นในการดำเนินงาน อย่างไรก็ตาม การพึ่งพาผู้ให้บริการที่หลากหลายและมีมาตรฐานที่แตกต่างกัน อาจก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล ความไม่เข้ากันของระบบ (Interoperability) และปัญหาในการรักษาอธิปไตยทางข้อมูลของประเทศ

ด้วยเหตุนี้ จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการ **กำหนดมาตรฐานสำหรับผู้ให้บริการคลาวด์ (Cloud Provider Standards)** ที่ชัดเจน เพื่อใช้เป็นเกณฑ์ประกันคุณภาพและความน่าเชื่อถือของผู้ที่จะเข้ามาให้บริการแก่ภาครัฐ ให้มั่นใจได้ว่ามีมาตรการรักษาความมั่นคงปลอดภัยที่ได้มาตรฐานสากล มีธรรมาภิบาลในการบริหารจัดการข้อมูล และสามารถเชื่อมโยงระบบเข้ากับโครงสร้างพื้นฐานกลางของรัฐได้อย่างเป็นเอกภาพ อันจะนำไปสู่การสร้างระบบนิเวศคลาวด์ภาครัฐที่มั่นคง ปลอดภัย และคุ้มค่าในระยะยาว

1.2 วัตถุประสงค์

1) เพื่อให้ผู้ให้บริการคลาวด์และผู้ประกอบการที่เกี่ยวข้อง รับทราบถึงหลักเกณฑ์ เงื่อนไข และมาตรฐานต่าง ๆ ที่ต้องปฏิบัติตาม ในการให้บริการคลาวด์แก่หน่วยงานของรัฐ
2) เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับกระบวนการและกลไกในการประกาศรายชื่อผู้ให้บริการคลาวด์ (shortlist) แก่ข้าราชการ บุคลากรภาครัฐ และผู้มีส่วนเกี่ยวข้อง
3) เพื่อนำเสนอข้อมูลเกี่ยวกับมาตรฐาน หลักเกณฑ์ แนวปฏิบัติ และข้อกำหนด ทั้งของไทยและสากลในด้านการคัดกรองผู้ให้บริการคลาวด์

1.3 ขอบข่าย

มาตรฐานรัฐบาลดิจิทัลฉบับนี้ ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ จัดทำขึ้นเพื่อเป็นแนวทางและข้อเสนอแนะสำหรับการประกาศรายชื่อผู้ให้บริการคลาวด์ (shortlist) ให้มีการบริการจัดการที่ดี มีความมั่นคงปลอดภัยสูง ให้สอดคล้องกับนโยบายภาครัฐ

ขอบเขตของมาตรฐานครอบคลุม

1) กระบวนการและกลไก ในการประกาศรายชื่อผู้ให้บริการคลาวด์ (shortlist)
2) ข้อเสนอแนะกรอบแนวทางการขับเคลื่อน ที่เกี่ยวข้อง

3) ข้อมูลเกี่ยวกับมาตรฐาน หลักเกณฑ์ แนวปฏิบัติ และข้อกำหนด ทั้งของประเทศไทยและมาตรฐานสากล สำหรับการคัดกรองผู้ให้บริการคลาวด์

มาตรฐานนี้ได้ถูกพัฒนาขึ้นโดยยึดมั่นในแนวทางและหลักการที่สอดคล้องกับ ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง กรอบแนวทางการบริหารจัดการระบบคลาวด์ภาครัฐ

ทั้งนี้ คู่มือการประกาศรายชื่อผู้ให้บริการคลาวด์ (shortlist) และแนวทางการตรวจประเมินผู้ให้บริการคลาวด์ (Cloud Service Provider) ที่สอดคล้องกับมาตรฐานฉบับนี้ จะเป็นไปตามประกาศของสำนักงานพัฒนารัฐบาลดิจิทัล หรือประกาศอื่น ๆ ที่เกี่ยวข้องต่อไป

1.4 บทนิยาม

นิยามคำศัพท์ที่เกี่ยวข้องกับมาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ มีดังนี้

หน่วยงานของรัฐ หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์การมหาชน รัฐสภา ศาล องค์กรอิสระตามรัฐธรรมนูญ องค์กรอัยการ สถาบันอุดมศึกษาของรัฐ และหน่วยงานอิสระของรัฐ

ผู้ใช้บริการ หมายความว่า หน่วยงานของรัฐทั้งราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณองค์การมหาชน องค์กรอิสระ องค์กรตามรัฐธรรมนูญ หรือหน่วยงานอื่นของรัฐตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองกิจกรรมด้าน บริการคลาวด์สำหรับหน่วยงานภาครัฐ

ผู้ให้บริการคลาวด์ (Cloud Service Provider) หมายรวมถึงหน่วยงานของเอกชน หรือของรัฐทั้งภายในประเทศและต่างประเทศ ที่ให้บริการด้านคลาวด์

บัญชีรายชื่อผู้ให้บริการคลาวด์ (Shortlist) หมายความว่า บัญชีของผู้ให้บริการคลาวด์ ตัวแทน และอื่น ๆ ที่ผ่านการพิจารณาคุณสมบัติตามมาตรฐานที่กำหนด

คลาวด์สาธารณะ (Public Cloud) หมายความว่า บริการคลาวด์ที่เปิดให้บริการกับผู้ใช้บริการทั่วไป โดยทรัพยากรทั้งหมดอยู่ภายใต้การควบคุมของผู้ให้บริการคลาวด์

คลาวด์ส่วนตัว (Private Cloud) หมายความว่า บริการคลาวด์ที่ใช้งานโดยผู้ใช้บริการเพียง รายเดียว โดยทรัพยากรทั้งหมดอยู่ภายใต้การควบคุมของผู้ใช้บริการรายนั้น

คลาวด์แบบกลุ่ม (Community Cloud) หมายความว่า บริการคลาวด์ที่ใช้เฉพาะกลุ่มผู้ใช้บริการ ที่มีความต้องการใช้งานและมีความเกี่ยวข้องกัน ซึ่งทรัพยากรถูกควบคุมโดยสมาชิกในกลุ่ม

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

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

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

การให้บริการซอฟต์แวร์ (Software as a Service: SaaS) หมายความว่า หมวดหมู่ของบริการคลาวด์ที่ผู้ใช้บริการสามารถใช้งานแอปพลิเคชันที่ผู้ให้บริการจัดเตรียมไว้ได้

ข้อมูลที่สามารถเปิดเผยได้ (Official Data) หมายความว่า ข้อมูลที่สร้าง ประมวลผล ส่ง หรือรับของหน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้อง ซึ่งอาจก่อให้เกิดความเสียหายได้ไม่เกินความเสียหายในระดับต่ำ หากมีการละเมิดความปลอดภัยจะมีการใช้มาตรฐานการควบคุมที่สามารถคุ้มครองข้อมูลให้มีความปลอดภัยจากการโจมตีในรูปแบบต่าง ๆ 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 ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ มีความเกี่ยวข้องกับกฎหมายหรือแนวปฏิบัติ ดังนี้

1) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มาตรา 4 เพื่อให้การบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวกรวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน (2) การพัฒนามาตรฐาน

หลักเกณฑ์ และวิธีการเกี่ยวกับระบบดิจิทัล และพัฒนาโครงสร้างพื้นฐานด้านดิจิทัลที่จำเป็น ให้เป็นไปตามมาตรฐานสากล เพื่อสร้างและพัฒนากระบวนการทำงานของหน่วยงานของรัฐให้มีความสอดคล้องและมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกัน รวมทั้งมีความมั่นคงปลอดภัยและน่าเชื่อถือ โดยมีการบูรณาการและสามารถทำงานร่วมกันอย่างเป็นเอกภาพเกิดการพัฒนาการบริการภาครัฐที่มีประสิทธิภาพและนำไปสู่การบริหารราชการและการบริการประชาชนแบบบูรณาการ รวมทั้งให้ประชาชนเข้าถึงได้โดยสะดวก

2) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง กรอบแนวทางการบริหารจัดการระบบคลาวด์ภาครัฐ หน่วยงานของรัฐต้องจัดให้มี การบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล ซึ่งมีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัย และมีธรรมาภิบาล จึงจำเป็นต้องมีกรอบแนวทางการบริหารจัดการระบบคลาวด์ภาครัฐ สนับสนุนให้หน่วยงานของรัฐสามารถพิจารณาการใช้คลาวด์เป็นหลักเพื่อมุ่งสู่การเป็นรัฐบาลดิจิทัลต่อไป
3) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อการใช้บริการคลาวด์สาธารณะให้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
4) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการใช้บริการคลาวด์ พ.ศ. 2562 เนื่องจากมีการให้บริการธุรกรรมทางอิเล็กทรอนิกส์มีการใช้บริการคลาวด์ (Cloud Computing) อย่างแพร่หลาย โดยอาศัยจากการให้บริการคลาวด์จากผู้ประกอบการเพื่อให้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่ใช้บริการคลาวด์ มีความมั่นคงปลอดภัย ความน่าเชื่อถือ และมาตรฐานในการให้บริการ ซึ่งเป็นที่ยอมรับในระดับสากล
5) มติคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ เรื่อง แนวทางการดำเนินการตามมติคณะรัฐมนตรี เกี่ยวกับการจัดซื้อจัดจ้างหรือเช่าใช้บริการระบบคลาวด์ ประจำปีงบประมาณ พ.ศ. 2568 การกำหนดแนวทางทางการดำเนินการตามมติคณะรัฐมนตรี เกี่ยวกับการจัดซื้อจัดจ้างหรือเช่าใช้บริการระบบคลาวด์ของหน่วยงานภาครัฐ
6) ประกาศสำนักคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการใช้บริการคลาวด์สาธารณะที่มีศูนย์ข้อมูลหลักในประเทศไทย พ.ศ. 2567
7) ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ข้อเสนอแนะแนวทางการจัดทำนิติกรรมหรือสัญญาในรูปแบบอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
8) ประกาศคณะกรรมการความร่วมมือป้องกันการทุจริต เรื่อง วงเงินในการจัดซื้อจัดจ้างและมาตรฐานขั้นต่ำของนโยบายและแนวทางป้องกันการทุจริตในการจัดซื้อจัดจ้างที่ผู้ประกอบการต้องจัดให้มีตามมาตรา 19 แห่งพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560

2. มาตรฐาน กฎระเบียบ และแนวปฏิบัติสากลที่เกี่ยวข้องกับการบริหารจัดการบริการคลาวด์

2.1 มาตรฐาน และกฎระเบียบที่เกี่ยวข้อง

มาตรฐาน มีบทบาทสำคัญอย่างยิ่งในการตัดสินใจเลือกใช้บริการคลาวด์ เนื่องจาก การดำเนินงานของผู้ให้บริการคลาวด์ ส่งผลโดยตรงต่อประสิทธิภาพ ความปลอดภัย และความสำเร็จของการนำเทคโนโลยีคลาวด์ไปใช้งานในภารกิจและกิจกรรมต่าง ๆ ของผู้ใช้บริการ การปฏิบัติตามมาตรฐานที่กำหนดช่วยให้องค์กรมีความมั่นใจในการใช้บริการ และลดความเสี่ยงที่อาจเกิดขึ้นได้

สำหรับประเทศไทย ข้อกำหนดเชิงมาตรฐานสำคัญที่มีอยู่ในปัจจุบัน ซึ่งเป็นแนวทางในการคัดเลือกและกำกับดูแลผู้ให้บริการคลาวด์ มีดังนี้

1) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
2) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวทางการใช้บริการคลาวด์ พ.ศ. 2562 ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)
3) คู่มือการเลือกใช้บริการ Cloud Computing ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
4) ข้อเสนอแนะเชิงนโยบาย กฎระเบียบ มาตรการ มาตรฐานที่เกี่ยวข้องกับการให้และการใช้บริการระบบคลาวด์ที่เหมาะสมสำหรับหน่วยงานภาครัฐ ของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (DE) และมูลนิธิสถาบันวิจัยเพื่อการพัฒนาประเทศไทย (ทีดีอาร์ไอ)

ข้อกำหนดเชิงมาตรฐานต่าง ๆ ข้างบน สามารถสรุป มาตรฐานที่ผู้ให้บริการคลาวด์ควรได้รับการรับรอง เพื่อใช้ในการคัดกรองผู้ให้บริการคลาวด์ โดยแบ่งออกเป็น 5 ด้านหลัก ดังนี้

2.1.1 ด้านการขออนุญาตและการปฏิบัติตามกฎหมาย (Licensing & Legal Compliance)

ในการประกอบธุรกิจการให้บริการคลาวด์ ผู้ให้บริการมีความจำเป็นต้องดำเนินการให้ถูกต้องตามกฎหมายและปฏิบัติตามกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด รวมถึงการขออนุญาตต่าง ๆ เพื่อให้การดำเนินงานเป็นไปอย่างโปร่งใสและชอบด้วยกฎหมาย ตัวอย่างเช่น

- ใบอนุญาตประกอบธุรกิจ จากกรมพัฒนาธุรกิจการค้า (DBD)
- ใบอนุญาตประกอบกิจการโทรคมนาคม จากสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) สำหรับผู้ประกอบการที่มีการจัดตั้งศูนย์ข้อมูลหรือ Data Center และต้องขออนุญาตตามที่กำหนด

2.1.2 ด้านการรักษาความมั่นคงปลอดภัยในการใช้คลาวด์ (Cloud Security)

ด้านนี้มีความสำคัญสูงสุดสำหรับการให้บริการแก่หน่วยงานของรัฐ เนื่องจากเป็นส่วนที่สร้างความมั่นใจแก่ประชาชนผู้ใช้งานแพลตฟอร์มของภาครัฐ การรักษาความมั่นคงปลอดภัยสำหรับบริการคลาวด์ที่ให้บริการแพลตฟอร์มควรเป็นไปตามมาตรฐานที่ได้รับการยอมรับ ซึ่งรวมถึง มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ของ สกมช. หรือสามารถใช้ มาตรฐานสากลที่มีความเทียบเท่าหรือดีกว่า เช่น

- ISO/IEC 27001 (Information Security Management System - ISMS): มาตรฐานสากลที่ได้รับการยอมรับอย่างกว้างขวางที่สุดสำหรับการจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ผู้ให้บริการคลาวด์สามารถระบุ จัดการ และลดความเสี่ยงด้านความปลอดภัยสารสนเทศได้อย่างมีประสิทธิภาพ
- ISO/IEC 27017 (Cloud Security Controls): มาตรฐานการรักษาความปลอดภัยข้อมูลของการประมวลผลระบบคลาวด์ ซึ่งเป็นการปรับใช้การควบคุมความปลอดภัยข้อมูลที่เพิ่มเติมจากมาตรฐาน ISO/IEC 27001 และ ISO/IEC 27002 ที่ผู้ให้บริการคลาวด์จำเป็นต้องมีเพื่อสร้างความน่าเชื่อถือให้แก่ผู้ใช้บริการ
- CSA STAR: Cloud Security Alliance: มาตรฐานที่ครอบคลุมเรื่องความโปร่งใสและการตรวจสอบที่เข้มงวดตาม Cloud Controls Matrix (CCM) ซึ่งเป็นชุดข้อกำหนดด้านความปลอดภัยที่ผู้ให้บริการต้องปฏิบัติตาม เพื่อสร้างความน่าเชื่อถือให้แก่ผู้ใช้บริการคลาวด์ในเรื่องความปลอดภัย

มาตรฐานอื่น ๆ ที่อาจพิจารณาเลือกใช้เพื่อให้สอดคล้องกับภารกิจของหน่วยงาน หรือเฉพาะด้านตามความเหมาะสม (เช่น FedRAMP สำหรับบริการคลาวด์ในสหรัฐอเมริกา, NIST Cybersecurity Framework)

2.1.3 ด้านการบริหารจัดการบริการ (Service Management)

การบริหารจัดการบริการคลาวด์ เป็นสิ่งสำคัญอย่างยิ่งที่ช่วยสร้างความมั่นใจแก่หน่วยงานภาครัฐว่าบริการจากผู้ให้บริการคลาวด์จะดำเนินไปได้อย่างราบรื่น มีแผนรองรับเมื่อเกิดปัญหา และสามารถลดความเสี่ยงจากการหยุดชะงักของบริการ มาตรฐานที่เกี่ยวข้องในด้านนี้คือ

- ISO/IEC 20000 (IT Service Management): มาตรฐานสากลนี้กำหนดข้อกำหนดสำหรับ ระบบการบริหารจัดการบริการสารสนเทศ (Service Management System - SMS) ครอบคลุมการวางแผน การออกแบบ การส่งมอบ การดำเนินงาน และการปรับปรุงบริการอย่างต่อเนื่อง มาตรฐาน ISO/IEC 20000 ให้ความสำคัญกับการทำความเข้าใจ การตกลงร่วมกัน และการบรรลุความต้องการของผู้ใช้บริการ โดยมีกลไกในการรายงานผลและตรวจสอบคุณภาพบริการที่ส่งมอบอย่างสม่ำเสมอ ซึ่งจะผลักดันให้เกิดการปรับปรุงกระบวนการและเพิ่มความพึงพอใจของผู้ใช้บริการ

สำหรับผู้ให้บริการคลาวด์ (Cloud Provider) หรือตัวแทน ที่มีความประสงค์จะให้บริการในรูปแบบ Managed Service แก่หน่วยงานของรัฐ เช่น การสนับสนุนการนำเข้า ประมวลผล และบริหารจัดการข้อมูล การมีมาตรฐาน ISO/IEC 20000 (IT Service Management) ถือเป็นสิ่งสำคัญอย่างยิ่ง

การได้รับการรับรองมาตรฐานนี้แสดงให้เห็นว่าผู้ให้บริการมี กระบวนการจัดการบริการ (Service Management Processes) ที่เป็นระบบ มีประสิทธิภาพ และเป็นไปตามแนวปฏิบัติที่เป็นที่ยอมรับในระดับสากล ประโยชน์ของการมีมาตรฐาน ISO/IEC 20000 สำหรับผู้ให้บริการคลาวด์ หรือตัวแทน

- สร้างความน่าเชื่อถือและความมั่นใจ: การมีมาตรฐานรับรองแสดงถึงความมุ่งมั่นในการให้บริการที่มีคุณภาพและสอดคล้องกับข้อกำหนด ทำให้หน่วยงานภาครัฐมีความมั่นใจในการเลือกใช้บริการมากยิ่งขึ้น
- รับประกันคุณภาพและประสิทธิภาพของบริการ: มาตรฐานนี้ช่วยให้ผู้ให้บริการสามารถส่งมอบบริการได้อย่างสอดคล้อง โปร่งใส และมีประสิทธิภาพ ทำให้หน่วยงานภาครัฐได้รับบริการที่ตรงตามความคาดหวังและข้อตกลงระดับบริการ (SLA) ที่กำหนดไว้
- ลดความเสี่ยง: การจัดการบริการที่เป็นระบบช่วยลดความเสี่ยงในการดำเนินงาน ปัญหาที่อาจเกิดขึ้น และรับประกันความต่อเนื่องของบริการ
- การปรับปรุงอย่างต่อเนื่อง: มาตรฐานส่งเสริมให้มีการทบทวนและปรับปรุงกระบวนการบริการอยู่เสมอ เพื่อให้สอดรับกับการเปลี่ยนแปลงของเทคโนโลยีและความต้องการของผู้ใช้บริการ

ดังนั้น การที่ผู้ให้บริการคลาวด์หรือตัวแทน มีการรับรองมาตรฐาน ISO/IEC 20000 จะช่วยให้การบริการเป็นไปอย่างมีมาตรฐาน สร้างความน่าเชื่อถือ และตอบโจทย์ความต้องการของหน่วยงานภาครัฐในการนำเทคโนโลยีคลาวด์มาใช้ได้อย่างมีประสิทธิภาพและปลอดภัย

นอกจาก ISO/IEC 20000 แล้ว มาตรฐานอื่น ๆ ที่อาจพิจารณาเลือกใช้เพื่อให้สอดคล้องกับภารกิจของหน่วยงาน หรือเฉพาะด้านตามความเหมาะสม (เช่น ITIL ซึ่งเป็นกรอบแนวทางปฏิบัติสำหรับการบริหารจัดการบริการ IT) ก็สามารถนำมาประกอบการพิจารณาได้เช่นกัน

2.1.4 ด้านการป้องกันข้อมูลส่วนบุคคล (Data Protection/Privacy)

การปกป้องข้อมูลมีความสำคัญอย่างยิ่งต่อการให้บริการของภาครัฐ โดยเฉพาะอย่างยิ่งข้อมูลบางประเภทที่มีความละเอียดอ่อนและต้องดำเนินการตามระเบียบหรือกฎหมายที่เกี่ยวข้อง การปกป้องข้อมูลควรมีการดำเนินการที่เทียบเท่ามาตรฐานอย่างน้อยดังนี้

- ISO/IEC 27018 (Protection of Personal Data in Cloud): หลักปฏิบัติที่มุ่งเน้นการปกป้องข้อมูลส่วนบุคคลบนคลาวด์ ซึ่งเป็นไปตามมาตรฐานความปลอดภัยของข้อมูล ISO/IEC 27002 โดยเน้นการปกป้องข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ (Personally Identifiable Information - PII) จึงเป็นมาตรฐานที่เหมาะกับผู้ให้บริการคลาวด์ที่มีการประมวลผลข้อมูลส่วนบุคคล
- ISO/IEC 27701 (Privacy Information Management System - PIMS): มาตรฐานสากลที่เกี่ยวข้องกับการควบคุมความเป็นส่วนตัวของข้อมูล ซึ่งเป็นส่วนหนึ่งของมาตรฐาน ISO/IEC 27001 ที่เน้นการควบคุมความเป็นส่วนตัวในระบบบริหารความปลอดภัยข้อมูล (ISMS) มาตรฐานนี้ช่วยในการสร้างโครงสร้างและกระบวนการที่เหมาะสมเพื่อใช้ในการควบคุมความเป็นส่วนตัวของข้อมูลในการประมวลผลข้อมูลส่วนตัวของผู้ใช้บริการคลาวด์

มาตรฐานอื่น ๆ ที่อาจพิจารณาเลือกใช้เพื่อให้สอดคล้องกับภารกิจของหน่วยงาน หรือเฉพาะด้านตามความเหมาะสม (เช่น GDPR สำหรับข้อมูลพลเมืองยุโรป, CCPA สำหรับข้อมูลพลเมืองแคลิฟอร์เนีย หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลของไทย)

ทั้งนี้มาตรฐานที่กล่าวมาทั้งหมดนั้น เป็นมาตรฐานที่โดยปกติผู้ให้บริการคลาวด์จะทำการตรวจประเมินผ่านหน่วยงานที่ดำเนินการตรวจประเมิน (Certified Body) เพื่อให้ได้รับการรับรองจากหน่วยงานรับรอง (Accreditation Body) เป็นสิ่งที่สร้างความมั่นใจให้กับผู้ใช้บริการคลาวด์อยู่แล้ว โดยทั่วไปหน่วยกำกับดูแล (Regulation) จึงมักตรวจจากหน่วยงานรับรอง ว่าผู้ให้บริการคลาวด์ได้รับใบรับรองอย่างถูกต้องโดยไม่จำเป็นต้องดำเนินการตรวจประเมินเพิ่มเติมอีก เพื่อให้สามารถดำเนินการได้อย่างถูกต้องและรวดเร็ว และไม่ผิดไปจากวัตถุประสงค์ที่ต้องการให้บัญชีผู้ให้บริการคลาวด์ถูกนำไปใช้ในกระบวนการจัดซื้อจัดจ้างได้

มาตรฐานที่จำเป็นขั้นต่ำที่กำหนดสามารถเทียบเคียงได้กับด้าน ต่าง ๆ ที่ระบุไว้ โดยสามารถแบ่งมิติออกเป็นกลุ่มของประเภทของข้อมูลหรือระบบสารสนเทศตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 ประกอบด้วย ผลกระทบระดับต่ำ (สีเหลือง) ผลกระทบระดับกลาง (สีส้ม) ผลกระทบระดับสูง (สีแดง) โดยมีรายละเอียดตามตาราง

มาตรฐานในด้านต่าง ๆ สำหรับผู้ให้บริการคลาวด์	CSA STAR	ISO/IEC 20000	ISO/IEC 27001	ISO/IEC 27701	ISO/IEC 27017	ISO/IEC 27018
ข้อมูลหรือระบบสารสนเทศซึ่งมีผลกระทบระดับต่ำ	✔	✔	✔	-	-	-
ข้อมูลหรือระบบสารสนเทศซึ่งมีผลกระทบระดับกลาง	✔	✔	✔	✔	-	-
ข้อมูลหรือระบบสารสนเทศซึ่งมีผลกระทบระดับสูง	✔	✔	✔	✔	✔	✔

ตารางที่ 1 ตารางแสดงมาตรฐานจำแนกตามด้านต่าง ๆ (สำหรับผู้ให้บริการคลาวด์)

มาตรฐานในด้านต่าง ๆ สำหรับตัวแทนและอื่น ๆ	ISO/IEC 20000	CSA STAR	ISO/IEC 27001	ISO/IEC 27701	ISO/IEC 27017	ISO/IEC 27018
ข้อมูลหรือระบบสารสนเทศซึ่งมีผลกระทบระดับต่ำ	✔	-	-	-	-	-
ข้อมูลหรือระบบสารสนเทศซึ่งมีผลกระทบระดับกลาง	✔	-	-	-	-	-
ข้อมูลหรือระบบสารสนเทศซึ่งมีผลกระทบระดับสูง	✔	-	-	-	-	-

ตารางที่ 2 ตารางแสดงมาตรฐานจำแนกตามด้านต่าง ๆ (สำหรับตัวแทนและอื่น ๆ)

2.1.5 ด้านการป้องกันการทุจริตในการจัดซื้อจัดจ้าง

การป้องกันการทุจริตในการจัดซื้อจัดจ้างมีความสำคัญอย่างยิ่งในการดำเนินการจัดซื้อจัดจ้างบริการคลาวด์ของหน่วยงานของรัฐ ผู้ให้บริการคลาวด์หรือตัวแทนเป็นคู่สัญญาจัดหาบริการคลาวด์ให้แก่หน่วยงานของรัฐ ก็ต้องมีมาตรฐานหรือแนวทางป้องกันการทุจริตในการจัดซื้อจัดจ้างที่ดี เพื่อส่งเสริมความโปร่งใสในกระบวนการจัดซื้อจัดจ้างบริการคลาวด์โดยต้องปฏิบัติตามข้อกำหนดในประกาศคณะกรรมการความร่วมมือป้องกันการทุจริต เรื่อง วงเงินในการจัดซื้อจัดจ้างและมาตรฐานขั้นต่ำของนโยบายและแนวทางป้องกันการทุจริตในการจัดซื้อจัดจ้างที่ผู้ประกอบการต้องจัดให้มี ตามมาตรา 19 แห่งพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560

2.2 บทเรียนกรณีศึกษาต่างประเทศ

จากการศึกษาการบริหารจัดการบริการคลาวด์ (Supply) ในต่างประเทศ พบว่าแต่ละประเทศมีกระบวนการคัดเลือกหรือกลั่นกรองผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) หรือตัวแทนที่ผ่านมาตรฐานหรือข้อกำหนดเฉพาะของตนเอง เพื่อให้หน่วยงานภาครัฐสามารถเลือกใช้บริการคลาวด์ได้อย่างเหมาะสมและมั่นใจ

สหรัฐอเมริกา

สหรัฐอเมริกาดำเนินโครงการ **Federal Risk and Authorization Management Program (FedRAMP)** ซึ่งเป็นฐานข้อมูลสาธารณะที่รวบรวมรายชื่อบริการคลาวด์ (Cloud Service Offers: CSOs) ที่ได้รับการรับรองจากกระบวนการกลั่นกรองมาตรฐานความปลอดภัยอันเข้มงวดของ FedRAMP หน่วยงานภาครัฐสามารถเข้าสืบค้นฐานข้อมูลนี้เพื่อประกอบการพิจารณาจัดซื้อจัดจ้างบริการระบบคลาวด์

ญี่ปุ่น

ญี่ปุ่นได้จัดทำ **แนวทางกำกับดูแลกลาง** เพียงฉบับเดียว ซึ่งเชื่อมโยงกับมาตรฐานสากลและมาตรฐานภายในประเทศของญี่ปุ่นเอง โดยมีกฎระเบียบภายในประเทศที่ CSP ต้องปฏิบัติตาม หน่วยงานกำกับดูแลทั้งหมด อาทิ NISC, Digital Agency, METI, IPA, และ JASA ทำงานร่วมกันในลักษณะ **Centralized Regulation** เพื่อกำกับดูแลระบบคลาวด์ภาครัฐ

สหราชอาณาจักร

สหราชอาณาจักรใช้ **กรอบกลไก G-Cloud** ซึ่งเป็นรายการผู้ให้บริการที่ผ่านการกลั่นกรองเบื้องต้น หน่วยงานภาครัฐสามารถออกคำขอใบเสนอราคาและทำสัญญาใช้บริการระบบคลาวด์โดยตรงกับผู้ให้บริการที่อยู่ในรายการนี้

เครือรัฐออสเตรเลีย

เครือรัฐออสเตรเลียมีแพลตฟอร์ม **BuyICT** ทำหน้าที่เป็นรายการผู้ให้บริการที่ผ่านการกลั่นกรองเบื้องต้นเช่นกัน หน่วยงานผู้ใช้งานสามารถออกคำขอใบเสนอราคาและทำสัญญาใช้บริการระบบคลาวด์โดยตรงกับผู้ให้บริการที่ระบุในแพลตฟอร์ม

สหภาพยุโรป

สหภาพยุโรปได้พัฒนาแพลตฟอร์ม **CLOUD III DPS** โดยหน่วยงาน DIGIT ซึ่งเป็นแพลตฟอร์มที่รวบรวมผู้ให้บริการที่ผ่านการกลั่นกรองแล้ว หน่วยงานที่ต้องการใช้บริการสามารถ "โพสต์" ความต้องการของตนลงบนแพลตฟอร์ม เพื่อให้ผู้ให้บริการเหล่านั้นเสนอราคาและบริการ นอกจากนี้ **Cloud Infrastructure Services Providers in Europe (CISPE)** ยังได้จัดทำเอกสารเพื่อให้คำแนะนำแก่หน่วยงานที่ต้องการจัดซื้อบริการคลาวด์ แต่ขาดความเชี่ยวชาญในการร่างข้อตกลงกรอบงาน ซึ่งเอกสารนี้จะประกอบด้วยตัวอย่างและแนวปฏิบัติที่ดี รวมถึงการถอดบทเรียนในมิติต่างๆ และภาคผนวกที่แสดงตัวอย่างข้อกำหนดทางเทคนิค (Technical Requirement) และแนวทางตัวอย่างการตรวจสอบระบบและ Workload

สำหรับบริการบางประเภท ซึ่งสามารถนำมาประยุกต์ใช้ในการกำหนดเกณฑ์การพิจารณาและแนวทางการตรวจประเมิน CSP ได้

สาธารณรัฐสิงคโปร์

สิงคโปร์ดำเนินโครงการ **Government on Commercial Cloud (GCC)** โดยหน่วยงาน GovTech ซึ่งทำหน้าที่ในการจัดซื้อจัดจ้างโดยตรงกับผู้ให้บริการ และเป็นผู้กำหนดผู้ให้บริการคลาวด์ที่จะทำสัญญาจัดซื้อจัดจ้างในรูปแบบการจ่ายตามปริมาณการใช้งานจริง (Pay-per-use)

มาเลเซีย

มาเลเซียได้ริเริ่มนโยบาย **Cloud First Strategy** เพื่อส่งเสริมการใช้คลาวด์ในภาครัฐ โดยหน่วยงาน **Malaysian Administrative Modernisation and Management Planning Unit (MAMPU)** เป็นแกนหลักในการขับเคลื่อน พวกเขาได้จัดทำ **MyGovCloud** ซึ่งเป็นแพลตฟอร์มคลาวด์กลางภาครัฐที่ควบคุมโดย MAMPU เพื่อให้บริการโครงสร้างพื้นฐานคลาวด์ที่ได้มาตรฐานความปลอดภัยและสอดคล้องกับกฎระเบียบภายในประเทศ รวมถึงมีการกำหนดแนวทางการประเมินผู้ให้บริการคลาวด์เพื่อรับรองคุณสมบัติให้หน่วยงานภาครัฐสามารถเลือกใช้ได้อย่างมั่นใจ โดยเฉพาะอย่างยิ่งสำหรับข้อมูลที่มีความอ่อนไหวสูง

3. แนวทางการบริหารจัดการบริการคลาวด์ของไทย

3.1 กรอบแนวทางการบริหารจัดการคลาวด์ประเทศไทย (Framework T-Cloud)

จากผลการศึกษาการบริหารจัดการบริการคลาวด์ (Supply) ในต่างประเทศ ซึ่งแต่ละประเทศล้วนมีกระบวนการคัดเลือกหรือกลั่นกรองผู้ให้บริการคลาวด์ (CSP) หรือตัวแทนที่ผ่านเกณฑ์มาตรฐานหรือข้อกำหนดเฉพาะของตนเอง เพื่อให้หน่วยงานภาครัฐสามารถเลือกใช้บริการได้อย่างเหมาะสม ภายใต้กฎหมายและระเบียบต่าง ๆ ที่เกี่ยวข้อง ประเทศไทยจึงได้พัฒนากรอบแนวทางการบริหารจัดการคลาวด์ขึ้นในรูปแบบ **Framework T-Cloud** โดยตัว "T-Cloud" ย่อมาจาก "Thailand Cloud" ซึ่งเป็นแบบจำลองที่ประกอบด้วยกระบวนการสำคัญ 4 ขั้นตอนหลัก ดังนี้

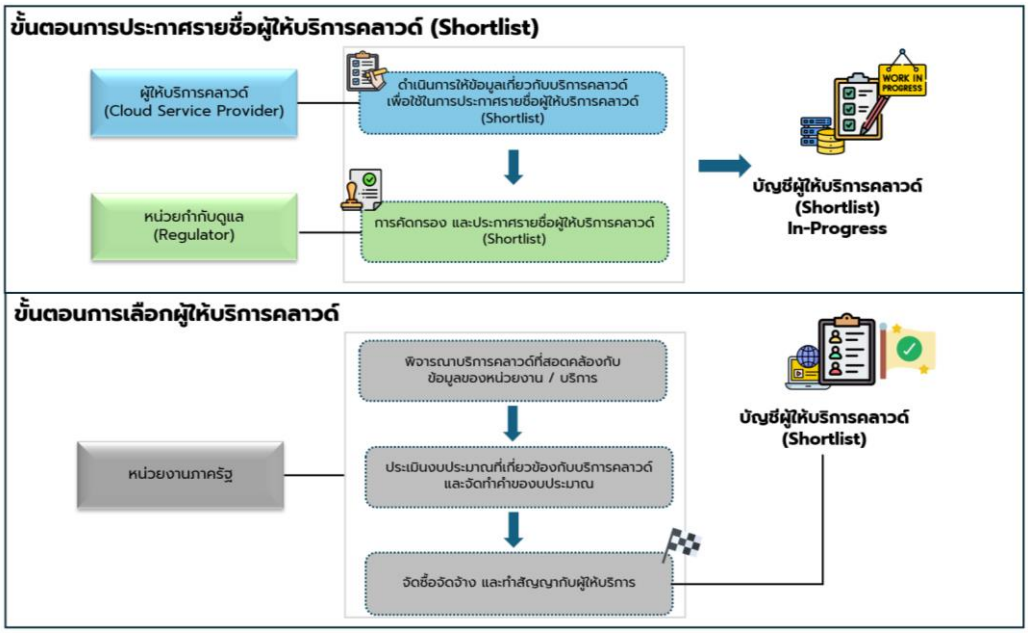
1. **การกำหนดนโยบาย:** ขั้นตอนแรกคือการวางรากฐานนโยบายและกรอบการทำงานที่ชัดเจน
2. **ด้านงบประมาณ:** การจัดสรรและบริหารจัดการงบประมาณอย่างมีประสิทธิภาพ
3. **การเตรียมการ:** การเตรียมความพร้อมของหน่วยงานและผู้ให้บริการ
4. **การดำเนินการ:** การนำนโยบายและแผนไปสู่การปฏิบัติจริง

ในแต่ละขั้นตอนดังกล่าว จะมีหน่วยงานที่เกี่ยวข้องเข้ามามีบทบาทตามภารกิจของตน อาทิ คณะกรรมการพัฒนารัฐบาลดิจิทัล, หน่วยงานกำกับดูแล, หน่วยงานภาครัฐผู้ใช้งาน และหน่วยงานบริหารจัดการบริการคลาวด์ โดยเฉพาะอย่างยิ่ง **คณะกรรมการพัฒนารัฐบาลดิจิทัล** ที่จะกำหนดแนวนโยบายหลักที่เกี่ยวข้อง ผ่านประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล มาตรฐาน และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้อง

โดยสิ่งที่สำคัญที่สุด คือ การเตรียมความพร้อมของหน่วยงานภาครัฐ และผู้ให้บริการคลาวด์ ดังจะเห็นจากแนวทางการกำหนดรายชื่อผู้ให้บริการคลาวด์ (Shortlist) สำหรับผู้ให้บริการตามระดับความสามารถในการให้บริการ (Cloud Service Provider Tier) ที่จะกล่าวถึงในหัวข้อต่อไป

3.2 รายชื่อผู้ให้บริการคลาวด์ (Shortlist)

จากการศึกษาตามกรณีศึกษาต่าง ๆ รวมถึงแบบจำลอง **Framework T-Cloud** ที่ได้กล่าวมาแล้ว จะเห็นได้อย่างชัดเจนว่าการจัดทำ **รายชื่อผู้ให้บริการคลาวด์ (shortlist)** นั้นมีความสำคัญอย่างยิ่ง เนื่องจากหน่วยงานภาครัฐควรเลือกใช้บริการจากผู้ให้บริการคลาวด์หรือตัวแทนที่อยู่ในรายชื่อที่ผ่านการประกาศแล้วเท่านั้น ซึ่งกลไกนี้จะช่วยสร้างความมั่นใจได้ว่าผู้ให้บริการคลาวด์หรือตัวแทนที่ได้รับการคัดเลือกนั้นมีมาตรฐานการให้บริการที่สามารถปฏิบัติได้จริง และยังช่วยให้หน่วยงานภาครัฐสามารถจัดทำคำของบประมาณได้อย่างราบรื่นและเป็นไปตามหลักเกณฑ์



ภาพที่ 1 กระบวนการเพื่อการประกาศรายชื่อผู้ให้บริการคลาวด์ (shortlist)

ผู้ให้บริการคลาวด์หรือตัวแทนที่ประสงค์จะให้บริการแก่หน่วยงานภาครัฐจะต้องดำเนินการตามกระบวนการที่กำหนด เพื่อให้ได้รับการประกาศในรายชื่อผู้ให้บริการคลาวด์หรือตัวแทนที่ผ่านการคัดกรอง (Shortlist) โดยมีวัตถุประสงค์หลักคือ เพื่อให้หน่วยงานภาครัฐมั่นใจในการเลือกใช้บริการ และป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการเลือกผู้ให้บริการคลาวด์หรือตัวแทนที่ไม่เป็นไปตามมาตรฐาน

บทบาทและความรับผิดชอบ

1. **บทบาทของผู้สมัคร (ผู้ให้บริการคลาวด์ หรือตัวแทน)** ผู้ให้บริการคลาวด์ หรือตัวแทนมีหน้าที่หลัก ในการประเมินตนเอง (Self-Assessment) และจัดเตรียมข้อมูลเอกสารหลักฐานที่เกี่ยวข้องอย่างครบถ้วนและเพียงพอ ซึ่งรวมถึงการระบุว่าบริการคลาวด์ที่นำเสนอมีการปฏิบัติตามกฎหมายหรือกฎระเบียบใดบ้าง โดยจะต้องกรอก แบบฟอร์ม “การเปิดเผยข้อมูลของผู้ให้บริการคลาวด์” ซึ่งเป็นชุดคำถามที่ครอบคลุมหมวดหมู่ต่าง ๆ ที่เกี่ยวข้องกับการบริการคลาวด์ ข้อมูลเหล่านี้จะถูกนำส่งให้แก่หน่วยงานกำกับดูแลเพื่อใช้ในการพิจารณา

แบบฟอร์ม “การเปิดเผยข้อมูลของผู้ให้บริการคลาวด์” มีหัวข้อต่าง ๆ ดังนี้

1) ข้อมูลติดต่อผู้ให้บริการคลาวด์ (Cloud Service Provider Contact Information)
ข้อมูลดังกล่าวเป็นข้อมูลทั่วไปสำหรับการติดต่อผู้ให้บริการคลาวด์ เช่น ที่อยู่ เบอร์โทรศัพท์
2) รายละเอียดของผู้ให้บริการคลาวด์ (Cloud Service Provider Background)
เป็นข้อมูลภาพรวมของการให้บริการคลาวด์ เช่น เป็นคลาวด์ที่ให้บริการเป็นคลาวด์สาธารณะ เป็นต้น
3) กฎหมายและการปฏิบัติตามกฎระเบียบ (Legal and Compliance)
4) ข้อมูลของผู้ให้บริการคลาวด์ที่มีการปฏิบัติตามมาตรฐาน ISO ต่าง ๆ หรือ PDPA รวมถึงระเบียบต่าง ๆ ที่มีความจำเป็นในการดำเนินการ
5) การควบคุมข้อมูล (Data Control)
เป็นข้อมูลเบื้องต้นสำหรับสถานที่การจัดเก็บข้อมูลของลูกค้าหรือหน่วยงานไว้ในประเทศ หรือนอกประเทศ ทั้งนี้รวมถึงระยะเวลาการรักษาข้อมูลในกรณีที่ลูกค้าไม่ได้ใช้บริการคลาวด์นั้นแล้ว
6) ประสิทธิภาพของผู้ให้บริการ (Provider Performance)
7) ข้อมูลเกี่ยวกับความพร้อมใช้ในการให้บริการ การใช้งานบริการอื่น ๆ ร่วมกับบริการคลาวด์ รวมถึงแผนความต่อเนื่องทางธุรกิจการให้บริการคลาวด์
8) การสนับสนุนบริการ (Service support)
ข้อมูลเกี่ยวกับการแจ้งเตือนต่าง ๆ ในการใช้บริการคลาวด์ การดำเนินการในเรื่องความช่วยเหลือผู้ใช้บริการคลาวด์ในกรณีที่เกิดปัญหาขึ้น หรือมีความจำเป็นในการโยกย้ายข้อมูล
9) การกำหนดค่าความปลอดภัย (Security Configurations)
ข้อมูลเกี่ยวกับการบังคับใช้เรื่องการกำหนดค่าความปลอดภัย การปรับแต่ค่ากำหนดความปลอดภัยในกรณีที่บริการคลาวด์สาธารณะ และต้องปรับให้สามารถใช้กับผู้ใช้บริการคลาวด์ที่มีความพิเศษ
10) ความยืดหยุ่นของบริการ (Service Elasticity)
ข้อมูลเกี่ยวกับการเพิ่มทรัพยากรให้อัตโนมัติแบบชั่วคราว กรณีที่ยังไม่สามารถปรับเปลี่ยนค่าใช้บริการคลาวด์ที่สูงขึ้นได้แบบทันที หรือการเชื่อมต่ออินเทอร์เน็ตที่มีมากกว่า 1 เส้นทางเพื่อช่วยกรณีที่เกิดปัญหา

โดยแนวทางการเปิดเผยข้อมูลของผู้ให้บริการคลาวด์ และตัวอย่างแบบฟอร์มการเปิดเผยข้อมูลของผู้ให้บริการคลาวด์ สามารถทราบรายละเอียดได้ในบทที่ 4

2. บทบาทของผู้ตรวจประเมิน (หน่วยงานกำกับดูแล) หน่วยงานกำกับดูแลจะทำหน้าที่ตรวจสอบและคัดกรองข้อมูลและเอกสารหลักฐานที่ได้รับจากผู้สมัครเป็นหลัก เพื่อประเมินความเหมาะสมในการให้บริการคลาวด์แก่ภาครัฐ โดยจะพิจารณาจากหลักการประเมินที่มีความสำคัญ เช่น

- การควบคุมข้อมูล (Data Control): มาตรการและนโยบายในการจัดการและปกป้องข้อมูลของผู้ใช้บริการ
- การกำหนดค่าความปลอดภัย (Security Configuration): มาตรฐานและแนวปฏิบัติด้านความปลอดภัยที่ผู้ให้บริการนำมาใช้
- การปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้อง (Compliance): การยืนยันว่าบริการเป็นไปตามข้อกำหนดทางกฎหมายของประเทศไทย

ขั้นตอนการตรวจประเมินของผู้ตรวจประเมิน

กระบวนการตรวจประเมินของผู้ตรวจประเมินจะดำเนินการอย่างเป็นระบบเพื่อให้มั่นใจในความถูกต้องและครบถ้วนของข้อมูลที่ได้รับจากผู้ให้บริการคลาวด์ โดยมีขั้นตอนหลักดังนี้

1. การตรวจสอบเอกสารเบื้องต้น (Initial Document Review)
    - รับและทบทวนแบบฟอร์มการเปิดเผยข้อมูล: ตรวจสอบความครบถ้วนของข้อมูลและเอกสารที่ผู้สมัครส่งมา เช่น ใบอนุญาตประกอบธุรกิจ, ใบรับรองมาตรฐานต่าง ๆ (เช่น ISO 27001, ISO 20000), นโยบายความปลอดภัย, แผนการกู้คืนระบบจากภัยพิบัติ (DRP) และนโยบายความเป็นส่วนตัวของข้อมูล
    - การยืนยันข้อมูลจากแหล่งอ้างอิงภายนอก: หากจำเป็น อาจมีการตรวจสอบข้อมูลบางส่วนกับหน่วยงานที่ออกใบรับรองมาตรฐาน หรือแหล่งข้อมูลสาธารณะอื่น ๆ เพื่อยืนยันความถูกต้อง
2. การวิเคราะห์และประเมินคุณสมบัติ (Qualification Analysis & Assessment)
    - ประเมินตามเกณฑ์ที่กำหนด: ผู้ตรวจประเมินจะนำข้อมูลที่ได้มาวิเคราะห์ตามเกณฑ์การคัดเลือกที่ได้กำหนดไว้ เช่น เกณฑ์ด้านความปลอดภัย, ประสิทธิภาพ, การบริหารจัดการ, และการปฏิบัติตามกฎหมาย
    - ระบุช่องว่างหรือข้อสงสัย: หากพบข้อมูลที่ไม่ครบถ้วน ขัดแย้ง หรือมีข้อสงสัย ผู้ตรวจประเมินจะรวบรวมประเด็นเหล่านี้เพื่อสอบถามเพิ่มเติม
3. การตรวจสอบ, การขอข้อมูล และการเข้าถึง (Review, Information Request, and Access)
    - การสื่อสารกับผู้สมัคร: ติดต่อผู้ให้บริการคลาวด์เพื่อขอคำชี้แจงหรือเอกสารหลักฐานเพิ่มเติมในประเด็นที่มีข้อสงสัยหรือข้อมูลไม่เพียงพอ
    - การสัมภาษณ์หรือนำเสนอ: ในบางกรณี อาจมีการจัดให้มีการสัมภาษณ์หรือการนำเสนอจากผู้ให้บริการคลาวด์ เพื่อให้ได้ข้อมูลเชิงลึกและทำความเข้าใจในบริการได้ดียิ่งขึ้น รวมถึงอาจจะต้องเข้าถึงอุปกรณ์ พื้นที่ บุคลากร และผู้รับจ้างของผู้ขอรับการตรวจประเมินตามความเหมาะสม
4. การจัดทำรายงานผลการประเมิน (Assessment Report Generation)
    - สรุปผลการประเมิน: จัดทำรายงานสรุปผลการประเมินผู้ให้บริการคลาวด์แต่ละรายโดยระบุจุดแข็ง จุดที่ต้องปรับปรุง และข้อจำกัด (ถ้ามี)
    - ข้อเสนอแนะ: นำเสนอข้อเสนอแนะว่าผู้ให้บริการรายใดสมควรได้รับการประกาศในรายชื่อ Shortlist และด้วยเงื่อนไขใด

การเจรจาต่อรอง และการจัดทำข้อตกลงระดับรัฐบาล

นอกจากนี้ รัฐบาลอาจกำหนดหน่วยงานกลางผู้ทำหน้าที่เจรจาต่อรอง ในประเด็นสำคัญต่าง ๆ กับผู้ให้บริการคลาวด์ที่ผ่านการคัดกรอง เพื่อให้ได้ข้อตกลงที่เป็นประโยชน์สูงสุดต่อหน่วยงานภาครัฐ รวมถึงการพิจารณาจัดทำข้อตกลงในรูปแบบ Whole-of-Government ตามความจำเป็น ประเด็นการเจรจาต่อรองที่สำคัญได้แก่

- ข้อตกลงระดับการให้บริการ (Service Level Agreement - SLA): การเจรจากำหนดตัวชี้วัดประสิทธิภาพ, ความพร้อมใช้งาน, ระยะเวลาการแก้ไขปัญหา (Resolution Time), และบทลงโทษหากไม่เป็นไปตามข้อตกลง
- การจัดเก็บและบริหารจัดการข้อมูล (Data Storage & Management): การเจรจาเกี่ยวกับตำแหน่งที่ตั้งของศูนย์ข้อมูล, นโยบายการสำรองและกู้คืนข้อมูล, การเข้ารหัสข้อมูล, และการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- การเจรจาด้านราคาและรูปแบบการคิดค่าบริการ (Pricing & Billing Models): การต่อรองราคา, โครงสร้างค่าใช้จ่าย (เช่น Pay-as-you-go, Reserved Instances), ส่วนลดสำหรับปริมาณมาก (Volume Discounts), และความโปร่งใสของบิลลิ่ง
- ข้อกำหนดด้านความปลอดภัยและการกำกับดูแลเพิ่มเติม (Additional Security & Governance Requirements): การเจรจาเพื่อเพิ่มข้อกำหนดด้านความปลอดภัยหรือการตรวจสอบที่เฉพาะเจาะจงตามความต้องการของหน่วยงานภาครัฐ
- เงื่อนไขการออกจากระบบคลาวด์ (Exit Strategy Conditions): การกำหนดเงื่อนไขและกระบวนการสำหรับการย้ายข้อมูลและบริการออกจากผู้ให้บริการคลาวด์ (Data Portability and Migration Assistance) เพื่อป้องกันปัญหา Vendor Lock-in

ประโยชน์ของการคัดกรองเพื่อหน่วยงานภาครัฐ

การจัดทำและประกาศ รายชื่อผู้ให้บริการคลาวด์ที่ผ่านการคัดกรอง (Shortlist) นี้ จะส่งผลประโยชน์อย่างมากต่อหน่วยงานภาครัฐ ดังนี้

- สร้างความมั่นใจ: หน่วยงานภาครัฐสามารถเลือกผู้ให้บริการจากบัญชีที่ได้รับการรับรองและตรวจสอบแล้ว ทำให้มั่นใจในคุณภาพและความปลอดภัยของบริการ
- อำนวยความสะดวกในการจัดซื้อจัดจ้าง: ช่วยลดขั้นตอนและเวลาในการตรวจสอบคุณสมบัติของผู้ให้บริการเบื้องต้น ทำให้สามารถดำเนินการตามกลไกงบบูรณาการดิจิทัลภาครัฐ และดำเนินการจัดซื้อจัดจ้าง รวมถึงทำสัญญากับผู้ให้บริการคลาวด์ได้อย่างรวดเร็วและเป็นไปตามหลักเกณฑ์ที่กำหนด
- ลดความเสี่ยง: การคัดกรองตั้งแต่ต้นทางและการเจรจาต่อรองเชิงรุกช่วยลดความเสี่ยงด้านความปลอดภัย การปฏิบัติตามกฎระเบียบ และคุณภาพของบริการที่อาจเกิดขึ้นในภายหลัง

3.3 คุณสมบัติของผู้ให้บริการคลาวด์และการจัดระดับความสามารถในการให้บริการ (Cloud Service Provider Tier)

คณะกรรมการพัฒนารัฐบาลดิจิทัลได้มีมติเห็นชอบกรอบหลักเกณฑ์และเงื่อนไขในการตรวจประเมินและบริหารจัดการคลาวด์ของผู้ให้บริการคลาวด์ โดยให้ความสำคัญกับการ **กำหนดมาตรฐานผู้ให้บริการแบบแบ่งชั้น (Tiered Security)** เพื่อกำหนดมาตรการทางเทคนิคและการรักษาความมั่นคงปลอดภัยให้สอดคล้องกับระดับความสำคัญของข้อมูล

กรอบหลักเกณฑ์ดังกล่าวมีวัตถุประสงค์เพื่อให้หน่วยงานภาครัฐในฐานะผู้ใช้บริการ มีกลไกในการเปรียบเทียบระดับความสามารถของผู้ให้บริการกับข้อกำหนดมาตรฐานในด้านต่าง ๆ ซึ่งจะเป็นประโยชน์อย่างยิ่งต่อการตัดสินใจเลือกใช้บริการ โดยช่วยสร้างความมั่นใจว่าผู้ให้บริการแต่ละรายในแต่ละระดับชั้น (Tier) มีขีดความสามารถและมาตรการป้องกันที่เพียงพอและสอดคล้องกับความเสี่ยงของข้อมูลตามข้อกำหนดพื้นฐานที่ยอมรับได้

การแบ่งระดับผู้ให้บริการคลาวด์ (Tier)

Cloud Service Provider Tier ถูกแบ่งออกเป็น 3 ระดับหลัก โดยพิจารณาจากคุณสมบัติพื้นฐาน มาตรฐานที่ได้รับการรับรอง และลำดับชั้นข้อมูลที่เหมาะสมในแต่ละระดับ ดังนี้:

1. **Cloud Service Provider Tier 1**
    - **ความเหมาะสม:** เหมาะสำหรับการให้บริการทั่วไป หรือบริการที่เกี่ยวข้องกับ **ข้อมูลที่สามารถเปิดเผยได้ (Official Data)** ของทางราชการ
    - **ตัวอย่างการใช้งาน:** การโฮสต์เว็บไซต์, แอปพลิเคชันทั่วไป, การทดสอบและพัฒนาระบบ, การจำลองระบบงานทั่วไปที่ไม่เกี่ยวกับข้อมูลสำคัญ
2. **Cloud Service Provider Tier 2**

ความเหมาะสม: เหมาะสำหรับการตอบสนองความต้องการของหน่วยงานที่ต้องจัดการ **ข้อมูลและระบบงานที่สำคัญ** ซึ่งเกี่ยวข้องกับ **ข้อมูลที่สามารถเปิดเผยได้ (Official Data) และ ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data)** ของทางราชการ ซึ่งเป็นข้อมูลในระดับชั้น ลับ (Confidential) ลับมาก (Secret) ให้ใช้คลาวด์สาธารณะ (Public Cloud) ที่มีมาตรการ**ด้าน**ความปลอดภัยสูง เช่น คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud)

- **ตัวอย่างการใช้งาน:** ระบบงานหรือบริการสำคัญของหน่วยงานที่ต้องการความมั่นคงปลอดภัยในระดับหนึ่ง เช่น ระบบฐานข้อมูลทะเบียนบางประเภท หรือแอปพลิเคชันที่ประมวลผลข้อมูลส่วนบุคคลทั่วไป

3. **Cloud Service Provider Tier 3**
    - **ความเหมาะสม:** เหมาะสำหรับหน่วยงานที่อยู่ภายใต้การควบคุมที่มีข้อกำหนดเฉพาะและข้อกำหนดด้านความปลอดภัยที่เข้มงวดยิ่งขึ้น นอกจากนี้ อาจต้องมีการปฏิบัติตามกฎระเบียบเฉพาะด้านร่วมกับการควบคุมพื้นฐาน โดยบริการในระดับนี้เกี่ยวข้องกับ**ข้อมูลที่**

ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) ซึ่งเป็นข้อมูลในระดับชั้น ลับที่สุด ของทางราชการ **เท่านั้น**

- **ตัวอย่างการใช้งาน:** ระบบงานหรือบริการที่สำคัญและมีความอ่อนไหวสูง ซึ่งเกี่ยวข้องกับข้อมูลลับมากหรือลับที่สุด เช่น ระบบงานด้านความมั่นคงของชาติ, ข้อมูลทางการเงินลับสุดยอด, หรือระบบที่เกี่ยวข้องกับการบริหารจัดการโครงสร้างพื้นฐานสำคัญของประเทศ

องค์ประกอบและความสัมพันธ์ระหว่างคุณสมบัติ มาตรฐาน และลำดับชั้นข้อมูล เมื่อแบ่งออกตาม Tier สามารถแบ่งออกตามด้านต่าง ๆ

	Cloud Service Provider Tier 1	Cloud Service Provider Tier 2	Cloud Service Provider Tier 3
คุณสมบัติ	1. เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย และมีทุนจดทะเบียน โดยจะต้องพิจารณามูลค่าของทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ทำข้อตกลง 2. กรณีเป็นตัวแทนจัดจำหน่ายจะต้องมีหนังสือแต่งตั้งจากผู้ให้บริการคลาวด์ หรือผู้จัดจำหน่ายประเภท Distributor ของผู้ให้บริการคลาวด์ต้นทาง 3. มีบริการและผลิตภัณฑ์อยู่ในกลุ่มบริการในการเลือกใช้บริการคลาวด์ พร้อมรายละเอียดและราคาต่อหน่วย		คุณสมบัติของผู้ยื่นคำขอ Tier 1-2 และ เป็นผู้ให้บริการคลาวด์อธิปไตย (Sovereign Cloud) หรือ คลาวด์แบบผสม (Hybrid Cloud) ตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กำหนด
เสถียรภาพทางการเงิน	1. เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย และมีทุนจดทะเบียน โดยจะต้องพิจารณามูลค่าของทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ทำข้อตกลง 2. หลังได้รับการตรวจประเมินแล้ว สำนักงานจะพิจารณาจาก ผลการดำเนินการและรายงานสถานะทางการเงิน อย่างต่อเนื่อง หากพบว่ามีความเสี่ยงต่อการให้บริการ ผู้ให้บริการจะต้องจัดทำรายละเอียดเพื่อชี้แจงเพิ่มเติม เช่น แผนการชดเชยหรือเยียวยาผู้ใช้บริการ		
มาตรฐานที่จำเป็น	1. CSA STAR 2. ISO/IEC 20000 3. ISO/IEC 27001 4. ISO/IEC 27701	1. CSA STAR 2. ISO/IEC 20000 3. ISO/IEC 27001 4. ISO/IEC 27701 5. ISO/IEC 27017 6. ISO/IEC 27018	1. CSA STAR 2. ISO/IEC 20000 3. ISO/IEC 27001 4. ISO/IEC 27701 5. ISO/IEC 27017 6. ISO/IEC 27018 และมาตรการรักษาความมั่นคงปลอดภัยเพิ่มเติม เช่น การใช้ isolated network

	Cloud Service Provider Tier 1	Cloud Service Provider Tier 2	Cloud Service Provider Tier 3
ระดับชั้นข้อมูลที่ให้บริการกับหน่วยงานภาครัฐได้	ข้อมูลที่สามารถเปิดเผยได้ (Official Data)	ข้อมูลที่สามารถเปิดเผยได้ (Official Data) และข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data)	ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) เท่านั้น

ตารางที่ 3 ตารางแสดงองค์ประกอบและความสัมพันธ์ระหว่างคุณสมบัติ มาตรฐาน และลำดับชั้นข้อมูล

ข้อกำหนดและมาตรการรักษาความมั่นคงปลอดภัยเพิ่มเติมสำหรับการให้บริการคลาวด์ภาครัฐ

1. ข้อกำหนดเพิ่มเติมด้านโครงสร้างพื้นฐาน (Infrastructure Requirements) สำหรับการให้บริการคลาวด์ภาครัฐ

	Cloud Service Provider Tier 1	Cloud Service Provider Tier 2	Cloud Service Provider Tier 3
Network Protection	- กำหนดสถาปัตยกรรมเครือข่ายคลาวด์ให้มีความมั่นปลอดภัยโดยใช้แนวคิดเช่น DMZ (Demilitarised Zones) และ Screened Subnets เพื่อรองรับความต้องการด้านความปลอดภัยต่างๆ - แบ่งแยกสภาพแวดล้อมเครือข่ายเพื่อจำกัดการเชื่อมต่อระหว่างเครือข่ายที่เชื่อถือได้และไม่น่าเชื่อถือ โดยใช้ ไฟร์วอลล์ที่ได้รับอนุมัติ ตามการออกแบบสถาปัตยกรรม ISMS เพื่อปกป้องข้อมูลสำคัญและบริการสำคัญ เช่น การยืนยันตัวตนผู้ใช้ - ติดตั้งไฟร์วอลล์ เพื่อป้องกันการเข้าถึงอินเทอร์เน็ตโดยตรง	ข้อกำหนดตามระดับที่ 1 และ - จำกัดการรับส่งข้อมูลทั้งขาเข้าและขาออกระหว่างเครือข่ายที่เก็บข้อมูลสำคัญและเครือข่ายที่ไม่น่าเชื่อถือ - จำกัดการรับส่งข้อมูลอินเทอร์เน็ตที่ไม่ปลอดภัยให้อยู่ในโซนที่ไม่ปลอดภัยของเครือข่ายให้บริการคลาวด์และเครือข่ายการจัดการบริการคลาวด์เท่านั้น - ห้ามไม่ให้มีการเข้าถึงระบบที่เก็บข้อมูลสำคัญจาก	ข้อกำหนดตามระดับที่ 2 และ - ส่วนประกอบของระบบที่จัดเก็บข้อมูลลูกค้า จะต้องถูกวางไว้ในโซนที่มีความปลอดภัยสูง และแยกออกจากโซนอื่นที่มีความปลอดภัยน้อยกว่า - สามารถแยกเครือข่ายการให้บริการตามกลุ่มการใช้งาน (Secure Isolated Network) ตามความเหมาะสม -

	Cloud Service Provider Tier 1	Cloud Service Provider Tier 2	Cloud Service Provider Tier 3
	ยกเว้นผ่านเซิร์ฟเวอร์ที่กำหนด - ตรวจสอบแผนภาพสถาปัตยกรรมเครือข่ายและกฎไฟร์วอลล์เป็นประจำ - ระบุสภาพแวดล้อมที่มีความเสี่ยงสูงและแผนภาพสถาปัตยกรรมเครือข่ายการไหลของข้อมูลที่อาจส่งผลกระทบต่อการปฏิบัติตามกฎระเบียบ - จำกัดการเข้าถึงระบบโครงสร้างพื้นฐานเครือข่ายที่ใช้ร่วมกัน: อนุญาตเฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้น - ใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-factor Authentication - MFA): สำหรับการเข้าถึงของผู้ใช้ระยะไกลทั้งหมด - จำกัดการเข้าถึงชั้นเวอร์ชวลไลเซชัน: รวมถึงซอฟต์แวร์จัดการไฮเปอร์ไวเซอร์ - ใช้ MFA และ/หรือ Split Control สำหรับไฮเปอร์ไวเซอร์: เพื่อจำกัดการเข้าถึง และปิดการจัดการไฮเปอร์ไวเซอร์จากระยะไกลสำหรับ	ภายนอกโดยตรงโดยเด็ดขาด - นำการตรวจสอบสถานะมาใช้งาน - ป้องกันการเปิดเผยที่อยู่ IP ภายใน - ใช้ไฟร์วอลล์เพื่อแยกส่วนระบบออกจากเครือข่ายที่ไม่น่าเชื่อถือ หรือส่วนเครือข่ายที่มีระดับความน่าเชื่อถือแตกต่างกัน	

	Cloud Service Provider Tier 1	Cloud Service Provider Tier 2	Cloud Service Provider Tier 3
	คลาวด์ที่ใช้เทคโนโลยีเวอร์ชวลไลเซชัน - ติดตั้งและกำหนดค่าไฟร์วอลล์สำหรับเครือข่ายไร้สาย: ระหว่างเครือข่ายไร้สาย โครงสร้างพื้นฐานคลาวด์ และเครือข่ายจัดการบริการคลาวด์ โดยกำหนดค่าให้ ปฏิเสธการรับส่งข้อมูลใดๆ จากสภาพแวดล้อมไร้สาย - รักษาความปลอดภัยการเข้าถึงระยะไกล Edge Node: ด้วยโปรโตคอลที่ปลอดภัย เช่น HTTPS, SSH, SFTP		
Virtual Machine (VM)	- Virtual Machines ต้องเข้ารหัส Data in Transit และ Data at Rest เพื่อป้องกันการโจรกรรมข้อมูล		
General Storage Technology	- การควบคุมการเข้าถึง (Access controls) ถูกใช้เพื่อจำกัดอุปกรณ์ที่สามารถสื่อสารกับอุปกรณ์จัดเก็บข้อมูลที่เชื่อมต่อกับเครือข่าย (Network Attached Storage devices) ได้ - มีกระบวนการสำหรับการเผยแพร่การเปลี่ยนแปลงการตั้งค่าทั้งหมด และเพื่อให้มั่นใจว่าเครือข่ายจัดเก็บข้อมูล (SAN) และสวิตช์ที่เกี่ยวข้องได้รับการตั้งค่าอย่างถูกต้อง	ข้อกำหนดตามระดับที่ 1 และ - มีการจำกัดการเข้าถึงจากอุปกรณ์ภายนอก - มีการจำกัดการทำงานของแต่ละพอร์ต (Port) - มีการยืนยันตัวตนร่วมกันระหว่างอุปกรณ์ (Mutual Authentication) - อุปกรณ์จะตอบสนองเฉพาะกับอุปกรณ์ที่ได้รับอนุญาตเท่านั้น	ข้อกำหนดตามระดับที่ 2 และ - ใช้ประโยชน์จากการกำหนดค่า Hard Zones ใน Fibre Channel Switch หรือการควบคุมที่คล้ายกัน - ใช้ประโยชน์จากการ Masking Logical Unit Numbers หรือการควบคุมที่คล้ายกันบนอุปกรณ์จัดเก็บข้อมูล หากสามารถทำได้ - ต้องมีการเข้ารหัส (Encryption) เพื่อ

	Cloud Service Provider Tier 1	Cloud Service Provider Tier 2	Cloud Service Provider Tier 3
			ปกป้องข้อมูลทั้งในขณะที่ จัดเก็บอยู่ (data at rest) และ ในระหว่างการส่งผ่าน (in transit) ระหว่างอุปกรณ์จัดเก็บข้อมูล รวมถึงที่ Edge Nodes และ Cloud Central Servers ด้วย - ผู้ให้บริการคลาวด์ (CSP) จะต้องมีทางเลือกให้ลูกค้าสามารถ ควบคุมคีย์เข้ารหัส ได้ด้วยตนเอง
การแบ่งแยกข้อมูล	ไม่มีข้อกำหนด	มีการแบ่งแยกการเข้าถึงข้อมูล log และคีย์เข้ารหัส แบบ logical	ข้อกำหนดตามระดับ 2 และ ผู้ใช้บริการสามารถกำหนดคีย์เข้ารหัสข้อมูลและสำรอง (Backup)

2. ข้อกำหนดเพิ่มเติมด้านการจัดหาและพัฒนาระบบ (System Acquisitions and Development)

ผู้ให้บริการคลาวด์ที่จำเป็นต้องจัดหา และพัฒนาระบบเพื่อใช้ในการให้บริการ เช่น บริการในรูปแบบ Software-as-a-Service (SaaS) หรือ บริการในรูปแบบ Platform-as-a-Service (PaaS) หรือ ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้อง เช่น เว็บพอร์ทัลสำหรับผู้ดูแลระบบ ให้ดำเนินการ ดังนี้

- พัฒนาแอปพลิเคชันซอฟต์แวร์ (ทั้งภายในและภายนอก รวมถึงการเข้าถึงแอปพลิเคชันผ่านเว็บสำหรับการจัดการ) ตามแนวปฏิบัติที่เป็นที่ยอมรับในอุตสาหกรรม และ ผนวกความปลอดภัยของข้อมูลเข้าตลอดวงจรชีวิตของการพัฒนาซอฟต์แวร์
- ลบบัญชีแอปพลิเคชันที่กำหนดเอง, User ID, และรหัสผ่าน ก่อนที่แอปพลิเคชันจะเริ่มใช้งานจริงหรือเผยแพร่ให้ลูกค้า
- ลบข้อมูลและบัญชีทดสอบ ก่อนที่ระบบเวอร์ชันใช้งานจริงจะเริ่มทำงาน
- ป้องกันช่องโหว่ในการเขียนโค้ดที่พบบ่อยในกระบวนการพัฒนาซอฟต์แวร์ โดยการตรวจสอบแอปพลิเคชันเทียบกับมาตรฐานอุตสาหกรรม

- ใช้การแบ่งแยกเครือข่าย สำหรับสภาพแวดล้อมการพัฒนา การทดสอบ และการใช้งานจริง
- ไม่สนับสนุนการแก้ไขแพ็กเกจซอฟต์แวร์ โดยจำกัดการแก้ไขเฉพาะที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องมีการควบคุมอย่างเข้มงวด
- กำหนดเกณฑ์การยอมรับและทำการทดสอบที่เหมาะสม กับแอปพลิเคชันในระหว่างการพัฒนาและก่อนการยอมรับ
- ตรวจสอบให้แน่ใจว่าข้อกำหนดด้านความปลอดภัยถูกพิจารณาเป็นส่วนหนึ่งของข้อกำหนดทางธุรกิจ
- ตรวจสอบความถูกต้องของข้อมูลที่ป้อนเข้าแอปพลิเคชัน เพื่อให้แน่ใจว่าข้อมูลนั้นถูกต้องและเหมาะสม
- มีกระบวนการเพื่อให้แน่ใจว่าโปรแกรม ปราศจาก Spyware, Trojan, Backdoor และโค้ดที่ไม่ได้รับอนุญาตอื่น ๆ

3. ผู้ให้บริการคลาวด์ต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer DPO) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
4. กรณีที่ผู้ให้บริการคลาวด์ใช้อุปกรณ์และระบบที่ผ่านการรับรองมาตรฐานที่กำหนดแล้ว และได้รับสิทธิในการใช้อุปกรณ์ดังกล่าว สามารถยื่นหลักฐานแสดงการรับรองมาตรฐานได้ ทั้งนี้ผู้ตรวจประเมินสามารถร้องขอเอกสารหลักฐานอื่น ๆ ได้ ทั้งนี้เป็นไปตามหลักเกณฑ์ วิธีการและเงื่อนไขการตรวจประเมินกำหนด
5. กรณีที่ผู้ให้บริการคลาวด์ไม่มีมาตรฐานการให้บริการตามข้อกำหนด ผู้ให้บริการคลาวด์จะต้องจัดให้มีการตรวจเพื่อการรับรองมาตรฐานสากล (Certification Audit) โดยมีผู้ตรวจสอบที่ได้รับอนุญาต Certified Auditors ตรวจและลงนามรับรองให้สอดคล้องกับการตรวจสอบตามมาตรฐานที่เป็นทางการ เพื่อให้การรับรอง (Certification) หรือเพื่อยืนยันความสอดคล้อง (Compliance) ของระบบหรือองค์กรกับข้อกำหนดที่เกี่ยวข้อง ทั้งนี้ต้องจัดให้มีผู้ดำเนินการและบริหารจัดการที่เป็นไปตามข้อกำหนดดังกล่าวครบถ้วนในการให้บริการ และผู้ให้บริการคลาวด์จะต้องมีมาตรฐานดังกล่าวเป็นของตนเองภายใน 1 ปีนับจากเริ่มให้บริการคลาวด์ภาครัฐ

   *** สำหรับกรณีผู้ให้บริการที่ยังไม่ได้รับการรับรองมาตรฐาน ISO/IEC 27017 แต่ผู้ให้บริการได้รับการรับรองมาตรฐาน CSA STAR Level 2/CCM การพิจารณามาตรฐานดังกล่าวให้เป็นไปตามข้อกำหนดในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567
6. มีข้อตกลงระดับการให้บริการ (Service Level Agreement (SLA)) ไม่ต่ำกว่า 99.9%
7. ผู้ให้บริการคลาวด์ต้องมีรายละเอียดสนับสนุนที่เกี่ยวกับข้อกำหนดในการโอนย้ายข้อมูลไปยังผู้ให้บริการคลาวด์รายใหม่ สรุปได้ดังนี้

   • ความสามารถในการเปลี่ยน (Capabilities to facilitate switching) เช่น การจัดเตรียมอินเทอร์เฟซแบบเปิด (Open interfaces) เพื่อให้สามารถพัฒนาเครื่องมือเชื่อมต่อได้ ซึ่งรวมถึงรองรับการโอนย้ายข้อมูลไปยัง On-Premise แบบไม่มีค่าใช้จ่ายหรือมีค่าใช้จ่ายเท่าที่จำเป็นเท่านั้น

   • ข้อกำหนดที่เกี่ยวข้องกับการโอนย้ายข้อมูลที่เหมาะสม เช่น นโยบายการนำข้อมูลออกโดยอาจการกำหนดเงื่อนไขระยะเวลาการแจ้งยกเลิกใช้บริการไม่เกิน 2 เดือน และกำหนดระยะเวลาการโอนย้าย

ข้อมูลจากระบบเก่าไปสู่ระบบใหม่ไม่เกิน 30 วัน การกำหนดสิทธิและอำนาจในการจัดการข้อมูล การระบุความเป็นเจ้าของข้อมูลและการเข้าถึงข้อมูล เช่น การระบุในสัญญาอย่างชัดเจนว่า ข้อมูลทั้งหมดเป็นของผู้ใช้บริการแต่เพียงผู้เดียว โดยผู้ให้บริการคลาวด์ไม่มีสิทธิในการนำข้อมูลนั้นไปใช้ ทำซ้ำ หรือเผยแพร่เพื่อประโยชน์ทางการค้าของตนเองหรือบุคคลที่สาม พร้อมกำหนดเงื่อนไขการเข้าถึงข้อมูลให้เข้มงวด

• การสนับสนุนทางเทคนิค เช่น เอกสารคู่มือหรือขั้นตอนการนำข้อมูลออกหรือการโอนข้อมูลจากระบบเดิมไปยังระบบใหม่

• เครื่องมือที่จำเป็น (Necessary Tools) เช่น การมีมาตรการการรองรับการส่งออกข้อมูล ที่สามารถใช้งานร่วมกันได้ (Common Specifications / Harmonised Standards) เช่น รูปแบบไฟล์มาตรฐาน หรือ API ที่เข้าถึงได้ง่าย ในกรณีที่ไม่มีมาตรการการที่ใช้งานร่วมกันได้ ผู้ให้บริการคลาวด์ต้องส่งออกข้อมูลในรูปแบบที่มีโครงสร้าง สามารถใช้งานทั่วไป และเครื่องสามารถอ่านได้ (Machine Readable)

8. จัดให้มีมาตรการ (Security Control) ด้านความมั่นคงปลอดภัยที่เหมาะสม เช่น

• Security Information and Event Management (SIEM) : ระบบที่รวบรวม วิเคราะห์ และเชื่อมโยงข้อมูลเหตุการณ์ความปลอดภัยจากแหล่งต่าง ๆ ทั่วทั้งองค์กร เพื่อช่วยตรวจจับภัยคุกคามและแจ้งเตือนแบบเรียลไทม์

• Endpoint Detection and Response (EDR) : ระบบที่เฝ้าระวังและเก็บข้อมูลกิจกรรมบนเครื่องปลายทาง (เช่น เซิร์ฟเวอร์ คอมพิวเตอร์) อย่างต่อเนื่อง เพื่อตรวจจับพฤติกรรมที่ผิดปกติ การโจมตี และช่วยในการตอบสนองอย่างรวดเร็ว

• Vulnerability Assessment (VA) : กระบวนการสแกนและประเมินระบบเพื่อค้นหาช่องโหว่ จุดอ่อนด้านความปลอดภัย หรือข้อผิดพลาดในการตั้งค่าที่อาจถูกโจมตีได้

• Penetration Testing : การทดสอบเจาะระบบ โดยจำลองการโจมตีจากผู้ไม่หวังดี เพื่อค้นหาช่องโหว่ที่สามารถถูกเจาะได้จริง และประเมินความแข็งแกร่งของมาตรการป้องกันที่มีอยู่

• Web Application Firewall : ระบบที่ออกแบบมาเพื่อปกป้อง Web Application หรือ Application โดยเฉพาะโดยจะตรวจสอบและกรองการรับส่งข้อมูล เพื่อป้องกันการโจมตีที่มุ่งเป้ามายังช่องโหว่ของเว็บไซต์โดยตรง

• Log management : กระบวนการจัดการ การรวบรวม การวิเคราะห์ และการเก็บบันทึกข้อมูลจากระบบและแอปพลิเคชันต่าง ๆ ที่เกี่ยวข้องกับการทำงานขององค์กรเพื่อให้สามารถตรวจสอบ ตรวจจับ และวิเคราะห์เหตุการณ์ที่เกิดขึ้นในระบบได้อย่างมีประสิทธิภาพ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562

• Cybersecurity Operations Center (CSOC) : ศูนย์ปฏิบัติการความปลอดภัยทางไซเบอร์ที่มีหน้าที่หลักในการเฝ้าระวัง ควบคุม วิเคราะห์ และตรวจสอบภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นในระบบ รวมถึงให้คำแนะนำแก่ผู้ดูแลระบบในการตอบสนองต่อภัยคุกคามเหล่านั้น โดยการเฝ้าระวังภัยคุกคาม

4. แนวทางการจัดเตรียมข้อมูลและเอกสารหลักฐานประกอบสำหรับการขอรับการตรวจประเมินผู้ให้บริการคลาวด์

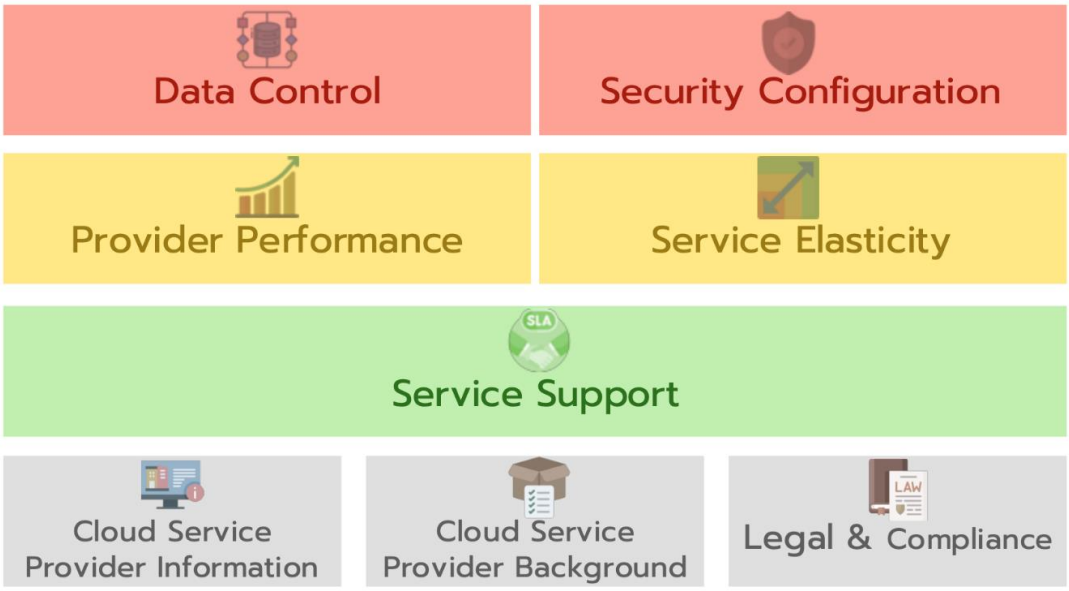
แนวทางการจัดเตรียมข้อมูลและเอกสารหลักฐานประกอบ นี้ จัดทำขึ้นสำหรับผู้ให้บริการคลาวด์ (Cloud Service Provider) หรือ ตัวแทน ที่ประสงค์จะเข้าร่วมในกระบวนการพิจารณาเพื่อขึ้นบัญชี รายชื่อผู้ให้บริการคลาวด์ที่ผ่านการคัดกรอง (Shortlist) สำหรับหน่วยงานภาครัฐ ซึ่งจะช่วยให้หน่วยงานภาครัฐมีตัวเลือกผู้ให้บริการคลาวด์ที่ผ่านการตรวจสอบเบื้องต้น และสามารถนำรายชื่อเหล่านี้ไปใช้ในกระบวนการจัดซื้อจัดจ้างต่อไปได้อย่างมั่นใจ

แนวทางการจัดเตรียมข้อมูลนี้มีความสำคัญดังนี้

- ลดความซับซ้อน: การกำหนดให้ผู้ให้บริการคลาวด์จัดเตรียมและกรอกข้อมูลที่เกี่ยวข้องในแบบฟอร์มมาตรฐาน ช่วยให้หน่วยงานกำกับดูแลสามารถคัดกรองผู้ให้บริการเบื้องต้นได้อย่างมีประสิทธิภาพและเป็นระบบ
- สร้างความโปร่งใส: ผู้ให้บริการคลาวด์ต้องเปิดเผยข้อมูลสำคัญที่จำเป็นต่อการตัดสินใจของหน่วยงานภาครัฐ โดยแสดงรายละเอียดเกี่ยวกับบริการ ความสามารถ และการปฏิบัติตามข้อกำหนด เพื่อให้หน่วยงานภาครัฐสามารถนำไปพิจารณาได้อย่างโปร่งใสและเป็นธรรม
- เพิ่มประสิทธิภาพในการจัดซื้อจัดจ้าง: ผู้ให้บริการคลาวด์ที่ผ่านการตรวจประเมินเบื้องต้นได้ผ่านการตรวจสอบคุณสมบัติที่สำคัญแล้ว ทำให้หน่วยงานภาครัฐสามารถใช้รายชื่อผู้ให้บริการคลาวด์ที่ผ่านการคัดกรอง (shortlist) ในการเลือกและเปรียบเทียบบริการจากผู้ให้บริการคลาวด์ได้อย่างรวดเร็วและมีประสิทธิภาพมากขึ้น

4.1 กรอบการจัดเตรียมข้อมูลและเอกสารหลักฐาน

แนวทางการจัดเตรียมข้อมูลนี้ได้กำหนดกรอบสำหรับผู้ให้บริการคลาวด์ในการรวบรวมและนำเสนอข้อมูลที่จำเป็นสำหรับการประเมินคุณสมบัติของผู้ให้บริการคลาวด์ หรือตัวแทน โดยจัดทำเป็น แบบฟอร์มการเปิดเผยข้อมูลของผู้ให้บริการคลาวด์ ซึ่งเป็นข้อมูลในด้านต่าง ๆ ที่สำคัญสำหรับการบริการคลาวด์ อาทิ ข้อมูลผู้ติดต่อผู้ให้บริการคลาวด์ (Cloud Service Provider Information) รายละเอียดของผู้ให้บริการคลาวด์ (Cloud Service Provider Background) กฎหมายและการปฏิบัติตามกฎระเบียบ (Legal and Compliance) เป็นต้น



ภาพที่ 2 เกณฑ์ที่นำมาใช้ในแนวทางการประเมินตนเอง

4.2 การอ้างอิงมาตรฐานและแนวปฏิบัติสากล

แบบฟอร์มการเปิดเผยข้อมูลของผู้ให้บริการคลาวด์ฉบับนี้ ได้รับการพัฒนาโดยอ้างอิงแนวทางและรูปแบบการเปิดเผยข้อมูลสำหรับผู้ให้บริการคลาวด์ตามมาตรฐานสากลที่เป็นที่ยอมรับจากประเทศต่าง ๆ เช่น แบบฟอร์ม Cloud Service Provider Disclosure ของสิงคโปร์ และประเทศอื่น ๆ ที่มีมาตรฐานการประเมินผู้ให้บริการคลาวด์ที่เป็นที่ยอมรับในระดับสากล

หัวข้อ	ประเทศสิงคโปร์		ประเทศอังกฤษ
1. Cloud Service Provider Information	• General Information • Certification Body Information		Information
2. Cloud Service Provider Background	• Overview • Service Model • Deployment Model • Tier		What the service is
3. Legal & Compliance	• Right to audit • Compliance		Compliance
4. Data Control	• Data ownership • Data retention	• Data Sovereignty • Non-disclosure	Hosting options and locations
5. Provider Performance	• Availability • 3rd party dependency • BCP/DR	• Liability • Shared responsibility	The levels of data backup and restore, and disaster recovery you'll provide, such as business continuity and disaster recovery plans
6. Service Support	• Change management • Self service provisioning and management portal • Incident and problem management	• Billing • Data portability • Interoperability • Access • User management • Life cycle	• Any onboarding and offboarding support you provide • Service levels like performance, availability and support hours • After sales support • Any technical requirements Outage and maintenance management • Access to data (upon exit)
7. Security Configuration	• Security configuration checks • Multi-tenancy • Hybrid cloud provisioning		Security
8. Service Elasticity	• Capacity elasticity • Network resiliency and elasticity • Storage redundancy and elasticity		Service constraints like maintenance windows or the level of customization allowed

ภาพที่ 3 หัวข้อ/เกณฑ์ที่นำมาใช้ในแนวทางการประเมินตนเองเปรียบเทียบกับของต่างประเทศ

การปรับปรุงแบบฟอร์มนี้ได้คำนึงถึงบริบทและความต้องการเฉพาะของหน่วยงานภาครัฐในประเทศไทย เพื่อให้มั่นใจว่าข้อมูลที่ผู้ให้บริการคลาวด์เปิดเผยนั้นสอดคล้องกับมาตรฐานด้านความปลอดภัย, ความยืดหยุ่น, การปฏิบัติตามข้อกำหนด, และความโปร่งใส ซึ่งจะช่วยสนับสนุนการตัดสินใจของหน่วยงานภาครัฐที่ต้องการใช้บริการคลาวด์ได้อย่างมีประสิทธิภาพและมั่นใจในคุณภาพของบริการ

4.3 แบบฟอร์มการเปิดเผยข้อมูลของผู้ให้บริการคลาวด์

ในมาตรฐานว่าด้วยเรื่องแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ฉบับนี้ ได้กำหนด แบบฟอร์มการเปิดเผยข้อมูลของผู้ให้บริการคลาวด์ ขึ้น เพื่อเป็นกรอบสำหรับ การจัดเตรียมข้อมูลและเอกสารหลักฐานประกอบการขอรับการตรวจประเมิน

แบบฟอร์มนี้เป็นแนวทางให้ผู้ให้บริการคลาวด์ ตัวแทน เตรียมข้อมูลที่จำเป็นได้อย่างเป็นระบบและเป็นมาตรฐาน โดยสามารถให้ข้อมูลตามความเหมาะสม ขอบเขต และข้อจำกัดของการให้บริการคลาวด์นั้น ๆ (ทั้งนี้ การเปิดเผยข้อมูลบางส่วนอาจเป็นไปตามข้อตกลงระหว่างผู้ให้บริการและผู้ใช้บริการ)

เพื่อให้การตรวจประเมินเป็นไปอย่างมีประสิทธิภาพและมาตรฐาน ผู้ให้บริการคลาวด์จะต้องกรอกข้อมูลและรายละเอียดตามหัวข้อต่าง ๆ ที่กำหนดไว้ในแบบฟอร์ม เพื่อนำเสนอคุณสมบัติและความสามารถของตนแก่หน่วยงานกำกับดูแล

1. ข้อมูลติดต่อผู้ให้บริการคลาวด์ (Cloud Service Provider Information) หัวข้อนี้มีวัตถุประสงค์เพื่อรวบรวมข้อมูลพื้นฐานที่เกี่ยวข้องกับผู้ให้บริการคลาวด์ ทำให้หน่วยงานของรัฐสามารถติดต่อสื่อสาร และตรวจสอบสถานะของผู้ให้บริการได้อย่างชัดเจนและเป็นทางการ โดยรวมถึงข้อมูลของบริษัทผู้ให้บริการและผู้ติดต่อที่ได้รับมอบหมาย เพื่อช่วยยืนยันความน่าเชื่อถือและสถานะขององค์กรที่ให้บริการ ประกอบไปด้วย

- **ชื่อบริษัท (Company Name)** ชื่อทางการของผู้ให้บริการคลาวด์
- **ที่อยู่หลักของบริษัท (Primary Address)** ที่อยู่สำนักงานใหญ่ของบริษัท
- **ที่อยู่เว็บไซต์ (Web Address)** ระบุลิงค์ของเว็บไซต์ของผู้ให้บริการ
- **ชื่อผู้ติดต่อ (Contact Name)** ระบุชื่อของบุคคลที่สามารถติดต่อได้
- **เบอร์ติดต่อ (Contact Number)** ระบุหมายเลขโทรศัพท์สำหรับการติดต่อ
- **อีเมลติดต่อ (Contact E-mail)** ระบุที่อยู่อีเมลสำหรับการสื่อสาร
- **ตราประทับของบริษัทและลายมือชื่อตัวแทนบริษัท (Company Chop and Representative Signature)** เพื่อยืนยันความถูกต้องของข้อมูล

2. ข้อมูลติดต่อหน่วยงานรับรอง (Certification Body Contact Information) หัวข้อนี้มีวัตถุประสงค์เพื่อบันทึกข้อมูลการติดต่อของหน่วยงานที่ทำหน้าที่รับรองมาตรฐานหรือคุณภาพการให้บริการของผู้ให้บริการคลาวด์ เพื่อยืนยันความน่าเชื่อถือของผู้ให้บริการคลาวด์ผ่านการรับรองจากหน่วยงานที่เป็นที่ยอมรับ และแสดงความโปร่งใสในกระบวนการรับรองมาตรฐานของผู้ให้บริการคลาวด์ ประกอบไปด้วย

- **ชื่อบริษัท (Company Name)** ระบุชื่อทางการของหน่วยงานรับรอง
- **ที่อยู่หลักของบริษัท (Primary Address)** ระบุที่ตั้งสำนักงานใหญ่ของหน่วยงานรับรอง

- **ที่อยู่เว็บไซต์ (Web Address)** ระบุลิงค์ของเว็บไซต์ของหน่วยงานรับรอง

- ชื่อผู้ติดต่อ (Contact Name) ระบุชื่อผู้ติดต่อของหน่วยงานรับรองที่ประสานงานได้

- **เบอร์ติดต่อ (Contact Number)** ระบุหมายเลขโทรศัพท์ของหน่วยงานรับรองที่สามารถติดต่อได้

- **อีเมลติดต่อ (Contact E-mail)** ระบุอีเมลของหน่วยงานรับรองที่ใช้ติดต่อประสานงานได้

ในส่วนที่ผ่านมา เป็นการรวบรวมข้อมูลพื้นฐานเกี่ยวกับผู้ให้บริการคลาวด์ เพื่อยืนยันตัวตนของผู้ให้บริการและสร้างช่องทางติดต่อที่ชัดเจนระหว่างหน่วยงานของรัฐและผู้ให้บริการคลาวด์

หลังจากที่ผู้ให้บริการคลาวด์ได้ระบุข้อมูลพื้นฐาน และข้อมูลของหน่วยงานรับรองเรียบร้อยแล้ว ขั้นตอนต่อไปคือ การให้รายละเอียดเกี่ยวกับผู้ให้บริการในเชิงลึก ซึ่งประกอบด้วยรูปแบบการให้บริการ (Service Model), รูปแบบการปรับใช้ และลักษณะการดำเนินงานที่สำคัญในฐานะผู้ให้บริการคลาวด์ ข้อมูลนี้จะเป็นเกณฑ์สำคัญในการประเมินความเหมาะสมและศักยภาพของผู้ให้บริการต่อความต้องการของหน่วยงานของรัฐ

3. รายละเอียดของผู้ให้บริการคลาวด์ (Cloud Service Provider Background) หัวข้อนี้มีวัตถุประสงค์เพื่อให้ผู้ให้บริการคลาวด์ ระบุรายละเอียดที่เกี่ยวข้องกับลักษณะการให้บริการ และศักยภาพขององค์กรในบริบทของการให้บริการคลาวด์แก่หน่วยงานของรัฐ เพื่อแสดงความเหมาะสมและความสามารถในการตอบสนองความต้องการของผู้ใช้บริการ โดยประกอบไปด้วยหัวข้อดังนี้

- **ภาพรวมของการให้บริการ (Overview of Service Offering)** เป็นการระบุข้อมูลสำคัญเกี่ยวกับประเภทและลักษณะของบริการที่นำเสนอ ของผู้ให้บริการคลาวด์ เพื่อช่วยให้หน่วยงานของรัฐหรือผู้ประเมินเข้าใจภาพรวมของการให้บริการอย่างชัดเจน และประเมินได้อย่างถูกต้อง

- **รูปแบบการบริการ (Service Model)** ในการจัดเตรียมข้อมูลและเอกสารหลักฐาน ผู้ให้บริการคลาวด์จะต้อง ระบุรูปแบบของบริการคลาวด์ที่นำเสนออย่างชัดเจน โดยอ้างอิงถึงประเภทของบริการตามโมเดลมาตรฐานสากล . การระบุนี้มีวัตถุประสงค์เพื่อช่วยให้ผู้ตรวจประเมินเข้าใจขอบเขตการให้บริการ และ ความเหมาะสมของบริการ สำหรับการใช้งานในบริบทต่าง ๆ ของหน่วยงานภาครัฐ ผู้ให้บริการสามารถเลือกและระบุรูปแบบบริการได้ มากกว่า 1 ตัวเลือก ตามที่บริการของตนครอบคลุม ดังนี้

  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)

- **รูปแบบการปรับใช้ (Deployment Model)** เป็นการระบุลักษณะการปรับใช้บริการคลาวด์ที่ผู้ให้บริการคลาวด์นำเสนอ โดยเน้นที่วิธีการจัดสรรทรัพยากรและการเข้าถึงบริการ ซึ่งมีความสำคัญต่อการพิจารณาความเหมาะสมของบริการคลาวด์กับความต้องการของหน่วยงานภาครัฐ โดยความหมายของรูปแบบการปรับใช้ (Deployment Model) สามารถดูได้ในบทนิยามของมาตรฐาน โดยสามารถระบุตัวเลือกได้มากกว่าหนึ่งตัวเลือก

  - คลาวด์ส่วนตัว (Private cloud)
  - ระบบคลาวด์ชุมชน/คลาวด์แบบกลุ่ม (Community cloud)
  - คลาวด์ผสม (Hybrid cloud)

- คลาวด์สาธารณะ (Public cloud)
- คลาวด์อธิปไตย (Sovereign Cloud)
- คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud)

เมื่อผู้ให้บริการคลาวด์ได้แสดงรายละเอียดเกี่ยวกับศักยภาพและลักษณะการให้บริการในภาพรวมแล้ว ขั้นตอนถัดไปคือการแสดงให้เห็นถึงการปฏิบัติตามกฎหมาย ข้อกำหนด และมาตรฐานที่เกี่ยวข้อง เพื่อสร้างความมั่นใจว่าผู้ให้บริการคลาวด์ มีความโปร่งใสและมีศักยภาพเพียงพอในการปฏิบัติตามข้อกำหนดของภาครัฐ

- **ความสามารถในการให้บริการ (Cloud Service Provider Tier)** เป็นการเปรียบเทียบระดับความสามารถของผู้ให้บริการเทียบกับข้อกำหนดพื้นฐานในด้านต่าง ๆ ซึ่งจะเป็นประโยชน์ต่อการเลือกใช้บริการ โดยให้ความมั่นใจแก่ผู้ใช้บริการว่าผู้ให้บริการสามารถปฏิบัติตามข้อกำหนดพื้นฐานขั้นต่ำที่ยอมรับสำหรับแต่ละระดับได้ สามารถระบุตัวเลือกที่สอดคล้องมากที่สุด

- ระดับ 1 (CSP Tier 1)
- ระดับ 2 (CSP Tier 2)
- ระดับ 3 (CSP Tier 3)

เมื่อผู้ให้บริการคลาวด์ได้แสดงรายละเอียดเกี่ยวกับศักยภาพและลักษณะการให้บริการในภาพรวมแล้ว ขั้นตอนถัดไปคือการแสดงให้เห็นถึงการปฏิบัติตามกฎหมาย ข้อกำหนด และมาตรฐานที่เกี่ยวข้อง เพื่อสร้างความมั่นใจว่าผู้ให้บริการคลาวด์ มีความโปร่งใสและมีศักยภาพเพียงพอในการปฏิบัติตามข้อกำหนดของภาครัฐ

4. กฎหมายและการปฏิบัติตามกฎระเบียบ (Legal & Compliance) หัวข้อนี้มีวัตถุประสงค์เพื่อให้ผู้ให้บริการคลาวด์ ระบุข้อมูลที่เกี่ยวข้องกับการปฏิบัติตามกฎหมาย ข้อกำหนด และมาตรฐานต่าง ๆ ที่เกี่ยวข้องกับการให้บริการคลาวด์ รวมถึงการแสดงให้เห็นถึงความสามารถในการปฏิบัติตามข้อกำหนดทางกฎหมายในระดับประเทศและระดับสากล เพื่อให้หน่วยงานของรัฐมั่นใจว่าผู้ให้บริการคลาวด์ปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA, GDPR) และกฎหมายความมั่นคงทางไซเบอร์ รวมถึงรวมถึงความน่าเชื่อถือของผู้ให้บริการในการปฏิบัติตามมาตรฐานสากล เช่น ISO/IEC 27001 ซึ่งประกอบไปด้วยหัวข้อที่ผู้ให้บริการคลาวด์ต้องระบุ ประกอบไปด้วย

1) สิทธิในการตรวจสอบต่าง ๆ (Right to Audit)

- **ลูกค้าบริการคลาวด์มีสิทธิ์ตรวจสอบ (The Cloud service customer has the right to audit)** หัวข้อนี้ระบุถึงสิทธิ์ตามข้อตกลง ที่ลูกค้าหรือผู้ใช้บริการคลาวด์ สามารถดำเนินการตรวจสอบ หรือเข้าถึงข้อมูลที่เกี่ยวข้องกับการดำเนินงานของผู้ให้บริการคลาวด์ โดยมีวัตถุประสงค์เพื่อประเมินว่าผู้ให้บริการคลาวด์ ปฏิบัติตามข้อกำหนดทางกฎหมาย มาตรฐานด้านความปลอดภัย และข้อกำหนดทางเทคนิคที่ระบุไว้ในข้อตกลงการให้บริการ (Service Level Agreement - SLA) หรือสัญญา (ทั้งนี้เป็นไปตามข้อตกลงระหว่างผู้ให้บริการและผู้ใช้บริการ) ผู้ให้บริการคลาวด์สามารถระบุตัวเลือกได้มากกว่าหนึ่งตัวเลือก ดังนี้

- เครื่องเสมือนที่ลูกค้าระบบคลาวด์เป็นเจ้าของ (Virtual Machine instances owned by the cloud service customer)
- สิ่งอำนวยความสะดวกของระบบเครือข่าย (Network facilities)
- การปฏิบัติตามมาตรฐานที่บังคับใช้ (Compliance with applicable standards)
- การควบคุมทางเทคนิค (Technical controls)
- นโยบายและการกำกับดูแล (Policies and governance)
- สิ่งอำนวยความสะดวกของศูนย์ข้อมูล (Data Center facilities)
- อื่น ๆ (Other)
- ไม่มี (None)

- **หน่วยงานกำกับดูแลที่กฎหมายไทยยอมรับมีสิทธิในการตรวจสอบ (Regulators recognized by the Thai law have the right to audit)** หัวข้อนี้ระบุถึงสิทธิ์ตามกฎหมายของหน่วยงานกำกับดูแลที่ได้รับการยอมรับตามกฎหมายของประเทศไทย ในการตรวจสอบกิจกรรมหรือกระบวนการที่เกี่ยวข้องกับบริการของผู้ให้บริการคลาวด์ เพื่อให้มั่นใจว่าการดำเนินงานและการจัดการข้อมูลสอดคล้องกับกฎหมาย ข้อกำหนด และมาตรฐานที่เกี่ยวข้อง ผู้ให้บริการคลาวด์สามารถระบุตัวเลือกได้มากกว่าหนึ่งตัวเลือก ดังนี้

- เครื่องเสมือนที่ลูกค้าระบบคลาวด์เป็นเจ้าของ (Virtual Machine instances owned by the cloud service customer)
- สิ่งอำนวยความสะดวกของระบบเครือข่าย (Network facilities)
- การปฏิบัติตามมาตรฐานที่บังคับใช้ (Compliance with applicable standards)
- การควบคุมทางเทคนิค (Technical controls)
- นโยบายและการกำกับดูแล (Policies and governance)
- สิ่งอำนวยความสะดวกของศูนย์ข้อมูล (Data Center facilities)
- อื่น ๆ (Other) พร้อมระบุรายละเอียดที่เกี่ยวข้อง
- ไม่มี (None)

- **รายงานการตรวจสอบ/การประเมินที่สามารถจัดทำได้ตามคำขอ (Audit/assessment reports that can be made available on request)** หัวข้อนี้ระบุถึงความพร้อมของผู้ให้บริการคลาวด์ ในการตรวจสอบ/ประเมินเพื่อให้เป็นไปตามกฎหมาย และจัดเตรียมและส่งมอบเอกสารหรือรายงานการตรวจสอบและการประเมิน (Audit/Assessment Reports) ที่แสดงถึงการปฏิบัติตามมาตรฐานและข้อกำหนดต่าง ๆ ให้กับลูกค้า/ผู้ใช้บริการคลาวด์ หรือหน่วยงานกำกับดูแลที่ร้องขอ เพื่อสร้างความโปร่งใสและแสดงถึงความน่าเชื่อถือของผู้ให้บริการ ผู้ให้บริการคลาวด์สามารถระบุตัวเลือกได้มากกว่าหนึ่งตัวเลือก ดังนี้

- การทดสอบการเจาะระบบ (Penetration Test)
- การประเมินความเสี่ยงด้านภัยคุกคามและช่องโหว่ (Threat and Vulnerability risk assessment)
- การสแกนช่องโหว่ของระบบ (Vulnerability scan)
- รายงานการตรวจสอบหรือการประเมิน (Audit reports)

2) การปฏิบัติตามกฎระเบียบ (Compliance) หัวข้อนี้ระบุถึงการที่ผู้ให้บริการคลาวด์ปฏิบัติตามกฎหมาย ข้อบังคับ มาตรฐาน และข้อกำหนดที่เกี่ยวข้อง เพื่อแสดงให้เห็นถึงความสอดคล้องกับข้อกำหนดด้านกฎหมาย ความปลอดภัย และการจัดการข้อมูลในระดับประเทศและสากล โดยมีวัตถุประสงค์ถึงการสร้างความมั่นใจให้กับลูกค้า/ผู้ใช้บริการคลาวด์ ลดความเสี่ยงทางกฎหมาย รวมถึงยืนยันความน่าเชื่อถือของผู้ให้บริการคลาวด์ เช่น การปฏิบัติตามมาตรฐาน เช่น ISO/IEC 27001, ISO/IEC 20000 หรือ CSA STARS ช่วยแสดงถึงความมุ่งมั่นในการปฏิบัติตามข้อกำหนดที่ได้รับการยอมรับ แบบฟอร์มนี้ผู้ให้บริการคลาวด์สามารถระบุตัวเลือกได้มากกว่าหนึ่งตัวเลือก ดังนี้

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act)
- ISO/IEC 27001
- ISO/IEC 27701
- ISO/IEC 27017
- ISO/IEC 27018
- ISO/IEC 20000
- CSA STARS
- อื่น ๆ (Other) พร้อมระบุรายละเอียดที่เกี่ยวข้อง

5. การควบคุมข้อมูล (Data Control) หัวข้อนี้มีวัตถุประสงค์เพื่อให้ผู้ให้บริการคลาวด์ แสดงความสามารถและแนวทางในการจัดการและควบคุมข้อมูลที่อยู่ในระบบคลาวด์ รวมถึงการกำหนดสิทธิ์ ความเป็นเจ้าของ และกระบวนการที่เกี่ยวข้องกับการจัดเก็บ การเข้าถึง และการประมวลผลข้อมูล เพื่อสร้างความมั่นใจให้กับลูกค้า/ผู้ใช้บริการคลาวด์ ว่าข้อมูลของพวกเขาได้รับการจัดการอย่างเหมาะสม ซึ่งประกอบไปด้วยหัวข้อที่ผู้ให้บริการคลาวด์ต้องระบุ ประกอบไปด้วย

1) ความเป็นเจ้าของข้อมูล (Data ownership) หัวข้อนี้หมายถึง สิทธิ์ทางกฎหมายและความรับผิดชอบ ในการเป็นเจ้าของข้อมูลที่จัดเก็บหรือประมวลผลในระบบคลาวด์ ซึ่งระบุอย่างชัดเจนว่าลูกค้า/ผู้ใช้บริการคลาวด์ หรือผู้ให้บริการคลาวด์ เป็นเจ้าของข้อมูลนั้น เช่น ข้อมูลของลูกค้าจะยังคงเป็นทรัพย์สินของลูกค้า/ผู้ใช้บริการคลาวด์ ไม่ใช่ผู้ให้บริการคลาวด์ ช่วยให้ทั้งลูกค้า/ผู้ใช้บริการคลาวด์ และผู้ให้บริการคลาวด์เข้าใจขอบเขตความรับผิดชอบ เช่น การเข้าถึง การแก้ไข การถ่ายโอน หรือการลบข้อมูล โดยผู้ให้บริการคลาวด์สามารถกรอกข้อมูลโดยมีรายละเอียด ดังนี้

- ระบุรายละเอียดที่เกี่ยวข้องกับข้อมูลที่ยกเว้น นอกเหนือจากข้อมูลทั้งหมดบนบริการคลาวด์ที่เป็นของลูกค้าบริการคลาวด์
- ระบุความเป็นเจ้าของข้อมูลที่ได้รับหรือแอตทริบิวต์ของการใช้งานระบบคลาวด์ยกเว้นสิ่งต่อไปนี้
    - ☐ การโฆษณาหรือการตลาด (Advertising or marketing)
    - ☐ การวิเคราะห์สถิติการใช้งาน (Statistics analysis on usage)
    - ☐ อื่น ๆ (Other) พร้อมระบุรายละเอียดที่เกี่ยวข้อง

2) การเก็บรักษาข้อมูล (Data Retention) หัวข้อนี้หมายถึงระยะเวลาและแนวทางที่ผู้ให้บริการคลาวด์ จะเก็บข้อมูลของลูกค้า/ผู้ใช้บริการคลาวด์ ไว้ในระบบคลาวด์นานเพียงใด ในระหว่างการใช้งาน รวมถึงข้อกำหนดหรือเงื่อนไขในการจัดเก็บข้อมูลหลังจากหมดอายุการใช้งาน หรือเมื่อสัญญาให้บริการสิ้นสุด (ทั้งนี้เป็นไปตามข้อตกลงระหว่างผู้ให้บริการและผู้ใช้บริการ) โดยผู้ให้บริการคลาวด์สามารถกรอกข้อมูล/ตัวเลือก ดังนี้

- ข้อมูลที่ลูกค้าบริการคลาวด์ที่ลบจะถูกเก็บไว้
    - ☐ ระยะเวลาการเก็บรักษาข้อมูลขั้นต่ำ พร้อมระบุรายละเอียด
    - ☐ ระยะเวลาการเก็บรักษาข้อมูลสูงสุด พร้อมระบุรายละเอียด
    - ☐ ลบทันที
- ข้อมูล Log จะถูกเก็บไว้เป็นระยะเวลา
    - ☐ ระยะเวลาการเก็บรักษาข้อมูลขั้นต่ำ พร้อมระบุรายละเอียด
    - ☐ ระยะเวลาการเก็บรักษาข้อมูลสูงสุด พร้อมระบุรายละเอียด
    - ☐ ไม่เก็บรักษาไว้
- ข้อมูลลูกค้าบริการคลาวด์จะถูกเก็บไว้เป็นระยะเวลา
    - ☐ ระยะเวลาการเก็บรักษาข้อมูลขั้นต่ำ พร้อมระบุรายละเอียด
    - ☐ ระยะเวลาการเก็บรักษาข้อมูลสูงสุด พร้อมระบุรายละเอียด
    - ☐ ไม่เก็บรักษาไว้ พร้อมระบุรายละเอียด
- ข้อมูลชนิดต่อไปนี้สามารถดาวน์โหลดได้โดยลูกค้าบริการระบบคลาวด์
    - ☐ ข้อมูล Log
    - ☐ อื่น ๆ (Other) พร้อมระบุรายละเอียดที่เกี่ยวข้อง

3) อำนาจอธิปไตยของข้อมูล (Data sovereignty) หมายถึง การจัดเก็บข้อมูลที่สามารถจัดเก็บข้อมูลที่ไหนก็ได้ โดยสิทธิในการครอบครองและการควบคุมข้อมูลต้องดำเนินการตามกฎหมายของประเทศที่เป็นเจ้าของข้อมูล โดยผู้ให้บริการคลาวด์สามารถกรอกข้อมูล/ตัวเลือก โดยสามารถระบุตัวเลือกได้มากกว่าหนึ่งตัวเลือก ดังนี้

- ตำแหน่งข้อมูลหลัก
  - ☐ ประเทศไทย
  - ☐ เอเชียตะวันออกเฉียงใต้ (พร้อมระบุรายละเอียด)
  - ☐ เขตปกครองพิเศษฮ่องกง
  - ☐ เอเชียแปซิฟิก (พร้อมระบุรายละเอียด)
  - ☐ ยุโรป (พร้อมระบุรายละเอียด)
  - ☐ สหรัฐอเมริกา
  - ☐ อื่น ๆ (พร้อมระบุรายละเอียด)
- ตำแหน่งข้อมูลสำรอง
  - ☐ ประเทศไทย
  - ☐ เอเชียตะวันออกเฉียงใต้ (พร้อมระบุรายละเอียด)
  - ☐ เขตปกครองพิเศษฮ่องกง
  - ☐ เอเชียแปซิฟิก (พร้อมระบุรายละเอียด)
  - ☐ ยุโรป (พร้อมระบุรายละเอียด)
  - ☐ สหรัฐอเมริกา
  - ☐ อื่น ๆ (พร้อมระบุรายละเอียด)
- จำนวนของประเทศที่มีการดำเนินงานศูนย์ข้อมูล (พร้อมระบุรายละเอียด)

4) การไม่เปิดเผยข้อมูล (Non-disclosure) หมายถึง ข้อกำหนดหรือข้อตกลงที่ผู้ให้บริการคลาวด์ รับรองว่าจะไม่เปิดเผยข้อมูลของลูกค้า/ผู้ใช้บริการคลาวด์ ต่อบุคคลที่สามหรือองค์กรอื่น ๆ โดยไม่ได้รับความยินยอมจากลูกค้า เว้นแต่จะมีข้อกำหนดทางกฎหมายหรือคำสั่งศาลที่บังคับใช้ โดยมีวัตถุประสงค์เพื่อปกป้องความลับทางธุรกิจและข้อมูลส่วนบุคคลของลูกค้า/ผู้ใช้บริการคลาวด์ และสร้างความไว้วางใจระหว่างลูกค้าและผู้ให้บริการคลาวด์ แบบฟอร์มนี้ผู้ให้บริการคลาวด์ สามารถระบุตัวเลือกได้มากกว่าหนึ่งตัวเลือก ดังนี้

- รูปแบบข้อตกลงในการไม่เปิดเผยข้อมูลสามารถจัดทำได้โดยผู้ให้บริการคลาวด์
- ผู้ให้บริการคลาวด์อาจใช้ข้อตกลงในการไม่เปิดเผยข้อมูลของลูกค้า

6. ประสิทธิภาพของผู้ให้บริการ (Provider Performance) หัวข้อนี้มีวัตถุประสงค์เพื่อให้ผู้ให้บริการคลาวด์ แสดงความสามารถและคุณภาพในการดำเนินงาน การรับประกันความพร้อมใช้งานของระบบ (Availability), แผนความต่อเนื่องทางธุรกิจ / การฟื้นฟูจาก ภัยพิบัติ (Business Continuity Plan / Disaster Recovery), ความรับผิด (Liability) และความรับผิดชอบร่วม (Shared responsibility) เพื่อรองรับความต้องการของลูกค้าอย่างมีประสิทธิภาพ ซึ่งประกอบไปด้วยหัวข้อที่ผู้ให้บริการคลาวด์ต้องระบุ ประกอบไปด้วย

1) ความพร้อมใช้งาน (Availability) หมายถึง ความสามารถของระบบหรือบริการในการให้บริการลูกค้า/ผู้ใช้บริการคลาวด์ ได้อย่างต่อเนื่องตามที่กำหนดไว้ในข้อตกลงระดับการให้บริการ (Service Level Agreement - SLA) โดยไม่มีการหยุดชะงักหรือ Downtime เกินกว่าที่ระบุไว้ ซึ่งเป็นตัวชี้วัดสำคัญของความน่าเชื่อถือของผู้ให้บริการคลาวด์ ความพร้อมใช้งานครอบคลุมทั้งโครงสร้างพื้นฐานด้านเครือข่ายและ

ระบบ โดยมักระบุเป็นเปอร์เซ็นต์ เพื่อให้ลูกค้าทราบถึงขอบเขตของบริการและความเสถียรของระบบที่พวกเขาสามารถคาดหวังได้ โดยผู้ให้บริการคลาวด์สามารถกรอกข้อมูล/ตัวเลือก ดังนี้

- การให้สัญญาว่าเครือข่ายจะทำงานได้
  ☐ (พร้อมระบุรายละเอียดร้อยละ)
- แตกต่างกันไปตามแผนราคา
- การให้สัญญาว่าตัวระบบจะทำงานได้
  ☐ (พร้อมระบุรายละเอียดร้อยละ)
- แตกต่างกันไปตามแผนราคา
- สภาพแวดล้อมระบบคลาวด์มีจุดเดียวของความล้มเหลวดังต่อไปนี้
  ☐ (พร้อมระบุรายละเอียด)
- ☐ ไม่มี

2) การขึ้นอยู่กับการใช้บุคคลที่สาม (3rd party dependency) หมายถึง ความจำเป็นที่ผู้ให้บริการคลาวด์ ต้องพึ่งพาทรัพยากรหรือบริการจากผู้ให้บริการในด้านอื่น ๆ เช่น โครงสร้างพื้นฐานเครือข่าย บริการด้านความปลอดภัย การจัดเก็บข้อมูล หรือบริการสนับสนุนอื่น ๆ ที่มีบทบาทสำคัญต่อการส่งมอบบริการคลาวด์แก่ลูกค้า/ผู้ใช้บริการคลาวด์ โดยการพึ่งพานี้อาจส่งผลต่อความพร้อมใช้งาน ความต่อเนื่องหรือคุณภาพของบริการในกรณีที่ผู้ให้บริการด้านนั้นประสบปัญหาหรือหยุดให้บริการ ดังนั้น การระบุความพึ่งพานี้ช่วยสร้างความโปร่งใส และเป็นส่วนสำคัญในการประเมินความเสี่ยงและความน่าเชื่อถือของบริการโดยผู้ให้บริการคลาวด์

3) แผนความต่อเนื่องทางธุรกิจ / การฟื้นฟูจาก ภัยพิบัติ (Business Continuity Plan / Disaster Recovery) หมายถึง แนวทางและมาตรการที่ผู้ให้บริการคลาวด์ จัดทำขึ้นเพื่อรับมือกับเหตุการณ์ที่อาจส่งผลกระทบต่อการดำเนินงาน เช่น ภัยพิบัติทางธรรมชาติ การโจมตีทางไซเบอร์ หรือความล้มเหลวของระบบ โดยมีเป้าหมายเพื่อรักษาความต่อเนื่องของการให้บริการ ลดผลกระทบต่อผู้ใช้งาน และกู้คืนระบบให้กลับมาใช้งานได้ภายในระยะเวลาที่กำหนดตามข้อตกลง เช่น Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) ซึ่งสะท้อนถึงความน่าเชื่อถือและความพร้อมของผู้ให้บริการในการจัดการกับสถานการณ์ฉุกเฉิน โดยผู้ให้บริการคลาวด์สามารถกรอกข้อมูล/ตัวเลือก ดังนี้

- การป้องกันความเสียหายที่เกิดจากเหตุภัยพิบัติ (Disaster recovery protection)
- บริการสำรองและกู้คืน (Backup and restore service)
- บริการคลาวด์ที่ลูกค้าเลือกแผนการสำรองข้อมูลได้ (Cloud service customer selectable backup plans)
- การจัดเตรียมสัญญา (Escrow arrangements)
- ไม่มีแผน BCP/DR (No BCP/DR is available)
- จำนวนเวลาที่ยอมรับความเสียหายได้ (Recovery Point Objective: RPO) (พร้อมระบุรายละเอียด)

- จำนวนเวลาที่ใช้ในการกู้คืนระบบได้ (Recovery Time Objective: RTO) (พร้อมระบุรายละเอียด)
- อื่น ๆ (พร้อมระบุรายละเอียด)

4) ความรับผิด (Liability) หมายถึง ความรับผิดชอบของผู้ให้บริการคลาวด์ ที่จะต้องชดเชยหรือดำเนินการตามที่ระบุไว้ในข้อตกลงระดับการให้บริการ (Service Level Agreement - SLA) กรณีที่ไม่สามารถปฏิบัติตามเงื่อนไขที่ตกลงไว้ได้ เช่น ความล้มเหลวของเครือข่าย (Network Failure), โครงสร้างพื้นฐาน (Infrastructure Failure), หรือการหยุดทำงานที่ไม่ได้แจ้งล่วงหน้า (Unscheduled Downtime) โดยความรับผิดนี้อาจแสดงออกในรูปแบบของการคืนค่าบริการ ชดเชยเวลาบริการเพิ่มเติม หรือมาตรการแก้ไขปัญหาที่ชัดเจน เพื่อรักษาความน่าเชื่อถือและสร้างความมั่นใจให้กับลูกค้าบริการคลาวด์ โดยผู้ให้บริการคลาวด์สามารถกรอกรายละเอียดในแต่ละสถานการณ์ตามแบบฟอร์ม ดังนี้

- เครือข่ายพบปัญหาจนไม่สามารถให้บริการได้ (Network failure)
- โครงสร้างพื้นฐานพบปัญหาจนไม่สามารถให้บริการได้ (Infrastructure failure) เครื่องเสมือนพบปัญหาจนไม่สามารถให้บริการได้ (Virtual Machine instance failure)
- การโยกย้ายระบบและไม่สามารถให้บริการได้ (Migrations)
- เกิดการหยุดทำงานที่ไม่ได้กำหนดไว้หรือแจ้งไว้ (Unscheduled downtime)
- ฐานข้อมูลเกิดปัญหาและไม่สามารถใช้งานได้ (Database failure)
- การตรวจสอบหรือการสังเกตเหตุผิดปกติล้มเหลว (Monitoring failure)

5) ความรับผิดชอบร่วม (Shared responsibility) หมายถึง การแบ่งความรับผิดชอบระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์ เช่น การแบ่งบทบาทและหน้าที่ระหว่างผู้ให้บริการคลาวด์และลูกค้า/ผู้ใช้บริการคลาวด์ ในการดูแลและจัดการระบบคลาวด์ โดยผู้ให้บริการคลาวด์รับผิดชอบส่วนโครงสร้างพื้นฐาน เช่น ฮาร์ดแวร์ เครือข่าย และความปลอดภัยของศูนย์ข้อมูล ขณะที่ลูกค้า/ผู้ใช้บริการคลาวด์รับผิดชอบการจัดการข้อมูล การตั้งค่าความปลอดภัยของแอปพลิเคชัน และการควบคุมการเข้าถึง ทั้งนี้เพื่อให้การใช้งานระบบคลาวด์เป็นไปอย่างปลอดภัยและมีประสิทธิภาพตามบทบาทของแต่ละฝ่าย โดยผู้ให้บริการคลาวด์สามารถกรอกรายละเอียดหรือแนบเอกสารได้ตามความเหมาะสม

7. การสนับสนุนบริการ (Service support) หัวข้อนี้มีวัตถุประสงค์เพื่อให้ผู้ให้บริการคลาวด์ แสดงถึงการให้ความช่วยเหลือและการบริการหลังการขาย ให้กับลูกค้า/ผู้ใช้บริการบริการคลาวด์ เพื่อช่วยให้การใช้งานบริการคลาวด์เป็นไปอย่างราบรื่นและมีประสิทธิภาพ ซึ่งอาจครอบคลุมถึงการตอบคำถาม การแก้ไขปัญหาทางเทคนิค การอัปเดตสถานะบริการ และการให้คำปรึกษาในกรณีที่เกิดปัญหา ซึ่งประกอบไปด้วยหัวข้อที่ผู้ให้บริการคลาวด์ต้องระบุ ประกอบไปด้วย

1) การจัดการการเปลี่ยนแปลง (Change management) หมายถึง กระบวนการและมาตรการที่ผู้ให้บริการคลาวด์ ใช้ในการวางแผน สื่อสาร และดำเนินการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อบริการคลาวด์ เช่น การอัปเดต การโยกย้าย การหยุดทำงาน หรือเหตุการณ์ที่อาจก่อให้เกิดความไม่ต่อเนื่อง โดยมีเป้าหมายเพื่อลดผลกระทบที่เกิดขึ้นกับลูกค้า สนับสนุนการโยกย้ายหรือปรับตัวตามความจำเป็น และรักษา

ประสิทธิภาพการดำเนินงานอย่างต่อเนื่องผ่านการสื่อสารและความโปร่งใส โดยผู้ให้บริการคลาวด์ สามารถเลือกรายละเอียดในแต่ละสถานการณ์ ดังนี้

- แผนและขั้นตอนการสื่อสารเพื่อแจ้งล่วงหน้า (Communication plan and procedures foe proactive notification)
- ความช่วยเหลือในการโยกย้ายไปยังบริการใหม่เมื่อโซลูชันเดิมถูกยกเลิก (Assistance in migration to new services when legacy solutions are discontinued)
- ความสามารถในการคงเวอร์ชันเก่าตามระยะเวลาที่กำหนด (Ability to remain on old versions for a defined time period)
- ความสามารถในการเลือกช่วงเวลาในการเกิดผลกระทบ (Ability to choose timing of impact)

2) พอร์ทัลการจัดเตรียมและ การจัดการแบบบริการตนเอง (Self-service provisioning and management portal) หมายถึง เครื่องมือหรือแพลตฟอร์มที่ผู้ให้บริการคลาวด์ จัดเตรียมไว้ให้ลูกค้า/ผู้ใช้บริการคลาวด์ เพื่อจัดการบริการคลาวด์ได้ด้วยตนเองแบบอัตโนมัติ ฟังก์ชันของพอร์ทัลอาจครอบคลุมถึง การจัดสรรทรัพยากร (Provisioning), การควบคุมการเข้าถึงตามบทบาท (RBAC), การจัดการวงจรชีวิตของบริการ (Service Lifecycle Management), การติดตามการใช้งานทรัพยากร และการตรวจสอบสุขภาพของระบบ (Health Monitoring) โดยมีเป้าหมายเพื่อเพิ่มความสะดวก ลดขั้นตอนการติดต่อผู้ให้บริการ และช่วยให้ลูกค้าสามารถควบคุมการใช้งานคลาวด์ได้อย่างมีประสิทธิภาพ และมีการสรุปข้อมูลส่งต่อไปยังหน่วยงานหรือระบบที่กำหนดเช่น excel , api หรือ วิธีการอื่น ๆ ตามกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ โดยผู้ให้บริการคลาวด์ สามารถกรอกรายละเอียดตามแบบฟอร์ม ดังนี้

- มีการจัดเตรียมไว้
- ไม่มีการจัดเตรียมไว้
- อนุญาตการควบคุมการเข้าถึงตามบทบาท (RBAC: Allow role-based access control)
- การจัดการทรัพยากรร่วมกัน (เช่น VM ที่เก็บข้อมูล และเครือข่าย) และเทมเพลตบริการ (Management resource pools (e.g. VMs, storage, and network) and service template)
- การติดตามและการจัดการวงจรชีวิตของแต่ละบริการ (Track and manage the lifecycle of each service)
- การติดตามการใช้บริการ (Track consumption of services)
- การตรวจสอบสุขภาพพื้นฐานตัวบริการ (Health Monitoring)
- อื่น ๆ (พร้อมระบุรายละเอียด)

3) การจัดการเหตุการณ์และปัญหา (Incident and problem management) หมายถึง กระบวนการที่ผู้ให้บริการคลาวด์ ใช้ในการรับมือและจัดการเหตุการณ์ที่ไม่คาดคิด หรือปัญหาที่เกิดขึ้นระหว่างการให้บริการคลาวด์ เช่น การหยุดทำงานของระบบ ความล้มเหลวของเครือข่าย หรือการ

ละเมิดความปลอดภัย โดยมีเป้าหมายเพื่อระบุ แก้ไข และป้องกันเหตุการณ์ดังกล่าวอย่างรวดเร็วและมีประสิทธิภาพ พร้อมทั้งสื่อสารกับลูกค้าเกี่ยวกับสถานะของเหตุการณ์ ช่องทางการแจ้งเตือน และระยะเวลาที่ใช้ในการแก้ไข เพื่อรักษาความน่าเชื่อถือและความต่อเนื่องของบริการ โดยผู้ให้บริการคลาวด์ สามารถกรอกรายละเอียดในแต่ละสถานการณ์ ดังนี้

- ช่องการในการติดต่อเมื่อเกิดปัญหา
  ☐ เข้าถึงผ่านทางอีเมล (Access via email)
  ☐ เข้าถึงผ่านพอร์ทัล (Access via portal)
  ☐ เข้าถึงผ่านการสนับสนุนทางโทรศัพท์ (Access via phone support)
  ☐ ติดต่อวิศวกรสนับสนุนโดยตรง (Direct access to support engineers)
- ความพร้อมของการสนับสนุน (Availability of support)
  ☐ 24X7
  ☐ ในช่วงเวลาทำการ (During office hours support) (โปรดระบุเวลาทำการ)
  ☐ การสนับสนุนหลังเวลาทำการ (After office hours support) (โปรดระบุเวลาทำการ)
- เวลาตอบสนองบริการ
- เวลาแจ้งเหตุการณ์การหยุดให้บริการคลาวด์
- ช่องทางการสื่อสารที่ใช้สำหรับการแจ้งเตือนเหตุการณ์การหยุดทำงานของบริการคลาวด์
- สิ่งต่อไปนี้มีให้สำหรับลูกค้าระบบคลาวด์เมื่อมีการร้องขอ
  ☐ การเข้าถึงบันทึกการตรวจสอบของอินสแตนซ์ของลูกค้าอย่างถาวร
  ☐ ความช่วยเหลือในการจัดการเหตุการณ์
- เวลาตอบสนองต่อเหตุการณ์
- เวลาเฉลี่ยในการซ่อมแซมเมื่อตรวจพบความผิดพลาด

4) การเรียกเก็บเงิน (Billing) หมายถึง กระบวนการที่ผู้ให้บริการคลาวด์ ใช้ในการกำหนด คำนวณ และแจ้งค่าใช้จ่ายสำหรับบริการคลาวด์ที่ลูกค้า/ผู้ใช้บริการคลาวด์ ใช้งาน โดยรูปแบบการเรียกเก็บเงินอาจมีหลากหลาย เช่น การจ่ายตามการใช้งานจริง (Pay per use) การกำหนดราคาคงที่ (Fixed Pricing) หรือรูปแบบอื่น ๆ ทั้งนี้ยังครอบคลุมถึงการให้ข้อมูลที่โปร่งใสเกี่ยวกับโครงสร้างค่าบริการ การวัดปริมาณการใช้งาน และการเข้าถึงประวัติการเรียกเก็บเงิน เพื่อให้ลูกค้าสามารถตรวจสอบและวางแผนการใช้งานได้อย่างมีประสิทธิภาพ โดยผู้ให้บริการคลาวด์สามารถกรอกรายละเอียดในแต่ละโหมดการเก็บเงิน ดังนี้

- จ่ายเมื่อมีการใช้งาน (Pay per use) (สูงสุดต่อนาที/ชั่วโมง/วัน/เดือนสำหรับการประมวลผล/พื้นที่จัดเก็บข้อมูลสำหรับ IaaS/PaaS และต่อลูกค้าบริการคลาวด์ต่อชั่วโมง/วัน/เดือน/ปีสำหรับ SaaS)
- ราคาคงที่ (สูงสุดรายปี/รายเดือน/รายวัน)
- รูปแบบการกำหนดราคาอื่น ๆ

- ไม่เปิดเผย
- ประวัติการเรียกเก็บเงินที่เรียกดูได้ (ระยะเวลา)

5) การเคลื่อนย้ายข้อมูล (Data portability) หมายถึง การที่ผู้ให้บริการคลาวด์กำหนดให้ลูกค้า/ผู้ใช้บริการคลาวด์ ในการถ่ายโอนข้อมูลหรือทรัพยากรดิจิทัล เช่น เครื่องเสมือน (VM), ฐานข้อมูล หรือไฟล์ข้อมูล จากผู้ให้บริการคลาวด์ รายหนึ่งไปยังรายอื่น หรือดาวน์โหลดข้อมูลออกมาเพื่อการใช้งานภายนอก โดยผู้ให้บริการต้องระบุรูปแบบที่รองรับ เช่น รูปแบบไฟล์ ระบบปฏิบัติการที่สนับสนุน รวมถึงวิธีการจัดการเมื่อบริการสิ้นสุดหรือเกิดเหตุการณ์หยุดชะงัก เพื่อให้มั่นใจว่าลูกค้าสามารถเข้าถึงข้อมูลได้อย่างต่อเนื่องและไม่มีข้อจำกัดที่ไม่เหมาะสม โดยผู้ให้บริการคลาวด์สามารถกรอกรายละเอียดรูปแบบการเคลื่อนย้ายข้อมูลตามรายละเอียด ดังนี้

- รูปแบบ VM ในการนำเข้าระบบ
- รูปแบบที่ดาวน์โหลดได้
- ระบบปฏิบัติการที่รองรับ
- เวอร์ชันภาษาของระบบปฏิบัติการที่รองรับ
- รองรับรูปแบบฐานข้อมูล
- มีนโยบาย/คำแนะนำ (Policy/guide available)
- API:
  ☐ ทั่วไป
  ☐ ปรับแต่ง
- เมื่อบริการสิ้นสุดลงหรือหยุดทำงานเป็นเวลานาน ข้อมูลจะพร้อมใช้งานผ่านทาง:
  ☐ ผ่านทางสื่อจัดเก็บข้อมูลแบบต่าง ๆ
  ☐ วิธีการมาตรฐานตามที่อธิบายไว้ข้างต้น
  ☐ วิธีอื่น ๆ

6) การทำงานร่วมกัน (Interoperability) หมายถึง การที่ผู้ให้บริการคลาวด์กำหนดบริการคลาวด์ (Cloud Service) ในการรองรับการผสานรวมกับระบบหรือบริการอื่น ๆ อย่างราบรื่น โดยใช้มาตรฐานอุตสาหกรรม เช่น รูปแบบการสื่อสาร (Transport) เช่น HTTPS (Hypertext Transfer Protocol Secure) หรือ MQTT (Message Queuing Telemetry Transport) รูปแบบข้อมูลที่รองรับ (Formats) เช่น JSON หรือ XML และ API ที่เปิดให้ใช้งาน เช่น RESTful API หรือ GraphQL ผู้ให้บริการคลาวด์จำเป็นต้องระบุข้อมูลเหล่านี้อย่างชัดเจน พร้อมจัดเตรียมเอกสารหรือคู่มือ เพื่อให้ลูกค้าสามารถใช้บริการคลาวด์ร่วมกับระบบที่มีอยู่ หรือย้ายข้อมูลและทรัพยากรระหว่างแพลตฟอร์มได้ง่ายขึ้น โดยผู้ให้บริการคลาวด์สามารถกรอกรายละเอียดรูปแบบการทำงานร่วมกัน ดังนี้

- Transport ที่รองรับ (เช่น HTTPS/MQTT ที่ใช้ REST)
- รูปแบบที่รองรับ (เช่น JSON/XML)

- API ที่รองรับ
- วิธีการอื่น ๆ
- มีคู่มือ

7) การเข้าถึงบริการ (Access) หมายถึง การที่ผู้ให้บริการคลาวด์ กำหนดวิธีการที่ลูกค้าสามารถเข้าถึงบริการคลาวด์ ซึ่งอาจผ่านเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต (Public Access) หรือเครือข่ายส่วนตัว เช่น VPN หรือลิงก์เฉพาะ (Private Access) นอกจากนี้ อาจครอบคลุมถึงการรองรับโปรโตคอล เช่น IPv6 และวิธีการอื่น ๆ ที่อำนวยความสะดวกให้กับการเข้าถึง ทั้งนี้ยังรวมถึงการระบุความเร็วสูงสุดของการเชื่อมต่อในรูปแบบแบนด์วิดท์ที่ใช้ร่วมกัน เพื่อให้ลูกค้าทราบถึงข้อกำหนดและข้อจำกัดในการใช้งานบริการโดยผู้ให้บริการคลาวด์สามารถกรอกรายละเอียดของการเข้าถึงบริการ ดังนี้

- การเข้าถึงสาธารณะ
- การเข้าถึงส่วนตัว
- รองรับการเข้าถึง IPv6
- วิธีการเข้าถึงอื่น ๆ
- ความเร็วในการเข้าถึงสาธารณะ (แบนด์วิดท์ที่ใช้ร่วมกัน) เป็น Mbps

8) การจัดการผู้ใช้ (User management) หมายถึง การที่ผู้ให้บริการคลาวด์มีการจัดการข้อมูล และสิทธิ์การเข้าถึงของผู้ใช้งานระบบคลาวด์ ซึ่งครอบคลุมถึงการสร้างและดูแลข้อมูลประจำตัวของผู้ใช้ (Identity Management), การกำหนดสิทธิ์การเข้าถึงตามบทบาท (Role Based Access Control - RBAC), การจัดการการเข้าถึงแบบรวมศูนย์ (Federated Access Model) เช่น การเชื่อมโยง Single Sign-On (SSO) และการผสานรวมกับโซลูชันจัดการข้อมูลประจำตัวอื่น ๆ เช่น Azure AD หรือ Okta โดยมุ่งเน้นให้เกิดความปลอดภัย ความยืดหยุ่น และความสะดวกในการควบคุมการเข้าถึงบริการของผู้ใช้งาน โดยผู้ให้บริการคลาวด์สามารถกรอกรายละเอียดของการจัดการผู้ใช้ ดังนี้

- การจัดการข้อมูลประจำตัว
- การควบคุมการเข้าถึงตามบทบาท
- รูปแบบการเข้าถึงแบบรวมศูนย์
- การผสานรวมกับโซลูชันการจัดการข้อมูลประจำตัว
- อื่น ๆ

9) วงจรชีวิต (Lifecycle) หมายถึง การที่ผู้ให้บริการคลาวด์มีกระบวนการจัดการและการปรับเปลี่ยนทรัพยากร หรือบริการคลาวด์ในระยะต่าง ๆ ตั้งแต่การจัดเตรียม (Provisioning) การใช้งาน การอัปเกรด ไปจนถึงการยกเลิก โดยมุ่งเน้นการสนับสนุนลูกค้าด้วยวิธีการที่ยืดหยุ่น เช่น การจัดสรรทรัพยากรโดยอัตโนมัติ (Automatic Provisioning) เพื่อปรับตัวตามความต้องการแบบเรียลไทม์ หรือการอนุญาตให้ลูกค้าปรับแต่งการจัดเตรียมทรัพยากรด้วยตนเอง (Customizable Provisioning) เพื่อให้สอดคล้องกับความ

ต้องการเฉพาะของธุรกิจ โดยผู้ให้บริการคลาวด์สามารถกรอกรายละเอียดของวงจรชีวิต (Lifecycle) โดยมีรายละเอียด ดังนี้

- การจัดสรรอัตโนมัติ
- บริการคลาวด์ที่ลูกค้าปรับแต่งการจัดเตรียม

8. Security Configuration หัวข้อนี้มีวัตถุประสงค์เพื่อให้ผู้ให้บริการคลาวด์ ระบุวิธีการและกระบวนการที่ใช้เพื่อจัดการและตรวจสอบการตั้งค่าความปลอดภัยของระบบคลาวด์ เพื่อให้มั่นใจว่าการตั้งค่าดังกล่าวถูกใช้งานอย่างเหมาะสมและปฏิบัติตามมาตรฐานความปลอดภัย โดยเฉพาะการปกป้องข้อมูลและทรัพยากรในระบบคลาวด์จากภัยคุกคามหรือช่องโหว่ที่อาจเกิดขึ้น ซึ่งประกอบไปด้วยหัวข้อที่ผู้ให้บริการคลาวด์ต้องระบุ ประกอบไปด้วย

1) การตรวจสอบการบังคับใช้ การกำหนดค่าความปลอดภัย (Security configuration enforcement checks) หมายถึง การที่ผู้ให้บริการคลาวด์มีกระบวนการเพื่อตรวจสอบและยืนยันว่าการกำหนดค่าความปลอดภัยที่ระบุไว้ ได้ถูกนำมาใช้และปฏิบัติอย่างถูกต้องและครบถ้วนตามมาตรฐานที่กำหนด โดยอาจดำเนินการผ่านการตรวจสอบด้วยตนเอง (Manual Checks) หรือใช้เครื่องมืออัตโนมัติ (Automated Tools) เพื่อความแม่นยำและรวดเร็ว ความถี่ในการตรวจสอบสามารถกำหนดตามลักษณะและความสำคัญของระบบ เช่น การตรวจสอบรายวัน รายสัปดาห์ หรือเมื่อมีการเปลี่ยนแปลงการตั้งค่า เพื่อให้มั่นใจว่าระบบมีความปลอดภัยและลดความเสี่ยงจากช่องโหว่หรือการโจมตี โดยผู้ให้บริการคลาวด์ สามารถกรอกรายละเอียดดังนี้

- ด้วยตนเอง
- การใช้เครื่องมืออัตโนมัติ
- มีการตรวจสอบการบังคับใช้บ่อยแค่ไหนเพื่อให้แน่ใจว่ามีการใช้การกำหนดค่าความปลอดภัยทั้งหมด

2) การเช่าหลายรายการ (Muti-tenancy) หมายถึง การที่ผู้ให้บริการคลาวด์สามารถรองรับลูกค้าหลายราย (Tenants) บนโครงสร้างพื้นฐานเดียวกัน โดยยังคงรักษาความปลอดภัย ความเป็นส่วนตัว และการแยกทรัพยากรระหว่างลูกค้า เช่น การแยกโฮสต์ทางกายภาพ การจัดกลุ่มเครื่องเสมือน (VM) หรือการกำหนดนโยบายความปลอดภัยเฉพาะลูกค้า (Customer Definable Security Domains) ทั้งนี้ยังครอบคลุมถึงการให้ลูกค้าสามารถปรับแต่งไฟร์วอลล์และกำหนดนโยบายการเข้าถึงตามความต้องการ เพื่อสร้างความยืดหยุ่นและความปลอดภัยในสภาพแวดล้อมการใช้งานร่วมกัน โดยผู้ให้บริการคลาวด์ สามารถกรอกรายละเอียด ดังนี้

- โฮสต์ทางกายภาพที่แตกต่างกัน
- โครงสร้างพื้นฐานเครือข่ายทางกายภาพที่แตกต่างกัน
- การจัดกลุ่ม VM
- โดเมนความปลอดภัยที่ลูกค้ากำหนดได้ของบริการคลาวด์
- บริการคลาวด์ที่ปรับแต่งไฟร์วอลล์ให้ลูกค้าได้
- นโยบายการเข้าถึงที่กำหนดได้ของลูกค้าบริการคลาวด์

3) การจัดเตรียมระบบคลาวด์แบบผสม (Hybrid cloud provision) หมายถึง การที่ผู้ให้บริการคลาวด์ระบุความสามารถในการสนับสนุนการจัดการปริมาณงาน (Workloads) บนระบบคลาวด์แบบผสม (Hybrid Cloud) โดยให้ข้อมูลเกี่ยวกับการตรวจสอบ การติดตาม และการบังคับใช้นโยบายด้านความปลอดภัย และความเป็นส่วนตัวของศูนย์บริการลูกค้า/ผู้ใช้บริการคลาวด์ ในปริมาณงานที่ใช้ระบบคลาวด์ โดยผู้ให้บริการคลาวด์ สามารถกรอกรายละเอียด ดังนี้

- การจัดการคีย์การปกป้องและการเข้ารหัสข้อมูล การบังคับใช้ตามตำแหน่งทางภูมิศาสตร์/ทรัพยากร และการโยกย้ายปริมาณงานบนคลาวด์อย่างปลอดภัย
- การจัดการคีย์และการจัดเก็บคีย์ มีการควบคุมโดยศูนย์บริการลูกค้า
- การแบ่งส่วนการไหลของข้อมูลแบบถาวรก่อนและหลังการโยกย้ายที่ปลอดภัยตามตำแหน่งทางภูมิศาสตร์/แหล่งทรัพยากร
- การบังคับใช้การปฏิบัติตามข้อกำหนดสำหรับปริมาณงานที่มีการควบคุมระหว่างระบบคลาวด์ส่วนตัวในองค์กร และระบบคลาวด์แบบผสม/สาธารณะ
- อื่น ๆ

9. Service Elasticity หัวข้อนี้มีวัตถุประสงค์เพื่อให้ผู้ให้บริการคลาวด์ ระบุการปรับเปลี่ยนทรัพยากรที่ใช้บริการได้อย่างยืดหยุ่น และเป็นไปโดยอัตโนมัติเพื่อตอบสนองความต้องการที่เปลี่ยนแปลงของลูกค้า/ผู้ใช้บริการคลาวด์ ไม่ว่าจะเป็นการเพิ่ม (Scale Up) หรือลด (Scale Down) ทรัพยากร เช่น หน่วยประมวลผล (CPU), หน่วยความจำ (RAM), หรือพื้นที่จัดเก็บข้อมูล (Storage) ในแบบเรียลไทม์ หรือในช่วงเวลาที่กำหนด ทั้งนี้เพื่อให้การใช้งานทรัพยากรเป็นไปอย่างมีประสิทธิภาพ ประหยัดค่าใช้จ่าย และรองรับปริมาณงานได้อย่างเหมาะสมตามความต้องการที่เปลี่ยนแปลง นอกจากนี้ยังครอบคลุมถึงความสามารถในการปรับปรุงบริการโดยไม่ต้องหยุดชะงัก และช่วยให้ลูกค้าสามารถจัดการทรัพยากรได้สะดวกขึ้นผ่านการปรับตั้งค่าอัตโนมัติที่กำหนดไว้ล่วงหน้า ซึ่งประกอบไปด้วยหัวข้อที่ผู้ให้บริการคลาวด์ต้องระบุ ประกอบไปด้วย

1) ความยืดหยุ่นของการใช้ทรัพยากร (Capacity elasticity) หมายถึง การที่ผู้ให้บริการคลาวด์ระบุความสามารถในการปรับเปลี่ยนปริมาณทรัพยากรที่ใช้งาน เช่น การเพิ่มหรือลดขนาดทรัพยากรการประมวลผล (Computing Resources), หน่วยความจำ (Memory) หรือพื้นที่จัดเก็บข้อมูล (Storage) ตามความต้องการของลูกค้าแบบเรียลไทม์หรือในเวลาที่กำหนดไว้ โดยมุ่งเน้นการตอบสนองต่อการใช้งานที่เปลี่ยนแปลง เช่น การเพิ่มทรัพยากรในช่วงที่มีการใช้งานสูงสุด (Peak Usage) หรือการแจ้งเตือนเมื่อมีการใช้งานที่ผิดปกติ ทั้งนี้เพื่อให้ลูกค้าสามารถบริหารจัดการทรัพยากรได้อย่างคุ้มค่า มีประสิทธิภาพ และพร้อมใช้งานอย่างต่อเนื่อง โดยผู้ให้บริการคลาวด์สามารถกรอกรายละเอียด ดังนี้

- อินเทอร์เฟซแบบเป็นโปรแกรมเพื่อขยายหรือลดขนาด
- เวลาเฉลี่ยในการเริ่มต้นและสิ้นสุด VM ใหม่
- การแจ้งเตือนที่จะส่งสำหรับการใช้งานสูงผิดปกติ
- ประสิทธิภาพขั้นต่ำในช่วงพีค
- ระยะเวลาขั้นต่ำในการขยายขนาดทรัพยากรการประมวลผล
- รับประกันความจุเพิ่มเติมขั้นต่ำต่อบัญชี (จำนวน Core และหน่วยความจำ GB)

2) ความยืดหยุ่นและความยืดหยุ่นของเครือข่าย (Network resiliency and elasticity) การที่ผู้ให้บริการคลาวด์ระบุความสามารถของระบบเครือข่ายที่ให้บริการบนคลาวด์ ในการรับมือกับสถานการณ์ที่ไม่คาดคิด เช่น การเชื่อมต่อขัดข้อง หรือปริมาณการใช้งานสูงผิดปกติ โดยยังคงความต่อเนื่องของการให้บริการ พร้อมทั้งมีความยืดหยุ่น (Elasticity) ในการปรับเพิ่มหรือลดทรัพยากรเครือข่าย เช่น แบนด์วิดท์, IP Address, หรือความสามารถในการโหลดบาลานซ์ เพื่อรองรับความต้องการที่เปลี่ยนแปลงแบบเรียลไทม์ ทั้งนี้ยังครอบคลุมถึงการป้องกันภัยคุกคาม เช่น การป้องกัน DDOS และการควบคุมการรับส่งข้อมูลที่สำคัญผ่าน QoS เพื่อให้การใช้งานเป็นไปอย่างมีประสิทธิภาพและปลอดภัย โดยผู้ให้บริการคลาวด์ สามารถกรอกรายละเอียดตามแบบฟอร์ม ดังนี้

- มีการเชื่อมต่ออินเทอร์เน็ตสำรองกรณีเกิดปัญหาแบบมากกว่า 1 ลิงก์
- มีการเชื่อมต่ออินเทอร์เน็ตสำรองกรณีเกิดปัญหา
- แบนด์วิดท์ที่เลือกได้สูงสุด
- จำนวน IP ที่ใช้งานได้สูงสุด
- จำนวนพอร์ตโหลดบาลานซ์
- โปรโตคอลโหลดบาลานซ์
- ใช้ระบบหรือบริการป้องกัน DDOS
- กลไกการป้องกันเชิงลึก
- การแยกการรับส่งข้อมูลเครือข่าย
- แบนด์วิดท์ที่ใช้ร่วมกันหรือแยกเฉพาะ
- บริการควบคุมการรับส่งข้อมูลด้วยวิธี QoS
- การแจ้งเตือนที่จะส่งสำหรับการใช้งานสูงผิดปกติ
- ประสิทธิภาพขั้นต่ำที่ใช้ได้ในช่วงที่มีการใช้งานสูงสุด
- ระยะเวลาขั้นต่ำในการขยายปริมาณงานเครือข่าย

3) การป้องกันความเสียหายที่เกิดกับอุปกรณ์เก็บข้อมูลและความยืดหยุ่นของการจัดเก็บ (Storage redundancy and elasticity) หมายถึง การที่ผู้ให้บริการคลาวด์ระบุความสามารถในการจัดการพื้นที่จัดเก็บข้อมูล (Storage) ให้มีความพร้อมใช้งานและปลอดภัย โดยรองรับการป้องกันความเสียหายของอุปกรณ์หรือการเชื่อมต่อทั้งภายในและระหว่างศูนย์ข้อมูล พร้อมทั้งมีความยืดหยุ่นในการขยายขนาดพื้นที่จัดเก็บหรือประสิทธิภาพการประมวลผล I/O ของระบบตามความต้องการของลูกค้า ทั้งยังรวมถึงการควบคุมทราฟฟิกข้อมูล การแจ้งเตือนเมื่อมีการใช้งานผิดปกติ และการรับประกันประสิทธิภาพขั้นต่ำในช่วงที่มีการใช้งานสูง เพื่อให้มั่นใจว่าระบบสามารถรองรับการใช้งานได้อย่างต่อเนื่องและเชื่อถือได้ โดยผู้ให้บริการคลาวด์สามารถกรอกรายละเอียด ดังนี้

- การป้องกันการเชื่อมต่อที่เก็บข้อมูลเสียหาย ภายในศูนย์ข้อมูลแต่ละแห่ง
- การป้องกันการเชื่อมต่อที่เก็บข้อมูลเสียหาย ระหว่างศูนย์ข้อมูลที่อยู่ในระบบคลาวด์เดียวกัน

- วิธีการแบ่งแยกการรับ-ส่งข้อมูล เพื่อการจัดเก็บ
- แบนด์วิดท์ของการเชื่อมต่อที่เก็บข้อมูลที่ใช้ร่วมกันหรือเฉพาะ
- มีการควบคุมคุณภาพของบริการ การจัดเก็บ และ บริการควบคุมการรับส่งข้อมูล
- ความจุสูงสุดสำหรับระบบคลาวด์ทั้งหมด
- ความจุสูงสุดสำหรับลูกค้าบริการคลาวด์รายเดียว
- พื้นที่เก็บข้อมูลที่ขยายได้สูงสุด โปรดระบุ
- การแจ้งเตือนที่จะส่งสำหรับการใช้งานสูงผิดปกติ
- ประสิทธิภาพ I/O ของพื้นที่จัดเก็บข้อมูลขั้นต่ำในช่วงที่มีการใช้งานสูงสุด
- ระยะเวลาขั้นต่ำในการขยายขนาดปริมาณการประมวลผล I/O ของพื้นที่จัดเก็บ

4.4 ตัวอย่างการกรอกแบบฟอร์มการเปิดเผยข้อมูลของผู้ให้บริการคลาวด์

เพื่อให้ผู้ให้บริการคลาวด์ เข้าใจถึงวิธีการกรอก**แบบฟอร์มการเปิดเผยข้อมูลของผู้ให้บริการคลาวด์** อย่างถูกต้อง ครบถ้วน และสอดคล้องกับเกณฑ์ที่กำหนดไว้ เราได้จัดเตรียมตัวอย่างการกรอกแบบฟอร์มที่เสร็จสมบูรณ์ไว้เป็นแนวทาง โดยตัวอย่างดังกล่าวแสดงถึงรายละเอียดที่ควรระบุในแต่ละหัวข้อ พร้อมทั้งตัวเลือกและคำอธิบายเพิ่มเติมที่สอดคล้องกับข้อกำหนดด้านความปลอดภัย การจัดการทรัพยากร และการปฏิบัติตามกฎระเบียบ ทั้งนี้เพื่อสนับสนุนให้การประเมินตนเองมีความโปร่งใสและนำไปสู่กระบวนการตรวจสอบที่มีประสิทธิภาพ สามารถดูตัวอย่างการกรอกข้อมูลทางการตรวจประเมินตนเองได้จากภาพด้านล่างนี้ รวมถึงสามารถดูแนวทางการกรอกข้อมูลใน**แบบฟอร์มการเปิดเผยข้อมูลของผู้ให้บริการคลาวด์**ได้ที่ภาคผนวก

Version 0.1

การเปิดเผยข้อมูลของผู้ให้บริการคลาวด์

แบบฟอร์มจะต้องกรอกสำหรับบริการคลาวด์แต่ละรายการที่มีให้ สำหรับคำถามที่ไม่เกี่ยวข้องหรือไม่เปิดเผย ให้ระบุในข้อสังเกต

The form is to be completed for each cloud service provided. For questions not applicable or not disclosed, indicate accordingly in the remarks. rks.

วันที่เปิดเผยข้อมูล Date of Disclosure: [2][0] / [0][8] / [2][5][6][8] (รูปแบบ วัน/เดือน/ปี พ.ศ.: Format Date/Month/Year B.E.))

ประเภทผู้ให้บริการ Applicable type : [/] ผู้ให้บริการคลาวด์ (Cloud Service Provider) [ ] ตัวแทน (Representative)

[ ] อื่น ๆ (Other) .....

บริการคลาวด์ที่ใช้งานได้ Applicable cloud service (s): .....IaaS, PaaS.....

ข้อมูลติดต่อผู้ให้บริการคลาวด์ | Cloud Service Provider Contact Information:
ชื่อบริษัท (Company name): .....บริษัท ตัวอย่าง จำกัด.....
ที่อยู่หลักของบริษัท (Primary address): .....123/45 ถนนสายหลัก เขตบางกอกน้อย .....
.....กรุงเทพฯ 10100.....
ที่อยู่เว็บไซต์ (Web address:): ..... https://www.examplecloud.com.....
ชื่อผู้ติดต่อ (Contact name): .....นายสมชาย ตัวอย่าง.....
เบอร์ติดต่อ (Contact number): ..... +66-1234-5678..... อีเมลติดต่อ (Contact e-mail): ..... contact@examplecloud.com.....
ตราประทับของบริษัท ลายเซ็นผู้แทนบริษัท
(Company Chop): ..... (Company Representative Signature): .....
ข้อมูลติดต่อหน่วยงานรับรอง | Certification Body Contact Information:
ชื่อบริษัท (Company name): ..... TÜV NORD Rheinland.....
ที่อยู่หลักของบริษัท (Primary address): .....678/91 ถนนสายหลัก เขตบางกอกน้อย .....
.....กรุงเทพฯ 10100.....
ที่อยู่เว็บไซต์ (Web address:): ..... https://rheinland.tuv-nord.com.....
ชื่อผู้ติดต่อ (Contact name): .....นายทดสอบ ตัวอย่าง.....
เบอร์ติดต่อ (Contact number): ..... +66-1234-5678..... อีเมลติดต่อ (Contact e-mail): ..... contact@certification.com.....

Version 0.1

รายละเอียดของผู้ให้บริการคลาวด์ | Cloud Service Provider Background

ภาพรวมของการให้บริการ (Overview of service offering):

.....ให้บริการเครื่องเสมือน ระบบเครือข่าย และบริการสำรองข้อมูลในรูปแบบ IaaS และ PaaS .....

.....

.....

.....

รูปแบบการบริการ (Service Model):

- ☑ เครื่องเสมือนที่ลูกค้าระบบคลาวด์เป็นเจ้าของ (Virtual Machine instances owned by the cloud service customer)
- ☑ สิ่งอำนวยความสะดวกสำหรับระบบเครือข่าย (Network Facillities)
- ☑ การปฏิบัติตามมาตรฐานที่บังคับใช้ (Compliance with applicable standards)

รูปแบบการปรับใช้ (Deployment Model):

- ☑ คลาวด์ส่วนตัว (Private cloud)
- ☐ ระบบคลาวด์ชุมชน/คลาวด์แบบกลุ่ม (Community cloud)
- ☑ คลาวด์ผสม (Hybrid cloud)
- ☑ คลาวด์สาธารณะ (Public cloud)
- ☐ คลาวด์อธิปไตย (Sovereign Cloud)
- ☐ คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud)

ภาพที่ 4 ตัวอย่างการกรอกข้อมูลแบบฟอร์มการเปิดเผยข้อมูลของผู้ให้บริการคลาวด์

ภาคผนวก

แนวทางการกรอกข้อมูลในแบบฟอร์มการเปิดเผยข้อมูลของผู้ให้บริการคลาวด์

แบบฟอร์มนี้ถูกออกแบบมาเพื่อรวบรวมข้อมูลสำคัญจากผู้ให้บริการคลาวด์ (Cloud Service Provider) โดยครอบคลุมหัวข้อต่าง ๆ ที่สะท้อนถึงคุณสมบัติ มาตรฐาน และบริการที่มีให้ โดยในแต่ละหัวข้อผู้ให้บริการจำเป็นต้องกรอกข้อมูลในส่วนที่เกี่ยวข้องให้ครบถ้วน และเลือกตัวเลือกที่ตรงกับบริการหรือกระบวนการขององค์กรมากที่สุด เช่น การระบุรูปแบบการให้บริการ การกำหนดขอบเขตการตรวจสอบ หรือการอธิบายมาตรการความปลอดภัย โดยในแต่ละตัวเลือกหรือช่องกรอกข้อมูล คำแนะนำได้ถูกกำหนดไว้อย่างชัดเจนเพื่อช่วยให้การกรอกข้อมูลเป็นไปอย่างถูกต้องและโปร่งใส ทั้งนี้การกรอกข้อมูลควรเน้นความถูกต้อง โปร่งใส และตรวจสอบได้ เพื่อสร้างความไว้วางใจให้กับลูกค้า/ผู้ใช้บริการคลาวด์ และหน่วยงานที่เกี่ยวข้อง โดยสามารถทำความเข้าใจในการกรอกข้อมูลผู้ให้บริการคลาวด์ในแต่ละส่วนของแบบบฟอร์มดังนี้

1. รายละเอียดของผู้ให้บริการคลาวด์ (Cloud Service Provider Background)

หัวข้อ	ข้อมูลที่ต้องกรอก	หมายเหตุ
ภาพรวมของการให้บริการ (Overview of Service Offering)	ระบุข้อมูลสรุปเกี่ยวกับบริการคลาวด์ที่ผู้ให้บริการนำเสนอ เช่น ให้บริการเครื่องเสมือน ระบบเครือข่าย และบริการสำรองข้อมูลในรูปแบบ IaaS และ PaaS หรืออธิบายจุดเด่นของบริการ เช่น การสนับสนุนมาตรฐานความปลอดภัยสูง	*ไม่มี*
รูปแบบการบริการ (Service Model)	☐ Infrastructure as a Service (IaaS) ☐ Platform as a Service (PaaS) ☐ Software as a Service (SaaS)	*ข้อมูลนี้ใช้เพื่อเลือกและระบุประเภทบริการที่สอดคล้องกับความต้องการของผู้ให้บริการระบบคลาวด์*
รูปแบบการปรับใช้ (Deployment Model)	☐ คลาวด์ส่วนตัว (Private Cloud): เลือกตัวเลือกนี้หากบริการของบริษัทเป็นโครงสร้างเฉพาะที่ให้บริการลูกค้ารายเดียว ☐ ระบบคลาวด์ชุมชน/คลาวด์แบบกลุ่ม (Community Cloud): เลือกตัวเลือกนี้หากบริการคลาวด์ถูกออกแบบมาสำหรับการใช้งานร่วมกันในกลุ่มองค์กร ☐ คลาวด์ผสม (Hybrid Cloud): เลือกตัวเลือกนี้หากบริการรองรับการใช้งานแบบผสมระหว่างคลาวด์ส่วนตัวและคลาวด์สาธารณะ ☐ คลาวด์สาธารณะ (Public Cloud): เลือกตัวเลือกนี้หากบริการเปิดให้ผู้ใช้งานทั่วไปสามารถเข้าถึงและใช้งานได้ ☐คลาวด์อธิปไตย (Sovereign Cloud): เลือกตัวเลือกนี้หากบริการคลาวด์อธิปไตย (Sovereign Cloud) ตามที่กระทรวงดิจิทัลฯ กำหนด ☐คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud):	*ระบุรูปแบบการปรับใช้ที่เหมาะสมสำหรับบริการที่นำเสนอ เพื่อให้ชัดเจนและโปร่งใสสำหรับลูกค้าหรือผู้ประเมิน*

	เลือกตัวเลือกนี้หากบริการคลาวด์สาธารณะมีการเพิ่มมาตรการคุ้มครองข้อมูลมากกว่าการใช้งานคลาวด์สาธารณะทั่วไป โดยมีการแยกการบริหารจัดการทรัพยากรและการใช้งานเฉพาะผู้ให้บริการแต่ละราย	

2. กฎหมายและการปฏิบัติตามกฎระเบียบ | Legal and Compliance

หัวข้อ	ข้อมูลที่ต้องกรอก	หมายเหตุ
ลูกค้าบริการคลาวด์มีสิทธิ์ตรวจสอบ (The Cloud service customer has the right to audit)	☐ เครื่องเสมือนที่ลูกค้าระบบคลาวด์เป็นเจ้าของ (Virtual Machine instances owned by the cloud service customer): เลือกตัวเลือกนี้หากลูกค้าต้องการตรวจสอบการตั้งค่า ความปลอดภัย หรือการใช้งานเครื่องเสมือนที่พวกเขาเป็นเจ้าของ ☐ สิ่งอำนวยความสะดวกของระบบเครือข่าย (Network facilities): เลือกตัวเลือกนี้หากลูกค้าต้องการตรวจสอบเครือข่าย เช่น การตั้งค่าเครือข่ายเสมือน (VPC) หรือความพร้อมใช้งานของเครือข่าย ☐ การปฏิบัติตามมาตรฐานที่บังคับใช้ (Compliance with applicable standards): เลือกตัวเลือกนี้หากลูกค้าต้องการตรวจสอบว่าผู้ให้บริการคลาวด์ปฏิบัติตามมาตรฐานที่เกี่ยวข้อง เช่น ISO 27001 หรือ GDPR ☐ การควบคุมทางเทคนิค (Technical controls): เลือกตัวเลือกนี้หากลูกค้าต้องการตรวจสอบมาตรการควบคุมทางเทคนิค เช่น ไฟร์วอลล์ การเข้ารหัส หรือการควบคุมการเข้าถึง	*ใช้สำหรับตรวจสอบสิทธิ์การเข้าถึงระบบของลูกค้า และประเมินความปลอดภัยในระดับต่าง ๆ*

หัวข้อ	ข้อมูลที่ต้องกรอก	หมายเหตุ
หน่วยงานกำกับดูแลที่กฎหมายไทยยอมรับมีสิทธิในการตรวจสอบ (Regulators recognized by the Thai law have the right to audit)	☐ เครื่องเสมือนที่ลูกค้าระบบคลาวด์เป็นเจ้าของ (Virtual Machine instances owned by the cloud service customer): เลือกตัวเลือกนี้หากกฎหมายหรือหน่วยงานกำกับดูแลต้องการตรวจสอบความถูกต้องของข้อมูลหรือการตั้งค่าของเครื่องเสมือน ☐ สิ่งอำนวยความสะดวกของระบบเครือข่าย (Network facilities): เลือกตัวเลือกนี้หากหน่วยงานต้องการตรวจสอบความปลอดภัยของเครือข่าย เช่น การจัดการ IP และการแยกเครือข่าย ☐ การปฏิบัติตามมาตรฐานที่บังคับใช้ (Compliance with applicable standards): เลือกตัวเลือกนี้หากหน่วยงานต้องการตรวจสอบว่าผู้ให้บริการปฏิบัติตามข้อกำหนดของกฎหมายหรือมาตรฐานระหว่างประเทศ ☐ การควบคุมทางเทคนิค (Technical controls): เลือกตัวเลือกนี้หากหน่วยงานต้องการตรวจสอบมาตรการรักษาความปลอดภัยที่ใช้ในระบบคลาวด์ ☐ นโยบายและการกำกับดูแล (Policies and governance): เลือกตัวเลือกนี้หากต้องการตรวจสอบนโยบายหรือกระบวนการของผู้ให้บริการที่เกี่ยวข้องกับความปลอดภัยของข้อมูล ☐ สิ่งอำนวยความสะดวกของศูนย์ข้อมูล (Data Center facilities): เลือกตัวเลือกนี้หากต้องการตรวจสอบโครงสร้างพื้นฐานของศูนย์ข้อมูล เช่น การเข้าถึงทางกายภาพ ☐ อื่น ๆ (Other): ..... เลือกตัวเลือกนี้หากต้องการระบุเงื่อนไขอื่นที่หน่วยงานต้องการตรวจสอบ ☐ ไม่มี (None): เลือกตัวเลือกนี้หากไม่ต้องการสิทธิในการตรวจสอบ	*ใช้สำหรับกำหนดเงื่อนไขและขอบเขตที่หน่วยงานกำกับดูแลสามารถเข้าถึงข้อมูลและระบบของผู้ให้บริการได้*

หัวข้อ	ข้อมูลที่ต้องกรอก	หมายเหตุ
รายงานการตรวจสอบ/การประเมินที่สามารถจัดทำได้ตามคำขอ (Audit/assessment reports that can be made available on request)	☐ การทดสอบการเจาะระบบ (Penetration Test): เลือกตัวเลือกนี้หากลูกค้าต้องการรายงานผลการทดสอบการเจาะระบบเพื่อประเมินความปลอดภัย ☐ การประเมินความเสี่ยงด้านภัยคุกคามและช่องโหว่ (Threat and Vulnerability risk assessment): เลือกตัวเลือกนี้หากต้องการข้อมูลเกี่ยวกับการประเมินความเสี่ยงในระบบ ☐ การสแกนช่องโหว่ของระบบ (Vulnerability scan): เลือกตัวเลือกนี้หากต้องการผลการสแกนช่องโหว่ของระบบในระดับเทคนิค ☐ รายงานการตรวจสอบหรือการประเมิน (Audit reports): เลือกตัวเลือกนี้หากต้องการรายงานการตรวจสอบที่แสดงความสอดคล้องกับมาตรฐานที่กำหนด	*ใช้สำหรับระบุประเภทของรายงานที่ลูกค้าสามารถขอรับได้จากผู้ให้บริการระบบคลาวด์*

บรรณานุกรม

[1] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560, [ออนไลน์].
สืบค้นที่:
https://www.parliament.go.th/ewtcommittee/ewt/draftconstitution2/more_news.php?cid=87
วันที่สืบค้น พฤศจิกายน 2567

[2] พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562, [ออนไลน์].
สืบค้นที่: https://www.dga.or.th/wp-content/uploads/2021/02/5.pdf
วันที่สืบค้น พฤศจิกายน 2567

[3] NIST Cloud Computing Reference Architecture, [ออนไลน์].
สืบค้นที่: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf
วันที่สืบค้น พฤศจิกายน 2567

[4] CISPE-Buying-Cloud-Services-in-Public-Sector-Handbook-v2-FEB-2022-3, [ออนไลน์].
สืบค้นที่: https://cispe.cloud/website_cispe/wp-content/uploads/2022/02/CISPE-Buying-Cloud-Services-in-Public-Sector-Handbook-v2-FEB-2022-3.pdf
วันที่สืบค้น ธันวาคม 2567

[5] สถาบันวิจัยเพื่อการพัฒนาประเทศไทย (TDRI). (2567). กิจกรรมด้านบริการคลาวด์สำหรับหรับหน่วยงานภาครัฐ

[6] สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2567). ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

[7] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2562). ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการใช้บริการคลาวด์ พ.ศ. 2562

[8] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. (2567). มติคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ เรื่อง แนวทางการดำเนินการตามมติคณะรัฐมนตรี เกี่ยวกับการจัดซื้อจัดจ้างหรือเช่าใช้บริการระบบคลาวด์ ประจำปีงบประมาณ พ.ศ. 2568

[9] Information System Security Management and Assessment Program ISMAP, [ออนไลน์].
สืบค้นที่:
https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010301&sys_kb_id=9b6741cec3058210327132011501 31c2&spa=1
วันที่สืบค้น พฤศจิกายน 2567

[10] Clod service provider disclosure (MTCS SS584:2020), [ออนไลน์].
สืบค้นที่: https://www.imda.gov.sg/-/media/imda/files/industry-development/infrastructure/csp-selfdisclosure-formalibaba-cloudsigned.pdf
วันที่สืบค้น พฤศจิกายน 2567