**แบบประเมินสถานภาพการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ สำหรับผู้ใช้บริการ (Cloud Security Standard Self-Assessment for Cloud Service Customer) ตามประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567**

**คำชี้แจง** แบบประเมินนี้ใช้เพื่อการประเมินสถานภาพการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งมีฐานะเป็นผู้ใช้บริการคลาวด์ สำหรับตรวจสอบและประเมินความมั่นคงปลอดภัยของข้อมูลหรือระบบสารสนเทศของหน่วยงานที่ใช้งานบนระบบคลาวด์สาธารณะ เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ภายใต้หลักการความร่วมรับผิดชอบ (Shared Responsibilities) ระหว่างผู้ใช้บริการและผู้ให้บริการ โดยแบบประเมินนี้จะแปรผันเกณฑ์ข้อกำหนดขั้นต่ำตามระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ (ระดับต่ำ ระดับกลาง และระดับสูง) ซึ่งหน่วยงานสามารถใช้แบบประเมินนี้เป็นเครื่องมือในการวิเคราะห์ช่องว่าง (Gap Analysis) ในการเตรียมความพร้อมของมาตรการควบคุมภายใน นโยบายความปลอดภัย และจัดเตรียมเอกสารหลักฐานอ้างอิงให้ถูกต้องครบถ้วน เพื่อเตรียมความพร้อมรองรับการตรวจประเมินอย่างมีประสิทธิภาพ

**คำแนะนำ**

1. ให้หน่วยงานกรอกข้อมูลในส่วนที่ 1 สำหรับระบบสารสนเทศที่ใช้งานบนระบบคลาวด์สาธารณะ **โดยให้ทำการประเมินแยกเป็นรายระบบงาน** (เช่น ระบบงานสารบรรณอิเล็กทรอนิกส์, ระบบบริหารทรัพยากรบุคคล, ระบบให้บริการประชาชน เป็นต้น) ทั้งนี้ โปรดทำเครื่องหมาย ✓ ลงในช่องที่ตรงกับสถานะการดำเนินการของระบบดังกล่าวมากที่สุด

2. ให้ประเมินการดำเนินการของระบบงาน (ที่ระบุในส่วนที่ 1) ตามข้อกำหนดในประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ในส่วนที่ 2 นี้ โดยทำเครื่องหมาย ✓ ลงในช่อง “สถานะการดำเนินการในปัจจุบัน” โดยมีคำอธิบายการประเมินแต่ละระดับดังนี้

**“มี/ดำเนินการแล้วเสร็จ”** กรณีที่หน่วยงานได้ดำเนินการตามข้อกำหนดของระบบงานที่ประเมินอย่างครบถ้วน พร้อมแนบรายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง

**“มี/ดำเนินการแล้วบางส่วน”** กรณีที่หน่วยงานได้ดำเนินการตามข้อกำหนดของระบบงานที่ประเมินแล้วแต่ยังไม่ครบถ้วน พร้อมแนบรายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง

**“อยู่ระหว่างการดำเนินการ”** กรณีที่หน่วยงานกำลังดำเนินการตามข้อกำหนดของระบบงานที่ประเมิน พร้อมแนบรายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง

**“ไม่มี/ยังไม่ได้ดำเนินการ”** กรณีที่หน่วยงานยังไม่ได้มีการดำเนินการตามข้อกำหนดของระบบงานที่ประเมิน

**“ไม่เกี่ยวข้อง”** กรณีที่หน่วยงานไม่ต้องดำเนินการ เนื่องจากข้อกำหนดไม่เข้าข่ายเกณฑ์ขั้นต่ำตามระดับผลกระทบของระบบงานที่ประเมิน

**หมายเหตุ** รายการตัวอย่างหลักฐานซึ่งแสดงในแต่ละข้อ เป็นเพียงรายการตัวอย่างเบื้องต้นเท่านั้น ทั้งนี้ แต่ละหน่วยงานอาจใช้เอกสาร/หลักฐานซึ่งมีชื่อเรียกที่แตกต่างจากเอกสารตัวอย่างดังกล่าว แต่มีเนื้อหาที่เกี่ยวข้องกับข้อคำถามนั้นเป็นหลักฐานประกอบการประเมินได้ หากเอกสารดังกล่าวมีรายละเอียดครบถ้วนตามประเด็นคำถามในแต่ละข้อ

## ส่วนที่ 1 ข้อมูลทั่วไปและการกำหนดระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ

**คำชี้แจง** ส่วนนี้มีวัตถุประสงค์เพื่อรวบรวมข้อมูลพื้นฐานของระบบสารสนเทศที่นำไปใช้งานบนระบบคลาวด์สาธารณะ และเพื่อดำเนินการประเมินระดับผลกระทบตามประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 โดยผู้ประเมินจะต้องพิจารณาความเสียหายที่อาจเกิดขึ้นในด้านการรักษาความลับ (Confidentiality) ด้านการรักษาความถูกต้องและครบถ้วน (Integrity) และด้านการรักษาสภาพพร้อมใช้งาน (Availability) เพื่อกำหนดว่าระบบนี้มีผลกระทบอยู่ในระดับต่ำ, ระดับกลาง, หรือระดับสูง ซึ่งผลการประเมินนี้จะถูกนำไปใช้เป็นเกณฑ์ในการกำหนดขอบเขตข้อกำหนดขั้นต่ำที่หน่วยงานต้องดำเนินการประเมินในส่วนที่ 2 ต่อไป

**หมวดที่ 1** ข้อมูลหน่วยงาน และข้อมูลที่เกี่ยวข้องกับผู้รับผิดชอบในการประเมินข้อมูลหรือระบบสารสนเทศที่ใช้งานบนคลาวด์สาธารณะ

**หน่วยงาน:** _____

**ข้อมูลผู้รับผิดชอบในการประเมินข้อมูลหรือระบบสารสนเทศ:**

ชื่อผู้ประเมิน: _____ ตำแหน่ง: _____

สังกัดหน่วยงาน (ภายใน): _____

เบอร์โทร: _____ อีเมล: _____

**หมวดที่ 2** ข้อมูลหรือระบบสารสนเทศ และการใช้บริการคลาวด์สาธารณะ

**2.1 ชื่อข้อมูลหรือระบบสารสนเทศ:** _____

**2.2 รูปแบบ/ประเภทบริการคลาวด์ที่ใช้:**

- ☐ Infrastructure as a Service : IaaS
- ☐ Platform as a Service : PaaS
- ☐ Software as a Service : SaaS
- ☐ รูปแบบ/บริการอื่น ๆ (ระบุ): _____

**2.3 ชื่อผู้ให้บริการคลาวด์:** _____

**<u>หมวดที่ 3</u>** การประเมินระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ

| ข้อ | รายการ | สถานะการดำเนินการในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|
| 1 | **การประเมินระดับผลกระทบ:**<br>หน่วยงานได้ดำเนินการประเมินระดับผลกระทบของระบบงาน ตามมาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 แล้วหรือไม่?<br>**ระดับผลกระทบที่ต้องประเมินได้ในแต่ละด้าน:**<br>1. การรักษาความลับ (Confidentiality: C)<br>2. การรักษาความถูกต้องและครบถ้วน (Integrity: I)<br>3. การรักษาสภาพพร้อมใช้งาน (Availability: A)<br>**หมายเหตุ** หากมีข้อมูลส่วนบุคคล ให้จัดระดับผลกระทบด้าน<u>การรักษาความลับระดับกลาง</u>เป็นอย่างน้อย | ☐ ประเมินแล้ว<br><br>**ระดับที่ประเมินได้:**<br>C = [ ต่ำ / กลาง / สูง ]<br>I = [ ต่ำ / กลาง / สูง ]<br>A = [ ต่ำ / กลาง / สูง ] | *<u>ตัวอย่างหลักฐาน</u>*<br>*- รายงานผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) ในส่วนที่เกี่ยวข้องกับข้อมูลหรือระบบสารสนเทศที่ทำงานอยู่บนคลาวด์* |
| 2 | **การประเมินระดับผลกระทบ:**<br>จากผลการประเมินในข้อ 1 ระบบงานที่ประเมินถูกจัดอยู่ในระดับผลกระทบใด? | ☐ ผลกระทบระดับต่ำ<br>☐ ผลกระทบระดับกลาง<br>☐ ผลกระทบระดับสูง | |
| 3 | **การกำหนดขอบเขตข้อกำหนดขั้นต่ำ:**<br>หน่วยงานได้นำระดับการประเมินจากข้อ 2 มาเทียบกับ **ข้อ 4 ข้อกำหนดขั้นต่ำและการตรวจรับรองสำหรับผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์** ของมาตรฐานคลาวด์ฯ เพื่อกำหนดขอบเขตข้อกำหนดที่ต้องปฏิบัติตามแล้วหรือไม่? | ☐ ดำเนินการแล้ว<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | |

## ส่วนที่ 2 การประเมินความสอดคล้องตามข้อกำหนดขั้นต่ำของมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

**คำชี้แจง** ส่วนนี้มีวัตถุประสงค์เพื่อประเมินความสอดคล้องในการดำเนินการของหน่วยงานตาม ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 โดยผู้ประเมินจะต้องพิจารณาข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในแต่ละหมวดหมู่ เฉพาะข้อกำหนดที่มีเกณฑ์บังคับใช้สอดคล้องกับระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศที่ท่านประเมินได้จากส่วนที่ 1 เพื่อใช้ประมวลผลเป็นระดับความพร้อมโดยรวมของระบบสารสนเทศ และจัดทำเป็นรายงานผลเสนอต่อผู้บริหารของหน่วยงานเพื่อพิจารณาอนุมัติต่อไป

### หมวดที่ 1 การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์ (Cloud Security Governance)

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินการในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| **นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)** | | | | | |
| 1 | หน่วยงานได้กำหนดและประกาศใช้นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์เป็นลายลักษณ์อักษร (ไม่ว่าจะจัดทำเป็นเอกสารนโยบายเฉพาะหัวข้อ หรือเขียนเป็นส่วนขยายจากนโยบายความปลอดภัยหลัก อย่างชัดเจน) โดยมาตรการควบคุมความปลอดภัยที่กำหนดในนโยบายนั้น สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ด้านความมั่นคงปลอดภัยสารสนเทศ ที่มีต่อข้อมูลและทรัพย์สินอื่น ๆ ของหน่วยงานแล้ว ใช่หรือไม่?<br>*แนวทางการประเมิน/ตรวจสอบ*<br>*- ตรวจสอบว่าหน่วยงานมีเอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ที่เป็นทางการและมีการอนุมัติใช้งานจริง โดยพิจารณาว่านโยบายนั้นแยกเป็นเอกสารเฉพาะ หรือเขียนเป็นส่วนขยาย (Addendum) ของนโยบายความมั่นคงปลอดภัยหลักอย่างชัดเจนและครอบคลุมบริบทของระบบคลาวด์*<br>*- พิจารณาว่ามาตรการควบคุมทางเทคนิคและการบริหารจัดการที่กำหนดไว้ในนโยบายคลาวด์ มีความสอดคล้องและเหมาะสมกับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ต่อข้อมูลและทรัพย์สินอื่น ๆ ของหน่วยงานจริงหรือไม่* | ทุกระดับ | 5.1.1 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *ตัวอย่างหลักฐาน*<br>*- เอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์*<br>*- เอกสารระดับความเสี่ยงที่ยอมรับได้ของหน่วยงาน* |
| 2 | เมื่อกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ หน่วยงานได้พิจารณาและกำหนดแนวทางจัดการความเสี่ยงที่ครอบคลุมปัจจัยสำคัญ 6 ด้าน ได้แก่ การเข้าถึงและจัดการข้อมูลโดยผู้ให้บริการคลาวด์ การดูแลรักษาทรัพย์สินไอทีและแอปพลิเคชัน การทำงานบนระบบเสมือนที่ใช้งานร่วมกัน (Multi-tenancy) กลุ่มผู้ใช้งานและบริบทการใช้ | ทุกระดับ | 5.1.1 (ข) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *ตัวอย่างหลักฐาน*<br>*- เอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์*<br>*- ข้อตกลงการรักษาความลับ (NDA) และสัญญาการใช้บริการคลาวด์*<br>*- นโยบายความปลอดภัยของซอฟต์แวร์และการจัดการช่องโหว่* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินการในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | งาน การควบคุมผู้ดูแลระบบที่ได้รับสิทธิพิเศษ (Privileged Admin) และสถานที่ตั้งทางภูมิศาสตร์ในการจัดเก็บข้อมูลของผู้ให้บริการคลาวด์ ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*รายละเอียดแนวทางที่ต้องระบุในนโยบายเพื่อลดความเสี่ยง*<br>*- มีข้อกำหนดชัดเจนเรื่องการเข้ารหัสข้อมูล (Encryption), การจำกัดสิทธิการเข้าถึงข้อมูลของเจ้าหน้าที่ผู้ให้บริการคลาวด์ (CSP), และข้อตกลงการรักษาความลับ (NDA)*<br>*- มีมาตรการคุ้มครองแอปพลิเคชันและซอร์สโค้ดบนคลาวด์ เช่น การควบคุมการเข้าถึงและยืนยันตัวตน, การป้องกันขอบเขตแอปพลิเคชัน (Application Boundary), และการจัดการช่องโหว่ของสภาพแวดล้อมระบบ*<br>*- มีข้อกำหนดเรื่องการแยกทรัพยากรเสมือน (Logical Separation/VPC) เพื่อป้องกันการรั่วไหลของข้อมูลระหว่างผู้เช่ารายอื่นที่ใช้คลาวด์ร่วมกัน และมาตรการรองรับกรณีประสิทธิภาพของระบบได้รับผลกระทบจากการแชร์ทรัพยากร*<br>*- มีการกำหนดสิทธิขั้นต่ำเท่าที่จำเป็น (Least Privilege), บังคับใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) ผ่านช่องทางปลอดภัย (เช่น VPN เท่านั้น), รวมถึงระบบบันทึกและทบทวนประวัติการทำงานของ Admin*<br>*- มีข้อกำหนดด้านสถานที่จัดเก็บข้อมูล (Data Residency) เพื่อป้องกันไม่ให้ข้อมูลสำคัญหรือข้อมูลส่วนบุคคลรั่วไหลออกนอกประเทศ หรือระบุข้อจำกัดในการโอนข้อมูลข้ามพรมแดน*<br>*- มีมาตรการควบคุมความปลอดภัยที่ยืดหยุ่นตามบริบท เช่น การเข้าใช้งานผ่านเครือข่ายสาธารณะ, การควบคุมการใช้อุปกรณ์ส่วนตัวที่ไม่ได้ลงทะเบียน (BYOD), และการจำกัดข้อมูลที่เข้าถึงได้ตามระดับความเสี่ยงของพนักงาน* | | | | *- นโยบายการควบคุมการเข้าถึง (Access Control Policy)*<br>*- นโยบายการถ่ายโอนข้อมูลของหน่วยงาน* |
| 3 | หน่วยงานได้ระบุข้อความแสดงความมุ่งมั่นที่จะปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และเงื่อนไขทางสัญญาที่ตกลงร่วมกับผู้ให้บริการคลาวด์ (เช่น การจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA) และแนวทางการติดตามการปฏิบัติตามข้อกำหนดของผู้ให้บริการ) ไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กรอย่างชัดเจน ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่านโยบายคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน มีการระบุบทบัญญัติ ข้อกำหนด หรือเงื่อนไขเกี่ยวกับข้อตกลงทางสัญญาระหว่างหน่วยงาน (ผู้ควบคุมข้อมูล) และผู้ให้บริการคลาวด์ (ผู้ประมวลผลข้อมูล) ไว้อย่างชัดเจนและเป็นทางการ*<br>*- ตรวจสอบว่านโยบายครอบคลุมประเด็นเชิงปฏิบัติการที่สำคัญ เช่น ข้อบังคับในการจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) ร่วมกับผู้* | ทุกระดับ | 5.1.1 (ค) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารนโยบายคุ้มครองข้อมูลส่วนบุคคล ที่มีการระบุข้อกำหนดสัญญากับผู้ประมวลผลข้อมูลคลาวด์*<br>*- ข้อกำหนดขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่หน่วยงานกำหนดให้ผู้ให้บริการคลาวด์ต้องปฏิบัติตาม*<br>*- เอกสารข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) ที่ลงนามร่วมกับผู้ให้บริการคลาวด์* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินการในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *ให้บริการคลาวด์ และกระบวนการติดตามตรวจสอบว่าผู้ให้บริการคลาวด์ปฏิบัติตามเกณฑ์เหล่านั้นจริงอย่างต่อเนื่อง* | | | | |
| 4 | หน่วยงานได้ทำข้อตกลงทางสัญญา (เช่น สัญญาบริการคลาวด์ หรือเอกสารแนบท้าย DPA) ที่แบ่งขอบเขตหน้าที่การคุ้มครองข้อมูลส่วนบุคคลระหว่าง 3 ฝ่าย ได้แก่ หน่วยงาน (ผู้ควบคุมข้อมูล), ผู้ให้บริการคลาวด์ (ผู้ประมวลผลข้อมูล) และผู้รับจ้างช่วง (Sub-contractors) ไว้อย่างชัดเจน โดยรายละเอียดหน้าที่นั้นสอดคล้องกับประเภทบริการคลาวด์ที่ใช้งานจริง (IaaS, PaaS หรือ SaaS) ใช่หรือไม่?<br><u>แนวทางการประเมิน/ตรวจสอบ</u><br>*- ตรวจสอบว่าในข้อตกลงทางสัญญามีการระบุหน้าที่และขอบเขตความรับผิดชอบร่วมกันระหว่างสามฝ่ายอย่างเป็นลายลักษณ์อักษร ได้แก่ ผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์ (CSP), ผู้รับจ้างช่วง (Sub-contractors) และหน่วยงาน (ผู้ใช้บริการคลาวด์) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล*<br>*- ตรวจสอบว่าข้อตกลงทางสัญญามีการระบุหน้าที่ของแต่ละฝ่าย ควรครอบคลุมในประเด็นควบคุมหลักด้านข้อมูลส่วนบุคคล เช่น*<br>*- การเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลเท่านั้น*<br>*- การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศของข้อมูลที่เพียงพอ*<br>*- ขั้นตอนและกรอบเวลาการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่ชัดเจน*<br>*- การตอบสนองต่อคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)*<br>*- การลบหรือส่งคืนข้อมูลทั้งหมดเมื่อสิ้นสุดข้อตกลงการให้บริการ*<br>*- ประเมินว่าสัญญามีการแยกแยะบทบาทความรับผิดชอบตามประเภทคลาวด์ที่ใช้จริง เนื่องจากสิทธิการเข้าถึงและการควบคุมในแต่ละระดับย่อมมีความแตกต่างกันอย่างมีนัยสำคัญ เช่น ขอบเขตความรับผิดชอบในการควบคุมความปลอดภัยระดับแอปพลิเคชัน (Application-level Control) บนบริการประเภท SaaS หรือ PaaS จะต้องแตกต่างไปจากบริการประเภท IaaS* | ทุกระดับ | 5.1.1 (ง) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | <u>ตัวอย่างหลักฐาน</u><br>*- สัญญาหรือข้อตกลงการใช้บริการคลาวด์ (Cloud Service Agreement) ที่ลงนามร่วมกันอย่างเป็นทางการ*<br>*- เอกสารข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement หรือ DPA) ที่ระบุขอบเขตความรับผิดชอบสามฝ่าย*<br>*- เอกสารแนบท้ายสัญญาที่ระบุรายชื่อผู้รับจ้างช่วงที่ได้รับอนุญาต (Authorized Sub-contractors List) และมาตรการควบคุมความปลอดภัยข้อมูลส่วนบุคคลของผู้รับจ้างช่วงดังกล่าว* |
| **โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)** | | | | | |
| 5 | หน่วยงานได้ทำข้อตกลงเป็นลายลักษณ์อักษรร่วมกับผู้ให้บริการคลาวด์ ที่มีการระบุการแบ่งบทบาทหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของทั้งสองฝ่ายอย่างชัดเจน และหน่วยงานได้ทบทวนเพื่อยืนยัน | ทุกระดับ | 5.1.2.1 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ | <u>ตัวอย่างหลักฐาน</u><br>*- เอกสารสัญญาหรือข้อตกลงการใช้บริการคลาวด์ (Cloud Service Agreement) หรือข้อตกลงระดับการให้บริการ (SLA) รวมถึงภาคผนวก* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินการในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | แล้วว่ามีความพร้อมและความสามารถในการปฏิบัติงานตามบทบาทที่ได้รับจัดสรรนั้นได้จริง ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานและผู้ให้บริการคลาวด์มีเอกสารข้อตกลงร่วมกันที่ระบุการแบ่งบทบาท หน้าที่ และความรับผิดชอบอย่างชัดเจน โดยข้อตกลงดังกล่าวอาจอยู่ในรูปแบบของสัญญาบริการคลาวด์ (Cloud Service Agreement), ภาคผนวกด้านความมั่นคงปลอดภัย (Security Addendum/Annex) หรือเอกสารแนบอื่น ๆ ที่มีผลผูกพันทางกฎหมายระหว่างสองฝ่ายอย่างเป็นทางการ*<br>*- ตรวจสอบว่าในข้อตกลงมีการระบุการจัดแบ่งหน้าที่ความรับผิดชอบของทั้งหน่วยงานและผู้ให้บริการคลาวด์ ครอบคลุมกระบวนการและมาตรการด้านเทคนิค อาทิ*<br>*- การจัดการช่องโหว่และการแพตช์ระบบ (Vulnerability Management & Patching)*<br>*- การควบคุมการเข้าถึงระบบ (Access Control)*<br>*- การเข้ารหัสลับข้อมูลและการจัดการกุญแจเข้ารหัส (Cryptography & Key Management)*<br>*- การสำรองและการกู้คืนข้อมูล (Information Backup & Recovery)*<br>*- การเฝ้าระวังและการบันทึกเหตุการณ์ความปลอดภัย (Event Logging & Monitoring)*<br>*- การรับมือและตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Incident Management)*<br>*- การตรวจสอบและปฏิบัติตามกฎหมายที่เกี่ยวข้อง (Compliance)*<br>*- สอบทานว่าหน่วยงานมีกระบวนการภายในที่ใช้ทบทวน หรือรับรองศักยภาพของเจ้าหน้าที่ทรัพยากร และระบบงาน ว่ามีความสามารถในการปฏิบัติงานตามบทบาทหน้าที่ที่ได้รับจัดสรรในสัญญาได้จริง* | | | ☐ ไม่มี/ยังไม่ได้ดำเนินการ | *ความมั่นคงปลอดภัย (Security Addendum) ที่ลงนามตกลงร่วมกับผู้ให้บริการ*<br>*- เอกสารระบุขอบเขตความรับผิดชอบสำหรับการประมวลผลคลาวด์ (Shared Responsibility Details) ที่ระบุแบ่งบทบาทหน้าที่การควบคุมทางเทคนิคของสองฝ่าย*<br>*- เอกสารหลักฐานแสดงความพร้อมปฏิบัติงานของหน่วยงาน เช่น รายชื่อผู้ประสานงานและสิทธิผู้ดูแลระบบ, รายงานผลการทดสอบการสำรองและกู้คืนข้อมูลจริง (Backup Restoration Test Report) ในส่วนงานที่หน่วยงานต้องรับผิดชอบ, หรือบันทึกผลการประเมินความพร้อมและฝึกอบรมของทีมผู้ดูแลระบบคลาวด์ของหน่วยงาน* |
| 6 | หน่วยงานได้กำหนดและบริหารจัดการความสัมพันธ์กับหน่วยงานสนับสนุนและดูแลลูกค้า (Customer Support) ของผู้ให้บริการคลาวด์อย่างเป็นระบบและเป็นลายลักษณ์อักษร (โดยมีการระบุระดับการดูแล ระดับความเร็วในการแก้ปัญหา (SLA) ช่องทางการติดต่อ และขั้นตอนการแจ้งปัญหาฉุกเฉินอย่างชัดเจน) ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>* | ทุกระดับ | 5.1.2.1 (ข) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารข้อตกลงระดับการให้บริการ (SLA) ด้านการสนับสนุน หรือเอกสารระบุสิทธิแผนการสนับสนุน (Support Plan details) จากผู้ให้บริการคลาวด์ ทะเบียนรายชื่อผู้ประสานงานของทั้งสองฝ่ายพร้อมช่องทางการติดต่อ*<br>*- คู่มือหรือขั้นตอนปฏิบัติกระบวนการยกระดับปัญหา (Escalation Path / Support Matrix Document) ที่มีการกำหนดผู้ดูแลรับผิดชอบและขอบเขต* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินการในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *- ตรวจสอบเอกสาร บันทึก หรือคู่มือการปฏิบัติงานที่แสดงถึงการจัดการความสัมพันธ์และการประสานงานกับส่วนงานสนับสนุน (Customer Support Team) และฟังก์ชันการดูแลระบบของผู้ให้บริการคลาวด์อย่างเป็นรูปธรรม*<br>*- พิจารณาว่าข้อมูลสนับสนุนที่ระบุนั้นครอบคลุมระดับการดูแลที่หน่วยงานได้รับจริง (เช่น แผนการสนับสนุนระดับ Basic, Standard หรือ Premium), ช่องทางการติดต่อสื่อสารทางเทคนิค, และขีดจำกัดความรับผิดชอบในข้อตกลงระดับการให้บริการ (SLA)*<br>*- ตรวจสอบว่ามีผังหรือกระบวนการยกระดับปัญหา (Escalation Path) ที่ระบุขั้นตอนการประสานงานกรณีเกิดปัญหาทางปฏิบัติการหรือภัยคุกคามที่ไม่สามารถแก้ไขได้ในระดับผู้ดูแลระบบปกติ เพื่อส่งต่อเรื่องไปยังผู้เชี่ยวชาญเฉพาะทางของผู้ให้บริการคลาวด์ได้อย่างรวดเร็ว* | | | | *กรอบระยะเวลา (SLA Response Time) ในแต่ละระดับความรุนแรงของปัญหาอย่างชัดเจน* |
| 7 | หน่วยงาน (ในฐานะผู้ใช้บริการคลาวด์) ได้มีการระบุและทำรายชื่อหน่วยงานควบคุมหรือกำกับดูแล หรือผู้มีอำนาจตามกฎหมายที่เกี่ยวข้องกับการดำเนินงานร่วมกันระหว่างหน่วยงานและผู้ให้บริการคลาวด์ พร้อมทั้งระบุช่องทางติดต่อและผู้ประสานงานหลักของแต่ละหน่วยงานไว้อย่างชัดเจน ไว้หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- พิจารณาว่า เมื่อมีการนำระบบคลาวด์มาใช้ จะต้องปฏิบัติตามข้อกำหนดของหน่วยงานกำกับดูแลใดบ้าง (เช่น สกมช., สคส., ธปท., กลต. เป็นต้น)*<br>*- ตรวจสอบรายละเอียดพิกัดทางภูมิศาสตร์ของศูนย์ข้อมูล (Data Center) ของผู้ให้บริการคลาวด์ที่จัดเก็บข้อมูลของหน่วยงาน เป็นข้อมูลสำหรับการระบุเขตอำนาจศาลหากต้องดำเนินคดีทางกฎหมายร่วมกัน*<br>*- ตรวจสอบว่าหน่วยงานมีทะเบียนรายชื่อหน่วยงานภายนอกที่เกี่ยวข้อง พร้อมช่องทางติดต่อและผู้ประสานงานหลักของหน่วยงานภายนอกเหล่านั้น ได้แก่ ชื่อหน่วยงาน ช่องทางการติดต่อ (เบอร์โทรศัพท์ อีเมลในการติดต่อประสานงานปกติ เบอร์สายด่วนฉุกเฉิน อีเมลหรือระบบรับแจ้งเหตุ) และระบุตัวบุคคลหรือฝ่ายงานของหน่วยงานที่เป็นผู้รับผิดชอบหลักในการติดต่อประสานงาน* | ทุกระดับ | 5.1.2.2 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารรายชื่อหน่วยงานภายนอกที่เกี่ยวข้องพร้อมข้อมูลในการติดต่อ* |
| **การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)** | | | | | |
| 8 | หน่วยงานได้พิจารณาและวิเคราะห์หรือไม่ว่า บริการคลาวด์ที่เลือกใช้งาน ตกอยู่ภายใต้กฎหมายหรือเขตอำนาจศาลของประเทศที่เป็นที่ตั้งของผู้ให้บริการคลาวด์ ซึ่งอาจอยู่นอกเหนือไปจากกฎหมายของไทย ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>* | ระดับกลาง ระดับสูง | 5.1.3.1 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารสัญญาบริการคลาวด์ (Cloud Service Contract/EULA) ในส่วนที่ระบุประเด็นกฎหมายที่ใช้บังคับและเขตอำนาจศาล* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินการในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *- เพื่อให้หน่วยงานสามารถประเมินความสอดคล้องเกี่ยวกับประเด็นเขตอำนาจศาลทางกฎหมายทับซ้อน (Cross-Border Jurisdictions) บนระบบคลาวด์ สำหรับข้อกำหนดในส่วนที่ 2 ของมาตรฐานคลาวด์ฯ ได้อย่างรัดกุมและถูกต้องตามหลักกฎหมายสากล*<br>*- ตรวจสอบว่าสัญญาการใช้บริการคลาวด์ (Cloud Service Agreement) หรือข้อกำหนดการอนุญาตสิทธิใช้งาน (EULA) มีการระบุขอบเขตเรื่องกฎหมายและเขตอำนาจศาลที่ใช้บังคับ (Governing Law and Jurisdiction) ไว้อย่างชัดเจนเป็นลายลักษณ์อักษร*<br>*- ตรวจสอบว่าหน่วยงานมีกระบวนการทบทวนด้านกฎหมายที่เป็นทางการ ซึ่งครอบคลุมการวิเคราะห์ประเด็นเขตอำนาจศาลที่ควบคุมบริการคลาวด์ เพื่อประเมินและป้องกันผลกระทบต่อภาระผูกพันหรือความปลอดภัยของข้อมูลหน่วยงานอย่างเหมาะสม* | | | ☐ ไม่เกี่ยวข้อง | *- เอกสารระบุขั้นตอนหรือกระบวนการทบทวนด้านกฎหมายของหน่วยงานสำหรับกรณีการจัดซื้อจัดจ้างระบบคลาวด์* |
| 9 | หน่วยงานได้กำหนดมาตรฐานความปลอดภัยและกฎหมายที่เกี่ยวข้องกับระบบคลาวด์ พร้อมทั้งร้องขอและตรวจสอบเอกสารหลักฐานรับรองความปลอดภัยของผู้ให้บริการคลาวด์ (เช่น ใบรับรอง ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, CSA STAR หรือรายงานผลการตรวจสอบจากผู้ตรวจสอบภายนอก) เพื่อยืนยันว่ามีความปลอดภัย สอดคล้องกับขอบเขตการใช้งานจริงของหน่วยงาน และยังมีผลบังคับใช้ (ไม่หมดอายุ) ใช่หรือไม่?<br><u>แนวทางการประเมิน/ตรวจสอบ</u><br>*- ตรวจสอบว่าหน่วยงานมีการจัดทำและระบุรายการกฎระเบียบ มาตรฐาน หรือข้อบังคับต่าง ๆ ที่ผู้ให้บริการคลาวด์ต้องปฏิบัติตามอย่างชัดเจน โดยรายการดังกล่าวต้องสอดคล้องและครอบคลุมภาระผูกพันทางกฎหมายของหน่วยงานเอง เช่น พ.ร.บ. ไซเบอร์ พ.ศ. 2562, มาตรฐานคลาวด์ฯ พ.ศ. 2567, พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎระเบียบเฉพาะภาคส่วนที่หน่วยงานสังกัดอยู่*<br>*- ตรวจสอบว่าหน่วยงานได้รับหลักฐานใบรับรองมาตรฐานระบบ (เช่น ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, หรือ CSA STAR) หรือรายงานผลการตรวจสอบระบบโดยผู้ตรวจสอบภายนอกที่น่าเชื่อถือ (เช่น SOC 2 Report) จากผู้ให้บริการคลาวด์จริง*<br>*- ตรวจสอบเงื่อนไขความถูกต้องของหลักฐานอย่างละเอียด ได้แก่ วันที่ออกเอกสาร วันหมดอายุ ขอบเขตการรับรอง (Scope of Certification) และตรวจสอบความสอดคล้องกันระหว่างขอบเขตการตรวจรับรองนั้นกับบริการหรือระบบคลาวด์ที่หน่วยงานเลือกใช้งานจริง เพื่อป้องกันกรณีใบรับรองไม่ครอบคลุมบริการที่ใช้งาน* | ระดับกลาง ระดับสูง | 5.1.3.1 (ข) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | <u>*ตัวอย่างหลักฐาน*</u><br>*- เอกสารทะเบียนหรือรายการกฎระเบียบและมาตรฐาน ที่หน่วยงานกำหนดให้ผู้ให้บริการคลาวด์ต้องปฏิบัติตาม*<br>*- สำเนาใบรับรองมาตรฐาน (เช่น ใบรับรอง ISO/IEC 27001, ISO/IEC 27017, หรือรายงาน SOC 2 Type II) ของผู้ให้บริการคลาวด์ที่ยังไม่หมดอายุ และระบุขอบเขตการรับรองครอบคลุมบริการที่ใช้งาน*<br>*- บันทึกหรือเอกสารสรุปผลการตรวจประเมินความสอดคล้องของใบรับรองที่ระบุผลการสอบทานขอบเขตการรับรองเทียบกับระบบที่ใช้งานจริงของหน่วยงาน* |
| 10 | หน่วยงานมีขั้นตอนปฏิบัติในการตรวจสอบเงื่อนไขการอนุญาตให้ใช้สิทธิการใช้งาน (License Agreement) ของซอฟต์แวร์เชิงพาณิชย์สำหรับระบบคลาวด์ก่อนอนุญาตให้ติดตั้ง และมีการควบคุมป้องกันกรณีระบบคลาวด์ขยายตัว | ระดับกลาง ระดับสูง | 5.1.3.2 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ | <u>*ตัวอย่างหลักฐาน*</u><br>*- เอกสารนโยบายหรือขั้นตอนปฏิบัติสำหรับการตรวจสอบสัญญาอนุญาตให้ใช้สิทธิ (License Agreement) สำหรับระบบคลาวด์ก่อนการติดตั้งซอฟต์แวร์* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินการในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | อัตโนมัติ (Elasticity/Auto-scaling) จนส่งผลให้จำนวนเครื่องเสมือนหรือแกนประมวลผล (Processor Cores) เกินกว่าสิทธิลิขสิทธิที่ได้รับตามสัญญา ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีนโยบายหรือคู่มือการดำเนินงานที่บังคับให้มีการทบทวนและตรวจสอบเงื่อนไขสัญญา/เงื่อนไขการอนุญาตให้ใช้สิทธิ (License Agreement) สำหรับซอฟต์แวร์เชิงพาณิชย์ที่จะนำมาติดตั้งบนคลาวด์ทุกครั้ง*<br>*- สอบทานว่าขั้นตอนปฏิบัติด้านสิทธิการใช้งานมีเกณฑ์เฉพาะเพื่อควบคุมการทำงานของคุณสมบัติ Auto-scaling ของคลาวด์ ซึ่งเป็นสาเหตุทางเทคนิคที่มักทำให้จำนวนแกนประมวลผล (Cores) เพิ่มขึ้นโดยอัตโนมัติและส่งผลต่อการละเมิดเงื่อนไขสัญญาลิขสิทธิเดิมโดยไม่ได้เจตนา* | | | ☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *- บันทึกหรือรายงานคำขอติดตั้งซอฟต์แวร์ที่ได้รับอนุญาตในเชิงพาณิชย์บนคลาวด์ ที่ระบุรายละเอียดการตรวจสอบความคุ้มครองจำนวน Core หรือโควตาสิทธิการใช้งาน พร้อมลายมือชื่ออนุมัติจากผู้เกี่ยวข้อง* |
| 11 | หน่วยงานได้ร้องขอและได้รับข้อมูลเกี่ยวกับมาตรการปกป้องบันทึกข้อมูล (Protection of Records) ที่ผู้ให้บริการคลาวด์ รวบรวมและจัดเก็บ และได้ตรวจสอบแล้วว่าสอดคล้องตามนโยบายของหน่วยงานและข้อกำหนดทางกฎหมาย (เช่น พ.ร.บ. คอมพิวเตอร์ฯ หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล) ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานได้มีการระบุรายละเอียดบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์อย่างครบถ้วน ซึ่งครอบคลุมประเภทบันทึกที่สำคัญ เช่น บันทึกการเข้าถึง (Access Log) บันทึกการเปลี่ยนแปลงระบบ (Change Log) บันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Event Log) และบันทึกธุรกรรมต่าง ๆ (Transaction Log)*<br>*- สอบทานว่าผู้ให้บริการคลาวด์มีมาตรการที่เพียงพอในการรักษาความถูกต้องครบถ้วนของบันทึกข้อมูล มีการจำกัดสิทธิและควบคุมการเข้าถึงบันทึก ตลอดจนมีกระบวนการและขั้นตอนปฏิบัติในการลบหรือทำลายบันทึกข้อมูลอย่างปลอดภัยเมื่อครบกำหนดเวลา*<br>*- ประเมินและวิเคราะห์มาตรการปกป้องและระยะเวลาในการจัดเก็บบันทึกข้อมูล (Log Retention Period) ของผู้ให้บริการคลาวด์ ว่าสอดคล้องกับข้อบังคับทางกฎหมายที่หน่วยงานต้องปฏิบัติตาม (เช่น พ.ร.บ.คอมพิวเตอร์ และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล) รวมถึงตรงตามข้อบังคับและนโยบายการทำงานภายในของหน่วยงานเอง* | ระดับกลาง ระดับสูง | 5.1.3.3 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารระบุรายละเอียดบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์ พร้อมมาตรการและขั้นตอนปฏิบัติในการควบคุมปกป้องบันทึกดังกล่าว*<br>*- รายงานผลการเปรียบเทียบหรือผลการทบทวนความสอดคล้อง ระหว่างมาตรการจัดเก็บและทำลายบันทึกข้อมูลของผู้ให้บริการคลาวด์ เทียบกับข้อกำหนดกฎหมาย และนโยบายภายในของหน่วยงาน* |
| 12 | หน่วยงานได้ตรวจสอบและยืนยันหรือไม่ว่า มาตรการเข้ารหัสข้อมูล (Cryptographic Controls) ที่ใช้งานบนระบบคลาวด์ ทั้งการเข้ารหัสข้อมูลขณะจัดเก็บ (At-Rest) และระหว่างการส่งผ่าน (In-Transit) มีความปลอดภัยที่ | ระดับกลาง ระดับสูง | 5.1.3.4 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารระบุมาตรการควบคุมการเข้ารหัสข้อมูลที่ใช้งานบนบริการคลาวด์*<br>*- รายการกฎหมาย ระเบียบข้อบังคับและข้อตกลงที่เกี่ยวข้องกับการเข้ารหัส* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินการในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | แข็งแรงเพียงพอ และสอดคล้องตามสัญญา ข้อตกลง กฎหมาย หรือระเบียบข้อบังคับที่เกี่ยวข้องอย่างครบถ้วน ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีเอกสารที่ระบุมาตรการควบคุมการเข้ารหัสข้อมูลที่ใช้งานอยู่บนบริการคลาวด์อย่างครบถ้วน โดยเอกสารดังกล่าวต้องแสดงคุณลักษณะทางเทคนิคสำคัญ ได้แก่ อัลกอริทึมการเข้ารหัส ความยาวของกุญแจเข้ารหัส และโปรโตคอลการเข้ารหัสที่ใช้ทั้งในสถานะจัดเก็บข้อมูล (At-rest) และระหว่างการส่งผ่าน (In-transit) รวมถึงระบุกระบวนการจัดการวงจรชีวิตของกุญแจเข้ารหัสด้วย*<br>*- ตรวจสอบว่ามีการรวบรวมและจัดทำทะเบียนหรือรายการกฎหมาย ระเบียบข้อบังคับและข้อตกลงทางสัญญาที่เกี่ยวข้องกับการเข้ารหัสข้อมูลอย่างเป็นระบบ*<br>*- ประเมินความสอดคล้องโดยการนำเทคโนโลยีการเข้ารหัสที่ใช้งานจริง (เช่น ชนิดอัลกอริทึม ความยาวกุญแจ และโปรโตคอล) ไปตรวจสอบเปรียบเทียบกับข้อกำหนดขั้นต่ำที่กฎหมายหรือข้อตกลงที่เกี่ยวข้องกำหนดไว้ เพื่อชี้บ่งและแก้ไขช่องว่างอย่างเหมาะสม* | | | ☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | |
| 13 | หน่วยงานได้ร้องขอและตรวจสอบเอกสารหลักฐาน (เช่น ใบรับรองมาตรฐานสากล หรือรายงานผลการตรวจสอบจากผู้ตรวจสอบภายนอก) เพื่อยืนยันว่าผู้ให้บริการคลาวด์มีระบบความปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคลจริงตามที่กล่าวอ้าง โดยมีการตรวจสอบวันหมดอายุ ขอบเขตการรับรองที่ตรงกับบริการที่ใช้งานจริง และพิจารณาข้อจำกัดของระบบคลาวด์เพื่อป้องกันความเสี่ยงอย่างรัดกุม ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีกระบวนการตรวจสอบและประเมินมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการคลาวด์อย่างเป็นระบบเพื่อยืนยันว่าสอดคล้องตามข้อกล่าวอ้าง*<br>*- ตรวจสอบหลักฐานใบรับรองมาตรฐานจากหน่วยรับรองที่ได้รับการรับรอง หรือรายงานผลการตรวจสอบโดยผู้ตรวจสอบภายนอกที่น่าเชื่อถือ โดยประเมินว่าหลักฐานจัดทำโดยผู้ตรวจสอบอิสระที่มีคุณสมบัติและได้รับการยอมรับ, ยังอยู่ในระยะเวลาที่มีผลบังคับใช้ (ไม่หมดอายุ), มีขอบเขตการรับรองครอบคลุมบริการคลาวด์ที่หน่วยงานใช้งานจริง, และไม่มีข้อยกเว้นหรือข้อจำกัดที่มีนัยสำคัญต่อความปลอดภัยของหน่วยงาน* | ระดับกลาง ระดับสูง | 5.1.3.5 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารใบรับรองมาตรฐานหรือรายงานการตรวจสอบผู้ให้บริการคลาวด์ (เช่น ใบรับรอง ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701 หรือ CSA STAR) ที่ยังไม่หมดอายุและครอบคลุมบริการที่ใช้งานจริง*<br>*- บันทึกหรือเอกสารประเมินผลการทบทวนความน่าเชื่อถือและความสอดคล้องของหลักฐาน (เช่น รายงานวิเคราะห์ขอบเขตใบรับรองเทียบกับระบบงานคลาวด์ที่ใช้งานจริง และบันทึกการพิจารณาข้อยกเว้นหรือข้อจำกัดทางเทคนิค)* |

## หมวดที่ 2 การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์ (Cloud Infrastructure Security and Operation)

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| **การบริหารทรัพยากรมนุษย์ (Human Resource Security)** | | | | | |
| 1 | หน่วยงานได้จัดให้มีโปรแกรมสร้างความตระหนักรู้ การศึกษา และการฝึกอบรม (Awareness, Education, and Training) ด้านความมั่นคงปลอดภัยระบบคลาวด์ สำหรับกลุ่มพนักงานปฏิบัติการและผู้ใช้งานทั่วไป (Operational & Technical Staffs) ครอบคลุมบุคลากรทุกกลุ่มที่เกี่ยวข้อง (ผู้จัดการ ผู้ดูแลระบบ ผู้ประกอบบริการ ผู้ใช้งานคลาวด์ พนักงาน และผู้รับจ้าง) โดยมีเนื้อหาครอบคลุมประเด็นสำคัญ (มาตรฐานและขั้นตอนการใช้งาน ความเสี่ยงและวิธีจัดการด้านสารสนเทศและเครือข่าย การคุ้มครองข้อมูลส่วนบุคคล และข้อกฎหมายที่เกี่ยวข้อง) ครบถ้วน ใช่หรือไม่?<br>*แนวทางการประเมิน/ตรวจสอบ*<br>*- ตรวจสอบว่าหน่วยงานมีเอกสารแผนการสร้างความตระหนักรู้ การศึกษา และการฝึกอบรมที่ระบุหัวข้อเนื้อหาเกี่ยวกับการใช้งานระบบคลาวด์ โดยควรจัดให้มีแผนหลักสูตร สื่อการเรียนรู้ และกำหนดรอบเวลาการจัดอบรมที่ชัดเจน*<br>*- ตรวจทานว่าโปรแกรมดังกล่าวมีการกำหนดเป้าหมายผู้เข้ารับการอบรมที่ครอบคลุมครบทุกบทบาทตามที่มาตรฐานกำหนด ได้แก่*<br>*- ผู้จัดการธุรกิจบริการคลาวด์ (Cloud Service Business Managers) ฝ่ายจัดซื้อจัดจ้าง, ฝ่ายกฎหมาย/บริหารสัญญา, ผู้จัดการหน่วยงานธุรกิจ (Business Unit Heads), หรือผู้ดูแลต้นทุนคลาวด์ เป็นต้น (Non-technical)*<br>*- ผู้ดูแลระบบบริการคลาวด์ (Cloud Service Administrators) ฝ่ายเทคนิค (IT SysAdmin/Cloud Admin) ที่มีสิทธิพิเศษในการตั้งค่าโครงสร้างพื้นฐาน ความปลอดภัย การจัดการสิทธิ (IAM) และเครือข่าย เป็นต้น*<br>*- ผู้ประกอบบริการคลาวด์ (Cloud Service Integrators) นักพัฒนา (Developers) หรือสถาปนิกผู้ออกแบบระบบ (Cloud Architects) ที่ทำหน้าที่เชื่อมต่อระบบคลาวด์ขององค์กรเข้ากับแอปพลิเคชันหรือระบบอื่น ๆ*<br>*- ผู้ใช้บริการคลาวด์ทั่วไป (Cloud Service Users) พนักงานหรือผู้ปฏิบัติงานทั่วไปในองค์กรที่เข้าใช้งานแอปพลิเคชันหรือบริการคลาวด์ในชีวิตประจำวัน*<br>*- ผู้รับจ้างของหน่วยงานที่มีหน้าที่เกี่ยวข้องกับระบบคลาวด์*<br>*โดยเนื้อหาการอบรมควรได้รับการออกแบบให้เหมาะสมกับระดับสิทธิและหน้าที่ความรับผิดชอบเฉพาะของบุคลากรแต่ละกลุ่มด้วย* | ทุกระดับ | 5.2.1.1 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *ตัวอย่างหลักฐาน*<br>*- เอกสารแผนงานโครงการหรือกำหนดการจัดอบรม/สร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยสารสนเทศที่ระบุขอบเขตเนื้อหาด้านคลาวด์ไว้อย่างเป็นลายลักษณ์อักษร*<br>*- ชุดสื่อการเรียนรู้ สไลด์นำเสนอ หรือเอกสารหลักสูตร (Training Courseware / Presentation Materials) ที่แสดงรายละเอียดเนื้อหาครอบคลุมประเด็นสำคัญทั้ง 5 ประเด็นครบถ้วน*<br>*- บันทึกการเข้าฝึกอบรม (Training Logs / Attendance Sheets) และเอกสารรายงานสถิติร้อยละของผู้ผ่านการอบรม แยกตามรายกลุ่มเป้าหมายบุคลากรภายในและผู้รับจ้าง* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *- สอบทานว่าชุดการฝึกอบรมและการสื่อสารเพื่อสร้างความตระหนักรู้ มีขอบเขตเนื้อหาที่ครอบคลุมประเด็นควบคุมตามเกณฑ์มาตรฐานทั้ง 5 ด้านอย่างครบถ้วน*<br>*1. มาตรฐานและขั้นตอนปฏิบัติ ในการเข้าใช้งานหรือใช้บริการคลาวด์ของหน่วยงาน*<br>*2. ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ที่เกี่ยวข้องกับบริการคลาวด์ และขั้นตอนกระบวนการในการจัดการความเสี่ยงเหล่านั้น*<br>*3. ความเสี่ยงทางกายภาพและด้านสภาพแวดล้อม ของระบบและสถาปัตยกรรมเครือข่ายที่เกิดจากการประมวลผลบนคลาวด์*<br>*4. มาตรการและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลบนสภาพแวดล้อมคลาวด์*<br>*5. ข้อพิจารณาทางกฎหมาย กฎระเบียบ ข้อบังคับ และข้อสัญญาอื่น ๆ ที่เกี่ยวข้องกับการใช้บริการคลาวด์* | | | | |
| 2 | หน่วยงานได้จัดให้มีโปรแกรมสร้างความตระหนักรู้ การศึกษา และการฝึกอบรม (Awareness, Education, and Training) ด้านความมั่นคงปลอดภัยระบบคลาวด์ สำหรับกลุ่มผู้บริหารและผู้ควบคุมสายงานธุรกิจ (Management & Business Units) ที่ได้รับการออกแบบเนื้อหาขึ้นเป็นการเฉพาะ (อาทิ การกำกับดูแลความเสี่ยงคลาวด์ การตัดสินใจเชิงกลยุทธ์ และการบริหารงบประมาณคลาวด์อย่างปลอดภัย เพื่อสนับสนุนการประสานงานกิจกรรมความมั่นคงปลอดภัยสารสนเทศอย่างมีประสิทธิภาพ) ใช่หรือไม่?<br>*แนวทางการประเมิน/ตรวจสอบ*<br>*- ตรวจสอบว่าหน่วยงานมีเอกสารแผนการฝึกอบรม โครงสร้างหลักสูตร และสื่อการเรียนรู้ด้านคลาวด์ที่ออกแบบขึ้นมาโดยเฉพาะสำหรับกลุ่มผู้บริหาร ผู้จัดการที่กำกับดูแล และหน่วยงานธุรกิจ (Business Units) โดยเนื้อหาจะต้องเหมาะสมกับบทบาทของกลุ่มเป้าหมายดังกล่าว ไม่ใช่หลักสูตรเชิงเทคนิคทั่วไป (Non-technical / Governance Focus)*<br>*- พิจารณาว่ารายละเอียดของเนื้อหาครอบคลุมมิติด้านการบริหารจัดการและการควบคุมระดับความเสี่ยงของหน่วยงาน เช่น การกำกับดูแลความเสี่ยงด้านคลาวด์ (Cloud Risk Governance) การประเมินผลตอบแทนและการลงทุนคลาวด์อย่างปลอดภัย และข้อกฎหมาย/การปฏิบัติตามกฎเกณฑ์ควบคุมที่ผู้บริหารต้องรับทราบ ควรเน้นย้ำถึงเรื่องความปลอดภัยในการบริหารจัดการ และกระบวนการสนับสนุนประสานงานกิจกรรมความมั่นคงปลอดภัยสารสนเทศระหว่างฝ่ายไอทีและฝั่งธุรกิจ* | ทุกระดับ | 5.2.1.1 (ข) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *ตัวอย่างหลักฐาน*<br>*- เอกสารแผนการสร้างความตระหนักรู้ การศึกษา และการฝึกอบรมสำหรับผู้บริหารและหน่วยงานธุรกิจ (ที่ได้รับการอนุมัติใช้งานอย่างเป็นทางการ)*<br>*- เอกสารโครงสร้างหลักสูตรและสื่อการเรียนรู้ (Syllabus & Training Materials) ที่มีเนื้อหาเน้นการกำกับดูแลความเสี่ยง การตัดสินใจ และความคุ้มค่าด้านงบประมาณความปลอดภัยคลาวด์*<br>*- บันทึกการเข้าร่วมกิจกรรมหรือรายงานผลการฝึกอบรม (Training Logs / Attendance Sheets) ของกลุ่มผู้บริหารและตัวแทนจากหน่วยงานธุรกิจต่าง ๆ* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| **การจัดการทรัพยสิน (Asset Management)** | | | | | |
| 3 | หน่วยงานได้จัดทำและปรับปรุงทะเบียนทรัพย์สิน (Inventory of Assets) ที่ครอบคลุมข้อมูลและทรัพย์สินทั้งหมดบนระบบคลาวด์อย่างครบถ้วน โดยระบุสถานที่จัดเก็บทางเทคนิคอย่างชัดเจน (เช่น ชื่อผู้ให้บริการคลาวด์, Region หรือ Zone) และมีขั้นตอนปฏิบัติที่เป็นทางการในการปรับปรุงข้อมูลทะเบียนทรัพย์สินให้เป็นปัจจุบันอยู่เสมอเมื่อมีการเปลี่ยนแปลง ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีทะเบียนทรัพย์สินระบบคลาวด์ที่รวบรวม ข้อมูล บริการของหน่วยงาน และโปรแกรมแอปพลิเคชันที่รันหรือเก็บรักษาอยู่บนสภาพแวดล้อมคลาวด์อย่างครบถ้วนและไม่ตกหล่น*<br>*- ตรวจสอบว่าทะเบียนทรัพย์สินระบุสถานที่จัดเก็บทั้งทาง Physical และ Logical อย่างชัดเจน โดยต้องระบุชื่อผู้ให้บริการคลาวด์ รวมถึงภูมิภาค (Region) หรือเขตพื้นที่ให้บริการ/โซนจัดเก็บ (Zone) และรายละเอียดอื่น ๆ ที่จำเป็นในการระบุพิกัดหรือสถาปัตยกรรมของทรัพยากร*<br>*- พิจารณาว่าหน่วยงานมีกระบวนการและขั้นตอนปฏิบัติเพื่อการทบทวนและปรับปรุงข้อมูลในทะเบียนทรัพย์สินให้ถูกต้อง ทันสมัย อยู่เสมอ โดยสุ่มตรวจสอบรายงานประวัติการขอเพิ่ม แก้ไข หรือลบรายการทรัพย์สินเมื่อสภาพแวดล้อมคลาวด์มีการเปลี่ยนแปลงจริง* | ทุกระดับ | 5.2.2.1 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารทะเบียนทรัพย์สิน (Inventory of Assets) ที่ครอบคลุมข้อมูล ทรัพย์สิน และบริการบนระบบคลาวด์อย่างละเอียด*<br>*- ขั้นตอนปฏิบัติสำหรับการปรับปรุงทะเบียนทรัพย์สินที่มีผลบังคับใช้อย่างเป็นทางการ*<br>*- บันทึกการขอเปลี่ยนแปลงรายการทรัพย์สินบนคลาวด์ (เช่น Change Request Ticket, รายงานการทบทวนและการอนุมัติเพิ่มหรือถอนระบบประมวลผลคลาวด์)* |
| 4 | หน่วยงานได้กำหนดและปฏิบัติตามขั้นตอนการติดป้ายระบุประเภทข้อมูล (Information Labelling) บนระบบคลาวด์ โดยระบุวิธีการกำหนดระดับชั้นความลับและผู้รับผิดชอบอย่างชัดเจน พร้อมทั้งคำนึงถึงลักษณะเฉพาะของคลาวด์ (เช่น การติดแท็ก (Tags) หรือการใส่เมทาดาตา (Metadata) บนพื้นที่เก็บข้อมูลเสมือน เครื่องแม่ข่ายเสมือน และคอนเทนเนอร์) และมีหลักฐานการติดป้ายระบุจริงในระบบคลาวด์ของหน่วยงาน ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีการจัดทำ "ขั้นตอนปฏิบัติสำหรับการบ่งชี้/ระบุประเภทข้อมูล" (Labelling Procedure) เป็นลายลักษณ์อักษรที่มีการประกาศใช้อย่างเป็นทางการ โดยกระบวนการดังกล่าวจะต้องครอบคลุมสิทธิและหน้าที่ของผู้รับผิดชอบ วิธีการทำสัญลักษณ์หรือกำหนดระดับชั้นความลับ และมีแนวปฏิบัติทางเทคนิคในการจำกัดสิทธิเพื่อรักษาความปลอดภัยของข้อมูลบนสภาพแวดล้อมคลาวด์อย่างชัดเจน*<br>*- พิจารณาว่าข้อกำหนดของหน่วยงานมีการประยุกต์ใช้เครื่องมือจำแนกทางเทคนิคที่เหมาะสมกับโครงสร้างของระบบคลาวด์จริง เช่น วิธีการบ่งชี้และการแยกประเภทความ* | ทุกระดับ | 5.2.2.2 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารขั้นตอนปฏิบัติสำหรับการบ่งชี้/ระบุประเภทข้อมูลของหน่วยงาน (Labelling Procedure)*<br>*- เอกสารทะเบียนทรัพย์สินสารสนเทศคลาวด์ที่ระบุระดับชั้นความลับอย่างชัดเจน (Asset Inventory with Data Classification)*<br>*- ตัวอย่างสกรีนช็อตรูปภาพหลักฐานการบ่งชี้ข้อมูลและทรัพย์สินจริงบนระบบคลาวด์ (เช่น บันทึกภาพการตั้งค่า Resource Tags, นโยบาย Resource Access Policy หรือหน้าจอกำหนดสิทธิจัดกลุ่มความปลอดภัยข้อมูล)* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *ปลอดภัยบนพื้นที่เก็บข้อมูลแบบ Object Storage, การบ่งชี้และตั้งชื่อระดับชั้นความปลอดภัยบนเครื่องแม่ข่ายเสมือน (Virtual Machines) และ Containers, ตลอดจนกำหนดนโยบายการประยุกต์ใช้โครงสร้างการติดแท็ก (Tags) และชุดข้อมูลอธิบายตัวแปร (Metadata) ตามที่ผู้ให้บริการคลาวด์แต่ละรายอนุญาตให้ตั้งค่าได้* | | | | |
| **การควบคุมการเข้าถึง (Access Control)** | | | | | |
| 5 | หน่วยงานมีนโยบายควบคุมการเข้าถึงเครือข่ายที่เป็นลายลักษณ์อักษรเพื่อใช้งานบริการคลาวด์ (ไม่จำกัดเฉพาะเครือข่ายภายใน) และกำหนดเงื่อนไขการเข้าถึงเฉพาะของแต่ละบริการคลาวด์อย่างเหมาะสมตามระดับความเสี่ยง (เช่น กำหนดช่องทาง VPN, วิธีการยืนยันตัวตน หรือข้อจำกัดอุปกรณ์และสถานที่) พร้อมทั้งนำข้อกำหนดไปตั้งค่าระบบและปฏิบัติจริง ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบเอกสารนโยบายการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่ายที่เป็นลายลักษณ์อักษร เพื่อยืนยันว่านโยบายครอบคลุมการเข้าถึงบริการคลาวด์ผ่านระบบเครือข่ายจากภายนอกหน่วยงานอย่างครบถ้วน <u>ไม่ใช่เพียงแค่ควบคุมโครงสร้างเครือข่ายภายใน</u> (On-Premise LAN/WAN) เท่านั้น*<br>*- ตรวจสอบว่าในรายละเอียดนโยบายมีการระบุเกณฑ์ควบคุมทางเทคนิคแยกเฉพาะตามความเสี่ยงของแต่ละระบบคลาวด์อย่างเหมาะสม เช่น ระบบคลาวด์ที่ประมวลผลข้อมูลที่มีความอ่อนไหวสูงหรือ Admin Console ต้องกำหนดมาตรการเข้าถึงทางเครือข่ายที่เข้มงวดและปลอดภัยสูงกว่าระบบทั่วไป*<br>*- พิจารณาว่าข้อกำหนดระบุเงื่อนไขการเข้าใช้งานที่ครอบคลุมมิติสำคัญ เช่ร เงื่อนไขการเข้าถึง, วิธีการพิสูจน์ตัวตน (เช่น SSO, MFA), ช่องทางเครือข่ายที่อนุญาต (เช่น VPN, Private Link หรือ Direct Connect), เงื่อนไขด้านตำแหน่ง/อุปกรณ์เชื่อมต่อ (เช่น ระบุ IP Whitelist หรือต้องใช้เครื่องคอมพิวเตอร์/อุปกรณ์ของหน่วยงานเท่านั้น), และการจัดระดับสิทธิการใช้งานตามบทบาท (Role-based access)* | ทุกระดับ | 5.2.3.1 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารนโยบายการควบคุมการเข้าถึงสำหรับการใช้บริการเครือข่าย ที่ครอบคลุมบริการคลาวด์ของหน่วยงาน*<br>*- เอกสารข้อกำหนดการเข้าถึงเฉพาะเจาะจง (Access Matrix / Requirements) สำหรับบริการคลาวด์แต่ละรายการ*<br>*- หลักฐานการนำข้อกำหนดควบคุมการเข้าถึงไปกำหนดค่าจริงบนคลาวด์ (เช่น ภาพที่แสดงหน้าจอการตั้งค่า Router/Firewall Rules, Virtual Private Cloud (VPC) Route Tables, Security Group Rules หรือการตั้งค่า VPN/Direct Connect)* |
| 6 | หน่วยงานมีขั้นตอนปฏิบัติที่เป็นลายลักษณ์อักษรสำหรับการลงทะเบียนและยกเลิกบัญชีผู้ใช้งานระบบคลาวด์ (User Registration & Deregistration) ที่ครอบคลุมทั้งการทำงานในสภาวะปกติ และมีกระบวนการรับมือทันทีเมื่อบัญชีหรือรหัสผ่านถูกเปิดเผยโดยไม่ตั้งใจ (เช่น การระงับบัญชีทันที การบังคับรีเซ็ตรหัสผ่าน และการตรวจสอบตัวตนอย่างเข้มงวดก่อนอนุญาตให้เข้าใช้งานใหม่เมื่อถูกแฮ็กหรือรั่วไหล) ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>* | ทุกระดับ | 5.2.3.2 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารขั้นตอนปฏิบัติสำหรับการลงทะเบียนและยกเลิกการลงทะเบียนผู้ใช้บนบริการคลาวด์ ที่ครอบคลุมทั้งวงจรชีวิตบัญชี (User Account Lifecycle)*<br>*- เอกสารขั้นตอนปฏิบัติเฉพาะสำหรับสถานการณ์ที่การควบคุมการเข้าถึงหรือบัญชีถูกคุกคาม (Compromised Account Response Procedure)* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *- ตรวจสอบว่าหน่วยงานมีคู่มือหรือขั้นตอนปฏิบัติที่เป็นลายลักษณ์อักษรที่ประกาศใช้อย่างเป็นทางการในการจัดการบัญชีผู้ใช้บนคลาวด์ (User Lifecycle Management) ครอบคลุมการลงทะเบียนขอบัญชีใหม่ การโยกย้ายหรือแก้ไขสิทธิระหว่างการทำงาน และการดำเนินการยกเลิกสิทธิอย่างสมบูรณ์เมื่อพ้นสภาพหรือหมดความจำเป็น*<br>*- ตรวจสอบอย่างถี่ถ้วนว่ากระบวนการทำงานมีขั้นตอนการตรวจจับ บรรเทา และฟื้นฟูสภาพความเสียหายในกรณีเกิดเหตุผิดปกติ เช่น รหัสผ่านรั่วไหลสู่สาธารณะ บัญชีผู้ดูแลระบบถูกแฮ็กเข้าใช้งาน หรือได้รับการแจ้งเตือนช่องโหว่ความมั่นคงปลอดภัย/การละเมิดสิทธิโดยตรงจากผู้ให้บริการคลาวด์*<br>*- ทบทวนว่าแผนการจัดการมีขั้นตอนที่รวดเร็วและเด็ดขาดเพื่อสกัดกั้นภัยคุกคามทันทีประกอบด้วย*<br>*- การสั่งระงับ (Suspend) บัญชีผู้ใช้งานหรือตัดสิทธิการเข้าถึงของบัญชีต้องสงสัยทันทีที่ได้รับแจ้งเตือน*<br>*- การบังคับใช้คำสั่งเปลี่ยนข้อมูลยืนยันตัวตนหรือรีเซ็ตรหัสผ่านแบบฉุกเฉิน (Emergency Password/Credential Reset)*<br>*- การกำหนดกระบวนการระบุตัวตนและตรวจสอบสิทธิขั้นสูง ก่อนพิจารณาอนุญาตให้ผู้ใช้ที่เคยถูกโจมตีเข้าลงทะเบียนเพื่อรับสิทธิเปิดใช้งานบัญชีใหม่อีกครั้ง*<br>*- กระบวนการกระจายข้อมูลและแจ้งเตือนผู้มีส่วนได้ส่วนเสีย บุคลากรภายในตลอดจนผู้ดูแลสิทธิตามลำดับขั้นการสื่อสาร* | | | | *- หลักฐานการจัดการเหตุละเมิดสิทธิบัญชี (เช่น ภาพหน้าจอบันทึกประวัติคำสั่งล็อกบัญชี (Disable Log) หรือบันทึกการซักซ้อมแผนรับมือกรณีสิทธิเข้าถึงของแอดมินรั่วไหล หรือรายงานผลการบังคับรีเซ็ตการตั้งค่าสิทธิผ่านระบบ IAM คอนโซลจริง)* |
| 7 | หน่วยงานได้บังคับใช้ระบบยืนยันตัวตนแบบหลายปัจจัย (MFA) กับผู้ดูแลระบบคลาวด์ที่มีสิทธิสูง (Privileged Admin) ในทุกช่องทางเข้าถึง (เช่น Web Console, API, CLI) พร้อมทั้งมีนโยบายการยืนยันตัวตน และทะเบียนรายชื่อผู้ดูแลระบบที่เป็นปัจจุบัน ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีการกำหนดเทคนิคการยืนยันตัวตนสำหรับผู้ดูแลระบบบริการคลาวด์ที่ได้รับสิทธิพิเศษ (Privileged Users) โดยมีเอกสารนโยบายหรือขั้นตอนปฏิบัติที่ระบุเทคนิคการยืนยันตัวตนที่ต้องใช้งานอย่างเป็นทางการ เช่น รูปแบบและปัจจัยของ MFA รวมถึงเงื่อนไขในการบังคับใช้*<br>*- ตรวจสอบว่ามีทะเบียนรายชื่อผู้ดูแลระบบบริการคลาวด์ที่ได้รับสิทธิพิเศษ ที่มีความเป็นปัจจุบัน โดยระบุบทบาท หน้าที่ ระดับสิทธิ และระบบบริการคลาวด์เฉพาะที่แต่ละบุคคลมีหน้าที่ดูแลอย่างชัดเจน*<br>*- พิจารณาว่าเทคนิคการยืนยันตัวตนที่เลือกใช้มีความเข้มแข็งและเพียงพอต่อระดับความเสี่ยงของการเข้าถึงระบบ เช่น การประยุกต์ใช้การยืนยันตัวตนแบบหลายปัจจัยที่ต้านทานการแฮ็กหรือฟิชชิง (Phishing-resistant MFA) สำหรับระบบที่มีความอ่อนไหวสูงมาก* | ทุกระดับ | 5.2.3.4 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารนโยบายหรือขั้นตอนปฏิบัติเกี่ยวกับการเข้าถึงและการยืนยันตัวตนสำหรับผู้ดูแลระบบคลาวด์*<br>*- ทะเบียนรายชื่อผู้ดูแลระบบบริการคลาวด์ที่ได้รับสิทธิพิเศษ*<br>*- หลักฐานการเปิดใช้งานและบังคับใช้ MFA จริงของทุกบัญชีสิทธิพิเศษ (เช่น ภาพถ่ายคอนโซลควบคุมสิทธิ IAM ที่แสดงสถานะ “MFA Enabled” ของผู้ดูแลระบบทุกคน หรือรายงานผลการตรวจสอบสถานะสิทธิจากระบบคลาวด์)* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *- สอบทานว่ามาตรการความปลอดภัยไม่ได้บังคับใช้แค่เพียงหน้าเว็บคอนโซล (Web Portal) แต่ต้องบังคับใช้ครอบคลุมทุกช่องทางเชื่อมต่อทางเทคนิคที่แอดมินสามารถสั่งการได้ เช่น การเรียกใช้งานผ่าน Programmatic API, การส่งคำสั่งผ่าน Command Line Interface (CLI) หรือเครื่องมือบริหารจัดการระบบอื่น ๆ* | | | | |
| 8 | หน่วยงานได้ตรวจสอบและยืนยันแล้วว่า กระบวนการจัดการรหัสผ่านของผู้ให้บริการคลาวด์ (เช่น ความซับซ้อนและอายุรหัสผ่าน, การส่งรหัสผ่านเริ่มต้นอย่างปลอดภัย, การบังคับเปลี่ยนรหัสผ่านเมื่อเข้าใช้ครั้งแรก และกลไกการรีเซ็ตรหัสผ่าน) สามารถรองรับและปฏิบัติตามนโยบายที่หน่วยงานกำหนดไว้ได้จริง ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีข้อกำหนดด้านการจัดการข้อมูลการตรวจสอบความลับ (Secret Authentication Information) กำหนดไว้อย่างชัดเจนและเป็นลายลักษณ์อักษร โดยต้องพิจารณาความครอบคลุมของเกณฑ์ควบคุมหลัก เช่น นโยบายความปลอดภัยของรหัสผ่าน การจัดส่งรหัสผ่านเริ่มต้นที่ปลอดภัยเพื่อป้องกันการลักลอบดักข้อมูล การบังคับเปลี่ยนรหัสผ่านทันทีเมื่อใช้งานครั้งแรกเพื่อป้องกันบัญชีค้าง และระบบการกู้คืนหรือรีเซ็ตรหัสผ่านที่มีกระบวนการพิสูจน์ตัวตนที่รัดกุม*<br>*- ตรวจสอบว่าหน่วยงานมีรายงานหรือบันทึกประวัติผลการเปรียบเทียบระหว่างข้อกำหนดความปลอดภัยของหน่วยงาน กับขั้นตอนการจัดการและจัดสรรข้อมูลการตรวจสอบความลับของผู้ให้บริการคลาวด์ เพื่อชี้บ่งและแก้ไขช่องว่างอย่างเหมาะสม* | ทุกระดับ | 5.2.3.5 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารข้อกำหนดด้านการจัดการข้อมูลการตรวจสอบความลับ ของหน่วยงาน (Secret Authentication Information/Password Policy)*<br>*- เอกสารขั้นตอนการจัดการและจัดสรรข้อมูลการตรวจสอบความลับของผู้ให้บริการคลาวด์*<br>*- รายงานผลการเปรียบเทียบหรือผลการประเมินความสอดคล้อง ระหว่างนโยบายการตรวจสอบความลับของหน่วยงาน เทียบกับขีดความสามารถและกระบวนการทำงานจริงบนบริการคลาวด์* |
| 9 | หน่วยงานได้จำกัดสิทธิการเข้าถึงข้อมูลและบริการต่าง ๆ บนคลาวด์อย่างเคร่งครัดตามนโยบายที่กำหนดไว้ (ครอบคลุมทั้ง Management Console พื้นที่เก็บข้อมูล ฐานข้อมูล และระบบประมวลผล) โดยไม่มีข้อมูลหรือบริการใดที่สามารถเข้าถึงได้โดยไม่มีการควบคุมสิทธิ ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ต้องกำหนดหลักการควบคุมและจำกัดการเข้าถึงข้อมูลคลาวด์ไว้อย่างเป็นทางการ โดยอาศัยหลักการสิทธิน้อยที่สุดที่จำเป็น (Principle of Least Privilege), หลักความจำเป็นต้องรู้ (Need-to-Know), การควบคุมสิทธิตามบทบาทหน้าที่ (Role-Based Access Control: RBAC) และกำหนดเงื่อนไขการเข้าถึงเฉพาะเจาะจงสำหรับแต่ละบริการและข้อมูล*<br>*- ต้องจัดให้มีหลักฐานการตั้งค่าเพื่อควบคุมและจำกัดการเข้าถึงสิทธิจริงบนคอนโซลคลาวด์อย่างรอบด้าน เช่น การจัดการและจัดสรรสิทธิผ่าน IAM Policy, การควบคุมความปลอดภัยของเครือข่ายเชื่อมต่อ (Network Access Policy เช่น Security Group) และการจำกัดสิทธิเข้าถึงพื้นที่เก็บรักษาข้อมูล (Resource Access Policy เช่น Bucket Policy หรือ* | ทุกระดับ | 5.2.3.6 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารนโยบายการควบคุมการเข้าถึงที่ครอบคลุมบริการคลาวด์ (Access Control Policy)*<br>*- หลักฐานสกรีนช็อตรูปภาพแสดงการกำหนดสิทธิจริงบนคลาวด์คอนโซล อาทิ การตั้งค่า IAM Policy, Network Access Policy (Security Group) และ Resource Access Policy (Bucket Policy)*<br>*- ตัวอย่างข้อมูลหรือรายงานบันทึกการเข้าใช้งานจริง (Access Logs) ที่ส่งออกจากคลาวด์คอนโซล*<br>*- รายงานผลการตรวจสอบทบทวนสิทธิการเข้าใช้งานระบบคลาวด์ (Access Privilege Review Report)* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *Access Control List: ACL) เพื่อให้มั่นใจว่าจะไม่มีบริการหรือข้อมูลสำคัญใด ๆ ของหน่วยงานถูกเข้าถึงโดยปราศจากการควบคุม*<br>*- ต้องกำหนดให้มีกลไกตรวจสอบและบังคับใช้ข้อจำกัดสิทธิการเข้าถึงอย่างต่อเนื่อง โดยจัดให้มีการตรวจสอบทบทวนสิทธิการเข้าใช้งานเป็นระยะอย่างสม่ำเสมอ, มีระบบแจ้งเตือนเมื่อตรวจพบพฤติกรรมการเข้าใช้งานคลาวด์ที่ผิดปกติ และเก็บบันทึกประวัติการเข้าใช้งาน (Access Logs) เพื่อใช้สำหรับวิเคราะห์และตรวจสอบย้อนหลังเมื่อเกิดเหตุความมั่นคงปลอดภัย* | | | | |
| 10 | ในกรณีที่หน่วยงานมีการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์ที่มีสิทธิสูง หรือโปรแกรมอรรถประโยชน์พิเศษ (Privileged Utility Programs เช่น Cloud CLI, Cloud Shell, Terraform หรือเครื่องมือจัดการฐานข้อมูล) บนระบบคลาวด์ หน่วยงานได้ตรวจสอบและยืนยันแล้วว่าเครื่องมือเหล่านี้ไม่รบกวนหรือ Override ระบบความปลอดภัยหลักของคลาวด์ ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบเอกสารทะเบียนควบคุมรายการโปรแกรมอรรถประโยชน์พิเศษ (Privileged Utility Programs) ที่ได้รับอนุญาตให้ใช้งานในระบบคลาวด์ โดยข้อมูลต้องระบุคุณลักษณะทางเทคนิคสำคัญ เช่น ชื่อโปรแกรม, วัตถุประสงค์การใช้งานเชิงเทคนิค, ข้อกำหนดหรือเงื่อนไขจำกัดในการรัน และระบุรายชื่อเจ้าหน้าที่ผู้ดูแลระบบที่มีสิทธิเข้าใช้งานอย่างเป็นทางการ*<br>*- ตรวจสอบหลักฐานและผลการประเมินความเสี่ยงอย่างเป็นลายลักษณ์อักษรก่อนเริ่มใช้งานโปรแกรมอรรถประโยชน์ เพื่อให้มั่นใจได้ว่าโปรแกรมจะไม่รบกวน Override หรือแก้ไขกลไกความปลอดภัยตามปกติของระบบคลาวด์ โดยตัวอย่างเครื่องมือที่มีความเสี่ยงสูงภายใต้ข้อกำหนดนี้ อาทิ*<br>*- Cloud CLIs: เช่น AWS CLI, Azure CLI, gcloud CLI (ความเสี่ยง: สั่งจัดการสิทธิทรัพยากร และข้อมูลโดยตรงผ่าน Command Line)*<br>*- Cloud Shells: เช่น Google Cloud Shell, Azure Cloud Shell (ความเสี่ยง: สั่งเปลี่ยนสถาปัตยกรรมและค่าคอนฟิกูเรชันผ่านเว็บบราวเซอร์)*<br>*- Infrastructure as Code (IaC) Engines: เช่น Terraform, Pulumi, AWS CloudFormation (ความเสี่ยง: การรันสคริปต์สิทธิสูงเปลี่ยนค่าระดับ Global ส่งผลกระทบต่อสถาปัตยกรรมและการแยกส่วนผู้เช่าร่วม)*<br>*- Storage Explorers: เช่น Azure Storage Explorer, Cyberduck, gsutil (ความเสี่ยง: ลักลอบเข้าถึง ดาวน์โหลด หรือลบข้อมูลปริมาณมหาศาลข้ามพ้นระบบการจำกัดสิทธิของหน้าแอปพลิเคชันปกติ)* | ทุกระดับ | 5.2.3.7 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารทะเบียนหรือบัญชีรายชื่อโปรแกรมอรรถประโยชน์พิเศษที่ได้รับอนุมัติให้ใช้งานจริงบนระบบคลาวด์*<br>*- เอกสารขั้นตอนปฏิบัติในการประเมินและอนุมัติการใช้งานเครื่องมือหรือโปรแกรมอรรถประโยชน์*<br>*- หลักฐานสกรีนช็อตรูปภาพแสดงการตั้งค่าเชิงเทคนิคจริง (เช่น การระบุ Role/Policy บนระบบ IAM, การจำกัดพอร์ต/ไอพีต้นทาง หรือประวัติการหมุนเวียน Access Keys สำหรับ CLI)*<br>*- ตัวอย่างรายงานประวัติการรันคำสั่งพิเศษ (CloudTrail/Cloud Audit Logs) ที่แสดงรายละเอียดบัญชีผู้รัน คำสั่ง วันเวลา และผลลัพธ์การทำงานอย่างโปร่งใส* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *- API Debugging Tools / DMS: เช่น Postman, cURL หรือ DMS Utilities (ความเสี่ยง: เข้าถึงและทำสำเนาโครงสร้างฐานข้อมูลเชิงลึก หรือส่งคำสั่ง API สั่งลบและแก้ไขค่าทรัพยากรบนคลาวด์โดยตรงเมื่อใช้ร่วมกับ Admin API Keys)* | | | | |
| 11 | หน่วยงานได้กำหนดขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยเป็นลายลักษณ์อักษรและตั้งค่าทางเทคนิคบนระบบคลาวด์เพื่อบังคับใช้งานจริงกับทุกประเภทบัญชี (ผู้ดูแลระบบ ผู้ใช้ทั่วไป และบัญชีบริการ/Service Account) โดยครอบคลุมเกณฑ์ควบคุมทางเทคนิค (เช่น นโยบายรหัสผ่าน MFA จำกัดจำนวนครั้งที่ใส่รหัสผิดแล้วล็อกอัตโนมัติ แจ้งเตือนเมื่อล็อกอินล้มเหลว กำหนดหมดเวลาใช้งาน/Session Timeout และบันทึก Log) เพื่อให้ระบบบังคับใช้อย่างเคร่งครัดใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีคู่มือหรือขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษรอย่างเป็นทางการที่ครอบคลุมมิติควบคุมทางเทคนิคในการเข้าสู่ระบบ ได้แก่ นโยบายความยากง่ายของรหัสผ่าน, การบังคับใช้ MFA, เกณฑ์การจำกัดจำนวนครั้งและระยะเวลาการล็อกบัญชี, ระบบการแจ้งเตือนความล้มเหลวในการเชื่อมต่อ, ระยะเวลาสิ้นสุดของ Session, และการเก็บบันทึกประวัติการพิสูจน์ตัวตน/การเข้าใช้งาน*<br>*- สอบทานว่าขั้นตอนและนโยบายความมั่นคงปลอดภัยนี้ระบุข้อกำหนดบังคับใช้กับบัญชีผู้ใช้ระบบคลาวด์ทุกประเภทที่หน่วยงานดูแล ได้แก่ บัญชีผู้ดูแลระบบ (Admin Accounts), บัญชีผู้ใช้งานทั่วไป (User Accounts), และบัญชีบริการ (Service Accounts / Programmatic Accounts) เพื่อให้มั่นใจว่าไม่มีช่องโหว่การละเลยสิทธิ*<br>*- ตรวจสอบว่าระบบคลาวด์ได้รับการกำหนดค่านโยบายความมั่นคงปลอดภัย (Security Policies / IAM Policies) จากศูนย์กลางเพื่อบังคับควบคุมโดยระบบโดยตรง โดยไม่ปล่อยให้การเปิดใช้มาตรการเหล่านั้น (เช่น การตั้งรหัสผ่านที่ซับซ้อน หรือการลงทะเบียน MFA) ขึ้นอยู่กับความสมัครใจหรือวิจารณญาณส่วนบุคคลของผู้ใช้งาน* | ทุกระดับ | 5.2.3.8 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารขั้นตอนสำหรับการเข้าสู่ระบบอย่างปลอดภัยบนบริการคลาวด์ (Secure Log-on Document)*<br>*- หลักฐานเชิงประจักษ์การตั้งค่าคอนฟิกระบบจริง (เช่น ภาพสกรีนช็อตรูปภาพแสดงการเปิดใช้งานเทคนิคบังคับ MFA ระดับ Domain, การตั้งค่า Account Lockout Policy, การตั้งค่า Idle Session Timeout ของระบบ Identity Provider (IdP) หรือหน้าคอนโซลคลาวด์หลัก)*<br>*- หลักฐานบันทึกเหตุการณ์การตรวจสอบสิทธิจริง (เช่น บันทึกประวัติประเภทรหัสการเข้าใช้งาน (Sign-in Logs) บนระบบ และบันทึกกิจกรรมการเข้าสู่ระบบที่ผิดพลาดซึ่งจัดเก็บไว้บนพื้นที่เก็บบันทึกประวัติอย่างปลอดภัย)* |
| **การเข้ารหัส (Cryptography)** | | | | | |
| 12 | หน่วยงานได้กำหนดและบังคับใช้มาตรการเข้ารหัสข้อมูล (Cryptographic Controls) บนระบบคลาวด์ที่ปลอดภัยและเหมาะสมกับความระดับเสี่ยง โดยครอบคลุมทั้งข้อมูลขณะจัดเก็บ (At-Rest) และระหว่างการส่งผ่าน (In-Transit) ไม่ว่าจะเป็นการตั้งค่าโดยหน่วยงานเอง หรือใช้ระบบของผู้ให้บริการคลาวด์ และหลีกเลี่ยงการใช้อัลกอริทึมที่ล้าสมัยหรือมีช่องโหว่ ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>* | ทุกระดับ | 5.2.4.1 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารนโยบายหรือข้อกำหนดด้านการเข้ารหัสสำหรับบริการคลาวด์ (Cryptography Policy / Encryption Standards for Cloud Services)*<br>*- รายงานผลการประเมินความเสี่ยง (Risk Assessment Report) ที่แสดงความเกี่ยวข้องและเชื่อมโยงมาเป็น* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *- ตรวจสอบว่าหน่วยงานมีมาตรการควบคุมการเข้ารหัส (Cryptographic Controls) ที่มีความแข็งแรงเพียงพอสำหรับระบบคลาวด์ที่ใช้งาน โดยสอดรับกับผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของข้อมูลและทรัพย์สินเฉพาะของระบบนั้น ๆ เช่น การเลือกขนาดความยาวกุญแจและอัลกอริทึมที่แปรผันตามระดับความสำคัญของข้อมูล*<br>*- พิจารณาว่ามาตรการเข้ารหัสปกป้องข้อมูลอย่างรอบด้าน ได้แก่ ข้อมูลขณะจัดเก็บ (Data at Rest) เช่น บน Object Storage, Block Storage หรือ Database และข้อมูลระหว่างการส่งผ่าน (Data in Transit) เช่น การรับส่งข้อมูลระหว่างผู้ใช้กับคลาวด์ หรือระหว่างระบบคลาวด์กับระบบภายในหน่วยงาน (On-Premise) ไม่ว่าจะเป็นการตั้งค่าโดยหน่วยงานเอง หรือใช้ระบบของผู้ให้บริการคลาวด์*<br>*- ตรวจสอบรายละเอียดการตั้งค่าใช้งานจริงบนระบบคลาวด์ เพื่อยืนยันว่าเป็นไปตามเกณฑ์มาตรฐานขั้นต่ำและไม่มีช่องโหว่ที่ทราบในปัจจุบัน อาทิ*<br>*- การใช้งานอัลกอริทึม AES-256 หรือเทียบเท่าสำหรับการเข้ารหัสข้อมูลขณะจัดเก็บ (Data at Rest)*<br>*- การใช้งานโปรโตคอล TLS 1.2 ขึ้นไป สำหรับการเข้ารหัสข้อมูลระหว่างส่งผ่าน (Data in Transit) และปิดการใช้งาน SSL/TLS เวอร์ชันเก่าที่มีช่องโหว่ความปลอดภัย* | | | | *เกณฑ์พื้นฐานในการออกแบบและเลือกมาตรการควบคุมการเข้ารหัสข้อมูล*<br>*- หลักฐานการตั้งค่าการเข้ารหัสจริงบนระบบคลาวด์ เช่น ภาพสกรีนช็อตรูปภาพแสดงสถานะการเปิดใช้มาตรการเข้ารหัสฝั่ง Server-side (เช่น SSE-S3, SSE-KMS ที่ระบุอัลกอริทึมความปลอดภัยสูงอย่าง AES-256) บนระบบจัดเก็บข้อมูล, ภาพรายงานผลทดสอบความมั่นคงปลอดภัยของพอร์ตเชื่อมต่อเว็บไซต์/API (เช่น SSL Labs Report) ที่ยืนยันการรองรับเฉพาะโปรโตคอล TLS 1.2 หรือ TLS 1.3 และปฏิเสธโปรโตคอลเวอร์ชันเก่า* |
| 13 | ในกรณีที่ผู้ให้บริการคลาวด์ มีการจัดหาระบบเข้ารหัสลับข้อมูลให้ใช้งาน หน่วยงานได้ขอข้อมูลมาทบทวนตรวจสอบ และบันทึกผลยืนยันหรือไม่ว่ามาตรการเข้ารหัสของผู้ให้บริการนั้น สอดคล้องตามนโยบายของหน่วยงาน เข้ากันได้กับระบบความปลอดภัยเดิมที่หน่วยงานใช้อยู่ และครอบคลุมการปกป้องข้อมูลทั้งขณะจัดเก็บ (At-Rest) และระหว่างการส่งผ่าน (In-Transit) ทั้งภายในและภายนอกระบบคลาวด์อย่างครบถ้วน ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีกระบวนการและมีการจัดทำบันทึกผลการตรวจสอบข้อมูลรายละเอียดคุณลักษณะการเข้ารหัสที่ได้รับจากผู้ให้บริการคลาวด์อย่างเป็นระบบและเป็นรูปธรรม*<br>*- สอบทานว่ามีการนำคุณลักษณะทางเทคนิคการเข้ารหัสที่ผู้ให้บริการใช้งานจริง (ได้แก่ ชนิดของ Algorithm ขนาดความยาวกุญแจ Protocol และกระบวนการจัดการคีย์) มาวิเคราะห์เปรียบเทียบกับเกณฑ์มาตรฐานขั้นต่ำที่กำหนดไว้ในนโยบายหรือมาตรฐานการเข้ารหัสภายในของหน่วยงาน*<br>*- ตรวจสอบระบบการเข้ารหัสและการจัดการกุญแจของผู้ให้บริการคลาวด์ สามารถทำงานร่วมกันได้ดี (Compatible) กับสถาปัตยกรรมระบบความปลอดภัยหรือระบบบริหารจัดการคีย์ (Key Management System) เดิมของหน่วยงาน เพื่อรับประกันว่าจะไม่มีปัญหาใน* | ทุกระดับ | 5.2.4.1 (ข) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารบันทึกหรือรายงานผลการประเมินความสอดคล้องของการเข้ารหัสของผู้ให้บริการคลาวด์ เทียบกับข้อกำหนดนโยบายความปลอดภัยไซเบอร์ของหน่วยงาน*<br>*- รายงานผลการวิเคราะห์ความเข้ากันได้เชิงระบบ (Compatibility & Integration Report) ที่ครอบคลุมความสามารถในการแลกเปลี่ยนข้อมูลและจัดการกุญแจเข้ารหัสร่วมกันโดยปราศจากข้อผิดพลาด*<br>*- หลักฐานการตรวจสอบยืนยันการปกป้องข้อมูลทั้งขณะจัดเก็บและระหว่างการโอนถ่าย (เช่น แผนภาพสถาปัตยกรรมโครงสร้างข้อมูล (Data Flow Diagram) และบันทึกผลทดสอบการแลกเปลี่ยนคีย์หรือการเข้ารหัสในแต่ละช่องทางการรับส่งข้อมูล)* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *การเข้ารหัสหรือถอดรหัสข้อมูลข้ามระบบ และไม่ก่อให้เกิดผลกระทบต่อประสิทธิภาพการปฏิบัติงานปกติ*<br>*- ประเมินบันทึกผลการตรวจทานว่าการเข้ารหัสของผู้ให้บริการครอบคลุมการคุ้มครองข้อมูลอย่างครบถ้วน ทั้งข้อมูลในขณะจัดเก็บ (Data at Rest) ในพื้นที่จัดเก็บของผู้ให้บริการ, ระหว่างการส่งผ่านข้อมูลภายในบริการคลาวด์ (Data in Transit), ระหว่างบริการคลาวด์ด้วยกัน และกรณีที่มีการส่งข้อมูลเชื่อมโยงกลับมายังโครงสร้างพื้นฐานหรือระบบภายในหน่วยงาน (On-Premise)* | | | | |
| 14 | หน่วยงานได้จัดทำทะเบียนและขั้นตอนปฏิบัติในการจัดการกุญแจเข้ารหัส (Key Management) เป็นลายลักษณ์อักษร เพื่อควบคุมกุญแจในทุกบริการคลาวด์อย่างครบถ้วนตลอดวงจรชีวิต (ตั้งแต่เริ่มสร้าง เปลี่ยนแปลงหรือปรับปรุง เก็บรักษาอย่างปลอดภัย จนถึงทำลายเมื่อเลิกใช้) พร้อมทั้งจำกัดสิทธิเข้าถึง และเก็บบันทึกประวัติการทำงาน (Audit Logs) เพื่อป้องกันความเสี่ยงและการตรวจสอบย้อนหลัง ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานจัดทำและปรับปรุงทะเบียนหรือบัญชีรายการกุญแจเข้ารหัสแยกตามบริการคลาวด์จริง โดยต้องระบุรายละเอียดสำคัญครบถ้วน ได้แก่ ชื่อหรือรหัสกุญแจ, บริการคลาวด์ที่ใช้งาน, วัตถุประสงค์, ประเภทกุญแจ (เช่น Secret Key, Private Key, Public Key, Master Key, Data Key), ผู้รับผิดชอบ และสถานที่จัดเก็บกุญแจอย่างมีระบบ*<br>*- ตรวจสอบความถูกต้องของคู่มือปฏิบัติการจัดการกุญแจ (Key Management Procedure) ว่าครอบคลุมขั้นตอนการทำงานทุกระยะของวงจรชีวิตกุญแจ ได้แก่ การสร้าง (Generation), การเปลี่ยนแปลงหรือปรับปรุง (Modification/Rotation), การจัดเก็บอย่างปลอดภัย (Secure Storage), การหมดอายุใช้งาน (Expiration), การเรียกคืน (Revocation), การเก็บรักษาสำรอง (Archive), และการทำลายกุญแจอย่างถาวร (Destruction)*<br>*- ตรวจสอบการใช้งานจริงว่ามีการจำกัดสิทธิการเข้าถึงกุญแจเข้ารหัสและระบบจัดการกุญแจ (Key Management Service - KMS) เฉพาะผู้ปฏิบัติงานที่มีความจำเป็นตามสิทธิขั้นต่ำและมีอำนาจหน้าที่เท่านั้น (Need-to-Know)*<br>*- สอบทานว่ามีบันทึกประวัติการดำเนินการ (Audit Logs) ที่สืบย้อนได้ในการสร้าง การหมุนเวียนคีย์ และการทำลายคีย์ ที่เป็นปัจจุบัน และป้องกันไม่ให้มีการแก้ไขหรือลบประวัติเหล่านั้น* | ทุกระดับ | 5.2.4.2 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารทะเบียนหรือบัญชีรายการกุญแจเข้ารหัสแยกตามบริการคลาวด์*<br>*- ขั้นตอนปฏิบัติหรือคู่มือการจัดการกุญแจเข้ารหัส (Key Management Procedure) ที่ครอบคลุมวงจรชีวิตของคีย์ทั้งหมด*<br>*- หลักฐานบันทึกการดำเนินการเกี่ยวกับกุญแจเข้ารหัส (Key Lifecycle Audit Logs) (เช่น รายงานหรือบันทึกประวัติการสร้าง การหมุนเวียน (Rotation) และการทำลายกุญแจจากระบบ KMS หรือ CloudTrail)*<br>*- ภาพหน้าจอแสดงการจำกัดสิทธิการเข้าถึงกุญแจ (Key Access Policy / Key Permission Settings) เช่น การตั้งค่า Key Policy บน Cloud KMS หรือ AWS KMS ที่จำกัดสิทธิเฉพาะบริการหรือผู้ใช้ที่เกี่ยวข้อง* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| 15 | ในกรณีที่หน่วยงานใช้งานระบบในการจัดการกุญแจเข้ารหัส (Key Management) ของผู้ให้บริการคลาวด์ หน่วยงานได้มีการร้องขอ ได้รับ และตรวจสอบเอกสาร/ข้อมูลจากผู้ให้บริการคลาวด์อย่างครบถ้วน (ครอบคลุมประเภทกุญแจ ข้อกำหนดเฉพาะของระบบการจัดการ ขั้นตอนปฏิบัติตลอดวงจรชีวิตของกุญแจ และคู่มือแนวทางจัดการกุญแจที่ปลอดภัยสำหรับผู้ใช้งาน) เพื่อใช้ดำเนินการอย่างปลอดภัย ใช่หรือไม่?<br>*แนวทางการประเมิน/ตรวจสอบ*<br>*- ตรวจสอบว่าหน่วยงานได้รับเอกสารคู่มือระบุรายละเอียดประเภทของกุญแจทั้งหมดที่ฟังก์ชันของระบบคลาวด์รองรับอย่างชัดเจน เช่น Secret Key, Private Key, Public Key, Master Key, Data Key, Customer Managed Key หรือ Provider Managed Key รวมถึงข้อมูลเกี่ยวกับระบบอัลกอริทึมและระดับความยาวของกุญแจที่ฟังก์ชันนั้น ๆ รองรับสำหรับการเข้ารหัสจริง*<br>*- ตรวจทานว่าระบบการจัดการกุญแจที่ผู้ให้บริการใช้มีการระบุคุณลักษณะเฉพาะและระดับการรักษาความมั่นคงปลอดภัยที่เป็นมาตรฐานสากล เช่น การได้รับการรับรองมาตรฐานระดับความปลอดภัยทางกายภาพและตรรกะระดับ FIPS 140-2 ตลอดจนระบุกระบวนการและรายละเอียดของกลไกสำรองกุญแจ (Key Backup Mechanisms) เพื่อป้องกันกรณีคีย์สูญหาย*<br>*- ประเมินพิจารณาว่ารายละเอียดขั้นตอนการปฏิบัติงานครอบคลุมกิจกรรมการควบคุมความปลอดภัยของกุญแจเข้ารหัสอย่างครบถ้วน ครอบคลุมขั้นตอนการทำงานทุกระยะของวงจรชีวิตกุญแจ ได้แก่ การสร้าง (Generation), การเปลี่ยนแปลงหรือปรับปรุง (Modification/Rotation), การจัดเก็บอย่างปลอดภัย (Secure Storage), การหมดอายุใช้งาน (Expiration), การเรียกคืน (Revocation), การเก็บรักษาสำรอง (Archive), และการทำลายกุญแจอย่างถาวร (Destruction)*<br>*- ตรวจสอบว่าหน่วยงานได้รับข้อมูลเกี่ยวกับคู่มือหรือแนวทางปฏิบัติแนะนำสำหรับการใช้งานจริงที่ผู้ให้บริการคลาวด์จัดเตรียมไว้ให้เพื่อลดความเสี่ยง เช่น ความถี่ขั้นต่ำที่เหมาะสมในการกำหนดให้มีการหมุนเวียนกุญแจ (Recommended Key Rotation Frequency), วิธีการหรือแนวปฏิบัติในการดูแลรักษาและจัดเก็บกุญแจอย่างปลอดภัย, ขั้นตอนการสถาปนาระบบสำรองและกู้คืนกุญแจเข้ารหัสกลับมาใช้งานใหม่เมื่อเกิดวิกฤต ตลอดจนข้อพิจารณาหรือข้อควรระวังพิเศษทางเทคนิคในการใช้งาน* | ทุกระดับ | 5.2.4.2 (ข) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *ตัวอย่างหลักฐาน*<br>*- เอกสารชี้แจงรายละเอียดประเภทของกุญแจที่รองรับ รวมถึงรายละเอียดข้อมูลอัลกอริทึมและการตั้งค่าความยาวกุญแจที่ได้รับจากผู้ให้บริการคลาวด์*<br>*- เอกสารข้อกำหนดเฉพาะของระบบจัดการกุญแจคลาวด์ และหลักฐานการรับรองมาตรฐานความปลอดภัยของระบบ (เช่น เอกสารรับรองสากล FIPS 140-2 หรือข้อมูลสถาปัตยกรรมระบบสำรองกุญแจ)*<br>*- เอกสารคู่มือหรือขั้นตอนปฏิบัติการจัดการกุญแจตลอดอายุการใช้งาน (Key Lifecycle) ที่ครอบคลุมทุกวงจรการบริหารคีย์อย่างปลอดภัย*<br>*- เอกสารแนวทางการบริหารจัดการกุญแจที่แนะนำสำหรับหน่วยงาน (เช่น บันทึกข้อตกลงหรือคำแนะนำเกณฑ์การหมุนเวียนคีย์ วิธีการเก็บบันทึกประวัติ หรือขั้นตอนการกู้คืนกุญแจเมื่อเกิดสถานการณ์ภัยพิบัติ)* |
| 16 | ในกรณีที่หน่วยงานเลือกใช้กุญแจเข้ารหัสของตนเอง (เช่น BYOK หรือ HYOK) หน่วยงานมีข้อตกลงในสัญญาบริการคลาวด์ที่ห้ามผู้ให้บริการคลาวด์เข้าถึง จัดเก็บ หรือจัดการกุญแจโดยปริยาย โดยอาจมีการออกแบบสถาปัตยกรรม | ทุกระดับ | 5.2.4.2 (ค) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน | *ตัวอย่างหลักฐาน*<br>*- เอกสารสัญญาบริการคลาวด์ (Cloud Service Agreement) ในส่วนเนื้อหาที่ระบุ ข้อจำกัดสิทธิและการห้ามผู้* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | ทางเทคนิคจริงเพื่อบล็อกไม่ให้ผู้ให้บริการเข้าถึงกุญแจเข้ารหัสได้ในทางปฏิบัติ (เช่น การใช้ Client-side Encryption หรือจัดเก็บกุญแจไว้ในอุปกรณ์ HSM ภายในหน่วยงาน) ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- สอบทานว่าในสัญญาการใช้บริการคลาวด์ มีข้อตกลงที่เป็นลายลักษณ์อักษรที่ระบุอย่างเป็นทางการว่าผู้ให้บริการคลาวด์ไม่มีสิทธิในการจัดเก็บ ประมวลผล หรือจัดการกุญแจเข้ารหัสที่เป็นของหน่วยงาน และต้องปราศจากข้อกำหนดใด ๆ ที่อนุญาตให้ผู้ให้บริการล่วงรู้หรือเข้าถึงข้อมูลกุญแจเข้ารหัสโดยปริยาย*<br>*- ประเมินความมั่นใจทางเทคนิคว่าระบบคลาวด์ของผู้ให้บริการจะไม่สามารถเข้าถึง จัดเก็บหรือบริหารจัดการกุญแจเข้ารหัสของหน่วยงานได้ โดยตรวจสอบวิธีการตั้งค่าการใช้งานจริง*<br>*- Client-side Encryption: ตรวจสอบว่าระบบจัดทำกระบวนการเข้ารหัสลับที่ฝั่งต้นทาง (ผู้ใช้บริการ) เสร็จสิ้นสมบูรณ์ก่อนที่จะมีการส่งต่อไฟล์ข้อมูลขึ้นไปจัดเก็บบนคลาวด์ เพื่อรับประกันว่าชุดกุญแจเข้ารหัสจะไม่มีวันถูกส่งผ่านทางเครือข่ายไปยังพื้นที่ของผู้ให้บริการ*<br>*- Hold Your Own Key (HYOK): สอบทานการเชื่อมโยงระบบเข้ารหัสโดยที่หน่วยงานคงความเป็นเจ้าของและควบคุมดูแลกระบวนการถอนและเข้ารหัสไว้ภายนอกพื้นที่คลาวด์ของผู้ให้บริการอย่างเด็ดขาด*<br>*- Hardware Security Module (HSM): ตรวจสอบพิกัดการจัดเก็บกุญแจลับว่าถูกป้องกันอยู่ภายในอุปกรณ์ฮาร์ดแวร์ความปลอดภัยสูง (HSM) ที่ตั้งอยู่ภายในศูนย์ข้อมูลของหน่วยงานเอง เพื่อทำหน้าที่จัดการและหมุนเวียนกุญแจทดแทนการพึ่งพาระบบของผู้ให้บริการ* | | | ☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *ให้บริการเข้าถึงหรือจัดการกุญแจเข้ารหัสของหน่วยงาน*<br>*- แผนภาพสถาปัตยกรรมการจัดการกุญแจ (Key Management Architecture Diagram) และผลการตรวจสอบการตั้งค่า Client-side Encryption จริง*<br>*- เอกสารสถาปัตยกรรมระบบคลาวด์ที่ระบุเทคนิคการจัดการกุญแจและการระบุพิกัดที่ตั้งของอุปกรณ์ HSM หรือระบบจัดเก็บกุญแจหลักภายนอกผู้ให้บริการคลาวด์* |
| **การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)** | | | | | |
| 17 | หน่วยงานได้บังคับใช้มาตรการควบคุมที่ตั้งข้อมูล (Data Localization) โดย<u>กำหนดให้ใช้ศูนย์ข้อมูลหลักในประเทศไทย</u> และตรวจสอบการตั้งค่าระบบ (Region Configuration) จริง ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีนโยบายหรือข้อกำหนดที่เป็นลายลักษณ์อักษรที่ระบุอย่างเป็นทางการให้ใช้ศูนย์ข้อมูลหลักที่ตั้งอยู่ในประเทศไทยสำหรับการจัดเก็บและประมวลผลข้อมูล โดยต้องมีการระบุประเภทข้อมูลที่ต้องจัดเก็บในประเทศไทย ข้อยกเว้น (ถ้ามี) และระบุเหตุผลทางกฎหมายหรือกฎระเบียบที่สนับสนุนข้อกำหนดดังกล่าวอย่างชัดเจน*<br>*- สอบทานสัญญาการใช้บริการคลาวด์ ว่าระบุข้อกำหนดให้ใช้ศูนย์ข้อมูลหลักในประเทศไทยอย่างชัดเจน โดยครอบคลุมถึงการระบุพิกัดที่ตั้งศูนย์ข้อมูลหลักที่จะใช้ ข้อจำกัดการโอนย้าย* | ระดับสูง | 5.2.5.1 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารนโยบายหรือข้อกำหนดด้าน Data Localization ของหน่วยงาน*<br>*- สัญญาบริการคลาวด์ (Cloud Service Agreement) หรือข้อตกลงระดับบริการ (SLA) ที่ระบุข้อกำหนดด้านที่ตั้งศูนย์ข้อมูลหลัก ข้อจำกัดการโอนย้ายข้อมูล และการแจ้งเตือนเมื่อมีการเปลี่ยนแปลง*<br>*- หลักฐานการตั้งค่าภูมิภาคจริงบนบริการคลาวด์ (Region Configuration Screenshots)* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *ข้อมูลออกนอกประเทศ เงื่อนไขในการแจ้งเตือนล่วงหน้าหากผู้ให้บริการคลาวด์มีการเปลี่ยนแปลงที่ตั้งศูนย์ข้อมูล และระบุบทลงโทษกรณีที่ผู้ให้บริการไม่ปฏิบัติตามสัญญา*<br>*- พิจารณาและตรวจสอบจากข้อมูลที่ผู้ให้บริการคลาวด์จัดเตรียมให้ เช่น เอกสารสถาปัตยกรรม (Architecture) หลักฐานพิกัดที่ตั้งทางกายภาพของศูนย์ข้อมูล เพื่อยืนยันว่าข้อมูลของหน่วยงานถูกจัดเก็บและประมวลผลในศูนย์ข้อมูลที่ตั้งอยู่ในประเทศไทยจริง* | | | | |
| 18 | หน่วยงานได้ร้องขอและได้รับเอกสารหลักฐานยืนยันจากผู้ให้บริการคลาวด์หรือไม่ว่า มีนโยบายและขั้นตอนปฏิบัติในการกำจัด ทำลาย หรือนำอุปกรณ์จัดเก็บข้อมูลและทรัพยากรระบบกลับมาหมุนเวียนใช้ใหม่ซ้ำอย่างปลอดภัย (Secure Disposal or Reuse of Resources) เพื่อให้มั่นใจได้ว่าข้อมูลของหน่วยงานจะไม่สามารถถูกกู้คืนกลับมาได้อีกหลังจากเลิกใช้งาน ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีพยานหลักฐานที่ชัดเจนในการขอและได้รับเอกสารยืนยันคุณลักษณะการทำงานจากผู้ให้บริการคลาวด์ ว่ามีกระบวนการและระบบที่ได้มาตรฐานสากลในการทำลาย การคืนสภาพ หรือกำจัดทรัพยากร (เช่น อุปกรณ์ฮาร์ดแวร์จัดเก็บข้อมูล ไฟล์ข้อมูล หรือหน่วยความจำชั่วคราว) อย่างปลอดภัยและทันท่วงทีเมื่อหมดวาระการใช้งาน*<br>*- ทบทวนว่ากระบวนการประเมินของผู้ให้บริการคลาวด์ มีการระบุมาตรการขั้นสูงสำหรับการทำลายข้อมูลส่วนบุคคล โดยกำหนดให้อุปกรณ์ที่มีสื่อจัดเก็บข้อมูลที่อาจมีข้อมูลส่วนบุคคลของหน่วยงานตกค้างอยู่ ต้องได้รับการปฏิบัติตามมาตรฐานความปลอดภัยเสมือนว่ามีข้อมูลส่วนบุคคลจริงบันทึกอยู่ เพื่อป้องกันการรั่วไหล* | ระดับสูง | 5.2.5.2 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *<u>ตัวอย่างหลักฐาน</u>*<br>*- สำเนานโยบายและขั้นตอนการปฏิบัติงานจริง ของผู้ให้บริการคลาวด์ (Secure Disposal Policy / Sanitization SOP of CSP)*<br>*- ใบรับรองมาตรฐานสากล ที่ครอบคลุมขอบเขตการกำจัดและทำลายข้อมูล (เช่น ISO/IEC 27001, ISO/IEC 27017 หรือ ISO/IEC 27018 Certification)*<br>*- รายงานการตรวจสอบที่จัดทำโดยบุคคลที่สามหรือผู้ตรวจสอบอิสระภายนอก ที่น่าเชื่อถือ (เช่น Reports on Compliance, SOC 2 Type II Report) ในหัวข้อความปลอดภัยทางกายภาพและการทำลายอุปกรณ์จัดเก็บข้อมูล* |
| **การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)** | | | | | |
| 19 | หน่วยงานได้จัดทำกระบวนการจัดการการเปลี่ยนแปลง (Change Management) เป็นลายลักษณ์อักษร ซึ่งรองรับการรับแจ้งและวิเคราะห์ผลกระทบจากการเปลี่ยนแปลงฝั่งผู้ให้บริการคลาวด์ (เช่น การปรับโครงสร้างพื้นฐาน, การปิดหรือเปลี่ยนฟีเจอร์, การซ่อมบำรุงตามรอบ, การย้ายตำแหน่งศูนย์ข้อมูล หรือการเปลี่ยนเงื่อนไขบริการ) ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- สอบทานว่าหน่วยงานมีคู่มือหรือเอกสารขั้นตอนปฏิบัติงาน “การจัดการการเปลี่ยนแปลง” (Change Management Procedure) ที่ผ่านการอนุมัติใช้งานอย่างเป็นทางการ โดยมีเนื้อหาที่ระบุถึงวิธีการรับมือ ตรวจสอบ และวิเคราะห์ผลกระทบเชิงความมั่นคงปลอดภัย* | ระดับสูง | 5.2.6.1 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารขั้นตอนปฏิบัติการจัดการการเปลี่ยนแปลงของหน่วยงาน (Change Management Procedure) ที่มีขอบเขตและระบุกระบวนการรับมือผลกระทบจากผู้ให้บริการคลาวด์อย่างมีลายลักษณ์อักษร*<br>*- หลักฐานการรับแจ้งการเปลี่ยนแปลงที่ได้รับจากผู้ให้บริการคลาวด์ (Change Notifications / Advisories) (เช่น ภาพหน้าจอคอนโซลการแจ้งเตือนจากระบบ Cloud Portal, อีเมลแจ้งเตือนกำหนดเวลา* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *และประสิทธิภาพของระบบที่อาจเกิดขึ้นจากการดำเนินการใด ๆ ของผู้ให้บริการคลาวด์อย่างชัดเจน*<br>*- ตรวจสอบช่องทางที่หน่วยงานเลือกใช้ในการเฝ้าติดตามข่าวสารและสืบค้นแผนการปรับปรุงระบบงานล่วงหน้าจากผู้ให้บริการคลาวด์ เพื่อยืนยันว่าช่องทางนั้นมีความน่าเชื่อถือและทำงานร่วมกันเป็นระบบ (เช่น การรับข้อความผ่าน Cloud Service Health Dashboard, อีเมลแจ้งเตือนผู้ดูแลระบบ หรือช่องทางประสานงานทางเทคนิคอื่น ๆ)*<br>*- ทบทวนว่าเอกสารกระบวนการและกิจกรรมประเมินผลกระทบของหน่วยงาน ครอบคลุมชนิดและกรอบของการเปลี่ยนแปลงทางฝั่งผู้ให้บริการครบทุก ประเภทหลักตามที่เกณฑ์มาตรฐานกำหนดอย่างถูกต้อง* | | | | *ซ่อมบำรุงล่วงหน้า หรือประกาศปรับเปลี่ยนเงื่อนไขการใช้บริการ)*<br>*- บันทึกผลการประเมินผลกระทบและแผนรองรับการเปลี่ยนแปลง (Impact Assessment and Action Plan Reports) สำหรับการเปลี่ยนแปลงทางเทคนิคและข้อตกลงที่ได้รับการทบทวนและผ่านกระบวนการลงนามอนุมัติโดยหัวหน้างานหรือคณะทำงานไอทีของหน่วยงาน* |
| 20 | หน่วยงานได้ตรวจสอบและมั่นใจว่า ประสิทธิภาพและขนาดทรัพยากรคลาวด์ (เช่น CPU, RAM, พื้นที่จัดเก็บข้อมูล และ Bandwidth) ที่ใช้งานจริง ตรงตามความต้องการและข้อตกลงระดับการให้บริการ (SLA) และใช้เครื่องมือตรวจสอบ (Monitoring Tools) เพื่อติดตามและเปรียบเทียบประสิทธิภาพอย่างสม่ำเสมอ ใช่หรือไม่?<br><u>*แนวทางการประเมิน/ตรวจสอบ*</u><br>*- ตรวจสอบสัญญาการใช้บริการคลาวด์ หรือข้อตกลงระดับการให้บริการ (SLA) ว่ามีการระบุขีดความสามารถของทรัพยากรที่ผู้ให้บริการรับประกันไว้อย่างเป็นลายลักษณ์อักษรและชัดเจน (อาทิ ขนาดพื้นที่จัดเก็บข้อมูล (Storage Size), จำนวนแกนประมวลผล (CPU Cores), หน่วยความจำ (Memory) และแบนด์วิดท์ (Bandwidth) เป็นต้น)*<br>*- พิจารณากระบวนการตรวจสอบประสิทธิภาพว่าหน่วยงานมีขั้นตอนปฏิบัติในการเฝ้าติดตามการใช้งานจริงว่าตรงตามข้อตกลงหรือไม่ โดยตรวจดูว่ามีการใช้งานเครื่องมือตรวจสอบประสิทธิภาพ (Monitoring Tools) ของคลาวด์เพื่อดึงข้อมูลสถิติมาเปรียบเทียบกับข้อตกลงระดับการให้บริการใน SLA อย่างสม่ำเสมอ* | ระดับสูง | 5.2.6.2 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | <u>*ตัวอย่างหลักฐาน*</u><br>*- เอกสารสัญญาบริการคลาวด์ (Cloud Service Agreement) หรือข้อตกลงระดับการให้บริการ (SLA) ส่วนที่ระบุข้อกำหนดการรับประกันขีดความสามารถของทรัพยากร*<br>*- สกรีนช็อตรูปภาพแสดงการตั้งค่าและหน้าแดชบอร์ดของเครื่องมือตรวจสอบประสิทธิภาพ (Monitoring Tools Dashboard) ที่ใช้งานจริงบนระบบคลาวด์*<br>*- รายงานสถิติประสิทธิภาพและการใช้งานทรัพยากรคลาวด์ (Performance & Resource Utilization Reports) ที่ได้จากเครื่องมือติดตาม เพื่อเปรียบเทียบความสอดคล้องกับเกณฑ์ใน SLA* |
| 21 | หน่วยงานมีการติดตามการใช้งานบริการคลาวด์อย่างสม่ำเสมอ และมีกระบวนการคาดการณ์ความต้องการทรัพยากรล่วงหน้า (Capacity Forecasting) เพื่อรักษาประสิทธิภาพการทำงานของระบบในระยะยาวและพร้อมรองรับการเติบโตในอนาคต ใช่หรือไม่?<br><u>*แนวทางการประเมิน/ตรวจสอบ*</u><br>*- ตรวจสอบว่าหน่วยงานจัดให้มีระบบ ขั้นตอน หรือเครื่องมือในการติดตามปริมาณและประสิทธิภาพการใช้งานทรัพยากรจริงบนระบบคลาวด์ (Cloud Service Usage Monitoring) เป็นประจำและต่อเนื่อง (เช่น เครื่องแม่ข่ายเสมือน (Compute), พื้นที่จัดเก็บ* | ระดับสูง | 5.2.6.2 (ข) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | <u>*ตัวอย่างหลักฐาน*</u><br>*- รายงานการวิเคราะห์แนวโน้มการใช้ทรัพยากร (Resource Trend Analysis Report) ย้อนหลัง เพื่อแสดงสถิติประวัติการใช้งานจริง*<br>*- เอกสารการคาดการณ์ความต้องการด้านขีดความสามารถของทรัพยากร (Capacity Forecasting) หรือแผนการขยายความจุคลาวด์ในอนาคตที่ผ่านการอนุมัติ* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *ข้อมูล (Storage) และแบนด์วิดท์เครือข่าย (Network Bandwidth)) เพื่อวิเคราะห์สถานะการทำงานในปัจจุบัน*<br>*- ตรวจสอบว่าหน่วยงานจัดให้มีกระบวนการวิเคราะห์และคาดการณ์ความต้องการด้านขีดความสามารถของทรัพยากรล่วงหน้า (Capacity Forecasting) เพื่อเตรียมพร้อมขยายระบบหรือปรับเปลี่ยนขนาดทรัพยากรให้สอดคล้องกับแนวโน้มปริมาณงานและการเติบโตทางธุรกิจในอนาคต ป้องกันปัญหาคอขวด (Bottleneck) หรือความล่าช้าในการประมวลผล*<br>*- ทบทวนว่ารายงานหรือผลลัพธ์การคาดการณ์มีการอ้างอิงจากข้อมูลสถิติจริงที่เก็บรวบรวมไว้ เพื่อประเมินความสมเหตุสมผลของการคาดการณ์* | | | | *- ภาพสกรีนช็อตรูปภาพแสดงผลการทำงานและแดชบอร์ดการตั้งค่าแจ้งเตือน (Alert Configuration Metrics) ของเครื่องมือตรวจสอบประสิทธิภาพเมื่อระบบมีปริมาณการใช้งานทรัพยากรเข้าใกล้ขีดจำกัดสูงสุด (เช่น แจ้งเตือนเมื่อ CPU/Disk เกิน 80%)* |
| 22 | ในกรณีที่ผู้ให้บริการคลาวด์มีระบบสำรองข้อมูลให้ใช้งาน หน่วยงานได้กำหนดความต้องการในการสำรองข้อมูลของตนเองอย่างไว้ชัดเจน และได้ขอเอกสารข้อมูลจำเพาะด้านความสามารถในการสำรองข้อมูล (Backup Specifications) จากผู้ให้บริการคลาวด์ เพื่อมาเปรียบเทียบและยืนยันว่าระบบสำรองข้อมูลของคลาวด์นั้นตอบโจทย์และตรงตามข้อกำหนดของหน่วยงานจริง ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- สอบทานว่าหน่วยงานจัดทำนโยบาย คู่มือ หรือขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษรที่ระบุข้อกำหนดด้านการสำรองข้อมูล (Backup Requirements) โดยข้อกำหนดดังกล่าวต้องระบุเงื่อนไขและเป้าหมายการดำเนินงานอย่างชัดเจน ครอบคลุมถึง ขอบเขตข้อมูลที่ต้องสำรอง, ความถี่ในการรันระบบสำรองข้อมูล, ระยะเวลาการจัดเก็บรักษาข้อมูลสำรอง (Retention Period), ข้อกำหนดการเข้ารหัสเพื่อความปลอดภัยของข้อมูลสำรอง, สถานที่หรือภูมิภาคที่ระบุจัดเก็บข้อมูลสำรอง, รวมถึงเป้าหมายระยะเวลาสูงสุดที่ยอมรับได้ในการกู้คืนระบบ (Recovery Time Objective: RTO) และเป้าหมายจุดเวลาการสูญเสียข้อมูลสูงสุดที่ยอมรับได้ (Recovery Point Objective: RPO)*<br>*- ตรวจสอบหลักฐานการร้องขอและเอกสารแสดงรายละเอียดข้อมูลจำเพาะความสามารถในการสำรองข้อมูล (Backup Specifications) ที่ได้รับจากผู้ให้บริการคลาวด์ ซึ่งต้องระบุคุณลักษณะทางเทคนิคอย่างครอบคลุม ได้แก่ ขอบเขตและตารางเวลาสำรอง, วิธีการและฟอร์แมตข้อมูล, วิธีการเข้ารหัสข้อมูล, ระยะเวลารับประกันการจัดเก็บข้อมูลสำรอง, กระบวนการตรวจสอบความครบถ้วนและถูกต้อง (Integrity Check), ขั้นตอนและระยะเวลาในการกู้คืนระบบจากข้อมูลสำรอง, ขั้นตอนการทำซ้ำหรือซ้อมทดสอบระบบสำรองข้อมูล และสถานที่จัดเก็บกู้ข้อมูลสำรองจริง*<br>*- ตรวจสอบรายงานผลการเปรียบเทียบและการประเมินว่าขีดความสามารถการสำรองข้อมูลจริงที่ผู้ให้บริการคลาวด์จัดหาให้นั้น สอดคล้องและตอบสนองต่อเงื่อนไขข้อกำหนดด้านการสำรองข้อมูลของหน่วยงานหรือไม่ รวมถึงตรวจสอบประวัติการระบุช่องว่างด้าน* | ระดับสูง | 5.2.6.3 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารข้อกำหนดด้านการสำรองข้อมูลของหน่วยงาน (Backup Requirements)*<br>*- ข้อมูลจำเพาะความสามารถในการสำรองข้อมูลที่ได้รับจากผู้ให้บริการคลาวด์ (Backup Specifications from CSP)*<br>*- รายงานการเปรียบเทียบและวิเคราะห์ความสอดคล้องระหว่างข้อกำหนดของหน่วยงานกับขีดความสามารถจริงของคลาวด์ (Gap Analysis & Comparison Report)* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *ความปลอดภัย (Gaps) และแผนบริหารจัดการเพื่อลดหรือควบคุมความเสี่ยงจากช่องว่างที่พบอย่างเป็นระบบ* | | | | |
| 23 | ในกรณีที่ผู้ให้บริการคลาวด์ไม่ได้มีระบบสำรองข้อมูลให้ใช้งาน หน่วยงานได้จัดทำขั้นตอนปฏิบัติและทำการสำรองข้อมูลด้วยตนเอง (Self-managed Backup) โดยครอบคลุมตั้งแต่ ขอบเขตข้อมูล ความถี่ วิธีการ สถานที่จัดเก็บ การเข้ารหัส ระยะเวลาเก็บรักษา และขั้นตอนการกู้คืนข้อมูลจริง ใช่หรือไม่?<br>*แนวทางการประเมิน/ตรวจสอบ*<br>*- ตรวจสอบว่าหน่วยงานมีเอกสารคู่มือหรือขั้นตอนปฏิบัติที่เป็นลายลักษณ์อักษรสำหรับการสำรองข้อมูลด้วยตนเอง (Self-managed Backup Procedure) ที่ประกาศใช้อย่างเป็นทางการ โดยรายละเอียดต้องไม่เป็นเพียงโครงร่างกว้าง ๆ แต่ต้องครอบคลุมพารามิเตอร์ควบคุมสำคัญทุกประการ ขอบเขตข้อมูล, ความถี่, วิธีการและฟอร์แมตข้อมูล, สถานที่จัดเก็บ, มาตรการเข้ารหัสความมั่นคงปลอดภัย, ระยะเวลาจัดเก็บ (Retention Period) และขั้นตอนการกู้คืนระบบ*<br>*- ทำการตรวจสอบเพื่อยืนยันว่าหน่วยงานมีการบังคับใช้ขั้นตอนปฏิบัติดังกล่าวจริงบนระบบงานคลาวด์ โดยตรวจสอบว่ามีระบบหรือเครื่องมืออัตโนมัติ (เช่น Cron jobs, Cloud Native Backup Policies, Scripts) ที่รันกิจกรรมการสำรองข้อมูลสอดคล้องตามขอบเขตและรอบความถี่ที่กำหนดไว้ในเอกสารจริง*<br>*- สอบทานว่าขั้นตอนการกู้คืน (Restore/Recovery Procedure) มีกระบวนการที่เป็นรูปธรรม มีการระบุขั้นตอนแก้ไขปัญหาเมื่อระบบล้มเหลว และมีการซักซ้อมหรือทดสอบนำไฟล์สำรองดังกล่าวมากู้คืนใช้งานจริงเพื่อตรวจสอบความถูกต้องสมบูรณ์ของข้อมูลอย่างสม่ำเสมอ* | ระดับสูง | 5.2.6.3 (ข) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *ตัวอย่างหลักฐาน*<br>*- เอกสารขั้นตอนปฏิบัติสำหรับการสำรองข้อมูลที่อยู่ในความรับผิดชอบของผู้ใช้บริการ (Self-managed Backup Procedures)*<br>*- หลักฐานการตั้งค่าเชิงเทคนิคจริงบนระบบคลาวด์ (เช่น ภาพสกรีนช็อตรูปภาพการตั้งค่า Backup Job, Configuration policy บนบริการคลาวด์ หรือสคริปต์อัตโนมัติที่ใช้จัดเก็บไฟล์)*<br>*- หลักฐานบันทึกผลการสำรองและกู้คืนข้อมูลจริง (เช่น รายงานผลสำเร็จของการ Backup ย้อนหลัง, บันทึกการรันระบบสำรองข้อมูล (Backup Logs) หรือรายงานบันทึกการซักซ้อมแผนทดสอบกู้คืนข้อมูลสำรอง (Restore Test Logs))* |
| 24 | หน่วยงานได้จัดทำข้อกำหนดการบันทึกเหตุการณ์ (Event Logging) เป็นลายลักษณ์อักษร และตรวจสอบแล้วว่าบริการคลาวด์ที่ใช้งานมีการเปิดใช้งานนั้นตรงตามเกณฑ์ของหน่วยงานจริง ใช่หรือไม่?<br>*แนวทางการประเมิน/ตรวจสอบ*<br>*- ตรวจสอบว่าหน่วยงานมีเอกสารระบุข้อกำหนดด้านการเก็บบันทึกเหตุการณ์ (Event Logging Requirements) ที่ผ่านการอนุมัติและประกาศใช้อย่างเป็นทางการ ควรครอบคลุมประเด็นสำคัญ ดังนี้*<br>*- ประเภทเหตุการณ์ที่ต้องบันทึก: ครอบคลุมเหตุการณ์เชิงระบบและพฤติกรรมผู้ใช้ที่สำคัญ เช่น การเข้าสู่ระบบ (Log-on), การเปลี่ยนแปลงสิทธิการใช้งาน (Privilege Changes), การเข้าถึงข้อมูลสำคัญ, การดำเนินกิจกรรมของบัญชีผู้ดูแลระบบ* | ระดับสูง | 5.2.6.4 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *ตัวอย่างหลักฐาน*<br>*- เอกสารข้อกำหนดสำหรับการบันทึกเหตุการณ์ของหน่วยงาน (Event Logging Requirements)*<br>*- รายงานการเปรียบเทียบข้อกำหนดกับความสามารถจริงของผู้ให้บริการคลาวด์ (Gap Analysis Report)*<br>*- หลักฐานการตั้งค่าการบันทึกเหตุการณ์จริงบนบริการคลาวด์ (Configuration Screenshots)*<br>*- ตัวอย่างบันทึกเหตุการณ์จริงจากระบบงาน (Sample Audit Logs)*<br>*- เอกสารหรือหลักฐานการตั้งสิทธิควบคุมการเข้าถึงระบบ Log (เช่น S3* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *(Administrator/Privileged Activities) และการเปลี่ยนแปลงค่ากำหนดและการตั้งค่าความมั่นคงปลอดภัยของระบบ*<br>*- รายละเอียดข้อมูลที่ต้องบันทึกในแต่ละ Log: อย่างน้อยต้องประกอบด้วย วันและเวลาที่เกิดเหตุการณ์ (Timestamp), บัญชีผู้ใช้หรือผู้ดำเนินกิจกรรม (Actor/User ID), ทรัพยากรระบบหรือข้อมูลที่ถูกเข้าถึง (Target Resource) และผลลัพธ์ของการดำเนินการ (สำเร็จหรือล้มเหลว)*<br>*- การเก็บรักษาและการปกป้องความสมบูรณ์: กำหนดกรอบระยะเวลาจัดเก็บรักษา Log และบังคับใช้กลไกในการปกป้องความสมบูรณ์และครบถ้วนของบันทึกเหตุการณ์ เพื่อป้องกันการแก้ไข ดัดแปลง หรือลบทำลายบันทึกอย่างไม่เหมาะสม*<br>*- สอบทานบันทึกรายงานหรือผลการเปรียบเทียบระหว่างคุณลักษณะความปลอดภัยด้านการบันทึกเหตุการณ์ที่ผู้ให้บริการคลาวด์มีให้ตามปกติ กับข้อกำหนดขั้นต่ำของหน่วยงาน เพื่อชี้บ่งจุดที่ยังเป็นช่องว่าง (Gaps) และกำหนดแผนงานบริหารความเสี่ยงหรือระบบจัดการ Log เสริมมาตรการความปลอดภัยในส่วนที่ผู้ให้บริการคลาวด์ไม่มีบริการรองรับ*<br>*- ตรวจสอบสถานะการเปิดใช้งานเชิงเทคนิคจริงบนคอนโซลควบคุมบริการคลาวด์ เพื่อรับประกันว่าระบบบันทึกเหตุการณ์ที่สำคัญได้รับการเปิดใช้งานอย่างสมบูรณ์ (เช่น Audit Log, Access Log, Activity Log หรือ System Log) และมีการตั้งนโยบายอายุการจัดเก็บข้อมูล (Retention Policy) สอดคล้องตามระยะเวลาที่กฎหมายและนโยบายระบุไว้* | | | | *Bucket Lock, Log Destination Policies หรือ IAM Restriction)* |
| 25 | ในกรณีที่บันทึกเหตุการณ์ (Event Logs) มีข้อมูลส่วนบุคคลปะปนอยู่ หน่วยงานได้จำกัดสิทธิการเข้าถึงตามความจำเป็น (Need-to-Know) และใช้มาตรการทางเทคนิคเพื่อปกป้องข้อมูลส่วนบุคคลใน Log (เช่น การเข้ารหัส การปิดบังข้อมูล/Masking และการสุ่มทบทวนสิทธิเข้าใช้งานอย่างสม่ำเสมอ) เพื่อป้องกันไม่ให้มีการนำข้อมูล Log ไปใช้งานผิดวัตถุประสงค์ ใช่หรือไม่?<br><u>แนวทางการประเมิน/ตรวจสอบ</u><br>*- ตรวจสอบว่าหน่วยงานจัดให้มีมาตรการจำกัดสิทธิเข้าถึงบันทึกเหตุการณ์ (Event Logs) ที่อาจมีข้อมูลส่วนบุคคลปะปนอยู่ เพื่อควบคุมการใช้งานให้เป็นไปตามวัตถุประสงค์ที่กำหนดเท่านั้น โดยพิจารณาจากการกำหนดสิทธิการเข้าถึงตามหลักการความจำเป็นต้องรู้ (Need-to-Know), กระบวนการยืนยันตัวตนของผู้เข้าถึง, การบันทึกกิจกรรมหรือประวัติการเข้าใช้งานบันทึกเหตุการณ์ดังกล่าว และกระบวนการทบทวนสิทธิการเข้าใช้งานอย่างเป็นรอบระยะเวลาที่สม่ำเสมอ*<br>*- ตรวจทานประสิทธิภาพการตั้งค่าการปกป้องข้อมูลส่วนบุคคลภายในข้อมูลบันทึกเหตุการณ์ โดยครอบคลุมการเข้ารหัสบันทึกข้อมูลทั้งขณะจัดเก็บ (At-rest) และระหว่างส่งผ่านเครือข่าย (In-transit) รวมถึงการใช้มาตรการทางเทคนิคอื่น ๆ เช่น การปิดบังข้อมูล* | ระดับสูง | 5.2.6.5 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | <u>*ตัวอย่างหลักฐาน*</u><br>*- ภาพสกรีนช็อตรูปภาพแสดงการกำหนดสิทธิ และรายชื่อบัญชีผู้ใช้ที่ได้รับสิทธิการเข้าใช้งานหรือเรียกดูบันทึกเหตุการณ์ (เช่น การตั้งค่าบน IAM Policies หรือ Log Storage Destination Policies) ตามหลักสิทธิเท่าที่จำเป็น*<br>*- รายงานหรือบันทึกประวัติผลการตรวจสอบทบทวนสิทธิเข้าถึง Log (Access Privilege Review Report) ย้อนหลังตามรอบเวลา*<br>*- ภาพหน้าจอแสดงการตั้งค่าสถาปัตยกรรมเข้ารหัสข้อมูล Log ขณะจัดเก็บ (เช่น AWS KMS / Azure Key Vault บนที่เก็บ Log) และโปรโตคอลความปลอดภัย (เช่น HTTPS/TLS) ระหว่างการส่ง Log ไปยังเซิร์ฟเวอร์ส่วนกลาง* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *อ่อนไหว (Data Masking) หรือการแปลงข้อมูลเป็นแฝงตัวตน (Pseudonymization) ในกรณีที่ไม่มีความจำเป็นต้องชี้เฉพาะถึงตัวบุคคลในบางบริบท ตลอดจนตรวจสอบเกณฑ์การตั้งค่าระยะเวลาจัดเก็บรักษาข้อมูล Log เท่าที่จำเป็นสอดคล้องตามหลักการ* | | | | *- ภาพแสดงตัวอย่างผลลัพธ์ข้อมูล Log ที่ผ่านการทำ Data Masking หรือ Pseudonymization บนระบบจัดการข้อมูลหรือเครื่องมือสืบค้น Log* |
| 26 | หน่วยงานได้กำหนดระยะเวลาเก็บรักษาบันทึกเหตุการณ์ (Log Retention) ไว้ในเอกสารอย่างชัดเจน และมีขั้นตอนการลบ Log ที่หมดอายุ (โดยแนะนำให้ตั้งค่าระบบให้ลบอัตโนมัติ เช่น S3 Lifecycle หรือ CloudWatch Retention) เพื่อให้มั่นใจว่าข้อมูล Log จะถูกทำลายอย่างปลอดภัยตามรอบระยะเวลาที่นโยบายและกฎหมายกำหนด ใช่หรือไม่?<br><u>*แนวทางการประเมิน/ตรวจสอบ*</u><br>*- การจัดทำนโยบายและระยะเวลาจัดเก็บ (Log Retention Policy) ต้องจัดทำเอกสารอย่างเป็นทางการที่ระบุกรอบระยะเวลาเก็บรักษาบันทึกเหตุการณ์แต่ละประเภทอย่างเหมาะสม โดยระยะเวลาดังกล่าวต้องมีความสอดคล้องกับข้อกำหนดทางกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด เช่น พ.ร.บ. คอมพิวเตอร์ฯ และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล*<br>*- การบังคับใช้งานระบบอัตโนมัติในการลบข้อมูล (Automated Purging) ควรเปิดใช้งานเทคโนโลยีหรือคุณลักษณะที่ผู้ให้บริการคลาวด์มีให้ เพื่อสั่งทำลายข้อมูล Log โดยอัตโนมัติทันทีที่ครบกำหนดระยะเวลาเก็บรักษา (เช่น S3 Lifecycle Policy บน AWS, CloudWatch Logs Retention หรือ Azure Log Analytics Retention Rules) เพื่อป้องกันข้อผิดพลาดที่เกิดจากการลบโดยมนุษย์*<br>*- ในกรณีที่ไม่สามารถเลือกใช้งานระบบลบแบบอัตโนมัติได้ หน่วยงานจะต้องเตรียมเอกสารคู่มือขั้นตอนปฏิบัติงาน ในการเข้าลบบันทึกเหตุการณ์อย่างปลอดภัย โดยระบุวิธีการลบ ผู้มีอำนาจรับผิดชอบ ความถี่ในการตรวจสอบ และระบบควบคุมเพื่อบันทึกประวัติการตรวจสอบผลการลบจริงอย่างเป็นรูปธรรม* | ระดับสูง | 5.2.6.5 (ข) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | <u>*ตัวอย่างหลักฐาน*</u><br>*- เอกสารกำหนดระยะเวลาเก็บรักษาบันทึกเหตุการณ์ (Log Retention Policy)*<br>*- ภาพหน้าจอการตั้งค่าอัตโนมัติจริง (เช่น CloudWatch Logs Retention, S3 Lifecycle Policy หรือ Log Analytics Rules)*<br>*- คู่มือขั้นตอนปฏิบัติการลบบันทึกเหตุการณ์ (Log Purge Procedure)*<br>*- รายงานหรือบันทึกตรวจสอบการยืนยันผลการลบข้อมูล (Disposal Logs)* |
| 27 | หากหน่วยงานมีการมอบหมายสิทธิดูแลระบบหรือสิทธิพิเศษ (Privileged/Admin Access) บนคลาวด์ ได้เปิดใช้งานการบันทึกประวัติ (Log) ของการใช้งานสิทธินั้น พร้อมทั้งประเมินความเพียงพอของระบบ Log ของผู้ให้บริการคลาวด์และมีการติดตั้งระบบบันทึก Log เพิ่มเติม (เช่น ระบบ SIEM หรือ Log ส่วนกลาง) ในกรณีที่ระบบพื้นฐานของคลาวด์ไม่เพียงพอสำหรับการตรวจสอบความปลอดภัย ใช่หรือไม่?<br><u>*แนวทางการประเมิน/ตรวจสอบ*</u><br>*- ตรวจสอบความพร้อมและยืนยันว่าระบบคลาวด์ได้รับการเปิดใช้งานฟังก์ชันบันทึกกิจกรรมสำหรับบัญชีที่มีสิทธิพิเศษ (Privileged / Administrator Accounts) ทุกรายการ* | ระดับสูง | 5.2.6.6 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | <u>*ตัวอย่างหลักฐาน*</u><br>*- เอกสารระบุข้อกำหนดหรือมาตรฐานในการเก็บบันทึกเหตุการณ์สำหรับผู้ใช้สิทธิพิเศษ (Privileged Logging Requirements)*<br>*- ตัวอย่างไฟล์ข้อมูล Log ของกิจกรรมแอดมินหรือผู้ดูแลระบบจริง (Sample Privileged Activity Log Records)*<br>*- เอกสารรายงานเปรียบเทียบความต้องการด้าน Logging กับขีดความสามารถที่ผู้ให้บริการคลาวด์มอบให้ (Logging Gap Analysis Report)* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *จริง โดยเนื้อหาข้อมูล Log ควรครอบคลุมธุรกรรมและพฤติกรรมที่มีความอ่อนไหวสูงอย่างรอบด้าน ได้แก่*<br>*- การลงชื่อเข้าใช้งานระบบคลาวด์ด้วยบัญชีสิทธิพิเศษ (Privileged Log-on)*<br>*- การเปลี่ยนแปลงหรือแก้ไขค่าการตั้งค่าโครงสร้างระบบ (System Configuration Changes)*<br>*- การจัดการบัญชีผู้ใช้งานระบบ เช่น การสร้าง แก้ไข หรือลบบัญชี (User Account Management Actions)*<br>*- การปรับแต่ง เปลี่ยนแปลง หรือเพิ่มขอบข่ายระดับสิทธิการเข้าถึงข้อมูลและทรัพยากร (Privilege and Permission Alterations)*<br>*- กิจกรรมการเข้าถึง เรียกดู หรือเคลื่อนย้ายชุดข้อมูลที่มีความอ่อนไหวสูง (Sensitive Data Access)*<br>*- การดำเนินการหรือสั่งรันคำสั่งใด ๆ ที่ส่งผลกระทบต่อเสถียรภาพและความพร้อมใช้งานของระบบ (Service Availability Impacting Actions)*<br>*- สอบทานว่าพารามิเตอร์ข้อมูลในไฟล์ Log มีความละเอียดครบถ้วนเพียงพอสำหรับการสืบสวนย้อนกลับเชิงลึก (Security Traceability) โดยข้อมูล Log แต่ละรายการต้องระบุคุณลักษณะสำคัญได้แก่*<br>*- ผู้ดำเนินกิจกรรมหรือบัญชีที่สั่งรันคำสั่ง (Actor / User Identity)*<br>*- วันและเวลาที่บันทึกเกิดเหตุการณ์ที่เที่ยงตรงระดับสากล (Timestamp)*<br>*- รายละเอียดของกิจกรรมที่กำลังประมวลผล (Action / API Call)*<br>*- ทรัพยากรระบบหรือไอดีทรัพยากรที่เกี่ยวข้องกับการรันงาน (Target Resources)*<br>*- ผลลัพธ์สุดท้ายของการทำงาน (Execution Status: Success or Failure)*<br>*- ตรวจสอบบันทึกผลการตรวจสอบของหน่วยงาน ในการนำคุณสมบัติความสามารถการเก็บบันทึก Log พื้นฐานที่ผู้ให้บริการคลาวด์มอบให้ มาวิเคราะห์ประเมินเปรียบเทียบกับเกณฑ์ความต้องการความมั่นคงปลอดภัยของหน่วยงาน เพื่อชี้บ่งจุดเสี่ยงหรือช่องว่าง และประกอบการตัดสินใจว่าจำเป็นต้องเปิดใช้งานคุณสมบัติวิเคราะห์ข้อมูล Log เสริมหรือไม่*<br>*- หากผลการประเมินช่องว่างระบุว่าข้อมูล Log เดิมไม่เพียงพอหรือมีจุดอ่อน ตรวจสอบว่าหน่วยงานได้มีมาตรการบูรณาการหรือตั้งค่าระบบเพิ่มเติมจริง เช่น การเปิดส่งออก Log ไปจัดเก็บแบบศูนย์รวมความปลอดภัยภายนอก (Centralized Storage), การเชื่อมต่อไปยังระบบ SIEM (Security Information and Event Management) หรือการประยุกต์ใช้เครื่องมือของบุคคลที่สามเพื่อวิเคราะห์และเชื่อมโยงพฤติกรรมสิทธิสูง* | | | | *- เอกสารแนวทางปฏิบัติด้านการเฝ้าระวังประวัติการเข้าใช้งานคลาวด์*<br>*- ภาพสกรีนช็อตรูปภาพแสดงการตั้งค่าส่งต่อไฟล์ข้อมูล Log ไประบบกลาง (เช่น S3 Bucket Export Rules, Log Analytics Workspace หรือ SIEM connectors)* |
| 28 | หน่วยงานได้ร้องขอและได้รับข้อมูลการตั้งค่าเวลา (Clock Synchronization) ของระบบผู้ให้บริการคลาวด์ เพื่อให้การบันทึกเวลาของระบบงานและบันทึกเหตุการณ์ (Logs) มีความถูกต้องแม่นยำตรงกัน ใช่หรือไม่? | ระดับสูง | 5.2.6.7 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารชี้แจงมาตรฐานข้อมูลเกี่ยวกับการซิงโครไนซ์นาฬิกาที่ได้รับจากผู้* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานได้รับข้อมูลที่เป็นลายลักษณ์อักษรหรือเอกสารยืนยันเกี่ยวกับการปรับเทียบเวลา (Clock Synchronization) จากผู้ให้บริการคลาวด์*<br>*- ตรวจสอบข้อมูลที่ได้รับว่าครอบคลุมรายละเอียดทางเทคนิคที่จำเป็นครบถ้วนทุกประเด็นหลัก อาทิ*<br>*- แหล่งเวลาอ้างอิง (Reference Time Source): เช่น การระบุการใช้ระบบ GPS, นาฬิกาอะตอม (Atomic Clock) หรือการอ้างอิงระบบ Stratum-1 NTP Server เพื่อเป็นมาตรฐานเวลาหลักที่มีความมั่นคงน่าเชื่อถือสูง*<br>*- โปรโตคอลที่ใช้ในการซิงโครไนซ์ (Synchronization Protocol): เช่น โปรโตคอล NTP (Network Time Protocol) หรือ PTP (Precision Time Protocol) ที่ใช้ปรับปรุงความเหลื่อมล้ำของเวลาบนเครือข่ายคลาวด์*<br>*- โซนเวลาเริ่มต้นของระบบ (Default Time Zone): เช่น การระบุโซนเวลาอ้างอิงเป็นมาตรฐานสากล UTC หรือ GMT+0 เพื่อใช้เป็นเกณฑ์ในการเทียบเคียงเวลาระหว่าง Logs หลายแหล่ง*<br>*- ระดับความแม่นยำของการซิงโครไนซ์ (Accuracy): เช่น การระบุระดับความคลาดเคลื่อนของเวลาที่ยอมรับได้ในระบบ ซึ่งตามมาตรฐานควรวัดในระดับมิลลิวินาที (Milliseconds) หรือไมโครวินาที (Microseconds)*<br>*- ตรวจทานเงื่อนไขเพิ่มเติมที่ผู้ให้บริการคลาวด์ให้มาเกี่ยวกับวิธีการหรือคำแนะนำที่หน่วยงานสามารถนำไปใช้ตั้งค่าเพื่อซิงโครไนซ์ระบบงานภายในของหน่วยงาน (On-Premise) หรือระบบย่อยบนคลาวด์ให้ตรงกับเวลากลางของผู้ให้บริการ เพื่อป้องกันปัญหาเวลาบันทึก Logs คลาดเคลื่อนข้ามระบบ* | | | ☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *ให้บริการคลาวด์ (Clock Synchronization Specification)*<br>*- การตั้งค่าทางเทคนิคจริงบนคลาวด์ (NTP/Time Sync Configuration) เช่น ภาพสกรีนช็อตรูปภาพแสดงนโยบายปรับเทียบเวลาระบบไอที หรือการตั้งค่า NTP Daemon/Client บนเครื่องแม่ข่ายเสมือน (Virtual Machines) เพื่อเชื่อมต่อไปยัง Time Provider ของระบบคลาวด์*<br>*- ตัวอย่างบันทึกประวัติพฤติกรรมจริง (Sample Event Logs with Timestamps) ที่ใช้ตรวจสอบประทับเวลาว่ามีระดับความละเอียดและความสอดคล้องกันข้ามระบบบริการคลาวด์ต่าง ๆ* |
| 29 | หน่วยงานได้ร้องขอและได้รับข้อมูลการจัดการช่องโหว่จากผู้ให้บริการคลาวด์ เพื่อระบุขอบเขตความรับผิดชอบของตนเองอย่างชัดเจน และจัดทำกระบวนการจัดการช่องโหว่ทางเทคนิคเป็นลายลักษณ์อักษร ครอบคลุมการตรวจหา ประเมินความรุนแรง และแก้ไขปรับปรุงตามกรอบเวลา สำหรับทรัพยากรทั้งหมดที่หน่วยงานดูแล (เช่น OS, Application, Container, Source Code และ Third-party Libraries) ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานได้รับและจัดเก็บเอกสารอย่างเป็นทางการจากผู้ให้บริการคลาวด์ ซึ่งต้องครอบคลุมประเด็นสำคัญ ได้แก่ นโยบายการจัดการช่องโหว่ของผู้ให้บริการ, ขอบเขตและหน้าที่ความรับผิดชอบที่แบ่งแยกกันอย่างชัดเจน, รายการช่องโหว่ที่อาจส่งผลกระทบ* | ระดับสูง | 5.2.6.8 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารข้อมูลหรือแนวทางการจัดการช่องโหว่ทางเทคนิคที่ได้รับจากผู้ให้บริการคลาวด์ (CSP Vulnerability Management & Shared Responsibility Guide)*<br>*- เอกสารขั้นตอนปฏิบัติการจัดการช่องโหว่ทางเทคนิคของหน่วยงาน (Technical Vulnerability Management)*<br>*- รายงานผลการตรวจหาช่องโหว่บนระบบคลาวด์ (Vulnerability Assessment / Scan Reports) แยกตามรายระบบงาน* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *ต่อระบบคลาวด์ที่ใช้งาน และแนวปฏิบัติหรือสิ่งที่หน่วยงานต้องดำเนินงานในฐานะผู้ใช้บริการ*<br>*- สอบทานคู่มือหรือแนวทางปฏิบัติที่เป็นลายลักษณ์อักษรของหน่วยงาน (Vulnerability Management Policy/Procedure) สำหรับส่วนงานหรือระบบที่หน่วยงานเป็นผู้รับผิดชอบ โดยกระบวนการดังกล่าวต้องเป็นระบบและสอดคล้องกับแนวทางปฏิบัติสากลครอบคลุมตั้งแต่*<br>*- การค้นหาและระบุช่องโหว่ (Vulnerability Identification) เช่น การทำ Vulnerability Assessment หรือการสแกนระบบ*<br>*- การประเมินความรุนแรงและผลกระทบ (Risk Assessment) เพื่อจัดลำดับความสำคัญในการแก้ไข*<br>*- การดำเนินการแก้ไขหรือบรรเทาความเสียหาย (Remediation/Mitigation) เช่น การติดตั้งแพตช์ความมั่นคงปลอดภัย (Patching) การปรับเปลี่ยนค่ากำหนดความปลอดภัย (Hardening/Configuration) หรือการกำหนดมาตรการควบคุมชดเชยกรณีไม่สามารถแพตช์ได้*<br>*- การกำหนดกรอบเวลาการดำเนินงาน (Remediation Timeline) ที่เหมาะสมกับระดับความรุนแรงของช่องโหว่*<br>*- พิจารณาว่ากระบวนการจัดการช่องโหว่ได้รับการนำไปปฏิบัติและบังคับใช้อย่างครอบคลุมทรัพยากรบนคลาวด์ที่อยู่ภายใต้ความรับผิดชอบของหน่วยงานจริง ได้แก่ ระบบปฏิบัติการ (Operating System), แอปพลิเคชัน (Application), คอนเทนเนอร์ (Container), ซอร์สโค้ด (Source Code) ตลอดจนซอฟต์แวร์ย่อยหรือไลบรารีของบุคคลที่สาม (Third-party Libraries)* | | | | *- บันทึกการวิเคราะห์และหลักฐานการดำเนินการแก้ไขช่องโหว่ (Remediation Logs & Patching Evidence) เช่น บันทึกการติดตั้งแพตช์ความมั่นคงปลอดภัย หรือประวัติการตั้งค่าระบบเพื่อปิดช่องโหว่* |
| 30 | ในกรณีที่หลีกเลี่ยงไม่ได้และจำเป็นต้องใช้ข้อมูลส่วนบุคคลในการทดสอบระบบ หน่วยงานมีนโยบายควบคุมและประเมินความเสี่ยงอย่างเป็นระบบ พร้อมทั้งบังคับใช้มาตรการทางเทคนิค (เช่น การทำ Data Masking/ Pseudonymization การเข้ารหัส บันทึกการเข้าถึง และลบทำลายข้อมูลเมื่อเสร็จสิ้น) ร่วมกับมาตรการบริหารจัดการ (เช่น ต้องขออนุมัติก่อนใช้ กำหนดระยะเวลาใช้งาน และทบทวนความจำเป็นสม่ำเสมอ) เพื่อลดความเสี่ยงให้อยู่ในระดับต่ำที่สุดที่จะเป็นไปได้ ใช่หรือไม่?<br><u>แนวทางการประเมิน/ตรวจสอบ</u><br>*- ตรวจสอบว่าหน่วยงานมีเอกสารนโยบายหรือข้อกำหนดที่เป็นลายลักษณ์อักษรเกี่ยวกับการใช้ข้อมูลส่วนบุคคลเพื่อการทดสอบ โดยนโยบายต้องระบุหลักการชัดเจนว่า “หลีกเลี่ยง* | ระดับสูง | 5.2.6.9 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | <u>ตัวอย่างหลักฐาน</u><br>*- เอกสารข้อกำหนดหรือคู่มือหลักการปฏิบัติเกี่ยวกับการใช้ข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ในการทดสอบ*<br>*- หลักฐานการประเมินความเสี่ยงจากการใช้ข้อมูลส่วนบุคคลในการทดสอบ*<br>*- หลักฐานการใช้มาตรการทางเทคนิคเพื่อลดความเสี่ยง เช่น ภาพสกรีนช็อตการตั้งค่าปิดบังข้อมูล (Data Masking) หรือผลลัพธ์การสแกนการแปลงข้อมูลแฝงตัวตน (Pseudonymization Result) ในฐานข้อมูลทดสอบ และหลักฐานการทำลายข้อมูล*<br>*- หลักฐานการใช้มาตรการด้านการจัดการหน่วยงานเพื่อลดความเสี่ยง เช่น* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *การใช้ข้อมูลส่วนบุคคลจริงในการทดสอบ" และกำหนดเงื่อนไขที่เข้มงวดให้ใช้งานได้เฉพาะกรณีที่จำเป็นอย่างยิ่งและไม่สามารถหลีกเลี่ยงได้เท่านั้น*<br>*- ตรวจสอบบันทึกหลักฐานการประเมินความเสี่ยงเมื่อมีการนำข้อมูลส่วนบุคคลจริงไปใช้ในการทดสอบระบบงานคลาวด์ โดยควรครอบคลุมมิติความเสี่ยงสำคัญ ได้แก่*<br>*- ความเสี่ยงจากการเข้าถึงข้อมูลโดยบุคลากรที่ไม่มีสิทธิเกี่ยวข้อง (เช่น นักพัฒนาซอฟต์แวร์ หรือผู้ทดสอบระบบภายนอก)*<br>*- ความเสี่ยงต่อการรั่วไหลของข้อมูลส่วนบุคคลจริงออกจากสภาพแวดล้อมทดสอบ (Testing Environment)*<br>*- ความเสี่ยงจากกรณีข้อมูลตกค้างหลงเหลืออยู่ในระบบภายหลังการทดสอบเสร็จสิ้น*<br>*- พิจารณาการตั้งค่าเทคโนโลยีความปลอดภัยจริงบนคลาวด์เพื่อลดความเสี่ยง ซึ่งต้องครอบคลุมกลไกการแปลงข้อมูลแฝงตัวตน (Pseudonymization) หรือการปิดบังข้อมูล (Data Masking), การเข้ารหัสข้อมูล (Encryption), การเปิดระบบเก็บบันทึกประวัติการเข้าถึงข้อมูล (Access Logging) ตลอดจนกระบวนการทำลายข้อมูลอย่างรวดเร็วและปลอดภัยเมื่อใช้งานทดสอบเสร็จสิ้น*<br>*- สอบทานขั้นตอนการควบคุมการปฏิบัติงาน เช่น การกำหนดให้มีกระบวนการขออนุมัติอย่างเป็นทางการจากผู้มีอำนาจก่อนนำข้อมูลจริงไปใช้, การจำกัดช่วงเวลาและสิทธิการเข้าถึงข้อมูลชั่วคราว และการกำหนดรอบทบทวนความจำเป็นของการใช้ข้อมูลส่วนบุคคลอย่างสม่ำเสมอ* | | | | *เอกสารแบบฟอร์มการขออนุมัติใช้ข้อมูลจริง บันทึกกำหนดระยะเวลาการเข้าถึง และรายงานการประเมินความพึงพอใจและการทบทวนความสอดคล้อง* |
| **การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security)** | | | | | |
| 31 | หากหน่วยงานมีการโอนย้ายข้อมูลส่วนบุคคลด้วยสื่อทางกายภาพ (เช่น USB, Hard disk, เทปสำรองข้อมูล หรือ DVD) หน่วยงานได้จัดให้มีระบบหรือทะเบียนบันทึกการเข้า-ออกของสื่อเหล่านั้น โดยระบุประเภทสื่อ, ผู้ส่งและผู้รับที่ได้รับอนุญาต, วันเวลา และจำนวนอย่างครบถ้วนและปลอดภัย ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานจัดให้มีระบบลงทะเบียน ทะเบียน สมุดบันทึก หรือระบบอิเล็กทรอนิกส์สำหรับบันทึกการใช้งานสื่อทางกายภาพที่ใช้ถ่ายโอนข้อมูลซึ่งมีข้อมูลส่วนบุคคลอย่างชัดเจนและเป็นระบบ โดยระบบนี้ต้องครอบคลุมการบันทึกสื่อทางกายภาพทุกรายการทั้งขาเข้า (เข้ามาภายในหน่วยงาน) และขาออก (ส่งออกไปภายนอก)*<br>*- ทำการสุ่มตัวอย่างบันทึกหรือประวัติการถ่ายโอนข้อมูลบนสื่อทางกายภาพ เพื่อตรวจสอบความครบถ้วนและถูกต้องของข้อมูลตามที่มาตรฐานระบุ*<br>*- ประเภทของสื่อทางกายภาพ (เช่น Hard disk, USB, เทปสำรองข้อมูล, DVD)*<br>*- ผู้ส่งและผู้รับที่ได้รับอนุญาตให้เข้าถึงและจัดการข้อมูลอย่างถูกต้องตามสิทธิ* | ระดับกลาง ระดับสูง | 5.2.7.1 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารขั้นตอนปฏิบัติสำหรับบริการหรือระบบการถ่ายโอนข้อมูลผ่านสื่อทางกายภาพ (Physical Information Transfer Procedure)*<br>*- ทะเบียนหรือสมุดบันทึกรายละเอียดสื่อทางกายภาพที่ใช้ถ่ายโอนข้อมูลส่วนบุคคล (Physical Media Log / Registry) ทั้งรูปแบบเล่มบันทึกหรือไฟล์ดิจิทัล*<br>*- ตัวอย่างบันทึกรายการเข้าออกของสื่อจริง (Sample Transfer Records) หรือภาพสกรีนช็อตรูปภาพแสดงผลจากหน้าจอระบบลงทะเบียนควบคุมสื่อทางกายภาพย้อนหลัง* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *- วันที่และเวลาที่มีการรับส่งหรือดำเนินกิจกรรม*<br>*- จำนวนชิ้นสื่อทางกายภาพทั้งหมดที่มีการโอนย้ายในแต่ละรอบ*<br>*- สอบทานขั้นตอนการควบคุมเชิงรุกว่ามีกระบวนการจำกัด ตรวจสอบ หรือคัดกรองที่มีประสิทธิภาพ เพื่อให้มั่นใจได้จริงว่าไม่มีการนำสื่อบันทึกข้อมูลส่วนบุคคลออกนอกหน่วยงานหรือนำเข้ามาประมวลผลโดยไม่ได้บันทึกรายละเอียดลงทะเบียนเข้าระบบตามที่กำหนด* | | | | |
| 32 | หน่วยงานได้ร้องขอให้ผู้ให้บริการคลาวด์ใช้มาตรการเพิ่มเติม (เช่น การเข้ารหัสข้อมูล) เพื่อให้มั่นใจว่าข้อมูลจะถูกเข้าถึงได้เฉพาะที่จุดปลายทางเท่านั้น และไม่สามารถถูกดักรับหรือเข้าถึงระหว่างการรับส่ง (Data in Transit) ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจประเมินว่าหน่วยงานมีพยานหลักฐานที่ยืนยันการยื่นคำร้องขอ ความประสงค์ หรือการระบุข้อตกลงร่วมกับผู้ให้บริการคลาวด์ เพื่อให้ผู้ให้บริการจัดเตรียมหรือใช้มาตรการปกป้องข้อมูลระหว่างการถ่ายโอนอย่างเข้มงวด โดยการพิจารณาข้อสัญญา เอกสารจดหมายประสานงาน หรืออีเมลสื่อสารอย่างเป็นทางการ*<br>*- ตรวจทานประสิทธิภาพการตั้งค่าการรับส่งข้อมูลผ่านเครือข่าย เพื่อยืนยันว่าข้อมูลไม่ถูกเปิดเผยหรือถูกเข้าถึงโดยผู้ไม่มีสิทธิในระหว่างทาง (In-Transit) และจำกัดสิทธิการเข้าถึงให้เกิดขึ้นเฉพาะที่จุดปลายทาง (Destination Endpoint) เท่านั้น ซึ่งพิจารณาจากเกณฑ์ทางเทคนิคดังนี้*<br>*- Encryption in Transit: ตรวจสอบการเปิดใช้งานโปรโตคอลการเข้ารหัสการสื่อสารที่ปลอดภัยและเป็นที่ยอมรับระดับสากล เช่น TLS 1.2 หรือ TLS 1.3 เป็นขั้นต่ำ*<br>*- Secure Connection: ตรวจสอบการโอนย้ายข้อมูลผ่านช่องทางเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) หรือบริการเชื่อมต่อตรงเฉพาะหน่วยงาน (Private/Dedicated Link).*<br>*- Client-side Encryption: ในกรณีของข้อมูลที่มีความอ่อนไหวสูงมาก ทบทวนการใช้สถาปัตยกรรมเข้ารหัสข้อมูลตั้งแต่ฝั่งหน่วยงานซึ่งเป็นผู้ใช้บริการ (Client-side) เพื่อรับประกันว่าข้อมูลจะถูกส่งในรูปแบบที่มีการเข้ารหัสอย่างรัดกุมตลอดกระบวนการเดินทางโดยที่ผู้ให้บริการคลาวด์ไม่สามารถสืบค้นเนื้อหาหรือกุญแจเข้ารหัสลับได้* | ระดับกลาง ระดับสูง | 5.2.7.1 (ข) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารสัญญาบริการคลาวด์ (Cloud Service Agreement) หรือข้อตกลงระดับบริการ (SLA) ส่วนที่ระบุหน้าที่การรับส่งข้อมูลอย่างปลอดภัย*<br>*- หลักฐานบันทึกการส่งคำขอทางเทคนิค หรือจดหมาย/อีเมลติดต่อยืนความประสงค์กับผู้ให้บริการ*<br>*- ภาพสกรีนช็อตรูปภาพแสดงผลการตั้งค่าโปรโตคอลความปลอดภัยจริงบนเครื่องแม่ข่ายหรือระบบบริการคลาวด์ (เช่น Web Server/API Gateway TLS Settings)*<br>*- รายงานผลการสแกนความมั่นคงปลอดภัยบนเครือข่าย (Network Vulnerability Report)*<br>*- เอกสารแผนภาพแสดงสถาปัตยกรรมการไหลของข้อมูล (Data Flow & Network Diagram)*<br>*- หลักฐานแสดงการเปิดและตั้งค่าการทำงานของระบบ Client-side Encryption Tool หรือการเชื่อมโยงระบบเครือข่าย VPN* |
| 33 | ในสภาพแวดล้อมคลาวด์ที่มีการใช้งานร่วมกัน (Shared Environment) หน่วยงานได้จัดทำข้อกำหนดการแยกเครือข่าย (Network Segregation) เพื่อป้องกันการเชื่อมต่อหรือเข้าถึงข้อมูลข้ามกันระหว่างผู้เช่ารายอื่น (Tenant Isolation) ไว้เป็นลายลักษณ์อักษร และได้ตรวจเช็กกับสถาปัตยกรรมเครือข่ายของผู้ให้บริการคลาวด์เพื่อยืนยันว่ามีมาตรการป้องกันที่ได้มาตรฐานและปลอดภัยจริง ใช่หรือไม่? | ระดับกลาง ระดับสูง | 5.2.7.2 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารข้อกำหนดด้านการแยกเครือข่ายสำหรับบริการคลาวด์ (Virtual Network Segregation Requirements Document) ของหน่วยงาน*<br>*- รายงานสถาปัตยกรรมการแยกเครือข่ายที่ได้รับจากผู้ให้บริการคลาวด์* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีเอกสารข้อกำหนดด้านการแยกเครือข่ายเพื่อแยกผู้เช่าในสภาพแวดล้อมคลาวด์ที่ใช้ร่วมกันอย่างเป็นทางการ โดยเนื้อหาทางเทคนิคต้องระบุอย่างชัดเจนในเรื่อง*<br>*- ระดับการแยกแยะเครือข่าย: กำหนดรูปแบบการแยกแยะอย่างเหมาะสม เช่น การแยกทางตรรกะ (Logical Isolation) หรือการแยกทางกายภาพ (Physical Isolation)*<br>*- มาตรการป้องกันการสื่อสารข้ามผู้เช่า: มาตรการและกลไกป้องกันการรั่วไหลหรือการสื่อสารข้อมูลข้ามกลุ่มผู้เช่า (Cross-tenant Communication Protection)*<br>*- มาตรฐานการแบ่งส่วนเครือข่ายเสมือน: มีเกณฑ์มาตรฐานในการแบ่งส่วนระบบเครือข่ายเสมือน (Virtual Network Segmentation Standards) เช่น การจัดทำ Virtual Private Cloud (VPC), Subnets, หรือการตั้งค่า Security Groups*<br>*- ตรวจสอบบันทึกผลการเปรียบเทียบระหว่างข้อกำหนดความปลอดภัยของเครือข่ายที่หน่วยงานต้องการ กับขีดความสามารถการแยกแยะและระบบป้องกันจริงที่ผู้ให้บริการคลาวด์จัดหาให้ เพื่อรับประกันความปลอดภัยของสภาพแวดล้อมระบบงาน* | | | | *(CSP Network Isolation & Tenant Segregation Report / Whitepaper)*<br>*- รายงานการเปรียบเทียบข้อกำหนดของหน่วยงานกับคุณสมบัติจริงของผู้ให้บริการคลาวด์ (Network Segregation Gap Analysis & Comparison Report)* |
| **การจัดหา การพัฒนา และการบำรุงรักษา (System Acquisition, Development, and Maintenance)** | | | | | |
| 34 | หน่วยงานได้กำหนดความต้องการด้านความปลอดภัยข้อมูลสำหรับการใช้บริการคลาวด์ไว้เป็นลายลักษณ์อักษร และมีกระบวนการประเมินอย่างเป็นระบบเพื่อเปรียบเทียบว่า บริการของผู้ให้บริการคลาวด์สามารถตอบสนองเกณฑ์ความปลอดภัยของหน่วยงานได้อย่างครบถ้วนและเหมาะสม ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีเอกสารข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ที่เป็นทางการ โดยเอกสารข้อกำหนดดังกล่าวต้องครอบคลุมประเด็นควบคุมสำคัญและมีความสอดคล้องตามประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567*<br>*- พิจารณาว่าหน่วยงานมีขั้นตอนปฏิบัติที่เป็นระบบในการประเมินและทบทวนความสามารถของผู้ให้บริการคลาวด์ โดยนำข้อกำหนดความมั่นคงปลอดภัยที่หน่วยงานระบุไว้ ไปเปรียบเทียบกับขีดความสามารถการรักษาความปลอดภัยจริงที่ผู้ให้บริการจัดหาให้ เพื่อชี้บ่งและรับรองว่าผู้ให้บริการคลาวด์สามารถตอบสนองความต้องการของหน่วยงานได้อย่างครบถ้วน* | ทุกระดับ | 5.2.8.1 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับการใช้บริการคลาวด์ของหน่วยงาน*<br>*- บันทึกหรือรายงานผลการประเมินขีดความสามารถและความปลอดภัยของผู้ให้บริการคลาวด์ (CSP Security Capability Assessment / Gap Analysis Report)* |
| 35 | หน่วยงานได้ร้องขอและได้รับเอกสารข้อมูลความสามารถด้านความปลอดภัย (Information Security Capabilities) จากผู้ให้บริการคลาวด์เพื่อใช้ตรวจสอบและประเมินว่า มาตรการรักษาความปลอดภัยของระบบคลาวด์นั้น | ทุกระดับ | 5.2.8.1 (ข) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารข้อมูลความสามารถด้านความมั่นคงปลอดภัยที่ได้รับจากผู้ให้บริการคลาวด์ (CSP Information Security* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | สอดคล้องตามเกณฑ์และนโยบายความมั่นคงปลอดภัยของหน่วยงานจริง ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบความพร้อมและความมีอยู่ของพยานหลักฐานเอกสารระบุคุณสมบัติหรือแนวทางการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานได้รับจากผู้ให้บริการคลาวด์*<br>*- สอบทานเพื่อยืนยันว่าหน่วยงานได้นำเอกสารหรือข้อมูลขีดความสามารถที่ได้รับจากผู้ให้บริการคลาวด์ ไปใช้เป็นฐานอ้างอิงในการเปรียบเทียบ วิเคราะห์ และประเมินความสอดคล้อง (Gap Analysis) ร่วมกับนโยบายและข้อกำหนดมาตรฐานความปลอดภัยไซเบอร์ภายในหน่วยงานอย่างแท้จริง*<br>*- ทบทวนว่าข้อมูลขีดความสามารถความปลอดภัยที่รวบรวมมานั้น ครอบคลุมชนิดบริการคลาวด์ที่ใช้งานจริง และเป็นข้อมูลที่ผ่านการตรวจสอบโดยผู้ตรวจสอบอิสระภายนอกหรือมีใบรับรองตามมาตรฐานสากลที่ยังไม่หมดอายุการบังคับใช้* | | | ☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *Capabilities) เช่น เอกสารคู่มือคำอธิบายทางเทคนิค (Technical Security Specifications), รายงานเอกสารความรับผิดชอบร่วมด้านความปลอดภัย (Shared Responsibility Matrix), หรือรายงานผลการตรวจสอบความปลอดภัยของคลาวด์จากผู้ตรวจสอบอิสระภายนอก*<br>*- รายงานบันทึกผลการประเมินความสอดคล้อง (Security Capabilities Assessment / Gap Analysis Report) เอกสารการวิเคราะห์เปรียบเทียบความสามารถของผู้ให้บริการคลาวด์ที่ใช้จริงเทียบกับเกณฑ์ความต้องการความปลอดภัยของระบบงาน* |
| 36 | หน่วยงานได้ร้องขอและได้รับข้อมูลเกี่ยวกับขั้นตอนและวิธีปฏิบัติในการพัฒนาซอฟต์แวร์หรือระบบอย่างปลอดภัย (Secure Development Policy and Procedures) จากผู้ให้บริการคลาวด์ เพื่อใช้สอบทานและสร้างความมั่นใจว่าบริการคลาวด์ที่นำมาใช้งานถูกออกแบบและพัฒนาขึ้นอย่างปลอดภัยจากการถูกโจมตี ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานได้รับข้อมูลเกี่ยวกับขั้นตอนและวิธีปฏิบัติในการพัฒนาที่ปลอดภัยของบริการคลาวด์จากผู้ให้บริการคลาวด์จริง*<br>*โดยข้อมูลดังกล่าวอาจเป็นข้อมูลการรับรอง เอกสารการปฏิบัติตามมาตรฐาน หรือรายละเอียดขั้นตอนที่ผู้ให้บริการจัดเตรียมไว้ให้ภายใต้นโยบายการเปิดเผยข้อมูลของตนเอง*<br>*- พิจารณาและตรวจสอบว่าข้อมูลที่ได้รับจากผู้ให้บริการคลาวด์นั้น มีรายละเอียดที่เพียงพอและครอบคลุมกระบวนการสำคัญในการพัฒนาซอฟต์แวร์อย่างปลอดภัย (เช่น วงจรการพัฒนาซอฟต์แวร์อย่างปลอดภัย หรือ Secure Software Development Life Cycle: SSDLC, การทดสอบความมั่นคงปลอดภัยของโค้ด, และการจัดการช่องโหว่ระหว่างพัฒนา) เพื่อใช้ประเมินความมั่นใจในความปลอดภัยของบริการคลาวด์ที่พัฒนาโดยผู้ให้บริการก่อนนำมาใช้งานจริง*<br>*- ทบทวนบันทึกหลักฐานการประเมินของผู้ใช้งาน ว่าได้นำข้อมูลด้าน Secure Development ของผู้ให้บริการมาพิจารณาร่วมกับข้อกำหนดความปลอดภัยของหน่วยงานอย่างเหมาะสมหรือไม่* | ทุกระดับ | 5.2.8.2 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารข้อมูลเกี่ยวกับขั้นตอนและวิธีปฏิบัติในการพัฒนาที่ปลอดภัยที่ได้รับจากผู้ให้บริการคลาวด์ (Secure Development Policy and SSDLC Specification) ซึ่งระบุแนวทางการพัฒนาที่ปลอดภัยของผู้ให้บริการ*<br>*- หลักฐานการร้องขอข้อมูลจากผู้ให้บริการคลาวด์ เช่น อีเมลประสานงานอย่างเป็นทางการ, บันทึกการเจรจาข้อสัญญา หรือพยานหลักฐานการเข้าถึงพอร์ทัลความปลอดภัยของผู้ให้บริการเพื่อเรียกดูรายงาน*<br>*- บันทึกผลการทบทวนและการประเมินความมั่นใจในความปลอดภัยของบริการคลาวด์ (Secure Development Evaluation Report) ที่จัดทำโดยคณะทำงานของหน่วยงานเพื่อรับรองผลการประเมินก่อนนำระบบคลาวด์มาใช้งานจริง* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| **การจัดการผู้ให้บริการภายนอก (Supplier Relationships)** | | | | | |
| 37 | หน่วยงานได้ระบุให้ผู้ให้บริการคลาวด์เป็นผู้ให้บริการภายนอก (Supplier) ประเภทหนึ่งในนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก เพื่อควบคุมการเข้าใช้งานและลดความเสี่ยงจากการที่ผู้ให้บริการคลาวด์เข้าถึงหรือจัดการข้อมูลของหน่วยงาน ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีเอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships) หรือนโยบายที่ดูแลคู่ค้า (Supplier Policy) ที่จัดทำขึ้นเป็นลายลักษณ์อักษรและประกาศใช้งานอย่างเป็นทางการภายในหน่วยงาน*<br>*- ทบทวนว่ารายละเอียดภายในตัวเล่มนโยบายความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอกดังกล่าว มีการระบุคำนิยาม ขอบเขต หรือประเภทให้ครอบคลุมถึง “ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP)” เป็นหนึ่งในผู้ให้บริการภายนอกของหน่วยงานอย่างเป็นระบบ เพื่อรับประกันว่าระบบและบริการคลาวด์ที่ใช้งานจะอยู่ภายใต้การควบคุมความมั่นคงปลอดภัยเช่นกัน*<br>*- ตรวจสอบว่านโยบายมีการกำหนดมาตรการ แนวปฏิบัติ หรือข้อตกลงระดับบริการเพื่อควบคุมและลดความเสี่ยงในจุดที่ข้อมูลของหน่วยงานอาจอยู่ภายใต้สิทธิการเข้าใช้งาน การเรียกดู หรือการจัดการโดยเจ้าหน้าที่หรือระบบของผู้ให้บริการคลาวด์ (เช่น ข้อกำหนดด้านการเข้ารหัสข้อมูล หรือข้อกำหนดสิทธิการเข้าถึงต่ำสุดเท่าที่จำเป็น)* | ทุกระดับ | 5.2.9.1 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships) ส่วนที่ระบุขอบเขตครอบคลุมหรือจัดประเภทผู้ให้บริการคลาวด์เป็นผู้ให้บริการภายนอกอย่างชัดเจน*<br>*- เอกสารบันทึกข้อกำหนดความปลอดภัยของคู่ค้า หรือแบบฟอร์มการประเมินความมั่นคงปลอดภัยในการเลือกใช้ผู้ให้บริการภายนอก (Supplier Security Assessment) ที่มีการประเมินผู้ให้บริการคลาวด์ก่อนเริ่มสัญญา*<br>*- เอกสารสัญญาบริการคลาวด์ (Cloud Service Agreement) หรือข้อตกลงระดับบริการ (SLA) ส่วนที่สะท้อนการนำข้อกำหนดในนโยบายข้างต้นไปบังคับใช้จริงทางสัญญาเพื่อควบคุมขอบเขตสิทธิในการเข้าถึงและจัดการข้อมูล* |
| 38 | หน่วยงานได้ตกลงและระบุการแบ่งบทบาทและความรับผิดชอบด้านความปลอดภัยกับผู้ให้บริการคลาวด์ไว้ในสัญญาหรือข้อตกลงการให้บริการอย่างชัดเจนและมีผลผูกพัน โดยครอบคลุมกระบวนการสำคัญ ได้แก่ การป้องกันมัลแวร์ การสำรองข้อมูล มาตรการควบคุมการเข้ารหัส การจัดการช่องโหว่ การจัดการเหตุการณ์ การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค การทดสอบความปลอดภัย การตรวจสอบ การรวบรวม การบำรุงรักษา และการปกป้องหลักฐาน รวมถึงบันทึกและเส้นทางการตรวจสอบ การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ การยืนยันตัวตนและการควบคุมการเข้าถึง และการจัดการข้อมูลประจำตัวและการเข้าถึง เพื่อป้องกันความสับสนในการปฏิบัติงาน ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>* | ทุกระดับ | 5.2.9.2 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารขอบเขตความรับผิดชอบสำหรับบริการคลาวด์ที่เป็นส่วนหนึ่งของข้อตกลง (Responsibility Matrix for Cloud Services as part of Supplier Agreement)*<br>*- เอกสารสัญญาบริการคลาวด์ (Cloud Service Agreement) ข้อตกลงระดับบริการ (SLA) หรือข้อสัญญาแนบท้ายด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล (Security & Data Processing Addendum: DPA)* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *- ตรวจสอบว่าข้อตกลงการให้บริการคลาวด์ (Cloud Service Agreement) หรือเอกสารแนบท้ายด้านความมั่นคงปลอดภัย (Security Addendum) มีการระบุขอบเขตบทบาทหน้าที่อย่างชัดเจน เป็นลายลักษณ์อักษร และมีผลผูกพันทางกฎหมายระหว่างหน่วยงาน (ผู้ใช้บริการคลาวด์) และผู้ให้บริการคลาวด์*<br>*- พิจารณาข้อตกลงเพื่อยืนยันว่ามีการระบุส่วนงานและขอบเขตความรับผิดชอบของแต่ละฝ่าย (Shared Responsibility Matrix) ในกิจกรรมความปลอดภัยทางเทคนิคและการปฏิบัติงานอย่างครบถ้วน ได้แก่*<br>*- การป้องกันมัลแวร์: ระบุชัดเจนว่าฝ่ายใดรับผิดชอบในการติดตั้งและจัดการระบบป้องกันมัลแวร์ในแต่ละเลเยอร์ของสถาปัตยกรรมระบบคลาวด์ (เช่น ในระดับ Virtual Machine, Containers, หรือระดับ Software/Application)*<br>*- การสำรองข้อมูล: กำหนดฝ่ายรับผิดชอบในการสำรองข้อมูล รวมถึงพิกัดสถานที่จัดเก็บ รอบความถี่ และขั้นตอนปฏิบัติในการทดสอบกู้คืนข้อมูลสำรองเพื่อยืนยันความพร้อมใช้งาน*<br>*- มาตรการควบคุมการเข้ารหัส: กำหนดผู้รับผิดชอบการตั้งค่าเข้ารหัสข้อมูลขณะจัดเก็บ (At-rest) ระหว่างส่งผ่าน (In-transit) ตลอดจนการบริหารจัดการวงจรชีวิตกุญแจเข้ารหัส (Key Management)*<br>*- การจัดการช่องโหว่: ระบุบทบาทในการสแกนหาช่องโหว่ การวิเคราะห์ผล และหน้าที่ในการติดตั้งแพตช์ (Patching) ในแต่ละเลเยอร์ที่อยู่ภายใต้การดูแล*<br>*- การจัดการเหตุการณ์: กำหนดสิทธิและหน้าที่การเฝ้าระวัง การตรวจจับ การตอบสนอง การแจ้งเตือน และการประสานงานร่วมกันเพื่อกู้คืนระบบเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์*<br>*- การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค: ระบุผู้มีหน้าที่รับผิดชอบในการตรวจประเมินระบบเชิงเทคนิคและการรายงานผลการดำเนินงานความปลอดภัย*<br>*- การทดสอบความปลอดภัย: กำหนดข้อตกลงด้านสิทธิ ความถี่ และขั้นตอนในการทำทดสอบเจาะระบบ (Penetration Testing) หรือการสแกนหาจุดอ่อนโดยไม่กระทบต่อผู้เช่ารายอื่น*<br>*- การตรวจสอบ (Audit): ระบุสิทธิของหน่วยงานในการเข้าตรวจประเมินความปลอดภัย ขอบเขตในการเข้าถึงพยานหลักฐาน และรอบความถี่ในการเข้าตรวจสอบระบบของผู้ให้บริการคลาวด์*<br>*- การรวบรวม การบำรุงรักษา และการปกป้องหลักฐาน: กำหนดบทบาทในการจัดเก็บรักษาไฟล์บันทึกเหตุการณ์ (Logs) และเส้นทางการตรวจสอบ (Audit Trail) ให้ปลอดภัยจากการแก้ไข เพื่อใช้เป็นพยานหลักฐานทางกฎหมายและนิติวิรเวชดิจิทัล* | | | | |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *- การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ: ระบุขั้นตอนการส่งคืนข้อมูล การลบ หรือการทำลายไฟล์ข้อมูลของหน่วยงานอย่างปลอดภัยและถาวรหลังจากเลิกใช้บริการคลาวด์*<br>*- การยืนยันตัวตนและการควบคุมการเข้าถึง: ระบุกลไกทางเทคนิคและสิทธิในการควบคุมการเข้าถึงระบบของผู้ให้บริการและหน่วยงาน*<br>*- การจัดการข้อมูลประจำตัวและการเข้าถึง: กำหนดฝ่ายรับผิดชอบในการบริหารจัดการวงจรชีวิตบัญชีผู้ใช้งานระบบ (IAM) และการกำหนดระดับสิทธิใช้งาน* | | | | |
| **การจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management)** | | | | | |
| 39 | หน่วยงานได้ตรวจสอบการแบ่งแยกหน้าที่ความรับผิดชอบในการรับมือและจัดการเหตุภัยคุกคาม (Incident Management) ร่วมกับผู้ให้บริการคลาวด์ และทวนสอบแล้วว่าการแบ่งหน้าที่ดังกล่าวนั้นครอบคลุมและตรงตามเกณฑ์หรือแผนการรับมือภัยไซเบอร์ของหน่วยงานจริง ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่าหน่วยงานมีการจัดทำนโยบาย แผนเผชิญเหตุ หรือคู่มือขั้นตอนการปฏิบัติงานสำหรับการจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Incident Response Policy/Procedure) ที่ระบุขอบเขตการทำงาน เกณฑ์การระบุภัยคุกคาม และขั้นตอนการแก้ไขอย่างชัดเจน*<br>*- ตรวจสอบบันทึกการทบทวนจัดสรรความรับผิดชอบระหว่างหน่วยงาน (ในฐานะผู้ใช้บริการคลาวด์) และผู้ให้บริการคลาวด์ในเรื่องการรับมือและระงับเหตุภัยคุกคามร่วมกัน โดยพิจารณาว่าครอบคลุมกิจกรรมการปฏิบัติงานทางเทคนิคในทุกขั้นอย่างโปร่งใส ไร้รอยต่อรอยรั่ว ได้แก่*<br>*- การตรวจจับภัยคุกคาม (Detection): ระบุช่องทางและกลไกประสานงานเมื่อระบบคลาวด์แจ้งเตือนความผิดปกติ*<br>*- การควบคุมขอบเขตความเสียหาย (Containment): ระบุผู้มีสิทธิสั่งบล็อก พอร์ต รันคำสั่ง หรือปิดเครื่องเสมือนที่ถูกควบคุม*<br>*- การกู้คืนระบบ (Recovery): กำหนดบทบาทในการสำรอง คลีนระบบ และดึงทรัพยากรกลับมาให้พร้อมบริการ*<br>*- ตรวจสอบกระบวนการประเมินว่า กรอบระยะเวลาและขั้นตอนการแจ้งเหตุ (Incident Notification Timeline) ที่ผู้ให้บริการคลาวด์กำหนดไว้นั้น สอดรับกับเป้าหมายแผนงานความมั่นคงปลอดภัยและสอดคล้องกับเงื่อนไขบังคับแจ้งเหตุตามที่ พ.ร.บ. ไซเบอร์ และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ระบุไว้หรือไม่* | ระดับกลาง ระดับสูง | 5.2.10.1 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารข้อกำหนดหรือขั้นตอนปฏิบัติสำหรับการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของหน่วยงาน (Security Incident Management Requirements / Incident Response Procedure)*<br>*- เอกสารตารางแสดงขอบเขตความรับผิดชอบและการประสานงานร่วมกันด้านการจัดการเหตุการณ์คลาวด์ (Shared Incident Response Responsibility Matrix / RACI Matrix for Cloud Incidents)*<br>*- บันทึกผลการประเมินและทบทวนความสอดคล้องของข้อกำหนดผู้ให้บริการคลาวด์ เทียบกับเป้าหมายความเร็วในการแก้ไขระงับเหตุและข้อกำหนดทางกฎหมายของหน่วยงาน (Cloud Service Incident Response Evaluation Report)* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| 40 | เมื่อเกิดเหตุการณ์ผิดปกติหรือภัยคุกคามด้านความมั่นคงปลอดภัย (Information Security Incident) บนระบบคลาวด์ หน่วยงานได้กำหนดให้มีขั้นตอนการทบทวน (ไม่ว่าจะดำเนินงานเอง หรือทำร่วมกับผู้ให้บริการคลาวด์) เพื่อประเมินและตรวจสอบว่าเหตุการณ์นั้นทำให้เกิด <u>การละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach)</u> หรือไม่ ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบว่ากระบวนการจัดการเหตุภัยคุกคามทางสารสนเทศของหน่วยงาน มีขั้นตอนการประเมินและทบทวนเพื่อตรวจสอบหาโอกาสการละเมิดข้อมูลส่วนบุคคลบรรจุไว้ชัดเจน โดยกำหนดให้ทุกเหตุภัยคุกคามทางสารสนเทศที่เกิดขึ้นบนบริการคลาวด์ต้องผ่านกระบวนการนี้เป็นมาตรฐานในการวิเคราะห์ประเมินสถานการณ์ความเสี่ยง*<br>*- ตรวจสอบความพร้อมของแนวทางในการประสานงานร่วมกับผู้ให้บริการคลาวด์ โดยมีเกณฑ์ตัดสินใจชัดเจนว่าเมื่อใดที่ต้องทบทวนร่วมกัน (เช่น เหตุคุกคามที่เกิดจากระบบโครงสร้างพื้นฐานหรือระบบฐานรากของผู้ให้บริการคลาวด์ หรือประเด็นความมั่นคงปลอดภัยเครือข่ายเสมือนการแยกผู้เช่า) พร้อมระบุช่องทางการติดต่อ และขั้นตอนการส่งต่อหรือแลกเปลี่ยนข้อมูล/หลักฐานที่จำเป็นต่อการสืบสวนทบทวนร่วมกัน* | ระดับกลาง ระดับสูง | 5.2.10.1 (ข) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารขั้นตอนปฏิบัติงานมาตรฐานสำหรับการจัดการเหตุภัยคุกคามทางสารสนเทศของหน่วยงาน (Incident Response / Threat Management Procedure / SOP) ที่ระบุขั้นตอนวิเคราะห์ประเด็นข้อมูลส่วนบุคคลอย่างครบถ้วน*<br>*- เอกสารแนวทางการประสานงานและทบทวนความเสี่ยงภัยคุกคามร่วมกับผู้ให้บริการคลาวด์*<br>*- รายละเอียดช่องทางการรายงานเหตุและรูปแบบการขอพยานหลักฐาน (เช่น บันทึก Log หรือ VM Evidence) จากผู้ให้บริการ* |
| 41 | หน่วยงานได้ร้องขอและได้รับข้อมูลเกี่ยวกับช่องทางและขั้นตอนในการแจ้งเหตุ (Report) และติดตามสถานะเหตุการณ์ผิดปกติ (Incident Tracking) จากผู้ให้บริการคลาวด์ ทั้งในกรณีที่องค์กรตรวจพบและต้องการแจ้งไปยังผู้ให้บริการคลาวด์ กรณีที่ผู้ให้บริการคลาวด์ตรวจพบและต้องแจ้งเตือนมายังหน่วยงาน และช่องทางสำหรับติดตามความคืบหน้าของเหตุการณ์ที่ได้แจ้งไป ใช่หรือไม่?<br>*<u>แนวทางการประเมิน/ตรวจสอบ</u>*<br>*- ตรวจสอบความพร้อมและความมีอยู่จริงของข้อมูลช่องทางสำหรับการแจ้งเหตุภัยคุกคามความปลอดภัยที่หน่วยงานตรวจพบไปยังผู้ให้บริการคลาวด์ (เช่น พอร์ทัลระบบบริการ, อีเมลฉุกเฉินเฉพาะด้าน หรือหมายเลขโทรศัพท์สายด่วนช่วยเหลือด่วนของผู้ให้บริการคลาวด์) รวมถึงพิจารณาความพร้อมในการกำหนดรายการชุดข้อมูลสารสนเทศสำคัญที่หน่วยงานต้องจัดเตรียมเพื่อประกอบการแจ้งเหตุ ตลอดจนการมอบหมายระบุกลุ่มเจ้าหน้าที่หรือบุคลากรภายในหน่วยงานที่มีสิทธิและหน้าที่เป็นผู้รับผิดชอบหลักในการส่งแจ้งรายงานภัยคุกคามดังกล่าว*<br>*- ตรวจสอบพยานข้อมูลว่าหน่วยงานรับทราบช่องทางและรูปแบบขั้นตอนปฏิบัติที่ผู้ให้บริการคลาวด์กำหนดใช้สำหรับรายงานหรือแจ้งคำเตือนเข้ามายังหน่วยงานเมื่อผู้ให้บริการตรวจพบเหตุการณ์ภัยคุกคามขึ้นบนระบบคลาวด์ โดยครอบคลุมถึงขอบเขตความเข้าใจประเภทระดับความรุนแรงของภัยคุกคามที่จะต้องแจ้งเตือน กรอบเวลาเป้าหมายความเร็ว* | ระดับกลาง ระดับสูง | 5.2.10.2 (ก) | ☐ มี/ดำเนินการแล้วเสร็จ<br>☐ มี/ดำเนินการแล้วบางส่วน<br>☐ อยู่ระหว่างการดำเนินการ<br>☐ ไม่มี/ยังไม่ได้ดำเนินการ<br>☐ ไม่เกี่ยวข้อง | *<u>ตัวอย่างหลักฐาน</u>*<br>*- เอกสารคู่มือขั้นตอนการแจ้งเหตุภัยคุกคามความปลอดภัยระบบไอที (Incident Response and Reporting Procedure)*<br>*- ทะเบียนรายชื่อบุคลากรที่ได้รับมอบหมายและข้อมูลช่องทางการติดต่อผู้ประสานงานของหน่วยงานและผู้ให้บริการคลาวด์ (Contact Matrix)*<br>*- เอกสารแนวทางการรับแจ้งและประสานงานภัยคุกคามระบบคลาวด์ (CSP Security Incident Notification Specification)*<br>*- ภาพหน้าจอแสดงการตรวจสอบการตั้งค่าผู้รับข้อมูลความมั่นคงปลอดภัยส่วนกลางเพื่อรับอีเมลหรือระบบแจ้งเตือนกรณีฉุกเฉิน (เช่น Security Admin Contacts in Cloud Portal)*<br>*- ภาพหน้าจอยืนยันการมีอยู่และการเข้าใช้งานพอร์ทัลในการติดตามสถานะการรายงานเหตุการณ์ด้านความ* |

| ข้อ | รายการ | ระดับที่บังคับใช้ | ข้อกำหนด | สถานะการดำเนินงานในปัจจุบัน | หลักฐาน/เอกสารอ้างอิง |
|---|---|---|---|---|---|
| | *ของการแจ้งเหตุ (Notification SLA) และรายละเอียดคุณลักษณะของพยานหลักฐานหรือบันทึกข้อมูลที่จะได้รับจากผู้ให้บริการคลาวด์*<br>*- ตรวจสอบระบบในการควบคุม ติดตาม และอัปเดตสถานะของตั๋วหรือกรณีเกิดเหตุการณ์ที่ได้รายงานไปอย่างเป็นระบบ (เช่น ช่องทางการตรวจสอบประวัติผ่านตั๋ว/Ticket ID หรือระบบพอร์ทัล และการได้รับรายงานอัปเดตความคืบหน้าเป็นระยะ) โดยตรวจสอบข้อมูลเงื่อนไขรอบระยะเวลาความถี่ในการแจ้งอัปเดตจากผู้ให้บริการ และรูปแบบรายละเอียดโครงสร้างข้อมูลสถานะความคืบหน้าที่จะได้รับจากผู้ให้บริการจนสิ้นสุดมาตรการระงับเหตุ* | | | | *ปลอดภัย (เช่น Cloud Provider Support Center / Security Ticket Dashboard)*<br>*- ตัวอย่างเอกสารบันทึกหรือบันทึกประวัติการส่งตั๋วและติดตามสถานะประสานการระงับเหตุความผิดปกติระบบคลาวด์ ร่วมกับผู้ให้บริการคลาวด์* |

ข้าพเจ้ารับทราบและยืนยันว่า ผลการประเมินสถานภาพตนเอง ตามแบบประเมินสถานภาพการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ สำหรับผู้ใช้บริการ ตลอดจนรายละเอียดข้อมูล เอกสาร และหลักฐานทั้งหมดที่แนบประกอบในแบบประเมินฯ ฉบับนี้ มีความถูกต้อง ครบถ้วน และตรงกับความเป็นจริงทุกประการ โดยเป็นการประเมินความสอดคล้องตามเกณฑ์ข้อกำหนดขั้นต่ำของ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ของ _____[ ระบุชื่อหน่วยงาน ]_____ สำหรับระบบสารสนเทศ _____ _____[ ระบุชื่อระบบสารสนเทศ ]_____ ซึ่งประเมินแล้วเสร็จเมื่อวันที่ _____[ ระบุ วัน เดือน ปี ที่ประเมินเสร็จสิ้น ]_____

ลงชื่อ _____ ผู้ประเมิน
( _____ )
ตำแหน่ง _____
วันที่ประเมิน ____/____/____

ลงชื่อ _____ ผู้อนุมัติ
( _____ )
ตำแหน่ง _____
วันที่อนุมัติ ____/____/____

**เอกสารอ้างอิง**

1. ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 : https://ratchakitcha.soc.go.th/documents/43184.pdf
2. ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 : https://ratchakitcha.soc.go.th/documents/17286.pdf

**ข้อสงสัย/ข้อเสนอแนะ** หากหน่วยงานพบปัญหา ข้อขัดข้อง มีข้อสอบถาม หรือมีความประสงค์จะเสนอแนะเพิ่มเติมเกี่ยวกับการดำเนินการตามแบบประเมินนี้ สามารถติดต่อและส่งข้อมูลได้ที่อีเมล cloudsecurity.info@ncsa.or.th ทั้งนี้ หน่วยงานสามารถติดตามข่าวสารล่าสุดเกี่ยวกับมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ได้ที่เว็บไซต์ https://cloudsecurity.ncsa.or.th/