**ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ**
**เรื่อง กรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์**
**(Thailand's National Cloud Security Framework)**

---

โดยที่เป็นการสมควรกำหนดกรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Cloud Security Framework) เพื่อให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง สามารถใช้เป็นกรอบในการเตรียมความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ประกอบประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ เป็นไปอย่างมีประสิทธิภาพ มีมาตรฐาน มีความมั่นคงปลอดภัยไซเบอร์ และเท่าทันความก้าวหน้าทางเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็วในปัจจุบัน

อาศัยอำนาจตามความในข้อ ๗ ของประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง กรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Thailand's National Cloud Security Framework)"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันประกาศเป็นต้นไป

ข้อ ๓ เพื่อประโยชน์ในการดำเนินการตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ ให้มีประสิทธิภาพ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง นำกรอบการทำงานแนบท้ายประกาศนี้ มาใช้เป็นแนวทางในการดำเนินการของตน

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้เลขาธิการมีอำนาจตีความและวินิจฉัยชี้ขาด แล้วรายงานให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทราบ ทั้งนี้ การตีความ และคำวินิจฉัยของเลขาธิการให้เป็นที่สุด

ประกาศ ณ วันที่ ๑๐ มีนาคม พ.ศ. ๒๕๖๘

พลอากาศตรี
(อมร ชมเชย)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

# กรอบการทำงาน
# ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์
# (Thailand's National Cloud Security Framework)

เวอร์ชัน 1.0

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

# คำนำ

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศมีบทบาทสำคัญต่อการดำเนินชีวิตและการดำเนินธุรกิจ ความมั่นคงปลอดภัยทางไซเบอร์จึงกลายเป็นประเด็นที่มีความสำคัญอย่างยิ่ง โดยเฉพาะในบริบทของระบบคลาวด์ที่ได้รับความนิยมอย่างแพร่หลาย การจัดเก็บข้อมูลและการให้บริการบนคลาวด์ช่วยเพิ่มความสะดวกสบายและประสิทธิภาพ แต่ขณะเดียวกันก็เปิดโอกาสให้เกิดภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้น ซึ่งอาจส่งผลกระทบร้ายแรงต่อบริการภาครัฐที่สำคัญและโครงสร้างพื้นฐานด้านสารสนเทศ ทั้งนี้ ผลกระทบดังกล่าวอาจลุกลามไปสู่เศรษฐกิจ สังคม และประชาชนในวงกว้างอย่างหลีกเลี่ยงไม่ได้

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จึงได้จัดทำกรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ เพื่อตอบสนองต่อความท้าทายเหล่านี้ โดยมุ่งหวังให้ผู้ใช้บริการคลาวด์ (Cloud Service Customer) และผู้ให้บริการคลาวด์ (Cloud Service Provider) รวมถึงหน่วยงานอื่นที่เกี่ยวข้อง มีความพร้อมทางด้านบุคลากร กระบวนการ และเทคโนโลยี ที่จะปฏิบัติตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ ซึ่งจะมีผลบังคับใช้ในวันที่ ๑๐ กันยายน ๒๕๖๙

หัวใจสำคัญที่จะทำให้เกิดการดำเนินการตามกรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ได้แก่ การกำหนดมาตรการและแนวทางเพื่อสนับสนุนมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ ร่วมกับทุกภาคส่วนที่เกี่ยวข้อง ทั้งหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สถาบันการศึกษา หน่วยงานกำหนดนโยบาย ผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และผู้ให้บริการคลาวด์ทั้งภายในและต่างประเทศ เป็นต้น รวมถึงความจำเป็นที่ สกมช. จะประสานการทำงานกับทุกภาคส่วนดังกล่าวในการขับเคลื่อนมาตรการและแนวทางให้เกิดความเป็นรูปธรรมต่อไป

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

# กิตติกรรมประกาศ

“กรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Thailand’s National Cloud Security Framework)” ได้รับความอนุเคราะห์ในการสนับสนุนและช่วยเหลือในการดำเนินจัดทำจาก ดร. ธัชพล โปษยานนท์ ร่วมกับ บริษัท พาโล อัลโต เน็ตเวิร์กส์ (ประเทศไทย) จำกัด รวมถึง พลอากาศตรี จเด็ด คูหะก้องกิจ ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ซึ่งได้ใช้ความรู้ ความสามารถ และประสบการณ์ของท่านในการจัดทำกรอบการทำงานฉบับนี้ร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) อันจะเป็นประโยชน์กับผู้สนใจและหน่วยงานที่ปฏิบัติงานเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์เป็นอย่างมาก ในโอกาสนี้ สกมช. จึงขอแสดงความขอบคุณบุคคลและหน่วยงาน ที่ได้ให้การสนับสนุนและช่วยเหลือในการดำเนินจัดทำกรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Thailand’s National Cloud Security Framework)” ซึ่งทำให้การดำเนินงานเป็นไปได้อย่างราบรื่นและประสบความสำเร็จมา ณ โอกาสนี้

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

# สารบัญ

# บทที่ 1 บทนำ

## 1.1 หลักการและเหตุผล

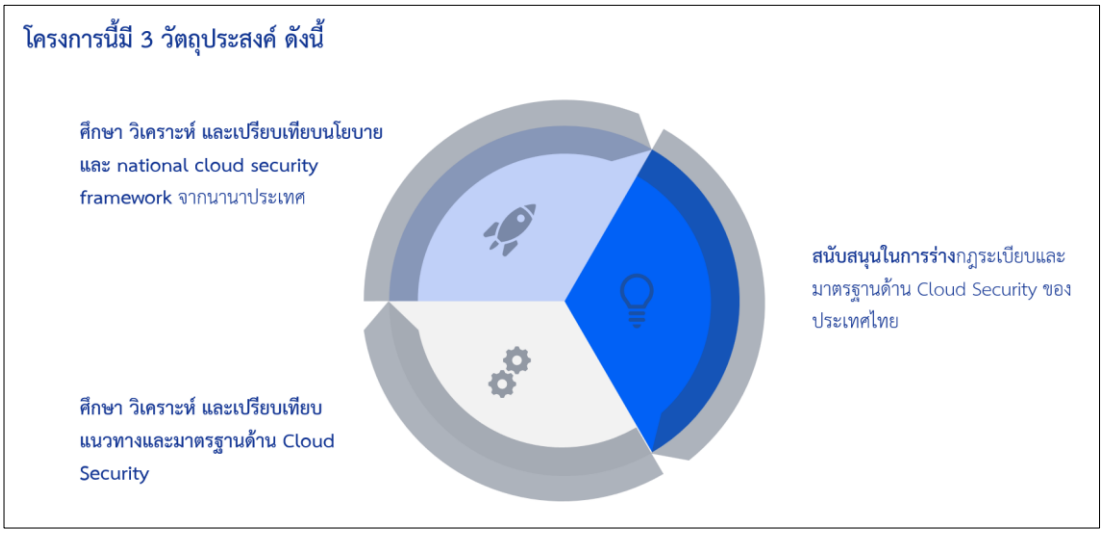
ประเทศไทยได้กำหนดนโยบาย Cloud First Policy เพื่อส่งเสริมการใช้งานระบบคลาวด์ในภาครัฐ และขับเคลื่อนการเปลี่ยนผ่านสู่รัฐบาลดิจิทัล โดยมุ่งเน้นการเพิ่มประสิทธิภาพของบริการสาธารณะ และการจัดการข้อมูลที่ปลอดภัย นโยบายนี้อยู่ภายใต้แผนพัฒนาดิจิทัลแห่งชาติ ซึ่งมีเป้าหมายที่จะทำให้ประเทศไทยเป็นศูนย์กลางเศรษฐกิจดิจิทัลในภูมิภาค โดยภายในปี 2025 รัฐบาลตั้งเป้าย้ายระบบของหน่วยงานรัฐกว่า 10% ไปยังคลาวด์ รวมถึงการพัฒนามาตรฐานความปลอดภัยและแพลตฟอร์มบริหารจัดการคลาวด์เพื่อรองรับการใช้งานที่หลากหลาย ทั้งนี้ การดำเนินนโยบายดังกล่าวยังสอดคล้องกับแนวโน้มการลงทุนในโครงสร้างพื้นฐานด้านคลาวด์จากบริษัทเทคโนโลยีชั้นนำระดับโลก

อย่างไรก็ตาม การนำระบบคลาวด์มาใช้มากขึ้นในประเทศไทยก่อให้เกิดความเสี่ยงทางไซเบอร์ที่ซับซ้อนและหลากหลายมากขึ้น เช่น การโจมตีด้วยมัลแวร์ขั้นสูง การละเมิดข้อมูลส่วนบุคคล และช่องโหว่ในระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) ทั้งนี้ รายงานจาก ThaiCERT ระบุว่า การโจมตีทางไซเบอร์ในปี 2023 เพิ่มขึ้นอย่างมีนัยสำคัญ โดยเฉพาะในภาคการศึกษาและหน่วยงานรัฐ เพื่อรับมือกับความเสี่ยงเหล่านี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จึงได้ออกมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 เพื่อกำหนดแนวทางปฏิบัติที่ชัดเจนสำหรับผู้ใช้บริการคลาวด์ (Cloud Service Customer) และผู้ให้บริการคลาวด์ (Cloud Service Provider)

การศึกษา National Cloud Security Framework ของประเทศต่าง ๆ เช่น สิงคโปร์ ออสเตรเลีย สหรัฐอเมริกา และอินเดีย ช่วยให้เห็นถึงแนวทางที่หลากหลายในการจัดการความปลอดภัยของระบบคลาวด์ ตัวอย่างเช่น สิงคโปร์เน้นการกำกับดูแลที่เข้มงวดผ่านมาตรฐาน Multi-Tier Cloud Security (MTCS) ส่วนออสเตรเลียใช้กรอบการทำงานเชิงบูรณาการ เช่น Information Security Manual (ISM) ขณะที่สหรัฐฯ มีมาตรฐาน NIST Cybersecurity Framework ที่ครอบคลุม และอินเดียมุ่งเน้นการพัฒนามาตรฐานความปลอดภัยเฉพาะสำหรับข้อมูลสำคัญ การเปรียบเทียบแนวทางเหล่านี้จะช่วยให้ประเทศไทยสามารถปรับปรุงกรอบการทำงานด้านความปลอดภัยไซเบอร์ให้เหมาะสมกับบริบทของประเทศและตอบสนองต่อความต้องการของผู้ใช้งานได้อย่างมีประสิทธิภาพ

## 1.2 วัตถุประสงค์ของการศึกษา

การศึกษากรอบมาตรฐานด้าน Cloud security ของต่างประเทศ และร่วมจัดทำกรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Thailand's National Cloud Security Framework) มีวัตถุประสงค์ การดำเนินงาน 3 ข้อ ได้แก่




รูปที่ 0-1: วัตถุประสงค์ของการดำเนินการ

1) เพื่อศึกษา วิเคราะห์ และเปรียบเทียบนโยบายและ National Cloud Security Framework จากนานาประเทศ
2) เพื่อศึกษา วิเคราะห์ และเปรียบเทียบแนวทางและมาตรฐานด้าน Cloud Security
3) เพื่อสนับสนุนในการร่างกฎระเบียบและมาตรฐานด้าน Cloud Security

### 1.3 แผนการดำเนินการ

เพื่อให้การดำเนินการบรรลุวัตถุประสงค์และเป้าหมายที่ตั้งไว้ ที่ปรึกษาจึงได้แบ่งการดำเนินการออกเป็น 3 ระยะ ดังสรุปได้ต่อไปนี้

**การดำเนินการระยะที่ 1** เป็นการวางแผนการดำเนินการโดยละเอียด เพื่อกำหนดรายละเอียดขั้นตอน และระยะเวลาของการดำเนินงานในทุกแผนงาน ซึ่งครอบคลุมทุกกิจกรรมตามขอบเขตการดำเนินงาน

**การดำเนินการระยะที่ 2** เป็นการศึกษาสถานการณ์ในประเทศไทยและต่างประเทศ และจัดทำ (ร่าง) นโยบาย เพื่อศึกษา ทบทวน ทำความเข้าใจเกี่ยวกับนโยบาย National cloud first policies และ National cloud security framework รวมถึงแนวทางและมาตรฐานด้าน Cloud security ที่เกิดขึ้นในต่างประเทศ เช่น สิงค์โปร์ ออสเตรเลีย อเมริกา และอินเดีย เป็นต้น ก่อนที่จะสรุปผลการดำเนินงานในส่วนนี้ เพื่อทำการศึกษาวิเคราะห์ความเป็นไปได้ และการจัดทำ (ร่าง) นโยบาย

**การดำเนินการระยะที่ 3** เป็นการสรุปผลการศึกษา โดยที่ปรึกษาจะสรุปผลการศึกษาและวิจัยข้อมูลที่ได้จากการดำเนินงาน เพื่อจัดทำและนำส่งรายงานการดำเนินการฉบับสมบูรณ์ (Final Report)

# บทที่ 2 การศึกษาการดำเนินนโยบาย National Cloud Security Framework ของแต่ละประเทศ

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| **หน่วยงานที่กำหนดหลักการ** | ➢ Info-communications Media Development Authority (IMDA)<br>เป็นหน่วยงานของรัฐบาลสิงคโปร์ที่มีหน้าที่หลักในการส่งเสริมและพัฒนาภาคสื่อสารและเทคโนโลยีสารสนเทศของประเทศ รวมถึงการกำกับดูแลกิจการกระจายเสียงและกิจการโทรคมนาคมหน่วยงานนี้มีบทบาทสำคัญในการขับเคลื่อนสิงคโปร์ให้เป็นศูนย์กลางด้านดิจิทัลและเทคโนโลยีสารสนเทศในภูมิภาคเอเชียตะวันออกเฉียงใต้ | ➢ National Institute of Standards and Technology (NIST)<br>เป็นหน่วยงานภายใต้กระทรวงพาณิชย์สหรัฐอเมริกา มาตรฐานต่าง ๆ ของ NIST ได้รับการยอมรับและนำไปใช้อย่างแพร่หลายทั้งในสหรัฐฯ และนานาประเทศ โดยเฉพาะมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ | ➢ Australian Signals Directorate (ASD)<br>เป็นหน่วยงานด้านความมั่นคงปลอดภัยสารสนเทศและการสื่อสารของรัฐบาลออสเตรเลีย ASD ทำงานร่วมกับหน่วยงานด้านความมั่นคงและการข่าวกรองอื่น ๆ เพื่อปกป้องผลประโยชน์แห่งชาติของออสเตรเลียจากภัยคุกคามไซเบอร์ต่าง ๆ<br>นอกจากนี้ ASD ยังมีบทบาทในการสนับสนุนภารกิจด้านการข่าวกรองและปฏิบัติการของกองทัพออสเตรเลียด้วย | ➢ Ministry of Electronics and Information Technology (MeitY)<br>เป็นหน่วยงานของรัฐบาลกลางอินเดีย MeitY ทำหน้าที่กำหนดนโยบาย หลักเกณฑ์ และหลักการต่าง ๆ เช่น National Cloud Security Policy และเป็นผู้ริเริ่มโครงการ GI Cloud Initiative เพื่อส่งเสริมการใช้คลาวด์ภาครัฐอย่างปลอดภัย<br>นอกจากนี้ MeitY ยังเป็นผู้กำหนดมาตรฐานและข้อปฏิบัติต่าง ๆ สำหรับความมั่นคงปลอดภัยดิจิทัลของอินเดีย เช่น ข้อกำหนดด้านการรักษาความปลอดภัยข้อมูลส่วนบุคคล (Data Protection Requirements) |
| **หน้าที่หลักของหน่วยงาน** | 1) ส่งเสริมและสนับสนุนการพัฒนาอุตสาหกรรมสื่อ เทคโนโลยีสารสนเทศ และโทรคมนาคมของสิงคโปร์ให้มีความแข็งแกร่งและทันสมัย<br>2) กำกับดูแลและกำหนดนโยบายสำหรับกิจการกระจายเสียง โทรคมนาคม และเนื้อหาดิจิทัล เพื่อคุ้มครองผู้บริโภคและส่งเสริมการแข่งขัน<br>3) จัดสรรและบริหารจัดการคลื่นความถี่วิทยุและทรัพยากรที่จำกัดอื่น ๆ อย่างมีประสิทธิภาพ<br>4) ส่งเสริมการพัฒนาโครงสร้างพื้นฐานดิจิทัลและการนำเทคโนโลยีใหม่ ๆ มาใช้ในสิงคโปร์ | 1) พัฒนาและส่งเสริมมาตรฐานทางเทคนิคต่าง ๆ สำหรับอุตสาหกรรมและภาคส่วนต่าง ๆ ทั้งภายในและต่างประเทศ รวมถึงมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์<br>2) ให้บริการด้านการวัดและทดสอบ รวมถึงค้นคว้าวิจัยเกี่ยวกับการวัดและมาตรฐาน<br>3) ส่งเสริมการถ่ายทอดเทคโนโลยี โดยทำงานร่วมกับภาคอุตสาหกรรมและสถาบันการศึกษา<br>4) ให้คำปรึกษาด้านเทคนิคแก่หน่วยงานของรัฐบาลกลาง | 1) ให้คำแนะนำและกำหนดนโยบายด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานรัฐบาลออสเตรเลียและองค์กรสำคัญของประเทศ<br>2) ดำเนินงานด้านการรักษาความปลอดภัยสารสนเทศและการสื่อสารของรัฐบาลออสเตรเลีย<br>3) จัดทำมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น Australian Information Security Manual (ISM)<br>4) ให้คำปรึกษาและความช่วยเหลือด้านความมั่นคงปลอดภัยไซเบอร์แก่หน่วยงานต่าง ๆ ของรัฐบาล | 1) กำหนดนโยบาย แนวทาง และมาตรฐานสำหรับเทคโนโลยีสารสนเทศและอิเล็กทรอนิกส์ของประเทศ<br>2) ส่งเสริมการพัฒนาอุตสาหกรรมไอทีและอิเล็กทรอนิกส์ของอินเดีย<br>3) ผลักดันการนำเทคโนโลยีดิจิทัลมาใช้ในหน่วยงานภาครัฐและภาคเอกชน<br>4) สนับสนุนการวิจัยและพัฒนาด้านอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศ<br>5) รับผิดชอบเรื่องนโยบายและความมั่นคงปลอดภัยไซเบอร์ของประเทศ |
| **จำนวนพนักงาน** | IMDA มีพนักงานประมาณ 900 คน และเป็นหน่วยงานภายใต้กระทรวงการสื่อสารและ | NIST มีพนักงานประมาณ 3,400 คน และเป็นหน่วยงานหลักในการกำหนดมาตรฐานและแนว | ASD มีพนักงานประมาณ 1,900 คน และเป็นหน่วยงานภายใต้กระทรวงกลาโหมของออสเตรเลีย (Department of Defence)[3] | MeitY มีพนักงานประมาณ 398 คน และเป็นหน่วยงานระดับกระทรวงที่รายงานตรงต่อรัฐมนตรีว่าการกระทรวงอิเล็กทรอนิกส์และ |

[3] อ้างอิง: Diversity of ASD Employees https://shorturl.asia/qEwBi (transparency.gov.au)

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| | สารสนเทศ (Ministry of Communications and Information) ของสิงคโปร์[1] | ปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ของสหรัฐฯ เช่น NIST Cybersecurity Framework[2] | | เทคโนโลยีสารสนเทศ ในด้านความมั่นคงปลอดภัยคลาวด์[4] |
| **Reference** | As of Mar 1st, 2024 | As of April 19, 2024 | As of 2022 | As of May, 2024 |
| **ผลการบังคับใช้** | การบังคับใช้ MTCS SS (Multi-Tier Cloud Security Standard for Singapore) ในสิงคโปร์จะแบ่งออกเป็น 2 ส่วนหลัก ดังนี้<br><br>**1) สำหรับผู้ให้บริการคลาวด์ (Cloud Service Providers)**<br>- ผู้ให้บริการคลาวด์ทุกรายที่ให้บริการในสิงคโปร์จะต้องปฏิบัติตามข้อกำหนด MTCS SS<br>- มาตรฐานได้แบ่งระดับความปลอดภัยออกเป็น 4 ระดับ ตั้งแต่ระดับ 1 ถึง 4 โดยผู้ให้บริการต้องรับรองระดับตามความเหมาะสม<br>- ผู้ให้บริการต้องดำเนินการประเมินความปลอดภัยโดยองค์กรที่ได้รับการรับรองจากรัฐบาลสิงคโปร์<br><br>**2) สำหรับผู้ใช้บริการคลาวด์ (Cloud Consumers)**<br>- องค์กร หน่วยงาน ทั้งภาครัฐและเอกชนที่ใช้บริการคลาวด์ในสิงคโปร์ควรเลือกใช้บริการจากผู้ให้บริการที่ได้รับการรับรอง MTCS SS | การบังคับใช้มาตรฐาน NIST 800-53 และ NIST 800-144 ในสหรัฐอเมริกาสำหรับผู้ให้บริการและผู้ใช้บริการคลาวด์ มีดังนี้<br><br>**1) สำหรับผู้ให้บริการคลาวด์ (Cloud Service Providers)**<br>- NIST 800-53 Rev.5 เป็นมาตรฐานควบคุมระบบสารสนเทศและความมั่นคงปลอดภัยที่หน่วยงานรัฐบาลกลางของสหรัฐฯ ต้องปฏิบัติตาม<br>- ผู้ให้บริการคลาวด์ที่ต้องการรับรองตาม FedRAMP (Federal Risk and Authorization Management Program) จำเป็นต้องผ่านการประเมินความสอดคล้องกับ NIST 800-53<br>- NIST 800-144 ให้คำแนะนำเกี่ยวกับการประเมินความปลอดภัยของผู้ให้บริการคลาวด์สำหรับหน่วยงานรัฐบาลกลาง<br><br>**2) สำหรับผู้ใช้บริการคลาวด์ (Cloud Consumers)**<br>- หน่วยงานรัฐบาลกลางของสหรัฐฯ จำเป็นต้องเลือกใช้บริการคลาวด์ที่ได้รับการรับรองตาม | ISM (Information Security Manual) เป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศที่บังคับใช้ในหน่วยงานรัฐบาลกลางของประเทศออสเตรเลีย มีรายละเอียดดังนี้<br><br>**1) สำหรับผู้ให้บริการคลาวด์ (Cloud Service Providers):**<br>- ISM เป็นข้อกำหนดที่บังคับใช้กับหน่วยงานรัฐบาลกลางของออสเตรเลีย<br>- ผู้ให้บริการคลาวด์ที่ต้องการให้บริการแก่หน่วยงานรัฐบาลจำเป็นต้องได้รับการรับรองให้สอดคล้องกับ ISM<br>- กระบวนการรับรองจะประเมินผู้ให้บริการในประเด็นต่าง ๆ เช่น การควบคุมการเข้าถึง, การบริหารจัดการ, และการดำเนินงาน<br>**2) สำหรับผู้ใช้บริการคลาวด์ (Cloud Consumers)**<br>- หน่วยงานรัฐบาลออสเตรเลียต้องปฏิบัติตามข้อกำหนด ISM ในการใช้งานคลาวด์<br>- ISM มีข้อแนะนำการบริหารความเสี่ยง, การประเมิน, และการตรวจสอบสำหรับผู้ใช้บริการคลาวด์<br>- หน่วยงานต้องเลือกใช้บริการจากผู้ให้บริการที่ผ่านการรับรองตาม ISM | Cloud Security Guidelines เป็นมาตรฐานที่ Ministry of Electronics and Information Technology (MeitY) ของประเทศอินเดียกำหนดไว้เพื่อให้ผู้ให้บริการและผู้ใช้บริการคลาวด์ในประเทศปฏิบัติตาม โดยมีรายละเอียดดังนี้<br><br>**1) สำหรับผู้ให้บริการคลาวด์ (Cloud Service Providers):**<br>- ผู้ให้บริการคลาวด์ต้องปฏิบัติตามข้อกำหนดใน Cloud Security Guidelines เพื่อให้บริการแก่หน่วยงานภาครัฐอินเดีย หลักเกณฑ์สำคัญได้แก่ มาตรการควบคุมการเข้าถึง, การเข้ารหัสข้อมูล, การตรวจสอบและบันทึกลงกิจกรรม, และการรักษาความลับของข้อมูล<br>- ผู้ให้บริการต้องผ่านการรับรองตามข้อกำหนดจากหน่วยงานรับรองที่ได้รับการแต่งตั้งจาก MeitY<br>**2) สำหรับผู้ใช้บริการคลาวด์ (Cloud Consumers)**<br>- หน่วยงานภาครัฐของอินเดียจำเป็นต้องเลือกใช้บริการจากผู้ให้บริการคลาวด์ที่ผ่านการรับรองจาก MeitY หน่วยงานต้องประเมินความเสี่ยงตามแนวทางของ MeitY ก่อนใช้บริการคลาวด์ |

[1] อ้างอิง: https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/imda-leveling-up-singapores-ai-talent-pool

[2] อ้างอิง: https://www.nist.gov/careers/pay-benefits-and-leave/nist-pay-charts

[4] อ้างอิง: https://www.zoominfo.com/pic/meity/464489291

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| | - ควรพิจารณาเลือกใช้ระดับความปลอดภัยที่เหมาะสมกับความต้องการของตน<br>- ต้องมีการประเมินความเสี่ยงด้านความปลอดภัยก่อนใช้งานบริการคลาวด์ | FedRAMP ซึ่งหมายถึงผ่านการประเมิน NIST 800-53 แล้ว<br>- NIST 800-144 ให้แนวทางการประเมินความเสี่ยงสำหรับผู้ใช้บริการคลาวด์ในภาครัฐ<br>- สำหรับภาคเอกชน ไม่มีข้อบังคับให้ต้องปฏิบัติตาม แต่อาจใช้เป็นแนวปฏิบัติได้ | - ISM ยังมีข้อกำหนดเพิ่มเติม เช่น ผู้รับผิดชอบด้านความมั่นคง, ผู้ตรวจสอบอิสระ, และการจัดหาระบบที่ปลอดภัย<br>- สำหรับภาคเอกชนไม่มีการบังคับให้ปฏิบัติตาม ISM โดยตรง แต่อาจใช้เป็นแนวทางปฏิบัติที่ดีในการบริหารความมั่นคงปลอดภัยสารสนเทศ | - หน่วยงานมีหน้าที่ต้องบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ, ควบคุมการเข้าถึงข้อมูล, และมีแผนรองรับเหตุฉุกเฉิน.<br>- สำหรับภาคเอกชนในอินเดีย : ไม่มีข้อบังคับตามกฎหมายให้ปฏิบัติตาม Cloud Security Guidelines แต่สามารถนำไปใช้เป็นแนวทางปฏิบัติที่ดี. |
| **อ้างอิง** | ➢ เว็บไซต์ของ Cyber Security Agency of Singapore (CSA) ซึ่งเป็นหน่วยงานกำกับดูแลมาตรฐาน MTCS SS[5]<br>➢ Multi-Tier Cloud Security Standard for Singapore (MTCS SS) Documentation Release 3.0 ฉบับปี 2020[6]<br>➢ บทความจาก Enterprise Singapore ซึ่งเป็นหน่วยงานส่งเสริมธุรกิจของสิงคโปร์[7] | ➢ NIST Special Publication 800-53 Rev.5 "Security and Privacy Controls for Information Systems and Organizations" [9] เป็นมาตรฐานการควบคุมความมั่นคงปลอดภัยสำหรับหน่วยงานรัฐบาลกลางสหรัฐฯ<br>➢ NIST Special Publication 800-144 "Guidelines on Security and Privacy in Public Cloud Computing"[10] ให้แนวทางการประเมินความเสี่ยงและความปลอดภัยของบริการคลาวด์สาธารณะ | ➢ Information Security Manual (ISM) - Australian Government[14] เว็บไซต์หลักของ Australian Cyber Security Centre ซึ่งเป็นผู้จัดทำและบริหารจัดการ ISM<br>➢ Information Security Manual (September 2022)[15] เอกสารฉบับล่าสุดของ ISM ที่ระบุหลักเกณฑ์และข้อกำหนดด้านความมั่นคงปลอดภัย<br>➢ Cloud Security Considerations[16] แนวทางการประเมินและจัดการความเสี่ยงด้านความมั่นคงสำหรับการใช้งานคลาวด์ | ➢ Cloud Security Guidelines[19] โดย MeitY เว็บไซต์ MeitY ด้านความมั่นคงปลอดภัยไซเบอร์[20]<br>➢ National Cloud Computing Compliance (NCCC)[21]<br>➢ รายชื่อผู้ตรวจสอบคลาวด์ที่ได้รับการแต่งตั้งจาก MeitY[22]<br>➢ Cloud Security Assessment Model จาก NCCC[23] |

[5] อ้างอิง: https://www.csa.gov.sg/singcert/publications/cloud-security-for-singapore, https://www.csa.gov.sg/programmes/certifications/multi-tier-cloud-security-standard-mtcs-ss

[6] อ้างอิง: https://www.csa.gov.sg/-/media/Csa/Documents/MTCS_Standard_Release_3_035d6d8bbb9cf49b489e1b3e6cf6e241c.pdf

[7] อ้างอิง: https://www.enterprisesg.gov.sg/keeping-businesses-secure/for-businesses/secure-cloud-resources/multi-tier-cloud-security-mtcs-standard

[9] อ้างอิง: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[10] อ้างอิง: https://csrc.nist.gov/publications/detail/sp/800-144/final

[14] อ้างอิง: https://www.cyber.gov.au/acsc/view-all-content/ism

[15] อ้างอิง: https://www.cyber.gov.au/acsc/view-all-content/ism/ism-release-september-2022

[16] อ้างอิง: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-security-considerations

[19] อ้างอิง: http://meity.gov.in/writereaddata/files/Guidelines-Cloud_Security.pdf

[20] อ้างอิง: https://www.meity.gov.in/cyber-security

[21] อ้างอิง: https://nccc.gov.in/

[22] อ้างอิง: https://nccc.gov.in/empaneledauditors

[23] อ้างอิง: https://nccc.gov.in/resources-references

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| | ➢ บทความจาก Singapore Data Center ซึ่งเป็นสมาคมของผู้ประกอบการดาต้าเซ็นเตอร์ในสิงคโปร์[8] | ➢ FedRAMP (Federal Risk and Authorization Management Program) [11] โปรแกรมการรับรองความปลอดภัยสำหรับผู้ให้บริการคลาวด์ที่ให้บริการแก่หน่วยงานรัฐบาลกลาง ใช้ NIST 800-53 เป็นมาตรฐานการประเมิน<br>➢ GSA's FedRAMP Tailored Rev.4 Baseline[12] แนวทางการนำ NIST 800-53 มาประยุกต์ใช้สำหรับบริการคลาวด์ที่ได้รับการรับรองจาก FedRAMP<br>➢ NIST Cloud Computing Program โครงการด้าน Cloud Computing ของ NIST รวบรวมมาตรฐานและแนวปฏิบัติที่เกี่ยวข้อง[13] | ➢ Australian Government Information Security Manual (ISM) Compliance[17] หน้าเว็บของ Australian Signals Directorate ซึ่งเป็นหน่วยงานรักษาความปลอดภัยของรัฐบาล อธิบายการปฏิบัติตาม ISM<br>➢ ISM Compliance and Certification ข้อมูลเกี่ยวกับโปรแกรมการรับรองความสอดคล้องกับ ISM สำหรับผู้ให้บริการคลาวด์[18] | ➢ บทความจาก CERT-In เกี่ยวกับความมั่นคงปลอดภัยคลาวด์[24]<br>➢ คู่มือความมั่นคงปลอดภัยคลาวด์ของ NIC-CERT[25]<br>➢ บทความจาก DSCI เกี่ยวกับ Cloud Security Guidelines ของ MeitY[26] |
| **มาตรฐานที่ใช้ในการจัดทำ** | **ISO/IEC 27001 - Information Security Management System**<br>1) เป็นมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่ได้รับการยอมรับในระดับสากล MTCS SS นำหลักการสำคัญของ ISO 27001 มาประยุกต์ใช้ | **NIST SP 800-53 และ NIST SP 800-144** ทั้งสองฉบับได้อ้างอิงและใช้แนวทางจากมาตรฐานต่าง ๆ ดังนี้<br>1) NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations<br>- อ้างอิงจากมาตรฐาน ISO/IEC 27001 Information Security Management ในส่วนของการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ | **ISM (Information Security Manual)** ของรัฐบาลออสเตรเลียได้นำเอาหลักการและแนวทางจากมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศหลายแห่งมาใช้ ดังนี้<br>1) ISO/IEC 27000 Series: ชุดมาตรฐานสากลที่ครอบคลุมระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการควบคุม<br>➢ ISM อ้างอิงมาตรฐาน ISO/IEC 27001 และ 27002 | **Cloud Security Guidelines** ที่ออกโดย Ministry of Electronics and Information Technology (MeitY) ของอินเดีย ได้อ้างอิงและใช้แนวทางจากมาตรฐานต่าง ๆ ดังนี้<br>1) ISO/IEC 27001 และ 27002<br>➢ Cloud Security Guidelines ได้นำแนวทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศจากมาตรฐาน ISO 27001 และ |

[8] อ้างอิง: https://www.singaporedatacenter.com/blog/2022/02/mtcs-certification-singapore/

[11] อ้างอิง: https://www.fedramp.gov/

[12] อ้างอิง: https://www.fedramp.gov/assets/resources/documents/FedRAMP_Tailored_Revision_4_Baseline.pdf

[13] อ้างอิง; https://csrc.nist.gov/projects/cloud-computing

[17] อ้างอิง: https://www.asd.gov.au/infosec/ism

[18] อ้างอิง: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/certified-clouds

[24] อ้างอิง: https://www.cert-in.org.in/Advisories/CloudSecurityBestPractices.htm

[25] อ้างอิง: https://cert.nic.in/nic-cert/viewpdf/cloud-security

[26] อ้างอิง: https://www.dsci.in/sites/default/files/documents/resourcecentre/GovCloud.pdf

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| | 2) ISO/IEC 27017 - Code of Practice for Information Security Controls for Cloud Services<br>3) เป็นมาตรฐานแนวปฏิบัติด้านการควบคุมความมั่นคงปลอดภัยสำหรับบริการคลาวด์ MTCS SS ได้นำข้อกำหนดจากมาตรฐานนี้มา integrate เอาไว้<br>4) Cloud Security Alliance (CSA) Cloud Controls Matrix<br>5) MTCS SS ได้พิจารณาประเด็นควบคุมความมั่นคงต่าง ๆ จากเครื่องมือ Cloud Controls Matrix ของ CSA<br>6) NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations<br>7) แม้ NIST 800-53 จะเป็นมาตรฐานของสหรัฐฯ แต่ MTCS SS ก็ได้นำบางข้อกำหนดมาประยุกต์ใช้ด้วย | - อ้างอิงจากแนวปฏิบัติของ ISACA ในส่วนนโยบายและแนวทางการรักษาความมั่นคงปลอดภัย<br>2) NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing<br>- อ้างอิงจาก NIST SP 800-53 และ NIST SP 800-37 Rev.2 ในการนำแนวปฏิบัติมาประยุกต์ใช้กับ Coud Computing<br>- อ้างอิงจากมาตรฐาน ISO/IEC 27017 และ 27018 สำหรับแนวทางด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคลบนคลาวด์<br>- อ้างอิงจากแนวปฏิบัติขององค์กรมาตรฐานต่าง ๆ เช่น CSA, ENISA, ISACA ในประเด็นที่เกี่ยวข้องกับคลาวด์ | 2) NIST Special Publications : เอกสารพิเศษของ National Institute of Standards and Technology (NIST), สหรัฐอเมริกา<br>■ เอกสาร ISM (Information Security Manual) ฉบับล่าสุดของรัฐบาลออสเตรเลีย (กันยายน 2022) จะพบรายละเอียดการอ้างอิงจาก NIST SP 800-53 ดังนี้ :<br>○ ในภาคผนวก 2 (Annex 2) หัวข้อ "Cross-reference of controls to other sources"<br>➢ มีการระบุว่าการควบคุมบางข้อใน ISM ได้อ้างอิงมาจากการควบคุมใน NIST SP 800-53 Rev.5<br>○ ตัวอย่างการอ้างอิงที่ระบุไว้ ได้แก่ :<br>➢ Control 0814 "Personnel Screening" อ้างอิงจาก NIST 800-53 Rev.5 Control PS-3<br>➢ Control 1372 "Remote Access" อ้างอิงจาก NIST 800-53 Rev.5 Control AC-17<br>➢ Control 1399 "Access Restrictions to Privileged Accounts" อ้างอิงจาก NIST 800-53 Rev.5 Control AC-6(7)<br>○ นอกจากนี้ภาคผนวก 2 ยังระบุว่า ISM ได้นำหลักการและแนวคิดบางส่วนจาก NIST SP 800-53 มาประยุกต์ใช้ด้วย โดยไม่ได้ระบุข้อควบคุมที่อ้างอิงโดยตรง<br>➢ รวมถึงอ้างอิง NIST SP 800-37 ในการบริหารจัดการความเสี่ยง<br>3) มาตรฐานระดับชาติของออสเตรเลีย : | ขั้นตอนปฏิบัติด้านการควบคุมจาก ISO 27002 มาประยุกต์ใช้<br>2) NIST Special Publications<br>➢ มีการอ้างอิงบางส่วนจาก NIST SP 800-144 เรื่องแนวทางความมั่นคงปลอดภัยสำหรับ Cloud Computing สาธารณะ<br>➢ รวมถึงอ้างอิงบางประเด็นจาก NIST SP 800-53 ส่วนของการควบคุมด้านความปลอดภัย<br>3) มาตรฐานอื่น ๆ<br>➢ Cloud Controls Matrix จาก Cloud Security Alliance (CSA)<br>➢ Agile development lifecycle และ DevSecOps |

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| | | | ➢ อ้างอิงมาตรฐาน Australian Government Information Security Manual (AG ISM) ซึ่งเป็นมาตรฐานเฉพาะของออสเตรเลีย | |
| **อ้างอิง** | 1) จากเอกสาร "MTCS Certification Requirements (Release 3)" หน้า 6 ระบุว่า :<br>"The MTCS Standard takes reference from industry Cloud security standards such as ISO/IEC 27017, CSA Cloud Controls Matrix and NIST SP 800-53."<br>2) ใน Frequently Asked Questions (FAQs) เกี่ยวกับ MTCS บนเว็บไซต์ของ CSA Singapore มีคำถาม :<br>"What are the standards referenced for MTCS?"<br>และคำตอบระบุว่า "The MTCS requirements are derived from recognized industry standards such as ISO 27001, ISO 27017, CSA Cloud Controls Matrix and NIST SP 800-53."<br>3) บทความจาก CSA Singapore เรื่อง "Singapore's Multi-Tier Cloud Security Standard" ระบุไว้ว่า : | 1) อ้างอิงได้จากหน้า 8 - 10 ใน NIST SP 800-53 Rev.5 [27]<br>2) อ้างอิงได้จากบทนำและเอกสารอ้างอิงใน NIST SP 800-144 [28] | 1) เอกสาร ISM ฉบับล่าสุด (Sep 2022) หน้า 6 - 7 ซึ่งมีข้อความระบุว่า :<br>"The guidance in this document is based on the Australian Government Information Security Manual (ISM), relevant standards from the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST), and guidance from other authoritative sources." [29] | 1) สามารถหาข้อมูลอ้างอิงได้จากหน้า 10 - 12 ใน Cloud Security Guidelines ฉบับปี 2019 จาก MeitY มีข้อความระบุว่า :<br>"These guidelines takes input from the international standards and best practices like ISO 27001, ISO 27002, NIST SP 800-144, NIST SP 800-53, CSA Cloud Control Matrix, Agile and DevSecOps models etc." [30] |

[27] อ้างอิง: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[28] อ้างอิง: https://csrc.nist.gov/publications/detail/sp/800-144/final

[29] อ้างอิง: Information Security Manual (September 2022) - https://www.cyber.gov.au/acsc/view-all-content/ism/ism-release-september-2022 และ Annex 2 of ISM - https://www.cyber.gov.au/acsc/view-all-content/ism/ism-release-september-2022/annex-2

[30] อ้างอิง: https://www.meity.gov.in/writereaddata/files/Guidelines-Cloud_Security.pdf

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| | "The MTCS Standard references globally recognized standards such as ISO 27001, ISO 27017, Cloud Security Alliance (CSA) Cloud Controls Matrix and NIST 800-53." | | | |
| **ข้อดี ข้อเสีย ของมาตรฐาน ที่ใช้จัดทำ** | ▪ ISO/IEC 27001<br>▪ ISO/IEC:27017<br>▪ ISO/IEC:27018<br>**ข้อดี**<br>**โครงสร้างที่ชัดเจน :** มีการกำหนดโครงสร้างและกระบวนการในการจัดการความปลอดภัยของข้อมูลอย่างเป็นระบบ<br>**การประเมินความเสี่ยง :** เน้นการประเมินและจัดการความเสี่ยง ซึ่งช่วยให้สามารถป้องกันและตอบสนองต่อภัยคุกคามได้ดี<br>**ข้อเสีย**<br>**ค่าใช้จ่ายสูง:** การนำมาใช้งานและการรักษามาตรฐานมีค่าใช้จ่ายสูง<br><br>CSA STAR :<br>**ข้อดี**<br>**ความยืดหยุ่น :** มีการรับรองหลายระดับที่สามารถปรับใช้ตามความต้องการและความสามารถขององค์กร<br>**ข้อเสีย**<br>**การประเมินซับซ้อน :** กระบวนการประเมินอาจซับซ้อนและต้องการความเชี่ยวชาญเฉพาะด้าน | ▪ ISO/IEC 27001<br>▪ ISO/IEC:27017<br>▪ ISO/IEC:27018<br>**ข้อดี**<br>**โครงสร้างที่ชัดเจน :** มีการกำหนดโครงสร้างและกระบวนการในการจัดการความปลอดภัยของข้อมูลอย่างเป็นระบบ<br>**การประเมินความเสี่ยง :** เน้นการประเมินและจัดการความเสี่ยง ซึ่งช่วยให้สามารถป้องกันและตอบสนองต่อภัยคุกคามได้ดี<br>**ข้อเสีย**<br>**ค่าใช้จ่ายสูง :** การนำมาใช้งานและการรักษามาตรฐานมีค่าใช้จ่ายสูง | ▪ ISO/IEC Series<br>**ข้อดี**<br>**โครงสร้างที่ชัดเจน :** มีการกำหนดโครงสร้างและกระบวนการในการจัดการความปลอดภัยของข้อมูลอย่างเป็นระบบ<br>**การประเมินความเสี่ยง :** เน้นการประเมินและจัดการความเสี่ยง ซึ่งช่วยให้สามารถป้องกันและตอบสนองต่อภัยคุกคามได้ดี<br>**ข้อเสีย**<br>**ค่าใช้จ่ายสูง :** การนำมาใช้งานและการรักษามาตรฐานมีค่าใช้จ่ายสูง | ▪ ISO/IEC 27017<br>**ข้อดี**<br>- ให้แนวทางปฏิบัติที่เฉพาะเจาะจงสำหรับความมั่นคงปลอดภัยบริการคลาวด์<br>- ครอบคลุมประเด็นสำคัญ เช่น การแบ่งแยกข้อมูล, การตรวจสอบการเข้าถึง, บัญชีผู้ใช้งาน เป็นต้น<br>- สอดคล้องกับ ISO/IEC 27001 ซึ่งเป็นมาตรฐานหลักด้านความมั่นคงปลอดภัยสารสนเทศ<br>**ข้อเสีย**<br>- เป็นมาตรฐานเฉพาะด้านคลาวด์ อาจต้องบูรณาการกับมาตรฐานอื่น ๆ เพื่อความครอบคลุม<br>- ต้องใช้ความรู้และประสบการณ์เฉพาะในการนำไปประยุกต์ใช้<br><br>ISO/IEC 27018<br>**ข้อดี**<br>- มุ่งเน้นการคุ้มครองข้อมูลส่วนบุคคลบนคลาวด์โดยเฉพาะ ซึ่งเป็นประเด็นสำคัญ<br>- ให้หลักการและแนวทางปฏิบัติที่เป็นรูปธรรมในการจัดการข้อมูลส่วนบุคคลบนคลาวด์<br>**ข้อเสีย**<br>- เป็นมาตรฐานเฉพาะด้านเพียงด้านเดียว อาจต้องใช้ร่วมกับมาตรฐานอื่น ๆ<br>- จำเป็นต้องมีความเข้าใจที่ดีเกี่ยวกับคลาวด์และการจัดการข้อมูลส่วนบุคคล |

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| | NIST SP 800-53 :<br>**ข้อดี**<br>**การปรับใช้ทั่วโลก :** ใช้กันอย่างแพร่หลายทั่วโลกและเป็นที่ยอมรับในการปฏิบัติด้านความปลอดภัยไซเบอร์<br>**ข้อเสีย**<br>**การปรับใช้งาน :** การปรับใช้มาตรฐานนี้ในบริบทขององค์กรต่าง ๆ ทำได้ยาก<br><br>CIS Controls :<br>**ข้อดี**<br>**การเน้นการปฏิบัติ :** มุ่งเน้นการปฏิบัติจริงที่ช่วยเสริมสร้างความปลอดภัยได้อย่างรวดเร็ว<br>**การประเมินตัวเอง :** องค์กรสามารถใช้แนวทางในการประเมินและปรับปรุงความปลอดภัยของตนเองได้<br>**ข้อเสีย**<br>**ความครอบคลุม :** ไม่ครอบคลุมความต้องการด้านความปลอดภัยทั้งหมดในองค์กร | | | NIST SP 800-144<br>**ข้อดี**<br>- ให้แนวทางที่ละเอียดเกี่ยวกับความมั่นคงปลอดภัยและความเป็นส่วนตัวบนคลาวด์สาธารณะ<br>- มาจากหน่วยงานที่น่าเชื่อถือและเป็นที่ยอมรับในระดับสากล<br>**ข้อเสีย**<br>- มุ่งเน้นไปที่คลาวด์สาธารณะเป็นหลัก อาจไม่ครอบคลุมคลาวด์ประเภทอื่น<br>- เป็นแนวทางที่ค่อนข้างละเอียดและซับซ้อน อาจต้องใช้ผู้เชี่ยวชาญในการนำไปประยุกต์ใช้<br><br>CSA CCM<br>**ข้อดี**<br>- ครอบคลุมหลักการควบคุมความมั่นคงปลอดภัยคลาวด์ในหลายด้าน<br>- พัฒนาโดยองค์กรผู้เชี่ยวชาญด้านความปลอดภัยคลาวด์โดยตรง<br>**ข้อเสีย**<br>เป็นเพียงกรอบแนวทางเท่านั้น ไม่ใช่มาตรฐานที่เป็นทางการ อาจต้องนำมาประยุกต์ใช้ร่วมกับมาตรฐานหรือแนวปฏิบัติอื่น ๆ |
| **นโยบายของแต่ละประเทศ** | **MTCS SS (Multi-Tier Cloud Security Standard for Singapore)**<br>เป็นมาตรฐานความปลอดภัยคลาวด์ที่กำหนดขึ้นโดย Info-communications Media Development Authority (IMDA) ของสิงคโปร์แบ่งออกเป็น 3 ระดับ (Tier 1, Tier 2, Tier 3) ซึ่งครอบคลุมความต้องการด้านความปลอดภัยที่แตกต่างกันตามความสำคัญของข้อมูลและการบริการ | เนื่องจากสหรัฐอเมริกาไม่ได้มีมาตรฐานหลักในการควบคุม Cloud Security แต่มีการบังคับใช้ในองค์กรภาครัฐทั้งหมด โดยได้รับการรับรองจากโปรแกรม Federal Risk and Authorization Management Program (FedRAMP) แต่ภาคเอกชนเอง ก็นำมาตรฐานของภาครัฐไปเป็นแนวทางเพื่อยกระดับความปลอดภัยและเพิ่มความน่าเชื่อถือของบริการคลาวด์เช่นกัน โดยมาตรฐานที่องค์กรภาครัฐนำมาใช้ คือ | Information Security Manual (ISM) เป็นมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่จัดทำโดย Australian Signals Directorate (ASD) ซึ่งเป็นหน่วยงานด้านความมั่นคงปลอดภัยสารสนเทศและการสื่อสารของรัฐบาลออสเตรเลีย<br>รายละเอียดของ ISM มีดังนี้ | Ministry of Electronics and Information Technology (MeitY) ได้จัดทำ Cloud Security Guidelines เพื่อกำหนดแนวทางและข้อกำหนดด้านความปลอดภัยในการใช้บริการคลาวด์ในอินเดีย โดยนโยบายนี้มีวัตถุประสงค์เพื่อปกป้องข้อมูลและระบบที่ใช้บริการคลาวด์อย่างมีประสิทธิภาพ นโยบายหลักประกอบด้วย<br>**นโยบายหลัก**<br>1) การรักษาความปลอดภัยของข้อมูล : |

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| | | 1) NIST Special Publication 800-53 (Security and Privacy Controls for Information Systems and Organizations): มาตรฐานนี้ให้แนวทางสำหรับการจัดการความเสี่ยงและการป้องกันข้อมูลในระบบสารสนเทศ รวมถึงการใช้คลาวด์<br>2) NIST Special Publication 800-144 (SP 800-144) "Guidelines on Security and Privacy in Public Cloud Computing" เป็นเอกสารที่ให้แนวทางเกี่ยวกับความปลอดภัยและความเป็นส่วนตัวในการใช้บริการคลาวด์สาธารณะ โดยเน้นไปที่การให้คำแนะนำแก่หน่วยงานและองค์กรที่ต้องการใช้คลาวด์สาธารณะ เพื่อให้มั่นใจว่าการย้ายไปยังคลาวด์จะไม่กระทบต่อความปลอดภัยและความเป็นส่วนตัวของข้อมูล | **หน่วยงานที่กำหนด :** ISM ถูกจัดทำโดย Australian Signals Directorate (ASD) ซึ่งเป็นหน่วยงานภายใต้กระทรวงกลาโหมของออสเตรเลีย<br>**วัตถุประสงค์ :** เพื่อกำหนดแนวทาง มาตรฐาน และข้อปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศสำหรับหน่วยงานรัฐบาลออสเตรเลียและองค์กรสำคัญต่าง ๆ<br>**เนื้อหาหลัก :** ISM ครอบคลุมหลักการ แนวทางปฏิบัติ และการควบคุมด้านความมั่นคงปลอดภัยในหลายด้าน เช่น การบริหารจัดการความเสี่ยง การควบคุมการเข้าถึง การรักษาความมั่นคงปลอดภัยเครือข่าย การป้องกันไวรัสและมัลแวร์ เป็นต้น<br>**การจัดระดับความสำคัญ :** ISM แบ่งระดับความสำคัญของข้อมูลและระบบออกเป็น 4 ระดับ คือ Unclassified, Protected, Secret และ Top Secret โดยมีข้อกำหนดและการควบคุมแตกต่างกันตามระดับความลับ<br>**บังคับใช้กับหน่วยงานและองค์กร :**<br>ISM เป็นมาตรฐานบังคับสำหรับหน่วยงานของรัฐบาลออสเตรเลีย และถือเป็นแนวปฏิบัติที่แนะนำสำหรับองค์กรภายนอกที่ต้องการรักษาความปลอดภัยในระดับสูง<br>**การปรับปรุงอย่างต่อเนื่อง :** ASD มีการทบทวนและปรับปรุง ISM อย่างสม่ำเสมอ เพื่อให้ทันสมัยและสอดคล้องกับภัยคุกคามและเทคโนโลยีใหม่ ๆ โดยมีการออกเวอร์ชันใหม่ทุกปี<br>ISM ถือเป็นมาตรฐานสำคัญที่ช่วยสร้างกรอบการรักษาความมั่นคงปลอดภัยสารสนเทศในระดับสูงให้กับออสเตรเลีย และส่งผลให้เกิดการยกระดับความปลอดภัยในหน่วยงานภาครัฐและองค์กรต่าง ๆ ด้วย | - ข้อมูลที่จัดเก็บและประมวลผลบนคลาวด์ต้องได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาตและการละเมิดความปลอดภัย<br>- มีการกำหนดมาตรการในการเข้ารหัสข้อมูลทั้งในระหว่างการส่งผ่านและขณะจัดเก็บ<br>2) การประเมินและจัดการความเสี่ยง : ทุกองค์กรต้องดำเนินการประเมินความเสี่ยงที่เกี่ยวข้องกับการใช้บริการคลาวด์<br>- มาตรการความปลอดภัยต้องถูกปรับปรุงอย่างสม่ำเสมอเพื่อลดความเสี่ยงที่อาจเกิดขึ้น<br>3) การควบคุมการเข้าถึง :<br>- มีการกำหนดนโยบายการควบคุมการเข้าถึงข้อมูลและทรัพยากรในคลาวด์อย่างเข้มงวด<br>- การใช้การตรวจสอบสิทธิ์หลายปัจจัย (Multi-Factor Authentication) และการควบคุมการเข้าถึงตามบทบาท (Role-Based Access Control)<br>4) การปฏิบัติตามกฎหมายและข้อบังคับ :<br>- องค์กรต้องปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและความเป็นส่วนตัว เช่น ข้อกำหนดของ ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, และแนวทางของ NIST<br>5) การตรวจสอบและการรายงาน :<br>- มีการตรวจสอบและการรายงานความปลอดภัยอย่างสม่ำเสมอ เพื่อให้แน่ใจว่าระบบมีความปลอดภัยและสามารถปรับตัวต่อภัยคุกคามใหม่ ๆ ได้<br>6) การจัดการเหตุการณ์ความปลอดภัย :<br>- องค์กรต้องมีแผนการตอบสนองและจัดการกับเหตุการณ์ความปลอดภัยอย่างมีประสิทธิภาพ |

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| | | | | - การฟื้นฟูสภาพการทำงานหลังเกิดเหตุการณ์ต้องเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ |
| **อ้างอิง** | MTCS SS 584 | NIST 800-53<br>NIST 800-144 | Information Security Manual | Cloud Security Best Practice |
| **ข้อดี ข้อด้อยของมาตรฐาน Cloud Security** | **ข้อดี**<br>1) มีความครอบคลุมถึงข้อกำหนดที่จำเป็นต่อความมั่นคงปลอดภัยของข้อมูลในหลาย ๆ หัวข้อ เช่น<br>1) การบริหารจัดการทรัพยากรบุคคล<br>- 7.3.1 ข้อกำหนดด้านความปลอดภัยกับบุคลากรก่อนจ้างงาน ในระหว่างจ้างและเมื่อสิ้นสุดการจ้าง<br>- 7.3.2 ข้อปฏิบัติและความรับผิดชอบด้านความปลอดภัยของบุคลากร<br>- 7.3.3 การฝึกอบรมและการให้ความรู้ด้านความปลอดภัยแก่บุคลากร<br>2) การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย<br>- 12.2.1 ขั้นตอนและแนวทางปฏิบัติในการจัดการและแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย<br>- 12.2.2 การบันทึก รวบรวม และวิเคราะห์เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย<br>3) การรักษาความปลอดภัยของสารสนเทศในกระบวนการจัดหาและ Supply Chain<br>- 11.1.1 นโยบายรักษาความปลอดภัยของระบบสารสนเทศในการจัดหาระบบ/ซอฟต์แวร์ | **มาตรฐาน NIST SP 800 - 53 Rev.5 Security and Privacy Controls for Information Systems and Organizations**<br>**ข้อดี**<br>1) ครอบคลุมการควบคุมที่ครบถ้วนและละเอียด โดยมาตรฐานประกอบด้วยแนวควบคุมหลัก 20 ด้าน แบ่งย่อยเป็น 265 แนวควบคุม เช่น แนวควบคุมด้านการเข้ารหัสข้อมูล (Cryptography) การบริหารจัดการโครงสร้างพื้นฐาน (System and Communications Protection) เป็นต้น<br>2) ให้คำนิยามและข้อกำหนดที่ชัดเจนสำหรับแต่ละแนวควบคุม เช่น แนวควบคุม IA-5 Authenticator Management ให้คำนิยามชัดเจนของ "Authenticator" และระบุข้อกำหนดในการบริหารจัดการอย่างละเอียด เป็นต้น<br>3) มีเอกสารประกอบสำหรับประเด็นเฉพาะทาง ตัวอย่าง : มี Appendix ประกอบ เช่น วิธีปฏิบัติในการจัดทำ System Security Plan หรือวิธีการประเมินความเสี่ยง<br>**ข้อด้อย**<br>1. มีความซับซ้อนและรายละเอียดมาก ทำให้ยากต่อการทำความเข้าใจและปฏิบัติตาม ตัวอย่าง : เอกสาร Rev.5 มีความยาวกว่า 460 หน้ากระดาษ A4 มีแนวควบคุมรวมทั้งสิ้น 265 ข้อ นอกจากนี้ยังมีเอกสารสนับสนุนอีกหลายฉบับ | **ข้อดี**<br>- ISM และแนวทางของ ACSC มีมาตรฐานที่เข้มงวดและชัดเจน ทำให้หน่วยงานสามารถปฏิบัติตามได้อย่างมั่นใจในเรื่องความปลอดภัย<br>- ISM เน้นหนักในเรื่องการบริหารความเสี่ยง โดยอ้างอิงจากมาตรฐาน ISO/IEC 27005, ISO/IEC 31000 Series รวมถึง NIST 800-30, 37 ทำให้มีความปลอดภัยและมีความยืดหยุ่น<br>- มีการสนับสนุนจากรัฐบาลในการพัฒนาและปรับปรุงมาตรฐานและแนวทางต่าง ๆ เพื่อให้ทันสมัยและสอดคล้องกับภัยคุกคามใหม่ ๆ<br>**ข้อด้อย**<br>- เป็นแนวทางในการจัดการกับ Cloud ของรัฐบาลเท่านั้น ทำให้การเข้าถึงข้อมูลและแนวทางบางส่วนอาจมีข้อจำกัด โดยเฉพาะสำหรับองค์กรที่ไม่ใช่หน่วยงานของรัฐบาล เช่น แนวทางที่เกี่ยวข้องกับการจัดการและป้องกันข้อมูลลับ ของรัฐบาลอาจมีข้อจำกัดในการเผยแพร่ เนื่องจากมีความสำคัญสูงและต้องการการป้องกันที่เข้มงวด<br>- เป็นมาตรฐานทางเทคนิคที่อาจมีความซับซ้อนสำหรับบางองค์กร โดยเฉพาะองค์กรขนาดเล็กที่มีทรัพยากรจำกัด<br>- มาตรฐานเน้นที่ความมั่นคงปลอดภัยเป็นสำคัญ อาจส่งผลกระทบต่อประสิทธิภาพและความสะดวกในการใช้งาน | **ข้อดี**<br>- เป็นแนวทางที่ครอบคลุมประเด็นสำคัญด้านความมั่นคงปลอดภัยคลาวด์ ทั้งด้านการบริหารจัดการสิทธิ์, การเข้ารหัสข้อมูล, บล็อกเชน และอื่น ๆ<br>- ให้กรอบมาตรฐานในการประเมินความเสี่ยงและควบคุมความมั่นคงปลอดภัยคลาวด์ที่เป็นระบบ<br>- ส่งเสริมให้นำระบบและมาตรฐานสากลด้านความมั่นคงปลอดภัย เช่น ISO 27001, NIST มาประยุกต์ใช้<br>- เปิดโอกาสให้ภาคเอกชนนำไปใช้เพื่อสร้างความน่าเชื่อถือในการบริการคลาวด์<br>**ข้อด้อย**<br>- มาตรฐานมีความซับซ้อนและรายละเอียดสูง โดยเฉพาะต้องจัดทำและบำรุงรักษาระบบการเข้ารหัสข้อมูลที่ซับซ้อนและต้องการผู้เชี่ยวชาญในการดำเนินการ เช่น มีการกำหนดให้มีการเข้ารหัสทั้งกระบวนการ ไม่ว่าจะเป็น Data in Transit, Data at Rest, Data in used และ End to end encryption ซึ่งยากในการปฏิบัติจริง |

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| | - 11.1.2 กระบวนการตรวจสอบความปลอดภัยสำหรับการจัดหาระบบ/ซอฟต์แวร์ตามนโยบาย<br>2) มาตรฐาน MTCS SS มีความยืดหยุ่นในการดำเนินการ โดยที่มีการกำหนดระดับความปลอดภัยที่แตกต่างกันตามระดับความเสี่ยงของข้อมูล มีทั้งหมด 4 ระดับ ดังนี้ :<br>- ระดับ 1 : ข้อมูลสาธารณะ<br>- ระดับ 2 : ข้อมูลที่ไม่ละเอียดอ่อน<br>- ระดับ 3 : ข้อมูลละเอียดอ่อน<br>- ระดับ 4 : ข้อมูลลับ<br>ซึ่งข้อกำหนดในแต่ละระดับจะมีความเข้มงวดและรายละเอียดที่แตกต่างกัน เพื่อให้เหมาะสมกับความเสี่ยงของข้อมูล<br>- ตัวอย่างข้อกำหนดที่แสดงถึงความยืดหยุ่น :<br><br>**การควบคุมการเข้าถึง**<br>- ระดับ 2 : 7.1.1 การจัดการสิทธิ์การเข้าถึงของผู้ใช้<br>- ระดับ 4 : 7.1.5 การควบคุมการเข้าถึงข้อมูลและระบบแอปพลิเคชันอย่างเหมาะสม<br><br>**การตรวจสอบและบันทึกเหตุการณ์**<br>- ระดับ 2 : 6.5.1 ต้องมีการดำเนินการเกี่ยวกับกระบวนการตรวจสอบ<br>- ระดับ 4 : 6.5.3 ต้องมีการจัดเก็บข้อมูลบันทึกเหตุการณ์อย่างเหมาะสม<br>ดังนั้น องค์กรสามารถเลือกระดับความปลอดภัยที่เหมาะสมกับความเสี่ยงของข้อมูลและ | 2. การปฏิบัติตามข้อกำหนดอาจมีค่าใช้จ่ายสูง ตัวอย่าง : การปรับปรุงระบบ กระบวนการ และนโยบายต่าง ๆ ให้สอดคล้องกับมาตรฐานอาจต้องใช้งบประมาณสูง<br><br>**มาตรฐาน NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing**<br>**<u>ข้อดี</u>**<br>1. ให้ภาพรวมของประเด็นความมั่นคงปลอดภัยในการใช้งานคลาวด์สาธารณะ ตัวอย่าง : อธิบายภาพรวมของการบริหารจัดการความเสี่ยงในการใช้บริการคลาวด์ สาธารณะ ตั้งแต่กระบวนการตัดสินใจ จนถึงการดำเนินการระหว่างการใช้บริการ<br>2. ครอบคลุมประเด็นทั้งมุมมองของผู้ให้บริการและผู้ใช้บริการ ตัวอย่าง : แนะนำถึงกิจกรรมที่ผู้ให้บริการควรดำเนินการ เช่น การประเมินความเสี่ยง และแนวทางสำหรับผู้ใช้บริการในการตรวจสอบผู้ให้บริการ<br>3. มีการอ้างอิงมาตรฐานอื่น ๆ ที่เกี่ยวข้อง ตัวอย่าง : มีการอ้างอิงถึงมาตรฐาน NIST SP 800-53, NIST SP 800-37 และเอกสารอื่น ๆ ที่สามารถนำไปใช้ประกอบได้<br>**<u>ข้อด้อย</u>**<br>1) มุ่งเน้นการใช้งานคลาวด์สาธารณะเป็นหลัก ตัวอย่าง : อาจไม่ครอบคลุมประเด็นทั้งหมดสำหรับคลาวด์ประเภทอื่น เช่น Private Cloud, Hybrid Cloud<br>2) เป็นเพียงแนวทางทั่วไป ไม่ได้ให้รายละเอียดปฏิบัติที่ชัดเจน ตัวอย่าง : แนะนำให้ตรวจสอบ | | |

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| | ระบบงานของตนได้ ช่วยให้การปฏิบัติตามมาตรฐานมีความยืดหยุ่นและเหมาะสมมากขึ้น<br>**<u>ข้อด้อย</u>**<br>แม้มาตรฐาน MTCS SS จะมีข้อดีหลายประการ แต่ก็มีข้อด้อยบางประการที่ควรพิจารณา เช่น :<br>1) ความซับซ้อน ตัวอย่างข้อกำหนด : 7.4 การป้องกันการรั่วไหลของข้อมูล มีรายละเอียดซับซ้อน เช่น 7.4.1 -7.4.6 กำหนดมาตรการต่าง ๆ ทำให้ยากต่อการปฏิบัติตาม<br>2) ค่าใช้จ่าย ตัวอย่างข้อกำหนด : 9.5 การเฝ้าระวังการคุกคามและเหตุการณ์ด้านความปลอดภัย ต้องมีระบบเฝ้าระวังตลอด 24 ช.ม. ต้องใช้ทรัพยากรและระบบที่มีค่าใช้จ่ายสูง<br>3) ความท้าทายในการตีความ ตัวอย่างข้อกำหนด : 8.6 การพัฒนาซอฟต์แวร์ที่ปลอดภัย การกำหนด "ปลอดภัย" มีความหมายค่อนข้างกว้าง ทำให้ยากในการตีความ | คุณสมบัติด้านความมั่นคงปลอดภัยของผู้ให้บริการ แต่ไม่ได้ระบุรายการตรวจสอบที่ชัดเจน | | |
| **อ้างอิง** | ➢ แหล่งอ้างอิงสำหรับข้อกำหนดต่าง ๆ ที่ยกมาจากเอกสาร "Multi - Tier Cloud Security Standard for Singapore (MTCS SS)" ฉบับล่าสุด (Release 3.0 ณ เดือนมกราคม 2563) โดยมีดังนี้[31]<br>1) การบริหารจัดการทรัพยากรบุคคล<br>▪ 7.3.1 หน้า 37<br>▪ 7.3.2 หน้า 38<br>▪ 7.3.3 หน้า 38 | NIST Special Publication 800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations,"<br>➢ <u>NIST SP 800-53 Rev. 5 (PDF)</u><br>NIST Special Publication 800-144, "Guidelines on Security and Privacy in Public Cloud Computing,"<br>➢ <u>NIST SP 800-144 PDF</u><br>➢ <u>NIST Publication Overview</u> | Australian Cyber Security Centre (ACSC) Information Security Manual (ISM)<br>➢ <u>ACSC Information Security Manual (Amazon Web Services (AWS) Docs)</u><br>➢ Direct access to the manual is restricted, so the reference is using the Amazon instead | แนวปฏิบัติว่าด้วยความมั่นคงปลอดภัยบนคลาวด์สำหรับรัฐบาลอินเดีย (Cloud Computing Security Guidelines for Government of India) โดยกระทรวงอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศ (Ministry of Electronics & Information Technology) [32] |

[31] อ้างอิง: ลิ้งค์เอกสาร MTCS SS: https://www.singaporestandardseshop.sg/Product/GetPdf?fileName=201029155934SS%20584-2020%20Preview.pdf&pdtid=b5430dc1-27f3-4203-bd8e-00345da6bed5

[32] อ้างอิง: ลิ้งค์เอกสาร https://www.meity.gov.in/writereaddata/files/cloud_security_guidelines_14_oct21.pdf

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| | 2) การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย<br>▪ 12.2.1 หน้า 58<br>▪ 12.2.2 หน้า 58<br>3) การรักษาความปลอดภัยในกระบวนการจัดหาและซัพพลายเชน<br>▪ 11.1.1 หน้า 53<br>▪ 11.1.2 หน้า 53 | | | |
| **การแบ่งประเภทตามขนาดของหน่วยงาน** | **ก) องค์กรขนาดเล็ก (Small Organisations)**<br>จำนวนพนักงาน : น้อยกว่า 50 คน<br>รายได้ต่อปี : ต่ำกว่า 10 ล้านดอลลาร์สิงคโปร์<br>ความต้องการ : ความปลอดภัยของข้อมูลที่มีขนาดเล็กและการบริหารจัดการที่ง่าย<br>แนวทาง : ใช้บริการคลาวด์สาธารณะที่มีมาตรฐานความปลอดภัยระดับพื้นฐานและมีค่าใช้จ่ายที่เหมาะสม<br><br>**ข) องค์กรขนาดกลาง (Medium Organisations) :**<br>จำนวนพนักงาน : 50-200 คน<br>รายได้ต่อปี : 10-50 ล้านดอลลาร์สิงคโปร์<br>ความต้องการ : ความปลอดภัยของข้อมูลที่ซับซ้อนมากขึ้นและการบริหารจัดการที่เป็นระบบ<br>แนวทาง : ใช้บริการคลาวด์สาธารณะหรือคลาวด์ส่วนตัวที่มีมาตรฐานความปลอดภัยสูงขึ้น และมีการตรวจสอบความปลอดภัยอย่างสม่ำเสมอ | มาตรฐานของ NIST ไม่ได้แบ่งการควบคุมตามขนาดขององค์กร แต่ใช้วิธีการแบ่งการควบคุมตามระดับของความเสี่ยงที่ระบบขององค์กรต้องเผชิญ | ISM ไม่ได้แบ่งประเภทตามขนาดของหน่วยงานโดยตรง แต่มีการกำหนดมาตรการและข้อกำหนดที่สามารถปรับใช้ได้ตามขนาดและประเภทขององค์กร โดยมีการแนะนำให้หน่วยงานประเมินความเสี่ยงและเลือกใช้มาตรการที่เหมาะสมกับขนาดและลักษณะขององค์กรตนเอง | ตามที่ได้ศึกษาเอกสาร "Cloud Security Baseline" ของอินเดียฉบับล่าสุด (เวอร์ชัน 1.0 เผยแพร่เมื่อเดือนกันยายน 2563) พบว่ายังไม่มีการระบุการแบ่งประเภทองค์กรตามขนาดไว้อย่างชัดเจน<br><br>อย่างไรก็ตาม เอกสารดังกล่าวได้ให้ข้อแนะนำที่สำคัญว่าหน่วยงานควรปรับใช้แนวปฏิบัตินี้ให้เหมาะสมกับ :<br>▪ ขนาดและความซับซ้อนขององค์กร<br>▪ บริบททางธุรกิจและความเสี่ยงที่องค์กรเผชิญ<br>▪ ประเภทของระบบสารสนเทศและบริการคลาวด์ที่องค์กรใช้งาน<br>นอกจากนี้ ยังระบุว่าหน่วยงานอาจต้องปรับเพิ่มเติมมาตรการความมั่นคงปลอดภัยตามความเหมาะสม หากมีข้อกำหนดเฉพาะทางกฎหมายหรือกฎระเบียบที่ต้องปฏิบัติตาม<br>ดังนั้น แม้จะไม่ได้ระบุการแบ่งประเภทตามขนาดองค์กรไว้โดยตรง แต่แนวปฏิบัตินี้ก็ได้เปิดช่องให้องค์กรสามารถปรับใช้ได้ตามความเหมาะสมกับบริบทและขนาดขององค์กร |

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| | **ค) องค์กรขนาดใหญ่ (Large Organizations) :**<br>จำนวนพนักงาน : มากกว่า 200 คน<br>รายได้ต่อปี : มากกว่า 50 ล้านดอลลาร์สิงคโปร์<br>ความต้องการ : ความปลอดภัยของข้อมูลที่มีความสำคัญมากและการบริหารจัดการที่มีความซับซ้อนสูง<br>แนวทาง : ใช้บริการคลาวด์ส่วนตัวหรือคลาวด์ไฮบริดที่มีมาตรฐานความปลอดภัยสูงสุด และมีการกำกับดูแลและตรวจสอบความปลอดภัยอย่างเข้มงวด | | | |
| **อ้างอิง** | Specification for multi - tiered cloud computing security[33] | NIST Special Publication 800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations,"<br>▪ NIST SP 800-53 Rev. 5 (PDF)<br>NIST Special Publication 800-144, "Guidelines on Security and Privacy in Public Cloud Computing,"<br>▪ NIST SP 800-144 PDF<br>▪ NIST Publication Overview | Australian Cyber Security Centre (ACSC) Information Security Manual (ISM)<br>*ACSC Information Security Manual (Amazon Web Services (AWS) Docs)<br>* Direct access to the manual is restricted, so the reference is using the Amazon instead | แนวปฏิบัติว่าด้วยความมั่นคงปลอดภัยบนคลาวด์สำหรับรัฐบาลอินเดีย (Cloud Computing Security Guidelines for Government of India) โดยกระทรวงอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศ (Ministry of Electronics & Information Technology) [34] |
| **การรับรองมาตรฐาน** | การรับรองมาตรฐาน SS 584 (Multi-Tier Cloud Security Standard)<br>1. **ความพร้อมขององค์กร** : องค์กรเอกชนที่เป็นผู้ให้บริการคลาวด์สามารถขอการรับรองมาตรฐาน SS 584 ได้ | การรับรองมาตรฐาน FedRAMP (Federal Risk and Authorization Management Program)<br>1. **ความพร้อมขององค์กร :** องค์กรเอกชนที่เป็นผู้ให้บริการคลาวด์สามารถขอการรับรองมาตรฐาน FedRAMP ได้ โดยเฉพาะอย่างยิ่งหากต้องการให้บริการแก่หน่วยงานรัฐบาลสหรัฐ | มาตรฐาน Information Security Manual (ISM) ของออสเตรเลียเป็นเอกสารแนวทางที่จัดทำโดย Australian Cyber Security Centre (ACSC) เพื่อให้คำแนะนำเกี่ยวกับการจัดการและการป้องกันภัยคุกคามทางไซเบอร์ในองค์กร ไม่ได้เป็นมาตรฐานที่ต้องผ่านการรับรองโดยตรงเหมือนกับมาตรฐานอื่น ๆ | Cloud Security Baseline ของ Ministry of Electronics and Information Technology (MeitY) ประเทศอินเดีย เป็นชุดของแนวทางปฏิบัติที่แนะนำสำหรับการรักษาความปลอดภัยของบริการคลาวด์ ซึ่งได้รับการพัฒนาเพื่อให้มั่นใจว่าบริการคลาวด์ที่ใช้งานในประเทศอินเดียมีความปลอดภัยเพียงพอ อย่างไรก็ตาม Cloud Security Baseline ของ MeitY ไม่ได้กำหนดให้ |

[33] อ้างอิง: https://www.singaporestandardseshop.sg/Product/GetPdf?fileName=201029155934SS%20584-2020%20Preview.pdf&pdtid=b5430dc1-27f3-4203-bd8e-00345da6bed5

[34] อ้างอิง: เอกสาร https://www.meity.gov.in/writereaddata/files/cloud_security_guidelines_14_oct21.pdf

| หัวข้อ | สิงคโปร์ | อเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|---|
| | 2. **กระบวนการรับรอง :**<br>• **การเตรียมตัวและการตรวจสอบภายใน** : องค์กรต้องเตรียมตัวและดำเนินการตรวจสอบภายในเพื่อให้มั่นใจว่าระบบความปลอดภัยของตนเป็นไปตามข้อกำหนดของมาตรฐาน SS 584<br>• **การตรวจสอบจากหน่วยงานรับรอง :** ติดต่อหน่วยงานรับรองที่ได้รับการรับรองจาก Singapore Accreditation Council (SAC) เพื่อขอการตรวจสอบและรับรอง<br>• **การออกใบรับรอง :** เมื่อผ่านการตรวจสอบ องค์กรจะได้รับใบรับรอง SS 584 จากหน่วยงานรับรอง | 2. **กระบวนการรับรอง :**<br>• **การหาหน่วยงานสนับสนุน (Sponsoring Agency) :** องค์กรต้องหาหน่วยงานรัฐบาลสหรัฐที่พร้อมจะสนับสนุนการขอการรับรอง FedRAMP<br>• **การเตรียมเอกสารระบบความปลอดภัย (System Security Plan, SSP) :** จัดทำ SSP และเอกสารที่เกี่ยวข้องตามข้อกำหนดของ FedRAMP<br>• **การประเมินโดยผู้ตรวจสอบที่สาม (Third - Party Assessment Organization, 3PAO) :** ติดต่อ 3PAO ที่ได้รับการรับรองจาก FedRAMP เพื่อดำเนินการประเมินระบบความปลอดภัย<br>• **การอนุมัติจากหน่วยงานสนับสนุนหรือ JAB :** ผลการประเมินจะถูกส่งไปยังหน่วยงานสนับสนุนหรือ Joint Authorization Board (JAB) เพื่อการตรวจสอบและอนุมัติ<br>• **การออกใบรับรอง :** หากผ่านการตรวจสอบ องค์กรจะได้รับการรับรองมาตรฐาน FedRAMP | เช่น ISO 27001 แต่เป็นการแนะนำแนวทางและวิธีปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัยทางไซเบอร์ | ต้องมีการรับรองอย่างเป็นทางการเหมือนมาตรฐานอื่น ๆ เช่น ISO 27001 หรือ FedRAMP |

# บทที่ 3 การวิเคราะห์เปรียบเทียบนโยบาย

## 3.1 การเปรียบเทียบกฎหมายที่เกี่ยวข้องกับผู้ให้บริการ Cloud (Cloud Service Provider: CSP)

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| **1. Multi-Tier Cloud Security (MTCS)**<br>เป็นมาตรฐานแรกของโลกที่ครอบคลุมความมั่นคงปลอดภัยของบริการคลาวด์ในหลายระดับ ได้รับการออกแบบมาเพื่อให้สอดคล้องกับกฎหมายและระเบียบ ข้อบังคับต่าง ๆ ของสิงคโปร์ โดยเฉพาะในเรื่องของการปกป้องข้อมูลและความมั่นคงปลอดภัยทางไซเบอร์ กฎหมายที่เกี่ยวข้องกับ MTCS ของสิงคโปร์ ได้แก่<br>**1.1) Personal Data Protection Act (PDPA)**<br>▪ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) เป็นกฎหมายหลักที่ใช้ในการปกป้องข้อมูลส่วนบุคคลของสิงคโปร์ กำหนดให้ผู้ให้บริการคลาวด์ต้องมีมาตรการที่เหมาะสมในการปกป้องข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม, ใช้งาน, หรือเปิดเผยผ่านบริการคลาวด์ MTCS ช่วยให้ผู้ให้บริการคลาวด์สามารถปฏิบัติตามข้อกำหนดของ PDPA ได้โดยการกำหนดมาตรการควบคุมความปลอดภัยที่เหมาะสมตามระดับของการให้บริการ [35] | **1. NIST SP 800-53 : Security and Privacy Controls for Information Systems and Organizations**<br>เป็นมาตรฐานที่ให้แนวทางในการจัดการและป้องกันความมั่นคงปลอดภัยของระบบสารสนเทศและองค์กร กฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องกับมาตรฐานนี้ ได้แก่<br>**1.1) Federal Information Security Modernization Act (FISMA)**<br>▪ พระราชบัญญัตินี้กำหนดให้องค์กรของรัฐบาลกลางต้องมีการป้องกันและจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศตามแนวทางของ NIST SP 800-53 โดยมีการตรวจสอบและรายงานผลการปฏิบัติให้สอดคล้องกับข้อกำหนดที่กำหนด[40]<br>**1.2) Privacy Act of 1974**<br>▪ พระราชบัญญัตินี้กำหนดให้องค์กรต้องปกป้องข้อมูลส่วนบุคคลของพลเมืองอเมริกันที่ถูกเก็บรวบรวมในระบบสารสนเทศ โดย NIST SP | **1. มาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Manual - ISM)**<br>กำกับดูแลโดยกฎหมายและระเบียบข้อบังคับ ได้แก่<br>**1.1) Privacy Act 1988**<br>▪ กฎหมายคุ้มครองข้อมูลส่วนบุคคล กำหนดหลักเกณฑ์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล [48]<br>**1.2) พระราชบัญญัติความมั่นคงของโครงสร้างพื้นฐานที่สำคัญ ค.ศ. 2018 (Security of Critical Infrastructure Act 2018)**<br>▪ บริหารจัดการความเสี่ยงด้านความมั่นคงของโครงสร้างพื้นฐานที่สำคัญ [49] | **1. กระทรวงอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศ (Ministry of Electronics and Information Technology หรือ MeitY)**<br>มีบทบาทในการกำหนดมาตรฐานและกฎระเบียบต่าง ๆ สำหรับผู้ให้บริการคลาวด์ (Cloud Service Provider) โดยมีกฎหมายและมาตรฐานที่สำคัญ ได้แก่<br>**1.1) Information Technology Act, 2000 และ (Amendments) Rules**<br>▪ เป็นกฎหมายหลักที่กำกับดูแลเทคโนโลยีสารสนเทศในอินเดีย รวมถึงการให้บริการคลาวด์ [50]<br>**1.2) Cloud Computing Empanelment and Future Skilling Requirements**<br>▪ มาตรฐานและข้อกำหนดสำหรับการจดทะเบียนผู้ให้บริการคลาวด์ภายใต้ MeitY [51] |

[35] อ้างอิง: ida_mtcs-x-cert---implementation-guideline-report_mtcs-to-iso270012013_release.pdf (imda.gov.sg)

[40] อ้างอิง: Federal Information Security Modernization Act (FISMA) | CMS Information Security & Privacy Group

[48] อ้างอิง: https://www.oaic.gov.au/privacy/the-privacy-act

[49] อ้างอิง: Security of Critical Infrastructure Act 2018 (SOCI) (cisc.gov.au)

[50] อ้างอิง: https://www.meity.gov.in/content/information-technology-act-2000

[51] อ้างอิง: https://www.meity.gov.in/writereaddata/files/cloudcomputingempanelment.pdf

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| **1.2) Cybersecurity Act**<br>▪ พระราชบัญญัติความมั่นคงทางไซเบอร์ของสิงคโปร์กำหนดกรอบการทำงานสำหรับการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ MTCS ช่วยให้ผู้ให้บริการคลาวด์ สามารถปฏิบัติตามข้อกำหนดของพระราชบัญญัตินี้ได้โดยการกำหนดมาตรการควบคุมความปลอดภัยที่เข้มงวดและการตรวจสอบความปลอดภัยอย่างสม่ำเสมอ [36]<br><br>**1.3) Electronic Transactions Act (ETA)**<br>▪ พระราชบัญญัติการทำธุรกรรมทางอิเล็กทรอนิกส์ (ETA) กำหนดกรอบการทำงานสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างปลอดภัย MTCS ช่วยให้ผู้ให้บริการคลาวด์สามารถปฏิบัติตามข้อกำหนดของ ETA ได้โดยการกำหนดมาตรการควบคุมที่เข้มงวดสำหรับการ | 800-53 ให้แนวทางในการจัดการและปกป้องข้อมูลส่วนบุคคลเหล่านี้ [41]<br><br>**1.3) Health Insurance Portability and Accountability Act (HIPAA)**<br>▪ พระราชบัญญัติ HIPAA กำหนดให้หน่วยงานที่เกี่ยวข้องกับข้อมูลสุขภาพต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยของข้อมูลสุขภาพ NIST SP 800-53 ให้แนวทางในการป้องกันและรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพ [42]<br><br>**1.4) Federal Risk and Authorization Management Program (FedRAMP)**<br>▪ โปรแกรมนี้กำหนดให้องค์กรของรัฐบาลกลางที่ใช้บริการคลาวด์ต้องปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยของ NIST SP 800-53 เพื่อให้มั่นใจว่าบริการคลาวด์มีความปลอดภัย [43]<br><br>**2. NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing** | | **1.3) Guidelines for Government Departments on Contractual Terms Related to Cloud Services**<br>▪ แนวทางสำหรับหน่วยงานรัฐในการทำสัญญากับผู้ให้บริการคลาวด์ [52]<br><br>**1.4) National Cyber Security Policy, 2013**<br>▪ นโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่ครอบคลุมถึงการให้บริการคลาวด์ [53]<br><br>**1.5) Data Protection Bill, 2021 (ร่างกฎหมาย)**<br>▪ ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่จะมีผลต่อผู้ให้บริการคลาวด์เมื่อมีผลบังคับใช้ [54] |

[36] อ้างอิง: https://sso.agc.gov.sg/Act-Rev/CA2018/Published/20211231?DocDate=20211231&ViewType=Pdf&_=20230508142246

[41] อ้างอิง: The Privacy Act of 1974 – EPIC – Electronic Privacy Information Center

[42] อ้างอิง: HIPAA for Professionals | HHS.gov

[43] อ้างอิง: Federal Risk and Authorization Management Program (FedRAMP) | CMS Information Security & Privacy Group

[52] อ้างอิง:https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf

[53] อ้างอิง: https://www.meity.gov.in/writereaddata/files/National_cyber_security_policy-2013%281%29.pdf

[54] อ้างอิง: https://prsindia.org/billtrack/the-data-protection-bill-2021

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| รักษาความปลอดภัยของข้อมูลและการรับรองความถูกต้องของข้อมูล [37]<br><br>**1.4) Telecommunications Act**<br>▪ พระราชบัญญัติการสื่อสารโทรคมนาคม (Telecommunications Act) กำหนดกรอบการทำงานสำหรับการให้บริการโทรคมนาคมในสิงคโปร์ MTCS ช่วยให้ผู้ให้บริการคลาวด์ที่เกี่ยวข้องกับการสื่อสารโทรคมนาคม สามารถปฏิบัติตามข้อกำหนดของพระราชบัญญัติ นี้ได้โดยการกำหนดมาตรการควบคุมความปลอดภัยที่เหมาะสม [38]<br><br>**1.5) Infocomm Media Development Authority (IMDA) Regulations**<br>▪ IMDA ซึ่งเป็นหน่วยงานที่รับผิดชอบการพัฒนาและควบคุมการสื่อสารและสื่อในสิงคโปร์ ได้กำหนดกฎระเบียบต่าง ๆ สำหรับผู้ให้บริการ คลาวด์ MTCS ช่วยให้ผู้ให้บริการคลาวด์สามารถปฏิบัติตามข้อกำหนด ของ IMDA ได้โดยการกำหนดมาตรการควบคุมความปลอดภัยที่สอดคล้องกับกฎระเบียบของ IMDA [39] | NIST SP 800-144 เป็นแนวทางสำหรับการจัดการความมั่นคงปลอดภัยและความเป็นส่วนตัวในการใช้บริการคลาวด์สาธารณะ กฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องกับมาตรฐานนี้ ได้แก่<br><br>**1.1) Federal Information Security Modernization Act (FISMA)**<br>▪ พระราชบัญญัติ FISMA กำหนดให้องค์กรของรัฐบาลกลางที่ใช้บริการคลาวด์สาธารณะต้องมีการป้องกันและจัดการความมั่นคงปลอดภัยตามแนวทางของ NIST SP 800-144 เพื่อป้องกันการรั่วไหลของข้อมูลสารสนเทศที่สำคัญ [44]<br><br>**1.2) Cloud Computing Strategy**<br>▪ ยุทธศาสตร์การใช้บริการคลาวด์ของรัฐบาลสหรัฐกำหนดให้องค์กรต้องปฏิบัติตามแนวทางของ NIST SP 800-144 เพื่อให้มั่นใจว่าการใช้บริการคลาวด์มีความปลอดภัยและเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัย [45]<br><br>**1.3) Office of Management and Budget (OMB) Circular A-130**<br>▪ แนวทางนี้กำหนดให้องค์กรของรัฐบาลต้องมีการป้องกันและจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศ โดย NIST SP 800-144 | | |

[37] อ้างอิง: https://sso.agc.gov.sg/Act/ETA2010

[38] อ้างอิง: Telecommunications Act 1999 - Singapore Statutes Online (agc.gov.sg)

[39] อ้างอิง: Architects of SG's Digital Future | IMDA - Infocomm Media Development Authority

[44] อ้างอิง: Federal Information Security Modernization Act (FISMA) | CMS Information Security & Privacy Group

[45] อ้างอิง: Strategy | Federal Cloud Computing Strategy (cio.gov)

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| | ให้แนวทางในการจัดการความเสี่ยงและการปกป้องข้อมูลในคลาวด์สาธารณะ [46]<br><br>**1.4) Federal Risk and Authorization Management Program (FedRAMP)**<br>▪ โปรแกรมนี้กำหนดให้ผู้ให้บริการคลาวด์ที่ต้องการให้บริการแก่หน่วยงานรัฐบาลกลางต้องปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยของ NIST SP 800-144 เพื่อให้บริการที่มีความปลอดภัยสูงสุด [47] | | |

## 3.2 การเปรียบเทียบกฎหมายที่เกี่ยวข้องกับผู้ใช้บริการ Cloud (Cloud Service Customer: CSC)

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| **1. มาตรฐาน Multi-Tier Cloud Security (MTCS)**<br>เป็นมาตรฐานแรกของโลกที่ครอบคลุมความมั่นคงปลอดภัยของบริการคลาวด์ในหลายระดับ ได้รับการออกแบบมาเพื่อให้สอดคล้องกับกฎหมายและระเบียบข้อบังคับต่างๆ ของสิงคโปร์ โดยเฉพาะในเรื่องของการปกป้องข้อมูลและความมั่นคงปลอดภัยทางไซเบอร์ กฎหมายที่เกี่ยวข้องกับ MTCS ของสิงคโปร์ ได้แก่<br>**1.1) Personal Data Protection Act (PDPA)** | **1. NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations**<br>เป็นมาตรฐานที่ให้แนวทางในการจัดการและป้องกันความมั่นคงปลอดภัยของระบบสารสนเทศและองค์กร กฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องกับมาตรฐานนี้ ได้แก่<br>**1.1) Federal Information Security Modernization Act (FISMA)**<br>▪ **รายละเอียด:** FISMA กำหนดให้หน่วยงานรัฐบาลกลางต้องพัฒนา เอกสาร และดำเนินการ | **1. พระราชบัญญัติอาชญากรรมไซเบอร์ พ.ศ. 2001 (Cybercrime Act 2001)**<br>▪ จัดการกับการกระทำผิดที่เกี่ยวข้องกับการละเมิดความปลอดภัยคอมพิวเตอร์ เช่น การเจาะระบบ การแพร่มัลแวร์ การโจมตีเพื่อปฏิเสธการให้บริการ เป็นต้น [66]<br>**2. Privacy Act 1988**<br>▪ กฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งระบุให้ต้องมีมาตรการรักษาความปลอดภัยของข้อมูลอย่างเหมาะสม [67] | ในประเทศอินเดีย ลูกค้าที่ใช้บริการคลาวด์ (Cloud Service Customer) จะต้องปฏิบัติตามกฎหมายและมาตรฐานต่าง ๆ ที่เกี่ยวข้อง โดยมีรายละเอียดดังนี้<br>**1. Information Technology Act, 2000 และ (Amendments) Rules**<br>▪ เป็นกฎหมายหลักที่กำกับดูแลเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการใช้บริการคลาวด์ [68]<br>**2. Guidelines for Government Departments on Contractual Terms Related to Cloud Services** |

[46] อ้างอิง: Policies & Priorities | CIO.GOV

[47] อ้างอิง: Federal Risk and Authorization Management Program (FedRAMP) | CMS Information Security & Privacy Group

[66] อ้างอิง: Federal Register of Legislation - Cybercrime Act 2001

[67] อ้างอิง: https://www.oaic.gov.au/privacy/the-privacy-act

[68] อ้างอิง: https://www.meity.gov.in/content/information-technology-act-2000

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| ▪ PDPA เป็นกฎหมายหลักที่กำหนดข้อกำหนดในการคุ้มครองข้อมูลส่วนบุคคลในสิงคโปร์ โดยเฉพาะสำหรับผู้ใช้บริการคลาวด์ที่มีการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลผ่านผู้ให้บริการคลาวด์ (CSPs) กฎหมายนี้กำหนดให้ผู้ใช้บริการคลาวด์ต้องมั่นใจว่าข้อมูลส่วนบุคคลได้รับการปกป้องอย่างเหมาะสม รวมถึงมีการปฏิบัติตามข้อกำหนดด้านการย้ายถ่ายข้อมูลไปยังต่างประเทศเมื่อใช้บริการคลาวด์ [55]<br><br>**1.2) Cybersecurity Act**<br>▪ พระราชบัญญัติความมั่นคงทางไซเบอร์ของสิงคโปร์กำหนดกรอบการป้องกันและจัดการกับภัยคุกคาม (Conventus Law) รวมถึงข้อ กำหนดสำหรับผู้ให้บริการคลาวด์และผู้ใช้บริการในการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ โดยเฉพาะอย่างยิ่งสำหรับโครงสร้างพื้น | ตามโครงการการรักษาความปลอดภัยข้อมูลตามมาตรฐาน NIST SP 800-53<br>▪ **การบังคับใช้ :** ผู้ใช้บริการคลาวด์ที่ทำงานกับหน่วยงานรัฐบาลกลางต้องมั่นใจว่ามีการปฏิบัติตามข้อกำหนดของ FISMA [58]<br><br>**1.2) Privacy Act of 1974**<br>▪ พระราชบัญญัตินี้กำหนดให้องค์กรต้องปกป้องข้อมูลส่วนบุคคลของพลเมืองอเมริกันที่ถูกเก็บรวบรวมในระบบสารสนเทศ โดย NIST SP 800-53 ให้แนวทางในการจัดการและปกป้องข้อมูลส่วนบุคคลเหล่านี้ [59]<br><br>**1.3) Health Insurance Portability and Accountability Act (HIPAA)**<br>▪ พระราชบัญญัติ HIPAA กำหนดให้หน่วยงานที่เกี่ยวข้องกับข้อมูลสุขภาพต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยของข้อมูลสุขภาพ NIST SP 800-53 ให้แนวทางในการป้องกันและรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพ [60] | | ▪ แนวทางสำหรับหน่วยงานรัฐในการทำสัญญากับผู้ให้บริการคลาวด์ ซึ่งลูกค้ารัฐบาลต้องปฏิบัติตาม [69]<br>**3. National Data Sharing and Accessibility Policy (NDSAP)**<br>▪ นโยบายการแบ่งปันและเข้าถึงข้อมูลระดับชาติ ซึ่งมีผลต่อการใช้บริการคลาวด์ในการจัดเก็บข้อมูล[70]<br>**4. Data Protection Bill, 2021 (ร่างกฎหมาย)**<br>▪ ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งเมื่อมีผลบังคับใช้จะมีผลต่อลูกค้าที่ใช้บริการคลาวด์ [71]<br>**5. Baseline Security Standard for Cloud Adoption**<br>▪ มาตรฐานความมั่นคงปลอดภัยขั้นพื้นฐานสำหรับการใช้บริการคลาวด์ที่ลูกค้าควรปฏิบัติตาม [72] |

[55] อ้างอิง: ida_mtcs-x-cert---implementation-guideline-report_mtcs-to-iso270012013_release.pdf (imda.gov.sg)

[58] อ้างอิง: Federal Information Security Modernization Act (FISMA) | CMS Information Security & Privacy Group

[59] อ้างอิง: The Privacy Act of 1974 – EPIC – Electronic Privacy Information Center

[60] อ้างอิง: HIPAA for Professionals | HHS.gov

[69] อ้างอิง: https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf

[70] อ้างอิง: https://data.gov.in/dataset-data-sharing-and-accessibility-policy-ndsap

[71] อ้างอิง: https://prsindia.org/billtrack/the-data-protection-bill-2021

[72] อ้างอิง: https://www.meity.gov.in/writereaddata/files/BaselineSecurityStandard.pdf

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| ฐานข้อมูลที่สำคัญ (Critical Information Infrastructure - CII) [56]<br><br>**1.3) พระราชบัญญัติการทำธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions Act - ETA)**<br>▪ ETA กำหนดกรอบการทำงานสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างปลอดภัย โดยมีข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลและการรับรองความถูกต้องของข้อมูล (ICLG IBR) ซึ่งเป็นข้อกำหนดที่สำคัญสำหรับผู้ใช้บริการคลาวด์ที่ทำธุรกรรมออนไลน์ [57] | **1.4) Federal Risk and Authorization Management Program (FedRAMP)**<br>▪ โปรแกรมนี้กำหนดให้องค์กรของรัฐบาลกลางที่ใช้บริการคลาวด์ต้องปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยของ NIST SP 800-53 เพื่อให้มั่นใจว่าบริการคลาวด์มีความปลอดภัย [61]<br><br>**2. NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing**<br>NIST SP 800-144 เป็นแนวทางสำหรับการจัดการความมั่นคงปลอดภัยและความเป็นส่วนตัวในการใช้บริการคลาวด์สาธารณะ กฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องกับมาตรฐานนี้ ได้แก่<br>**1.1) Federal Information Security Modernization Act (FISMA)**<br>▪ พระราชบัญญัติ FISMA กำหนดให้องค์กรของรัฐบาลกลางที่ใช้บริการคลาวด์สาธารณะต้องมีการป้องกันและจัดการความมั่นคงปลอดภัยตามแนวทางของ NIST SP 800-144 เพื่อป้องกันการรั่วไหลของข้อมูลสารสนเทศที่สำคัญ [62]<br>**1.2) Cloud Computing Strategy**<br>▪ ยุทธศาสตร์การใช้บริการคลาวด์ของรัฐบาลสหรัฐกำหนดให้องค์กรต้องปฏิบัติตามแนวทางของ NIST SP 800-144 เพื่อให้มั่นใจว่าการใช้ | | |

[56] อ้างอิง: https://sso.agc.gov.sg/Act-Rev/CA2018/Published/20211231?DocDate=20211231&ViewType=Pdf&_=20230508142246

[57] อ้างอิง: https://sso.agc.gov.sg/Act/ETA2010

[61] อ้างอิง: Federal Risk and Authorization Management Program (FedRAMP) | CMS Information Security & Privacy Group

[62] อ้างอิง: Federal Information Security Modernization Act (FISMA) | CMS Information Security & Privacy Group

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| | บริการคลาวด์มีความปลอดภัยและเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัย [63]<br><br>**1.3) Office of Management and Budget (OMB) Circular A-130**<br>▪ แนวทางนี้กำหนดให้องค์กรของรัฐบาลต้องมีการป้องกันและจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศ โดย NIST SP 800-144 ให้แนวทางในการจัดการความเสี่ยงและการปกป้องข้อมูลในคลาวด์สาธารณะ [64]<br><br>**1.4) Federal Risk and Authorization Management Program (FedRAMP)**<br>▪ โปรแกรมนี้กำหนดให้ผู้ให้บริการคลาวด์ที่ต้องการให้บริการแก่หน่วยงานรัฐบาลกลางต้องปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยของ NIST SP 800-144 เพื่อให้บริการที่มีความปลอดภัยสูงสุด [65] | | |

## 3.3 อ้างอิงตัวอย่างหน่วยงานหลัก ๆ ของแต่ละประเทศที่ได้รับการบังคับใช้

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| **หน่วยงานภาครัฐ**<br>▪ Ministry of Communications and Information (MCI) (https://www.mci.gov.sg/) | **หน่วยงานกลาง**<br>▪ Department of Defense (DoD) (https://www.defense.gov/) | **หน่วยงานกลาง**<br>▪ Department of Defence (https://www.defence.gov.au/) | **หน่วยงานกลาง**<br>▪ Ministry of Home Affairs (https://www.mha.gov.in/) |

[63] อ้างอิง: Strategy | Federal Cloud Computing Strategy (cio.gov)

[64] อ้างอิง: Policies & Priorities | CIO.GOV

[65] อ้างอิง: Federal Risk and Authorization Management Program (FedRAMP) | CMS Information Security & Privacy Group

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| ▪ Government Technology Agency (GovTech) (https://www.tech.gov.sg/)<br>▪ Cyber Security Agency of Singapore (CSA) (https://www.csa.gov.sg/)<br>▪ Infocomm Media Development Authority (IMDA) (https://www.imda.gov.sg/)<br><br>**สถาบันการเงิน**<br>▪ DBS Bank (https://www.dbs.com.sg/)<br>▪ OCBC Bank (https://www.ocbc.com/)<br>▪ United Overseas Bank (UOB) (https://www.uobgroup.com/singapore/index.html)<br>▪ Great Eastern Life (https://www.greateasternlife.com/sg/en/personal-insurance.html)<br>▪ AIA Singapore (https://www.aia.com.sg/)<br>**บริษัทเทคโนโลยี** | ▪ Department of Homeland Security (DHS) (https://www.dhs.gov/)<br>▪ Department of Energy (DOE) (https://www.energy.gov/)<br><br>**หน่วยงานความมั่นคงแห่งชาติ**<br>▪ National Security Agency (NSA) (https://www.nsa.gov/)<br>▪ Central Intelligence Agency (CIA) (https://www.cia.gov/)<br><br>**หน่วยงานบังคับใช้กฎหมาย**<br>▪ Federal Bureau of Investigation (FBI) (https://www.fbi.gov/)<br>▪ Drug Enforcement Administration (DEA) (https://www.dea.gov/)<br>**องค์กรอิสระ**<br>▪ National Aeronautics and Space Administration (NASA) (https://www.nasa.gov/)<br>▪ United States Postal Service (USPS) (https://www.usps.com/)<br>**หน่วยงานอื่นๆ** | ▪ Department of Home Affairs (https://www.homeaffairs.gov.au/)<br>▪ Australian Taxation Office (ATO) (https://www.ato.gov.au/)<br><br>**หน่วยงานความมั่นคงและกิจการต่างประเทศ**<br>▪ Australian Security Intelligence Organisation (ASIO) (https://www.asio.gov.au/)<br>▪ Australian Secret Intelligence Service (ASIS) (https://www.asis.gov.au/)<br>▪ Department of Foreign Affairs and Trade (DFAT) (https://www.dfat.gov.au/)<br><br>**หน่วยงานบังคับใช้กฎหมาย**<br>▪ Australian Federal Police (AFP) (https://www.afp.gov.au/)<br>▪ Australian Criminal Intelligence Commission (ACIC) (https://www.acic.gov.au/)<br>**หน่วยงานดูแลสาธารณสุขและสวัสดิการ** | ▪ Ministry of Defence (https://mod.gov.in/)<br>▪ Central Board of Direct Taxes (https://www.incometaxindia.gov.in/)<br><br>**หน่วยงานด้านความมั่นคง**<br>▪ Intelligence Bureau (IB) (https://www.mha.gov.in/div_isf/intro)<br>▪ Research and Analysis Wing (R&AW) (https://www.rawindia.gov.in/)<br>**หน่วยงานบังคับใช้กฎหมาย**<br>▪ Central Bureau of Investigation (CBI) (https://cbi.gov.in/)<br>▪ National Investigation Agency (NIA) (https://www.nia.gov.in/)<br><br>**หน่วยงานด้านสาธารณสุข**<br>▪ Ministry of Health and Family Welfare (https://www.mohfw.gov.in/) |

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| ▪ Singtel (https://www.singtel.com/)<br>▪ StarHub (https://www.starhub.com/)<br>▪ M1 Limited (https://www.m1.com.sg/)<br>▪ Amazon Web Services (AWS) (https://aws.amazon.com/singapore/)<br>▪ Microsoft (https://www.microsoft.com/en-sg)<br>**องค์กรด้านสาธารณสุข**<br>▪ Singapore General Hospital (SGH) (https://www.sgh.com.sg/)<br>▪ National University Hospital (NUH) (https://www.nuh.com.sg/)<br>▪ KK Women's and Children's Hospital (https://www.kkh.com.sg/)<br>▪ Changi General Hospital (https://www.cgh.com.sg/) | ▪ Department of Health and Human Services (HHS) (https://www.hhs.gov/)<br>▪ Department of Veterans Affairs (VA) (https://www.va.gov/)<br>▪ Social Security Administration (SSA) (https://www.ssa.gov/) | ▪ Department of Health (https://www.health.gov.au/)<br>▪ Services Australia (https://www.servicesaustralia.gov.au/)<br>**องค์กรอื่น ๆ**<br>▪ Australian Bureau of Statistics (ABS) (https://www.abs.gov.au/)<br>▪ Australian Postal Corporation (Australia Post) (https://auspost.com.au/) | ▪ Indian Council of Medical Research (ICMR) (https://www.icmr.gov.in/)<br>**องค์กรอื่น ๆ**<br>▪ Reserve Bank of India (RBI) (https://www.rbi.org.in/)<br>▪ Indian Space Research Organisation (ISRO) (https://www.isro.gov.in/) |

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| ▪ Raffles Medical Group (https://www.rafflesmedicalgroup.com/) | | | |

## 3.4 ปัญหาและอุปสรรค

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| 1) **ความซับซ้อนในการปรับใช้มาตรฐาน**<br>➢ การปรับใช้มาตรฐาน SS584 นั้น มีความซับซ้อนเนื่องจากมาตรฐานนี้ประกอบด้วยหลายระดับ (tiers) ซึ่งแต่ละระดับมีข้อกำหนดที่แตกต่างกันไปตามความสำคัญของข้อมูลและระบบที่ต้องการป้องกัน เช่น Tier 1 สำหรับข้อมูลที่ไม่สำคัญทางธุรกิจ, Tier 2 สำหรับข้อมูลที่สำคัญ และ Tier 3 สำหรับข้อมูลที่มีความสำคัญสูง เช่น ข้อมูลทางการเงินและการแพทย์<br>2) **การปรับปรุงระบบและกระบวนการ**<br>➢ องค์กรที่ต้องการรับรองตามมาตรฐาน SS584 ต้องปรับปรุงระบบและกระบวนการต่าง ๆ อย่างต่อเนื่อง เช่น การประเมินความเสี่ยงด้านความปลอดภัยของข้อมูล, การออกแบบและดำเนินการมาตรการควบคุมความปลอดภัยที่ครอบคลุม และการจัดการกระบวนการเพื่อให้มั่นใจว่ามาตรการความปลอดภัยของข้อมูลตอบสนองต่อความต้องการขององค์กรอย่างต่อเนื่อง<br>3) **การตรวจสอบและประเมินผล**<br>➢ การได้รับการรับรองตามมาตรฐาน SS584 ต้องผ่านการตรวจสอบและประเมินผลจาก | 1) **ความซับซ้อนของกระบวนการรับรอง**<br>➢ กระบวนการรับรองตามมาตรฐาน FedRAMP มีหลายขั้นตอนที่ต้องดำเนินการ เช่น การเตรียมเอกสารระบบความปลอดภัย (System Security Plan - SSP), การประเมินความปลอดภัยโดยองค์กรตรวจสอบภายนอก (Third Party Assessment Organization - 3PAO), และการตรวจสอบต่อเนื่อง (Continuous Monitoring) ซึ่งแต่ละขั้นตอนต้องใช้เวลาและทรัพยากรมาก<br>2) **ค่าใช้จ่ายที่สูง**<br>➢ ค่าใช้จ่ายในการขอรับรองตามมาตรฐาน FedRAMP สามารถสูงถึงหลายแสนถึงหลายล้านดอลลาร์ โดยค่าใช้จ่ายนี้รวมถึงค่าใช้จ่ายในการปรับปรุงระบบ, การจัดทำเอกสาร, การจ้าง 3PAO, และการตรวจสอบต่อเนื่อง องค์กรที่ไม่มีทรัพยากรภายในที่เพียงพออาจต้องจ้างที่ปรึกษาภายนอกซึ่งเพิ่มค่าใช้จ่ายขึ้นอีก<br>3) **ระยะเวลาที่ใช้ในการขอรับรอง**<br>➢ กระบวนการขอรับรอง FedRAMP อาจใช้เวลานานหลายเดือนถึงหลายปี ขึ้นอยู่กับความซับซ้อนของระบบและความพร้อมของเอกสารและข้อมูลที่ต้องใช้ในการประเมิน องค์กรต้องเตรียมความพร้อมและจัดการเวลาของทรัพยากรภายในให้เหมาะสม | 1) **ความซับซ้อนของมาตรฐาน**<br>➢ มาตรฐาน ISM มีข้อกำหนดและแนวทางที่ซับซ้อน ซึ่งครอบคลุมหลายด้านของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เช่น การกำกับดูแล การป้องกัน การตรวจจับ และการตอบสนอง องค์กรต้องมีการปรับปรุงระบบและกระบวนการอย่างต่อเนื่องเพื่อให้สอดคล้องกับข้อกำหนดเหล่านี้ ซึ่งเป็นภาระที่ยากสำหรับบางองค์กรในการปฏิบัติตามอย่างครบถ้วน<br>2) **การจัดการและการปรับปรุงระบบอย่างต่อเนื่อง**<br>➢ องค์กรต้องมีการประเมินและปรับปรุงระบบความมั่นคงปลอดภัยของข้อมูลอย่างต่อเนื่อง การตรวจสอบและทบทวนประสิทธิภาพของมาตรการที่ใช้อยู่เป็นสิ่งที่จำเป็นเพื่อให้มั่นใจว่าสามารถรับมือกับภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปได้อย่างมีประสิทธิภาพ<br>3) **การตรวจสอบและการประเมินผล**<br>➢ การขอรับรองมาตรฐาน ISM ต้องผ่านการตรวจสอบและประเมินผลจากหน่วยงานที่มีอำนาจรับรอง องค์กรต้องจัดเตรียมเอกสารและข้อมูลที่เกี่ยวข้องกับระบบความมั่นคงปลอดภัย รวมถึงการตรวจสอบประจำปีและการตรวจสอบต่อเนื่องเพื่อให้มั่นใจว่า | 1) **ความซับซ้อนของข้อกำหนดมาตรฐาน**<br>➢ มาตรฐาน Cloud Security Baseline มีรายละเอียดและข้อกำหนดที่ค่อนข้างซับซ้อน ครอบคลุมด้านการจัดการความเสี่ยง การควบคุมการเข้าถึง การบริหารจัดการการเปลี่ยนแปลง การตรวจสอบและติดตาม รวมถึงความมั่นคงปลอดภัยทางกายภาพ ทำให้องค์กรต้องทุ่มเททรัพยากรอย่างมากในการทำความเข้าใจและปฏิบัติตามข้อกำหนดเหล่านั้น<br>2) **ขาดแคลนบุคลากรผู้เชี่ยวชาญ**<br>➢ เนื่องจากมาตรฐานมีข้อกำหนดในด้าน technical ค่อนข้างละเอียด โดยเฉพาะในด้านมาตรฐานการเข้ารหัส ที่ค่อนข้างต้องการสูง ทำให้ยากในการหาทั้งผู้เชี่ยวชาญ รวมถึงมีค่าใช้จ่ายในการดูแลสูง<br>3) **การเข้าถึงเอกสารและแหล่งข้อมูลที่จำกัด**<br>➢ เนื่องจากมาตรฐานนี้ค่อนข้างใหม่ จึงมีเอกสารอ้างอิง แนวทางปฏิบัติ และแหล่งข้อมูลสาธารณะที่เกี่ยวข้องจำกัด ทำให้องค์กรต้องพึ่งพาแหล่งข้อมูล จากภายในหรือจากที่ปรึกษาภายนอกซึ่งมีค่าใช้จ่ายสูง<br>4) **ความยุ่งยากในการประเมินตนเองตามมาตรฐาน** |

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| หน่วยงานที่มีอำนาจรับรอง ซึ่งรวมถึงการตรวจสอบประจำปีและการตรวจสอบซ้ำทุกสามปี นอกจากนี้ องค์กรต้องพร้อมสำหรับการตรวจสอบที่ไม่กำหนดเวลา (spot checks) เพื่อให้มั่นใจว่ายังคงปฏิบัติตามข้อกำหนดของมาตรฐานนี้<br>**4) ค่าใช้จ่ายในการรับรอง**<br>➢ กระบวนการขอรับรองตามมาตรฐาน SS584 มักมีค่าใช้จ่ายสูง ทั้งในด้านค่าใช้จ่ายในการปรับปรุงระบบภายในองค์กร และค่าใช้จ่ายในการจ้างหน่วยงานที่มีอำนาจรับรองมาตรฐานเพื่อทำการตรวจสอบและประเมินผล การจัดเตรียมทรัพยากรและบุคลากรเพื่อดำเนินการตามข้อกำหนดของมาตรฐานนี้ก็เป็นอีกปัจจัยหนึ่งที่ทำให้เกิดค่าใช้จ่ายเพิ่มเติม<br>**5) การเปลี่ยนแปลงและการปรับตัวตามมาตรฐานใหม่**<br>➢ การปรับเปลี่ยนจากมาตรฐาน SS584 เวอร์ชันเก่า (2015) ไปยังเวอร์ชันใหม่ (2020) ต้องมีการปรับปรุงและเปลี่ยนแปลงระบบภายในองค์กรให้สอดคล้องกับข้อกำหนดใหม่ ซึ่งเป็นภาระเพิ่มเติมที่ต้องจัดการและใช้ทรัพยากรเพิ่มเติมในการดำเนินการให้เสร็จสิ้นภายในเวลาที่กำหนด [73] | เพื่อให้สามารถดำเนินการตามขั้นตอนต่าง ๆ ได้อย่างมีประสิทธิภาพ<br>**4) การตรวจสอบและประเมินผลต่อเนื่อง**<br>➢ หลังจากได้รับการรับรองแล้ว องค์กรต้องดำเนินการตรวจสอบและส่งรายงานการตรวจสอบความปลอดภัยเป็นประจำทุกเดือนเพื่อให้แน่ใจว่ายังคงปฏิบัติตามมาตรฐาน FedRAMP ซึ่งเพิ่มภาระงานและค่าใช้จ่ายในการดำเนินการต่อเนื่อง.<br>**5) การเปลี่ยนแปลงและการปรับตัวตามเทคโนโลยีใหม่**<br>➢ การเปลี่ยนแปลงเทคโนโลยีและมาตรฐานความปลอดภัยที่เปลี่ยนแปลงไปอย่างรวดเร็วทำให้องค์กรต้องมีการปรับปรุงและปรับตัวอย่างต่อเนื่อง ซึ่งเป็นภาระเพิ่มเติมที่ต้องจัดการและใช้ทรัพยากรเพิ่มเติมในการดำเนินการให้เสร็จสิ้นภายในเวลาที่กำหนด [74] | ยังคงปฏิบัติตามมาตรฐานนี้ ซึ่งเป็นภาระเพิ่มเติมในการดำเนินการ<br>**4) ค่าใช้จ่ายที่สูง**<br>➢ กระบวนการขอรับรองมาตรฐาน ISM มักมีค่าใช้จ่ายสูง ทั้งในด้านการปรับปรุงระบบ การจัดทำเอกสาร และการจ้างหน่วยงานตรวจสอบภายนอก ค่าใช้จ่ายเหล่านี้อาจเป็นอุปสรรคใหญ่สำหรับองค์กรขนาดเล็กหรือองค์กรที่มีงบประมาณจำกัด | ➢ องค์กรต้องดำเนินการประเมินตนเองอย่างละเอียดรอบคอบตามข้อกำหนดของมาตรฐาน ซึ่งมีรายละเอียดครอบคลุมหลายด้านและมีความซับซ้อนสูง จึงต้องใช้เวลาและความพยายามอย่างมากในการประเมิน |

[73] อ้างอิง:TÜV SÜD PSB on SS 584 MTCS Certification Infocomm Media Development Authority on Cloud Computing and Services (TÜV SÜD)

[74] อ้างอิง: Cloud Security Alliance on FedRAMP Security Boulevard on FedRAMP Challenges Citizens Against Government Waste on FedRAMP Solutions

## 3.5 ตัวอย่าง การบังคับใช้กฎหมายข้ามประเทศ

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| การบังคับใช้กฎหมายข้ามประเทศในกรณีของข้อมูลบนคลาวด์ในสิงคโปร์มีประเด็นที่น่าสนใจดังนี้<br>**1) Personal Data Protection Act (PDPA)**<br>➢ PDPA เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ ซึ่งมีผลบังคับใช้กับองค์กรที่ประมวลผลข้อมูลส่วนบุคคลของประชาชนสิงคโปร์ แม้ว่าข้อมูลนั้นจะถูกเก็บบนคลาวด์ในต่างประเทศก็ตาม<br>➢ องค์กรจะต้องปฏิบัติตามข้อกำหนดของ PDPA เช่น การขอความยินยอม การรักษาความปลอดภัยของข้อมูล และการส่งหรือโอนข้อมูลไปยังต่างประเทศ<br>**2) พระราชบัญญัติหลักความปลอดภัยทางไซเบอร์ (Cybersecurity Act)**<br>➢ พระราชบัญญัติฉบับนี้ให้อำนาจแก่คณะกรรมการความมั่นคงทางไซเบอร์ หรือ Cyber Security Agency (CSA) ในการสั่งให้ผู้ให้บริการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อแก้ไขหรือป้องกันภัยคุกคามทางไซเบอร์<br>➢ มาตราดังกล่าวอาจนำมาใช้บังคับกับคลาวด์ผู้ให้บริการที่มีข้อมูลหรือระบบที่ตั้งอยู่ในสิงคโปร์ แม้ว่าบริษัทนั้นจะมีสำนักงานใหญ่ในต่างประเทศ | การบังคับใช้กฎหมายข้ามประเทศในแง่ของข้อมูลบน Cloud ของประเทศสหรัฐอเมริกามีความซับซ้อนและเกี่ยวข้องกับหลายประเด็นหลัก ได้แก่ การคุ้มครองข้อมูลส่วนบุคคล การบังคับใช้กฎหมายท้องถิ่น และการปฏิบัติตามข้อกำหนดของกฎหมายระหว่างประเทศ บทความนี้จะครอบคลุมประเด็นสำคัญต่าง ๆ ดังนี้<br>**1) การคุ้มครองข้อมูลส่วนบุคคล (Data Protection)**<br>➢ สหรัฐอเมริกามีกฎหมายคุ้มครองข้อมูลหลายฉบับ ซึ่งรวมถึง Health Insurance Portability and Accountability Act (HIPAA) ที่คุ้มครองข้อมูลสุขภาพ, Children's Online Privacy Protection Act (COPPA) ที่คุ้มครองข้อมูลของเด็ก และ California Consumer Privacy Act (CCPA) ที่เน้นการคุ้มครองข้อมูลผู้บริโภคในรัฐแคลิฟอร์เนีย นอกจากนี้ยังมีกฎหมาย Cloud Act (Clarifying Lawful Overseas Use of Data Act) ที่อนุญาตให้รัฐบาลสหรัฐฯ สามารถเข้าถึงข้อมูลที่เก็บในCloud ได้ แม้ว่าจะอยู่ในประเทศอื่น หากมีการออกหมายจับหรือคำสั่งศาล<br>**2) การบังคับใช้กฎหมายท้องถิ่น (Local Law Enforcement)**<br>➢ การบังคับใช้กฎหมายท้องถิ่นของสหรัฐอเมริกามีผลกระทบโดยตรงต่อการจัดการข้อมูลบน Cloud บริษัทผู้ให้บริการ Cloud ต้องปฏิบัติตามกฎหมายและคำสั่งศาลที่ออกโดยหน่วยงานท้องถิ่น ซึ่งอาจรวมถึงการส่งมอบข้อมูลเมื่อมีการร้องขอ ทั้งนี้ การ | การบังคับใช้กฎหมายข้ามประเทศในแง่ของข้อมูลบน Cloud ที่ส่งออกจากประเทศออสเตรเลียมีความซับซ้อนและครอบคลุมหลายด้านเช่นเดียวกันกับประเทศอื่น ๆ บทความนี้จะครอบคลุมประเด็นสำคัญต่าง ๆ ดังนี้<br>**1) การคุ้มครองข้อมูลส่วนบุคคล (Data Protection)**<br>➢ ออสเตรเลียมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่สำคัญคือ Privacy Act 1988 ซึ่งกำหนดข้อกำหนดและหลักเกณฑ์เกี่ยวกับการจัดการข้อมูลส่วนบุคคล รวมถึง Australian Privacy Principles (APPs) ที่ให้แนวทางในการปฏิบัติต่อข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่ง APP 8 ที่กล่าวถึงการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยกำหนดให้ผู้ควบคุมข้อมูลต้องมั่นใจว่าข้อมูลนั้นจะได้รับการคุ้มครองตามมาตรฐานที่เพียงพอ<br>**2) การบังคับใช้กฎหมายท้องถิ่น (Local Law Enforcement)**<br>➢ กฎหมายท้องถิ่นของออสเตรเลีย เช่น Telecommunications (Interception and Access) Act 1979 และ Security of Critical Infrastructure Act 2018 กำหนดให้บริษัทผู้ให้บริการ Cloud ต้องปฏิบัติตามข้อกำหนดและคำสั่งของหน่วยงานท้องถิ่นในการจัดเก็บและส่งมอบข้อมูล ทั้งนี้รวมถึงการเข้าถึงข้อมูลเพื่อการสืบสวนสอบสวนและรักษาความมั่นคง<br>**3) ข้อกำหนดของกฎหมายระหว่างประเทศ (International Law Compliance)** | การบังคับใช้กฎหมายข้ามประเทศในแง่ของข้อมูลบน Cloud ที่ส่งออกจากประเทศอินเดียมีความซับซ้อนและเกี่ยวข้องกับหลายประเด็นหลัก ได้แก่ การคุ้มครองข้อมูลส่วนบุคคล การบังคับใช้กฎหมายท้องถิ่น และการปฏิบัติตามข้อกำหนดของกฎหมายระหว่างประเทศ บทความนี้จะครอบคลุมประเด็นสำคัญต่าง ๆ ดังนี้<br>**1) การคุ้มครองข้อมูลส่วนบุคคล (Data Protection)**<br>➢ อินเดียมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่สำคัญคือ Information Technology Act 2000 และ Personal Data Protection Bill 2019 (ยังอยู่ระหว่างการพิจารณา) ที่กำหนดข้อกำหนดและหลักเกณฑ์เกี่ยวกับการจัดการข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่ง Personal Data Protection Bill จะมีบทบัญญัติที่กล่าวถึงการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยกำหนดให้ผู้ควบคุมข้อมูลต้องมั่นใจว่าข้อมูลนั้นจะได้รับการคุ้มครองตามมาตรฐานที่เพียงพอ<br>**2) การบังคับใช้กฎหมายท้องถิ่น (Local Law Enforcement)**<br>➢ กฎหมายท้องถิ่นของอินเดีย เช่น Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 และ Indian Telegraph Act 1885 กำหนดให้บริษัทผู้ให้บริการ Cloud ต้องปฏิบัติตามข้อกำหนดและคำสั่งของหน่วยงานท้องถิ่นในการจัดเก็บและส่งมอบข้อมูล รวมถึงการ |

| สิงคโปร์ | สหรัฐอเมริกา | ออสเตรเลีย | อินเดีย |
|---|---|---|---|
| **3) ความร่วมมือข้ามพรมแดนและความตกลงทวิภาคี**<br>➢ สิงคโปร์มีความร่วมมือด้านการบังคับใช้กฎหมายข้ามพรมแดนกับหลายประเทศ เช่น สหรัฐอเมริกา สหราชอาณาจักร และประเทศในกลุ่มอาเซียน<br>➢ ในกรณีที่เกี่ยวข้องกับข้อมูลบนคลาวด์ หน่วยงานบังคับใช้กฎหมายของสิงคโปร์อาจร้องขอความร่วมมือจากหน่วยงานในต่างประเทศตามข้อตกลงระหว่างประเทศที่มีอยู่<br>➢ โดยสรุป สิงคโปร์มีกฎหมายและกรอบการทำงานในการเข้าถึงและบังคับใช้กฎหมายเกี่ยวกับข้อมูลบนคลาวด์ทั้งภายในประเทศและข้ามพรมแดน แต่ในทางปฏิบัติอาจยังมีข้อจำกัดหรือความท้าทายบางประการ ขึ้นอยู่กับเงื่อนไขและความสัมพันธ์ระหว่างประเทศที่เกี่ยวข้อง [75] | ส่งมอบข้อมูลจะต้องสอดคล้องกับข้อกำหนดทางกฎหมายที่เกี่ยวข้อง<br>**3) ข้อกำหนดของกฎหมายระหว่างประเทศ (International Law Compliance)**<br>➢ สหรัฐอเมริกายังมีการลงนามในข้อตกลงระหว่างประเทศหลายฉบับเพื่อความร่วมมือในการบังคับใช้กฎหมายและการแลกเปลี่ยนข้อมูล เช่น ข้อตกลงกับสหภาพยุโรปที่เน้นการคุ้มครองข้อมูลส่วนบุคคลผ่านกลไกต่าง ๆ เช่น Privacy Shield (แม้ว่า Privacy Shield จะถูกยกเลิกและแทนที่ด้วยกลไกอื่น) และ Mutual Legal Assistance Treaties (MLATs) ที่ช่วยในการแลกเปลี่ยนข้อมูลระหว่างประเทศเพื่อต่อต้านอาชญากรรม [76] | ➢ ออสเตรเลียยังมีการลงนามในข้อตกลงระหว่างประเทศเพื่อความร่วมมือในการบังคับใช้กฎหมายและการแลกเปลี่ยนข้อมูล เช่น Mutual Legal Assistance Treaties (MLATs) กับประเทศอื่นๆ ที่ช่วยในการแลกเปลี่ยนข้อมูลและปฏิบัติตามกฎหมายระหว่างประเทศ นอกจากนี้ ออสเตรเลียยังเป็นสมาชิกของ Asia-Pacific Economic Cooperation (APEC) ที่มีการกำหนดมาตรฐานการคุ้มครองข้อมูลข้ามพรมแดน [77] | เข้าถึงข้อมูลเพื่อการสืบสวนสอบสวนและรักษาความมั่นคง<br>**3) ข้อกำหนดของกฎหมายระหว่างประเทศ (International Law Compliance)**<br>➢ อินเดียยังมีการลงนามในข้อตกลงระหว่างประเทศเพื่อความร่วมมือในการบังคับใช้กฎหมายและการแลกเปลี่ยนข้อมูล เช่น Mutual Legal Assistance Treaties (MLATs) กับประเทศอื่น ๆ ที่ช่วยในการแลกเปลี่ยนข้อมูลและปฏิบัติตามกฎหมายระหว่างประเทศ นอกจากนี้ อินเดียยังมีการเข้าร่วมในเวทีระหว่างประเทศต่างๆ ที่มุ่งเน้นการคุ้มครองข้อมูลและความร่วมมือทางกฎหมาย [78] |

[75] อ้างอิง: Personal Data Protection Act: https://sso.agc.gov.sg/Act/PDPA2012, Cross-Border Data Transfers: https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Cross-border-Data-Transfers, Cloud Service Providers' Policies: https://aws.amazon.com/compliance/data-privacy-faq/, https://www.microsoft.com/en-us/trustcenter/privacy/data-location

[76] อ้างอิง: Cloud Act, California Consumer Privacy Act (CCPA), Health Insurance Portability and Accountability Act (HIPAA), Mutual Legal Assistance Treaties (MLATs)

[77] อ้างอิง: Privacy Act 1988, Australian Privacy Principles (APPs), Telecommunications (Interception and Access) Act 1979, Security of Critical Infrastructure Act 2018 (SOCI) (cisc.gov.au), Mutual Legal Assistance Treaties (MLATs)

[78] อ้างอิง: Information Technology Act 2000, Personal Data Protection Bill 2019, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, Indian Telegraph Act 1885

# บทที่ 4 การวิเคราะห์ความเป็นไปได้ และข้อเสนอแนะเชิงนโยบาย

## 4.1 การวิเคราะห์ความเป็นไปได้

4.1.1 ด้านการกำกับดูแลและโครงสร้างองค์กร

4.1.1.1 กำหนดให้มีหน่วยงานที่กำกับดูแลผู้ให้บริการคลาวด์ และผู้ใช้บริการคลาวด์ ที่ชัดเจนและเข้มงวด (สิงคโปร์, ออสเตรเลีย)

4.1.1.2 กำหนดกรอบการทำงานสำหรับการควบคุมและการจัดการความปลอดภัยสารสนเทศพร้อมบทบาทและความรับผิดชอบที่ระบุไว้ชัดเจน (สหรัฐอเมริกา, อินเดีย)

4.1.2 ด้านการจัดการความเสี่ยง

4.1.2.1 การจัดการความเสี่ยง ทั้งในส่วนของผู้ให้บริการคลาวด์ และผู้ใช้บริการคลาวด์ (สิงคโปร์, สหรัฐอเมริกา, ออสเตรเลีย, อินเดีย)

4.1.2.2 การจัดการความเสี่ยงตามระดับผลกระทบต่อข้อมูลหรือระบบสารสนเทศ (สิงคโปร์, สหรัฐอเมริกา)

4.1.2.3 การจัดการความเสี่ยงตามระดับข้อมูลอ่อนไหว (สิงคโปร์, สหรัฐอเมริกา)

4.1.3 ด้านมาตรการควบคุม

4.1.3.1 มาตรการควบคุมที่ครอบคลุมทั้งในด้านการบริหารจัดการ การระบุ การป้องกัน การเฝ้าระวัง การตอบสนอง และการกู้คืน (สิงคโปร์, สหรัฐอเมริกา, ออสเตรเลีย, อินเดีย)

4.1.4 ด้านการตรวจและให้การรับรอง

4.1.4.1 ต้องการการรับรองตามระดับบริการ พร้อมการตรวจสอบโดยเข้มงวด และเป็นประจำ (สิงคโปร์, ออสเตรเลีย, อินเดีย)

4.1.4.2 กำหนดให้มีการรับรองและการตรวจสอบเป็นประจำโดยหน่วยงานภายนอก (สหรัฐอเมริกา)

4.1.5 การจัดการเหตุการณ์ (Event/Incident)

4.1.5.1 มีขั้นตอนการจัดการเหตุการณ์โดยละเอียด พร้อมการรายงานที่ทันเวลา (สิงคโปร์, สหรัฐอเมริกา, อินเดีย)

4.1.5.2 มีแผนการจัดการเหตุการณ์ที่ครอบคลุมและชัดเจน (ออสเตรเลีย)

## 4.2 ข้อเสนอแนะเชิงนโยบาย

4.2.1 ด้านการกำกับดูแลและโครงสร้างองค์กร

- สกมช. ควรทำหน้าที่กำกับดูแลผู้ใช้บริการคลาวด์ (หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ) และผู้ให้บริการคลาวด์ (เฉพาะที่ให้บริการกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ) ตามหน้าที่และอำนาจที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

- ในส่วนของผู้ให้บริการคลาวด์ สกมช. อาจจะไม่สามารถกำกับดูแลได้โดยตรง เนื่องจากมิได้มีสถานะเป็นหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ตามที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคง

ปลอดภัยไซเบอร์ พ.ศ. 2562 จึงต้องพิจารณาทางเลือกอื่นในการดำเนินการ เช่น การกำกับดูแลทางอ้อมผ่านหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น

- ในส่วนของผู้ให้บริการคลาวด์ สกมช. อาจใช้กลไกการกำกับดูแลตามกฎหมายลำดับรองของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่สำคัญได้แก่ ผู้ตรวจรับรอง หรือหน่วยงานตรวจรับรอง ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566

4.2.2 ด้านการจัดการความเสี่ยง

- สกมช. ควรกำหนดมาตรการควบคุมตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ให้ครอบคลุมทั้งผู้ให้บริการคลาวด์ และผู้ใช้บริการคลาวด์

- สกมช. ควรจัดประเภทข้อมูลหรือระบบสารสนเทศของผู้ใช้บริการคลาวด์ ตามระดับผลกระทบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Security Categorization) เพื่อให้สามารถกำหนดมาตรการควบคุมตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ได้อย่างเหมาะสม และมีประสิทธิภาพ รวมถึงไม่เป็นภาระเกินความจำเป็นอีกด้วย

- นอกจากการจัดประเภทข้อมูลหรือระบบสารสนเทศของผู้ใช้บริการคลาวด์ตามระดับผลกระทบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Security Categorization) แล้ว สกมช. ควรจัดประเภทข้อมูลหรือระบบสารสนเทศโดยคำถึงข้อมูลอ่อนไหว (Sensitive Data) ด้วย โดยเฉพาะข้อมูลส่วนบุคคล ตามนิยามของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

4.2.3 ด้านมาตรการควบคุม

- สกมช. ควรจัดทำมาตรการควบคุมตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ให้มีความครอบคลุมทั้งในด้านการบริหารจัดการ การระบุ การป้องกัน การเฝ้าระวัง การตอบสนอง และการกู้คืน

- สกมช. ควรคำนึงถึงความเข้ากันได้กับมาตรฐานความปลอดภัยระบบคลาวด์ในระดับสากล เช่น ISO/IEC 27001, 27701, 27017, 27018, CSA STAR, NIST Cyber Security Framework, FedRAMP เป็นต้น

4.2.4 ด้านการตรวจและให้การรับรอง

- สกมช. ควรสร้างกลไกการตรวจสอบและให้การรับรองตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ทั้งในส่วนของผู้ให้บริการคลาวด์ และผู้ใช้บริการคลาวด์ โดยกลไกดังกล่าวต้องมีความเพียงพอ และมีคุณภาพตามมาตรฐานสากลด้วย

- สกมช. ควรส่งเสริมให้มีกลไกการตรวจสอบและให้การรับรองโดยหน่วยงานภายนอก (Third Party Auditing) ซึ่งอาจเป็นหน่วยงานในลักษณะ Certified Body หรือ หน่วยงานควบคุมหรือกำกับดูแล เป็นต้น

4.2.5 ด้านการจัดการเหตุการณ์ (Event/Incident)

- สกมช. ควรจัดให้มีกลไกการจัดการเหตุการณ์ กรณีเกิดขึ้นต่อข้อมูลหรือระบบสารสนเทศบนระบบคลาวด์ ทั้งกลไกในระดับประเทศ ระดับภาคส่วน และระดับหน่วยงาน

- สกมช. ควรกำหนดนิยาม บทบาท และหน้าที่ของหน่วยงานที่เกี่ยวข้องให้ชัดเจน กรณีเกิดเหตุภัยคุกคามทางไซเบอร์ต่อข้อมูลหรือระบบสารสนเทศบนระบบคลาวด์

- กลไกการจัดการเหตุการณ์ดังกล่าว ควรมีขั้นตอนการจัดการเหตุการณ์โดยละเอียด พร้อมการรายงานที่ทันเวลา และควรมีความสอดคล้องกับมาตรฐานสากลด้วย

# บทที่ 5 กรอบการดำเนินงาน

## 5.1 วัตถุประสงค์

(1) เพื่อผลักดันให้เกิดการดำเนินการตามประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 อย่างรวดเร็ว สะดวก และมีประสิทธิภาพ

(2) เพื่อยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ทั้งในส่วนของผู้ใช้บริการคลาวด์ (Cloud Service Customer) และผู้ให้บริการคลาวด์ (Cloud Service Provider)

(3) เพื่อให้เกิดการบูรณาการการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ระหว่าง สกมช. กับหน่วยงานที่เกี่ยวข้อง

## 5.2 ประโยชน์

(1) ลดความพยายามที่ซ้ำซ้อน ความไม่สอดคล้องกัน และความไม่มีประสิทธิภาพด้านต้นทุน

(2) สร้างความร่วมมือระหว่างภาครัฐและเอกชนเพื่อส่งเสริมนวัตกรรมและความก้าวหน้าของการประมวลผลคลาวด์ที่มีความปลอดภัยมากขึ้น

(3) ช่วยให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถเร่งการนำการประมวลผลคลาวด์มาใช้ โดยมีกระบวนการที่โปร่งใส และมีการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

## 5.3 หลักการสำคัญที่เกี่ยวข้อง

(1) ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

(2) ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

(3) ประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566

(4) ประกาศ กมช. เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564

(5) ประกาศ กกม. เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. 2567

(6) ประกาศ สกมช. เรื่อง แนวทางการจัดทำแผนการรักษาความมันคงปลอดภัยไซเบอร์ พ.ศ. 2567

**5.4 ผู้ที่เกี่ยวข้อง**

| ลำดับ | ผู้ที่เกี่ยวข้อง | คำอธิบาย |
|---|---|---|
| 1. | คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) | มีหน้าที่และอำนาจตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่เกี่ยวข้องได้แก่<br>มาตรา 9 (4) กำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน |
| 2. | คณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) | มีหน้าที่และอำนาจ<br>1. ส่งเสริมการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy)<br>2. จัดทำนโยบายที่เกี่ยวข้องกับการใช้คลาวด์ โครงสร้างการบริหาร แนวทางการบริหารจัดการด้านการจัดซื้อจัดจ้าง การบริหารจัดการข้อมูล กระบวนการในการเลือกใช้คลาวด์ การโอนย้ายระบบงานของภาครัฐ และเสนอต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ และคณะกรรมการพัฒนารัฐบาลดิจิทัล<br>3. เสนอแนะต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ และคณะกรรมการพัฒนารัฐบาลดิจิทัล เกี่ยวกับการดำเนินงานตามแนวทางการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) รวมทั้งเสนอมาตรการในการดำเนินการ และแก้ไขปัญหาอุปสรรคในการปฏิบัติการตามนโยบายดังกล่าว<br>4. กำกับดูแล ติดตาม และประเมินผลการดำเนินการตามแนวทางการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ของทุกภาคส่วนที่เกี่ยวข้อง และการส่งเสริมเศรษฐกิจดิจิทัลตามหมวด 5 ภายในขอบเขตอำนาจของคณะกรรมการเฉพาะด้านแล้วรายงานผลการดำเนินงานต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ และคณะกรรมการพัฒนารัฐบาลดิจิทัล<br>5. เชิญหน่วยงานของรัฐหรือบุคคลใดมาให้ข้อเท็จจริง ความเห็นหรือคำแนะนำ ตลอดจนส่งเอกสารหรือหลักฐานที่เกี่ยวข้องเพื่อประกอบการดำเนินงานได้ |

| ลำดับ | ผู้ที่เกี่ยวข้อง | คำอธิบาย |
|---|---|---|
| | | 6. แต่งตั้งคณะอนุกรรมการเพื่อปฏิบัติการอย่างใดอย่างหนึ่งตามที่คณะกรรมการเฉพาะด้านมอบหมาย<br>7. ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการดิจิทัลเพื่อเศรษฐกิจ และสังคมแห่งชาติ มอบหมายหรือตามที่มีกฎหมาย กำหนดให้เป็นหน้าที่ของคณะกรรมการเฉพาะด้าน |
| 3. | คณะกรรมการพัฒนารัฐบาลดิจิทัล | มีหน้าที่ดำเนินการกำหนดรายละเอียดที่เกี่ยวข้องกับนโยบายการใช้คลาวด์ การออกประกาศเพื่อกำหนดหลักเกณฑ์ และมาตรฐานประสานงานกับหน่วยงานที่เกี่ยวข้อง พัฒนาระบบบริหารจัดการความต้องการ และจัดหาคลาวด์ กำกับดูแลสร้างระบบนิเวศ และจัดซื้อจัดจ้าง ตามกรอบนโยบายที่ได้รับอนุมัติจากคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ รวมทั้งกรอบกฎหมายของหน่วยงานรัฐที่เกี่ยวข้อง |
| 4. | คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) | มีหน้าที่และอำนาจตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่เกี่ยวข้องได้แก่<br>มาตรา 53 ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน หากพบว่าหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่ได้มาตรฐาน ให้หน่วยงานควบคุมหรือกำกับดูแลนั้นรีบแจ้งให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ต่ำกว่ามาตรฐานแก้ไขให้ได้มาตรฐานโดยเร็ว หากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นยังคงเพิกเฉยไม่ดำเนินการ หรือไม่ดำเนินการให้แล้วเสร็จภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด ให้หน่วยงานควบคุมหรือกำกับดูแลส่งเรื่องให้ กกม. พิจารณาโดยไม่ชักช้า<br>เมื่อได้รับคำร้องเรียนตามวรรคหนึ่ง หาก กกม. พิจารณาแล้วเห็นว่ามีเหตุดังกล่าวและอาจทำให้เกิดภัยคุกคามทางไซเบอร์ ให้ กกม. ดำเนินการ ดังต่อไปนี้<br>(1) กรณีเป็นหน่วยงานของรัฐ ให้แจ้งต่อผู้บริหารระดับสูงสุดของหน่วยงานเพื่อใช้อำนาจในทางบริหาร สั่งการไปยังหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นเพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว |

| ลำดับ | ผู้ที่เกี่ยวข้อง | คำอธิบาย |
|---|---|---|
| | | (2) กรณีเป็นหน่วยงานเอกชน ให้แจ้งไปยังผู้บริหารระดับสูงสุดของหน่วยงาน ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นเพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว<br>ให้เลขาธิการดำเนินการติดตามเพื่อให้เป็นไปตามความในวรรคสองด้วย |
| 5. | สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ | มีหน้าที่และอำนาจตามมาตรา 22 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่เกี่ยวข้องได้แก่<br>มาตรา 22 (7) ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ หรือตามคำสั่งของคณะกรรมการ<br>มาตรา 22 (11) เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ<br>มาตรา 22 (14) ส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ |
| 6. | ผู้ใช้บริการคลาวด์ (Cloud Service Customer) | หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่มีข้อตกลงทางสัญญาอย่างเป็นทางการในการใช้บริการคลาวด์ที่ให้บริการโดยผู้ให้บริการคลาวด์ |
| 7. | ผู้ให้บริการคลาวด์ (Cloud Service Provider) | หน่วยงานของรัฐหรือเอกชนที่ทำให้บริการคลาวด์สามารถใช้ได้กับผู้ใช้บริการคลาวด์รวมถึงจัดการทรัพยากรเหล่านี้เพื่อให้มั่นใจว่ามีความพร้อมใช้งาน ความมั่นคงปลอดภัย และความสามารถในการขยายตัวสำหรับผู้ใช้บริการคลาวด์ของตน |
| 8. | หน่วยงานให้บริการตรวจรับรอง (Certify Body) | หน่วยงานให้บริการตรวจรับรองในระดับขั้นก้าวหน้า หรือสูงกว่าตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการ |

| ลำดับ | ผู้ที่เกี่ยวข้อง | คำอธิบาย |
|---|---|---|
| | | ให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566 ทั้งนี้ ในช่วงแรกของการดำเนินการที่สำนักงานยังมิได้ให้การรับรองหน่วยงานให้บริการตรวจรับรอง อาจดำเนินการโดยหน่วยงานให้บริการตรวจรับรองตามมาตรฐานสากลที่สำนักงานประกาศกำหนด ก็ได้ |
| 9. | ผู้ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Cloud Security Auditor) | บุคคลที่ทำหน้าที่ประเมินและตรวจสอบความปลอดภัยของระบบคลาวด์สำหรับผู้ใช้บริการคลาวด์ (Cloud Service Customer) หรือผู้ให้บริการคลาวด์ (Cloud Service Provider) ทั้งนี้ ผู้ตรวจสอบอาจใช้เกณฑ์การตรวจตามประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 หรือแนวปฏิบัติสากล รวมถึงจะต้องมีความรู้ความเข้าใจเกี่ยวกับกระบวนการตรวจสอบ (Audit Process) ที่ได้มาตรฐานด้วย |
| 10. | ผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Cloud Security Professional) | ผู้เชี่ยวชาญที่ทำหน้าที่ปกป้องข้อมูล ระบบ และแอปพลิเคชันต่าง ๆ ที่อยู่บนระบบคลาวด์ จากภัยคุกคามทางไซเบอร์และการเข้าถึงโดยไม่ได้รับอนุญาต สามารถบริหารความเสี่ยงทางไซเบอร์เพื่อวางแผนรับมือกับภัยคุกคามดังกล่าวได้ รวมทั้งสามารถพัฒนาและปรับปรุงระบบรักษาความปลอดภัยให้มีประสิทธิภาพและทันสมัย |

**5.5 กรอบแนวทางการทำงาน**

เนื่องจากประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ข้อ 2 ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสองปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป ประกอบกับการดำเนินการตามมาตรฐานฉบับนี้เกี่ยวข้องกับหน่วยงานจำนวนมาก ดังนั้น การเตรียมการเพื่อให้ทุกส่วนที่เกี่ยวข้องมีความพร้อมในการดำเนินการตามมาตรฐานฉบับนี้ได้อย่างรวดเร็ว สะดวก และมีประสิทธิภาพ สามารถยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ทั้งในส่วนของผู้ใช้บริการคลาวด์ (Cloud Service Customer) และผู้ให้บริการคลาวด์ (Cloud Service Provider) รวมถึงเกิดการบูรณาการการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ระหว่าง สกมช. กับหน่วยงานที่เกี่ยวข้อง สกมช. จึงได้จัดทำกรอบแนวทางการทำงานเพื่อใช้ขับเคลื่อนการเตรียมการร่วมกับหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชน ซึ่งจะส่งผลให้สามารถบรรลุผลได้อย่างมีประสิทธิภาพ และประสิทธิผล โดยมีรายละเอียดดังนี้

(1) ขั้นกำหนดความต้องการร่วมกัน (Mutually identify the preliminary national cloud security requirements) โดยความต้องการนี้คือสิ่งที่หน่วยงานต่าง ๆ ที่เกี่ยวข้องจำเป็นต้องใช้ในการนำมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ไปสู่การปฏิบัติ เช่น

(1.1) หลักเกณฑ์และวิธีการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้าง

พื้นฐานสำคัญทางสารสนเทศ ตามมาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

(1.2) หลักเกณฑ์และวิธีการแบ่งความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับการประมวลผลคลาวด์ (Security responsibilities within the shared responsibility model between cloud service customer and cloud service providers)

(1.3) หลักเกณฑ์และวิธีการตรวจรับรองโดยการประเมินตนเอง (Self-assessment)

(1.4) หลักเกณฑ์และวิธีการตรวจรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation)

(1.5) หลักเกณฑ์และวิธีการตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body)

(1.6) หลักเกณฑ์และวิธีการตรวจรับรองโดย สกมช. ให้กับหน่วยงานให้บริการตรวจรับรอง

(1.7) ประกาศ สกมช. เรื่อง หน่วยงานให้บริการตรวจรับรองตามมาตรฐานสากล

(1.8) คำสั่ง สกมช. เรื่อง แต่งตั้งคณะกรรมการคัดเลือกหน่วยงานให้บริการตรวจรับรองตามมาตรฐานสากล

(1.9) แนวปฏิบัติประกอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

(1.10) เครื่องมือ และเอกสารต้นแบบ (Templates)

(1.11) บุคลากรผู้ทำหน้าที่ผู้ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Cloud Security Auditor) และผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Cloud Security Professional)

(1.12) แพลตฟอร์มกลางหรือระบบฐานข้อมูลเพื่อสนับสนุนหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(1.13) กรอบการบริหารความเสี่ยงทางไซเบอร์ต่อระบบคลาวด์สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Risk Management Framework for Cloud Security)

(1.14) ความเชื่อมโยงระหว่างมาตรฐานฉบับนี้กับเอกสารอื่นที่เกี่ยวข้อง ทั้งภายในและระหว่างประเทศ

(1.15) โมเดลสถาปัตยกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(1.16) จัดทำเอกสาร White paper เพื่ออธิบายประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามมาตรฐานฉบับนี้ รวมถึงกฎหมายลำดับรองอื่น ๆ ที่เกี่ยวข้อง

(1.17) ทีมเฉพาะกิจจาก สกมช. มีหน้าที่ดำเนินการและประสานงานในการแก้ไขปัญหาและอุปสรรคต่าง ๆ

ทั้งนี้ สกมช. อาจจัดทำรายการความต้องการขั้นต้น แล้วแจ้งเวียนไปยังหน่วยงานที่เกี่ยวข้องเพื่อให้แสดงความคิดเห็น ระบุความต้องการ จัดลำดับความสำคัญ โดยแยกตามบทบาทหน้าที่หรือความเกี่ยวข้องกับมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 จากนั้นจะดำเนินการประมวลผลเพื่อใช้ในการดำเนินการในขั้นต่อไป

(2) ขั้นจัดลำดับความสำคัญ (Prioritize the national cloud security requirements) เนื่องจากความต้องการอาจมีจำนวนมาก ในขณะที่ทรัพยากรของหน่วยงานต่างๆ มีอย่างจำกัด รวมถึงมาตรฐานฉบับนี้ให้ใช้บังคับเมื่อพ้นกำหนดสองปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป ดังนั้น การจัดลำดับความสำคัญจึงมีความจำเป็นอย่างมากเพื่อให้เกิดความมั่นใจว่าสิ่งที่จำเป็นต้องดำเนินการจะได้รับการจัดสรรทรัพยากรอย่างเพียงพอ และสามารถดำเนินการจนบรรลุผลได้อย่างทันเวลา ทั้งนี้ สกมช. อาจดำเนินการในขั้นนี้โดยการแจ้งเวียนผลสรุปจากการดำเนินการในขั้นกำหนดความต้องการขั้นต้นร่วมกัน เพื่อให้ทุกส่วนที่เกี่ยวข้องได้เห็นภาพรวมของการดำเนินการ โดยอาจระบุหน่วยงานเจ้าภาพร่วมกับ สกมช. ด้วย จากนั้นจึงประกาศเผยแพร่ให้กับทุกภาคส่วนนำไปใช้ในการอ้างอิง จัดทำแผนรองรับ รวมถึงสื่อสารให้กับผู้บริหารระดับสูง และหน่วยงานต่างประเทศ รับทราบและเข้าใจไปในแนวทางเดียวกัน

(3) ขั้นจัดทำแผน (Plan) ในขั้นนี้ สกมช. จะมีการจัดทำแผนบูรณาการเพื่อขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 โดยอาจทำเป็นแผนระยะ 5 ปี โดยระบุยุทธศาสตร์ เป้าหมายของยุทธศาสตร์ กลยุทธ์ เป้าหมายของกลยุทธ์ ตัวชี้วัด/ค่าเป้าหมาย โครงการ/กิจกรรม/แผนงาน และหน่วยรับผิดชอบซึ่งอาจครอบคลุมทั้งหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่นๆ ที่เกี่ยวข้องทั้งภายในและต่างประเทศ จากนั้น อาจพิจารณาขออนุมัติต่อ กมช. หรือคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) รวมถึง ครม. ต่อไป โดยมีตัวอย่าง ดังนี้

(3.1) ยุทธศาสตร์ที่ 1 รวมพลังภาครัฐและเอกชน โดยสร้างเครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จากภาครัฐและเอกชน ทั้งภายในและต่างประเทศ ในลักษณะอาสาสมัคร (Voluntary) เพื่อจัดทำประกาศ คำสั่ง หลักเกณฑ์และวิธีการ ตามมาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 รวมถึงกฎหมายอื่นที่เกี่ยวข้อง ซึ่งจะทำให้ได้ผลผลิตที่รวดเร็ว ตรงตามความต้องการ โดยทุกภาคส่วนที่เกี่ยวข้องได้มีส่วนร่วมในการดำเนินการ และสอดคล้องกับมาตรฐาน ข้อกำหนด ระเบียบ ข้อบังคับของหน่วยงานควบคุมหรือกำกับดูแล รวมถึงมาตรฐานสากลด้วย

(3.2) ยุทธศาสตร์ที่ 2 สร้างสภาพแวดล้อมที่เอื้อต่อการดำเนินการตามมาตรฐาน ผ่านโครงการ/กิจกรรม/แผนงานต่าง ๆ เช่น การพัฒนากลไกการตรวจรับรองมาตรฐาน การเปิดบริการตรวจรับรองโดย สกมช. ให้กับหน่วยงานให้บริการตรวจรับรอง การพัฒนากลไกการกำกับดูแลโดยหน่วยงานควบคุมหรือกำกับดูแล การลดอุปสรรคในการดำเนินการให้กับผู้ให้บริการคลาวด์ทั้งภายในและต่างประเทศ การส่งเสริมให้เกิดความโปร่งใสตามหลักการและมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การพัฒนากลไกการศึกษาอบรม การสร้างความร่วมมือกับหน่วยงานหรือผู้ให้บริการจากต่างประเทศ (CSA, ISO, NIST, etc.)

(3.3) ยุทธศาสตร์ที่ 3 พัฒนาขีดความสามารถของหน่วยงานและบุคลากร ผ่านโครงการ/กิจกรรม/แผนงานต่างๆ เช่น การพัฒนาผู้ใช้บริการคลาวด์ (Cloud Service Customer) และผู้ให้บริการคลาวด์ (Cloud Service Provider) ผ่านการอบรมหลักสูตร Lead auditor/implementor หรือ Cloud security professional การให้คำปรึกษาผ่าน NCSA Cyber Clinic (SMART) บริการ Cloud security health check ช่องทางสอบถามข้อสงสัยเกี่ยวกับการ implement มาตรฐาน cloud การประเมินตนเอง (Self-assessment) เป็นต้น

(4) ขั้นดำเนินการตามแผน (Execute) ในขั้นนี้ จะเป็นการดำเนินการตามแผนดังที่ได้กล่าวมาแล้วในข้อ (3) โดยในระหว่างดำเนินการ สกมช. อาจจัดตั้งทีมเฉพาะให้มีหน้าที่ดำเนินการและประสานงานในการแก้ไขปัญหาและอุปสรรคต่าง ๆ โดยจะอยู่ภายใต้การบังคับบัญชาของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และการกำกับดูแลโดย กกม. และ กมช. รวมถึงความสอดคล้องกับทิศทางที่กำหนดโดยคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ด้วย

(5) ขั้นประเมินผลอย่างต่อเนื่อง (Evaluate) เนื่องจากกิจกรรมที่จะต้องดำเนินการตามกรอบแนวทาง รวมถึงแผนบูรณาการเพื่อขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 มีระยะเวลาที่จำกัด ดังนั้น จึงจำเป็นที่ สกมช. จะต้องมีการประเมินผลการดำเนินการอย่างใกล้ชิดและต่อเนื่อง และอาจมีความจำเป็นต้องปรับแผนการดำเนินการ เพื่อให้สอดคล้องกับนโยบายที่กำหนดโดยคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ด้วย ทั้งนี้ สกมช. อาจมีการเผยแพร่แผนการดำเนินการหรือกิจกรรมที่มีการเปลี่ยนแปลงในแพลตฟอร์มกลางหรือระบบฐานข้อมูลเพื่อสนับสนุนหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยขึ้นอยู่กับงบประมาณที่ได้รับการสนับสนุนด้วย