ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง แผนบูรณาการเพื่อขับเคลื่อนการดำเนินการตามมาตรฐาน
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์
พ.ศ. ๒๕๖๙ - ๒๕๗๓

เพื่อให้หน่วยงานที่เกี่ยวข้องตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ สามารถดำเนินการได้อย่างมีประสิทธิภาพ และยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ทั้งในส่วนของผู้ใช้บริการคลาวด์ และผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง อันจะนำไปสู่การบูรณาการการดำเนินงานร่วมกันอย่างเป็นรูปธรรม

อาศัยอำนาจตามความในข้อ ๗ ของประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๒/๒๕๖๙ เมื่อวันที่ ๒๗ กรกฎาคม ๒๕๖๙ เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แผนบูรณาการเพื่อขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๙ - ๒๕๗๓”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันประกาศเป็นต้นไป

ข้อ ๓ เพื่อประโยชน์ในการดำเนินการตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ ให้มีประสิทธิภาพ โดยให้หน่วยงานผู้ใช้บริการคลาวด์ และหน่วยงานผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง นำแผนบูรณาการตามแนบท้ายประกาศนี้ มาใช้เป็นแนวทางในการดำเนินการของตน

ข้อ ๔ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์ หรือวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีอำนาจตีความและวินิจฉัยชี้ขาดแล้วรายงานให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทราบ ทั้งนี้ การตีความ และคำวินิจฉัยของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้เป็นที่สุด

ประกาศ ณ วันที่ ๗ สิงหาคม พ.ศ. ๒๕๖๙

พลอากาศตรี

(อมร ชมเชย)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

แผนบูรณาการเพื่อขับเคลื่อนการดำเนินการตามมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2569-2573

แผนบูรณาการเพื่อขับเคลื่อน
การดำเนินการตามมาตรฐานด้านการรักษา
ความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์
พ.ศ. 2569-2573

เวอร์ชัน 1.0

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คำนำ

ในปัจจุบันการขับเคลื่อนประเทศสู่รัฐบาลดิจิทัลและเศรษฐกิจดิจิทัลได้ส่งผลให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงภาคเอกชน มีการนำระบบคลาวด์มาใช้เป็นโครงสร้างพื้นฐานหลักในการจัดเก็บข้อมูล การพัฒนาระบบ และการให้บริการสาธารณะอย่างแพร่หลาย อย่างไรก็ตาม การพึ่งพาระบบคลาวด์ที่เพิ่มขึ้นย่อมทำให้ความเสี่ยงและภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล มีความซับซ้อนและขยายตัวมากยิ่งขึ้น ซึ่งอาจส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศและบริการภาครัฐที่สำคัญ เศรษฐกิจ สังคม และความมั่นคงของประเทศ รวมถึงความเชื่อมั่นของประชาชน

เพื่อรองรับการเปลี่ยนแปลงดังกล่าว สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จึงได้ออกประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 โดยระบุข้อกำหนดขั้นต่ำในการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ สำหรับผู้ใช้บริการคลาวด์ และผู้ให้บริการคลาวด์ ซึ่งจะมีผลบังคับใช้ในวันที่ 10 กันยายน 2569 ทั้งนี้ เพื่อสนับสนุนการบังคับใช้มาตรฐานให้เกิดผลในทางปฏิบัติอย่างเป็นรูปธรรม สกมช. ได้จัดทำกรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Thailand's National Cloud Security Framework) เพื่อเป็นแนวทางในการเตรียมความพร้อมของทุกภาคส่วนอย่างเป็นระบบและรองรับการขับเคลื่อนเชิงบูรณาการในระยะยาว

ดังนั้น แผนบูรณาการเพื่อขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2569-2573 จึงได้ถูกจัดทำขึ้นโดยมีวัตถุประสงค์ในการบูรณาการความร่วมมือจากหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ หน่วยงานตรวจรับรองคุณภาพ ผู้เชี่ยวชาญ และหน่วยงานที่เกี่ยวข้อง เพื่อร่วมกันขับเคลื่อนการปฏิบัติตามยุทธศาสตร์ กลยุทธ์ โครงการ และตัวชี้วัด ซึ่งจะทำให้การดำเนินงานตามมาตรฐานดังกล่าวเกิดความชัดเจน มีประสิทธิภาพ และลดความซ้ำซ้อนในการดำเนินการ รวมถึงสอดคล้องกับแนวโน้มภัยคุกคามทางไซเบอร์ที่มีต่อประเทศไทยอีกด้วย

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สารบัญ

หน้า

บทที่ 1
บทสรุปผู้บริหาร

ในปัจจุบันบริบทการพัฒนาประเทศได้ก้าวเข้าสู่ยุคดิจิทัลอย่างเต็มรูปแบบ หน่วยงานภาครัฐ ภาคเอกชน และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต่างปรับเปลี่ยนรูปแบบการดำเนินงาน โดยนำเทคโนโลยีระบบคลาวด์ (Cloud Computing) มาประยุกต์ใช้ในการจัดเก็บข้อมูลและประมวลผล เพื่อเพิ่มประสิทธิภาพและความยืดหยุ่นในการให้บริการ โดยสอดคล้องกับนโยบายการใช้คลาวด์เป็นหลักของรัฐบาล อย่างไรก็ตาม การเปลี่ยนแปลงทางเทคโนโลยีดังกล่าวนำมาซึ่งความเสี่ยงและภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและรุนแรงยิ่งขึ้น ซึ่งสามารถส่งผลกระทบต่อความมั่นคงของชาติและความเชื่อมั่นของประชาชน ด้วยเหตุนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จึงได้ออกประกาศมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อการใช้บริการคลาวด์สาธารณะให้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ เพื่อให้หน่วยงานต่าง ๆ มีความพร้อมและสามารถปฏิบัติงานได้สอดคล้องกับมาตรฐานดังกล่าวก่อนที่จะมีผลบังคับใช้ในปี พ.ศ. 2569 จึงมีความจำเป็นต้องจัดทำแผนบูรณาการเพื่อขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ฉบับนี้ขึ้น เพื่อใช้เป็นกรอบแนวทางการดำเนินงานที่มีเอกภาพและเป็นไปในทิศทางเดียวกันทั้งประเทศ

การจัดทำแผนบูรณาการฯ ฉบับนี้ ยึดหลักการตามสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย (Thailand's National Cloud Security Architecture) ซึ่งถูกออกแบบมาเพื่อแก้ไขปัญหาความซ้ำซ้อนในการดำเนินงาน ลดความไม่สอดคล้องของการดำเนินงาน และเพิ่มประสิทธิภาพในการใช้งบประมาณ รวมทั้งได้กำหนดวิสัยทัศน์การรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย ยุทธศาสตร์ กลยุทธ์ เป้าหมายของกลยุทธ์ ตัวชี้วัด/ค่าเป้าหมาย โครงการ/กิจกรรม/แผนงาน หน่วยรับผิดชอบ และระยะเวลาในการดำเนินการ ให้สอดคล้องกันด้วย

ในการขับเคลื่อนแผนบูรณาการฯ ไปสู่การปฏิบัติอย่างเป็นรูปธรรม ได้กำหนดกรอบการดำเนินงานผ่าน 3 ยุทธศาสตร์หลัก โดยยุทธศาสตร์ที่ 1 มุ่งเน้นการรวมพลังภาครัฐและเอกชน เพื่อสร้างกลไกความร่วมมือที่เข้มแข็ง โดยจะมีการจัดตั้งเครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ระดับชาติ ขึ้นมาทำหน้าที่สนับสนุนทางวิชาการ แลกเปลี่ยนองค์ความรู้ และร่วมกันทบทวนหลักเกณฑ์มาตรฐาน และแนวปฏิบัติ ให้มีความทันสมัยและสอดคล้องกับบริบทของประเทศ รวมถึงการส่งเสริมความร่วมมือระหว่างประเทศกับองค์กรชั้นนำ เพื่อนำมาตรฐานสากลมาปรับใช้และยกระดับกระบวนการทำงานของไทยให้เป็นที่ยอมรับ

ยุทธศาสตร์ที่ 2 มุ่งเน้นการสร้างสภาพแวดล้อมที่เอื้อต่อการดำเนินการ โดยให้ความสำคัญกับการพัฒนาระบบนิเวศของการตรวจรับรองที่มีความโปร่งใสและตรวจสอบได้ ซึ่งครอบคลุมถึงการจัดทำมาตรฐานและแนวทางปฏิบัติ กลไกการกำกับดูแลโดยหน่วยงานที่เกี่ยวข้องกับการกำหนดนโยบาย (Policy Agencies) และหน่วยงานควบคุมหรือกำกับดูแล (Regulator) การพัฒนาหน่วยงานให้บริการตรวจรับรอง (Certify Body) ให้มีคุณภาพตามเกณฑ์มาตรฐานสากล นอกจากนั้นยังจะมีการพัฒนาแพลตฟอร์มกลางเพื่อใช้เป็นศูนย์รวมข้อมูลในการลงทะเบียน ติดตามสถานะการตรวจประเมิน และเผยแพร่รายชื่อผู้ให้บริการคลาวด์ที่ผ่านการรับรองให้สาธารณชนรับทราบ อันเป็นการสร้างความเชื่อมั่นให้กับผู้ใช้บริการและส่งเสริมความโปร่งใสในกระบวนการกำกับดูแล

ยุทธศาสตร์ที่ 3 มุ่งเน้นการพัฒนาขีดความสามารถของหน่วยงานและบุคลากร เพื่อเตรียมความพร้อมด้านทรัพยากรบุคคลและโครงสร้างการทำงานภายในองค์กร โดยจะดำเนินการพัฒนาหลักสูตรฝึกอบรมและกำหนดเส้นทางอาชีพด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ที่ชัดเจน นอกจากนี้จะมีการให้บริการที่ปรึกษาผ่าน NCSA Cyber Clinic เพื่อสนับสนุนให้หน่วยงานยกระดับความพร้อมด้านความมั่นคงปลอดภัยได้ด้วยตนเอง

สุดท้ายเพื่อให้การดำเนินงานตามแผนบูรณาการฯ บรรลุผลสัมฤทธิ์ตามเป้าหมายที่กำหนดไว้ ได้มีการวางระบบการกำกับดูแลและติดตามประเมินผลอย่างเป็นขั้นตอน โดยจัดให้มีคณะทำงานทำหน้าที่กำกับทิศทางและติดตามความก้าวหน้าของการดำเนินงานในแต่ละยุทธศาสตร์ รวมถึงกำหนดให้มีการรายงานผลการดำเนินงานเป็นระยะ และการประเมินผลเมื่อสิ้นสุดแผน เพื่อนำข้อมูลที่ได้มาวิเคราะห์และปรับปรุงแนวทางการดำเนินงานให้สอดคล้องกับสถานการณ์ภัยคุกคามและเทคโนโลยีที่เปลี่ยนแปลงไป ซึ่งจะช่วยให้ประเทศไทยมีระบบนิเวศด้านคลาวด์ที่มั่นคงปลอดภัย รองรับการพัฒนาเศรษฐกิจและสังคมดิจิทัลได้อย่างยั่งยืนต่อไป

บทที่ 2
บทนำ

2.1 หลักการและเหตุผล

ปัจจุบันภัยคุกคามทางไซเบอร์มีความซับซ้อนและทวีความรุนแรงมากขึ้น ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล ระบบสารสนเทศ และการดำเนินงานที่สำคัญของประเทศ ทั้งภาครัฐ ภาคเอกชน และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต่างเผชิญกับความเสี่ยงที่อาจก่อให้เกิดความเสียหายต่อความมั่นคง เศรษฐกิจ และสังคมโดยรวม ประเทศไทยจึงจำเป็นต้องมีกรอบกฎหมายและแนวทางปฏิบัติที่ชัดเจน เพื่อยกระดับมาตรการในการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากเหตุการณ์ทางไซเบอร์อย่างมีประสิทธิภาพทันต่อสถานการณ์ ตลอดจนเสริมสร้างความพร้อมและความเข้มแข็งของหน่วยงานที่เกี่ยวข้องในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็วและมีประสิทธิภาพ และเป็นไปในทิศทางเดียวกันสอดคล้องกับมาตรฐานสากล เพื่อสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ต่อมาจึงมีประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 เพื่อประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นแก่ข้อมูลหรือระบบสารสนเทศอันจะนำไปสู่การเลือกมาตรการในการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม เพื่อให้การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ และมีประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566 เพื่อกำหนดมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์และการรับรองคุณภาพของผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงกำหนดแนวทางส่งเสริมพัฒนาการให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การปฏิบัติงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

ต่อมาเมื่อหน่วยงานของรัฐ ภาคเอกชน และประชาชนทั่วไปมีการนำเทคโนโลยีระบบคลาวด์ (Cloud Computing) มาใช้ในการจัดเก็บข้อมูล ประมวลผล และให้บริการทางอิเล็กทรอนิกส์อย่างแพร่หลาย เนื่องจากคุณสมบัติของระบบคลาวด์มีความยืดหยุ่น ประหยัดค่าใช้จ่าย และสามารถขยายขีดความสามารถของระบบได้อย่างรวดเร็ว ทำให้สามารถรองรับการเปลี่ยนแปลงของการทำงานในปัจจุบันได้อย่างมีประสิทธิภาพ รวมถึงมีการผลักดันนโยบายการใช้คลาวด์เป็นหลัก ซึ่งมีเจตนามุ่งให้หน่วยงานของรัฐให้ความสำคัญกับการใช้บริการคลาวด์เป็นอันดับแรก นโยบายนี้ได้ถูกใช้เป็นเครื่องมือสำคัญในการเปลี่ยนผ่านสู่รัฐบาลดิจิทัลและเศรษฐกิจดิจิทัลของประเทศ อย่างไรก็ตาม การเปลี่ยนแปลงอย่างรวดเร็วของผู้ใช้งานจากการใช้เทคโนโลยีแบบดั้งเดิมเปลี่ยนมาใช้เทคโนโลยีคลาวด์ก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ การคุ้มครอง

ข้อมูลส่วนบุคคล และการกำกับดูแลข้อมูลของรัฐ ซึ่งสามารถส่งผลกระทบต่อความมั่นคงของประเทศ และความเชื่อมั่นของประชาชน หากไม่มีกรอบกฎหมายและมาตรฐานกลางที่ชัดเจนในการกำกับดูแล เมื่อการใช้งานเทคโนโลยีคลาวด์กลายเป็นโครงสร้างพื้นฐานที่จำเป็นของบริการดิจิทัล โครงสร้างพื้นฐานสำคัญทางสารสนเทศและบริการสาธารณะของประเทศมีความต้องการที่จะย้ายขึ้นสู่ระบบคลาวด์มากขึ้น รวมถึงความสำคัญของระบบคลาวด์ที่มีมากขึ้นและปัญหาภัยคุกคามทางไซเบอร์ที่มีรูปแบบเปลี่ยนไป

เพื่อให้การใช้บริการคลาวด์ของหน่วยงานภาครัฐและเอกชนเป็นไปอย่างมั่นคงปลอดภัย มีประสิทธิภาพ และสอดคล้องกับหลักธรรมาภิบาลข้อมูล ตลอดจนเพื่อสร้างความเชื่อมั่นให้แก่ผู้ใช้บริการและผู้ให้บริการคลาวด์ทั้งในและต่างประเทศ จึงมีความจำเป็นต้องมีมาตรการทางกฎหมายเพื่อควบคุมการใช้งานระบบคลาวด์ เพื่อกำหนดหลักเกณฑ์ มาตรการ และมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และการบริหารจัดการข้อมูลภาครัฐให้เป็นไปในทิศทางเดียวกัน ทั้งนี้ เพื่อให้ประเทศไทยมีระบบนิเวศด้านคลาวด์ที่มั่นคง ปลอดภัย และรองรับการพัฒนาเศรษฐกิจและสังคมดิจิทัลอย่างยั่งยืน

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่และอำนาจในการกำหนดมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ ด้วยความสำคัญของระบบคลาวด์ที่มีต่อหน่วยงานมากขึ้น จึงมีประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 เพื่อให้การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ โดยกำหนดแนวทางเฉพาะสำหรับการใช้บริการคลาวด์ได้อย่างปลอดภัย ทั้งในด้านเทคนิค การบริหารจัดการ และการกำกับดูแล โดยมาตรฐานได้มุ่งเน้นผู้ให้บริการและผู้ใช้บริการคลาวด์ต้องมีมาตรการด้านการป้องกัน การตรวจจับ การตอบสนอง และการกู้คืนระบบ

นอกจากนั้น เพื่อให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง มีการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์เป็นไปอย่างมีประสิทธิภาพ จึงได้มีประกาศ สกมช. เรื่อง กรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Thailand's National Cloud Security Framework) ที่สามารถใช้เป็นกรอบในการเตรียมความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ประกอบร่วมกับประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ทำให้เกิดประสิทธิภาพในการรักษาความมั่นคงปลอดภัย มีมาตรฐาน และเท่าทันความก้าวหน้าทางเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็วในปัจจุบัน

ดังนั้น เพื่อเตรียมความพร้อมให้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ หน่วยงานตรวจและให้การรับรอง และหน่วยงานที่เกี่ยวข้องตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 จึงได้ดำเนินการจัดทำ "แผนบูรณาการเพื่อขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2569-2573" เพื่อเป็นเครื่องมือในการหาความสอดคล้องระหว่างกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ และมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ รวบรวมแผนบูรณาการทางด้านสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยบนระบบคลาวด์ และกิจกรรมที่เกี่ยวข้องเพื่อให้สามารถส่งเสริมนโยบายการใช้คลาวด์และยกระดับมาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทยได้อย่างมีประสิทธิภาพ

ซึ่งแผนบูรณาการฉบับนี้มีความสอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565–2570) ยุทธศาสตร์ที่ 3: สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Resilience) กลยุทธ์ที่ 3.2 เรื่อง การกำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ข้อ 2 พัฒนากลไกแนวทางการกำกับดูแลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและพิจารณากำหนดให้ข้อมูลและบริการคลาวด์ (Data & Cloud Computing) เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ต้องมีการกำกับดูแลในระยะต่อไป

พัฒนาการของระบบนิเวศการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์และความท้าทาย

ในปัจจุบันระบบคลาวด์ได้ปฏิวัติมุมมองทางด้านเทคโนโลยีในช่วงสองทศวรรษที่ผ่านมา โดยเปลี่ยนจากการเป็นเพียงแนวคิดทางวิชาการไปสู่โครงสร้างพื้นฐานดิจิทัลที่สำคัญที่สุดของโลก โดยก่อนที่จะมีเทคโนโลยีคลาวด์มีแนวคิดของการทำ Utility Computing การให้บริการทรัพยากรคอมพิวเตอร์แก่ผู้ใช้หลายคนพร้อมกัน แนวคิดนี้เป็นรากฐานสำคัญของการประมวลผลด้วยระบบคลาวด์ มีหลักการคล้ายคลึงกันคือการให้บริการทรัพยากรคอมพิวเตอร์ เช่น พลังการประมวลผล พื้นที่จัดเก็บข้อมูล ตามความต้องการและคิดค่าบริการตามการใช้งานจริง โดยที่ผู้ใช้ไม่จำเป็นต้องเป็นเจ้าของและบำรุงรักษาส่วนประกอบฮาร์ดแวร์ด้วยตนเอง ซึ่งต่อมาแนวคิดนี้ถูกพัฒนามาเป็น Infrastructure as a Service (IaaS) ในปัจจุบัน ได้มีบริษัทที่ริเริ่มการให้เช่าทรัพยากรคอมพิวเตอร์ตามความต้องการของผู้ใช้งาน แม้จะมีความคล้ายคลึงกับระบบคลาวด์แต่บริการของ Utility Computing ยังมีความแตกต่างกับระบบคลาวด์ในปัจจุบันในหลายเรื่อง เช่น โมเดลการคำนวณค่าใช้จ่าย โมเดลในการให้บริการ วิธีการเข้าถึงทรัพยากรยังจำกัดในเครือข่าย รวมถึงยังไม่มีการกำหนดมาตรฐานหรือคุณลักษณะของคลาวด์อย่างชัดเจน

ในเชิงพาณิชย์ ผู้ให้บริการ Amazon Web Services (AWS) ได้เปิดตัว S3 (Simple Storage Service) ในปี ค.ศ. 2006 ตามด้วย EC2 (Elastic Compute Cloud) ถูกมองว่าเป็นจุดกำเนิดที่แท้จริงของโมเดล Infrastructure as a Service (IaaS) รวมถึงเป็นก้าวแรกในการเกิดขึ้นของตลาด Public Cloud ที่สร้างขึ้นเพื่อการใช้งานแบบเปิดสำหรับสาธารณะ

ต่อมาในปี ค.ศ. 2011 หน่วยงาน National Institute of Standards and Technology (NIST) ได้เผยแพร่เอกสาร NIST Special Publication 800-145: The NIST Definition of Cloud Computing ซึ่งปัจจุบันกลายเป็นเอกสารอ้างอิงหลักที่ใช้ในการกำหนดมาตรฐานและกรอบความคิดเกี่ยวกับ Cloud Computing และถูกใช้โดยหน่วยงานรัฐบาลและองค์กรเอกชนทั่วโลกในการทำความเข้าใจและประเมินบริการคลาวด์ โดยที่ได้ให้นิยามอย่างเป็นทางการของ Cloud Computing และอธิบายคุณสมบัติจำเป็น (Essential Characteristics) ของคลาวด์ไว้ 5 ประการ ได้แก่

- On-demand Self-service: ผู้ใช้สามารถจัดสรรทรัพยากรคอมพิวเตอร์ได้เอง ไม่จำเป็นต้องมีเจ้าหน้าที่ผู้ให้บริการ
- Broad Network Access: มีความสามารถในการเข้าถึงผ่านเครือข่ายได้จากหลากหลายอุปกรณ์
- Resource Pooling: ทรัพยากรของผู้ให้บริการถูกรวมไว้เพื่อให้บริการแก่ผู้ใช้หลายราย (Multi-tenant) สามารถจัดสรรและมอบหมายทรัพยากรใหม่ตามความต้องการของผู้ใช้งาน
- Rapid Elasticity: ความสามารถในการขยายและลดขนาดของทรัพยากรได้อย่างยืดหยุ่นและรวดเร็ว
- Measured Service: มีการควบคุมและวัดค่าการใช้ทรัพยากร เพื่อให้เกิดความโปร่งใสในการคิดค่าบริการ

ในเอกสารเผยแพร่ NIST SP 800-145 มีการกำหนดโมเดลการให้บริการ (Service Models) ของคลาวด์ไว้ใน 3 รูปแบบหลัก ได้แก่

• Software as a Service (SaaS) ผู้ใช้เข้าถึงซอฟต์แวร์หรือแอปพลิเคชันผ่านเครือข่าย ผู้ใช้ทำได้เพียงกำหนดค่าที่เกี่ยวข้องกับผู้ใช้เท่านั้น ไม่ต้องจัดการโครงสร้างพื้นฐานหรือแม้แต่ตัวแอปพลิเคชันเอง

• Platform as a Service (PaaS) ผู้ใช้สามารถใช้งานและปรับใช้แอปพลิเคชันที่สร้างขึ้นหรือซื้อมา ผู้ให้บริการจัดเตรียมแพลตฟอร์มสำหรับพัฒนาและรันแอปพลิเคชัน เช่น Runtime, Middleware, Database, API ส่วนผู้ใช้เพียงจัดการแอปพลิเคชันของตนเอง

• Infrastructure as a Service (IaaS) ผู้ใช้เช่าทรัพยากรคอมพิวเตอร์ในระดับโครงสร้างพื้นฐาน เช่น การประมวลผล พื้นที่เก็บข้อมูล และเครือข่าย โดยผู้ใช้ต้องจัดการระบบปฏิบัติการและแอปพลิเคชันเองทั้งหมด

นอกจากนั้น เอกสาร NIST SP 800-145 ได้กำหนดรูปแบบการใช้งานคลาวด์ (Deployment Models) เอาไว้ 4 รูปแบบที่ใช้ในการจัดวางและบริหารจัดการโครงสร้างพื้นฐานคลาวด์ ซึ่งปัจจุบันกลายเป็นกรอบอ้างอิงในการออกแบบสถาปัตยกรรมคลาวด์ ทั้งในหน่วยงานของรัฐ ธุรกิจเอกชน และโครงสร้างพื้นฐานสำคัญของประเทศ โดยแต่ละแบบมีความแตกต่างด้านการแบ่งปันทรัพยากร งบประมาณ และการควบคุมทางกฎหมาย ที่แตกต่างกัน ได้แก่

• Private Cloud: โครงสร้างพื้นฐานคลาวด์ถูกสร้างขึ้นเพื่อการใช้งานเฉพาะขององค์กรเดียว

• Community Cloud: โครงสร้างพื้นฐานคลาวด์ถูกสร้างขึ้นเพื่อการใช้งานร่วมกันของหลายองค์กรที่มีความสนใจและความต้องการด้านความปลอดภัย/กฎระเบียบที่คล้ายกัน

• Public Cloud: โครงสร้างพื้นฐานคลาวด์ถูกสร้างขึ้นเพื่อการใช้งานแบบเปิดสำหรับสาธารณะโดยทั่วไป

• Hybrid Cloud: โครงสร้างพื้นฐานคลาวด์เป็นการผสมผสานระหว่างคลาวด์อย่างน้อยสองประเภทขึ้นไป เช่น Private และ Public ที่ทั้งสองส่วนเป็นอิสระต่อกัน แต่มีการเชื่อมโยงกันด้วยเทคโนโลยีที่ช่วยให้ระบบสามารถเคลื่อนย้ายข้อมูลหรือเวิร์กโหลดข้ามสภาพแวดล้อมได้อย่างยืดหยุ่น

ในด้านมุมมองด้านความปลอดภัย ในช่วงยุคแรกของการใช้งานคลาวด์นี้จะมีความกังวลหลักในด้านความปลอดภัยของข้อมูล (Data Confidentiality) เนื่องจากองค์กรไม่ไว้วางใจที่จะนำข้อมูลสำคัญออกจากศูนย์ข้อมูลของตน นำไปไว้บนเซิร์ฟเวอร์ของบุคคลที่สาม ขณะเดียวกัน ความเสี่ยงจากการโจมตีในยุคแรกยังค่อนข้างต่ำเนื่องจากจำนวนผู้ใช้คลาวด์ยังไม่มาก

ต่อมาผู้ให้บริการรายอื่น เช่น Google และ Microsoft เริ่มเข้ามาแข่งขันในตลาดของคลาวด์ในแต่ละโมเดล ซึ่งผู้ให้บริการเริ่มพัฒนาและขยายบริการจาก Storage, Compute ไปจนถึงการแข่งขันเชิงนวัตกรรมของระบบประมวลผลขั้นสูง เช่น Big Data, AI และ Containerization อย่างต่อเนื่อง การยอมรับการใช้งานระบบคลาวด์มีการเติบโตอย่างรวดเร็ว

เมื่อเวลาผ่านไปการใช้งานคลาวด์ได้รับการตอบรับจากองค์กรมากขึ้น การประยุกต์ใช้งาน Hybrid Cloud ได้รับการยอมรับและกลายเป็นกลยุทธ์หลักที่มีความสำคัญสำหรับองค์กรขนาดใหญ่ เพื่อให้สามารถใช้ประโยชน์จากคุณสมบัติของคลาวด์สาธารณะ ในขณะที่ยังคงสามารถเก็บข้อมูลที่มีความอ่อนไหวไว้ใน Private Cloud หรือ On-Premises ได้ ซึ่งการที่องค์กรมีการยอมรับการใช้คลาวด์อย่างต่อเนื่องทำให้เกิดความกังวลทางด้านการรักษาความปลอดภัยมากขึ้น องค์กรจึงได้ให้ความใส่ใจไปที่เรื่องของการกำกับดูแล (Governance) และการปฏิบัติตามกฎระเบียบ (Compliance) เพราะองค์กรต้องทำให้มั่นใจว่าการใช้คลาวด์เป็นไปตามข้อกฎหมายและข้อบังคับที่กำหนดไว้ในแต่ละประเภทธุรกิจ เช่น HIPAA หรือ PCI DSS

ภายหลังมีการพัฒนาการใช้งานคลาวด์ที่แตกต่างจากเดิมที่เน้นในเรื่องของการย้ายระบบดั้งเดิมขึ้นบนคลาวด์ กลายเป็นการสร้างระบบบนคลาวด์ตั้งแต่เริ่มต้น (Cloud-Native) ซึ่งเป็นการใช้ทรัพยากรคลาวด์เพื่อพัฒนาระบบที่มีความยืดหยุ่นสูง สร้างและรันแอปพลิเคชันที่ใช้ประโยชน์จากความสามารถของคลาวด์อย่างเต็มที่ โดยจะเน้นที่ความรวดเร็ว ความยืดหยุ่น และความสามารถในการปรับขนาด (Scalability) ซึ่งเป็นแนวคิดของการออกแบบแอปพลิเคชันใหม่ทั้งหมดโดยคำนึงถึงสถาปัตยกรรมของคลาวด์ตั้งแต่เริ่มต้น ซึ่งการพัฒนานี้ทำให้ระบบของคลาวด์มีความซับซ้อนขึ้น มีแนวคิดและใช้งานเทคโนโลยีใหม่ เช่น Kubernetes, Microservices, Serverless และ DevOps เพื่อรองรับรูปแบบการทำงานแบบใหม่ ทำให้รูปแบบภัยคุกคามมีความซับซ้อนขึ้นจากโครงสร้างที่กระจายตัวมากขึ้นและการพึ่งพาบริการจำนวนมาก ส่งผลให้เกิดความท้าทายใหม่ในด้านของการรักษาความปลอดภัย เช่น ปัญหาการควบคุมสิทธิในการเข้าถึง (Identity and Access Management) การตั้งค่าที่ผิดพลาด (Misconfiguration) การโจมตีจากช่องโหว่ในระดับ Container และปัญหาการโจมตีที่ห่วงโซ่อุปทาน (Supply-Chain Attacks) กลายเป็นความเสี่ยงสำคัญในระบบนิเวศคลาวด์ยุคใหม่

จุดเปลี่ยนสำคัญที่เร่งกระบวนการเปลี่ยนผ่านสู่ระบบคลาวด์อย่างก้าวกระโดดเกิดขึ้นในปี 2019 ซึ่งมีการระบาดของโรค COVID-19 ทำให้องค์กรทั่วโลกต้องเปลี่ยนระบบไอทีให้รองรับการทำงานจากระยะไกล (Remote Work) ภายในเวลาที่จำกัด ทำให้เกิดการเร่งใช้บริการคลาวด์ การเคลื่อนย้ายระบบจำนวนมากในเวลาอันจำกัดส่งผลให้ความผิดพลาดด้านการตั้งค่าคลาวด์ (Misconfiguration) กลายเป็นช่องโหว่อันดับต้น ๆ ของเหตุการณ์ข้อมูลรั่วไหล

หลังจากการแพร่ระบาดของ COVID-19 จนถึงปัจจุบัน ด้วยการยอมรับการใช้งานคลาวด์ที่แพร่หลาย การประมวลผลด้วยคลาวด์ได้กลายเป็นโครงสร้างพื้นฐาน ทั้งในธุรกิจเอกชน รัฐบาล รวมถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) อย่างไรก็ตาม การเปลี่ยนแปลงทางเทคโนโลยีได้เพิ่มความซับซ้อนให้กับระบบนิเวศคลาวด์มากยิ่งขึ้น ได้แก่ Multi-Cloud กลยุทธ์การใช้ผู้ให้บริการคลาวด์หลายรายพร้อมกันกลายเป็นแนวทางหลักขององค์กร การย้ายการประมวลผลนั้นขยายไปสู่การประมวลผลใกล้แหล่งข้อมูล (Edge Computing) และ Generative AI การเข้ามาของเทคโนโลยีปัญญาประดิษฐ์ขั้นสูงที่กลายเป็นตัวขับเคลื่อนนวัตกรรมและภัยคุกคามรูปแบบใหม่

จากวิวัฒนาการของเทคโนโลยีและสถานการณ์ภัยคุกคามที่มีความซับซ้อนและทวีความรุนแรงยิ่งขึ้น สะท้อนให้เห็นว่าการบริหารจัดการความเสี่ยงในรูปแบบเดิมไม่อาจเพียงพอต่อการรับมือกับบริบทใหม่ของโลกไซเบอร์ แนวโน้มเหล่านี้ส่งผลให้ภาครัฐจำเป็นต้องมีมาตรการเชิงรุกในการกำหนดมาตรฐานและกลไกการกำกับดูแลเพื่อสร้างหลักประกันความมั่นคงปลอดภัยให้กับข้อมูลและบริการสาธารณะดิจิทัลของประเทศ

ด้วยเหตุผลดังกล่าว จึงนำมาสู่ความจำเป็นในการจัดทำ “แผนบูรณาการเพื่อขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2569-2573” เพื่อใช้เป็นกลไกหลักในการเตรียมความพร้อม ประสานความร่วมมือ และยกระดับขีดความสามารถของทุกภาคส่วนให้สามารถปฏิบัติตามมาตรฐานและรับมือกับความท้าทายในอนาคตได้อย่างมีประสิทธิภาพ

2.2 สถานการณ์ภัยคุกคามทางไซเบอร์ที่มีต่อระบบคลาวด์

บริษัท SentinelOne ได้รวบรวมข้อมูลและเผยแพร่สถิติความปลอดภัยบนคลาวด์ ในเดือนพฤศจิกายน ค.ศ. 2024 โดยระบุถึงความท้าทายที่สำคัญ เช่น การกำหนดค่าที่ไม่ถูกต้องบนคลาวด์ และการขาดการฝึกอบรมด้านความปลอดภัย ซึ่งเป็นสาเหตุหลักของเหตุการณ์การละเมิดข้อมูล โดยสถิติแสดงให้เห็นภาพเกี่ยวกับความรุนแรงและความถี่ของการโจมตีบนคลาวด์ที่เพิ่มขึ้นอย่างต่อเนื่อง เช่น พบการโจมตีด้านความปลอดภัยของระบบคลาวด์คิดเป็น 25% ของการโจมตีทางไซเบอร์ทั้งหมดทั่วโลก 80% ของบริษัทต่าง ๆ ได้พบกับการเพิ่มขึ้นของความถี่ในการโจมตีบนคลาวด์ที่เพิ่มสูงขึ้น โดย 83% ขององค์กรต่าง ๆ ประสบเหตุการณ์ด้านความปลอดภัยบนคลาวด์อย่างน้อยหนึ่งครั้งในปี 2024

นอกจากนั้น การละเมิดความปลอดภัยของคลาวด์ได้แซงหน้าการละเมิดข้อมูลในศูนย์ข้อมูลภายในองค์กร (On-premises data breaches) โดยจากรายงาน Cost of a Data Breach Report 2025 ของ IBM พบว่า 82% ของการละเมิดข้อมูลของปี ค.ศ. 2023 นั้นเกี่ยวข้องกับข้อมูลที่จัดเก็บในคลาวด์

เมื่อทำการวิเคราะห์ภาพรวม 5 ปีที่ผ่านมา สามารถแบ่งแนวโน้มที่เกี่ยวข้องกับการรักษาความปลอดภัยออกเป็น 5 ด้านหลัก ได้แก่

• การรีบเร่งย้ายสู่คลาวด์และความเสี่ยงจากการตั้งค่าผิดพลาด เช่น การย้ายระบบอย่างเร่งด่วนมักนำไปสู่ความผิดพลาดในการตั้งค่า (Misconfiguration) เช่น การเปิดเผยข้อมูลใน AWS S3 buckets หรือ Azure Blob Storage สู่สาธารณะโดยไม่ตั้งใจ

• การโจมตีแบบ Credential Attack และการยึดบัญชี (Cloud Account Takeover) เมื่อโครงสร้างพื้นฐานมีความแข็งแกร่งขึ้น อาชญากรไซเบอร์จึงเปลี่ยนเป้าหมายไปที่ “บัญชีผู้ใช้” (User Credentials) เพื่อใช้เป็นใบเบิกทางเข้าสู่ระบบ แทนการเจาะระบบโดยตรง

• การเพิ่มขึ้นของ Supply-Chain Cloud Compromise ผู้โจมตีมุ่งเน้นการฝังตัวผ่านผู้ให้บริการซอฟต์แวร์หรือบริการบุคคลที่สาม (Third-party Vendors) เพื่อสร้างผลกระทบในวงกว้างดังที่เห็นในเหตุการณ์ SolarWinds และ Microsoft Exchange Online

• การขยายตัวของ Multi-Cloud ที่มาพร้อมความเสี่ยงใหม่ องค์กรจำนวนมากเริ่มใช้งาน Multi-Cloud เช่น ใช้ AWS ร่วมกับ Azure และ GCP เพื่อเพิ่มความยืดหยุ่น แต่ต้องแลกมาด้วยพื้นที่การโจมตี (Attack Surface) ที่กว้างขึ้นจากการใช้งาน SaaS และ PaaS ที่หลากหลาย

• การใช้งานปัญญาประดิษฐ์ (AI) และ Large Language Models (LLMs) การผนวก AI และ Large Language Models (LLMs) เข้ากับโครงสร้างพื้นฐานคลาวด์ ทำให้เกิดความเสี่ยงใหม่ในขณะเดียวกัน ผู้โจมตีได้นำ AI มาใช้เพิ่มประสิทธิภาพและความรวดเร็วในการโจมตีเช่นกัน

ตัวอย่างสถานการณ์โจมตีบนระบบคลาวด์ที่สำคัญในช่วง ค.ศ. 2020–2025

ในปี ค.ศ. 2020 เกิดเหตุการณ์ SolarWinds Supply-Chain Attack เป็นหนึ่งในเหตุการณ์ด้านความมั่นคงไซเบอร์ที่มีผลต่อโครงสร้างพื้นฐานดิจิทัลของโลกอย่างรุนแรง ด้วยลักษณะการโจมตีผ่านห่วงโซ่อุปทาน (Supply Chain) ทำให้ผู้โจมตีสามารถเข้าถึงหน่วยงานรัฐบาลสหรัฐฯ บริษัทเทคโนโลยีระดับโลก และองค์กรสำคัญอีกกว่า 18,000 แห่ง ผ่านการอัปเดตซอฟต์แวร์ของ SolarWinds Orion ซึ่งเป็นแพลตฟอร์มสำหรับบริหารจัดการเครือข่าย (Network Monitoring & Management) ที่องค์กรขนาดใหญ่ทั่วโลกใช้งานเพื่อดูแลโครงสร้างพื้นฐานทั้งในองค์กรและบนระบบคลาวด์ การโจมตีเริ่มจากผู้โจมตีสามารถเจาะเข้าไปในกระบวนการพัฒนาและ build environment ของ SolarWinds และฝัง backdoor ชื่อ SUNBURST ลงในชุดอัปเดตของ Orion เมื่อลูกค้าดาวน์โหลดอัปเดตดังกล่าว มัลแวร์ก็ถูกติดตั้งลงไปโดยอัตโนมัติ

ทำให้ผู้โจมตีสามารถเข้าถึงระบบภายในขององค์กรที่ใช้ซอฟต์แวร์นี้ได้ทันที ผลที่เกิดขึ้นคือหน่วยงานโครงสร้างพื้นฐานของภาครัฐจำนวนมาก ได้รับผลกระทบจากการโจมตีครั้งนี้ ความรุนแรงของการโจมตีครั้งนี้ส่วนหนึ่งมาจากที่องค์กรจำนวนมากใช้ Orion เพื่อบริหารทรัพยากรทั้งใน Data Center และบน Cloud ทำให้การเข้าถึง Orion สามารถเข้าถึงโครงสร้างพื้นฐานทั้งองค์กรได้ นอกจากนั้นเมื่อผู้โจมตีได้สิทธิ์ในเครือข่ายขององค์กรแล้วสิ่งต่อมาคือการเจาะระบบ Cloud Identity เพื่อยกระดับการโจมตีได้ต่อไป

ในปี ค.ศ. 2021 เกิดเหตุการณ์ Kaseya VSA Ransomware Attack ซึ่งถือเป็นหนึ่งในเหตุการณ์ Supply-Chain Ransomware ที่ใหญ่ที่สุดในประวัติศาสตร์ และเป็นตัวอย่างสำคัญของภัยคุกคามที่โจมตีผ่านช่องโหว่ในโครงสร้างพื้นฐานด้านการบริหารจัดการ (IT Management Infrastructure) ของระบบคลาวด์เพื่อโจมตีลูกค้าจำนวนมากผ่านผู้ให้บริการ (Managed Service Providers: MSP)

Kaseya VSA เป็นแพลตฟอร์มที่ผู้ให้บริการ MSP ใช้สำหรับควบคุมและดูแลเครื่องลูกค้าจำนวนมาก เช่น การอัปเดตแพตช์ การติดตั้งซอฟต์แวร์ หรือการกำหนดค่าต่าง ๆ จากส่วนกลาง ซึ่งกลุ่มอาชญากรรมไซเบอร์ REvil ได้ใช้ช่องโหว่แบบ Zero-Day ในระบบบริหารจัดการไอที Kaseya VSA เพื่อกระจายแรนซัมแวร์ (Ransomware) ไปยังองค์กรจำนวนมากผ่านทางผู้ให้บริการจัดการระบบ (MSP) โดยจำนวน MSP ที่ถูกโจมตีโดยตรงมีเพียงประมาณ 60 ราย แต่ลูกค้าซึ่งเป็นองค์กรปลายทางกลับได้รับผลกระทบมากกว่า 1,500 หน่วยงานทั่วโลก

ในปี ค.ศ. 2021 ยังมีเหตุการณ์ช่องโหว่ที่ถือว่ารุนแรงที่สุดครั้งหนึ่ง คือ ช่องโหว่ Log4Shell (CVE-2021-44228) ซึ่งส่งผลกระทบต่อระบบคอมพิวเตอร์และบริการคลาวด์หลายแพลตฟอร์ม เนื่องจาก Log4j เป็นไลบรารีที่ถูกใช้อย่างแพร่หลายในการเก็บบันทึก (logging) ทั้งในซอฟต์แวร์องค์กร แอปพลิเคชันออนไลน์ ไปจนถึงบริการคลาวด์ขนาดใหญ่ ช่องโหว่นี้เปิดโอกาสให้ผู้โจมตีสามารถสั่งรันคำสั่งจากระยะไกล (Remote Code Execution: RCE) ได้โดยไม่ต้องมีสิทธิ์ สามารถโจมตีโดยส่งสตริงที่ออกแบบมาไปยังระบบที่มี Log4j อยู่ ซึ่งระบบจะรันคำสั่งให้ผู้โจมตีทันที ทำให้เป็นช่องโหว่ที่เรียบง่ายมีความรุนแรงและแพร่กระจายอย่างกว้างขวาง ลูกค้าบริการคลาวด์จำนวนมากพบว่า workload ของตนถูกพยายามโจมตีอย่างต่อเนื่องหลังช่องโหว่ถูกเผยแพร่ ซึ่งเหตุการณ์ในครั้งนี้แสดงให้เห็นว่า ช่องโหว่ของไลบรารีขนาดเล็กเพียงตัวเดียวที่สามารถกลายเป็นจุดเริ่มต้นของภัยคุกคามระดับโลกอย่างรวดเร็ว การพึ่งพา open-source libraries โดยไม่มีกลไกตรวจสอบจึงเป็นความเสี่ยงที่ต้องได้รับการดูแล ซึ่งช่องโหว่นี้มีผลกระทบต่อเนื่องมาจนถึงประมาณปี ค.ศ. 2023 เพราะหลายระบบบนคลาวด์และซอฟต์แวร์องค์กรยังคงใช้งาน Log4j ที่ไม่ได้อัปเดต

ในปี ค.ศ. 2024 แพลตฟอร์ม Snowflake ซึ่งเป็นบริการคลาวด์ด้าน Data Warehousing และ Analytics แบบ multi-tenant ได้ถูกโจมตีโดยเกิดเหตุการณ์รั่วไหลของข้อมูล (data breach) โดยมีลูกค้า หลายรายได้รับผลกระทบ ทำให้ข้อมูลสำคัญรั่วไหลออกไป การโจมตีนี้มุ่งเป้าไปที่บัญชีลูกค้าของ Snowflake โดยใช้ข้อมูลยืนยันตัวตนที่ถูกขโมยมาก่อนหน้านี้ผ่านทางมัลแวร์ โดย Snowflake ยืนยันว่าไม่มีหลักฐานแสดงถึงช่องโหว่หรือการละเมิดบนแพลตฟอร์มหลักของตนเอง แต่เป็นปัญหาด้านความปลอดภัยที่เกี่ยวข้องกับการจัดการบัญชีของลูกค้าแต่ละราย ซึ่งลูกค้าที่มีปัญหายังมีการใช้งาน Single Factor Authentication ทำให้ผู้โจมตีสามารถเข้าถึงบัญชีได้ง่ายด้วยข้อมูลประจำตัวที่ถูกขโมยมาเพียงอย่างเดียว บทเรียนสำคัญจากการโจมตี Snowflake Cloud Breach ในปี ค.ศ. 2024 เป็นการย้ำเตือนถึงความสำคัญของมาตรการรักษาความปลอดภัยขั้นพื้นฐานในสภาพแวดล้อมคลาวด์ ซึ่งเหตุการณ์ไม่ได้จำกัดอยู่แค่ผู้ใช้ Snowflake เท่านั้น แต่รวมถึงองค์กรที่ใช้บริการคลาวด์ทั้งหมดด้วย

นอกจากนี้ การโจมตีทางไซเบอร์จะมีผลกระทบกับผู้ใช้งานคลาวด์และผู้ให้บริการคลาวด์เป็นวงกว้างแล้ว สำหรับผู้ให้บริการคลาวด์บางครั้งก็มีเหตุการณ์ที่ไม่สามารถให้บริการ (Cloud outage) ที่ส่งผลกระทบเป็นวงกว้างกับผู้ใช้งานหลายครั้ง เช่น ในวันที่ 12 มิ.ย. 2025 ระบบคลาวด์ของ Google เกิดปัญหาไม่สามารถใช้งานได้จนกระทบกับผู้ใช้งานทั่วโลก โดยระบบ API และหลายผลิตภัณฑ์ของ Google Cloud ส่งค่าที่ผิดพลาดและไม่สามารถให้บริการได้ตามปกติ ทำให้เกิดผลกระทบรุนแรงทั้งต่อผลิตภัณฑ์ของ Google เอง และบริการของบุคคลที่ใช้บริการ Google Cloud เช่น Spotify และ Discord

อีกเหตุการณ์หนึ่ง ในวันที่ 20 ต.ค. 2025 ผู้ใช้ทั่วโลกเริ่มพบว่าหลายบริการของ AWS ไม่สามารถใช้งานได้หรือทำงานช้าลงอย่างผิดปกติ เมื่อบริษัทต่าง ๆ ตรวจสอบก็พบว่าบริการหลักหลายตัวของ AWS โดยเฉพาะใน Region US-EAST-1 มีอัตราความผิดพลาดสูงและมีความล่าช้า ซึ่ง AWS ได้ออกแถลงการณ์ว่าเกิดปัญหาที่ผิดปกติ และทีมงานกำลังเร่งจัดการอย่างเร่งด่วน หลังจากหลายชั่วโมงผ่านไปสถานะการให้บริการจึงฟื้นตัวจนกลับมาทำงานตามปกติ จากข้อมูลที่เปิดเผยภายหลัง AWS ระบุว่าสาเหตุหลักเริ่มจากปัญหาภายในระบบเครือข่ายและ DNS ของ AWS เอง ซึ่งเป็นปัญหาเชิงโครงสร้างพื้นฐานของผู้ให้บริการคลาวด์ (Cloud Provider Outage) โดยสำนักข่าวรายงานว่ามีผู้ใช้กว่า 8.1 ล้านรายได้รับผลกระทบทั่วโลก

2.3 กระบวนการจัดทำแผนบูรณาการฯ

เพื่อให้การดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 เป็นไปอย่างมีประสิทธิภาพในระยะเวลาที่กำหนด สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้กำหนดกรอบแนวทางการจัดทำแผนบูรณาการเพื่อขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ โดยแบ่งออกเป็น 5 ขั้นตอน ดังนี้

ขั้นตอนที่ 1: ทบทวนหลักการสำคัญ เป็นขั้นตอนพื้นฐานที่มุ่งศึกษาทบทวนหลักการสำคัญที่เกี่ยวข้องกับมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 รวมถึงกรอบแนวคิดอื่นที่เกี่ยวข้องกับการจัดระดับความเสี่ยง การกำหนดมาตรการควบคุม และข้อกำหนดด้านการบริหารจัดการความมั่นคงปลอดภัยในระบบคลาวด์ การทบทวนดังกล่าวช่วยให้การจัดทำแผนบูรณาการฯ มีความสอดคล้องกับวัตถุประสงค์ของมาตรฐานฯ และตอบโจทย์การนำไปใช้งานจริงของหน่วยงานที่เกี่ยวข้อง

ขั้นตอนที่ 2: ทบทวนมาตรการและกรอบปฏิบัติสากล เป็นการมุ่งเน้นการศึกษาและวิเคราะห์มาตรการด้านความมั่นคงปลอดภัยไซเบอร์บนระบบคลาวด์ตามแนวทางสากล ผ่านการคัดเลือกและพิจารณานโยบายที่เกี่ยวข้องจาก 3 ประเทศที่มีความก้าวหน้าในด้านการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลบริการคลาวด์ภาครัฐ การศึกษาดังกล่าวช่วยให้เห็นแนวปฏิบัติที่ได้รับการยอมรับในระดับนานาชาติ รวมถึงรูปแบบการกำหนดมาตรฐาน มาตรการควบคุม ขั้นตอนคัดกรองผู้ให้บริการคลาวด์ และกลไกกำกับติดตามที่ประเทศต่าง ๆ ใช้ในการยกระดับความมั่นคงปลอดภัยของข้อมูลภาครัฐ การทบทวนนี้จะสามารถนำมาประยุกต์ใช้ในการจัดทำแผนบูรณาการฯ 5 ปี ให้มีความเทียบเคียงกับมาตรฐานสากล มีความทันสมัยและสามารถตอบสนองภัยคุกคามไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็ว พร้อมทั้งช่วยลดช่องว่างระหว่างมาตรฐานของประเทศไทยกับการปฏิบัติในระดับนานาชาติ

ขั้นตอนที่ 3: ทบทวนกรณีศึกษา เป็นการศึกษากรณีภัยคุกคามที่เกิดขึ้นกับระบบคลาวด์ที่มีผลกระทบเป็นวงกว้าง โดยมุ่งวิเคราะห์รูปแบบการโจมตี และผลกระทบที่เกิดขึ้น ข้อมูลจากกรณีศึกษาเหล่านี้จะช่วยให้เห็นความเสี่ยงสำคัญที่ควรนำมาพิจารณาในการจัดทำแผนบูรณาการฯ และช่วยให้แผนมีความสอดคล้องกับสถานการณ์ภัยคุกคามที่เกิดขึ้นจริงในปัจจุบัน

ขั้นตอนที่ 4: จัดทำแผนบูรณาการฯ เมื่อได้ข้อมูลจากการทบทวนในขั้นตอนก่อนหน้าแล้ว สกมช. ดำเนินการสังเคราะห์ข้อมูลเพื่อจัดทำแผนบูรณาการฯ ระยะ 5 ปี โดยกำหนดวิสัยทัศน์ ยุทธศาสตร์ กลยุทธ์ แนวทางการดำเนินงาน มาตรการสำคัญ ตัวชี้วัด ระยะเวลา บทบาทของหน่วยงานที่เกี่ยวข้อง และแนวทางการประเมินผล เพื่อให้แผนบูรณาการฯ เป็นแผนปฏิบัติการหลักในการพัฒนาและยกระดับความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทยได้อย่างเป็นระบบ

ขั้นตอนที่ 5: รับฟังความคิดเห็นต่อแผนบูรณาการฯ เมื่อจัดทำแผนบูรณาการฯ ในขั้นตอนก่อนหน้าเป็นที่เรียบร้อย จึงจะดำเนินการเปิดรับฟังความคิดเห็นจากผู้มีส่วนเกี่ยวข้อง ได้แก่ หน่วยงานของรัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้เชี่ยวชาญภายนอก และภาคเอกชน เพื่อประเมินความเหมาะสม ความเป็นไปได้ และผลกระทบของแผนบูรณาการฯ โดยมีจุดประสงค์เพื่อทำการตรวจสอบความครบถ้วนและความเหมาะสมของแผนบูรณาการฯ ทั้งนี้ การรับฟังความคิดเห็นจะแบ่งเป็น 2 รอบ เพื่อให้ได้ข้อมูลที่รอบด้านและสะท้อนมุมมองของผู้มีส่วนได้ส่วนเสียและผู้ที่เกี่ยวข้องอย่างแท้จริง ได้แก่

- การประชุมแบบ Focus Group เพื่อรับฟังความคิดเห็นเชิงลึกจากผู้เชี่ยวชาญและหน่วยงานที่เกี่ยวข้องโดยตรง เน้นประเด็นด้านเทคนิค ความเป็นไปได้ในการปฏิบัติ และผลกระทบที่อาจเกิดขึ้น ช่วยให้แผนมีความถูกต้องและเหมาะสมเชิงเนื้อหา

- การรับฟังความคิดเห็นสาธารณะ (Public Hearing) เพื่อเปิดโอกาสให้หน่วยงานภาครัฐ ภาคเอกชน และสาธารณชนร่วมแสดงความคิดเห็นในวงกว้าง ทำให้แผนมีความโปร่งใส สอดคล้องกับความต้องการจริงของผู้ใช้งาน และได้รับความยอมรับในระดับประเทศ

การดำเนินการดังกล่าวช่วยให้สามารถปรับปรุงแผนบูรณาการฯ ให้มีความครอบคลุมและพร้อมนำไปใช้ได้อย่างมีประสิทธิภาพ

บทที่ 3
แผนบูรณาการเพื่อขับเคลื่อนการดำเนินการ

3.1 ความสอดคล้องกับหลักการสำคัญที่เกี่ยวข้องกับมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 และกรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Thailand's National Cloud Security Framework)

ความสอดคล้องกับมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 และกรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Thailand's National Cloud Security Framework) มีดังต่อไปนี้

3.1.1 นโยบายการใช้คลาวด์เป็นหลัก

มติคณะรัฐมนตรีเมื่อวันที่ 25 มิถุนายน 2567 เรื่อง การแต่งตั้งคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy)
1. แต่งตั้งคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ทั้งนี้ ให้มีผลตั้งแต่วันที่คณะรัฐมนตรีมีมติเป็นต้นไป 2. ให้คณะกรรมการพัฒนารัฐบาลดิจิทัลเป็นผู้ดำเนินการกำหนดรายละเอียดที่เกี่ยวข้องกับนโยบายการใช้คลาวด์ การออกประกาศเพื่อกำหนดหลักเกณฑ์และมาตรฐาน ประสานงานกับหน่วยงานที่เกี่ยวข้อง พัฒนาระบบบริหารจัดการความต้องการและจัดหาคลาวด์ กำกับดูแล สร้างระบบนิเวศและจัดซื้อจัดจ้างตามกรอบนโยบายที่ได้รับอนุมัติจากคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ รวมทั้งกรอบกฎหมายของหน่วยงานของรัฐที่เกี่ยวข้องต่อไป
การประชุมคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ครั้งที่ 1/2567
1. แต่งตั้งคณะอนุกรรมการด้านกฎหมายการจัดซื้อจัดจ้างบริการคลาวด์ภาครัฐ และได้เห็นชอบให้แต่งตั้งคณะอนุกรรมการด้านบริหารจัดการความต้องการใช้บริการคลาวด์ (Demand) การให้บริการคลาวด์ (Supply) และมาตรฐานการบริหารจัดการการบริการคลาวด์ภาครัฐ (Government Cloud Management) 2. ประเด็นสำคัญ เพื่อให้คณะอนุกรรมการฯ ที่จะแต่งตั้งไปประกอบการพิจารณา เช่น การแบ่งระดับชั้นข้อมูลภาครัฐ การเลือกใช้บริการคลาวด์ที่เหมาะสมกับการใช้งาน การส่งเสริมการลงทุนบริการคลาวด์ภายในประเทศและแต้มต่อของผู้ให้บริการคลาวด์ไทย รูปแบบของงบประมาณและการคิดค่าใช้จ่ายในอนาคตเพื่อรองรับการใช้บริการคลาวด์อย่างต่อเนื่อง ความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งมาตรฐานและการรับประกันคุณภาพการให้บริการคลาวด์
การประชุมคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ครั้งที่ 2/2567
1. กรอบแนวทางการบริหารจัดการระบบคลาวด์ภาครัฐ ประกอบไปด้วย 8 แนวทาง ได้แก่ 1.1 การใช้ Service ของ Public Cloud 1.2 การออกแบบระบบงานที่ใช้ Services ต่าง ๆ บนระบบ Cloud 1.3 การใช้ระบบและองค์ประกอบมาตรฐานของ Cloud 1.4 การปรับแต่งฟังก์ชัน (Function) หรือบริการ (Service) ต่าง ๆ ให้น้อยที่สุด โดยใช้การปรับแต่งระบบงานแทน (Avoid customization) 1.5 การติดตามการใช้และความสมบูรณ์ของระบบ

1.6 การติดตั้งระบบความมั่นคงปลอดภัยของระบบงานและ Application อย่างเหมาะสม และตรวจสอบความสมบูรณ์ของระบบงาน การปฏิบัติงานของผู้ให้บริการ Cloud อย่างสม่ำเสมอ 1.7 การจัดหาบริการ และผลิตภัณฑ์ ให้รัฐบาลเป็นผู้เห็นชอบกรอบบันทึกข้อตกลงสัญญากันก่อน 1.8 การจัดทำงบประมาณสำหรับโครงการที่จะเข้าข่ายการใช้คลาวด์เป็นหลัก 2. กรอบมาตรฐานความปลอดภัย 2.1 จำเป็นต้องศึกษากฎหมายและระเบียบมาตรฐานของต่างประเทศเพิ่มเติม เพื่อให้มีความรัดกุมต่อการเข้าถึงข้อมูลของระบบ Cloud ของประเทศไทย 2.2 กำหนดแนวทางประเภทของข้อมูลที่ห้ามทำสำเนาออกนอกประเทศ เพื่อกำหนดกรอบทิศทางของระบบ Cloud ในอนาคตให้มีความเหมาะสม 2.3 พร้อมต่อการใช้งานและสอดคล้องกับข้อกำหนดมาตรฐานและเงื่อนไขทั้งในประเทศไทยและต่างประเทศ
การประชุมคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ครั้งที่ 3/2567
เห็นชอบแผนการขับเคลื่อนนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ตามที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ได้วางแนวทางไว้ดังนี้ 1. กรอบการบริหารจัดการระบบคลาวด์ภาครัฐ ตามนโยบายการใช้คลาวด์เป็นหลัก ทั้งในการจัดทำร่างประกาศ รับฟังความคิดเห็น จัดทำแนวปฏิบัติ และให้คำแนะนำหน่วยงาน 2. แนวทางการจำแนกข้อมูล (Data Classification) เพื่อประกาศรายละเอียดเบื้องต้นให้หน่วยงานนำไปปฏิบัติได้ 3. แนวทางการบริหารการให้บริการคลาวด์ (Supply) จัดทำรายละเอียดข้อกำหนด มาตรฐานและเงื่อนไขสำหรับผู้ให้บริการ พร้อมรับฟังความคิดเห็นและหารือกับหน่วยงานที่เกี่ยวข้องเพื่อปรับแก้ระเบียบให้สอดคล้องกับนโยบาย 4. แนวทางการบริหารจัดการการบริการคลาวด์ภาครัฐ (Government Cloud Management) ในด้านการวิเคราะห์ ออกแบบ Government Cloud Management การพัฒนาระบบ การประสานเชื่อมโยงข้อมูลกับผู้ให้บริการ 5. แนวทางการเสนอโครงการและการประเมินงบประมาณ เพื่อให้สอดคล้องกับนโยบายของรัฐบาลที่ให้ความสำคัญเรื่อง Cloud First และ AI ที่ต้องการทราบความต้องการในภาพรวมของหน่วยงานภาครัฐเพื่อการจัดสรรงบประมาณแผ่นดินให้เกิดประโยชน์สูงสุดแก่ประเทศชาติได้ต่อไป

3.1.2 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ดังนี้

แนบท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567
1. บทนำ 1.7 กรอบแนวคิด 1.8 กระบวนการตรวจรับรองมาตรฐาน
2. ขอบเขต (Scope)
3. การอ้างอิงที่เกี่ยวข้อง (Normative Reference)
4. ข้อกำหนดขั้นต่ำและการตรวจรับรองสำหรับผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์

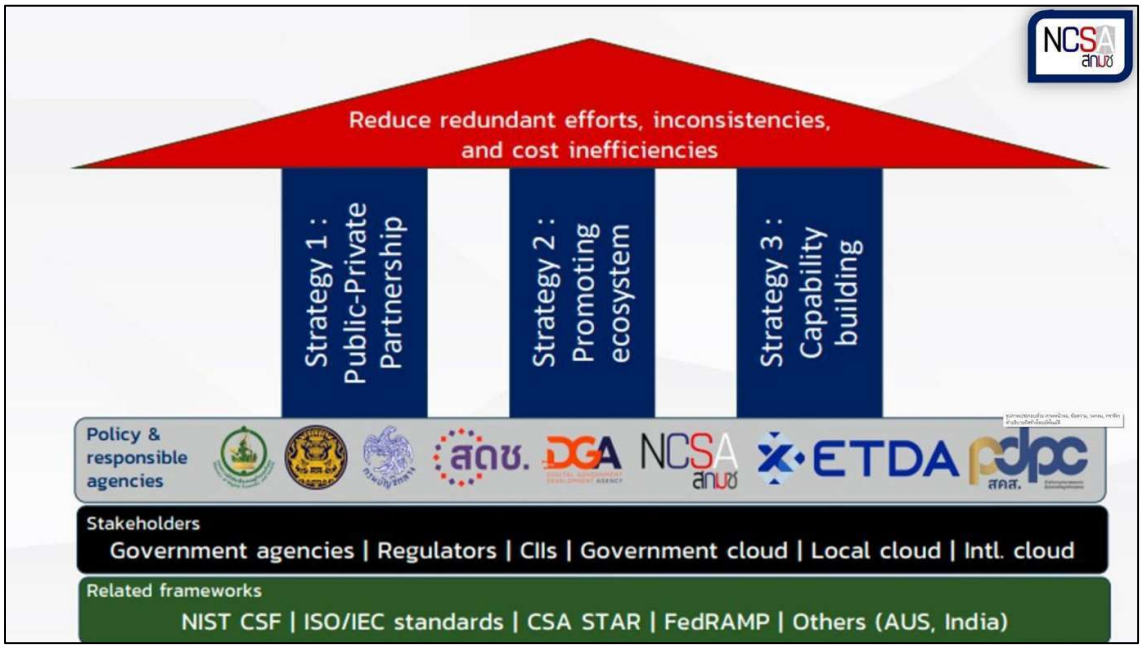
5. มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

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

กรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Thailand's National Cloud Security Framework)
บทที่ 4 การวิเคราะห์ความเป็นไปได้ และข้อเสนอแนะเชิงนโยบาย 4.1 การวิเคราะห์ความเป็นไปได้ 4.2 ข้อเสนอแนะเชิงนโยบาย
บทที่ 5 กรอบการดำเนินงาน 5.1 วัตถุประสงค์ 5.2 ประโยชน์ 5.3 หลักการสำคัญที่เกี่ยวข้อง 5.4 ผู้ที่เกี่ยวข้อง 5.5 กรอบแนวทางการทำงาน

3.2 สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย

ปัจจุบันหน่วยงานภาครัฐของประเทศไทยได้มีการขับเคลื่อนนโยบายที่เกี่ยวข้องกับการกำกับดูแลระบบคลาวด์เพื่อยกระดับการให้บริการดิจิทัลแก่ประชาชน อย่างไรก็ตาม การเปลี่ยนผ่านสู่ระบบคลาวด์นำมาซึ่งความเสี่ยงทางไซเบอร์รูปแบบใหม่ ทั้งการโจมตีโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการรั่วไหลของข้อมูลส่วนบุคคล เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศมีเอกภาพและประสิทธิภาพ จึงมีความจำเป็นต้องกำหนดสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ระดับชาติ เพื่อใช้เป็นโมเดลอ้างอิงในการยกระดับระบบนิเวศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย (Thailand's Cloud Security Ecosystem)



รูปที่ 1: สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย

สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย (Thailand's National Cloud Security Architecture) มีความจำเป็นต้องมีการคำนึงถึงบริบททางกฎหมายของไทยควบคู่ไปกับมาตรฐานสากล นอกจากนั้นยังจำเป็นต้องพิจารณาถึงผู้ที่มีส่วนได้ส่วนเสีย และแนวทางในการอ้างอิงมาตรฐานการรักษาความมั่นคงปลอดภัยระดับสากล โดยมีรายละเอียดองค์ประกอบดังนี้

1. เป้าหมายสูงสุด ส่วนยอดของโครงสร้างระบุวัตถุประสงค์หลักของการออกแบบสถาปัตยกรรมนี้คือการแก้ปัญหาเชิงโครงสร้างที่มีอยู่ในปัจจุบัน ได้แก่

- ลดความซ้ำซ้อนในการดำเนินงาน (Reduce redundant efforts): การบูรณาการทรัพยากรและนโยบายเพื่อไม่ให้หน่วยงานต่าง ๆ ทำงานทับซ้อนกัน
- ลดความไม่สอดคล้องในการดำเนินงาน (Reduce inconsistencies): สร้างมาตรฐานกลางเพื่อให้ระบบต่าง ๆ สามารถเชื่อมต่อและแลกเปลี่ยนข้อมูลกันได้อย่างปลอดภัย
- ลดความไร้ประสิทธิภาพด้านต้นทุน (Cost inefficiencies): การบริหารจัดการงบประมาณด้านความมั่นคงปลอดภัยให้เกิดประโยชน์สูงสุด

2. เสาหลักยุทธศาสตร์ การขับเคลื่อนเพื่อให้บรรลุเป้าหมาย ได้แก่

กลยุทธ์ที่ 1: ความร่วมมือระหว่างภาครัฐและเอกชน (Public-Private Partnership): การสร้างเครือข่ายความร่วมมือ แลกเปลี่ยนองค์ความรู้และทรัพยากรระหว่างหน่วยงานของรัฐและภาคธุรกิจ

กลยุทธ์ที่ 2: การส่งเสริมระบบนิเวศ (Promoting Ecosystem): การสร้างสภาพแวดล้อมที่เอื้อต่อความปลอดภัย ทั้งด้านกฎระเบียบ ตลาดผู้ให้บริการ และเทคโนโลยี

กลยุทธ์ที่ 3: การเสริมสร้างขีดความสามารถ (Capability Building): การพัฒนาบุคลากร การฝึกอบรมและการยกระดับทักษะด้านไซเบอร์ให้พร้อมรับมือภัยคุกคาม

3. ฐานรากการดำเนินงาน (The Foundation Layers) ความสำเร็จของยุทธศาสตร์ต้องอาศัยฐานรากที่เข้มแข็ง ซึ่งประกอบด้วย 3 ชั้นฐาน ดังนี้

3.1 ชั้นหน่วยงานกำกับดูแลและกำหนดนโยบาย เป็นการบูรณาการหน่วยงานสำคัญที่เกี่ยวข้องในระดับประเทศเพื่อให้เกิดการกำกับดูแลแบบองค์รวม ได้แก่

- กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นผู้รับผิดชอบหลักในการขับเคลื่อนยุทธศาสตร์ดิจิทัลของประเทศ และเป็นหน่วยงานต้นสังกัดของหน่วยงานปฏิบัติการ เพื่อให้เกิดการบูรณาการนโยบายไปในทิศทางเดียวกัน
- สำนักนายกรัฐมนตรี มีบทบาทในการออกมติคณะรัฐมนตรีเพื่อบังคับใช้นโยบายที่เกี่ยวข้อง เช่น การกำหนดให้หน่วยงานภาครัฐต้องใช้บริการคลาวด์กลางในนโยบายการใช้คลาวด์เป็นหลัก
- สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ มีหน้าที่กำหนดนโยบายและแผนแม่บทเกี่ยวกับโครงสร้างพื้นฐานดิจิทัลของประเทศ รวมถึงบริหารจัดการระบบคลาวด์กลางภาครัฐและดำเนินการจัดสรรงบประมาณจากกองทุนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อสนับสนุนโครงการต่าง ๆ ที่เกี่ยวข้องกับการพัฒนาโครงสร้างพื้นฐานดิจิทัล
- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รับผิดชอบตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดมาตรฐาน เฝ้าระวัง และรับมือภัยคุกคามทางไซเบอร์ เป็นผู้กำหนดมาตรฐานขั้นต่ำด้านความปลอดภัยสำหรับระบบคลาวด์ภาครัฐ และกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ปฏิบัติตามมาตรฐาน
- สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พัฒนาบริการดิจิทัลภาครัฐ และกำหนดมาตรฐานรัฐบาลดิจิทัล

• สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ส่งเสริมและดูแลความมั่นคงปลอดภัยของการทำธุรกรรมทางอิเล็กทรอนิกส์ รวมถึงการรับรองระบบสารสนเทศ

• สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รับผิดชอบการกำกับดูแลการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

• กรมบัญชีกลาง รับผิดชอบการกำกับดูแลกฎระเบียบด้านการจัดซื้อจัดจ้างและการเบิกจ่ายงบประมาณแผ่นดิน กำหนดระเบียบการเช่าใช้บริการระบบคลาวด์ รวมถึงกำหนดราคากลางมาตรฐานสำหรับบริการด้านมาตรฐานการรักษาความปลอดภัยสารสนเทศ และระบบคลาวด์ เพื่อให้หน่วยงานของรัฐสามารถตั้งงบประมาณได้อย่างถูกต้องและมีความโปร่งใส

3.2 ชั้นผู้มีส่วนได้ส่วนเสีย (Stakeholders) องค์ประกอบส่วนนี้สะท้อนถึงระบบนิเวศการดำเนินงาน (Operational Ecosystem) โดยจำแนกกลุ่มเป้าหมายตามบทบาทหน้าที่และความรับผิดชอบในห่วงโซ่อุปทานความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย

• หน่วยงาน (Government Agency): หน่วยงานของรัฐ

• หน่วยงานควบคุมหรือกำกับดูแล (Regulator): หน่วยงานของรัฐ หน่วยงานเอกชนหรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

• หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII): หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

• ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP): หน่วยงานของรัฐหรือหน่วยงานเอกชนที่ทำให้บริการคลาวด์สามารถใช้ได้กับผู้ใช้บริการคลาวด์ รวมถึงจัดการทรัพยากรเหล่านี้เพื่อให้มั่นใจว่ามีความพร้อมใช้งาน ความมั่นคงปลอดภัย และความสามารถในการขยายตัวสำหรับผู้ใช้บริการคลาวด์ของตน โดยจำแนกตามลักษณะการให้บริการและถิ่นที่ตั้ง ดังนี้

1) ผู้ให้บริการคลาวด์ภาครัฐ (Government Cloud Provider): สำหรับการให้บริการโครงสร้างพื้นฐานกลางแก่หน่วยงานของรัฐ

2) ผู้ให้บริการภายในประเทศ (Local Cloud Provider): ผู้ให้บริการคลาวด์ในประเทศที่ให้บริการโครงสร้างพื้นฐานกลางแก่หน่วยงานของรัฐโดยเฉพาะเพื่อสนับสนุนนโยบายอธิปไตยของข้อมูล (Data Sovereignty)

3) ผู้ให้บริการระดับสากล (International Cloud Provider): ผู้ให้บริการจากต่างประเทศสำหรับรองรับงานที่ต้องการขีดความสามารถในการประมวลผลระดับสูงหรือนวัตกรรมเฉพาะทาง

3.3 ชั้นกรอบมาตรฐานอ้างอิง (Related Frameworks) องค์ประกอบนี้ถือเป็นรากฐานสำคัญในการกำกับทิศทางและรองรับโครงสร้างสถาปัตยกรรมทั้งหมด โดยยึดหลักการสอดคล้องกับมาตรฐานสากลและการเลือกใช้แนวปฏิบัติที่ดีที่สุดตามบริบทของประเทศ เพื่อทำให้เกิดความเชื่อมั่นและยกระดับขีดความสามารถในการแข่งขันระดับนานาชาติ ตัวอย่างของมาตรฐานอ้างอิง ได้แก่

• NIST Cybersecurity Framework (NIST CSF) เป็นกรอบแนวทางมาตรฐานสำหรับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์แบบองค์รวม ถูกพัฒนาโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา (NIST - National Institute of Standards and Technology) มีความแพร่หลายและได้รับการยอมรับในระดับสากล

• ISO/IEC Standards เป็นชุดมาตรฐานสากลว่าด้วยระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) อาทิ ISO/IEC 27001 และ ISO/IEC 27017 ซึ่งเป็นเกณฑ์อ้างอิงหลักในการรับรองความปลอดภัยและความน่าเชื่อถือของกระบวนการดำเนินงานที่แพร่หลายและได้รับการยอมรับในระดับสากล

• CSA Security Trust Assurance and Risk (CSA STAR) เป็นมาตรฐานเฉพาะทางของ Cloud Security Assurance (CSA) ซึ่งครอบคลุมการควบคุมทางเทคนิคและการตรวจสอบความโปร่งใสของผู้ให้บริการระบบประมวลผลแบบคลาวด์ (Cloud Service Providers)

• Federal Risk and Authorization Management Program (FedRAMP) เป็นต้นแบบแนวทางการประเมินและอนุญาตให้ใช้งานระบบคลาวด์สำหรับหน่วยงานของรัฐ ซึ่งเน้นความเข้มงวดในการรักษาความมั่นคงปลอดภัยของข้อมูลภาครัฐที่นำมาประยุกต์ใช้เป็นกรณีศึกษา

• เกณฑ์มาตรฐานและแนวปฏิบัติสากลจากประเทศอื่น ๆ เป็นการนำกรอบมาตรฐานการรักษาความปลอดภัยในระบบคลาวด์ของประเทศชั้นนำที่มีความก้าวหน้าด้านการกำกับดูแลระบบคลาวด์เพื่อให้ครอบคลุมมิติการรักษาความมั่นคงปลอดภัยของระบบคลาวด์อย่างรอบด้าน เช่น สหรัฐอเมริกา อังกฤษ และสิงคโปร์

3.3 วิสัยทัศน์ หลักการกำกับการขับเคลื่อน เป้าหมายเชิงยุทธศาสตร์ ยุทธศาสตร์ กลยุทธ์ ตัวชี้วัด/ค่าเป้าหมาย โครงการ/กิจกรรม/แผนงาน และหน่วยรับผิดชอบ

3.3.1 วิสัยทัศน์การรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย

แผนบูรณาการเพื่อขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์นี้ ได้กำหนดวิสัยทัศน์การรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย คือ

“ประเทศไทยมีการใช้ระบบคลาวด์ที่มั่นคงปลอดภัย น่าเชื่อถือ มีเอกภาพ และมีประสิทธิภาพภายใต้อธิปไตยข้อมูลและความยืดหยุ่นทางไซเบอร์ โดยสอดคล้องกับมาตรฐานสากลเพื่อสนับสนุนนโยบายของประเทศในการใช้ระบบคลาวด์สำหรับภารกิจหรือการให้บริการดิจิทัลเพื่อเศรษฐกิจ สังคม ความมั่นคง และประชาชน”

3.3.2 หลักการกำกับการขับเคลื่อน (Guiding Principles)

เพื่อให้การขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทยเป็นไปในทิศทางเดียวกัน มีเอกภาพ และลดการตีความที่แตกต่างกันระหว่างหน่วยงาน จึงกำหนด “หลักการกำกับการขับเคลื่อน” เพื่อใช้เป็นกรอบพิจารณาร่วมกันในการออกแบบยุทธศาสตร์ ตัวชี้วัด โครงการ/กิจกรรม ตลอดจนการกำกับติดตามและประเมินผล โดยหลักการดังกล่าวสะท้อนความสมดุลระหว่างการยกระดับความมั่นคงปลอดภัยไซเบอร์กับภาระต้นทุนและความพร้อมของผู้มีส่วนเกี่ยวข้องทุกภาคส่วน ทั้งผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์ หน่วยงานกำกับดูแล และหน่วยงานตรวจประเมิน/รับรองมาตรฐาน ดังนี้

(1) การบริหารความเสี่ยงและกำหนดมาตรการแบบหลายระดับ (Risk-based and Multi-tier)

การกำหนดมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์จะยึดหลักการบริหารความเสี่ยงเป็นพื้นฐาน และใช้แนวคิดการจำแนกชั้นข้อมูลหรือระบบสารสนเทศตามระดับความอ่อนไหวและความสำคัญ/วิกฤต (Data sensitivity and data/System criticality) เพื่อให้มาตรการและการรับรองมาตรฐานมีความเหมาะสมกับระดับผลกระทบที่อาจเกิดขึ้นจริง ทั้งนี้ การกำหนดข้อกำหนดขั้นต่ำไม่ควรเป็นแบบเดียวกันทั้งหมด แต่ควรปรับระดับความเข้มข้นของมาตรการให้สอดคล้องกับบริบทของภารกิจ ข้อมูล และรูปแบบการใช้บริการคลาวด์

(2) ความรับผิดชอบร่วมกันและความรับผิดต่อผลลัพธ์ (Shared Responsibility and Accountability)

การใช้บริการคลาวด์ไม่ทำให้ความรับผิดชอบของหน่วยงานผู้ใช้บริการสิ้นสุดลง แต่เปลี่ยนลักษณะความรับผิดชอบให้ต้องบริหารจัดการร่วมกับผู้ให้บริการคลาวด์อย่างเป็นระบบ ดังนั้น พึงกำหนดบทบาทความรับผิดชอบ และขอบเขตการควบคุมของแต่ละฝ่ายให้ชัดเจนตามรูปแบบบริการ (เช่น IaaS/PaaS/SaaS) และกำหนดกลไกการพิสูจน์ได้ (accountability) ผ่านหลักฐาน/บันทึก (log/evidence) การรายงานและจัดการเหตุการณ์ การตรวจสอบ และข้อกำหนดในสัญญา/ข้อตกลงการให้บริการ เพื่อให้หน่วยงานกำกับดูแลสามารถติดตามความสอดคล้องและยกระดับคุณภาพการปฏิบัติได้อย่างเป็นรูปธรรม

(3) อธิปไตยข้อมูลและการปฏิบัติตามกฎหมายโดยออกแบบตั้งแต่ต้น (Data Sovereignty and Lawful Access-by-design)

การออกแบบและเลือกใช้บริการคลาวด์พึงคำนึงถึงอธิปไตยข้อมูล (Data Sovereignty) กฎหมายและข้อกำหนดด้านการคุ้มครองข้อมูล/ความมั่นคงของประเทศ ตลอดจนเงื่อนไขการจัดเก็บและประมวลผลข้อมูลข้ามพรมแดน โดยควรกำหนดแนวทางด้านถิ่นที่ตั้งข้อมูล (Residency) การเข้าถึงข้อมูล การร้องขอตามอำนาจกฎหมาย (Lawful Request) รวมถึงแนวทางการเข้ารหัสและการบริหารจัดการกุญแจเข้ารหัสที่ตรวจสอบได้ และการเก็บรักษาหลักฐานดิจิทัลให้เป็นมาตรฐานเดียวกันในระดับประเทศ รวมทั้งนำไปใช้ได้จริงในการจัดซื้อจัดจ้างและการทำสัญญา เพื่อให้การใช้คลาวด์สนับสนุนภารกิจของรัฐ เศรษฐกิจ สังคม และความมั่นคง โดยไม่เพิ่มความเสี่ยงด้านกฎหมายและการกำกับดูแล

(4) ความต่อเนื่อง ความยืดหยุ่น และความสามารถในการย้ายออก (Resilience, Continuity, and Portability-by-design)

ระบบและบริการสำคัญของประเทศบนคลาวด์พึงถูกออกแบบให้คงความพร้อมใช้งานและฟื้นตัวได้ตามระดับความสำคัญของภารกิจ โดยให้ความสำคัญกับการจัดทำและทบทวนแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) และแผนกู้คืนระบบจากภัยพิบัติ (DRP) รวมถึงการกำหนดเป้าหมายระยะเวลาในการกู้คืนระบบ (RTO) และจุดกู้คืนข้อมูล (RPO) ที่เหมาะสม รวมถึงการสำรองและทดสอบการกู้คืนอย่างสม่ำเสมอตลอดจนการออกแบบเพื่อลดการผูกติดกับผู้ให้บริการรายใดรายหนึ่ง (Lock-in) ผ่านแนวทางการพกพาย้ายระบบ/ข้อมูล (Portability) ความสามารถในการทำงานร่วมกัน (Interoperability) และ “แผนการย้ายออกจากคลาวด์ (Cloud Exit Strategy)” ที่ปฏิบัติได้จริง เพื่อยกระดับความทนทานต่อเหตุขัดข้องและภัยคุกคามในระยะยาว

(5) การประเมินความสอดคล้องอย่างต่อเนื่องโดยใช้ข้อมูลและระบบอัตโนมัติ (Continuous Assurance and Automation-first)

การกำกับดูแลและการรับรองมาตรฐานพึงมุ่งสู่การประเมินอย่างต่อเนื่อง (Continuous assurance) มากกว่าการตรวจเอกสารเป็นครั้งคราว โดยสนับสนุนการใช้เครื่องมืออัตโนมัติในการรวบรวมหลักฐานวัดผลความสอดคล้อง เฝ้าระวังความเสี่ยง และรายงานผลแบบเป็นระบบเพื่อเพิ่มความโปร่งใส ลดภาระเอกสารซ้ำซ้อน และทำให้การตัดสินใจของผู้บริหารอาศัยข้อมูลที่เชื่อถือได้ทั้งในระดับหน่วยงานและระดับประเทศ เช่น Dashboard/Registry และกลไกการรายงานผลที่เชื่อมโยงกันได้

(6) ความได้สัดส่วนและการสนับสนุนการนำไปใช้จริง (Proportionality and Inclusion)

มาตรการและกลไกกำกับดูแลพึงออกแบบให้ได้สัดส่วนกับความเสี่ยง และเอื้อต่อการนำไปใช้จริงโดยคำนึงถึงความแตกต่างด้านขนาด ภารกิจ และศักยภาพของหน่วยงานและผู้ประกอบการ เพื่อไม่ให้เกิดภาระเกินจำเป็น อันนำไปสู่ความไร้ประสิทธิภาพด้านต้นทุน ทั้งนี้ ภาครัฐพึงจัดให้มีเครื่องมือสนับสนุนการปฏิบัติ (เช่น

แม่แบบ/แนวปฏิบัติกลาง ข้อกำหนดใน TOR/สัญญา แนวทางจัดซื้อจัดจ้าง และกลไก One-stop) เพื่อช่วยลดความซ้ำซ้อน ลดความไม่สอดคล้อง และยกระดับมาตรฐานขั้นต่ำร่วมกันได้ทั้งประเทศ

3.3.3 เป้าหมายเชิงยุทธศาสตร์ (Strategic Outcomes)

จากวิสัยทัศน์และหลักการกำกับการขับเคลื่อนดังกล่าว จึงได้กำหนดเป้าหมายเชิงยุทธศาสตร์ (Strategic Outcomes) ที่ต้องการไว้ ดังนี้

เป้าหมายเชิงยุทธศาสตร์ที่ 1: ประเทศไทยมีการกำกับดูแลและการตรวจรับรองมาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ที่เป็นไปในแนวทางเดียวกัน (Unified Cloud Security Governance and Assurance)

เพื่อให้การดำเนินงานของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตลอดจนผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ มีเอกภาพ โปร่งใส ตรวจสอบได้ และอาศัยเกณฑ์เดียวกันทั้งประเทศ อันจะนำไปสู่การลดความซ้ำซ้อนในการดำเนินงาน (Reduce redundant efforts) ลดความไม่สอดคล้องในการดำเนินงาน (Reduce inconsistencies) และลดความไร้ประสิทธิภาพด้านต้นทุน (Cost inefficiencies) มิให้เป็นภาระเกินความจำเป็น

ทั้งนี้ การขับเคลื่อนผลลัพธ์ดังกล่าวให้เกิดขึ้นจริง ต้องมีกลไกการยอมรับผลเทียบเคียงและการใช้ประโยชน์จากผลการประเมินเดิมอย่างเป็นระบบ (Reuse และ Presumption of Adequacy) ควบคู่กับการยกระดับคุณภาพ มาตรฐานวิชาชีพ และการกำกับดูแลผู้ตรวจประเมิน/หน่วยงานให้บริการตรวจรับรอง (Auditor/Certify Body) เพื่อให้ผลการประเมินและการรับรองมีความน่าเชื่อถือ สอดคล้องกัน และสามารถนำไปใช้ต่อยอดในการกำกับดูแลและจัดซื้อจัดจ้างได้อย่างมีประสิทธิภาพ

ผลลัพธ์ที่คาดหวัง (Expected Deliverables) เช่น

- One-Stop Cloud Assurance and Registry แพลตฟอร์ม/ระบบกลางสำหรับขึ้นทะเบียน ติดตามสถานะการประเมินและการรับรอง และเผยแพร่รายชื่อผู้ให้บริการคลาวด์และหน่วยงานให้บริการตรวจรับรองที่เกี่ยวข้องในรูปแบบที่ใช้ร่วมกันทั้งประเทศ โดยมีกลไกการเข้าถึงข้อมูลตามสิทธิ (Role-based Access) และมีรูปแบบข้อมูล/เอกสารมาตรฐาน เพื่อลดการขอเอกสารซ้ำและลดภาระหน่วยงาน รวมถึงแบบฟอร์มกลางสำหรับ Cloud Security Transparency Profile/Self-Disclosure

- Reuse & Presumption of Adequacy Mechanism หลักเกณฑ์และกระบวนการยอมรับผลเทียบเคียง/ใช้ผลประเมินเดิมได้อย่างเป็นทางการ (เช่น การกำหนดเกณฑ์เทียบเคียงกับมาตรฐานสากล และการประเมินแบบ Delta/Gap Assessment เฉพาะส่วนที่ต่าง) รวมถึงแนวทาง Mutual Recognition/Fast-track สำหรับผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ที่มีผลการรับรอง/ผลการประเมินตามมาตรฐานที่เทียบเคียงได้ เพื่อลดภาระตรวจซ้ำซ้อน ลดต้นทุน และลดคอขวดของกระบวนการรับรอง

- Quality & Oversight for Auditor/Certify Body ระบบยกระดับคุณภาพผู้ตรวจประเมินและหน่วยงานให้บริการตรวจรับรองให้เป็นมาตรฐานเดียวกัน เช่น หลักเกณฑ์ด้านสมรรถนะและความเชี่ยวชาญ (Competency/Qualification) หลักความเป็นกลางและการจัดการผลประโยชน์ทับซ้อน (Impartiality/Conflict of Interest) แนวทางการทวนสอบคุณภาพงานตรวจ (Quality Review/Peer Review/Random Audit) กลไกรับเรื่องร้องเรียนและอุทธรณ์ที่ครอบคลุมกรณี CSP/ผู้เกี่ยวข้องในห่วงโซ่อุปทานด้วย และมาตรการทางปกครอง/วินัยตามสัดส่วน เพื่อให้เกิดความน่าเชื่อถือและความสอดคล้องของผลการตรวจประเมินทั่วประเทศ

- Unified Assurance SOP/Template/Evidence Pack ชุดแนวทางปฏิบัติมาตรฐาน (SOP) แม่แบบเอกสาร และรูปแบบชุดหลักฐานกลาง (Evidence Pack) ที่ใช้ร่วมกันระหว่างหน่วยงานกำกับดูแล

/หน่วยงานตรวจรับรอง/หน่วยงานผู้ใช้บริการ เพื่อให้การเตรียมหลักฐาน การยื่นขอรับรอง การทบทวนผล และการติดตามการแก้ไข เป็นไปในรูปแบบเดียวกัน ลดภาระและลดความคลาดเคลื่อนในการตีความ

- Procurement Pack + TOR/Contract Template + Whitelist ชุดเครื่องมือสนับสนุนการจัดซื้อจัดจ้างที่เชื่อมโยงกับผลการรับรองและระดับความเสี่ยง เช่น แนวทางกำหนดคุณสมบัติผู้ให้บริการ ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ใน TOR/สัญญา แม่แบบเงื่อนไขสำคัญ และบัญชีรายชื่อ/สถานะผู้ให้บริการที่ผ่านเกณฑ์ (Whitelist/Registry View) ที่จัดทำร่วมกับหน่วยงานที่เกี่ยวข้องเพื่อให้หน่วยงานนำไปใช้ได้ทันทีและลดความเสี่ยงจากการจัดซื้อจัดจ้างที่ไม่สอดคล้องกับมาตรฐาน

เป้าหมายเชิงยุทธศาสตร์ที่ 2: ผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์มีการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ตามระดับชั้นข้อมูลหรือระบบสารสนเทศ (Multi-tier Cloud Security) และตามรูปแบบการให้บริการคลาวด์ (Service Model) โดยกำหนดความรับผิดชอบร่วมกัน (Shared Responsibility) ให้ชัดเจน ครอบคลุมทั้ง IaaS/PaaS/SaaS และสภาพแวดล้อมแบบ Hybrid/Community/Private/Public

ทั้งนี้ เพื่อให้การคุ้มครองบริการภาครัฐที่สำคัญ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และข้อมูลส่วนบุคคลของคนไทย เป็นไปอย่างเหมาะสมตามระดับความอ่อนไหวและความสำคัญของข้อมูล/ระบบ (Data Sensitivity & Criticality) ภายใต้หลักการอธิปไตยข้อมูล (Data Sovereignty) ซึ่งหลักการนี้มีการใช้งานจริงและประสบความสำเร็จมาแล้วในต่างประเทศ โดยเฉพาะการควบคุมข้อมูลและการเข้าถึงข้อมูลข้ามพรมแดน และการบริหารจัดการกุญแจเข้ารหัส (Key Management) เพื่อให้หน่วยงานสามารถกำกับดูแลการเก็บ ใช้ โยกย้าย และทำลายข้อมูลได้อย่างตรวจสอบได้ และลดความเสี่ยงจากความคลุมเครือของบทบาทหน้าที่ระหว่าง CSC และ CSP เมื่อเกิดเหตุการณ์ทางไซเบอร์ (แนวคิดการแบ่งขอบเขตความรับผิดชอบตาม Service Model สอดคล้องกับกรอบนิยาม/คุณลักษณะและโมเดลบริการคลาวด์ของ NIST และแนวทางด้านความมั่นคงปลอดภัยใน Public Cloud ของ NIST)

ผลลัพธ์ที่คาดหวัง (Expected Deliverables) เช่น

- Government Data Classification-to-Cloud Mapping แนวทางกลางเพื่อให้หน่วยงานกำหนดระดับความสำคัญของข้อมูลหรือระบบสารสนเทศระดับใด ควรใช้งานบนสภาพแวดล้อมคลาวด์แบบใด และควรเลือกใช้บริการแบบใด ให้สอดคล้องกับระดับชั้นข้อมูล ความสำคัญของระบบ ข้อกำหนดด้านกฎหมาย และความคาดหวังด้านความต่อเนื่องของบริการ โดยกำหนดให้หน่วยงานดำเนินการจัดจำแนกประเภทข้อมูล (Data Classification) เป็นโครงสร้างพื้นฐานแรกเริ่มก่อนการเลือกระดับการเข้ารหัสและการบริหารจัดการสิทธิ์ ทั้งนี้ แนวทางดังกล่าวควรครอบคลุมทั้งการเลือก Deployment Model ที่เหมาะสม (เช่น การใช้งานในประเทศ/ข้ามพรมแดนตามเงื่อนไขที่กำหนด) และการเลือก Service Model (IaaS/PaaS/SaaS) พร้อมอธิบายเหตุผลเชิงความมั่นคงปลอดภัยและขอบเขตการควบคุมที่แตกต่างกันในแต่ละโมเดล ตลอดจนกำหนดเงื่อนไขในการปกป้องข้อมูล และมาตรการป้องกันการเข้าถึงข้อมูลชั้นความลับของผู้ใช้บริการโดยเด็ดขาด

- Shared Responsibility Matrix + RACI ที่ใช้ร่วมกันทั้งประเทศเป็นตารางกลางที่ระบุว่าใครต้องทำอะไรอย่างชัดเจนระหว่างผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) รวมถึงผู้มีส่วนเกี่ยวข้องที่จำเป็น (เช่น ผู้พัฒนา/ผู้รับจ้างพัฒนา ผู้ให้บริการบริหารจัดการระบบ ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ หรือผู้รับเหมาช่วง) โดยจัดทำให้สอดคล้องทั้งตาม Service Model และตาม Tier/ระดับชั้นข้อมูลหรือระบบสารสนเทศ เพื่อให้ทุกฝ่ายเข้าใจขอบเขตการควบคุมและความรับผิดชอบตรงกัน

- Multi-tier Cloud Control Baseline ที่บูรณาการอธิปไตยข้อมูลและการบริหารจัดการกุญแจเข้ารหัสเป็นแกนกลาง ปรับชุดข้อกำหนดขั้นต่ำให้มีความชัดเจนว่า “ความมั่นคงปลอดภัยไซเบอร์บนคลาวด์” มิได้หมายถึงเพียงการเข้ารหัสข้อมูลเท่านั้น แต่ต้องครอบคลุมมิติของอธิปไตยข้อมูลและการกำกับดูแลการเข้าถึง

ข้อมูลอย่างเป็นระบบ โดยกำหนดเป็นโปรไฟล์กลางที่หน่วยงานสามารถนำไปใช้ร่วมกับการกำหนด Tier ได้อย่างเป็นรูปธรรม เช่น หลักเกณฑ์ด้าน Data Residency/Data Location Transparency ข้อกำหนดด้านการเข้ารหัสขณะส่งผ่านและขณะจัดเก็บ (In-transit/At-rest) หลักเกณฑ์ เรื่องการเป็นเจ้าของและการควบคุมกุญแจ (Key Ownership & Control) ข้อกำหนดด้านวงจรชีวิตกุญแจ (Key Lifecycle) แนวทางการรองรับกรณีกุญแจรั่วไหล/ถูกเจาะ/ถูกบังคับเปิดเผย (Compromise-Recovery)

- Template สำหรับ Data Processing/Residency/Access & Lawful Request ในสัญญาและ TOR โดยให้ครอบคลุมข้อกำหนดอธิปไตยข้อมูลและกุญแจเข้ารหัสในภาษาสัญญาที่ใช้ได้จริง ตลอดจนข้อกำหนดที่ว่าข้อมูลสำคัญที่จะนำไปใช้ในสภาพแวดล้อมที่ไม่ใช่ Production จะต้องผ่านกระบวนการทำ Data Masking และสามารถใช้ร่วมกันได้อย่างเป็นมาตรฐาน ลดความต่างในการร่าง TOR และลดความเสี่ยงจากช่องว่างทางสัญญาที่กระทบต่ออธิปไตยข้อมูลในทางปฏิบัติ เช่น (1) หลักเกณฑ์และขั้นตอนเมื่อมีคำขอเข้าถึงข้อมูลจากหน่วยงานของรัฐต่างประเทศ/คำสั่งศาลต่างประเทศ (Lawful Request Handling) โดยกำหนดเงื่อนไขการแจ้งเตือน ช่องทางการประสานงาน และขอบเขตการเปิดเผยข้อมูลให้ชัดเจน (2) เงื่อนไขการใช้ผู้รับเหมาช่วง/ห่วงโซ่อุปทาน (Sub-processor/Supply Chain) รวมถึงการแจ้งเปลี่ยนแปลง ตรวจสอบช่องโหว่และการควบคุมความเสี่ยงที่เกี่ยวข้อง (3) สิทธิการตรวจสอบและหลักฐานการควบคุม (Audit & Evidence) ที่เชื่อมโยงกับ Shared Responsibility Matrix และ (4) เงื่อนไขการเข้ารหัสและการบริหารกุญแจที่สอดคล้องกับระดับชั้นข้อมูล รวมถึงความคาดหวังด้านการเก็บบันทึก การพิสูจน์เหตุการณ์ การสนับสนุนการสืบค้นร่องรอยเมื่อเกิดเหตุ และกระบวนการของผู้ให้บริการคลาวด์ในการลบและทำลายข้อมูลที่ค้างอยู่บนฮาร์ดแวร์อย่างถาวรในกรณีที่หน่วยงานยกเลิกการใช้บริการเพื่อไม่ให้เกิดการดึงข้อมูลกลับ

- Service Model-Aware Assessment เพื่อให้การตรวจรับรองสะท้อนความรับผิดชอบจริงในระบบคลาวด์ จัดทำแนวทางการประเมินที่กำหนดให้การตรวจประเมินต้องพิจารณาขอบเขตการควบคุมและหลักฐานตาม Service Model และตาม Tier อย่างเป็นระบบ เพื่อป้องกันการตรวจแบบเหมารวมที่ทำให้เรื่องที่อยู่ในความรับผิดชอบของฝ่ายหนึ่งถูกผลักภาระไปอีกฝ่ายโดยไม่ตั้งใจ รวมถึงให้รองรับแนวคิดการสืบทอดการควบคุม/การใช้ผลการประเมินร่วม (Control Inheritance /Reuse) อย่างมีมาตรฐาน

เป้าหมายเชิงยุทธศาสตร์ที่ 3: บริการภาครัฐที่สำคัญและโครงสร้างพื้นฐานสำคัญทางสารสนเทศบนคลาวด์มีความมั่นคงปลอดภัยและความยืดหยุ่นทางไซเบอร์ (National Cloud Security and Resilience) เพื่อให้สามารถให้บริการได้อย่างเที่ยงตรง มีความต่อเนื่อง ทนทานต่อภัยคุกคามทางไซเบอร์ และสามารถฟื้นตัวได้อย่างรวดเร็ว โดยยกระดับจากการติดตามแบบรายงานเป็นรอบไปสู่การประกันความมั่นคงปลอดภัยอย่างต่อเนื่อง (Continuous Assurance) ที่อาศัยข้อมูลเชิงเทคนิคและหลักฐานการปฏิบัติจริงในการเฝ้าระวังประเมินความเสี่ยง และกำกับการปรับแก้ให้ทันต่อสถานการณ์ ทั้งนี้ เพื่อสร้างและคงไว้ซึ่งความเชื่อมั่นต่อประชาชน เศรษฐกิจ สังคม และความมั่นคงของประเทศ

ผลลัพธ์ที่คาดหวัง (Expected Deliverables) เช่น

- การกำหนดขอบเขตบริการหรือภารกิจบนคลาวด์ที่มีนัยสำคัญระดับชาติ และเกณฑ์ความพร้อมด้านความต่อเนื่อง โดยกำหนดคุณลักษณะของหน่วยงานหรือบริการที่ต้องมีค่าเป้าหมายขั้นต่ำด้านความพร้อมให้บริการและการกู้คืน (เช่น RTO/RPO) ให้สอดคล้องกับระดับชั้นข้อมูลหรือระบบสารสนเทศ และระดับความสำคัญของภารกิจเพื่อให้ทุกหน่วยงานตีความและวางแผนได้ในแนวทางเดียวกัน

- การทดสอบความต่อเนื่องและการฟื้นตัวที่ “พิสูจน์ได้จริง” สำหรับภารกิจหรือบริการที่สำคัญ โดยกำหนดให้มีการทดสอบแผนความต่อเนื่อง/แผนกู้คืน (DR Test) และการทดสอบกู้คืนข้อมูลหรือระบบ (Restore Test) อย่างเป็นกิจวัตรตามระดับความสำคัญ รวมถึงการซ้อมตอบสนองเหตุและการฟื้นตัว

จากเหตุร้ายแรง (เช่น ransomware/cyber disruption) เพื่อยืนยันว่าแผนและขั้นตอนสามารถใช้งานได้จริงเมื่อเกิดเหตุ

- แนวทางการลดความเสี่ยงจากการพึ่งพาผู้ให้บริการรายใดรายหนึ่ง และการย้ายออกจากคลาวด์ที่ทำได้จริง (Cloud Exit Strategy) โดยจัดทำข้อกำหนดขั้นต่ำและแม่แบบแนวทางปฏิบัติที่ครอบคลุมการพกพาข้อมูล/เวิร์กโหลด การส่งมอบหลักฐาน/บันทึกที่จำเป็น การกำหนดกรอบเวลาการถอนย้าย และการทดสอบแผนย้ายออกเป็นระยะ เพื่อให้หน่วยงานสามารถลด lock-in และรักษาความต่อเนื่องของบริการได้อย่างเป็นรูปธรรม

- Minimum Cloud Security Operations Baseline สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่ครอบคลุมทั้งมิติความมั่นคงปลอดภัยและความยืดหยุ่นทางไซเบอร์ ตั้งแต่การบริหารตัวตนและสิทธิ์ (Identity/Access/Privilege) การจัดการช่องโหว่และแพตช์ (Vulnerability/Patch) การจัดการการเปลี่ยนแปลงและค่าตั้งต้นที่ปลอดภัย (Change/Secure Configuration) การบันทึกเหตุและการเฝ้าระวัง (Logging/Monitoring) การตอบสนองเหตุและความพร้อมด้านนิติพิสูจน์ (Incident Response/Forensics Readiness) ตลอดจนการประยุกต์ใช้แนวคิด Zero Trust ให้เหมาะสมกับบริบทของภารกิจ

- National Cloud Continuous Assurance Platform ซึ่งเป็นกลไกกลางสำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการติดตามสถานะความเสี่ยงและการปฏิบัติตามมาตรการที่สำคัญอย่างต่อเนื่อง เช่น การเชื่อมโยงข้อมูลสินทรัพย์และสภาพแวดล้อมคลาวด์ที่เกี่ยวข้อง การรวบรวมสัญญาณและหลักฐานอัตโนมัติจากการปฏิบัติจริง การประเมินความเสี่ยงแบบต่อเนื่องพร้อมกลไกการแจ้งเตือนอัตโนมัติเมื่อเกิดความไม่สอดคล้อง (Compliance drift) แพลตฟอร์มควรสนับสนุนรูปแบบข้อมูลที่เป็นมาตรฐานกลางสำหรับ automation เช่น Machine-readable Control/Evidence มีการจัดทำมุมมองรายงานผลที่เหมาะสมตามบทบาท การแลกเปลี่ยนและรายงานเหตุการณ์แบบอัตโนมัติ (threat/incident sharing) พร้อม playbook มาตรฐานกลาง เพื่อสนับสนุนการตอบสนองร่วมกันและลดเวลาการฟื้นตัว

- การตรวจสอบ (Cloud Security Auditing) ที่น่าเชื่อถือและสมดุล โดยออกแบบให้การตรวจสอบยืนยันผลลัพธ์สามารถทำได้ทั้งแบบตามรอบและแบบมุ่งเป้า (Risk-based/Random/Event-driven) และใช้ประโยชน์จากหลักฐานที่เกิดจากกลไก Continuous Assurance เพื่อลดความซ้ำซ้อน เพิ่มความเที่ยงตรงของผลการตรวจสอบ และทำให้การกำกับดูแลมีประสิทธิภาพมากยิ่งขึ้น

เป้าหมายเชิงยุทธศาสตร์ที่ 4: ประเทศไทยมีบุคลากรที่มีขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ที่ครอบคลุมและเพียงพอต่อการขับเคลื่อนประเทศ (Cloud Security Workforce and Capability) ทั้งในกลุ่มผู้บริหาร ผู้กำกับดูแล ผู้ตรวจประเมิน ผู้ปฏิบัติ รวมถึงบุคลากรด้านการจัดซื้อจัดจ้างและการบริหารงบประมาณที่เกี่ยวข้องกับบริการคลาวด์ โดยมีกรอบสมรรถนะและเส้นทางอาชีพที่ชัดเจน มีการพัฒนาองค์ความรู้และทักษะอย่างต่อเนื่องตามบทบาทหน้าที่ และมีระบบสนับสนุนเชิงปฏิบัติที่ช่วยให้หน่วยงานทุกขนาด โดยเฉพาะหน่วยงานขนาดเล็กและหน่วยงานระดับพื้นที่สามารถปฏิบัติตามมาตรฐานได้จริงอย่างสอดคล้องเป็นแนวทางเดียวกัน ลดความเสี่ยงด้านความมั่นคงปลอดภัย ลดภาระการตีความที่แตกต่าง และเพิ่มประสิทธิภาพในการใช้ทรัพยากรและงบประมาณของภาครัฐอย่างคุ้มค่า

ผลลัพธ์ที่คาดหวัง (Expected Deliverables) เช่น

- Role-based Competency and Career Pathway ที่ระบุความรู้ ทักษะ และความรับผิดชอบขั้นต่ำที่สอดคล้องกับบทบาทสำคัญ ได้แก่ ผู้บริหาร ผู้กำกับดูแล ผู้ตรวจประเมิน ผู้ปฏิบัติ (รวมถึงสายงานที่เกี่ยวข้องกับ Cloud Security/Cloud Operations/Incident Response) ตลอดจนแนวทางการประยุกต์ใช้กรอบบทบาทให้เป็นภาษากลางในการพัฒนาคน การสรรหา และการประเมินความพร้อมของหน่วยงาน

- Continuous Upskilling/Reskilling Program ครอบคลุมหลักสูตรขั้นต่ำที่ต้องมีในแต่ละบทบาท (เช่น Cloud Security Governance, Shared Responsibility ตาม Service Model, Security Operations บนคลาวด์, Incident Response/Forensics Readiness, Data Protection & Key Management) พร้อมแนวทาง Train-the-Trainer เพื่อให้หน่วยงานสามารถขยายผลได้ด้วยตนเองในระยะยาว

- Cloud Security Procurement & Contracting Enablement Pack เพื่อทำให้ข้อกำหนดด้านความมั่นคงปลอดภัยถูกนำไปใช้ได้จริงในขอบเขตของงาน TOR/สัญญา และลดความเสี่ยงจากการจัดซื้อจัดจ้างที่ไม่สอดคล้องกันระหว่างหน่วยงาน เช่น แม่แบบ TOR/สัญญา/เกณฑ์ประเมินข้อเสนอ (Evaluation Criteria) ที่ผูกกับข้อกำหนดมาตรฐาน หมวดเงื่อนไขด้านข้อมูลและความมั่นคงปลอดภัยที่สำคัญ แนวทางการจัดซื้อจัดจ้างที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานทุกขนาดเพื่อให้ดำเนินการได้เป็นแนวทางเดียวกัน

- Cloud Security Starter Kit for Small Agencies เพื่อให้เริ่มทำได้ทันทีโดยไม่ต้องออกแบบใหม่ทั้งหมด และลดความเสี่ยงจากการตีความคลาดเคลื่อน เช่น ชุดแนวทางขั้นต่ำที่ต้องทำ (Minimum-viable Controls) ตามระดับชั้นข้อมูล/บริการที่ใช้งาน ตัวอย่างสถาปัตยกรรมอ้างอิง (Reference Architecture) และตัวอย่างการตั้งค่าที่ปลอดภัย (Secure-by-Default Configuration) Checklists/Playbooks/แบบฟอร์มหลักฐานที่ใช้ยืนยันการปฏิบัติได้จริง แนวทางการเลือกใช้บริการ/ทางเลือกการพึ่งพาศูนย์กลาง (เช่น บริการที่ปรึกษากลาง/แนวทางใช้บริการร่วม)

- National Cloud Security Expert Network & Advisory ที่ทำหน้าที่เป็นกลไกช่วยนำไปใช้ ไม่ใช่เพียงเวทีแลกเปลี่ยนความรู้ โดยมีทั้งฐานความรู้กลาง (knowledge base) ช่องทางคำปรึกษาเชิงปฏิบัติ และแนวทางการส่งต่อ/ยกระดับกรณีที่หน่วยงานมีข้อจำกัดด้านบุคลากรหรือจำเป็นต้องเร่งรัดการแก้ไข

3.3.4 ยุทธศาสตร์ กลยุทธ์ ตัวชี้วัด/ค่าเป้าหมาย โครงการ/กิจกรรม/แผนงาน และหน่วยรับผิดชอบ

เพื่อให้บรรลุวิสัยทัศน์การรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทยดังกล่าว จึงได้กำหนดยุทธศาสตร์การดำเนินงาน 3 ยุทธศาสตร์ ดังนี้

ยุทธศาสตร์ที่ 1 รวมพลังภาครัฐและเอกชน

ยุทธศาสตร์ที่ 1 มีบทบาทเป็นกลไกกลางในการประสานผู้มีส่วนเกี่ยวข้อง เพื่อให้การดำเนินการตามมาตรฐานและมาตรการสำคัญของประเทศเกิดผลในทางปฏิบัติ โดยเชื่อมโยงการทำงานร่วมกันระหว่างภาครัฐ ภาคเอกชน และภาคส่วนระหว่างประเทศ ไปสู่เป้าหมายเชิงยุทธศาสตร์ของแผน ได้แก่ การกำกับดูแลและการตรวจรับรองที่เป็นเอกภาพ การรักษาความมั่นคงปลอดภัยไซเบอร์และคุ้มครองข้อมูลส่วนบุคคลตามระดับชั้นข้อมูลและรูปแบบบริการ การยกระดับความมั่นคงปลอดภัยและความยืดหยุ่นของบริการสำคัญบนคลาวด์ และการพัฒนาขีดความสามารถของบุคลากรให้เพียงพอต่อการขับเคลื่อนประเทศ

วัตถุประสงค์

1. เพื่อสร้างกลไกความร่วมมือระหว่างภาครัฐและเอกชนทั้งภายในและต่างประเทศ ในการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย รวมถึงการมีส่วนร่วมในการกำหนดทิศทางแนวทาง และมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ให้สอดคล้องกับกฎหมาย มาตรฐานสากล และความต้องการของประเทศ

2. เพื่อสร้างกลไกความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ในการสนับสนุนการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ และอาชญากรรมทางไซเบอร์ (หน่วยงานภาครัฐ เอกชน หน่วยงานต่างประเทศ หน่วยงานนโยบาย หน่วยงานบังคับใช้กฎหมาย)

3. เพื่อสร้างกลไกกลุ่มผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทยในการสนับสนุนการดำเนินงานตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

4. เพื่อสร้างกลไกการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานที่ช่วยให้การดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์มีประสิทธิภาพมากยิ่งขึ้น

กลยุทธ์การดำเนินงาน

กลยุทธ์ที่ 1.1

- ส่งเสริมและสนับสนุนความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนทั้งภายในและต่างประเทศ

เป้าหมายกลยุทธ์

- มีสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทยที่ครอบคลุมผู้มีส่วนได้ส่วนเสียและผู้ที่เกี่ยวข้อง (ยุทธศาสตร์ที่ 1 วัตถุประสงค์ที่ 1, 2 และ 4)
- มีกลไกความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนทั้งภายในและต่างประเทศ ในการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย รวมถึงการมีส่วนร่วมในการกำหนดทิศทาง แนวทาง และมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ให้สอดคล้องกับกฎหมาย มาตรฐานสากล และความต้องการของประเทศ (ยุทธศาสตร์ที่ 1 วัตถุประสงค์ที่ 1)

ตัวชี้วัดของกลยุทธ์/ค่าเป้าหมาย

ตัวชี้วัดที่ 1 มีการทบทวนสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย[1] ไม่น้อยกว่า 1 ครั้งต่อปี
ตัวชี้วัดที่ 2 มีการจัดทำหรือทบทวนแนวทางในการส่งเสริมและสนับสนุนความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนทั้งภายในและต่างประเทศ ไม่น้อยกว่า 1 ครั้งต่อปี
ตัวชี้วัดที่ 3 มีกิจกรรมส่งเสริมและสนับสนุนความร่วมมือ[2]ระหว่างหน่วยงานภาครัฐและเอกชนทั้งภายในและต่างประเทศ ไม่น้อยกว่า 3 กิจกรรมต่อปี
ตัวชี้วัดที่ 4 มีการจัดทำผลสรุปการรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียและผู้ที่เกี่ยวข้อง ไม่น้อยกว่า 1 ฉบับต่อปี
ตัวชี้วัดที่ 5 จำนวนคนหรือหน่วยงานที่นำเครื่องมือกลาง (template/TOR/evidence pack/registry view) ไปใช้ประโยชน์ รวมกันไม่น้อยกว่า 300 คนหรือหน่วยงาน ภายในปี พ.ศ. 2573

---

[1] สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย (Thailand's National Cloud Security Architecture) หมายถึง แผนผังแสดงสภาวะแวดล้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย โดยการกำหนดกลุ่มของผู้มีส่วนได้ส่วนเสียและผู้ที่เกี่ยวข้องทั้งภายในและต่างประเทศ ที่จะมาร่วมกันขับเคลื่อนประเทศไทยตามยุทธศาสตร์ทั้ง 3 เสาหลัก เพื่อให้บรรลุเป้าหมายและวิสัยทัศน์ของแผนบูรณาการฯ

[2] กิจกรรมส่งเสริมและสนับสนุนความร่วมมือ หมายถึง กิจกรรมใด ๆ ที่เป็นการดำเนินการร่วมกันโดยมีวัตถุประสงค์เพื่อการขับเคลื่อนแผนบูรณาการฯ รวมถึงการสนับสนุนการดำเนินงานตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 เช่น การทำ MOU การแลกเปลี่ยน การเยือน การจัดทำ action plan ร่วมกัน การประชุมเชิงปฏิบัติการ (Workshop) ทั้งในระดับประเทศและระดับนานาชาติ การส่งผู้แทนหน่วยงานเข้าร่วมกิจกรรม การสนับสนุนผู้เชี่ยวชาญ การแลกเปลี่ยนองค์ความรู้ การส่งบุคลากรเข้าร่วมกิจกรรมในเวทีนานาชาติ การจัดตั้งคณะทำงาน การสนับสนุนด้านเทคโนโลยี รวมถึงการจัดทำหรือพัฒนาแพลตฟอร์ม/อินเทอร์เฟซกลางสำหรับการแลกเปลี่ยนข้อมูลเชิงเทคนิคและหลักฐานแบบเป็นมาตรฐาน (machine-readable) เพื่อรองรับการติดตามและประเมินความเสี่ยงอย่างต่อเนื่องและลดภาระเอกสารซ้ำซ้อน เป็นต้น

โครงการขับเคลื่อนกลยุทธ์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
1.1.1 โครงการส่งเสริมและสนับสนุนความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชน ทั้งภายในและต่างประเทศ เพื่อยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย	1. กิจกรรมจัดตั้งกลไกความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ระหว่างหน่วยงานภาครัฐและเอกชน (Public–Private Cloud Security Collaboration Mechanism) • จัดทำหรือทบทวนสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย • จัดตั้งคณะกรรมการบริหารความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ • จัดทำหรือทบทวนแนวทางในการส่งเสริมและสนับสนุนความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชนทั้งในประเทศและต่างประเทศ • จัดการประชุมคณะกรรมการบริหารฯ อย่างน้อยปีละ 1–2 ครั้ง เพื่อกำหนดแนวทางและแผนการสร้างความร่วมมือและติดตามผลการดำเนินงานอย่างต่อเนื่อง 2. กิจกรรมกำหนดแนวทางส่งเสริมและสนับสนุนความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนทั้งภายในและต่างประเทศ • จัดทำรายชื่อหน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องทั้งภายในและต่างประเทศ • ประสานงานเพื่อกำหนดแนวทางการสร้างความร่วมมือ • จัดทำบันทึกความเข้าใจ (MOU) กับหน่วยงานภาครัฐและเอกชนทั้งภายในและต่างประเทศ รวมถึงหน่วยงานมาตรฐานและความมั่นคงปลอดภัยชั้นนำระดับโลก อาทิ ISO, CSA, ENISA, NIST, NCSC UK, IMDA Singapore โดยมุ่งเน้นในเรื่อง การเทียบเคียงระบบรับรองมาตรฐาน (Certification Alignment) กระบวนการจัดการเหตุการณ์ด้านความปลอดภัยไซเบอร์ (Incident Handling) แนวปฏิบัติที่ดีที่สุด (Best Practices) เป็นต้น	**หน่วยงานกำกับดูแล**[3] • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • หน่วยงานควบคุมหรือกำกับดูแล **หน่วยงานปฏิบัติ**[4] • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) • สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม (สมอ.) • หน่วยงานมาตรฐานและความมั่นคงปลอดภัย • หน่วยงานของรัฐ • หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ • ผู้ให้บริการคลาวด์ • หน่วยงานตรวจรับรองคุณภาพ • ภาคเอกชนหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

[3] หน่วยงานกำกับดูแล หมายถึง หน่วยงานที่มีหน้าที่ในการกำหนดแนวทางการดำเนินการและควบคุมกำกับดูแลให้โครงการหรือกิจกรรมตามที่ได้รับมอบหมายจากแผนบูรณาการฯ มีการปฏิบัติได้อย่างบรรลุผล รวมถึงการติดตาม ให้ความเห็น สนับสนุน และแก้ไขปัญหาอุปสรรคต่าง ๆ ที่อาจเกิดขึ้นด้วย

[4] หน่วยงานปฏิบัติ หมายถึง หน่วยงานที่มีหน้าที่ในการดำเนินการโครงการหรือกิจกรรมตามที่ได้รับมอบหมายจากแผนบูรณาการฯ มีการปฏิบัติได้อย่างบรรลุผล ทั้งนี้ อาจหมายรวมถึงการจัดทำคำของบประมาณไปยังผู้จัดสรรงบประมาณ หรือการจัดสรรงบประมาณของตนเพื่อตอบสนองต่อภารกิจหรือพันธกิจของหน่วยงาน รวมถึงนโยบายและแผนปฏิบัติการที่เกี่ยวข้องด้วย

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	3. กิจกรรมสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนทั้งภายในและต่างประเทศ • จัดกิจกรรมสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนในประเทศไทย โดยอาจเป็นกิจกรรมภายในประเทศหรือในระดับนานาชาติ • เข้าร่วมเวทีความร่วมมือระหว่างประเทศ เช่น การเข้าร่วมงานประชุมหรือเวิร์กช็อปด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ทั้งในระดับภูมิภาคและระดับนานาชาติ การนำผู้แทนจากทั้งภาครัฐและภาคเอกชนเข้าร่วมเสนอผลงาน กรณีศึกษา หรือมาตรฐานของไทย เพื่อสร้างภาพลักษณ์และรับข้อเสนอแนะ • การเสนอชื่อและสนับสนุนการแต่งตั้งผู้แทนจากประเทศไทยเข้าร่วมเป็นคณะทำงานจัดทำมาตรฐานสากลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ในเวทีสากล เช่น เสนอชื่อผู้แทนผ่านทางสำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม (สมอ.) เพื่อเข้าร่วมคณะทำงาน ISO ด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์	

กลยุทธ์ที่ 1.2

- จัดตั้งกลไกความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ในการสนับสนุนการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ และอาชญากรรมทางไซเบอร์

เป้าหมายกลยุทธ์

- มีกลไกความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ในการสนับสนุนการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ และอาชญากรรมทางไซเบอร์ (ยุทธศาสตร์ที่ 1 วัตถุประสงค์ที่ 2)
- มีกลไกการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานที่สอดคล้องกับมาตรฐานการแลกเปลี่ยนข้อมูลในระดับสากล[5] เพื่อสนับสนุนการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (ยุทธศาสตร์ที่ 1 วัตถุประสงค์ที่ 4)

ตัวชี้วัดของกลยุทธ์/ค่าเป้าหมาย

ตัวชี้วัดที่ 1 มีกิจกรรมเสริมสร้างความร่วมมือและการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ในการสนับสนุนการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ และอาชญากรรมทางไซเบอร์ จำนวนไม่น้อยกว่า 1 กิจกรรมต่อปี

ตัวชี้วัดที่ 2 มีแนวทางความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ในการสนับสนุนการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ และอาชญากรรมทางไซเบอร์ ภายในปี พ.ศ. 2569

ตัวชี้วัดที่ 3 มีกิจกรรมส่งเสริมและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานควบคุมหรือกำกับดูแล จำนวนไม่น้อยกว่า 1 กิจกรรมต่อปี

ตัวชี้วัดที่ 4 จำนวนหน่วยงานหรือผู้ให้บริการคลาวด์ที่เข้าร่วมกลไกแลกเปลี่ยนข้อมูล รวมจำนวนไม่น้อยกว่า 10 หน่วยงานหรือผู้ให้บริการคลาวด์ ภายในปี พ.ศ. 2573

โครงการขับเคลื่อนกลยุทธ์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
1.2.1 โครงการจัดตั้งและพัฒนากลไกความร่วมมือและการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ระบบ	1. กิจกรรมส่งเสริมและพัฒนากลไกความร่วมมือและการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ในการสนับสนุนการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์และอาชญากรรมทางไซเบอร์	**หน่วยงานกำกับดูแล** • กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.) • สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.)

[5] มาตรฐานการแลกเปลี่ยนข้อมูลในระดับสากล เช่น Traffic Light Protocol (TLP) หรือเทียบเท่า แนวทางการลบ/ปกปิดข้อมูลส่วนบุคคลที่ไม่จำเป็นในการแชร์ (PII scrubbing) และการเก็บรักษาหลักฐาน

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
คลาวด์ในการสนับสนุนการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์และอาชญากรรมทางไซเบอร์	• กำหนดมาตรฐานกลาง/ศัพท์กลาง/รูปแบบข้อมูลกลาง เพื่อให้หน่วยงานต่าง ๆ แลกเปลี่ยนข้อมูลได้ด้วยความรวดเร็วและลดความไม่สอดคล้อง เช่น ใช้ STIX/TAXII เป็น baseline สำหรับ CTI/IoC sharing และเชื่อมต่อเครื่องมือได้ • กำหนดหลักเกณฑ์ วิธีการ หรือแนวทางการจัดการเหตุภัยคุกคามทางไซเบอร์ระบบคลาวด์ พร้อมนิยามบทบาทหน้าที่ชัดเจน และการรายงานที่ทันเวลา • จัดทำบัญชีรายชื่อหน่วยงานที่เกี่ยวข้องในการป้องกันและรับมืออาชญากรรมทางไซเบอร์บนระบบคลาวด์ • จัดทำกรอบแนวทางการตอบสนองต่อเหตุการณ์อาชญากรรมทางไซเบอร์ที่เกี่ยวข้องกับระบบคลาวด์เพื่อใช้เป็นกรอบอ้างอิงสำหรับหน่วยงานที่เกี่ยวข้อง โดยระบุแนวทางการตอบสนองต่อเหตุการณ์ในแต่ละขั้นตอน ขั้นตอนการปฏิบัติ และแนวทางการกำหนดช่วงเวลาในการดำเนินการที่สอดคล้องกับกฎหมายที่เกี่ยวข้อง • กำหนดกลไกแลกเปลี่ยนข้อมูลให้สอดคล้องกับความรับผิดชอบร่วมระหว่าง Cloud Service Customer (CSC) และ Cloud Service Provider (CSP) โดยเฉพาะเรื่อง log/evidence, incident handling, และการติดตามสถานะเหตุการณ์ • พัฒนาแนวทางหรือข้อตกลงความร่วมมือในการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์โดยคำนึงถึงกรอบกฎหมายของประเทศ • ทำให้เกิดความชัดเจนในเรื่องการแบ่งชั้นความลับ/ความอ่อนไหวของข้อมูล กำหนดสิทธิ์เข้าถึงการประสาน การซ้อมแผนและการแจ้งเหตุข้ามหน่วยงาน รวมถึงกลไกยินยอม/อำนาจตามกฎหมายก่อนแลกเปลี่ยน โดยรองรับกรณีข้ามพรมแดน (เมื่อเกี่ยวกับผู้ให้บริการต่างประเทศ) • กำหนดแนวทางการจัดทำ baseline/โปรไฟล์ความเสี่ยงในระดับชาติ และระดับภาคส่วน 2. กิจกรรมส่งเสริมและพัฒนาศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้มีขีดความสามารถในการเฝ้าระวัง แจ้งเตือน และรับมือกับ	• สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • หน่วยงานควบคุมหรือกำกับดูแล **หน่วยงานปฏิบัติ** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • หน่วยงานควบคุมหรือกำกับดูแล • ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ • ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ • หน่วยงานของรัฐ • หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ • ผู้ให้บริการคลาวด์ • ภาคเอกชนหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	ภัยคุกคามทางไซเบอร์ที่มีต่อระบบคลาวด์ที่สำคัญ ได้แก่ การแลกเปลี่ยนข่าวกรองทางไซเบอร์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ในระดับภาคส่วน • รวบรวมข้อมูลเหตุการณ์/IoC/ช่องโหว่เฉพาะโดเมน และแลกเปลี่ยนข้อมูลตามแนวทางที่กำหนดไว้ในกลไกแลกเปลี่ยนข้อมูลในระดับชาติ และระดับภาคส่วน • ดำเนินการเชิงคุณภาพเพื่อกรองข้อมูลเหตุการณ์/IoC/ช่องโหว่เฉพาะโดเมน ให้มีคุณภาพก่อนนำเข้าสู่ระบบข่าวกรองทางไซเบอร์ โดยทำให้อยู่ในรูปแบบที่เป็นมาตรฐานด้วย 3. กิจกรรมส่งเสริมและพัฒนาความร่วมมือและการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานควบคุมหรือกำกับดูแล • ส่งเสริมการกำกับดูแลให้เกิดการจัดทำ baseline/โปรไฟล์ความเสี่ยงในระดับภาคส่วน • ส่งเสริมการกำกับดูแลให้เกิดการประสานงาน รวมถึงการซ้อมแผนและการแจ้งเหตุข้ามหน่วยงาน 4. กิจกรรมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ และอาชญากรรมทางไซเบอร์ที่เกี่ยวข้องกับระบบคลาวด์ • กำหนดประเด็นฝึก รวมถึงสถานการณ์และโจทย์ฝึกสำหรับการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Thailand's National Cyber Exercise) โดยให้ครอบคลุมในเรื่องภัยคุกคามทางไซเบอร์ และอาชญากรรมทางไซเบอร์ที่เกี่ยวข้องกับระบบคลาวด์ • กำหนดกรอบการฝึกเพื่อทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์และอาชญากรรมทางไซเบอร์ที่เกี่ยวข้องกับระบบคลาวด์ สำหรับการฝึกในระดับภาคส่วน และระดับหน่วยงาน • จัดทำหรือทบทวนเอกสารการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ (Table top exercise package) สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยให้ครอบคลุมในเรื่องภัยคุกคามทางไซเบอร์ และอาชญากรรมทางไซเบอร์ที่เกี่ยวข้องกับระบบคลาวด์	

กลยุทธ์ที่ 1.3

- จัดตั้งเครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย

เป้าหมายกลยุทธ์

- มีเครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ที่สามารถสนับสนุน บูรณาการ และแลกเปลี่ยนความรู้เพื่อยกระดับมาตรฐานความมั่นคงปลอดภัยด้านคลาวด์ของประเทศไทย (ยุทธศาสตร์ที่ 1 วัตถุประสงค์ที่ 3)

ตัวชี้วัดของกลยุทธ์/ค่าเป้าหมาย

ตัวชี้วัดที่ 1 มีผู้เชี่ยวชาญที่เข้าร่วมกิจกรรมกับเครือข่ายผู้เชี่ยวชาญฯ รวมจำนวนมากกว่า 100 คน ภายในระยะเวลา 5 ปี
ตัวชี้วัดที่ 2 มีกิจกรรมของเครือข่ายผู้เชี่ยวชาญฯ รวมจำนวนมากกว่า 50 กิจกรรม ภายในระยะเวลา 5 ปี

โครงการขับเคลื่อนกลยุทธ์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
1.3.1 โครงการจัดตั้งและพัฒนาเครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย	1. กิจกรรมสำรวจข้อมูลผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย • กำหนดหลักเกณฑ์และคุณสมบัติของผู้เชี่ยวชาญในสาขาที่เกี่ยวข้อง อาทิ ด้านสถาปัตยกรรมคลาวด์ (Cloud Architecture) ด้านวิศวกรรมความมั่นคงปลอดภัยคลาวด์ (Cloud Security Engineering) ด้านการบริหารความเสี่ยง (Risk Management) และด้านการปฏิบัติตามข้อกำหนด (Compliance) รวมถึงมีการกำหนดระดับของผู้เชี่ยวชาญตามการพิจารณาจากคุณสมบัติ เช่น ด้านความรู้ ความสามารถ หรือประสบการณ์ ตามที่ สกมช. กำหนด • สำรวจ รวบรวม และปรับปรุงฐานข้อมูลผู้เชี่ยวชาญอย่างต่อเนื่อง โดยแยกสาขาความเชี่ยวชาญให้ครอบคลุมอย่างน้อยด้านสถาปัตยกรรมคลาวด์ วิศวกรรมความมั่นคงปลอดภัยคลาวด์ การบริหารความเสี่ยง/การกำกับดูแล การปฏิบัติตามข้อกำหนด การตอบสนองเหตุ/นิติพิสูจน์ ความมั่นคงปลอดภัยข้อมูลและกุญแจเข้ารหัส ตลอดจนการตรวจประเมิน	**หน่วยงานกำกับดูแล** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) **หน่วยงานปฏิบัติ** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • หน่วยงานของรัฐ • หน่วยงานควบคุมหรือกำกับดูแล • หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ • ผู้ให้บริการคลาวด์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	• จัดทำรายงานผลสรุปการสำรวจข้อมูลผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย พร้อมเผยแพร่ให้หน่วยงานต่าง ๆ นำไปใช้เป็นข้อมูลสนับสนุนการดำเนินงาน 2. กิจกรรมจัดตั้งเครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย • กำหนดหลักเกณฑ์และบทบาทหน้าที่ของเครือข่ายผู้เชี่ยวชาญฯ เพื่อเป็นเวทีหลักในการหารือเกี่ยวกับมาตรฐาน แนวทางปฏิบัติ เทคนิคที่เกี่ยวข้อง ตลอดจนประเด็นปัญหาที่เกิดขึ้นจริง • ประชาสัมพันธ์แนวทางการเข้าร่วมเครือข่ายผู้เชี่ยวชาญฯ ไปยังหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ หน่วยงานตรวจรับรองคุณภาพ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง • เปิดรับสมัครและคัดเลือกผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์เข้าร่วมเครือข่ายผู้เชี่ยวชาญ โดยคัดเลือกตามเกณฑ์ความรู้ ความเชี่ยวชาญ และประสบการณ์ที่ สกมช. กำหนด • กำหนดระดับความเชี่ยวชาญและบทบาทการมีส่วนร่วมให้ชัดเจน เช่น ที่ปรึกษาเชิงปฏิบัติ ผู้พัฒนาแม่แบบกลาง ผู้ทวนสอบแนวทาง วิทยากร Train-the-Trainer ผู้เชี่ยวชาญเฉพาะกิจ เพื่อให้หน่วยงานสามารถเลือกใช้ได้ตรงตามความต้องการ 3. กิจกรรมพัฒนาแพลตฟอร์มกลางสำหรับเครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย โดยจัดทำระบบสมาชิก ระบบจัดเก็บเอกสาร และช่องทางสื่อสารออนไลน์ เพื่อใช้เป็นพื้นที่แลกเปลี่ยนข้อมูลและติดตามความก้าวหน้าการดำเนินงานของเครือข่าย • พัฒนาแพลตฟอร์มกลางที่รองรับฟังก์ชันที่หลากหลาย เช่น ระบบสมาชิกและการจัดการสิทธิ์ คลังความรู้/แม่แบบ/แนวปฏิบัติกลาง ระบบรับเรื่อง–จัดสรรผู้เชี่ยวชาญ–ติดตามผล พื้นที่ทำงานของคณะทำงาน/คอมมูนิตี้ พื้นที่แลกเปลี่ยนบทเรียนและคำเตือนเชิงปฏิบัติ	• หน่วยงานตรวจรับรองคุณภาพ • ภาคเอกชนหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	• วางแนวทางการเชื่อมโยงแพลตฟอร์มกับกลไกความร่วมมือด้านข้อมูลภัยคุกคาม/เหตุการณ์ในระดับประเทศ เช่น playbook มาตรฐานกลาง แนวทางประสานงาน เพื่อทำให้เครือข่ายฯ ช่วยลดเวลาในการตอบสนองและเพิ่มความพร้อมร่วมกันได้จริง สอดคล้องกับโมเดลความร่วมมือรัฐ–เอกชนที่เน้นการทำงานร่วมเชิงปฏิบัติและการแบ่งปันข้อมูลอย่างรวดเร็ว • จัดทำแคตตาล็อกบริการ (Service Catalogue) ของเครือข่ายฯ และช่องทางรับเรื่อง/คัดกรอง/จัดลำดับความเร่งด่วน เพื่อให้หน่วยงานเข้าถึงความช่วยเหลือได้จริง เช่น การให้คำปรึกษา/ทบทวนเชิงปฏิบัติด้านการตีความมาตรฐานและการจัดทำหลักฐาน (Evidence) การทบทวนสถาปัตยกรรมและแนวทางตั้งค่าปลอดภัย (Secure-by-Default) สำหรับงานสำคัญ การช่วยออกแบบ Shared Responsibility ตาม Service Model + RACI สำหรับกรณีที่หน่วยงานมีข้อจำกัดบุคลากร การสนับสนุนการจัดทำ playbook ขั้นต่ำสำหรับหน่วยงานขนาดเล็ก/ระดับพื้นที่ (โยง Starter Kit) • จัดให้มีคลินิก/ศูนย์ช่วยนำไปใช้ในรูปแบบที่ยืดหยุ่น เช่น virtual clinic, office hour, on-call advisory พร้อมระบบติดตามผลการให้คำปรึกษา (Case tracking) เพื่อให้เกิดการปิดงานและส่งมอบแนวปฏิบัติที่ใช้ได้จริง 4. กิจกรรมจัดทำธรรมนูญเครือข่ายและโครงสร้างธรรมาภิบาลด้านความเป็นกลาง (Charter and Impartiality Governance) • จัดทำธรรมนูญเครือข่ายผู้เชี่ยวชาญฯ ที่กำหนดบทบาท เป้าหมาย ขอบเขตงาน รูปแบบการให้ความช่วยเหลือ และกลไกตัดสินใจของเครือข่ายฯ ให้ชัดเจน โดยยืนยันว่าเครือข่ายฯ ทำหน้าที่สนับสนุนการนำไปใช้ และให้คำปรึกษาเชิงเทคนิค/เชิงกระบวนการ มิใช่หน่วยตัดสินผลการรับรองหรือทดแทนบทบาทของหน่วยงานตรวจรับรอง • จัดตั้งกลไกธรรมาภิบาลเพื่อความเป็นกลาง เช่น คณะกรรมการความเป็นกลางและจริยธรรม (Impartiality and Ethics Panel) และกำหนดมาตรการบริหารความขัดกันแห่งผลประโยชน์อย่างเป็นระบบ ได้แก่ การเปิดเผยผลประโยชน์ (Disclosure) การเว้นวรรค/ถอนตัวจากการพิจารณา	

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	(Recusal) การจัดการสิทธิ์การเข้าถึงข้อมูลตามบทบาท และแนวทางกำกับไม่ให้เกิดการชี้นำ/โฆษณาเชิงพาณิชย์ในนามเครือข่ายฯ • กำหนดกระบวนการบริหารความเสี่ยงด้านผลประโยชน์ทับซ้อนแบบต่อเนื่อง เพื่อรักษาความน่าเชื่อถือของการให้ความเห็นและข้อเสนอแนะทางเทคนิคของเครือข่ายฯ (แนวคิดสอดคล้องกับหลักการความเป็นกลางและการจัดการความขัดกันแห่งผลประโยชน์ในงานตรวจรับรอง/การประเมินความสอดคล้อง)	

ยุทธศาสตร์ที่ 2 สร้างสภาพแวดล้อมที่เอื้อต่อการดำเนินการตามมาตรฐาน

ยุทธศาสตร์ที่ 2 มีบทบาทในการสร้างระบบนิเวศและเครื่องมือสนับสนุนให้การปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์เกิดผลในทางปฏิบัติอย่างทั่วถึง โดยมุ่งพัฒนากลไกการตรวจรับรองที่โปร่งใส ตรวจสอบได้ และจัดระดับการรับรองตามความเสี่ยง พร้อมกำหนดแนวทางการยอมรับผลเทียบเคียง (Mutual Recognition) และกระบวนการ Fast-track เพื่อลดคอขวดและการตรวจซ้ำซ้อน ควบคู่กับการบูรณาการบทบาทของหน่วยงานกำหนดนโยบายและหน่วยงานควบคุมหรือกำกับดูแลให้เป็นเอกภาพ ลดภาระระเบียบและงานเอกสารด้วยขั้นตอนปฏิบัติมาตรฐาน/เอกสารต้นแบบ (SOP/Template) เครื่องมือประเมินตนเอง และการติดตามแบบต่อเนื่อง (Continuous Monitoring) ตลอดจนจัดทำและเผยแพร่รายชื่อผู้ให้บริการที่ผ่านมาตรฐาน (Whitelist) และพัฒนาแพลตฟอร์มกลางเพื่อขึ้นทะเบียน ติดตามสถานะ และเปิดช่องทางร้องเรียน (Whistleblowing) ผู้ให้บริการคลาวด์ที่ได้มาตรฐานเพื่อเสริมความเชื่อมั่นและความโปร่งใสในกระบวนการกำกับดูแล

วัตถุประสงค์

1. เพื่อสร้างกลไกการประเมินความสอดคล้องและตรวจรับรองมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์แบบครบวงจร โปร่งใส ตรวจสอบได้ และสอดคล้องกับมาตรฐานสากล

2. เพื่อสร้างกลไกการกำกับดูแลโดยหน่วยงานที่เกี่ยวข้องกับการกำหนดนโยบาย (Policy Agencies) และหน่วยงานควบคุมหรือกำกับดูแล (Regulator) ที่เป็นเอกภาพ โดยให้มีมาตรการ ข้อกำหนดหรือแนวปฏิบัติที่สอดคล้องกัน ลดความคลาดเคลื่อนในการตีความ ยกระดับการกำกับดูแลสู่รูปแบบอัตโนมัติเป็นหลัก (Automation-first) รวมถึงการจัดให้มีช่องทางร้องเรียนเพื่อเพิ่มความโปร่งใสและประสิทธิภาพการบังคับใช้

3. เพื่อลดอุปสรรคและความซ้ำซ้อนในการปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ทั้งในด้านกฎระเบียบ กระบวนการ และเงื่อนไขต่าง ๆ ที่อาจเป็นภาระเกินความจำเป็นต่อผู้ใช้บริการคลาวด์ (หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ) และผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

4. เพื่อส่งเสริมการวิจัยและนวัตกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ที่จะช่วยสนับสนุนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 โดยการพัฒนากลไกทดลองหรือพื้นที่ทดสอบเชิงนวัตกรรม (Sandbox) สำหรับเทคโนโลยีอุบัติใหม่ รวมถึงการนำผลลัพธ์ไปต่อยอดปรับปรุงมาตรฐาน กรอบกำกับดูแล และเครื่องมือสนับสนุนเพื่อให้การดำเนินการตามมาตรฐานมีประสิทธิภาพมากยิ่งขึ้นและทันต่อบริบทภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว

กลยุทธ์การดำเนินงาน

กลยุทธ์ที่ 2.1

- พัฒนากลไกการตรวจรับรองมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

เป้าหมายกลยุทธ์

- ประเทศไทยมีกลไกการตรวจรับรองมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ที่เป็นระบบ โปร่งใส ตรวจสอบได้ และใช้งานได้จริงทันต่อช่วงเริ่มบังคับใช้มาตรฐาน ครอบคลุมทั้งผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ตามระดับผลกระทบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Categorization) /ระดับชั้นข้อมูล (Data Classification) โดยกำหนดหลักเกณฑ์ กระบวนการ และคุณสมบัติของผู้ตรวจสอบ (Auditor) และหน่วยงานให้บริการตรวจรับรอง (Certify Body) ที่เทียบเคียงมาตรฐานสากล พร้อมแนวทางยอมรับผลการตรวจรับรองแบบเทียบเคียง (Mutual Recognition) และแนวทาง Fast-track เพื่อลดการตรวจซ้ำซ้อนและลดคอขวด รวมถึงมีระบบทะเบียนออนไลน์หรือแพลตฟอร์มกลางสำหรับการยื่นคำขอ ติดตามสถานะ ต่ออายุ และเผยแพร่สถานการณ์รับรอง/ขอบข่ายการรับรอง เพื่อสร้างความเชื่อมั่นและสนับสนุนการกำกับดูแลและการจัดซื้อจัดจ้างอย่างมีประสิทธิภาพ (ยุทธศาสตร์ที่ 2 วัตถุประสงค์ที่ 1)

ตัวชี้วัดของกลยุทธ์/ค่าเป้าหมาย

ตัวชี้วัดที่ 1 มีหลักเกณฑ์ กระบวนการ และคุณสมบัติสำหรับการตรวจรับรองมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ที่ครอบคลุมวงรอบการตรวจรับรอง การตรวจสำรวจ และการต่ออายุ หลักความเป็นอิสระ ความเที่ยงธรรม และการจัดการความขัดแย้งทางผลประโยชน์ กลไกอุทธรณ์ ร้องเรียน และการทบทวนคุณภาพผลการตรวจ รวมถึงหลักเกณฑ์การยอมรับผลการตรวจรับรองแบบเทียบเคียง (Mutual Recognition) และแนวทาง Fast-track ภายในปี พ.ศ. 2569

ตัวชี้วัดที่ 2 มีหน่วยงานให้บริการตรวจรับรอง (Certify Body) ได้รับการขึ้นทะเบียนหรืออยู่ระหว่างการขึ้นทะเบียนตามเกณฑ์ที่กำหนด ไม่น้อยกว่า 3 หน่วยงาน ภายในปี พ.ศ. 2569 และเพิ่มเป็นไม่น้อยกว่า 5 หน่วยงาน ภายในปี พ.ศ. 2571 พร้อมมีประกาศหรือบัญชีรายชื่อหน่วยงานตรวจรับรองตามมาตรฐานสากลที่ยอมรับหรือเทียบเคียงเพื่อรองรับช่วงเริ่มต้นและลดคอขวด ภายในปี พ.ศ. 2569

ตัวชี้วัดที่ 3 มีการให้บริการตรวจรับรองมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ สำหรับผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ รวมถึงกระบวนการ Fast-track หรือเทียบเคียง ภายในปี พ.ศ. 2570

ตัวชี้วัดที่ 4 มีระบบทะเบียนออนไลน์หรือแพลตฟอร์มกลางเพื่อการตรวจรับรองมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ สำหรับผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ ที่ครอบคลุมระบบทะเบียน ยื่นคำขอ ติดตามสถานะแบบขั้นต่ำ (MVP) และการเผยแพร่รายชื่อ Certify Body/Auditor ภายในปี พ.ศ. 2569 และมีแพลตฟอร์มกลางแบบครบวงจรสำหรับผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ ที่ครอบคลุม Dashboard สถานการณ์การรับรอง ขอบข่ายการรับรอง ระบบค้นหา ระบบแจ้งเตือนวันหมดอายุ และ API เชื่อมระบบภาครัฐที่เกี่ยวข้อง ภายในปี พ.ศ. 2571

โครงการขับเคลื่อนกลยุทธ์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
2.1.1 โครงการพัฒนากลไกการตรวจรับรองและการเทียบเคียงผลการตรวจรับรอง (Certification Scheme and Mutual Recognition)	1. กิจกรรมพัฒนากลไกการตรวจรับรองและการเทียบเคียงผลการตรวจรับรอง • จัดทำหลักเกณฑ์ กระบวนการ และคุณสมบัติของผู้ตรวจสอบ (Auditor) และหน่วยงานให้บริการตรวจรับรอง (Certify Body) เช่น หลักเกณฑ์เกี่ยวกับหน่วยงานให้บริการตรวจรับรองที่ได้มาตรฐานสำหรับผู้ให้บริการคลาวด์ ตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 หลักเกณฑ์และกระบวนการเทียบผลการตรวจรับรองมาตรฐานกรณีผู้ให้บริการคลาวด์หรือผู้ใช้บริการคลาวด์มีการตรวจรับรองมาตรฐานจากหน่วยงานให้บริการตรวจรับรองสากล การกำหนดบัญชีรายการมาตรฐานการรับรองสากลที่สามารถเทียบเคียงได้และหลักฐานขั้นต่ำที่ต้องใช้ รวมถึงกลไกอุทธรณ์ ร้องเรียน และแนวทางทบทวนคุณภาพผลการตรวจรับรอง (Quality Review) เป็นต้น • ศึกษาและวิเคราะห์มาตรฐานระดับชาติ และมาตรฐานสากล สำหรับการตรวจรับรองมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ จัดทำการวิเคราะห์ช่องว่าง (Gap Analysis) ระหว่างมาตรฐานระดับชาติและมาตรฐานสากล เพื่อระบุประเด็นที่ยังไม่สอดคล้องข้อจำกัด และแนวทางในการปรับปรุงได้อย่างเหมาะสม • พัฒนาและจัดทำเอกสารหลักเกณฑ์ กระบวนการ และคุณสมบัติของผู้ตรวจสอบและหน่วยงานให้บริการตรวจรับรองคุณภาพ ให้มีความชัดเจน • จัดทำแนวทางและวิธีการในการตรวจประเมินและการให้การรับรอง • เปิดรับฟังความคิดเห็นสาธารณะ (Public Hearing) จากผู้มีส่วนได้ส่วนเสียและหน่วยงานที่เกี่ยวข้อง • ประกาศใช้และเผยแพร่ รวมถึงประชาสัมพันธ์ 2. กิจกรรมจัดการอบรมสำหรับหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567	**หน่วยงานกำกับดูแล** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ **หน่วยงานปฏิบัติ** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สถาบันประเมินและรับรองเทคโนโลยีดิจิทัล (ปรด.) • สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม (สมอ.) • ภาคเอกชนหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	• ดำเนินการพัฒนาหลักสูตรฝึกอบรมด้านเกณฑ์มาตรฐานคลาวด์และขั้นตอนการตรวจสอบ ให้แก่หน่วยงานที่มีความสนใจจะขึ้นทะเบียนเป็นหน่วยงานตรวจรับรอง (CB) เพื่อส่งเสริมความเข้าใจในกรอบนโยบาย คอนฟิกความมั่นคงปลอดภัย และสัญญาระดับสิทธิการตรวจสอบ เพื่อช่วยเร่งรัดกระบวนการยกระดับขีดความสามารถของหน่วยงานตรวจในประเทศให้สามารถผ่านเกณฑ์และขึ้นทะเบียนได้ทันตามเป้าหมาย • จัดอบรมหลักสูตรเฉพาะด้านเกณฑ์เทคนิคและกฎหมายเฉพาะของไทย (เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567) ให้แก่หน่วยตรวจรับรองมาตรฐานสากลในประเทศ (เช่น ผู้ตรวจ ISO 27001 หรือ CSA STAR) เพื่อขยายขอบข่ายการยอมรับผลประเมินร่วม และเพิ่มความคล่องตัวในกระบวนการรับรองมาตรฐานระยะเริ่มต้น • จัดตั้งกลไกบริการที่ปรึกษาและให้ความช่วยเหลือ และการสัมมนาเชิงปฏิบัติการร่วมกับเครือข่ายผู้เชี่ยวชาญฯ เพื่อให้คำปรึกษาเชิงปฏิบัติแก่หน่วยงานที่มีฐานความพร้อมด้านการตรวจประเมินระบบสารสนเทศอยู่เดิม (เช่น CB ที่มีระบบบริหารงานคุณภาพ ISO/IEC 17021) ให้มีความเชี่ยวชาญในเชิงการตรวจประเมินตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ได้อย่างรวดเร็ว • กำหนดหลักเกณฑ์ที่โปร่งใสในการประเมิน และสอบทานสมรรถนะและความเชี่ยวชาญ (Competency/Qualification) ของผู้ตรวจประเมิน (Auditor) ในสังกัดของหน่วยงานให้บริการตรวจรับรอง (Certify Body) ที่ผ่านการอบรม ตลอดจนกำหนดเกณฑ์มาตรฐานด้านความเป็นกลางและการจัดการผลประโยชน์ทับซ้อน (Impartiality/Conflict of Interest) และจริยธรรมในการตรวจประเมิน เพื่อสร้างหลักประกันความน่าเชื่อถือและความสอดคล้องของผลการตรวจประเมินและใบรับรองในระดับประเทศ	

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
2.1.2 โครงการพัฒนาแพลตฟอร์มกลางเพื่อการตรวจรับรองมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Cloud Certification Platform and Registry)	1. กิจกรรมพัฒนาแพลตฟอร์มกลางหรือระบบทะเบียนออนไลน์สำหรับผู้ตรวจสอบ (Auditor Registry) และหน่วยงานให้บริการตรวจรับรอง (Certify Body) • พัฒนาระบบทะเบียนผู้ตรวจสอบ (Auditor Registry) ทะเบียนหน่วยงานให้บริการตรวจรับรอง (Certify Body) ระบบยื่นคำขอ ระบบติดตามสถานะการตรวจ และระบบบริหารวงรอบการตรวจสำรวจ/ต่ออายุ • เชื่อมโยงข้อมูลผลการอบรมของหน่วยงานต่าง ๆ เช่น สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ • เชื่อมโยงข้อมูลผู้ตรวจสอบ (Auditor) และหน่วยงานให้บริการตรวจรับรอง (Certify Body) ที่ผ่านการอบรมแล้วเข้ากับระบบกลาง แสดงความสามารถ/ระดับ (Competency Level) ของ Auditor สถานะและขอบข่ายการตรวจรับรองของหน่วยงานตรวจรับรองที่สามารถปฏิบัติงานได้ • จัดทำระบบค้นหา (Search Directory) สำหรับหน่วยงานของรัฐและเอกชน • จัดทำระบบแจ้งเตือนวันหมดอายุการรับรอง/อบรม (Re-certification) • พัฒนา API สำหรับการเชื่อมต่อกับระบบอื่นของภาครัฐ 2. กิจกรรมพัฒนาแพลตฟอร์มกลางหรือระบบทะเบียนออนไลน์สำหรับใช้ติดตามสถานการณ์ตรวจประเมินผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ • ระบบลงทะเบียนสำหรับผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ และยื่นขอการตรวจรับรอง • ระบบติดตามสถานการณ์ตรวจประเมิน • Dashboard เพื่อแสดงสถานะการรับรอง ให้สามารถเข้าถึงได้ง่าย ชัดเจน และเปิดเผยต่อสาธารณะ • เผยแพร่รายชื่อผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ที่ผ่านการรับรอง เพื่อสร้างความเชื่อมั่นบนแพลตฟอร์มกลาง	**หน่วยงานกำกับดูแล** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) • หน่วยงานควบคุมหรือกำกับดูแล **หน่วยงานปฏิบัติ** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) • สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) • ผู้ใช้บริการคลาวด์ • ผู้ให้บริการคลาวด์ • หน่วยงานตรวจรับรองคุณภาพ • ภาคเอกชนหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
2.1.3 โครงการยกระดับและขยายขีดความสามารถหน่วยงานให้บริการตรวจรับรอง และผู้ตรวจสอบ (Certify Body and Auditor Capacity Expansion)	1. กิจกรรมจัดการอบรมสำหรับหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 • พัฒนาหลักสูตรเฉพาะด้านสำหรับหน่วยงานให้บริการตรวจรับรอง (Certify Body) อาทิ เกณฑ์การประเมินคุณภาพ ข้อกำหนดด้านการบริหารงานคุณภาพ ตลอดจนหลักการด้านความเป็นอิสระความเที่ยงธรรมของกระบวนการตรวจประเมิน และแนวทางการตรวจรับรองคุณภาพตามมาตรฐานของประเทศไทย • พัฒนาเอกสารคู่มือและแนวทางปฏิบัติสำหรับหน่วยงานให้บริการตรวจรับรองคุณภาพ เช่น แนวทางการบริหารจัดการกระบวนการตรวจรับรอง การจัดทำรายงานผลการตรวจประเมิน และการจัดเก็บหลักฐานและข้อมูลที่เกี่ยวข้องอย่างเป็นระบบ • จัดอบรมแนวทางปฏิบัติสำหรับหน่วยงานให้บริการตรวจรับรอง (Certify Body) เพื่อเสริมสร้างความรู้ ความเข้าใจ และทักษะที่จำเป็นในการดำเนินการตรวจรับรองให้เป็นไปตามหลักเกณฑ์และมาตรฐานที่กำหนด • จัดทำมาตรการเพิ่มจำนวนและกระจายกำลังตรวจ เช่น โครงการพี่เลี้ยง (Mentoring), การทดสอบภาคปฏิบัติ, การประเมินซ้ำ/สุ่มตรวจคุณภาพ • จัดทำมาตรการบริหารคิวการตรวจรับรองและการติดตาม SLA เพื่อลดคอขวด และยกระดับคุณภาพ/ความน่าเชื่อถือของระบบตรวจรับรอง	**หน่วยงานกำกับดูแล** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) • หน่วยงานควบคุมหรือกำกับดูแล **หน่วยงานปฏิบัติ** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) • ผู้ใช้บริการคลาวด์ • ผู้ให้บริการคลาวด์ • หน่วยงานตรวจรับรองคุณภาพ • ภาคเอกชนหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

กลยุทธ์ที่ 2.2

- ส่งเสริมให้มีกลไกการกำกับดูแลโดยหน่วยงานที่เกี่ยวข้องกับการกำหนดนโยบาย (Policy Agencies) และหน่วยงานควบคุมหรือกำกับดูแล (Regulator) ที่เป็นเอกภาพ

เป้าหมายกลยุทธ์

- มีการส่งเสริมกลไกการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ร่วมกับหน่วยงานที่เกี่ยวข้องกับการกำหนดนโยบาย (Policy Agencies) และหน่วยงานควบคุมหรือกำกับดูแล (Regulator) เพื่อให้เกิดความเป็นเอกภาพกับการดำเนินการตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) (ยุทธศาสตร์ที่ 2 วัตถุประสงค์ที่ 2)

ตัวชี้วัดของกลยุทธ์/ค่าเป้าหมาย

ตัวชี้วัดที่ 1 มีกิจกรรมส่งเสริมกลไกการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ร่วมกับหน่วยงานที่เกี่ยวข้องกับการกำหนดนโยบาย (Policy Agencies) และหน่วยงานควบคุมหรือกำกับดูแล (Regulator) จำนวนไม่น้อยกว่า 2 ครั้งต่อปี

ตัวชี้วัดที่ 2 มีการทบทวนแผนบูรณาการเพื่อขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ โดยนำความคิดเห็นจากผู้มีส่วนได้ส่วนเสียและผู้ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์มาใช้ในการพิจารณา จำนวนไม่น้อยกว่า 1 ครั้งต่อปี

โครงการขับเคลื่อนกลยุทธ์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
2.2.1 โครงการส่งเสริมกลไกการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Cloud Security Governance) ร่วมกับหน่วยงานที่เกี่ยวข้องกับการกำหนดนโยบาย (Policy Agencies) และ	1. กิจกรรมส่งเสริมกลไกการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Cloud Security Governance) • จัดตั้งคณะกรรมการหรือคณะทำงานร่วมเพื่อบูรณาการกำกับดูแลความมั่นคงปลอดภัยระบบคลาวด์ (Joint Cloud Security Governance Committee/Working Group) ระหว่างหน่วยงานนโยบาย (Policy Agencies) และหน่วยงานควบคุมหรือกำกับดูแล (Regulator) • กำหนดกรอบบทบาทหน้าที่ของคณะกรรมการหรือคณะทำงานฯ ให้ชัดเจน เช่น การทบทวนความสอดคล้องระหว่างมาตรฐานของ สกมช. กับมาตรฐานรัฐบาลดิจิทัลหรือแนวทางที่เกี่ยวข้องของ สพร. • กำหนดหลักเกณฑ์ พิจารณาคัดเลือก และเชิญหน่วยงานของรัฐ หน่วยงานกำหนดนโยบาย หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานที่เกี่ยวข้อง เข้าร่วม	**หน่วยงานกำกับดูแล** • กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.) • สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) **หน่วยงานปฏิบัติ**

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
หน่วยงานควบคุมหรือกำกับดูแล (Regulator)	• จัดกิจกรรมส่งเสริมกลไกการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ เช่น เวทีเสวนาวิชาการ กิจกรรมฝึกอบรม หรือการประชุมเชิงปฏิบัติการ เพื่อพัฒนามาตรฐานหรือแนวทางร่วมในการกำกับดูแลระบบคลาวด์ • จัดทำแนวปฏิบัติหรือแนวทางการกำกับดูแลสำหรับหน่วยงานที่ทำหน้าที่กำกับดูแลตามแผนบูรณาการฯ ฉบับนี้ ตลอดจนแนวปฏิบัติหรือแนวทางการกำหนดมาตรฐานที่เหมาะสมและการตรวจสอบตามมาตรฐานขั้นต่ำสำหรับหน่วยงานควบคุมหรือกำกับดูแล (Regulator) ตามมาตรา 53 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่สอดคล้องกับแผนบูรณาการฯ ฉบับนี้ด้วย	• สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) • หน่วยงานควบคุมหรือกำกับดูแล
2.2.2 โครงการทบทวนแผนบูรณาการเพื่อขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์	1. กิจกรรมทบทวนแผนบูรณาการฯ เพื่อขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ • รวบรวมข้อมูลและความคิดเห็นจากผู้มีส่วนได้ส่วนเสียผ่านช่องทางต่าง ๆ เช่น แบบสำรวจความคิดเห็นผู้มีส่วนได้ส่วนเสีย หรือเวทีระดมความคิดเห็น (Focus Group) • วิเคราะห์ข้อมูลที่รวบรวมได้ร่วมกับแผนบูรณาการฯ ระบุส่วนที่ต้องปรับปรุง และจัดลำดับความสำคัญ • จัดประชุมเชิงปฏิบัติการเพื่อปรับปรุงแผนบูรณาการฯ พิจารณาข้อเสนอจากผู้มีส่วนได้ส่วนเสีย และพัฒนาแผนบูรณาการฯ ฉบับปรับปรุง	**หน่วยงานกำกับดูแล** • กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.) • สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) **หน่วยงานปฏิบัติ** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) • หน่วยงานของรัฐ • หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
		• หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ • ผู้ให้บริการคลาวด์ • หน่วยงานตรวจรับรองคุณภาพ • ภาคเอกชนหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

กลยุทธ์ที่ 2.3

- จัดทำแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง เพื่อส่งเสริมการปฏิบัติตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

เป้าหมายกลยุทธ์

- มีการจัดทำแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ในการปฏิบัติตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 (ยุทธศาสตร์ที่ 2 วัตถุประสงค์ที่ 3)
- มีกิจกรรมรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียและผู้ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์มาใช้ในการพิจารณาจัดทำแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ (ยุทธศาสตร์ที่ 2 วัตถุประสงค์ที่ 3)

ตัวชี้วัดของกลยุทธ์/ค่าเป้าหมาย

ตัวชี้วัดที่ 1 มีแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ตามลำดับความเร่งด่วน จำนวนไม่น้อยกว่า 3 รายการต่อปี ตั้งแต่ปี พ.ศ. 2569 เป็นต้นไป

ตัวชี้วัดที่ 2 มีกิจกรรมรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียและผู้ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์มาใช้ในการพิจารณาจัดทำแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ จำนวนไม่น้อยกว่า 2 กิจกรรมต่อปี

ตัวชี้วัดที่ 3 มีแบบประเมินเพื่อให้ความคิดเห็นในการปรับปรุงคุณภาพในแต่ละแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ

ตัวชี้วัดที่ 4 มีเครื่องมือในการประเมินตนเอง (Self-Assessment) เริ่มต้นใช้งานในปีพ.ศ. 2570

โครงการขับเคลื่อนกลยุทธ์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
2.3.1 โครงการจัดทำแนวทาง คำแนะนำ และเอกสารต้นแบบเพื่อขับเคลื่อนการปฏิบัติตาม	1. กิจกรรมจัดทำแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบเพื่อขับเคลื่อนการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ • จัดตั้งคณะทำงานจัดทำแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ โดยมีผู้แทนจากผู้มีส่วนได้ส่วนเสีย หรือผู้ที่เกี่ยวข้อง อาทิ หน่วยงานของรัฐ หน่วยงานควบคุมหรือ	**หน่วยงานกำกับดูแล** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์	กำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง • กำหนดหัวข้อแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบที่จะดำเนินการจัดทำ โดยพิจารณาความต้องการร่วมกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง เช่น ความสอดคล้องระหว่างมาตรฐาน สกมช. กับมาตรฐานอื่น ๆ ที่ดำเนินการอยู่แล้ว ความเชื่อมโยงระหว่างแผนบูรณาการฯ กับนโยบายและแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570) แนวทางการนำแผนบูรณาการฯ ไปใช้ประกอบการดำเนินการ เครื่องมือในการประเมินตนเอง (Self-Assessment) เครื่องมือในการประเมินระดับวุฒิภาวะ (Maturity assessment) คำแนะนำสำหรับผู้ให้บริการคลาวด์กรณีเกิดเหตุภัยคุกคามทางไซเบอร์ต่อผู้ใช้บริการคลาวด์ตามมาตรฐานฯ เป็นต้น • จัดลำดับความสำคัญรายการของแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ ตามความเร่งด่วน ความเชี่ยวชาญ และทรัพยากรที่มีอยู่ • ออกแบบและพัฒนาร่างแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ • จัดประชุมเชิงปฏิบัติการ (Workshop) และเวทีแลกเปลี่ยนความรู้ เพื่อหารือแนวทางการพัฒนามาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ และสนับสนุนการแบ่งปันประสบการณ์ รวมถึงแนวปฏิบัติที่ดี (Best practices) ระหว่างหน่วยงาน 2. กิจกรรมรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียและผู้ที่เกี่ยวข้อง • จัดกิจกรรมรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียและผู้ที่เกี่ยวข้อง เพื่อรวบรวมข้อคิดเห็น ประเด็นปัญหา ข้อเสนอแนะ และความต้องการ • ปรับปรุงแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ • เผยแพร่แนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบฉบับสมบูรณ์ • จัดทำคู่มือประกอบ เผยแพร่ผ่านเว็บไซต์หรือแพลตฟอร์มกลาง	**หน่วยงานปฏิบัติ** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานพัฒนารัฐบาลดิจิทัล (สพร.) • สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) • หน่วยงานของรัฐ • หน่วยงานควบคุมหรือกำกับดูแล • หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ • ผู้ให้บริการคลาวด์ • หน่วยงานตรวจรับรองคุณภาพ • ภาคเอกชนหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	• ส่งเสริมให้หน่วยงานผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์นำไปประยุกต์ใช้	
2.3.2 โครงการพัฒนาเครื่องมือในการประเมินตนเองตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	1. กิจกรรมแบบประเมินตนเอง (Self-Assessment) ตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 • ศึกษาและพัฒนาแบบประเมินตนเอง (Self-Assessment) • ทดสอบ ประเมินผล และปรับปรุงแบบประเมินตนเอง (Self-Assessment) • เผยแพร่เพื่อการใช้งาน 2. พัฒนาแพลตฟอร์มสำหรับประเมินตนเอง (Self-Assessment Platform) และพัฒนาเอกสารต้นแบบ (Template) สำหรับหน่วยงานเลือกใช้งาน 3. พัฒนาหลักสูตร E-learning สำหรับการประเมินตนเอง (Self-Assessment)	**หน่วยงานกำกับดูแล** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) **หน่วยงานปฏิบัติ** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) • สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) • หน่วยงานของรัฐ • หน่วยงานควบคุมหรือกำกับดูแล • หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ • ผู้ให้บริการคลาวด์ • หน่วยงานตรวจรับรองคุณภาพ • ภาคเอกชนหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง
2.3.3 โครงการทบทวนคุณภาพของแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบตาม	1. กิจกรรมทบทวนคุณภาพของแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ ตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ • วางแผนเตรียมการ กำหนดกรอบเนื้อหา แนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารที่ต้องการการทบทวนความคิดเห็น และจัดลำดับความสำคัญ	**หน่วยงานกำกับดูแล** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์	• รวบรวมความคิดเห็นและข้อเสนอแนะในการปรับปรุงคุณภาพของแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ โดยอาจรวบรวมจากผู้ใช้งานโดยตรงแบบสอบถาม หรือจากการจัดกิจกรรมรับฟังความคิดเห็น • จัดกิจกรรมรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียและผู้ที่เกี่ยวข้อง เพื่อรวบรวมข้อคิดเห็น ประเด็นปัญหา ข้อเสนอแนะ และความต้องการ • ดำเนินการวิเคราะห์ข้อมูลที่รวบรวมได้ และปรับปรุงร่างแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารที่ได้รับความคิดเห็น • เผยแพร่แนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารที่ได้รับการแก้ไขแล้ว	**หน่วยงานปฏิบัติ** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) • หน่วยงานของรัฐ • หน่วยงานควบคุมหรือกำกับดูแล • หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ • ผู้ให้บริการคลาวด์ • หน่วยงานตรวจรับรองคุณภาพ • ภาคเอกชนหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

กลยุทธ์ที่ 2.4

- ส่งเสริมการวิจัยและนวัตกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

เป้าหมายกลยุทธ์

- มีการวิจัยและนวัตกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ที่จะช่วยให้การดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 มีประสิทธิภาพมากยิ่งขึ้น (ยุทธศาสตร์ที่ 2 วัตถุประสงค์ที่ 4)

ตัวชี้วัดของกลยุทธ์/ค่าเป้าหมาย

ตัวชี้วัดที่ 1 มีกิจกรรมส่งเสริมการวิจัยและนวัตกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ จำนวนไม่น้อยกว่า 2 กิจกรรมต่อปี

โครงการขับเคลื่อนกลยุทธ์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
2.4.1 โครงการส่งเสริมการวิจัยและนวัตกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์	1. กิจกรรมส่งเสริมการวิจัยและนวัตกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ • กำหนดแนวทางระดับชาติด้านการส่งเสริมการวิจัยและนวัตกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ • กำหนดหัวข้อโครงการวิจัยนำร่อง เช่น Cross-Border Cloud Assurance, Data Residency, Sovereign Cloud, การจัดทำการเชื่อมโยงและเทียบเคียงข้อกำหนด (Mapping) ระหว่างกฎหมายที่เกี่ยวข้อง มาตรฐานระดับชาติ และมาตรฐานสากล เป็นต้น • นำผลลัพธ์และกรณีศึกษาจากโครงการนำร่องมาใช้เป็นฐาน เพื่อปรับปรุงมาตรฐาน กรอบกำกับดูแล และกฎระเบียบในประเทศ • นำผลลัพธ์จากการวิจัยและกรณีศึกษาจากโครงการมาจัดทำงานวิจัยเพื่อเผยแพร่ในที่ประชุมวิชาการระดับนานาชาติ • การเผยแพร่ประชาสัมพันธ์เพื่อสร้างการตระหนักรับรู้ และการนำการวิจัยและนวัตกรรมฯ ไปใช้ประโยชน์	**หน่วยงานกำกับดูแล** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (อว.) **หน่วยงานปฏิบัติ** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานสภานโยบายการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรมแห่งชาติ (สอวช.) • สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว.)

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
		• สำนักงานการวิจัยแห่งชาติ (วช.) • สำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) (สนช.) • สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) • สถาบันวิจัยวิทยาศาสตร์และเทคโนโลยีแห่งประเทศไทย (วว.) • หน่วยงานของรัฐ • หน่วยงานควบคุมหรือกำกับดูแล • หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ • ผู้ให้บริการคลาวด์ • หน่วยงานตรวจรับรองคุณภาพ • ภาคเอกชนหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

ยุทธศาสตร์ที่ 3 พัฒนาขีดความสามารถของหน่วยงานและบุคลากร

วัตถุประสงค์

1. เพื่อยกระดับขีดความสามารถของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้สามารถปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ได้อย่างมีประสิทธิภาพ

2. เพื่อเสริมสร้างทักษะด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ให้บุคลากรที่เกี่ยวข้อง

3. เพื่อพัฒนากลไกสนับสนุนด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ให้กับหน่วยงานและบุคลากรที่เกี่ยวข้อง

กลยุทธ์การดำเนินงาน

กลยุทธ์ที่ 3.1

- ยกระดับขีดความสามารถของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้สามารถปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ได้อย่างมีประสิทธิภาพ

เป้าหมายของกลยุทธ์

- หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้รับการยกระดับขีดความสามารถในการปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 (ยุทธศาสตร์ที่ 3 วัตถุประสงค์ที่ 1)

ตัวชี้วัดของกลยุทธ์/ค่าเป้าหมาย

ตัวชี้วัดที่ 1 มีกิจกรรมเพื่อยกระดับขีดความสามารถของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้สามารถปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 จำนวนไม่น้อยกว่า 1 กิจกรรมต่อปี

ตัวชี้วัดที่ 2 มีหลักสูตรมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จำนวนไม่น้อยกว่า 2 หลักสูตร ภายในปี พ.ศ. 2570

ตัวชี้วัดที่ 3 มีหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้รับการยกระดับขีดความสามารถการปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 รวมจำนวนไม่น้อยกว่า 250 หน่วยงาน ภายในปี พ.ศ. 2573

โครงการขับเคลื่อนกลยุทธ์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
3.1.1 โครงการยกระดับขีดความสามารถของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	1. กิจกรรมยกระดับขีดความสามารถของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 • สำรวจความต้องการของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อใช้เป็นข้อมูลประกอบการพัฒนาหลักสูตรและกำหนดรูปแบบกิจกรรม	**หน่วยงานกำกับดูแล** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.)

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
ในการปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567	• พัฒนาหลักสูตรเพื่อยกระดับขีดความสามารถให้สามารถปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 • จัดการฝึกอบรมตามหลักสูตรเพื่อยกระดับขีดความสามารถให้สามารถปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานที่เกี่ยวข้อง ทั้งด้านนโยบาย การบริหารจัดการ และการปฏิบัติในเชิงเทคนิค • จัดกิจกรรมเพื่อการยกระดับขีดความสามารถของหน่วยงาน ให้สามารถปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 เช่น การฝึกอบรมเชิงปฏิบัติการ (Workshop) หรือสัมมนาเชิงวิชาการ เพื่อเสริมสร้างความรู้ความเข้าใจอย่างมีประสิทธิภาพ	**หน่วยงานปฏิบัติ** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน) (สคช.) • หน่วยงานของรัฐ • หน่วยงานควบคุมหรือกำกับดูแล • หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ • ผู้ให้บริการคลาวด์ • ภาคเอกชนหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

กลยุทธ์ที่ 3.2

- เสริมสร้างทักษะด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ให้บุคลากรที่เกี่ยวข้อง

เป้าหมายของกลยุทธ์

- บุคลากรที่เกี่ยวข้องมีความรู้และทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (ยุทธศาสตร์ที่ 3 วัตถุประสงค์ที่ 2)

ตัวชี้วัดของกลยุทธ์/ค่าเป้าหมาย

ตัวชี้วัดที่ 1 มีหลักสูตรฝึกอบรมเฉพาะทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ รวมจำนวนไม่น้อยกว่า 10 หลักสูตร ภายในปี พ.ศ. 2573
ตัวชี้วัดที่ 2 มีผู้เข้ารับการอบรมในหลักสูตรฝึกอบรมเฉพาะทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ รวมจำนวนไม่น้อยกว่า 1,000 คน ภายในปี พ.ศ. 2573

โครงการขับเคลื่อนกลยุทธ์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
3.2.1 โครงการเสริมสร้างทักษะด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ให้บุคลากรที่เกี่ยวข้อง	1. กิจกรรมเสริมสร้างทักษะด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ให้บุคลากรที่เกี่ยวข้อง • ศึกษาความต้องการทักษะของบุคลากร และเส้นทางอาชีพ (Career Pathway) ของบุคลากรทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ • ศึกษาเนื้อหาประกาศนียบัตรตามมาตรฐานสากลและหลักสูตรจากหน่วยงานอื่น ๆ เพื่อการเทียบเคียงหลักสูตร • พัฒนาหลักสูตรฝึกอบรมเฉพาะทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ เช่น Cloud Architect, Cloud Security Engineer, Cloud Risk Officer โดยอาจเป็นภาษาไทยหรือภาษาอังกฤษ รวมถึงการสร้างความร่วมมือกับมหาวิทยาลัย สถานศึกษา ภาคเอกชน และผู้ให้บริการคลาวด์ ในการพัฒนาหลักสูตรฝึกอบรมเฉพาะทางที่เหมาะสมกับระดับทักษะของบุคลากร รวมถึงลดความซ้ำซ้อนและสามารถใช้ประโยชน์ร่วมกันได้ • จัดกิจกรรมฝึกอบรมและสัมมนาทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ โดยอาจดำเนินการโดย สกมช. หรือหน่วยงานภาครัฐและเอกชน • จัดการทดสอบเพื่อรับประกาศนียบัตรรับรองคุณวุฒิ	**หน่วยงานกำกับดูแล** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) **หน่วยงานปฏิบัติ** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) • สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
		• สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน) (สคช.) • กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (อว.) • ผู้ให้บริการคลาวด์ • ภาคเอกชนหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

กลยุทธ์ที่ 3.3

- พัฒนาระบบสนับสนุนด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานและบุคลากรที่เกี่ยวข้อง

เป้าหมายของกลยุทธ์

- มีกลไกสนับสนุนด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานและบุคลากรที่เกี่ยวข้อง (ยุทธศาสตร์ที่ 3 วัตถุประสงค์ที่ 3)

ตัวชี้วัดของกลยุทธ์/ค่าเป้าหมาย

ตัวชี้วัดที่ 1 มีบริการที่ปรึกษาและให้ความช่วยเหลือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่นที่เกี่ยวข้อง ที่สามารถเปิดให้บริการได้ภายในปี พ.ศ. 2569

ตัวชี้วัดที่ 2 มีระดับความพึงพอใจของบริการที่ปรึกษาและให้ความช่วยเหลือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ไม่น้อยกว่าร้อยละ 80

โครงการขับเคลื่อนกลยุทธ์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
3.3.1 โครงการพัฒนาระบบสนับสนุนด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานและบุคลากรที่เกี่ยวข้อง ตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567	1. กิจกรรมพัฒนาบริการที่ปรึกษาและให้ความช่วยเหลือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่นที่เกี่ยวข้อง • กำหนดแนวทาง ขอบเขต และกระบวนการสำหรับการให้คำปรึกษา และให้ความช่วยเหลือฯ เช่น การขอรับคำปรึกษาผ่านกลไก NCSA Cyber Clinic • กำหนดช่องทางการให้บริการที่ปรึกษาและให้ความช่วยเหลือฯ เช่น อีเมล หรือช่องทางสารบรรณ • กำหนดแนวทางการประเมินความพึงพอใจของบริการที่ปรึกษาและให้ความช่วยเหลือฯ • กำหนดมาตรฐานหรือข้อตกลงในการให้บริการทั้งในเชิงปริมาณและคุณภาพ เช่น การตอบสนองต่อการให้คำปรึกษาและให้ความช่วยเหลือฯ ภายในระยะเวลาที่กำหนด	**หน่วยงานกำกับดูแล** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) **หน่วยงานปฏิบัติ** • สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) • สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	2. กิจกรรมพัฒนาแพลตฟอร์มกลางเพื่อให้บริการที่ปรึกษาและให้ความช่วยเหลือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง • ระบบลงทะเบียนออนไลน์เพื่อให้หน่วยงานสามารถยื่นคำร้องขอเข้ารับบริการได้อย่างเป็นระบบ • การกำหนดข้อตกลงระดับการให้บริการ (SLA) สำหรับระบบการจองคิวเมื่อมีเหตุการณ์เร่งด่วน • การจัดหาทีมผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับทำหน้าที่เป็นที่ปรึกษา • การประชาสัมพันธ์เพื่อสร้างความตระหนักรับรู้	• สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) • สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) • หน่วยงานของรัฐ • หน่วยงานควบคุมหรือกำกับดูแล • หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ • ผู้ให้บริการคลาวด์ • ภาคเอกชนหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

3.4 ตารางสรุปโครงการและกิจกรรมขับเคลื่อนกลยุทธ์ เป้าหมาย ความเร่งด่วน งบประมาณและกรอบเวลา

คำชี้แจง

1. ตารางสรุปโครงการฯ นี้ มีวัตถุประสงค์เพื่อให้ สกมช. หน่วยงานกำกับดูแล หน่วยงานปฏิบัติ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง สามารถใช้เป็นแนวทางร่วมกันในการบูรณาการทรัพยากรเพื่อการขับเคลื่อนกลยุทธ์ต่าง ๆ ได้อย่างมีประสิทธิภาพ สอดคล้องกับความต้องการของผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์ และหน่วยงานด้านนโยบาย ตามวิสัยทัศน์ของแผนบูรณาการฯ ฉบับนี้
2. การกำหนดความเร่งด่วนของโครงการ เป็นไปตามประกาศ สกมช. เรื่อง กรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Thailand's National Cloud Security Framework) โดย สกมช. ได้มีหนังสือถึงผู้มีส่วนได้ส่วนเสีย และผู้ที่เกี่ยวข้อง เพื่อให้กำหนดลำดับความเร่งด่วนของการดำเนินการตามแผนบูรณาการฯ ซึ่งจะทำให้สามารถจัดสรรทรัพยากรที่มีอยู่อย่างจำกัดในการขับเคลื่อนการดำเนินการได้ตามวิสัยทัศน์ที่กำหนดไว้
3. แผนบูรณาการฯ ฉบับนี้ กำหนดความเร่งด่วนไว้ 3 ระยะ คือ ระยะสั้น (พ.ศ. 2569) ระยะกลาง (พ.ศ. 2570-2571) และระยะยาว (พ.ศ. 2572-2573)
4. ส่วนของงบประมาณและกรอบเวลาในตารางนี้ มีหน่วยเป็นล้านบาท

โครงการและกิจกรรม	เป้าหมาย	ความเร่งด่วน	งบประมาณและกรอบเวลา					หมายเหตุ
			69	70	71	72	73	
ยุทธศาสตร์ที่ 1 รวมพลังภาครัฐและเอกชน								
กลยุทธ์ที่ 1.1 ส่งเสริมและสนับสนุนความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชน ทั้งภายในและต่างประเทศ								
โครงการส่งเสริมและสนับสนุนความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชน ทั้งภายในและต่างประเทศ เพื่อยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย								
(1) กิจกรรมจัดตั้งกลไกความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ระหว่างหน่วยงานภาครัฐและเอกชน (Public–Private Cloud Security Collaboration Mechanism)	ตัวชี้วัดที่ 1, 2	ระยะสั้น - กลาง - ยาว	0	0	0	0	0	สกมช. สามารถดำเนินการได้โดยไม่ใช้งบประมาณ

โครงการและกิจกรรม	เป้าหมาย	ความเร่งด่วน	งบประมาณและกรอบเวลา					หมายเหตุ
			69	70	71	72	73	
(2) กิจกรรมกำหนดแนวทางส่งเสริมและสนับสนุนความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนทั้งภายในและต่างประเทศ	ตัวชี้วัดที่ 2	ระยะสั้น - กลาง - ยาว	0	0	0	0	0	สกมช. สามารถดำเนินการได้โดยไม่ใช้งบประมาณ
(3) กิจกรรมสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนทั้งภายในและต่างประเทศ	ตัวชี้วัดที่ 3	ระยะกลาง - ยาว	-	5	5	5	5	
กลยุทธ์ที่ 1.2 จัดตั้งกลไกความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ในการสนับสนุนการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ และอาชญากรรมทางไซเบอร์								
โครงการจัดตั้งกลไกความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ในการสนับสนุนการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์และอาชญากรรมทางไซเบอร์								
(1) กิจกรรมส่งเสริมและพัฒนากลไกความร่วมมือและการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ในการสนับสนุนการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ และอาชญากรรมทางไซเบอร์	ตัวชี้วัดที่ 1, 2	ระยะสั้น - กลาง - ยาว	0	5	5	5	5	
(2) กิจกรรมส่งเสริมและพัฒนาศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีขีดความสามารถในการเฝ้าระวัง แจ้งเตือนและรับมือกับภัยคุกคามทางไซเบอร์ที่มีต่อระบบคลาวด์	ตัวชี้วัดที่ 1, 2	ระยะกลาง - ยาว	-	10	10	10	10	
(3) กิจกรรมส่งเสริมและพัฒนาความร่วมมือและการแลกเปลี่ยนข้อมูลด้านความมั่นคง	ตัวชี้วัดที่ 1, 2	ระยะกลาง - ยาว	-	3	3	3	3	

โครงการและกิจกรรม	เป้าหมาย	ความเร่งด่วน	งบประมาณและกรอบเวลา					หมายเหตุ
			69	70	71	72	73	
ปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานควบคุมหรือกำกับดูแล								
(4) กิจกรรมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์และอาชญากรรมทางไซเบอร์ที่เกี่ยวข้องกับระบบคลาวด์	ตัวชี้วัดที่ 3	ระยะสั้น – กลาง – ยาว	0	5	5	5	5	ในปี 2569 สกมช. สามารถดำเนินการได้โดยไม่ใช้งบประมาณผ่านกิจกรรมการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ (Thailand's National Cyber Exercise) ส่วนปีต่อ ๆ ไปจะเป็นการจัดทำ Table-top exercise package และการส่งเสริมให้เกิดการใช้งานในหน่วยงานต่าง ๆ
กลยุทธ์ที่ 1.3 จัดตั้งเครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย								
โครงการจัดตั้งเครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย								
(1) กิจกรรมสำรวจข้อมูลผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย	ตัวชี้วัดที่ 1, 2	ระยะสั้น	0	-	-	-	-	สกมช. สามารถดำเนินการได้โดยไม่ใช้งบประมาณ
(2) กิจกรรมจัดตั้งเครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย	ตัวชี้วัดที่ 1, 2	ระยะสั้น – กลาง – ยาว	0	2	2	2	2	สกมช. สามารถดำเนินการได้ในช่วงแรก (2569) โดยไม่ใช้งบประมาณ หลังจากนั้นเมื่อเครือข่ายขยายใหญ่ขึ้น จึงจำเป็นต้องใช้งบประมาณในการยกระดับคุณภาพการบริหารเครือข่ายผู้เชี่ยวชาญฯ ให้สามารถตอบสนองความต้องการได้ดีขึ้น
(3) กิจกรรมพัฒนาแพลตฟอร์มกลางสำหรับเครือข่ายผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย	ตัวชี้วัดที่ 1, 2	ระยะกลาง	0	5	-	-	-	สกมช. สามารถดำเนินการออกแบบและเก็บความต้องการในปีงบประมาณ 2569 และเริ่มพัฒนาแพลตฟอร์มในปีงบประมาณ 2570
(4) กิจกรรมจัดทำธรรมนูญเครือข่ายและโครงสร้างธรรมาภิบาลด้านความเป็นกลาง	ตัวชี้วัดที่ 1, 2	ระยะกลาง	-	2	-	-	-	

โครงการและกิจกรรม	เป้าหมาย	ความเร่งด่วน	งบประมาณและกรอบเวลา					หมายเหตุ
			69	70	71	72	73	
ยุทธศาสตร์ที่ 2 สร้างสภาพแวดล้อมที่เอื้อต่อการดำเนินการตามมาตรฐาน								
กลยุทธ์ที่ 2.1 พัฒนากลไกการตรวจรับรองมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์								
โครงการพัฒนากลไกการตรวจรับรองมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์								
(1) กิจกรรมพัฒนากลไกการตรวจรับรองมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์	ตัวชี้วัดที่ 1	ระยะสั้น - กลาง	0	0	-	-	-	สกมช. สามารถดำเนินการได้โดยไม่ใช้งบประมาณ
(2) กิจกรรมจัดการอบรมสำหรับหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567	ตัวชี้วัดที่ 2	ระยะกลาง – ยาว	-	3	3	3	3	
โครงการพัฒนาแพลตฟอร์มกลางเพื่อการตรวจรับรองมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์								
(1) กิจกรรมพัฒนาแพลตฟอร์มกลางสำหรับการเชื่อมโยงข้อมูลผู้ตรวจสอบ (Auditor) และหน่วยงานให้บริการตรวจรับรอง (Certify Body) ที่ผ่านการอบรมแล้วเข้ากับระบบกลาง	ตัวชี้วัดที่ 3, 4	ระยะกลาง - ยาว	-	-	5	0	0	สกมช. สามารถดำเนินการออกแบบและเก็บความต้องการในปีงบประมาณ 2569 และเริ่มพัฒนาแพลตฟอร์มในปีงบประมาณ 2571
(2) กิจกรรมพัฒนาแพลตฟอร์มกลางสำหรับใช้ติดตามสถานการณ์ตรวจประเมินผู้ให้บริการคลาวด์	ตัวชี้วัดที่ 3, 4	ระยะกลาง - ยาว	-	-	5	0	0	สกมช. สามารถดำเนินการออกแบบและเก็บความต้องการในปีงบประมาณ 2569 และเริ่มพัฒนาแพลตฟอร์มในปีงบประมาณ 2571

โครงการและกิจกรรม	เป้าหมาย	ความเร่งด่วน	งบประมาณและกรอบเวลา					หมายเหตุ
			69	70	71	72	73	
โครงการยกระดับและขยายขีดความสามารถหน่วยงานตรวจรับรองและผู้ตรวจสอบ (Certify Body and Auditor Capacity Expansion)								
(1) กิจกรรมจัดการอบรมสำหรับหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567	ตัวชี้วัดที่ 2	ระยะกลาง – ยาว	-	3	3	3	3	
กลยุทธ์ที่ 2.2 ส่งเสริมให้มีกลไกการกำกับดูแลโดยหน่วยงานที่เกี่ยวข้องกับการกำหนดนโยบาย (Policy Agencies) และหน่วยงานควบคุมหรือกำกับดูแล (Regulator) ที่เป็นเอกภาพ								
โครงการส่งเสริมกลไกการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Cloud Security Governance) ร่วมกับหน่วยงานที่เกี่ยวข้องกับการกำหนดนโยบาย (Policy Agencies) และหน่วยงานควบคุมหรือกำกับดูแล (Regulator)								
(1) กิจกรรมส่งเสริมกลไกการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (Cloud Security Governance)	ตัวชี้วัดที่ 1	ระยะสั้น – กลาง – ยาว	0	3	3	3	3	ปีงบประมาณ 2569 ดำเนินการตั้งคณะทำงานและกำหนดหลักเกณฑ์ ส่วนกิจกรรมดำเนินการตั้งแต่ 2570 เป็นต้นไป (ปีละ 2 ครั้ง)
โครงการทบทวนแผนบูรณาการฯ เพื่อขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์								
(1) กิจกรรมทบทวนแผนบูรณาการฯ เพื่อขับเคลื่อนการดำเนินการตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์	ตัวชี้วัดที่ 2	ระยะสั้น – กลาง – ยาว	0	2	2	2	2	ปีงบประมาณ 2569 รวบรวมและวิเคราะห์ข้อมูล ส่วนกิจกรรมประชุมเชิงปฏิบัติการดำเนินการตั้งแต่ 2570 เป็นต้นไป

โครงการและกิจกรรม	เป้าหมาย	ความเร่งด่วน	งบประมาณและกรอบเวลา					หมายเหตุ
			69	70	71	72	73	
กลยุทธ์ที่ 2.3 จัดทำแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง เพื่อส่งเสริมการปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567								
โครงการจัดทำแนวทาง คำแนะนำ และเอกสารต้นแบบเพื่อขับเคลื่อนการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์								
(1) กิจกรรมจัดทำแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ เพื่อขับเคลื่อนการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์	ตัวชี้วัดที่ 1, 2	ระยะสั้น – กลาง – ยาว	0	2	2	2	2	กิจกรรมประชุมเชิงปฏิบัติการ (Workshop) และเวทีแลกเปลี่ยนความรู้ ดำเนินการปีงบประมาณ 2570 เป็นต้นไป
(2) กิจกรรมรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียและผู้ที่เกี่ยวข้อง	ตัวชี้วัดที่ 3	ระยะสั้น – กลาง – ยาว	0	0	0	0	0	สกมช. สามารถดำเนินการได้โดยไม่ใช้งบประมาณ
โครงการพัฒนาเครื่องมือในการประเมินตนเองตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ								
(1) กิจกรรมแบบประเมินตนเอง (Self-Assessment) ตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567	ตัวชี้วัดที่ 1, 2	ระยะสั้น – กลาง – ยาว	0	2	2	2	2	ปีงบประมาณ 2569 สกมช. สามารถดำเนินการได้โดยไม่ใช้งบประมาณ หลังจากการพัฒนาแบบประเมินแล้วเสร็จจะเป็นการจัดการประชุมเชิงปฏิบัติการให้กับหน่วยงานต่าง ๆ
(2) กิจกรรมพัฒนาแพลตฟอร์มสำหรับประเมินตนเอง (Self-Assessment Platform) และพัฒนาเอกสารต้นแบบ (Template) สำหรับหน่วยงานเลือกใช้งาน	ตัวชี้วัดที่ 1, 2, 3, 4	ระยะสั้น – กลาง – ยาว	0	5	0	0	0	สกมช. สามารถดำเนินการพัฒนารายการตรวจสอบต้นแบบ (Checklist) โดยไม่ใช้งบประมาณในปี 2569 หลังจากนั้นจึงพัฒนาแพลตฟอร์มสำหรับประเมินตนเอง

โครงการและกิจกรรม	เป้าหมาย	ความเร่งด่วน	งบประมาณและกรอบเวลา					หมายเหตุ
			69	70	71	72	73	
(3) กิจกรรมพัฒนาหลักสูตร E-learning สำหรับการประเมินตนเอง (Self-Assessment)	ตัวชี้วัดที่ 1, 2, 4	ระยะสั้น – กลาง – ยาว	0	2	0	0	0	
โครงการทบทวนคุณภาพของแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์								
(1) กิจกรรมทบทวนคุณภาพของแนวปฏิบัติ คำแนะนำ หลักเกณฑ์ วิธีการ เครื่องมือ หรือเอกสารต้นแบบ ตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์	ตัวชี้วัดที่ 2, 3	ระยะสั้น – กลาง – ยาว	0	0	0	0	0	สกมช. สามารถดำเนินการได้โดยไม่ใช้งบประมาณ
กลยุทธ์ที่ 2.4 ส่งเสริมการวิจัยและนวัตกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์								
โครงการส่งเสริมการวิจัยและนวัตกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์								
(1) กิจกรรมส่งเสริมการวิจัยและนวัตกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์	ตัวชี้วัดที่ 1	ระยะสั้น – กลาง – ยาว	0	1	1	1	1	มีค่าใช้จ่ายในการร่วมประชุมวิชาการระดับนานาชาติ
ยุทธศาสตร์ที่ 3 พัฒนาขีดความสามารถของหน่วยงานและบุคลากร								
กลยุทธ์ที่ 3.1 ยกระดับขีดความสามารถของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้สามารถปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ได้อย่างมีประสิทธิภาพ								
โครงการยกระดับขีดความสามารถของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการปฏิบัติตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัย								

โครงการและกิจกรรม	เป้าหมาย	ความเร่งด่วน	งบประมาณและกรอบเวลา					หมายเหตุ
			69	70	71	72	73	
ไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567								
(1) กิจกรรมยกระดับขีดความสามารถของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการปฏิบัติตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567	ตัวชี้วัดที่ 1, 2, 3	ระยะสั้น – กลาง – ยาว	0	5	5	5	5	
กลยุทธ์ที่ 3.2 เสริมสร้างทักษะด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ให้บุคลากรที่เกี่ยวข้อง								
โครงการเสริมสร้างทักษะด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ให้บุคลากรที่เกี่ยวข้อง								
(1) กิจกรรมเสริมสร้างทักษะด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ให้บุคลากรที่เกี่ยวข้อง	ตัวชี้วัดที่ 1, 2	ระยะสั้น – กลาง – ยาว	0	5	5	5	5	
กลยุทธ์ที่ 3.3 พัฒนาระบบสนับสนุนด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานและบุคลากรที่เกี่ยวข้อง								
โครงการพัฒนาระบบสนับสนุนด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานและบุคลากรที่เกี่ยวข้อง ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567								
(1) กิจกรรมพัฒนาบริการที่ปรึกษาและให้ความช่วยเหลือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานของรัฐ	ตัวชี้วัดที่ 1, 2	ระยะยาว	0	0	2	2	2	ปีงบประมาณ 2569 – 2570 สกมช. สามารถดำเนินการได้โดยไม่ใช้งบประมาณ หลังนั้นจะมีการยกระดับการบริการโดย

โครงการและกิจกรรม	เป้าหมาย	ความเร่งด่วน	งบประมาณและกรอบเวลา					หมายเหตุ
			69	70	71	72	73	
หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่นที่เกี่ยวข้อง								จัดหาที่ปรึกษาด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์มาสนับสนุนการดำเนินการ
(2) กิจกรรมพัฒนาแพลตฟอร์มกลางเพื่อให้บริการที่ปรึกษาและให้ความช่วยเหลือด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ รวมถึงหน่วยงานอื่นที่เกี่ยวข้อง	ตัวชี้วัดที่ 1, 2	ระยะสั้น – กลาง – ยาว	0	0	5	0	0	สกมช. สามารถดำเนินการออกแบบและเก็บความต้องการในปีงบประมาณ 2569 และเริ่มพัฒนาแพลตฟอร์มในปีงบประมาณ 2571

3.5 กระบวนการในการกำกับดูแล ติดตาม ประเมินผล และรายงานผล

เพื่อให้การดำเนินงานตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 เป็นไปอย่างมีประสิทธิภาพ โปร่งใส และสามารถบรรลุเป้าหมายตามแผนบูรณาการฯ ได้อย่างครบถ้วน จึงกำหนดกระบวนการกำกับดูแล ติดตาม ประเมินผล และรายงานผลแผนบูรณาการฯ ดังต่อไปนี้

3.5.1 กระบวนการกำกับดูแล

3.5.1.1 จัดตั้งคณะกรรมการหรือคณะทำงานกำกับการดำเนินงานตามแผนบูรณาการฯ

การกำกับดูแลถือเป็นกลไกหลักในการกำหนดทิศทางและสร้างความมั่นใจว่าการดำเนินงานเป็นไปตามแผนบูรณาการฯ ทั้งนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จะดำเนินการร่วมกับหน่วยงานระดับนโยบายที่เกี่ยวข้อง เช่น

- กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.)
- สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.)
- สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)
- ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค)
- หน่วยงานควบคุมหรือกำกับดูแลอื่นที่เกี่ยวข้อง
- หน่วยงานของรัฐอื่นที่เกี่ยวข้อง

3.5.1.2 กำหนดบทบาทและความรับผิดชอบของหน่วยงานกำกับดูแลและหน่วยงานปฏิบัติ

หน่วยงานกำกับดูแลซึ่งรับผิดชอบในการขับเคลื่อนแต่ละกลยุทธ์ จะต้องทำหน้าที่บริหารจัดการโครงการในภาพรวม ทั้งในด้านการวางแผน การจัดสรรทรัพยากร การประสานความร่วมมือ และการกำกับให้การดำเนินงานเป็นไปตามเป้าหมายที่กำหนดไว้ ขณะเดียวกัน หน่วยงานปฏิบัติจะทำหน้าที่ให้ความช่วยเหลือในด้านวิชาการ เทคโนโลยี งบประมาณ หรือทรัพยากรบุคคล ตามความเชี่ยวชาญและอำนาจหน้าที่ของแต่ละหน่วยงาน

เพื่อให้การดำเนินงานมีความคล่องตัว ต้องจัดให้มีช่องทางประสานงาน เช่น ช่องทางติดต่อประจำโครงการ กลไกติดตามงานแบบออนไลน์ หรือระบบรายงานความก้าวหน้า ซึ่งช่วยให้หน่วยงานที่เกี่ยวข้องสามารถแลกเปลี่ยนข้อมูล ประสานงาน และแจ้งประเด็นปัญหาได้อย่างเป็นระบบ

3.5.2 กระบวนการติดตามความก้าวหน้า

3.5.2.1 ดำเนินการติดตามผลเป็นรายครึ่งปี

เพื่อให้การขับเคลื่อนแผนบูรณาการฯ เป็นไปอย่างมีประสิทธิภาพและสามารถประเมินผลจึงกำหนดให้มีการดำเนินการติดตามผลการดำเนินงานอย่างน้อยปีละ 2 ครั้ง โดยเน้นการติดตามความก้าวหน้าในทุกระดับของแผนงาน ทั้งระดับยุทธศาสตร์ ระดับกลยุทธ์ และระดับโครงการ เพื่อให้สามารถประเมินได้ว่าการดำเนินงานเป็นไปตามเป้าหมายที่กำหนดไว้หรือไม่

การติดตามผลดังกล่าวครอบคลุมการตรวจสอบความก้าวหน้าของภารกิจและกิจกรรมสำคัญ ตลอดจนการประเมินผลสัมฤทธิ์ของตัวชี้วัดหลักตามค่าเป้าหมายที่กำหนดไว้ในแต่ละปี ทั้งนี้ เพื่อให้สามารถระบุประเด็นปัญหา อุปสรรค หรือความเสี่ยงที่อาจเกิดขึ้น และสามารถกำหนดแนวทางปรับปรุงหรือแก้ไขได้อย่างทันท่วงที

3.5.2.2 จัดประชุมติดตามผลร่วมกับหน่วยรับผิดชอบ

กำหนดให้มีการจัดประชุมติดตามผลร่วมกับหน่วยงานที่รับผิดชอบการดำเนินงานในแต่ละกลยุทธ์และโครงการอย่างสม่ำเสมอ โดยมีวัตถุประสงค์เพื่อทบทวนความคืบหน้าของการดำเนินงาน ตรวจสอบอุปสรรคหรือปัจจัยเสี่ยงที่อาจส่งผลกระทบต่อความสำเร็จของโครงการ รวมทั้งร่วมกันพิจารณาแนวทางแก้ไขหรือแนวทางปรับปรุงที่เหมาะสม เพื่อให้สามารถขับเคลื่อนงานได้ตามกรอบเวลาที่กำหนด

3.5.3 กระบวนการประเมินผล

เพื่อให้การดำเนินงานตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์เป็นไปอย่างมีประสิทธิผลและสามารถสะท้อนผลสัมฤทธิ์ของแผนได้อย่างชัดเจน แผนบูรณาการฯ จึงได้กำหนดกระบวนการประเมินผลซึ่งครอบคลุมทั้งการประเมินระหว่างดำเนินงานและการประเมินเมื่อสิ้นสุดแผน ดังต่อไปนี้

- การประเมินผลอย่างน้อยปีละ 2 ครั้ง เพื่อให้สามารถตรวจสอบความเหมาะสมของเป้าหมาย กลยุทธ์ และแนวทางการดำเนินงานภายใต้บริบทด้านเทคโนโลยีและภัยคุกคามที่มีการเปลี่ยนแปลง ซึ่งทำให้สามารถปรับปรุงทิศทางการขับเคลื่อนงานให้เท่าทันสถานการณ์และรองรับความเสี่ยงด้านความมั่นคงไซเบอร์ที่อาจเกิดขึ้นใหม่ได้

- การประเมินผลโดยพิจารณาจากตัวชี้วัดของแต่ละกลยุทธ์ โดยตรวจสอบผลการดำเนินงานตามเป้าหมายที่กำหนด เช่น จำนวนมาตรฐานหรือแนวทางปฏิบัติที่ต้องพัฒนาให้แล้วเสร็จภายในระยะเวลาที่กำหนด ทั้งนี้ โดยคำนึงถึงทรัพยากรที่ได้รับเพื่อขับเคลื่อนการดำเนินการตามแผนบูรณาการฯ รวมถึงนโยบาย

- การประเมินผลเมื่อแผนสิ้นสุด จะมีการประเมินผลสรุปภาพรวม โดยพิจารณาความสำเร็จของยุทธศาสตร์ กลยุทธ์ เป้าหมาย ตัวชี้วัด และโครงการต่าง ๆ รวมถึงปัญหาและอุปสรรคที่พบระหว่างการดำเนินงาน เพื่อกำหนดข้อเสนอแนะสำหรับการจัดทำแผนในระยะต่อไป

3.5.4 กระบวนการรายงานผล

3.5.4.1 จัดทำรายงานผลการดำเนินงานประจำปี

กำหนดให้มีการจัดทำรายงานผลการดำเนินงานประจำปี โดยรายงานฉบับดังกล่าวจะต้องสรุปผลการดำเนินงานในรอบปีงบประมาณอย่างครบถ้วน รวมถึงสรุปความก้าวหน้า ผลลัพธ์ที่เกิดขึ้นจริง ตัวชี้วัดตามเป้าหมายที่กำหนด ปัญหา อุปสรรค ตลอดจนความเสี่ยงที่พบในระหว่างดำเนินงาน พร้อมทั้งข้อเสนอแนะหรือแนวทางแก้ไขที่เหมาะสมเพื่อใช้ประกอบการพิจารณาในระยะต่อไป

รายงานผลการดำเนินงานประจำปีนี้จะถูกนำเสนอให้แก่ คณะกรรมการหรือคณะทำงานกำกับการดำเนินงานตามแผนบูรณาการฯ และผู้บริหารระดับสูงของหน่วยงานที่เกี่ยวข้อง เพื่อใช้ในการกำกับตัดสินใจเชิงนโยบาย และกำหนดทิศทางการพัฒนางานด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ต่อไป

3.5.4.2 เผยแพร่ผลสำคัญต่อสาธารณะ

จะมีการเผยแพร่ผลสำคัญของการดำเนินงานอย่างเป็นทางการต่อสาธารณะ โดยเนื้อหาที่เผยแพร่จะประกอบด้วยผลลัพธ์เชิงยุทธศาสตร์ ความก้าวหน้าของมาตรการสำคัญ ข้อค้นพบเชิงวิเคราะห์ ตลอดจนข้อมูลที่แสดงให้เห็นถึงการยกระดับความมั่นคงปลอดภัยของระบบคลาวด์ของประเทศโดยรวม เพื่อให้เกิดความโปร่งใส และความตระหนักรับรู้ถึงการดำเนินการของแผนบูรณาการฯ ด้วย

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
สำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
120 หมู่ 3 อาคารซี ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กทม. 10210
โทรศัพท์ 0 2502 7826
โทรสาร 0 2143 7593
อีเมล cii@ncsa.or.th