ระดับ 1 : Assessment

ตัวชี้วัด 4.20 : ระดับความสำเร็จของการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย (รอบ 5 เดือนหลัง) ของกองแผนงาน

ระดับ 1 : Assessment ศึกษาและการวิเคราะห์สถานการณ์ของการรักษาความมั่นคงปลอดภัยไซเบอร์

1.1 ผลการวิเคราะห์สถานการณ์ของตัวชี้วัด

กรมอนามัยเป็นหน่วยงานหลักในการดำเนินงานด้านการส่งเสริมสุขภาพและอนามัยสิ่งแวดล้อม โดยมีการนำระบบสารสนเทศและข้อมูลสุขภาพมาใช้เป็นกลไกสำคัญในการสนับสนุนการดำเนินงานและการให้บริการแก่ประชาชน ซึ่งระบบดังกล่าวถือเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ อย่างไรก็ตาม จากการพัฒนาองค์กรสู่ดิจิทัลด้านสุขภาพ ประกอบกับแนวโน้มภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นอย่างต่อเนื่อง ทำให้ระบบสารสนเทศและข้อมูลสุขภาพมีความเสี่ยงต่อการถูกโจมตี การเข้าถึงโดยไม่ได้รับอนุญาต และการรั่วไหลของข้อมูล ซึ่งอาจส่งผลกระทบต่อความต่อเนื่องของบริการ อีกทั้งยังพบข้อจำกัดด้านมาตรฐานการรักษาความมั่นคงปลอดภัยที่ยังไม่ครอบคลุมทุกหน่วยงาน และความตระหนักของบุคลากรที่ยังต้องได้รับการพัฒนา ดังนั้น กรมอนามัยจึงมีความจำเป็นต้องยกระดับการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้มีประสิทธิภาพ เพื่อป้องกันและลดความเสี่ยง รักษาความต่อเนื่องของบริการ และคุ้มครองข้อมูลสุขภาพของประชาชนอย่างเหมาะสม โดยมีการสรุปผลการวิเคราะห์สถานการณ์ของตัวชี้วัด และความรู้ที่นำมาใช้ประกอบการวิเคราะห์ ดังนี้

1.1.1 ผลผลิต/ ผลลัพธ์ระดับ Le (Level) ของผลการดำเนินการในปัจจุบัน

การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ จำเป็นต้องอาศัยกระบวนการที่เป็นระบบในทุกขั้นตอน เพื่อตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและมีประสิทธิภาพ โดยสามารถแบ่งออกเป็น 5ขั้นตอนสำคัญ ได้แก่

1) การบริหารจัดการความเสี่ยง (Identify)

2) การกำหนดมาตรการควบคุมเพื่อปกป้องระบบขององค์กร (Protect)

3) การกำหนดขั้นตอนและกระบวนการเพื่อตรวจจับสถานการณ์ผิดปกติ (Detect)

4) การกำหนดขั้นตอนและกระบวนการเพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น (Respond)

5) การกำหนดขั้นตอนและกระบวนการเพื่อให้องค์กรสามารถดำเนินงานได้อย่างต่อเนื่องและฟื้นฟูระบบให้กลับคืนสู่ภาวะปกติ (Recover)

ดังนั้น เพื่อแก้ไขปัญหาความเสี่ยงและยกระดับขีดความสามารถขององค์กร กระบวนการนี้จึงถูกนำมาใช้เป็นกลไกหลักในการขับเคลื่อนการดำเนินงาน โดยมุ่งเน้น 2 มิติสำคัญ ได้แก่

1) มิติด้านความมั่นคงปลอดภัย (Cyber Security & Governance) กำหนดมาตรฐานกลาง ยกระดับโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ และพัฒนาระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ เพื่อให้สามารถลดความเสี่ยงได้อย่างเป็นรูปธรรม

2) มิติการพัฒนาบุคลากร (Digital and Data Capability) พัฒนาทักษะของบุคลากรให้มีความรู้ความสามารถด้านข้อมูลและดิจิทัล ตลอดจนมีความตระหนักด้านความมั่นคงปลอดภัย เพื่อให้สามารถใช้ประโยชน์จากข้อมูลขนาดใหญ่ในการตัดสินใจและวางแผนยุทธศาสตร์ได้อย่างมีประสิทธิภาพ

ผลการดำเนินการในเดือนตุลาคม 2568 - กุมภาพันธ์ 2569 (รอบ 5 เดือนแรก) ดังนี้

การดำเนินงานเดือนตุลาคม 2568 - กุมภาพันธ์ 2569 ก่อให้เกิดผลสัมฤทธิ์ที่สำคัญในการยกระดับองค์กรอย่างชัดเจน ทั้งในมิติของความมั่นคงปลอดภัยทางไซเบอร์และความพร้อมด้านข้อมูล เพื่อรองรับการเป็นองค์กรที่ขับเคลื่อนด้วยข้อมูลจริง ดังนี้

1) ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) กรมอนามัยได้ดำเนินการยกระดับความมั่นคงปลอดภัยทางไซเบอร์อย่างครอบคลุม โดยเริ่มจากการทบทวนและปรับปรุงนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นปัจจุบัน พร้อมทั้งจัดทำแผนบริหารความเสี่ยง ประเมินและจัดลำดับความเสี่ยงด้านไซเบอร์ขององค์กร รวมถึงกำหนดมาตรการบริหารจัดการความเสี่ยงที่เหมาะสม พร้อมทั้งดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะมาตรา 54 ว่าด้วยการรายงานเหตุการณ์และการประสานงานกับหน่วยงานที่เกี่ยวข้อง

ทั้งนี้ได้กำหนดให้ใช้มาตรฐานกลางด้านความมั่นคงปลอดภัยโดยอ้างอิงเกณฑ์การประเมิน CTAM+ (Cybersecurity Technical Assessment Matrix Plus) ของสำนักงานปลัดกระทรวงสาธารณสุข ประจำปี 2569 ซึ่งประกอบด้วยข้อกำหนดหลัก 11 ข้อ ได้แก่ 1) Backup 2) Antivirus Software 3) Access Control 4) Privileged Access Management (PAM) 5) แผน BCP/DRP 6) OS Patching 7) Multi-Factor Authentication (2FA) 8) Web Application Firewall (WAF) 9) Log Management 10) Security Information and Event Management (SIEM) และ 11) Vulnerability Assessment (VA Scan) และข้อกำหนดเพิ่มเติม (Plus) อีก 6 ข้อ ครอบคลุมการสำรวจและปิดระบบที่ไม่ใช้งาน การอัปเดตซอฟต์แวร์ด้านความปลอดภัย Network Segmentation การใช้ซอฟต์แวร์ถูกลิขสิทธิ์ Penetration Testing และการจัดทำนโยบายไซเบอร์ควบคู่กับการพัฒนาบุคลากร

โดยกรมอนามัยได้เข้าร่วมการตรวจแนะนำจากหน่วยงานกำกับดูแล และเข้าร่วม Thailand Cyber Exercise เพื่อทดสอบความพร้อมในการรับมือภัยคุกคามในระดับประเทศ รวมถึงประสานการทำงานร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และสำนักงานปลัดกระทรวงสาธารณสุขในฐานะหน่วยงานกำกับดูแล (Regulator) อย่างต่อเนื่อง

2) ระบบเฝ้าระวังและลดภัยคุกคาม กรมอนามัยได้พัฒนาระบบเฝ้าระวังภัยคุกคามเชิงรุกในหลายมิติ โดยได้ติดตั้งและปรับปรุงอุปกรณ์ป้องกันภัยคุกคามเพิ่มเติม ได้แก่ Firewall, Web Application Firewall (WAF), Intrusion Prevention System (IPS), ระบบป้องกัน DDoS และระบบ Network Detection and Response (NDR) เพื่อเพิ่มขีดความสามารถในการตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที

ในด้านการเฝ้าระวังเชิงรุก ได้ดำเนินการ Vulnerability Assessment Scan (VA Scan) ด้วยโปรแกรม Nessus เป็นประจำทุกเดือน พร้อมติดตามและดำเนินการแก้ไขช่องโหว่อย่างต่อเนื่อง นอกจากนี้ยังได้จัดตั้งทีม Virtual SOC เพื่อเฝ้าระวังและตอบสนองต่อเหตุการณ์ด้านความปลอดภัยและดำเนินการซักซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP) อย่างสม่ำเสมอ

ในส่วนของความร่วมมือกับหน่วยงานภายนอก ได้เข้าร่วมโครงการกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ทั้งโครงการ Honeypot เพื่อดักจับและวิเคราะห์พฤติกรรมของผู้บุกรุก และโครงการตรวจจับ DNS ที่เป็นอันตรายผ่าน Cloudflare Gateway ส่งผลให้ความเสี่ยงถูกควบคุมและลดลงอย่างชัดเจน พบว่า รอบ 5 เดือนแรกตรวจพบเหตุภัยคุกคามหรือช่องโหว่รวม 6 ครั้ง

แบ่งเป็น Ransomware 1 ครั้ง, Log file expose 1 ครั้ง, Configuration files exposed 1 ครั้ง และ Directory listing vulnerability 3 ครั้ง โดยทุกกรณีได้ดำเนินการแก้ไขเรียบร้อยภายใน 24 ชั่วโมง และไม่พบความเสียหายที่ส่งผลกระทบต่อระบบงาน ระบบเครือข่าย และเว็บไซต์ของหน่วยงานในสังกัดกรมอนามัย ทำให้ผลการดำเนินงานเป็นไปตามเป้าหมายที่กำหนด และเป็นการเตรียมความพร้อมเพื่อบรรลุเป้าหมายการควบคุมและลดจำนวนการละเมิดความปลอดภัยทางไซเบอร์ลง 50% (จาก 25 ครั้ง/ปี เหลือไม่เกิน 13 ครั้ง/ปี)

3) ด้านการพัฒนาศักยภาพบุคลากร (Digital Skill) โครงการได้พัฒนาทักษะด้านเทคโนโลยีดิจิทัลแก่บุคลากรในทุกระดับ

3.1) การบริหารจัดการความมั่นคงปลอดภัย (Cyber Governance) ดำเนินการจัดประชุมเชิงปฏิบัติการ ขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2569 ให้แก่บุคลากรส่วนกลางและส่วนภูมิภาค จำนวน 60 คน เพื่อเสริมสร้างศักยภาพและความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของกรมอนามัยให้สอดคล้องกับสถานการณ์ภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว โดยได้รับเกียรติจากผู้เชี่ยวชาญด้าน Cybersecurity จากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และภาคเอกชน ร่วมบรรยายและถ่ายทอดองค์ความรู้ การประชุมประกอบด้วยหัวข้อความรู้สำคัญ ได้แก่

- แนวทางปฏิบัติตามเกณฑ์ CTAM Plus
- การจัดการครุภัณฑ์คอมพิวเตอร์ด้าน Cybersecurity
- การบริหารจัดการภัยคุกคามไซเบอร์ (IR Case Sharing)
- การใช้งานระบบ Wazuh และ SIEM พร้อมภาคปฏิบัติการแบบเข้มข้น
- การแลกเปลี่ยนเรียนรู้ด้านความมั่นคงปลอดภัยสารสนเทศจากหน่วยงานสังกัดกรมอนามัย

3.2) ทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล (Digital Literacy) ดำเนินการจัดประชุมเชิงปฏิบัติการพัฒนาศักยภาพสู่การเป็นองค์กรขับเคลื่อนด้วยข้อมูล (Data-Driven Organization) เพื่อพัฒนาศักยภาพบุคลากรด้านการจัดการ วิเคราะห์ และนำเสนอข้อมูล ด้วยเครื่องมือดิจิทัลสมัยใหม่ และวางรากฐานการใช้ข้อมูลเป็นเครื่องมือหลักในการตัดสินใจเชิงนโยบายของกรมอนามัย ให้แก่บุคลากรส่วนกลางและส่วนภูมิภาค จำนวน 60 คน

3.3) การฝึกซ้อมแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) กองแผนงานได้ดำเนินการฝึกซ้อมแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) ในรูปแบบTable Top Exercise โดยกำหนดสถานการณ์สมมุติกรณีเกิดเหตุเพลิงไหม้ภายในห้อง Server ซึ่งอาจส่งผลกระทบต่อระบบสารสนเทศ อุปกรณ์เครือข่าย และการให้บริการภารกิจสำคัญของหน่วยงาน การฝึกซ้อมครั้งนี้มีวัตถุประสงค์เพื่อทดสอบความพร้อมของบุคลากร กระบวนการแจ้งเหตุ การสั่งการ การประสานงาน การกู้คืนระบบ และแนวทางการปฏิบัติงานทดแทนภายใต้ภาวะฉุกเฉิน

1.2 ผลการวิเคราะห์ผู้รับบริการและผู้มีส่วนได้ส่วนเสียเพื่อขับเคลื่อนตัวชี้วัด

ผลการวิเคราะห์ผู้รับบริการและผู้มีส่วนได้ส่วนเสียเพื่อขับเคลื่อน ได้แก่ กลุ่มผู้รับบริการ และผู้มีส่วนได้ส่วนเสีย โดยมีการสรุปผล ดังนี้

1.2.1 กลุ่มผู้รับบริการ

รายการข้อมูล	รายละเอียด
กลุ่มผู้รับบริการ	1. เจ้าหน้าที่สังกัดกรมอนามัย 2. ประชาชน
ความต้องการ	ระบบงานที่มีความมั่นคงปลอดภัย สามารถป้องกันการเข้าถึงข้อมูลได้
ความคาดหวัง	การรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีระดับที่สูงขึ้นและการตอบสนองที่รวดเร็วต่อการละเมิดภัยคุกคามทางไซเบอร์
ความผูกพัน	การปฏิบัติตามกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
ความพึงพอใจ	ระบบการแจ้งเตือนทางไซเบอร์ที่ทำให้ผู้รับบริการมีความตระหนักถึงความเสี่ยงทางด้านความมั่นคงปลอดภัยทางไซเบอร์
ความไม่พึงพอใจ	1. การไม่เข้าใจในกระบวนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 2. การใช้ภาษาด้านเทคนิคเข้าใจยาก
ข้อเสนอแนะจากผู้รับบริการ	1. ความปลอดภัยของข้อมูลส่วนตัวที่ภาครัฐเก็บไว้ต้องมีการรักษาความมั่นคงปลอดภัยไซเบอร์ 2. เผยแพร่ความรู้และข้อมูลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

1.2.2 กลุ่มผู้มีส่วนได้ส่วนเสีย

รายการข้อมูล	รายละเอียด
กลุ่มผู้มีส่วนได้ส่วนเสียปัจจุบัน	1. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง กรมอนามัย (CIO) 2. เจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย (Anamai - CIRT) 3. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ด้านสาธารณสุข (Health-CIRT) 4. สำนักคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
ความต้องการ	การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องตามกฎหมาย มาตรฐาน และนโยบายที่เกี่ยวข้อง
ความคาดหวัง	การป้องกันการเข้าถึงข้อมูลที่เป็นความลับ สามารถเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

รายการข้อมูล	รายละเอียด
ความผูกพัน	การกำหนดนโยบายและมาตรการที่เข้มงวด เพื่อสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์
ความพึงพอใจ	ระบบการแจ้งเตือนทางไซเบอร์ที่ทำให้ผู้มีส่วนได้ส่วนเสียรับทราบและตระหนักถึงความเสี่ยงอย่างรวดเร็ว
ความไม่พึงพอใจ	การปรับปรุงระบบงานอาจต้องใช้งบประมาณจำนวนมากในการแก้ไขและปิดช่องโหว่ต่าง ๆ
ข้อเสนอแนะจากผู้มีส่วนได้ส่วนเสีย	1. การพัฒนาระบบงานให้เน้นที่ความมั่นคงปลอดภัยและประสิทธิภาพ 2. การพัฒนาทักษะบุคลากรและผู้ที่มีส่วนเกี่ยวข้องให้มีความตระหนักและการระมัดระวังต่อการละเมิดความปลอดภัยทางไซเบอร์ 3. ส่งเสริมและสนับสนุนให้ผู้ปฏิบัติงานมีเข้าใจเกี่ยวกับมาตรการป้องกันการโจมตีทางไซเบอร์

จากการวิเคราะห์สถานการณ์และผลการดำเนินงานเพื่อปิด GAP Analysis ให้บรรลุเป้าหมายของหน่วยงาน ดังนี้

1. ยกระดับมาตรฐานความมั่นคงปลอดภัยไซเบอร์ตามเกณฑ์ CTAM และ Smart Hospital
    - ยกระดับมาตรฐานความปลอดภัยให้ครบทุกหน่วย
    - ขยายการควบคุมการเข้าถึง ระบบสำรองข้อมูล เครือข่าย และอุปกรณ์คอมพิวเตอร์
    - ทำให้การประเมินเป็นวงรอบสม่ำเสมอทั้งองค์กร
2. เสริมมาตรการเฝ้าระวังและลดความเสี่ยงจากภัยคุกคามเชิงรุก
    - เพิ่มความสามารถในการตรวจจับเหตุการณ์ผิดปกติ (Detection)
    - ใช้ระบบเฝ้าระวังภัยไซเบอร์ที่ครอบคลุมมากขึ้น
    - ลดจำนวนเหตุการณ์ละเมิดให้เป็นไปตามเป้าหมาย 50% อย่างต่อเนื่อง
    - เชื่อมโยงข้อมูลความเสี่ยงกับการวางแผนเชิงรุก
3. พัฒนาศักยภาพบุคลากรและความตระหนักด้านความปลอดภัยข้อมูล
    - เพิ่มการอบรมเชิงลึกด้าน Incident Response, PDPA, และภัยคุกคามใหม่
    - สร้างช่องทางสื่อสารความรู้ด้านไซเบอร์ให้เข้าถึงง่าย
    - ลดช่องว่างความรู้ระหว่างเจ้าหน้าที่ส่วนกลางและส่วนภูมิภาค
    - เพิ่มกิจกรรมสร้างความตระหนัก เช่น คู่มือ, Infographic, การแจ้งเตือน