รายงานผลการประเมินสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประจำปีงบประมาณ พ.ศ. 2566

ส่วนที่ 1 ข้อมูลพื้นฐาน

1.1 วัตถุประสงค์การจัดตั้ง ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.1.1 เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

1.1.2 จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อ กกม. เพื่อให้ความเห็นชอบ

1.1.3 ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

1.1.4 ประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

1.1.5 ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับมอบหมายจากคณะกรรมการ

1.1.6 เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

1.1.7 ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือหน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ หรือตามคำสั่งของคณะกรรมการ

1.1.8 ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

1.1.9 เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน

1.1.10 เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน

1.1.11 เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชนทั้งในประเทศและต่างประเทศ

1.1.12 ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจากคณะกรรมการ

1.1.13 ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ

1.1.14 ส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

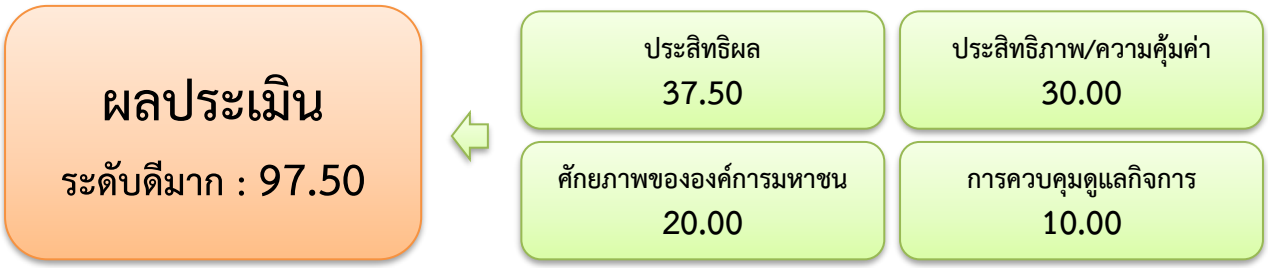
1.1.15 รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ รวมทั้ง ปัญหาและอุปสรรค เสนอต่อคณะกรรมการเพื่อพิจารณาดำเนินการ

1.2 วิสัยทัศน์ เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีประสิทธิภาพพร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ

1.3 งบประมาณและอัตรากำลัง

งบประมาณ	318.59 ล้านบาท
อัตรากำลัง	51 คน

ส่วนที่ 2 สรุปผลการประเมิน



ผลการประเมินของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประจำปีงบประมาณ พ.ศ. 2566 อยู่ในระดับดีมาก เท่ากับ 97.50 คะแนน สูงกว่าปีที่ผ่านมา (ปี 2565 = 91.83 คะแนน) เนื่องจากผลคะแนนในองค์ประกอบที่ 2 ประสิทธิภาพและความคุ้มค่าในการดำเนินงาน องค์ประกอบที่ 3 ศักยภาพขององค์การมหาชน และองค์ประกอบที่ 4 การควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน มีผลคะแนนเพิ่มขึ้นเมื่อเทียบกับปีที่ผ่านมา รวมทั้งสามารถบรรลุเป้าหมายทุกตัวชี้วัดในทั้งสามองค์ประกอบ รายละเอียดปรากฏตามเอกสารแนบ

ส่วนที่ 3 สรุปผลงานสำคัญ

3.1 ผลงานสำคัญของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

3.1.1 **ปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์** จำนวน 1,823 เหตุการณ์ เช่น การ Hacked Website หน่วยงานเฝ้าระวังและแจ้งเตือนภัยคุกคามให้กับหน่วยงานต่าง ๆ และประชาชน รวมทั้งให้ความช่วยเหลือหน่วยงานที่ถูกโจมตีทางไซเบอร์

3.1.2 **รายงานการปฏิบัติการความมั่นคงปลอดภัยไซเบอร์** จำนวน 365 ฉบับ ประกอบด้วยผลสรุปการสืบสวนวิเคราะห์ (Investigation) และการตรวจจับภัยคุกคามเชิงรุก (Threat Hunting) ผลสรุปการสืบสวนตรวจพิสูจน์หลักฐาน (Digital Forensic) และการทำวิศวกรรมย้อนกลับ (reverse engineering) ผลสรุปการตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบเพื่อทดสอบความปลอดภัย (Penetration Testing) และผลการดำเนินงานที่สำคัญอื่นๆ

3.1.3 **ฝึกและทดสอบแผนเผชิญเหตุการณ์เกิดเหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤติระดับประเทศ** ให้กับหน่วยงานต่าง ๆ เช่น หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวม 153 หน่วยงาน และสร้างความตระหนักรู้ให้กับประชาชนและพัฒนาบุคลากรมากกว่า 190,000 คน จากกิจกรรมต่าง ๆ เช่น NCSA Cyber Security Knowledge Sharing การแข่งขันทักษะทางไซเบอร์ Thailand Cyber Top Talent

3.1.4 **สร้างเครือข่ายความร่วมมือพหุภาคี** (Multilateral) จำนวน 6 กรอบความร่วมมือ และความร่วมมือทวิภาคี (Bilateral) จำนวน 13 ประเทศ สร้างเครือข่ายและช่องทางในการแจ้งเตือนภัยคุกคามทางไซเบอร์กับหน่วยงานปกครองส่วนท้องถิ่นทุกภูมิภาค เชื่อมต่อระบบแพลตฟอร์มสำหรับการรับและแบ่งปันเหตุการณ์ภัยคุกคามทางไซเบอร์กับ 10 หน่วยงาน ติดตั้งพัฒนาแพลตฟอร์มรักษาความปลอดภัยทางไซเบอร์เพื่อรับมือเหตุฉุกเฉินทางคอมพิวเตอร์สำหรับ Sectoral CERT ของหน่วยงานด้านสาธารณสุข จำนวน 15 โรงพยาบาล

3.2 ความสำคัญในการขับเคลื่อนการพัฒนาประเทศ

สกมช. มีภารกิจเสนอแนะนโยบาย ยุทธศาสตร์ และปรับปรุงกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กำกับดูแล เฝ้าระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือนและปฏิบัติการเพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ปกป้องระบบสารสนเทศที่สำคัญของประเทศไม่ให้เกิดความเสียหายจากการโจมตีทางดิจิทัลที่อาจมีผลกระทบทางกายภาพและเศรษฐกิจ เผยแพร่ความรู้ความเข้าใจ เสริมสร้างความตระหนักและสนับสนุนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการตรวจแก้ไขปัญหาเมื่อเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์เพื่อลดผลกระทบต่อประชาชนและระบบสารสนเทศของประเทศ รวมถึงสร้างความร่วมมือทางระหว่างประเทศเพื่อป้องกันและต่อต้านการกระทำทางไซเบอร์ที่อาจก่อให้เกิดความเสียหายต่อสันติภาพและความมั่นคงปลอดภัยทางไซเบอร์ในระดับนานาชาติ

ตารางสรุปผลการประเมินสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประจำปีงบประมาณ พ.ศ. 2566

ตัวชี้วัด	น้ำหนัก (ร้อยละ)	เกณฑ์การประเมิน/ค่าเป้าหมาย			ผลการดำเนินงาน		
		ขั้นต้น (50)	มาตรฐาน (75)	ขั้นสูง (100)	ผลการดำเนินงาน	คะแนนที่ได้	คะแนนถ่วงน้ำหนัก
องค์ประกอบที่ 1 ประสิทธิผลการดำเนินงาน (ร้อยละ 40)							
1.1 ความสำเร็จของการเผยแพร่และสร้างความเข้าใจในนโยบาย กฎระเบียบที่เกี่ยวข้องและการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	8	มีช่องทางการสื่อสาร 1 ช่องทาง และมีผู้เข้าร่วมไม่น้อยกว่า 9,000 คน	มีช่องทางการสื่อสาร 2 ช่องทาง และมีผู้เข้าร่วมไม่น้อยกว่า 10,000 คน	มีช่องทางการสื่อสาร 3 ช่องทางและมีผู้เข้าร่วมมากกว่า 10,000 คน	มีช่องทางการสื่อสาร 3 ช่องทางและมีผู้เข้าร่วม รวม 22,540 คน	100	8
1.2 ความสำเร็จของการสร้างเครือข่ายความร่วมมือด้านการวิจัยและด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศหรือระหว่างประเทศ	6	มีจำนวนกิจกรรมของการสร้างเครือข่ายความร่วมมือด้านการวิจัยและด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศหรือระหว่างประเทศ จำนวนไม่น้อยกว่า 150 ครั้ง	มีจำนวนกิจกรรมของการสร้างเครือข่ายความร่วมมือด้านการวิจัยและด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศหรือระหว่างประเทศ จำนวนไม่น้อยกว่า 200 ครั้ง	มีจำนวนกิจกรรมของการสร้างเครือข่ายความร่วมมือด้านการวิจัยและด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศหรือระหว่างประเทศ จำนวนไม่น้อยกว่า 250 ครั้ง	มีการจัดกิจกรรมเพื่อการวิจัย/สร้างเครือข่ายทั้งใน/ต่างประเทศรวม 219 ครั้ง	75	4.5
1.3 ร้อยละความสำเร็จการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (National CERT)	4	มีจำนวนหน่วยงานเป้าหมายที่ NCERT มีขีดความในการเฝ้าระวังและให้ความช่วยเหลือสนับสนุนการตอบสนองและรับมือภัยคุกคามทางไซเบอร์ในห้วงเวลาเดียวกัน 6 หน่วยงาน	มีจำนวนหน่วยงานเป้าหมายที่ NCERT มีขีดความในการเฝ้าระวังและให้ความช่วยเหลือสนับสนุนการตอบสนองและรับมือภัยคุกคามทางไซเบอร์ในห้วงเวลาเดียวกัน 12 หน่วยงาน	มีจำนวนหน่วยงานเป้าหมายที่ NCERT มีขีดความในการเฝ้าระวังและให้ความช่วยเหลือสนับสนุนการตอบสนองและรับมือภัยคุกคามทางไซเบอร์ในห้วงเวลาเดียวกัน มากกว่า 12 หน่วยงาน	มีจำนวนหน่วยงานเป้าหมายที่ NCERT มีขีดความในการเฝ้าระวังและให้ความช่วยเหลือสนับสนุนการตอบสนองและรับมือภัยคุกคามทางไซเบอร์ในห้วงเวลาเดียวกันจำนวน 24 หน่วยงาน	100	4
1.4 ร้อยละความสำเร็จการปฏิบัติการการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Lab)	4	จำนวนเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ NCERT มีขีดความสามารถในการปฏิบัติการทางไซเบอร์ในรอบปี 24 เหตุการณ์	จำนวนเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ NCERT มีขีดความสามารถในการปฏิบัติการทางไซเบอร์ในรอบปี 36 เหตุการณ์	มีจำนวนเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ NCERT มีขีดความสามารถในการปฏิบัติการทางไซเบอร์ มากกว่า 36 เหตุการณ์	จำนวนเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ NCERT มีขีดความสามารถในการปฏิบัติการทางไซเบอร์ในรอบปี จำนวน 115 เหตุการณ์	100	4

ตัวชี้วัด	น้ำหนัก (ร้อยละ)	เกณฑ์การประเมิน/ค่าเป้าหมาย			ผลการดำเนินงาน		
		ขั้นต้น (50)	มาตรฐาน (75)	ขั้นสูง (100)	ผลการดำเนินงาน	คะแนนที่ได้	คะแนนถ่วงน้ำหนัก
1.5 ร้อยละความสำเร็จในการช่วยเหลือ (Help Desk) ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	4	สามารถดำเนินการแก้ไขปัญหาจากการรับแจ้งเหตุภัยคุกคามได้ร้อยละ 25 ของจำนวนที่ได้รับแจ้ง	สามารถดำเนินการแก้ไขปัญหาจากการรับแจ้งเหตุภัยคุกคามได้ ร้อยละ 30 ของจำนวนที่ได้รับแจ้ง	สามารถดำเนินการแก้ไขปัญหาจากการรับแจ้งเหตุภัยคุกคามได้ร้อยละ 50 ของจำนวนที่ได้รับแจ้ง	มีจำนวนที่ได้รับแจ้ง 396 เรื่อง โดยมีการให้คำแนะ ช่วยตรวจสอบและดำเนินการตามที่ได้รับแจ้งแล้วจำนวนร้อยละ 71.20	100	4
1.6 ร้อยละความสำเร็จในการปฏิบัติการร่วมทางไซเบอร์ (NCSA War room)	4	ร้อยละ 25	ร้อยละ 30	มากกว่าร้อยละ 30	มากกว่าร้อยละ 30	100	4
1.7 ความสำเร็จในการยกระดับหรือพัฒนาขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานสากล	10	มีหลักสูตรการพัฒนาขีดความสามารถกระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากล	มีหลักสูตรการพัฒนาขีดความสามารถกระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากล และมีผู้ผ่านการอบรมจำนวนไม่น้อยกว่า 100 คน	มีหลักสูตรการพัฒนาขีดความสามารถกระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากล และมีผู้ผ่านการอบรมจำนวนไม่น้อยกว่า 200 คน และมีการจัดทำแนวทางการดำเนินการ Cybersecurity Self-Assessment และคู่มือจำนวน ๑ ฉบับ	• จำนวนผู้ผ่านการอบรมในแต่ละหลักสูตรไม่ครบ 200 คนได้แก่ -หลักสูตรผู้นำการปฏิบัติ (Lead Implementer) จำนวน 163 คน -หลักสูตรผู้นำการตรวจสอบ (Lead Auditor) จำนวน 156 คน • มีแนวทางการดำเนินการ Cybersecurity Self-Assessment สำหรับหน่วยงานรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (จำนวน 3 ฉบับ)	90	9
องค์ประกอบที่ 2 ประสิทธิภาพและความคุ้มค่าในการดำเนินงาน (ร้อยละ 30)							
2.1 ความสำเร็จในการจัดการฝึกและทดสอบแผนเผชิญเหตุในกรณีเกิดเหตุภัยคุกคามทาง ไซเบอร์ในระดับวิกฤติ	15	มีจำนวน 40 หน่วยงานเป้าหมายที่เข้าร่วมการฝึกและมีผู้เข้าร่วมฝึกและทดสอบแผนเผชิญเหตุอย่างน้อย 100 คน	มีจำนวน 50 หน่วยงานเป้าหมายที่เข้าร่วมการฝึกและมีผู้เข้าร่วมฝึกและทดสอบแผนเผชิญเหตุไม่น้อยกว่า 200 คน	มีจำนวน 60 หน่วยงานเป้าหมายที่เข้าร่วมการฝึกและมีผู้เข้าร่วมฝึกและทดสอบแผนเผชิญเหตุไม่น้อยกว่า 300 คน	มีจำนวน 153 หน่วยงานเป้าหมายที่เข้าร่วมการฝึกและมีผู้เข้าร่วมฝึกและทดสอบแผนเผชิญเหตุจำนวน 515 คน	100	15
2.2 ความสำเร็จในการจัดทำแผนเผชิญเหตุด้านไซเบอร์ของหน่วยงานภาครัฐ และหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ	15	มีจำนวน 30 หน่วยงานเป้าหมายมีแผนเผชิญเหตุด้านไซเบอร์ที่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน	มีจำนวน 40 หน่วยงานเป้าหมายมีแผนเผชิญเหตุด้านไซเบอร์ที่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน	มีจำนวน 50 หน่วยงานเป้าหมายมีแผนเผชิญเหตุด้านไซเบอร์ที่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน	มีจำนวน 50 หน่วยงานเป้าหมาย มีแผนเผชิญเหตุด้านไซเบอร์ที่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน	100	15

ตัวชี้วัด	น้ำหนัก (ร้อยละ)	เกณฑ์การประเมิน/ค่าเป้าหมาย			ผลการดำเนินงาน		
		ขั้นต้น (50)	มาตรฐาน (75)	ขั้นสูง (100)	ผลการดำเนินงาน	คะแนนที่ได้	คะแนนถ่วงน้ำหนัก
องค์ประกอบที่ 3 ศักยภาพขององค์การมหาชน (ร้อยละ 20)							
3.1 การพัฒนาองค์การสู่ดิจิทัล การพัฒนาระบบบัญชีข้อมูล (Data Catalog) เพื่อนำไปสู่การเปิดเผยข้อมูลภาครัฐ (Open Data)	10	- มีรายชื่อชุดข้อมูลที่มีคุณค่าสามารถนำไปใช้ตอบโจทย์การพัฒนาประเทศหรือการบริการประชาชน - มีคำอธิบายชุดข้อมูล (Metadata) ที่สอดคล้องตามมาตรฐานที่ สพร. กำหนด (14 รายการ) ของทุกชุดข้อมูล - มีคำอธิบายทรัพยากรข้อมูล (Resource) ของชุดข้อมูลเปิดทั้งหมด	- มีระบบบัญชีข้อมูลหน่วยงาน (Agency Data Catalog) พร้อมแจ้ง URL ระบบบัญชีข้อมูลหน่วยงาน และชุดข้อมูลคำอธิบายชุดข้อมูล ถูกนำขึ้นที่ระบบบัญชีข้อมูลหน่วยงาน และระบุทรัพยากรข้อมูล (Resource) ของชุดข้อมูลเปิดทั้งหมด (15 คะแนน) - ชุดข้อมูลเปิดทั้งหมด ถูกนำมาลงทะเบียนในระบบบัญชีข้อมูลภาครัฐ (GD Catalog) (10 คะแนน)	คุณภาพทุกชุดข้อมูลเป็นไปตามมาตรฐานคุณลักษณะแบบเปิดที่ สพร. กำหนด (20 คะแนน) - นำข้อมูลเปิดไปใช้ประโยชน์ได้อย่างเป็นรูปธรรมตอบโจทย์ตามประเด็นขอบเขตการนำข้อมูลไปใช้ประโยชน์ อย่างน้อย 1 ชุดข้อมูล (5 คะแนน)	100	100	10
3.2 การประเมินสถานะของหน่วยงานภาครัฐในการเป็นระบบราชการ 4.0 (PMQA 4.0)	10	350 คะแนน	400 คะแนน	450 คะแนน	457.53 คะแนน	100	10
องค์ประกอบที่ 4 การควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน (ร้อยละ 10)							
4.1 ร้อยละความสำเร็จของการพัฒนาด้านการควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน	10	50 คะแนน	75 คะแนน	100 คะแนน	100 คะแนน	100	10
						คะแนนรวม	**97.50**
						สรุปผลการประเมินระดับองค์กร	**ดีมาก**

สรุปผลการประเมินระดับองค์กร

ระดับดีมาก หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 90 - 100 คะแนน
ระดับดี หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 75 – 89.99 คะแนน
ระดับพอใช้ หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 60 – 74.99 คะแนน
ระดับต้องปรับปรุง หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ต่ำกว่า 60 คะแนน