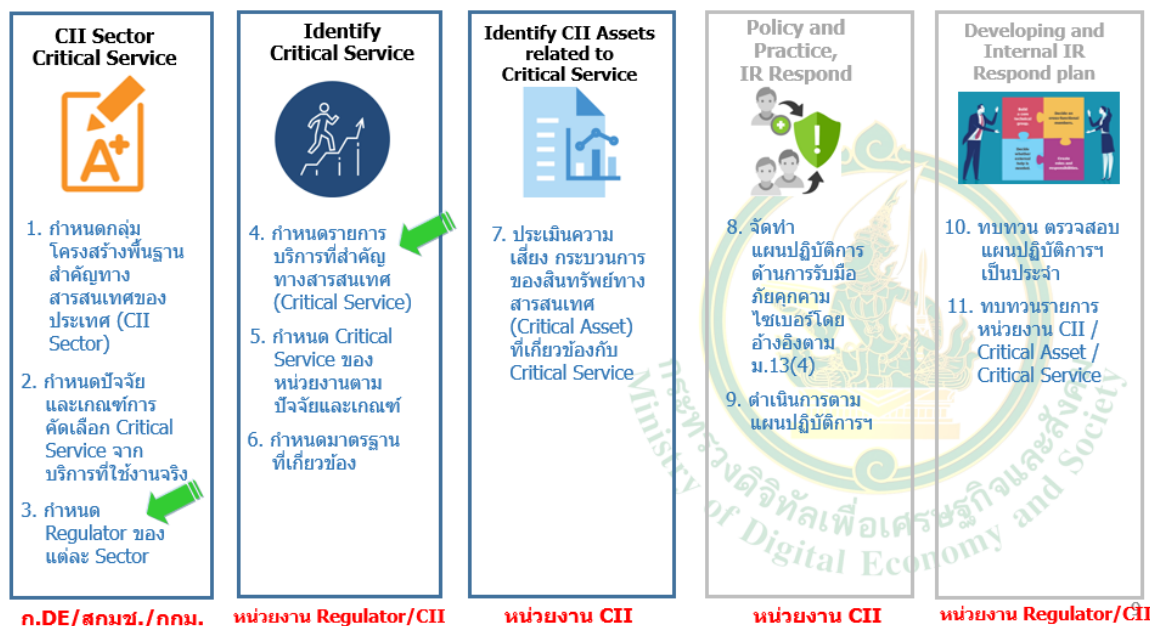


แนวทางกำหนดหลักเกณฑ์บริการที่จัดเป็น Critical Services สำหรับหน่วยงานควบคุมกำกับหรือดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลใช้บังคับ และคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ได้มีการประชุมครั้งที่ 1/2563 เมื่อวันที่ 13 มกราคม 2563 ขณะนี้อยู่ระหว่างสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จัดเตรียมแนวทางการกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งเป็นการดำเนินการตามมาตรา 13 (4) และ (5)

ภาพรวมการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เฉพาะที่เกี่ยวข้องกับแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ แบ่งออกเป็น 11 ขั้นตอน ดังนี้

ภาพรวมการดำเนินการ



ภาพที่ 1 ขั้นตอนการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การกำหนดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure Sector) ซึ่งกฎหมายได้ระบุไว้ 7 ด้าน ความในมาตรา 49 ได้กำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้แก่

ประเภทหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

Critical Information Infrastructure : CII



ภาพที่ 2 ประเภทหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

สำหรับหลักเกณฑ์การคัดเลือกบริการที่สำคัญ (Critical Services) ในเบื้องต้นจะพิจารณาจาก

- (1) ขอบเขตของผลกระทบ
- (2) ผลกระทบหรือความรุนแรงที่ตามมา
- (3) ระยะเวลาที่กระทบต่อการให้บริการ

ทั้งนี้การประเมินผลความสำคัญ ควรกำหนดเกณฑ์ความวิกฤตเพื่อระบุสินทรัพย์ที่สำคัญและตรวจสอบระบบทั้งหมด โดยควรพิจารณาอย่างน้อยสี่ประเด็นได้แก่

- 1 การพึ่งพาซึ่งกันและกันภายในด้านหรือ Sector เดียวกัน
- 2 การพึ่งพาซึ่งกันและกันระหว่าง Sector
- 3 การเชื่อมโยงระหว่างสินทรัพย์ของเครือข่ายการสื่อสาร
- 4 กรณีระดับประเทศหรือข้ามพรมแดน

ภาพที่ 3 ประเด็นพิจารณาเกณฑ์ความวิกฤต

จากข้างต้น สกมช. ได้นำเสนอปัจจัยในการพิจารณาคัดเลือกบริการที่สำคัญจำนวน 9 ปัจจัย พร้อมทั้งเกณฑ์การคัดเลือก (Threshold) เฉพาะผลกระทบระดับสูง ดังนี้

ปัจจัย	ผลกระทบระดับต่ำ	ผลกระทบระดับกลาง	ผลกระทบระดับสูง	ผลการประเมิน
1. ผลกระทบต่อประชาชน	ไม่มีผู้ใช้บริการได้รับผลกระทบต่อชีวิตร่างกายหรืออนามัย	ผู้ใช้บริการได้รับผลกระทบต่อร่างกายหรืออนามัย > 1 คน ≤ 1,000 คน	ผู้ใช้บริการได้รับผลกระทบต่อร่างกายหรืออนามัย > 1,000 คน หรือต่อชีวิตตั้งแต่ 1 คน	ร้ายแรง
2. ผลกระทบเชิงความหนาแน่นของประชากร	กระทบต่อชีวิตหรือการปฏิบัติงานของประชาชน < 10% ของประชากรในพื้นที่ระดับจังหวัดหรือเขตบริหาร	กระทบต่อชีวิตหรือการปฏิบัติงานของประชาชน 10% ≤ X ≤ 30% ของประชากรในพื้นที่ระดับจังหวัดหรือเขตบริหาร	กระทบต่อชีวิตหรือการปฏิบัติงานของประชาชน > 30% ของประชากรในพื้นที่ระดับจังหวัดหรือเขตบริหาร	ร้ายแรง
3. ผลกระทบด้านเศรษฐกิจ	≤ 1 ล้านบาท	> 1 ล้านบาท ≤ 100 ล้านบาท	> 100 ล้านบาท	ร้ายแรง
4. ผลกระทบต่อความเชื่อมั่นขององค์กรหรือต่อประเทศ	ไม่มีผลกระทบต่อภาพลักษณ์ขององค์กรหรือต่อประเทศ	มีผลกระทบต่อภาพลักษณ์ในระดับกลาง	เกิดผลกระทบรุนแรงต่อภาพลักษณ์	ร้ายแรง
5. ผลกระทบด้านความสัมพันธ์ระหว่างประเทศ				ร้ายแรง
6. ผลกระทบต่อความสงบเรียบร้อยในสังคม			เกิดผลกระทบรุนแรงต่อความสงบเรียบร้อยในสังคม หรือเป็นภัยต่อความมั่นคงของชาติ	ร้ายแรง
7. ผลกระทบต่อการดำเนินชีวิตประจำวันของประชาชน	กระทบต่อการปฏิบัติงานของประชาชน < 10,000 ราย	กระทบต่อการปฏิบัติงานของประชาชน 10,000 ≤ X ≤ 100,000 ราย	กระทบต่อการปฏิบัติงานของประชาชน > 100,000 ราย	ร้ายแรง
8. ผลกระทบต่อ CII อื่น หรือ Sector อื่น	< 3 บริการ	= 3	> 3 บริการ	ร้ายแรง
9. ผลกระทบต่อสิ่งแวดล้อม	ไม่รุนแรง	รุนแรงปานกลาง	รุนแรงมาก	ร้ายแรง

หมายเหตุ ข้อมูลเกณฑ์การคัดเลือก (Threshold) ในตารางข้างต้น เป็นตัวอย่างเบื้องต้น