ธนาคารแห่งประเทศไทย
BANK OF THAILAND

การดำเนินการตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

วันที่ 23 พฤศจิกายน 2565

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

Agenda

- พ.ร.บ. ไซเบอร์ และกฎหมายรอง (บางส่วน)
- ประกาศ สกมช. ที่เกี่ยวข้องกับการตรวจสอบด้าน Cyber
- ประกาศ สกมช. ที่เกี่ยวข้องกับการประเมินความเสี่ยงด้าน Cyber
- ประกาศ สกมช. ที่เกี่ยวข้องกับการแผนการรับมือภัยคุกคาม Cyber
- การดำเนินการในระยะถัดไป

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

พ.ร.บ. ไซเบอร์ และกฎหมายรอง (บางส่วน)

พรบ. ไซเบอร์ — เริ่ม 28 พ.ค. 62

มาตรา 44: Gov, Reg, CII จัดทำประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของตน ให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา 54: CII ต้องทำการ audit, ประเมิน risk อย่างน้อยปีละหนึ่งครั้ง และส่งรายงานสรุป

ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน — เริ่ม 9 ก.ย. 65

คำแนะนำแนวทางปฏิบัติการประเมิน risk และ audit — ก.ค. 65

ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน	พ.ร.บ. ไซเบอร์	
	มาตรา 44 (9 ก.ย. 65)	มาตรา 54
1. ประมวลแนวทางปฏิบัติ • แผนการตรวจสอบด้าน Cyber • แผนการประเมินความเสี่ยงด้าน Cyber • แผนการรับมือภัยคุกคาม Cyber	✓	จัดให้มีการ audit และประเมิน risk ปีละครั้ง และส่งผลสรุปรายงาน สกมช. ภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ ทั้งนี้ไม่เกิน 30 ม.ค.
2. กรอบมาตรฐาน 5 ด้าน 1. Identify 2. Protect 3. Detect 4. Response 5. Recovery	✓	

ประกาศ สกมช. ที่เกี่ยวข้องกับการตรวจสอบด้าน Cyber

เพิ่มเลขหนังสือ

ประกาศ ประมวลแนวทางปฏิบัติ และกรอบมาตรฐาน

ข้อ 17. แผนการตรวจสอบด้าน Cyber

17.1 ต้องจัดให้มีการตรวจสอบด้าน Cybersecurity โดย Internal หรือ External Audit อย่างน้อยปีละ 1 ครั้ง โดยมีขอบเขต ดังนี้

(ก) Business Impact Analysis: BIA

(ข) Critical Service ตามผลการวิเคราะห์ในข้อ (ก)

(ค) การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้อง

17.2 CII จัดส่งผลสรุปรายงานการตรวจสอบ ต่อสำนักงานภายในกำหนด 30 วัน นับแต่วันที่ดำเนินการแล้วเสร็จ พร้อมทั้งส่งสำเนาให้ Regulator

17.3 ส่งแผนการดำเนินการแก้ไขไปยังสำนักงานภายในกำหนด 30 วันนับแต่จากวันที่ได้รับรายงานการตรวจสอบ โดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดการดำเนินการแก้ไข และ กำหนดระยะเวลาดำเนินการ

17.4 ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้ CII ดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงานภายในระยะเวลาที่ กกม. กำหนด พร้อมส่งทั้งสำเนาให้ Regulator ด้วย

17.5 เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม. CII จะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้

คำแนะนำ แนวทางปฏิบัติการตรวจสอบ

หลักการ

- แนวทางปฏิบัติการตรวจสอบ ของ สกมช. ประยุกต์มาจาก NIST Special Publication 800-53A Rev.5 Assessing Security and Privacy Controls in Information Systems and Organizations
- CII อาจพิจารณาใช้หลักการตรวจสอบอื่นในลักษณะเดียวกับได้ เช่น NIST Special Publication 800-53A Rev.5, ISO 19011, ISO/IEC 27000 series โดยให้มีรายละเอียดครอบคลุมข้อ 17.1 ในประมวลฯ
- Audit Plan เป็น Annual Audit Plan หรือ Multi-year Audit Plan และตรวจตามระดับความเสี่ยง (Risk-based Audit Plan)

รูปแบบรายงาน

- หากหน่วยงานยังไม่มีแบบฟอร์มรายงาน อาจจัดทำแบบฟอร์มร่วมกับ Regulator หรือทำตาม Appendix E ของ NIST SP 800-53A Rev.5 โดยให้มีรายละเอียดครบถ้วนตามข้อ 17 ในประมวลฯ
- ควรจัดทำเป็นผลสรุปรายงานแยกจากรายงานฉบับเต็ม

ผู้ประเมิน มีความรู้ความเข้าใจด้านการตรวจสอบด้าน Cyber

ประกาศ สกมช. ที่เกี่ยวข้องกับการประเมินความเสี่ยงด้าน Cyber

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ประกาศ ประมวลแนวทางปฏิบัติ และกรอบมาตรฐาน

ข้อ 18. การประเมินความเสี่ยงด้าน Cyber

- กำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- จัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- จัดให้มีการประเมินความเสี่ยง อย่างน้อยปีละ 1 ครั้ง โดยต้องประกอบด้วยรายละเอียดอย่างน้อย ดังนี้

18.1 การประเมินความเสี่ยง (Risk Assessment)

ก) Risk Identification

ข) Risk Analysis

ค) Risk Evaluation

18.2 การจัดการความเสี่ยง (Risk Treatment) และกำหนด KRI ด้าน Cyber

18.3 การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

18.4 การรายงานความเสี่ยง (Risk Reporting)

คำแนะนำ แนวทางปฏิบัติการประเมินความเสี่ยง

หลักการ

- แนวทางประเมินความเสี่ยงของ สกมช. ประยุกต์มาจาก NIST 800-30 Rev1 Guide for Conducting Risk Assessments
- CII อาจพิจารณาใช้หลักการประเมินความเสี่ยงอื่นในลักษณะเดียวกับได้ เช่น NIST 800-30 Rev1, ISO/IEC 27001, COBIT, CIS CSC, ISA/IEC 62443 โดยให้มีรายละเอียดครอบคลุมข้อ 18 ในประมวลฯ

รูปแบบรายงาน

- หากหน่วยงานยังไม่มีแบบฟอร์มรายงาน อาจจัดทำแบบฟอร์มร่วมกับ Regulator หรือทำตาม NIST SP 800-30 Rev.1 โดยให้มีรายละเอียดครบถ้วนตามข้อ 18.1 ในประมวลฯ
- ควรจัดทำเป็นผลสรุปรายงานแยกจากรายงานฉบับเต็ม

ผู้ประเมิน มีความรู้ความเข้าใจด้านการประเมินความเสี่ยงด้าน Cyber และไม่ใช่เจ้าหน้าที่ 3rd Line

ประกาศ สกมช. ที่เกี่ยวข้องกับแผนการรับมือภัยคุกคาม Cyber

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ประกาศ ประมวลแนวทางปฏิบัติ และกรอบมาตรฐาน

ข้อ 19. แผนการรับมือภัยคุกคามทางไซเบอร์

19.1 จัดทำแผน Cybersecurity Incident Response Plan มีรายละเอียดอย่างน้อย ดังนี้

(ก) โครงสร้างทีม CIRT

(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(ง) ขั้นตอนจำกัดขอบเขต (Containment)

(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(ฉ) ขั้นตอนในการสอบสวน (Investigate)

(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence)

(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก

(ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process)

19.2 ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมด

19.3 ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง

19.4 ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์

การดำเนินการในระยะถัดไป

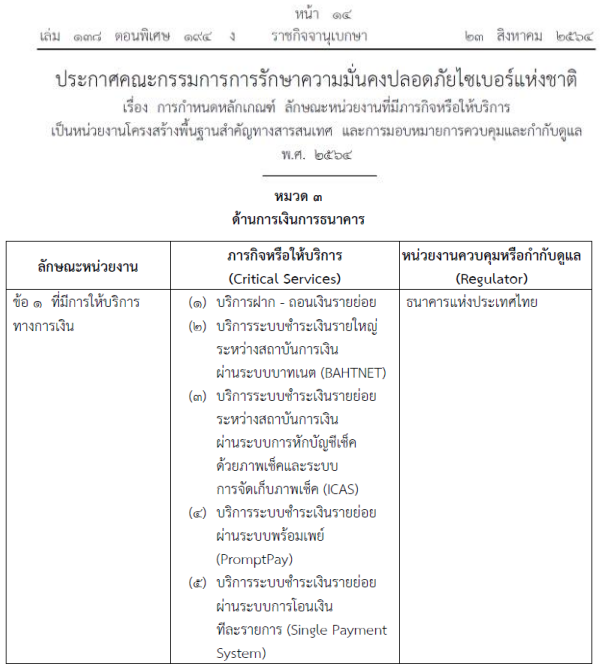
- การทบทวน Critical Services และ CII ในภาคธนาคาร

2562 พ.ร.บ. ไซเบอร์

มีผลบังคับใช้ 28 พ.ค. 62

2563 หารือ REG / CII

กระทรวง DE ทำหน้าที่ สกมช. หารือหน่วยงาน Regulator แต่ละ Sector พิจารณากำหนด CII



หน้า ๑๔
เล่ม ๑๓๘ ตอนพิเศษ ๑๙๔ ง ราชกิจจานุเบกษา ๒๓ สิงหาคม ๒๕๖๔

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ
เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล
พ.ศ. ๒๕๖๔

หมวด ๓
ด้านการเงินการธนาคาร

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
ข้อ ๑ ที่มีการให้บริการทางการเงิน	(๑) บริการฝาก - ถอนเงินรายย่อย (๒) บริการระบบชำระเงินรายใหญ่ระหว่างสถาบันการเงินผ่านระบบบาทเนต (BAHTNET) (๓) บริการระบบชำระเงินรายย่อยระหว่างสถาบันการเงินผ่านระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค (ICAS) (๔) บริการระบบชำระเงินรายย่อยผ่านระบบพร้อมเพย์ (PromptPay) (๕) บริการระบบชำระเงินรายย่อยผ่านระบบการโอนเงินทีละรายการ (Single Payment System)	ธนาคารแห่งประเทศไทย

2564 กฎหมายลูก

มค – กพ

- ยกร่าง ประกาศ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือบริการเป็น CII
- รับฟังความเห็นจากผู้ทรางคุณวุฒิ

มีค

- Focus Group

เมย

- นำเสนอ กมช. กกม.

สค

- มีผลบังคับใช้ 24 สค. 64

2565 ปรับปรุงประกาศ

สกมช. ปรับปรุงประกาศฯ

- รวบรวมข้อมูล
- ขอความเห็นจากหน่วยงาน Reg
- ยกร่าง
- Focus Group (กย.)
- ปรับปรุงร่าง
- ส่งร่างให้ Reg ยืนยัน
- Public hearing
- คณะอนุกรรมการด้าน กม.
- กมช.
- ลงประกาศในราชกิจจาฯ

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

Thank you