การประชุมแนวนโยบาย การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

วันที่ ๑๓ มีนาคม ๒๕๖๑ เวลา ๑๔.๓๐ - ๑๖.๓๐ น.

ณ ห้องประชุม Think Big ชั้น ๒๐ @ETDA

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ประเด็นซักซ้อมความเข้าใจ

๑. การทบทวนกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทย
๒. กรอบนโยบาย มาตรฐาน และแนวทางการประยุกต์ใช้งานที่จำเป็น
๓. แนวทางการทำ National Incident Flow (SOP) เพื่อทำงานร่วมกัน โดยเน้นรองรับเศรษฐกิจดิจิทัล

๑.การทบทวนกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทย

สถานการณ์ภัยคุกคามไซเบอร์ในต่างประเทศ

กลุ่มพลังงาน

- **มิถุนายน ๒๕๕๓ โรงไฟฟ้านิวเคลียร์อิหร่านถูกโจมตี**ด้วยมัลแวร์ Stuxnet ซึ่ง**ทำลายเครื่องจักร** “Centrifuges” ที่ใช้เพิ่มประสิทธิภาพของแร่ยูเรเนียม มากกว่า **๑,๐๐๐ เครื่อง** และแพร่กระจายไปยังคอมพิวเตอร์มากกว่า ๒๐๐,๐๐๐ เครื่อง
- **ธันวาคม ๒๕๕๘ เครือข่ายไฟฟ้ายูเครนถูกโจมตี** ประชาชนมากกว่า **๒๒๕,๕๐๐ คน ไม่มีไฟฟ้าใช้**เป็นเวลา ๑-๖ ชั่วโมง

กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม

- **กันยายน ๒๕๕๙** แฮกเกอร์ปล่อย **มัลแวร์ Mirai** ใช้ช่องโหว่ในอุปกรณ์ IoT **โจมตีเครื่องให้บริการชื่อโดเมน** ทำให้ไม่สามารถเข้าถึงเว็บไซต์ **กระทบผู้ใช้งานทั่วโลก**

กลุ่มการเงิน

- **กันยายน ๒๕๕๕ ปฏิบัติการ “Operation Ababil” สถาบันการเงินสำคัญของสหรัฐอเมริกา** เช่น New York Stock Exchange, J.P. Morgan Chase, Bank of America และอีกหลายแห่ง **ถูกโจมตี DDoS โดยกลุ่ม Qassam Cyber Fighters** ทำให้**การบริการเว็บไซต์หยุดชะงัก**
- **กุมภาพันธ์ ๒๕๕๙ ธนาคารกลางบังกลาเทศ** ถูกมิจฉาชีพลอบโอนเงิน **สูญ ๘๑ ล้านเหรียญสหรัฐฯ**

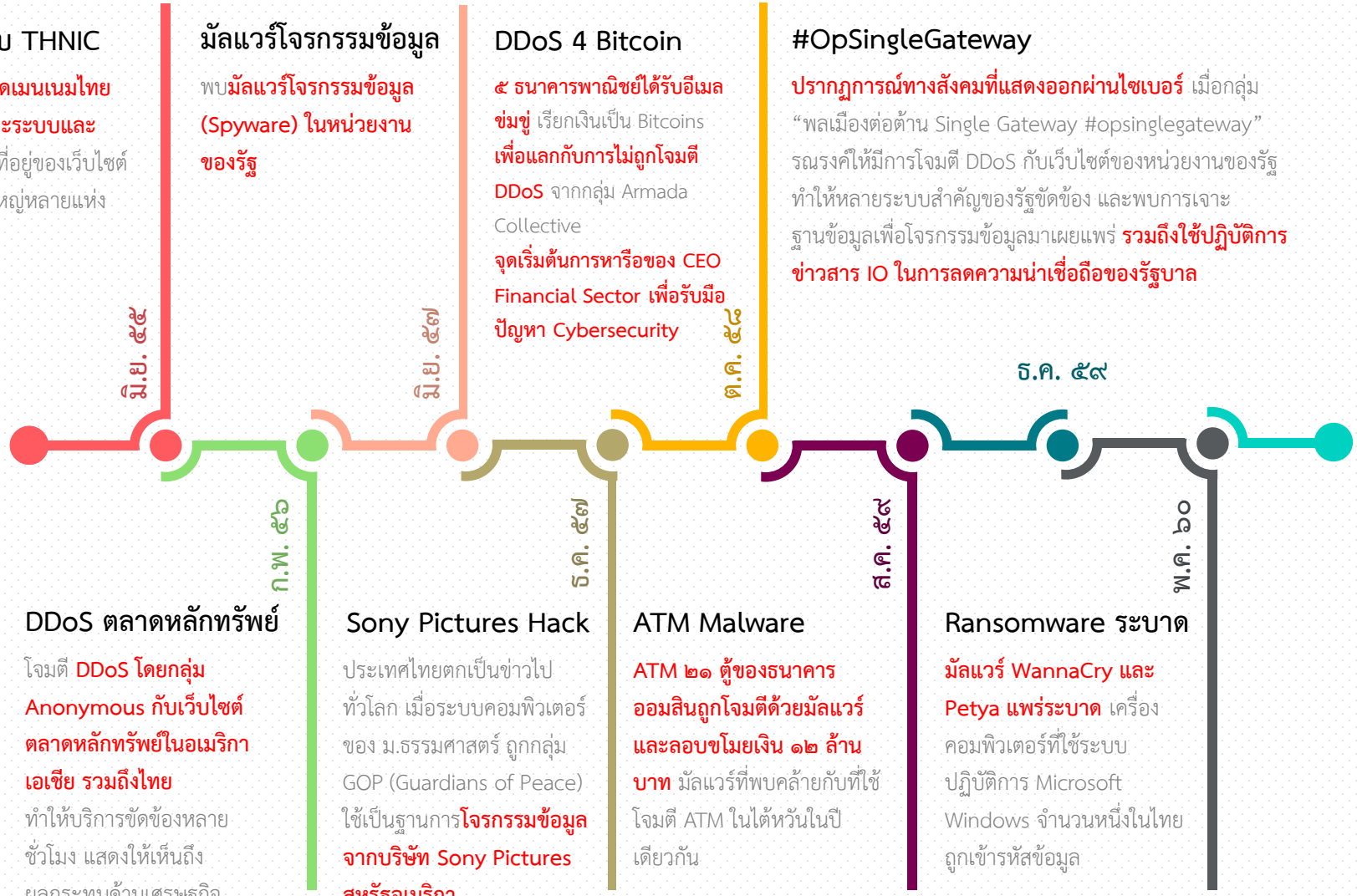
กลุ่มสาธารณสุข

- **พฤษภาคม ๒๕๖๐ มัลแวร์** WannaCry โจมตี**หน่วยงานสาธารณสุขของอังกฤษ ผู้ป่วยมากกว่า ๖,๙๐๐ ราย ไม่สามารถรับบริการ** และมัลแวร์แพร่กระจายไปมากกว่า ๑๕๐ ประเทศ

ข้อมูลส่วนบุคคล

- **กรกฎาคม ๒๕๖๐** บริษัท **Equifax ข้อมูลส่วนบุคคล**ของผู้บริโภคชาวสหรัฐฯ **รั่ว ๑๔๕.๕ ล้านคน**
- **พฤศจิกายน ๒๕๖๐** บริษัท **Uber ข้อมูลส่วนบุคคล**ของคนขับรถและผู้ใช้บริการ **รั่ว ๕๓ ล้านคน**

สถานการณ์ภัยคุกคามไซเบอร์ในประเทศไทย



คำอธิบายภัยคุกคามไซเบอร์ที่พบบ่อย

๑. Phishing

การหลอกให้เข้าเว็บไซต์ปลอมเพื่อลวงเอาข้อมูลที่สำคัญ เช่นการปลอมเว็บไซต์ธนาคารและส่งอีเมลแจ้งลูกค้าธนาคารให้เข้ามากรอกข้อมูล username และ password ที่เว็บปลอม และข้อมูลที่กรอกจะถูกส่งไปยังมิจฉาชีพ

๒. Data Breaches

การเจาะระบบและขโมยข้อมูลสำคัญออกไปขายหรือเผยแพร่ เช่น การนำข้อมูลส่วนบุคคลของลูกค้าไปขาย หรือการล้วงข้อมูลงานวิจัยเพื่อแข่งขันทางการค้าเป็นต้น

๓. Botnets

บ็อตเน็ตเป็นมัลแวร์ที่ฝังตัวอยู่ในเครื่องเหยื่อ และใช้เครื่องนั้นเป็นฐานโจมตีเป้าหมาย เช่น การฝังมัลแวร์ในกล้องเว็บแคม และสั่งให้เว็บแคมโจมตีเว็บไซต์เป้าหมาย

๔. Ransomware

แรนซัมแวร์เป็นมัลแวร์ที่เข้ารหัสลับข้อมูลในเครื่องเหยื่อ ทำให้ไม่สามารถเข้าถึงข้อมูลได้ และเรียกค่าไถ่จากเหยื่อเพื่อแลกกับการถอดรหัสลับ

๕. APT

Advanced Persistent Threat คือ การที่ผู้โจมตีฝังตัวอยู่ในระบบของเหยื่อเป็นเวลานานเพื่อเฝ้าดูพฤติกรรมและดักรับข้อมูล

ภูมิทัศน์ภัยคุกคามไซเบอร์

กลุ่มผู้ไม่หวังดี

HACKTIVISTS

- ต้องการแสดงออกทางการเมือง ทำลายชื่อเสียง เรียกร้องความสนใจเพื่อกดดันให้เกิดการเปลี่ยนแปลง

CRIMINALS

- การโกงผลประโยชน์ทางการเงิน การล่อลวง หรือหลอกลวงที่นำไปสู่การละเมิดผู้อื่น

INSIDERS

- การนำข้อมูลในหน่วยงานไปเผยแพร่ หรือการทำลายระบบเพื่อผลประโยชน์ทางการเงิน หรือการแก้แค้น

NATION STATES

- การจารกรรม บ่อนทำลาย หรือโจมตีผลประโยชน์ทางเศรษฐกิจ การเมือง หรือทางการทหาร

ประเภทภัยคุกคามไซเบอร์ที่พบบ่อย

- **DDoS**

Distributed Denial of Service เป็นการระดมการโจมตีเป้าหมายจากฐานการโจมตีจำนวนมาก ส่งผลให้เป้าหมายไม่สามารถให้บริการได้ตามปกติ

- **Defacement**

การลอบเจาะระบบเข้าไปเปลี่ยนหน้าเว็บไซต์ แสดงสัญลักษณ์ โอ้อวดความสามารถ หรือความเห็นทางการเมือง

- **Malware**

การหลอกให้ติดตั้ง หรือลอบฝังโปรแกรมในเครื่องของเหยื่อ เพื่อเรียกค่าไถ่ข้อมูล (Ransomware) หรือดักรับข้อมูล (Trojan) ฯลฯ

ผลกระทบ

- **ข้อมูล**ด้านเศรษฐกิจ หรือด้านความมั่นคงของชาติ **รั่วไหล**
- ประเทศ**สูญเสียความได้เปรียบ**ในการแข่งขัน
- ประเทศ**ถูกลดความน่าเชื่อถือ** ประชาชนสูญเสียความเชื่อมั่น
- การดำเนินงานขององค์กร หรือ CII **หยุดชะงัก**

ที่มา: https://www.csc.ncsu.edu/

Critical Infrastructures (CI) และ Critical Information Infrastructures (CII)
ความจำเป็นที่ต้องให้ความสำคัญและต้องทบทวน

“โครงสร้างพื้นฐานสำคัญของประเทศ” (Critical Infrastructure)

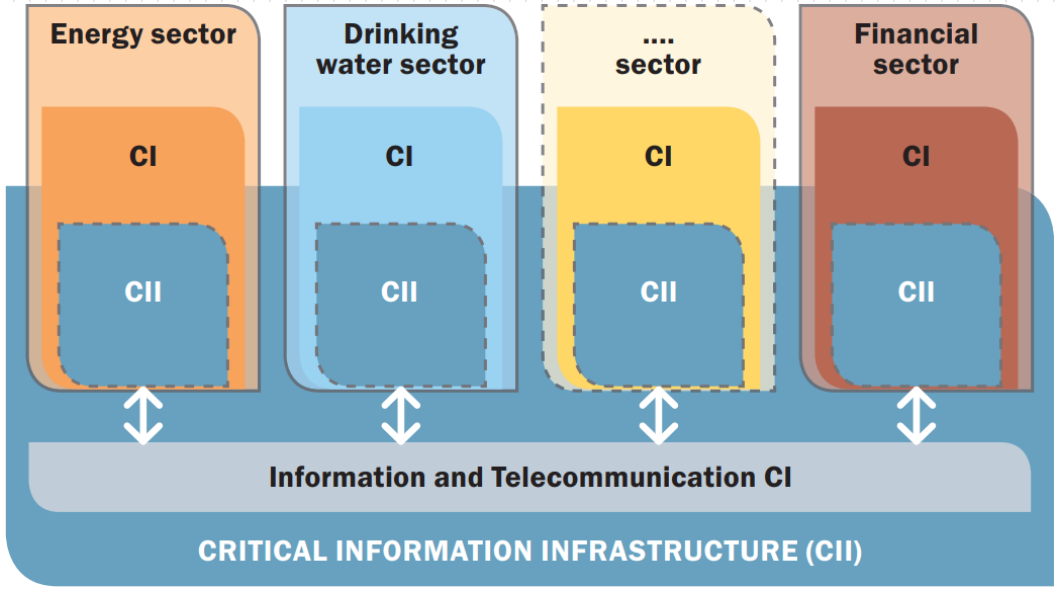
บรรดาหน่วยงานหรือองค์กร หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กร ซึ่งธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรนั้น มีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณชน

“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” (Critical Information Infrastructure)

ระบบสารสนเทศที่หน่วยงานซึ่งเป็นโครงสร้างพื้นฐานสำคัญของประเทศใช้ในการดำเนินงานและให้บริการ หากระบบถูกรบกวนจะทำให้ไม่สามารถดำเนินงานหรือให้บริการได้

Critical Infrastructures (CI): “Those infrastructures which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have serious consequences”

Critical Information Infrastructure (CII) : “Those interconnected information and communication infrastructures which are essential for the maintenance of vital societal functions, (health, safety, security, economic or social well-being of people) – the disruption or destruction of which would have serious consequence



ที่มา: https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

The Meridian Process aims to exchange ideas and initiate actions for the cooperation of governmental bodies on Critical Information Infrastructure Protection (CIIP) issues globally.

พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

การจัดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทย

๑๒๑ CI

๑๒๑ หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ

(ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์)

วิธีการแบบปลอดภัย

มาตรฐานการรักษาความมั่นคงปลอดภัยตามวิธีการแบบปลอดภัย

ความมั่นคงปลอดภัยทางกายภาพ

ความมั่นคงปลอดภัยของข้อมูล

- CII & Data Breaches
- Privacy
- Trade Secret
- Trust & Reliability

GDPR

ข้อพิจารณากลุ่ม CII

๑. ผลิตภัณฑ์มวลรวมภายในประเทศ (GDP)

๒. ระดับผลกระทบต่อด้านความมั่นคงของชาติ ด้านเศรษฐกิจและด้านสังคม

๓. ระดับการพึ่งพาเทคโนโลยีสารสนเทศ

๔. ศึกษาเปรียบเทียบกลุ่ม CII ในต่างประเทศ

Focus Groups

หน่วยงานกำกับดูแล

ส่วนราชการ

ภาคเอกชน

๖ กลุ่ม CII

กลุ่มความมั่นคงและบริการภาครัฐที่สำคัญ
หน่วยงานกำกับดูแล: ก.ดิจิทัลฯ และ ก.กลาโหม

กลุ่มการเงิน
หน่วยงานกำกับดูแล: ธปท. ก.ล.ต. และ คปภ.

กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม
หน่วยงานกำกับดูแล: กสทช.

กลุ่มการขนส่งและโลจิสติกส์
หน่วยงานกำกับดูแล: ก.คมนาคม

กลุ่มพลังงานและสาธารณูปโภค
หน่วยงานกำกับดูแล: ก.พลังงาน และ ก.มหาดไทย

กลุ่มสาธารณสุข
หน่วยงานกำกับดูแล: ก.สาธารณสุข

GDPR – The EU general Data Projection Regulation finally approved by the EU Parliament on 14 April 2016. *Enforcement date 25 May 2018*

๒. กรอบนโยบาย มาตรฐาน และแนวทางการประยุกต์ใช้งานที่จำเป็น

กรอบนโยบาย Cybersecurity
ที่จะเสนอคณะกรรมการเตรียมการ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๑. การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ
(Critical Information Infrastructure Protection : CIIP)

๒. การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์
(Emergency Readiness)

๓. การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ (Cybersecurity Governance)

๔. การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์
(Public-Private Partnership)

๕. การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Capacity Building)

๖. การพัฒนากฎหมาย ระเบียบ และมาตรฐานเพื่อความมั่นคงปลอดภัยไซเบอร์
(Law, Regulation and Standard)

๗. การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์
(International Cooperation)

๘. การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ (Research & Development)

มาตรการทางกฎหมายปัจจุบัน ที่กำหนดเกี่ยวกับการดูแล Cybersecurity ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ของประเทศ

หน่วยงาน	มาตรการด้านการดูแล ความมั่นคงปลอดภัยไซเบอร์	กฎหมาย/ระเบียบที่เกี่ยวข้อง
คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	กำหนดมาตรการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority)	ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวทางการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) พ.ศ. ๒๕๕๒
	กำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ด้วยวิธีการแบบปลอดภัย ของหน่วยงานของรัฐและเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญของประเทศ	• พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ • ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ • ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ • ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กรหรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ ซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. ๒๕๕๙
	กำหนดมาตรการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานของรัฐ	• พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ • ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

มาตรการทางกฎหมายปัจจุบัน ที่กำหนดเกี่ยวกับการดูแล Cybersecurity ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ของประเทศ

หน่วยงาน	มาตรการด้านการดูแลความมั่นคงปลอดภัยไซเบอร์	กฎหมาย/ระเบียบที่เกี่ยวข้อง
ธนาคารแห่งประเทศไทย (ผู้ให้บริการระบบการชำระเงิน)	กำหนดมาตรการรักษาความมั่นคงปลอดภัยของระบบชำระเงินที่เป็นโครงสร้างพื้นฐานของประเทศ	พระราชบัญญัติระบบการชำระเงิน พ.ศ. ๒๕๖๐ ม. ๗ (๕)
สำนักงาน ก.ล.ต. (บริษัทหลักทรัพย์)	กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทหลักทรัพย์	ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ อธ/น. ๕/๒๕๔๗ เรื่อง แนวทางปฏิบัติในการควบคุมการปฏิบัติงานและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์
สำนักงาน คปภ. (บริษัทประกันชีวิต และบริษัทประกันวินาศภัย)	กำหนดมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัย และการชดใช้เงินตามสัญญาประกันชีวิต โดยใช้วิธีการทางอิเล็กทรอนิกส์	ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์วิธีการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัยและการชดใช้เงินตามสัญญาประกันชีวิต โดยใช้วิธีการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๐
กรมสรรพากร (ผู้ประกอบการที่ออกใบกำกับภาษี)	กำหนดมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับการจัดทำใบกำกับภาษีอิเล็กทรอนิกส์หรือใบรับอิเล็กทรอนิกส์	ระเบียบกรมสรรพากร ว่าด้วยการจัดทำ ส่งมอบ และเก็บรักษาใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๐ ข้อ ๑๐

MAPPINGS TO THE CIS Critical Security Controls

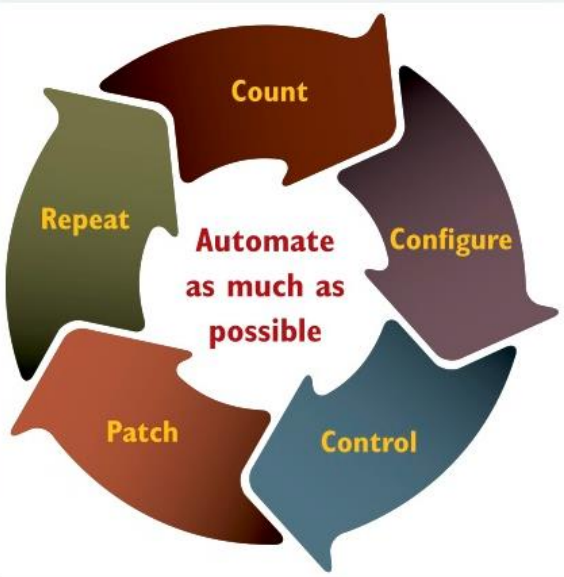
CIS CRITICAL SECURITY CONTROL	NIST 800-53 rev4*	NIST Core Framework	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	NSA MNP	Au Top 35	NSA Top 10	GCHQ 10 Steps	UK Cyber Essentials	UK ICO Protecting Data	PCI DSS 3.0	HIPAA	FFIEC Examiners Handbook	COBIT 5	NERC CIP v5	NERC CIP v4	NERC CIP v3	Cloud Security Alliance	FY15 FISMA Metrics	ITIL 2011 KPIs
1 Inventory of Authorized & Unauthorized Devices	CA-7 CM-8 IA-3 SA-4 SC-17 PM-5	ID.AM-1 ID.AM-3 PR.DS-3	• HWAM: Hardware Asset Management	A.8.1.1 A.9.1.2 A.13.1.1	A.7.1.1 A.10.6.2 A.10.6.1 A.11.4.6	• Map Your Network • Baseline Management • Disconnect Your Network • Personal Electronic Device Management • Network Access Control • Log Management					• Inappropriate Locations for Processing Data	2.4	• §64.310(b) Workstation Use – R • §64.310(c) Workstation Security – R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld) • BAM* Manage Assets	• APO13: Manage Security • DSS05: Manage Security Services	CIP-002-5 R1 CIP-002-5 R2	CIP-002-4 R1 CIP-004-4 R4 CIP-002-4 R2 CIP-005-4 R2 CIP-002-4 R3 CIP-006-4 R2 CIP-002-4 R5	CIP-002-3 R1 CIP-003-3 R5 CIP-002-3 R2 CIP-006-3 R4 CIP-002-3 R3 CIP-005-3 R2 CIP-002-3 R4 CIP-006-3 R3	DCS-01 MDS-09 MDS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
2 Inventory of Authorized & Unauthorized Software	CA-7 CM-8 SA-4 SI-4 CM-2 CM-10 SC-18 PM-5 CM-11 SC-34	ID.AM-2 PR.DS-6	• HWAM: Hardware Asset Management • SWAM: Software Asset Management	A.12.5.1 A.12.6.2		• Baseline Management • Executable Content Restrictions • Configuration and Change Management	1 14 17	• Application Whitelisting			• Decommissioning of Software or Services		• §64.310(b) Workstation Use – R • §64.310(c) Workstation Security – R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services				CCC-04 MOS-3 MDS-04 MDS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
3 Secure Configurations for Hardware & Software	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 MA-4 SC-34 CM-3 CM-9 MA-5 SI-2 CM-5 CM-9 SA-6 SI-4	PR.IP-1	• CM: Configuration Setting Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	3-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 4.2 11.5	• §64.310(b) Workstation Use – R • §64.310(c) Workstation Security – R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-007-6 R2 CIP-010-1 R2	CIP-003-4 R6 CIP-007-4 R3	CIP-003-3 R6 CIP-007-3 R3	BS-07 MDS-15 MDS-19 TVM-02	2: Continuous Monitoring	Information Security Management
4 Continuous Vulnerability Assessment & Remediation	CA-2 RA-5 SI-4 CA-7 SC-34 SI-7	ID.RA-1 DE.CM-8 ID.RA-2 RS.MI-3 PR.IP-12	• VUL: Vulnerability Management	A.12.6.1 A.14.2.8	A.12.6.1 A.13.1.2 A.15.2.2	• Patch Management • Log Management • Configuration and Change Management	2 3	• Take Advantage of Software Improvements		• Patch Management	• Software Updates	6.1 6.2 11.2	• §64.310(b) Workstation Use – R • §64.310(c) Workstation Security – R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R2 CIP-010-1 R3	CIP-005-4 R4 CIP-007-4 R3 CIP-007-4 R8	CIP-005-3 R4 CIP-007-3 R3 CIP-007-3 R8	RS-05 MDS-15 MDS-19 TVM-02	2: Continuous Monitoring	Information Security Management
5 Controlled Use of Administrative Privileges	AC-2 IA-4 IA-5 AC-6 CM-7 SI-4 AU-17 IA-8	PR.AC-4 PR.PA-2 PR.AT-2 PR.PT-3		A.9.1.1 A.9.2.2 – A.9.2.6 A.9.3.1 A.9.4.1 – A.9.4.4	A.10.6.4 A.11.5.1 – A.11.5.3	• User Access • Baseline Management • Log Management	4 9 11 25	• Control Administrative Privileges	• Monitoring	• Access Control	• Configuration of SSL and TLS • Default Credentials	2.1 7.1 – 7.3 8.1 – 8.3 8.7	• §64.310(b) Workstation Use – R • §64.310(c) Workstation Security – R	• Authentication and Access Controls	• APO13: Manage Security • DSS05: Manage Security Services	CIP-004-5 R4 CIP-006-5 R5 CIP-005-5 R5	CIP-004-4 R5 CIP-004-4 R4 CIP-005-4 R2 CIP-005-4 R3 CIP-006-4 R3 CIP-007-4 R3	CIP-005-3 R5 CIP-006-3 R4 CIP-005-3 R2 CIP-006-3 R3 CIP-007-3 R3	IAM-09 – IAM-13 MDS-14 MDS-20	3: Identity Credential & Access Management	Information Security Management
6 Maintenance, Monitoring, & Analysis of Audit Logs	AC-20 AU-6 AU-11 IA-10 AU-2 AU-7 AU-12 SI-4 AU-3 AU-8 AU-13 AU-4 AU-9 AU-14 AU-5 AU-10 CA-7	PR.PT-1 DE.AE-3 DE.CM-1 DE.DP-1 DE.DP-5 DE.DP-2	• Generic Audit Monitoring	A.12.4.1 – A.12.4.4 A.12.7.1	A.10.10.1 – A.10.10.3 A.10.10.6	• Log Management	15-16 35		• Monitoring			10.1 – 10.7	• §64.308(a)(1) Security Management Process – Information System Activity Review R • §64.308(a)(5) Security Awareness and Training – Log-in Monitoring A	• Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1	CIP-005-4 R3 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R6	RS-01 RS-03		Information Security Management
7 Email & Web Browser Protections	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 MA-4 SC-34 CM-3 CM-9 MA-5 SI-2 CM-5 CM-9 SA-6 SI-4	PR.IP-1	• CM: Configuration Setting Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	2-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 4.2 11.5	• §64.310(b) Workstation Use – R • §64.310(c) Workstation Security – R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-007-5 R2 CIP-010-1 R2	CIP-007-4 R6 CIP-007-4 R3	CIP-007-3 R6 CIP-007-3 R3	BS-07 MDS-15 MDS-19 TVM-02	2: Continuous Monitoring	Information Security Management
8 Malware Defenses	CA-7 SC-44 SI-4 SC-39 SI-3 SI-8	PR.PT-2 DE.CM-4 DE.CM-5	• Device Accessibility • Virus Scanners & Host Intrusion Prevention Systems • Security Gateways, Proxies, & Firewalls • Network Security Monitoring • Log Management	A.8.3.1 A.12.2.1 A.13.2.3	A.10.4.1 – A.10.4.2 A.10.7.1	• Use Anti-Virus File Reputation Services • Enable Anti-Exploitation Features	7 26 17 30 22		• Removable Media Controls • Malware Protection	• Malware Protection		5.1 – 5.4	• §64.308(a)(5) Security Awareness and Training – Protection from Malicious Software A • §64.310(d)(1) Device and Media Controls – Accountability A • §64.310(b) Workstation Use – R • §64.310(c) Workstation Security – R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R3	CIP-007-4 R4	CIP-007-3 R4	RS-01 MDS-15 TVM-01 TVM-02	4: Anti-Phishing & Malware Defense	Information Security Management
9 Limitation & Control of Network Ports	AS-1 AS-4 PM-13 AS-2 SA-11 PM-14 AS-3 SA-16 PM-16	PR.AC-5 DE.AE-1	• Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	A.10.6.1 – A.10.6.2 A.11.4.4	• Baseline Management • Configuration and Change Management	2 13 3 27 12	• Limit Workstation-to-Workstation Communication	• Network Security		• Decommissioning of Software or Services • Unnecessary Services	1.4	• §64.310(b) Workstation Use – R • §64.310(c) Workstation Security – R	• Network Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R1	CIP-007-4 R2	CIP-007-3 R2	DSI-02 RS-06 IPY-04		Information Security Management
10 Data Recovery Capability	CP-9 CP-10 PM-4	PR.IP-4		A.10.1.1 A.12.3.1	A.10.5.1 A.10.8.3	• Backup Strategy						4.1 9.5 – 9.7	• §64.308(a)(7) Contingency Plan – Data Backup Plan R • §64.308(a)(7) Contingency Plan – Disaster Recovery Plan R • §64.308(a)(7) Contingency Plan – Testing & Revision Procedure A • §64.310(d)(1) Device & Media Controls – Data Backup & Storage A	• Encryption	• APO13: Manage Security • DSS05: Manage Security Services		CIP-009-4 R4 CIP-009-4 R5	CIP-009-3 R4 CIP-009-3 R5	RIS-11		Information Security Management
11 Secure Configurations for Network Devices	AC-4 CA-9 CM-5 MA-4 CA-3 CM-2 CM-6 SC-20 CA-7 CM-3 CM-9 SI-4	PR.AC-5 PR.IP-1 PR.PT-4	• CM: Configuration Setting Management • Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.3	A.10.6.1 – A.10.6.2 A.11.4.5 A.11.4.7 A.11.5.1 – A.11.5.3	• Map Your Network • Patch Management • Baseline Management • Disconnect Your Network • Security Gateways, Proxies, and Firewalls • Configuration and Change Management	2 3 10	• Set a Secure Baseline Configuration • Segregate Networks and Functions	• Secure Configuration • Network Security	• Boundary Firewalls & Internet Gateways • Secure Configuration • Patch Management	• Software Updates • Inappropriate Locations for Processing Data	1.1 – 1.2 2.2 4.2	• §64.308(a)(4) Information Access Management – Isolating Health Care Clearinghouse Function R • §64.310(b) Workstation Use – R • §64.310(c) Workstation Security – R	• Network Security	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-005-5 R1 CIP-005-5 R2	CIP-003-4 R6 CIP-004-4 R4 CIP-005-4 R2 CIP-007-4 R6 CIP-005-4 R1 CIP-007-4 R3	CIP-003-3 R6 CIP-004-3 R4 CIP-006-3 R4 CIP-007-3 R3 CIP-005-3 R2 CIP-007-3 R6	DSI-02 IVS-09 IAM-03 MDS-19 RS-06 TVM-02	3: Identity Credential & Access Management 6: Network Defense 7: Boundary Protection	Information Security Management
12 Boundary Defense	AC-4 CA-7 SC-7 AC-17 CA-9 SC-8 AC-20 CM-2 SI-4 CA-3 SA-9	PR.AC-3 PR.AC-5 PR.PA-2 DE.AE-1	• Boundary Protection	A.9.1.2 A.12.4.1 A.13.1.3 A.13.1.1	A.10.6.1 – A.10.6.2 A.11.5.1 – A.11.5.2 A.11.5.3 – A.11.5.5 A.11.6.1 – A.11.6.2 A.11.7.1 – A.11.7.2 A.12.3.1 A.13.1.1 A.13.2.3 A.14.1.2 A.14.1.3 A.14.1.4 A.14.1.5 A.14.1.7	• Map Your Network • Network Architecture • Baseline Management • Disconnect Your Network • Personal Electronic Device Management • Security Gateways, Proxies, and Firewalls • Remote Access Security • Network Security Monitoring • Log Management	10-11 18-20 23 32-34	• Segregate Networks and Functions	• Home and Mobile Working • Monitoring • Network Security	• Boundary Firewalls & Internet Gateways	• Configuration of SSL and TLS • Inappropriate Locations for Processing Data	1.1 – 1.3 8.3 10.8 11.4	• §64.310(b) Workstation Use – R • §64.310(c) Workstation Security – R	• Network Security • Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-005-5 R4	CIP-005-4 R1 CIP-007-4 R3	CIP-005-3 R1 CIP-007-3 R6	DSI-02 RS-01 RS-04 RS-06 RS-09 MDS-16	3: Identity Credential & Access Management 6: Network Defense 7: Boundary Protection	Information Security Management
13 Data Protection	AC-3 CA-9 SC-8 SI-4 AC-4 IA-9 SC-28 AC-23 MP-2 SC-41 CA-7 SA-18 SC-43	PR.AC-5 PR.DS-1 PR.DS-5 PR.PT-2		A.8.3.1 A.10.1.1 – A.10.1.2 A.12.2.1 A.18.1.5	A.10.7.1 A.12.2.1 – A.12.2.2 A.12.5.4 A.15.1.6	• Network Architecture • Device Accessibility • Security Gateways, Proxies, and Firewalls • Network Security Monitoring	26		• Removable Media Controls			3.6 4.1 – 4.3	• §64.308(a)(4) Information Access Management – Isolating Health Care Clearinghouse Function R • §64.310(d)(1) Device and Media Controls – Accountability A • §64.312(a)(1) Access Control – Encryption and Decryption A • §64.312(e)(1) Transmission Security – Integrity Controls A • §64.312(e)(1) Transmission Security – Encryption A	• Encryption • Data Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-011-5 R1			DSI-02 DSI-03 EKM-03 – EKM-04 MDS-11	5: Data Protection	Information Security Management
14 Controlled Access Based on the Need to Know	AC-1 AC-6 IA-2 AC-2 AC-14 SC-16 AC-3 CA-7 SI-4 MP-3	PR.AC-4 PR.DS-2 PR.AC-1 PR.PT-2 PR.DS-1 PR.PT-3	• TBAT: Access Control Management • PAM: Privileges	A.8.1.1 A.9.1.1 A.10.1.1	A.10.7.1 A.10.8.1 – A.10.10.3 A.11.4.5 A.11.4.7 A.11.6.1 – A.11.6.2 A.12.5.4	• Network Architecture • Device Accessibility • User Access • Data-at-Rest Protection • Log Management	26	• Segregate Networks and Functions	• Managing User Privileges • Network Security	• Access Control	• Inappropriate Locations for Processing Data	1.3 – 1.4 4.3 7.1 – 7.3 8.7	• §64.308(a)(3) Security Management Process – Information System Activity Review R • §64.308(a)(4) Information Access Management – Isolating Health Care Clearinghouse Function R • §64.308(a)(4) Information Access Management – Access Authorization R • §64.308(a)(4) Information Access Management – Access Establishment and Modification R • §64.308(a)(5) Security Awareness and Training – Password Management R • §64.312(a)(1) Access Control – Encryption and Decryption A • §64.312(b) Audit Controls R • §64.312(c)(1) Integrity – Mechanism to Authenticate Electronic Protected Health Information A • §64.312(d) Person or Entity Authentication – R • §64.312(e)(1) Transmission Security – Integrity Controls A • §64.312(e)(1) Transmission Security – Encryption A	• Authentication and Access Controls • Encryption • Data Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-005-5 R3 CIP-011-5 R1	CIP-005-4 R5 CIP-005-4 R4 CIP-005-4 R2 CIP-006-4 R3	CIP-005-3 R5 CIP-006-3 R4 CIP-005-3 R2 CIP-006-3 R3	DSI-02 RS-09 MDS-11		Information Security Management
15 Wireless Access Control	AC-18 CM-2 SC-40 AC-19 IA-3 SI-4 CA-3 SC-8 CA-7 SC-17			A.10.1.1 A.12.4.1 A.12.7.1		• Map Your Network • Baseline Management • Disconnect Your Network • Personal Electronic Device Management • Network Access Control			• Monitoring • Network Security			4.3 11.1		• Network Security • Encryption • Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R4	CIP-005-4 R2 CIP-007-4 R6	CIP-005-3 R2 CIP-007-3 R6	RS-01 RS-06 RS-12 MDS-11		Information Security Management
16 Account Monitoring & Control	AC-2 CA-7 AC-1 IA-5 AC-7 IA-10 SI-4 AC-11 SC-17 AC-12 SC-23	PR.AC-1 PR.AC-4 PR.PT-1	• CRED: Credentials and Authentication Management	A.9.1.1 A.9.2.3 – A.9.2.6 A.9.3.1 A.9.4.3 – A.9.4.3 A.11.2.8	A.8.3.1 A.11.2.1 A.11.2.3 – A.11.2.4 A.11.3.1 – A.11.3.3 A.11.5.1 – A.11.5.3	• User Access • Baseline Management • Log Management	25		• Managing User Privileges	• Access Control	• Configuration of SSL and TLS	7.1 – 7.3 8.7 – 8.8	• §64.308(a)(3) Security Management Process – Information System Activity Review R • §64.308(a)(4) Information Access Management – Access Authorization A • §64.308(a)(4) Information Access Management – Access Establishment and Modification A • §64.308(a)(5) Security Awareness and Training – Password Management A • §64.312(a)(1) Access Control – Unique User Identification R • §64.312(a)(2) Access Control – Automatic Logoff A • §64.312(d) Person or Entity Authentication – R • §64.312(e)(1) Transmission Security – Integrity Controls A • §64.312(e)(1) Transmission Security – Encryption A	• Authentication and Access Controls	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-005-5 R3 CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R5 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R5 CIP-007-3 R6	IAM-02 IAM-09 – IAM-12 MDS-14 MDS-16 MDS-20	3: Identity Credential & Access Management	Information Security Management
17 Security Skills Assessment and Appropriate Training to Fill Gaps	AS-1 AS-4 PM-13 AS-2 SA-11 PM-14 AS-3 SA-16 PM-16	PR.AT-1 PR.AT-2 PR.AT-3	• HEMP: Security-Related Behavior Management	A.7.2.2	A.8.2.2	• Training	28		• User Education & Awareness			12.6	• §64.308(a)(5) Security Awareness and Training – Security Reminders A • §64.308(a)(5) Security Awareness and Training – Protection from Malicious Software A • §64.308(a)(5) Security Awareness and Training – Log-in Monitoring A • §64.308(a)(5) Security Awareness and Training – Password Management A	• Personnel Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-004-5 R1 CIP-004-5 R2	CIP-004-4 R1 CIP-004-4 R2	CIP-004-3 R1 CIP-004-3 R2	HRS-10 MOS-05	8: Training and Education	Information Security Management
18 Application Software Security	SA-13 SA-20 SI-11 SA-15 SA-21 SI-15 SA-16 SC-39 SI-16 SA-17 SA-10	PR.DS-7	• VUL: Vulnerability Management	A.9.4.5 A.12.1.4 A.18.2.1 A.14.2.6 – A.14.2.8	A.10.1.4 A.12.5.2 A.12.2.1 A.12.5.5 A.12.2.4	• Training	34				• SQL Injection	6.3 6.5 – 6.7		• Application Security • Software Development & Acquisition	• APO13: Manage Security • DSS05: Manage Security Services				AIS-01 CCC-02 AIS-03 CCC-03 AIS-04 IVS-08 CEC-01		Information Security Management
19 Incident Response & Management	IR-1 IR-4 IR-7 IR-2 IR-5 IR-8 IR-3 IR-6 IR-10	PR.IP-9 RS.AN-1 RS.AN-4 RS.CO-1 RS.CO-2 RS.CO-3 RS.IM-1	• Plan for Events • Respond to Events	A.6.1.3 A.7.2.1 A.16.1.2 A.16.1.4 – A.16.1.7	A.6.1.4 A.8.2.1 A.13.1.1 A.13.2.1 – A.13.2.2	• Incident Response and Disaster Recovery Plans			• Incident Management			12.10	• §64.308(a)(6) Security Incident Procedures – Response and Reporting R		• APO13: Manage Security • DSS05: Manage Security Services • DSS02: Manage Service Requests and Incidents	CIP-008-5 R1 CIP-008-5 R2 CIP-008-5 R3	CIP-008-4 R1 CIP-008-4 R2	CIP-008-3 R1 CIP-008-3 R2	SEF-01 – SEF-05	9: Incident Response	Information Security Management
20 Penetration Tests & Red Team Exercises	CA-2 CA-8 PM-14 CA-5 RA-6 PM-16 CA-6 SI-4			A.14.2.8 A.18.2.1 A.18.2.3	A.15.2.2 A.15.3.1	• Audit Strategy						11.3			• APO13: Manage Security • DSS05: Manage Security Services • MEA02: Monitor, Evaluate and Assess the System of Internal Control						Information Security Management

*NIST 800-53 LISTINGS

AC-1: Access Control Policy and Procedures
AC-2: Account Management
AC-3: Access Enforcement
AC-4: Information Flow Enforcement
AC-6: Least Privilege
AC-7: Unsuccessful Logon Attempts
AC-11: Session Lock
AC-12: Session Termination
AC-17: Remote Access
AC-18: Wireless Access
AC-19: Access Control for Mobile Devices
AC-20: Use of External Information Systems
AC-23: Data Mining Protection
AC-24: Access Control Decisions
AT-1: Security Awareness and Training Policy and Procedures
AT-2: Security Awareness Training
AT-3: Role-Based Security Training
AT-4: Security Training Records
AU-2: Audit Events
AU-3: Content of Audit Records
AU-4: Audit Storage Capacity
AU-5: Response to Audit Processing Failures
AU-6: Audit Review, Analysis, and Reporting
AU-7: Audit Reduction and Report Generation
AU-8: Time Stamps
AU-9: Protection of Audit Information
AU-10: Non-repudiation
AU-11: Audit Record Retention
AU-12: Audit Generation
AU-13: Monitoring for Information Disclosure
AU-14: Session Audit
CA-2: Security Assessments
CA-3: System Interconnections
CA-5: Plan of Action and Milestones
CA-6: Security Authorization
CA-7: Continuous Monitoring
CA-8: Penetration Testing
CA-9: Internal System Connections
CM-2: Baseline Configuration
CM-3: Configuration Change Control
CM-5: Access Restrictions for Change
CM-6: Configuration Settings
CM-7: Least Functionality
CM-8: Information System Component Inventory
CM-9: Configuration Management Plan
CM-10: Software Usage Restrictions
CM-11: User-Installed Software
CP-9: Information System Backup
CP-10: Information System Recovery and Reconstitution
IA-3: Device Identification and Authentication
IA-5: Authenticator Management
IA-10: Adaptive Identification and Authentication
IR-4: Incident Response Policy and Procedures
IR-6: Incident Response Training
IR-7: Incident Response Testing
IR-8: Incident Handling
IR-9: Incident Monitoring
IR-10: Incident Reporting
IR-1: Incident Response Assistance
IR-8: Incident Response Plan
IR-9: Information Spillage Response
SA-10: Integrated Information Security Analysis Team
MA-4: Nonlocal Maintenance
MP-2: Media Marking
MP-4: Media Storage
MP-5: Media Transport
PM-5: Information System Inventory
PM-6: Information Security Measures of Performance
PM-13: Information Security Workforce
PM-14: Testing, Training, & Monitoring
PM-16: Threat Awareness Program
RA-2: Security Categorization
RA-5: Vulnerability Scanning
RA-6: Technical Surveillance Countermeasures Survey
SA-4: Acquisition Process
SA-9: External Information System Services
SA-11: Developer Security Testing and Evaluation
SA-13: Trustworthiness
SA-15: Development Process, Standards, and Tools
SA-16: Developer-Provided Training
SA-17: Developer Security Architecture and Design
SA-18: Tamper Resistance and Detection
SA-20: Customized Development of Critical Components
SA-21: Developer Screening
SC-7: Boundary Protection
SC-8: Transmission Confidentiality and Integrity
SC-15: Collaborative Computing Devices
SC-16: Transmission of Security Attributes
SC-17: Public Key Infrastructure Certificates
SC-18: Mobile Code
SC-20: Secure Name/Address Resolution Service (Authoritative Source)
SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver)
SC-22: Architecture and Provisioning for Name/Address Resolution Service
SC-23: Session Authenticity
SC-24: Fail in Known State
SC-28: Protection of Information at Rest
SC-31: Covert Channel Analysis
SC-34: Non-Modifiable Executable Programs
SC-39: Process Isolation
SC-40: Wireless Link Protection
SC-41: Port and I/O Device Access
SC-44: Detonation Chambers
SC-2: Flaw Remediation
SI-2: Malicious Code Protection
SI-4: Information System Monitoring
SI-6: Security Function Verification
SI-7: Software, Firmware, and Information Integrity
SI-8: Spam Protection
SI-10: Information Input Validation
SI-11: Error Handling
SI-15: Information Output Filtering
SI-16: Memory Protection

CIS Critical Security Controls

CIS Critical Security Controls



มาตรฐานแนวปฏิบัติ / แนวทางในการประยุกต์ใช้งานในแต่ละระดับ

มาตรฐานและมาตรการ
เพื่อลดความเสี่ยง (ขั้นต่ำ)

การดูแลเว็บไซต์ในการถูกโจมตี

การดูแลระบบสารสนเทศ (ภาครัฐ)
บาง domain ของ ISO 27001

มาตรฐานและมาตรการสำหรับ CII

มาตรฐานทั่ว ๆ ไป

มาตรฐานและมาตรการสำหรับ
CII (เฉพาะด้าน)

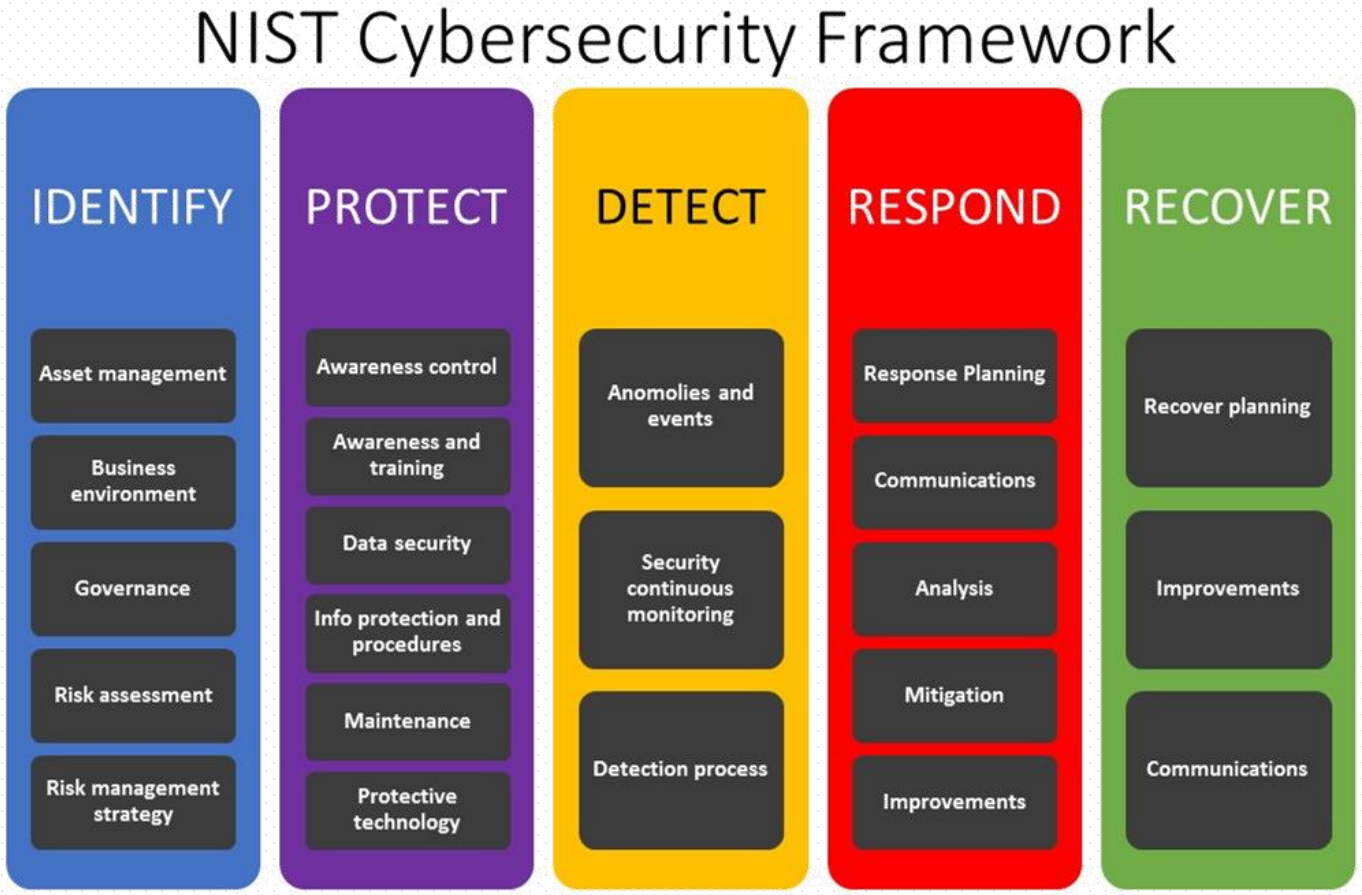
มาตรฐานที่ Specific เฉพาะแต่ละ Sector

มาตรฐานและมาตรการ ที่พึงนำไปใช้เป็นกรอบในการทำงานเพื่อลดความเสี่ยง

มาตรฐานการรักษาความมั่นคงปลอดภัย
สำหรับโปรแกรมประยุกต์บนเว็บไซต์
(Web Application Security Standard :WAS)

มาตรฐานการรักษาความมั่นคงปลอดภัย
สำหรับเว็บไซต์
(Website Security Standard :WSS)

มาตรฐานการรักษาความมั่นคงปลอดภัย
ตามวิธีการแบบปลอดภัย
พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์



ที่มา Website Security Standard (WSS) และ Web Application Security Standard (WAS) https://standard.etda.or.th/?page_id=7799

การใช้ NIST's Cybersecurity Framework (CSF) ควบคู่กับมาตรฐานด้านความมั่นคงปลอดภัยต่าง ๆ

มาตรฐานทั่ว ๆ ไป

- ISO/IEC 27001 การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
- HIPAA กฎหมายคุ้มครองข้อมูลสุขภาพ (สหรัฐอเมริกา)
- FFIEC คู่มือการตรวจไอทีของหน่วยงานกำกับดูแลกลุ่มการเงิน (สหรัฐอเมริกา)
- NERC CIP มาตรฐานความมั่นคงปลอดภัยในกลุ่มผู้ผลิตไฟฟ้า (อเมริกาเหนือ)

มาตรฐานที่ Specific เฉพาะแต่ละ Sector

- บริการ cloud computing - CSA Star
- กลุ่มสาธารณสุข - ISO 27799
- กลุ่มบริการชำระเงิน - PCI DSS (Data Security Standard)
- กลุ่มพลังงานไฟฟ้า NERC CIP

1.Inventory of Authorized and Unauthorized Devices 2.Inventory of Authorized and Unauthorized Software 3.Secure Configurations for Hardware and Software 4.Continuous Vulnerability Assessment and Remediation 5.Controlled Use of Administrative Privileges	6.Maintenance, Monitoring, and Analysis of Audit Logs 7.Email and Web Browser Protections 8.Malware Defenses 9.Limitation and Control of Network Ports 10.Data Recovery Capability	11.Secure Configurations for Network Devices 12.Boundary Defense 13.Data Protection 14.Controlled Access Based on the Need to Know 15.Wireless Access Control	16.Account Monitoring and Control 17.Security Skills Assessment and Appropriate Training to Fill Gaps 18.Application Software Security 19.Incident Response and Management 20.Penetration Tests and Red Team Exercise

ที่มา CIS: Security Control

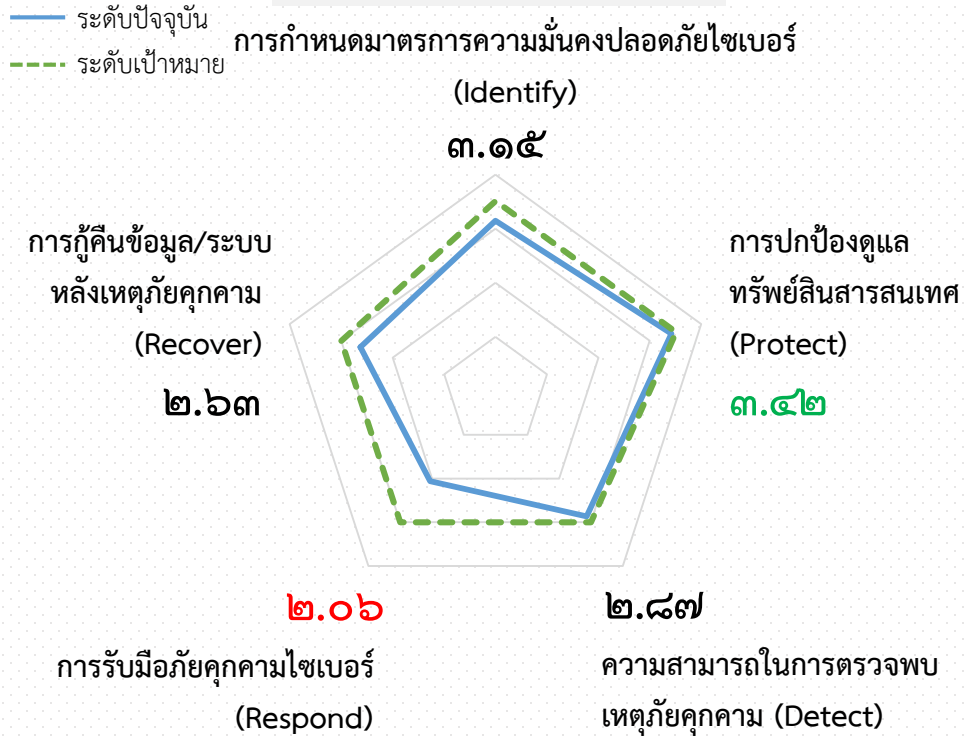
หมายเหตุ:
HIPAA = Health Insurance Portability and Accountability Act
FFIEC = Federal Financial Institutions Examination Council
NERC CIP = North American Electric Reliability Corporation critical infrastructure protection
CSA = Cloud Security Alliance

๓. แนวทางการทำ National Incident Flow (SOP) เพื่อทำงานร่วมกัน โดยเน้นรองรับเศรษฐกิจดิจิทัล

กรอบการรักษาความมั่นคงปลอดภัยสำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และผลการสำรวจความพร้อม

Identify	Protect	Detect	Respond	Recover
การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์	*การปกป้องดูแลทรัพย์สินสารสนเทศ*	*ความสามารถในการตรวจพบเหตุภัยคุกคามไซเบอร์*	*การรับมือภัยคุกคามไซเบอร์*	*การกู้คืนข้อมูลและระบบหลังเหตุภัยคุกคามไซเบอร์*

ผลการสำรวจความพร้อม



NIST Framework for Improving Critical Infrastructure Cybersecurity

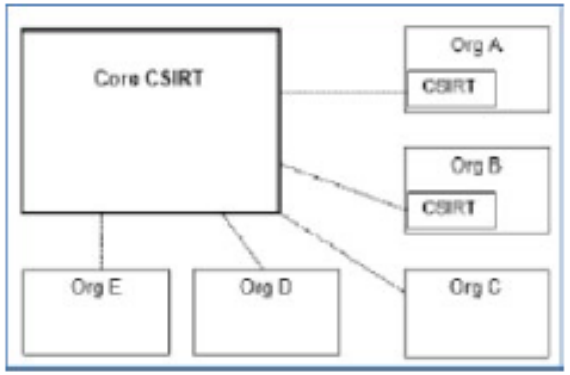
คือ กรอบแนวทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ประกาศโดยสหรัฐอเมริกา เพื่อกำหนดมาตรฐานขั้นต่ำ (benchmark) ของระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประกอบด้วยความสามารถของหน่วยงาน ๕ ด้าน คือ identify, protect, detect, respond และ recover

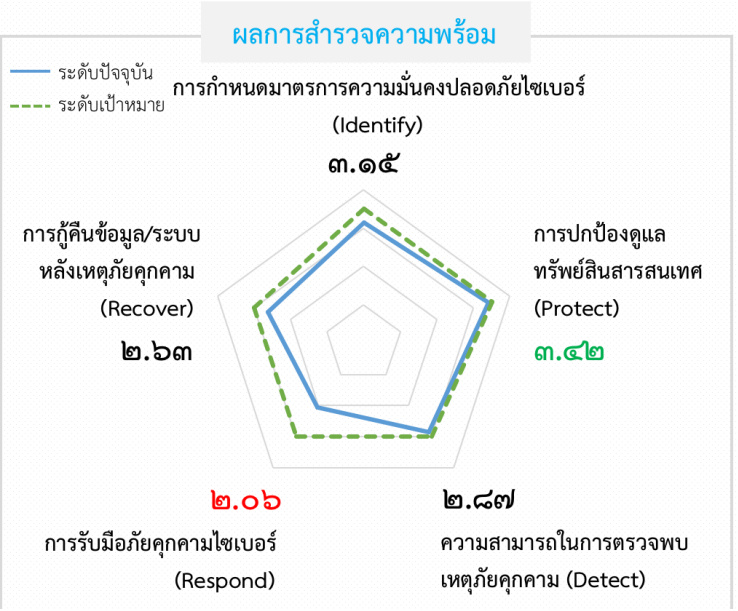
ที่มา: ผลการสำรวจข้อมูลจากหน่วยงานของรัฐและเอกชน จำนวน ๕๔๗ หน่วยงาน ในปี ๒๕๕๙ โดย สพธอ.

ความจำเป็นที่เราต้องทำงานในรูปแบบ SECTOR BASE' CSIRT

คู่มือสำหรับการจัดตั้งซีเซิร์ตในองค์กร มีรายละเอียดโดยสังเขปดังนี้

- การบริหารจัดการวงจรการทำงานของทีมและขีดความสามารถ
- การร่างกรอบงาน CSIRT
- การขออนุมัติจัดตั้ง CSIRT จากผู้บริหารระดับสูง
- การจัดตั้ง CSIRT และสภาวะแวดล้อมในการทำงาน
- กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม





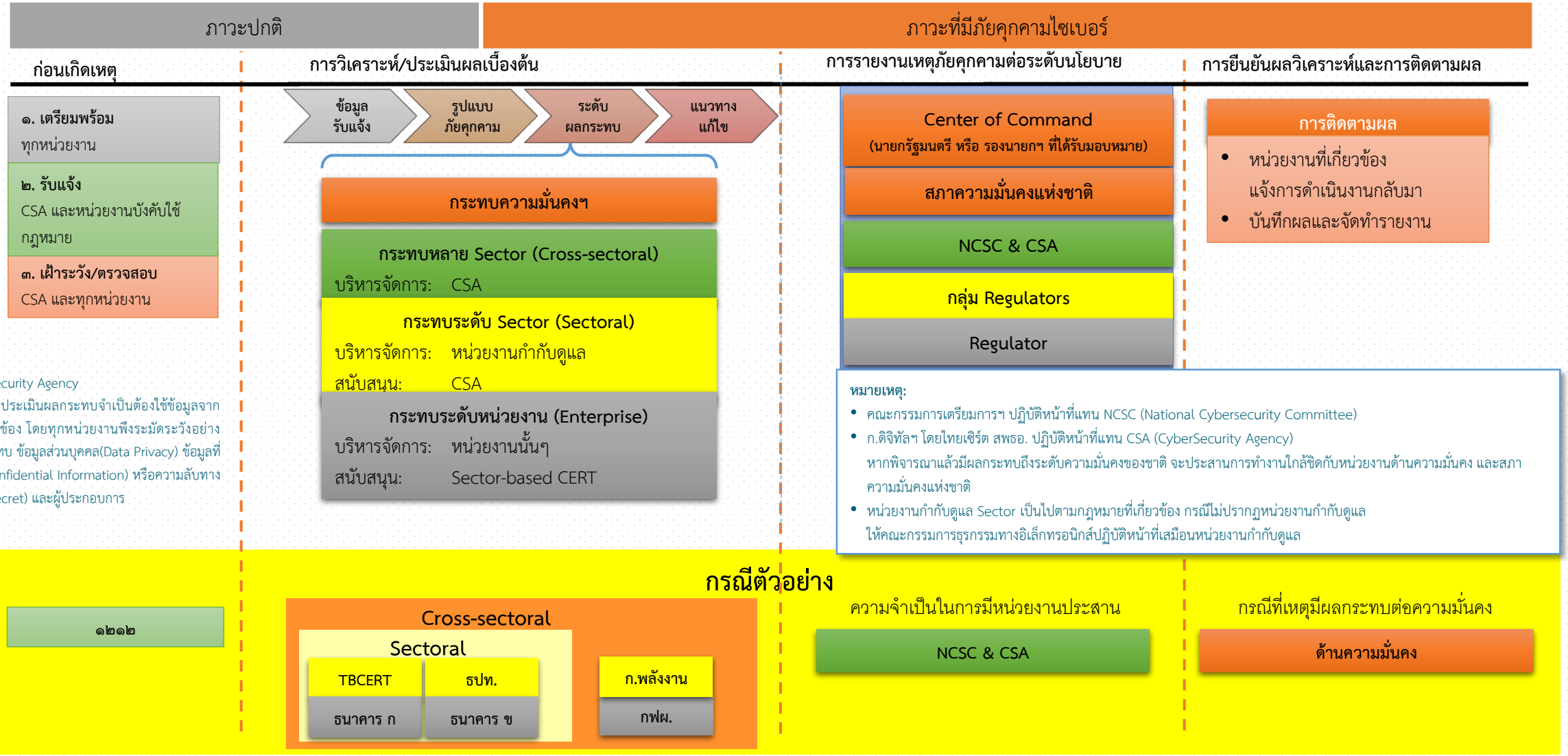
ที่มา https://www.thaicert.or.th/downloads/files/Establishing_a_CSIRT_th.pdf

ความจำเป็นในการประเมินวิธีการประเมินผลกระทบ Minimize Risk เพื่อ Take Action วิธีการประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์

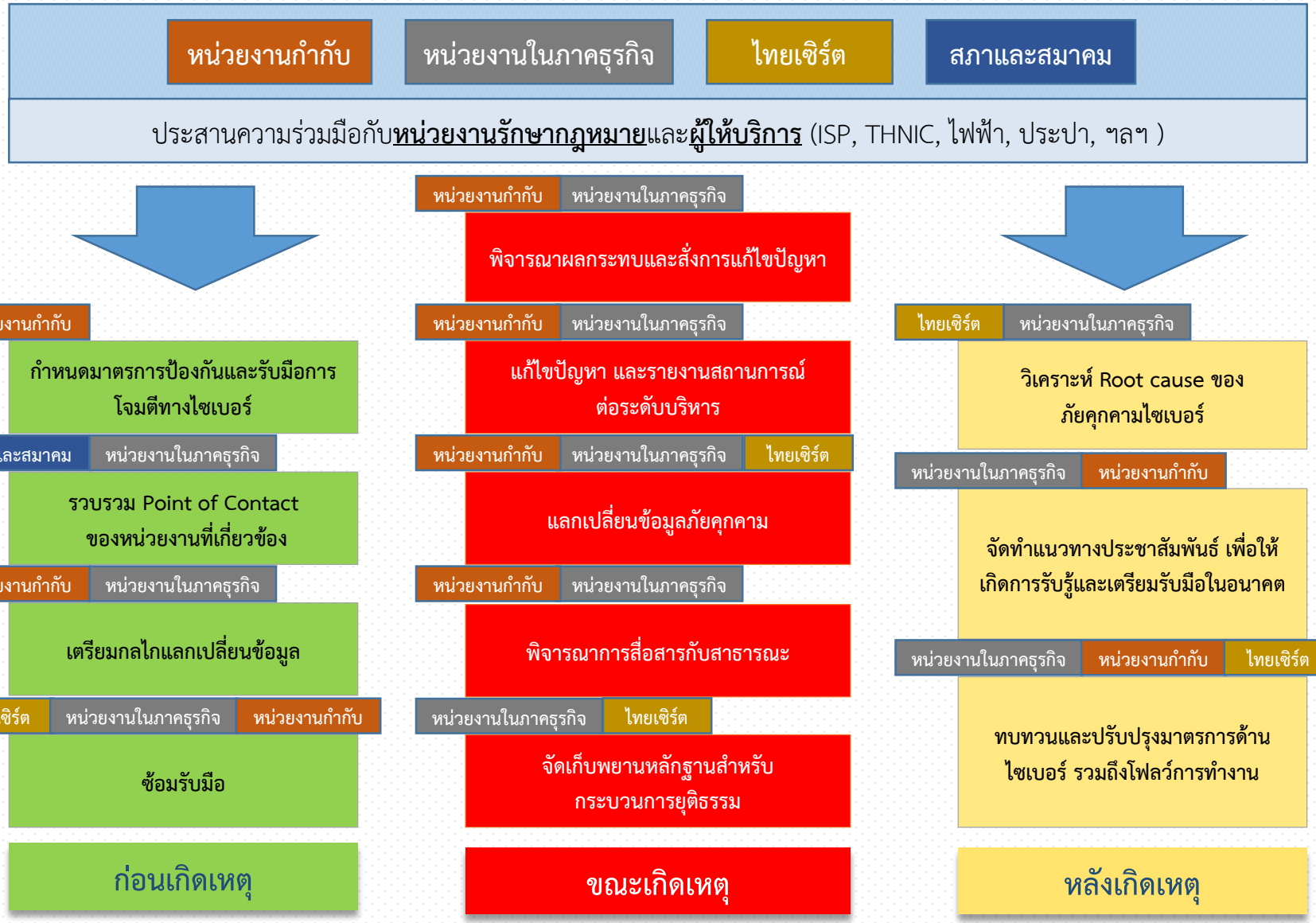
(อ้างอิงตามประกาศ คธอ. เรื่องประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕)

การประเมินระดับผลกระทบที่เกิดขึ้นใน ๑ วัน	Security Basic ผลกระทบระดับต่ำ	Security Medium ผลกระทบระดับปานกลาง	Security High ผลกระทบระดับสูง
(๑) ผลกระทบด้านมูลค่าความเสียหายทางการเงิน	< ๑ ล้านบาท	> ๑ ล้านบาท < ๑๐๐ ล้านบาท	> ๑๐๐ ล้านบาท
(๒) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัย	ไม่มีผู้ใช้บริการได้รับผลกระทบต่อชีวิต ร่างกายหรืออนามัย	ผู้ใช้บริการได้รับผลกระทบต่อร่างกายหรืออนามัย > ๑ คน < ๑,๐๐๐ คน	ผู้ใช้บริการได้รับผลกระทบ ต่อร่างกายหรืออนามัย ≧ ๑,๐๐๐ คน หรือ ต่อชีวิตตั้งแต่ ๑ คน
(๓) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่นใดนอกจาก (๒)	ผู้ใช้บริการได้รับผลกระทบ < ๑๐,๐๐๐ คน	ผู้ใช้บริการได้รับผลกระทบ >๑๐,๐๐๐ คน แต่ <๑๐๐,๐๐๐ คน	ผู้ใช้บริการได้รับผลกระทบ >๑๐๐,๐๐๐ คน
(๔) ผลกระทบด้านความมั่นคงของรัฐ	ไม่มีผลกระทบต่อความมั่นคงของรัฐ		มีผลกระทบต่อความมั่นคงของรัฐ

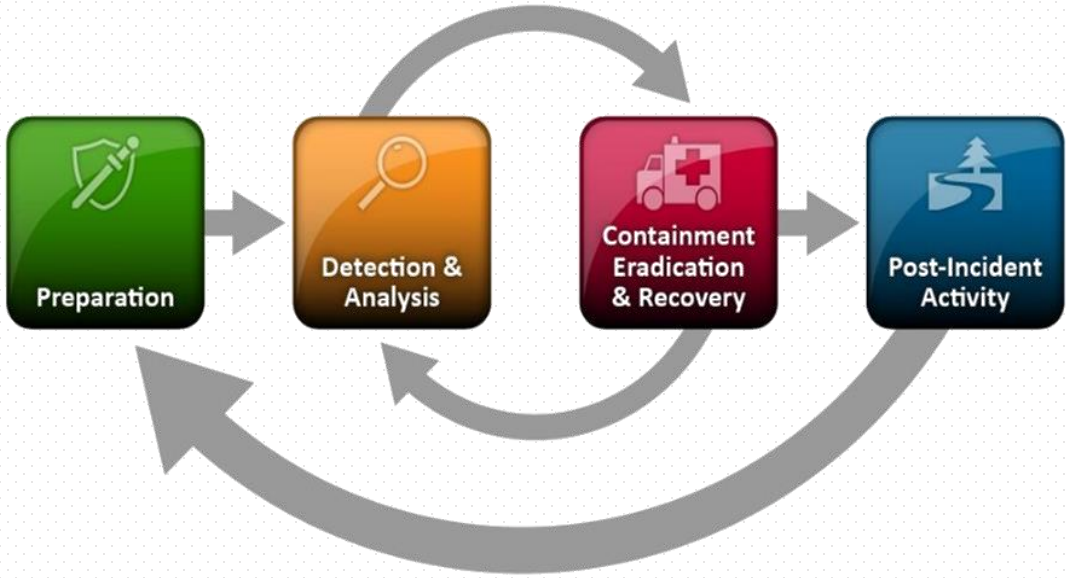
แนวทางการทำ National Incident Flow เพื่อทำงานร่วมกัน



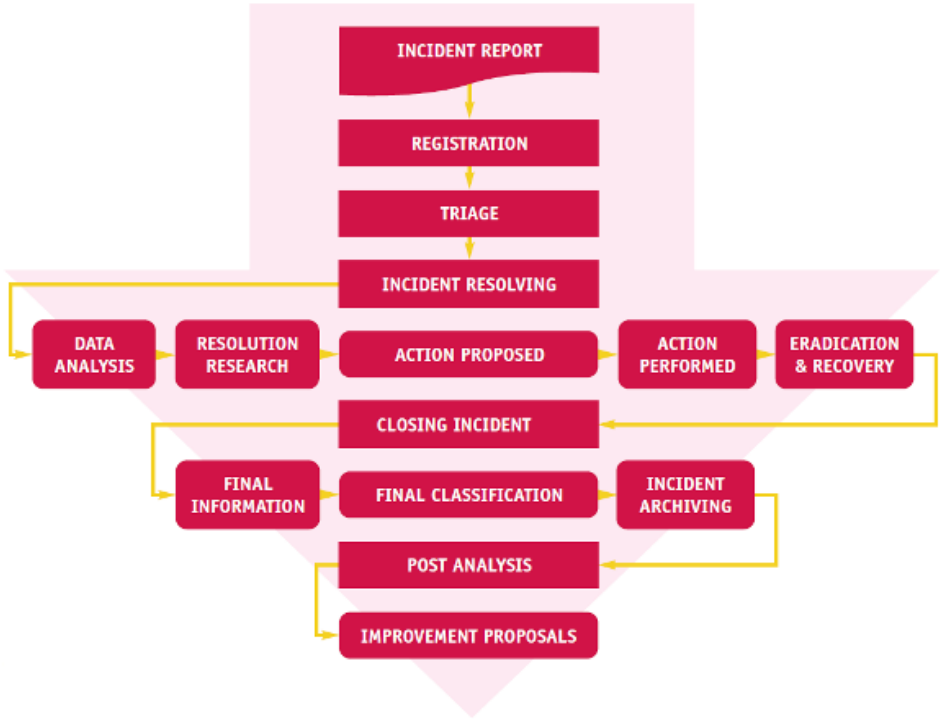
Crisis Management Flow ระดับกลุ่ม



แนวทางการวางแผนรับมือภัยคุกคาม



Computer Security Incident Handling Guide (NIST SP 800-61 Rev.2)



CERT (ENISA) Framework

ตัวอย่างขั้นตอนการตอบสนอง
ต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (ในระดับองค์กร)

๑.เฝ้าระวัง (Tier-1)
- ๑.๑ ระบบเฝ้าระวัง
- ๑.๒ ข่าวสารจากไทยเซิร์ต
- ๑.๓ ข่าวสารจากช่องทางเปิด

พบการโจมตี

๒.แจ้งเตือน
- ๒.๑ แจ้งผู้รับผิดชอบในส่วนที่ถูกโจมตี
- ๒.๒ แจ้งผู้บริหาร (กรณีสำคัญเร่งด่วน)
- ๒.๓ แจ้งไทยเซิร์ต

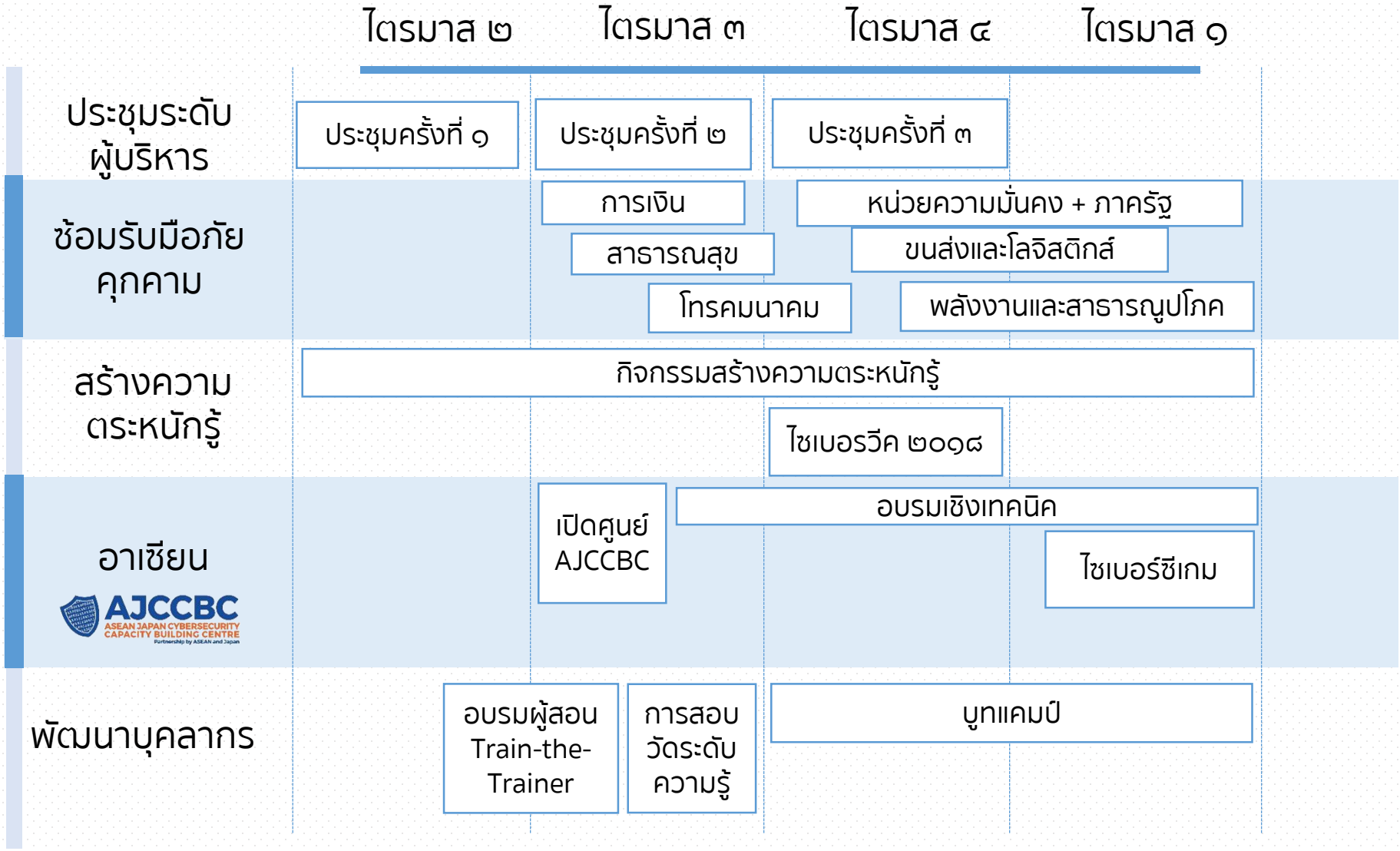
๓. วิเคราะห์ (Tier-2)
- ๓.๑ วิเคราะห์ Log หรือมัลแวร์
- ๓.๒ วิเคราะห์ผลกระทบรับมือภัยคุกคามและประสานงาน

ขอการสนับสนุน

ไทยเซิร์ต
- วิเคราะห์ภัยคุกคามและให้คำปรึกษา
- เก็บพยานหลักฐาน, กู้คืนระบบ
- ตรวจสอบช่องโหว่เว็บไซต์

๔. รายงาน
- ๔.๑ ผู้บริหาร
- ๔.๒ รายงานหน่วยกำกับดูแล

แผนการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ปี ๒๕๖๑



Key Messages

Information Sharing/Exercise/Drill
ไทยเป็นประธาน ASEAN ในเดือนพฤศจิกายนนี้
และ Cybersecurity เป็นวาระสำคัญของประเทศ

Cybersecurity Indicator
เพื่อตอบโจทย์ ITU, ASEAN
และควรมี
Cybersecurity Statement of Thailand

1. ความจำเป็นในการร่วมกันทบทวนการแบ่งกลุ่ม CIIP
2. ยกระดับความแข็งแรงของกรอบนโยบาย และมาตรการทางปฏิบัติ
3. คำนึงมาตรฐานขั้นต่ำ (Minimum Requirements) และรณรงค์ให้มีการใช้งานอย่างจริงจัง
4. Incident Flow Handling สำหรับองค์กรและประเทศที่ใช้ได้จริง / ข้อมูลผลกระทบ / และแนวทางการ Take Action ปรับ Flow ให้เหมาะกับบริบทการเปลี่ยนไปของระบบเศรษฐกิจและสังคม
5. การสร้างและพัฒนาคนทางไซเบอร์ เพื่อตอบสนอง Need ของประเทศ