หลักสูตรอบรมเชิงปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามข้อกำหนด กฎหมาย และกรอบการปฏิบัติ (Framework)ในระดับสากล

โครงการจ้างที่ปรึกษาจัดทำนโยบายและแผนปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา
ประจำปี พ.ศ. 2567 – 2570

สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา

General Ground Rules

Introduction to the course

Agenda & Timetable

09:00 - 10:30
10:45 – 12:00
13:00 – 14:15
14:30 – 16:00

Coffee Break & Lunch

10:30 - 10:45
12:00 - 13:00
14:15 - 14:30

Electronic Devices

Courtesy

Course Materials & Feedback

General Ground Rules

Agenda & Timetable

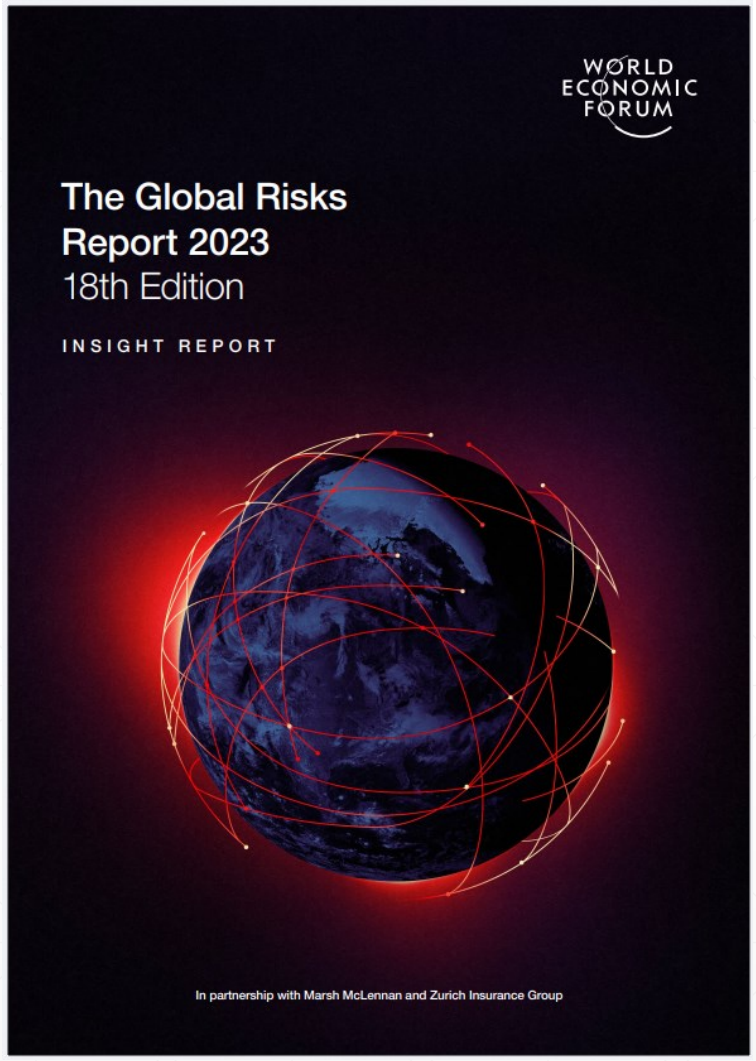
COURSE OUTLINE

	Time	Chapter	เนื้อหาหลักสูตรอบรม
	09:00 – 10:30	01	ความท้าทายและภัยคุกคามเกี่ยวกับไซเบอร์
		02	ภาพรวมกฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
	10:45 – 11:45	03	แนวปฏิบัติด้านเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยไซเบอร์
		04	ภาพรวมของ NIST Cybersecurity Framework
		05	องค์ประกอบของ NIST Cybersecurity Framework
	11:45 – 12:00		Workshop 1
	13:00 – 14:15	06	แนวปฏิบัติตาม NIST Cybersecurity Framework
	14:30 – 15:30	06	แนวปฏิบัติตาม NIST Cybersecurity Framework (ต่อ)
	15:30 – 16:00	-	Workshop 2

Introduction to Cyber

1

ความท้าทายและภัยคุกคามเกี่ยวกับไซเบอร์

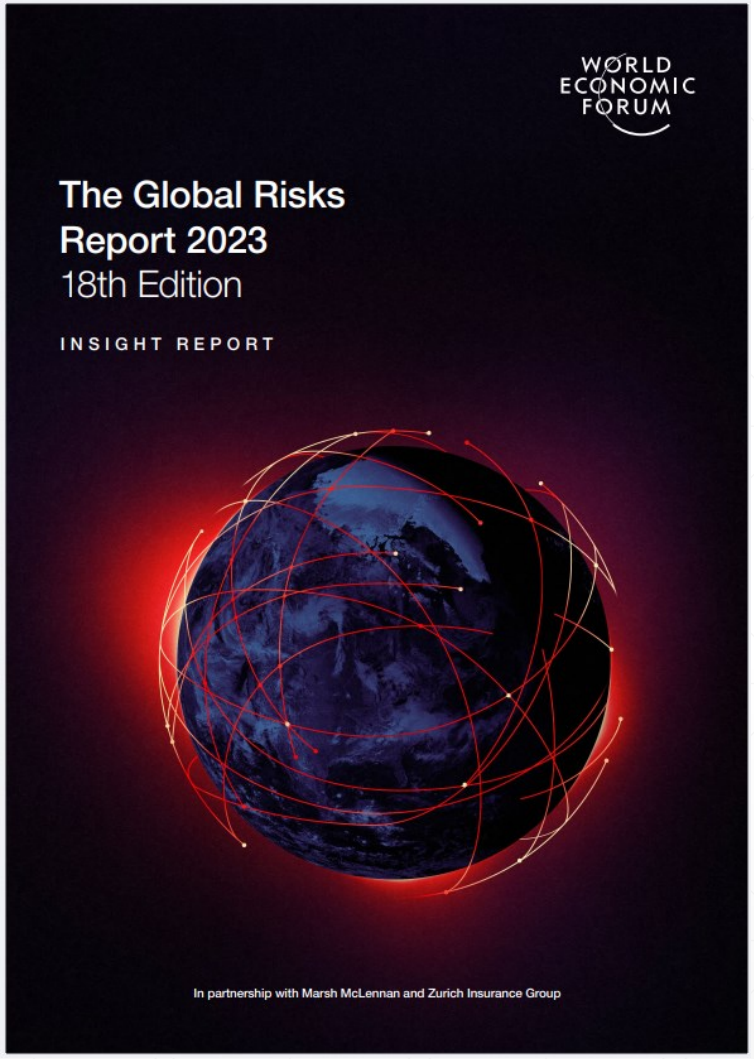


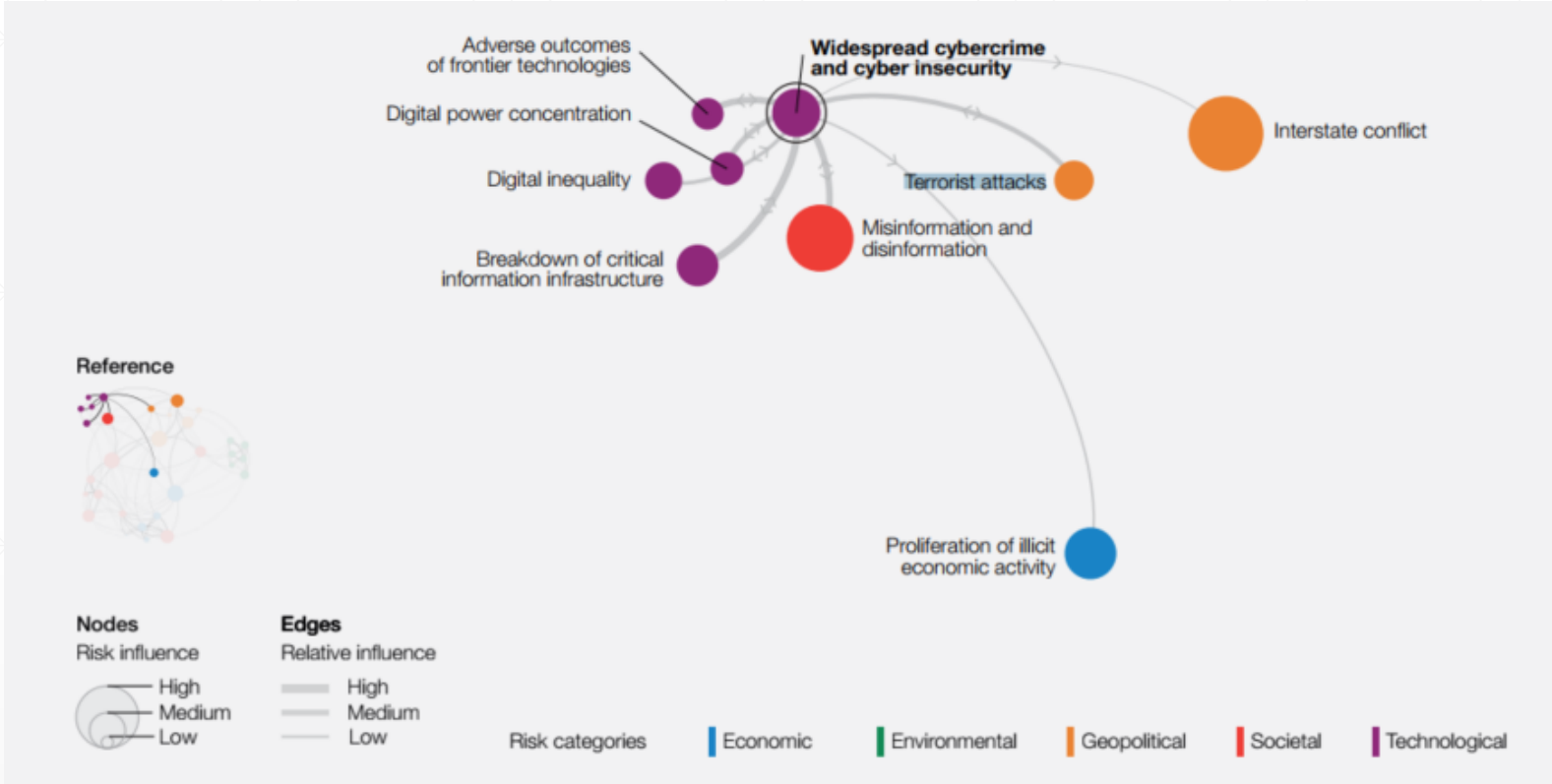
Source: www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Global risks ranked by severity over the short and long term

	2 years	10 years
1	Cost-of-living crisis	Failure to mitigate climate change
2	Natural disasters and extreme weather events	Failure of climate-change adaptation
3	Geoeconomic confrontation	Natural disasters and extreme weather events
4	Failure to mitigate climate change	Biodiversity loss and ecosystem collapse
5	Erosion of social cohesion and societal polarization	Large-scale involuntary migration
6	Large-scale environmental damage incidents	Natural resource crises
7	Failure of climate change adaptation	Erosion of social cohesion and societal polarization
8	Widespread cybercrime and cyber insecurity	Widespread cybercrime and cyber insecurity
9	Natural resource crises	Geoeconomic confrontation
10	Large-scale involuntary migration	Large-scale environmental damage incidents

Risk categories: Economic | Environmental | Geopolitical | Societal | Technological





Source: www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Figure 1: ENISA Threat Landscape 2022 - Prime threats

Source: ENISA Threat Landscape 2022

ภัยยุคก่อน	เทคโนโลยี	ภัยยุคไซเบอร์
 ลักทรัพย์	CCTV	แฮกขโมยข้อมูลที่เป็นทรัพย์สินสำคัญ (Hacking)
 หลอกขอข้อมูลทางโทรศัพท์	Cloud	หลอกขอข้อมูลทางอินเตอร์เน็ต (Phishing)
 กรรโชกทรัพย์	Internet	เรียกค่าไถ่ข้อมูล (Ransomware)
 การทุจริต	Mobile	ใช้อินเตอร์เน็ตเพื่อการทุจริต (Internet Fraud)
 ขโมยข้อมูลความเป็นตัวตน	Social Media	ขโมยข้อมูลความเป็นตัวตนเพื่อสวมรอย (Identity Theft)
 กลั่นแกล้ง	WiFi	กลั่นแกล้งทางไซเบอร์ (Cyber Bully)
	IoT	
	5G	

Top Ten Cybersecurity & Privacy Threats and Trends 2023

1. Security Awareness is Not Enough, Corporate needs to Cultivate Cyber Resilience Culture and Implement Cyber Attack Simulation
2. Adopt “Cyber Mindset” from “Are We Secure?” to “Are we Ready”
3. Digital Supply Chain @RISK
4. From “Cyber Drill” to “BAS” (Breach and Attack Simulation)
5. The Hidden Link between “Your Digital Footprint” & “Your Digital Identity”
6. From “Cyber Risk” to “Digital Risk” From “Digital Divide” to “Digital Inequality”
7. Preparing for “The Unknown Unknown Threats” Cyber Resilience : The Foundation of Digital Transformation Success
8. CIO & CISO need to be “Value Driven Professional”
9. Cybersecurity and DEI (Diversity, Equity, and Inclusion)
10. The Age of “Information Disorder”

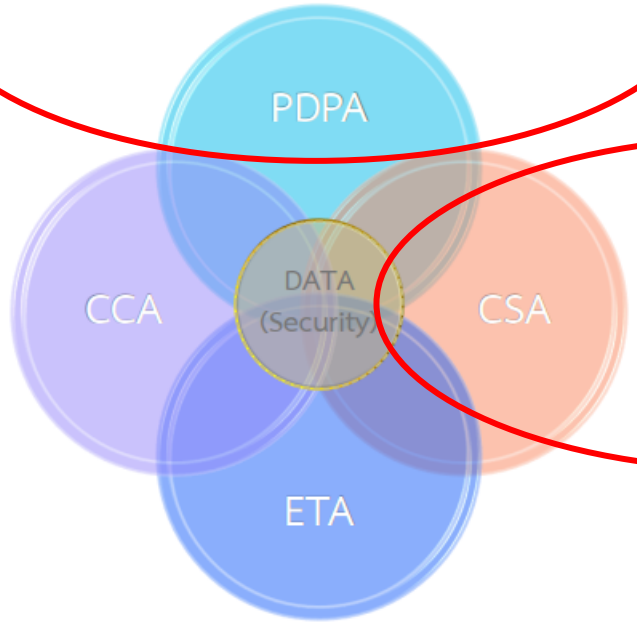
Overview of Cybersecurity Legal Regulations

2

ภาพรวมกฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ภาพรวมชุดกฎหมายดิจิทัล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
(Personal Data Protection Act)



พระราชบัญญัติ
ว่าด้วยการกระทำความผิด
เกี่ยวกับคอมพิวเตอร์
(Computer Crime Act)

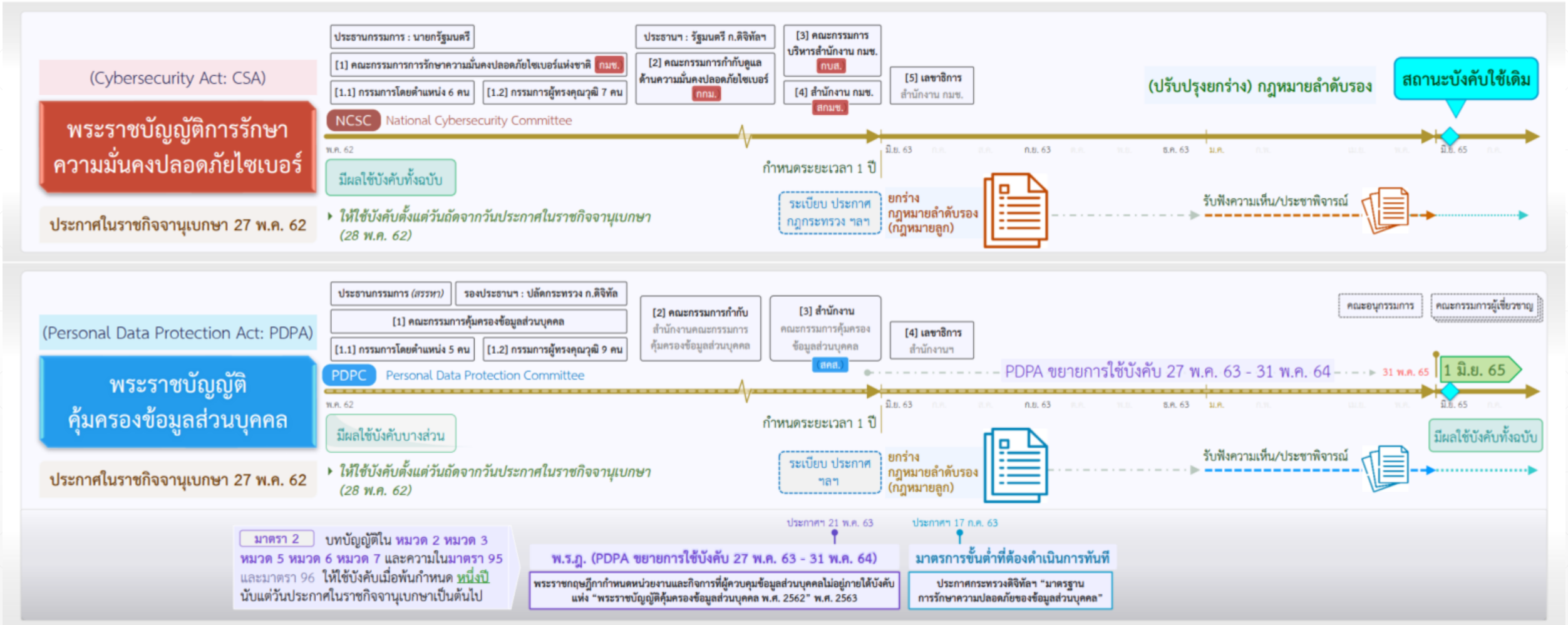
พระราชบัญญัติ
ความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Act)

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
(Electronic Transaction Act)

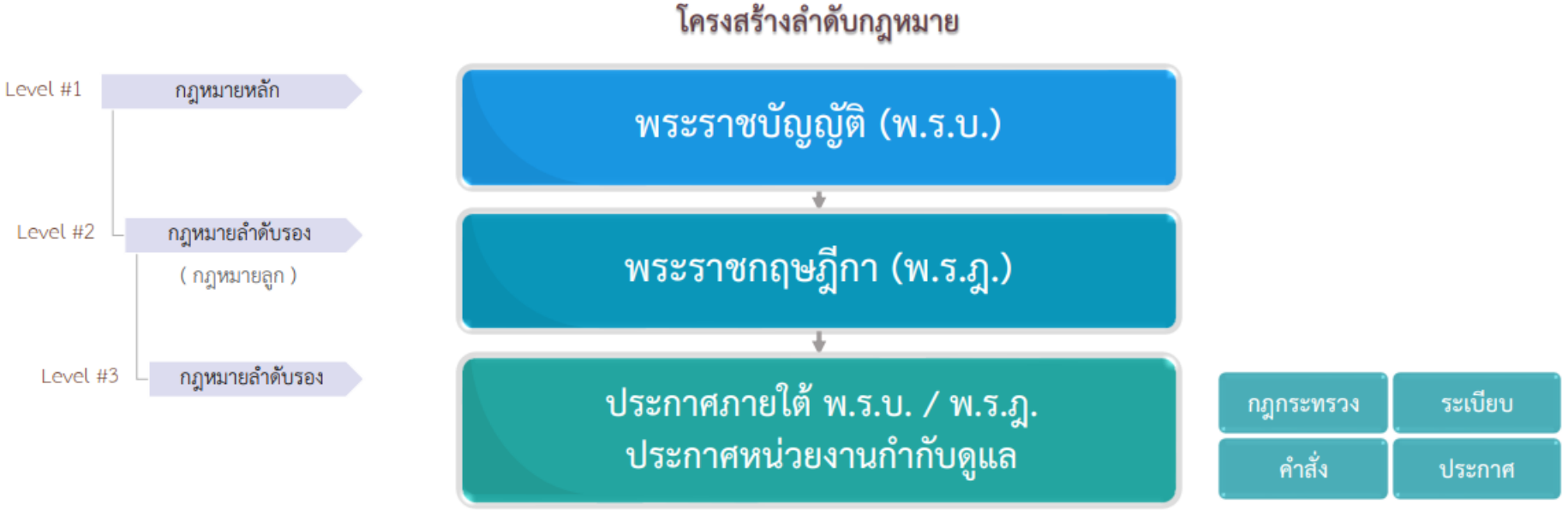
Digital Thailand	พระราชบัญญัติการพัฒนาดิจิทัล เพื่อเศรษฐกิจและสังคม
สภาดิจิทัลฯ	พระราชบัญญัติสภาดิจิทัล เพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
บริการภาครัฐระบบดิจิทัล	พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล
สพธอ. ETDA	พระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ภาพรวมการประกาศบังคับใช้กฎหมาย

“พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์” และ “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล”



ภาพรวมโครงสร้างลำดับกฎหมาย



หมายเหตุ: หน่วยงานกำกับดูแล

- คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.)
  สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
- คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กมช.)
  สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.)
- คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
  สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)
- ธนาคารแห่งประเทศไทย (ธปท.)
- คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)
- คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.)

ประโยชน์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ภาครัฐ

- ส่งเสริมภาพลักษณ์ประเทศ ให้ทัดเทียมนานาอารยประเทศในด้านกฎหมาย/กฎระเบียบในการคุ้มครองข้อมูลส่วนบุคคล
- มีมาตรการกำกับดูแลรวมถึงเครื่องมือกำกับการดำเนินงานการคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพ
- มีธรรมาภิบาลการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลมีความโปร่งใส ตรวจสอบได้
- สร้างสังคมที่เข็มแข็ง สามารถตรวจสอบการดำเนินงานภาครัฐและภาคธุรกิจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้มีความเหมาะสม

ภาคธุรกิจ

- เพิ่มความเชื่อมั่นในมาตรฐานการจัดเก็บ ใช้หรือเผยแพร่ข้อมูลส่วนบุคคลในระดับนานาชาติ
- เพิ่มขีดความสามารถและโอกาสในการทำธุรกิจที่มีการใช้ข้อมูลส่วนบุคคลร่วมกับต่างประเทศ
- มีกระบวนการทำงาน กลไกที่มีประสิทธิภาพในการคุ้มครองข้อมูลส่วนบุคคลขององค์กรที่เหมาะสม
- ส่งเสริมภาพลักษณ์องค์กรด้านธรรมาภิบาลการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลมีความโปร่งใส ตรวจสอบได้ รับผิดชอบต่อสังคม

ประชาชน

- มีสิทธิในการรับทราบวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล สิทธิให้/ถอนความยินยอม สิทธิขอเข้าถึง ขอลบข้อมูลส่วนบุคคลของตน
- ข้อมูลส่วนบุคคลได้รับการเก็บรักษาอย่างปลอดภัย และถูกใช้หรือเผยแพร่ภายใต้ขอบเขตวัตถุประสงค์ที่ได้รับแจ้ง และมีสิทธิร้องเรียนในกรณีที่พบว่ามีการใช้เกินขอบเขตวัตถุประสงค์
- ลดความเสียหาย ความเดือดร้อนอันเกิดจากการละเมิดข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือกฎหมาย PDPA (Personal Data Protection Act) มีผลบังคับใช้เมื่อวันที่ 1 มิ.ย. 2565

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
  - (ภาษาไทย)
    - พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
  - (Eng)
    - Personal Data Protection Act,B.E. 2562 (2019)
  - (คำอธิบาย)
    - สรุปสาระสำคัญพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
  - พระราชกฤษฎีกา
    - พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (สิ้นผลใช้บังคับแล้ว)
    - พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (ฉบับที่ ๒) พ.ศ. ๒๕๖๔ (สิ้นผลใช้บังคับแล้ว)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- กฎกระทรวง
- ระเบียบ
  - ระเบียบว่าด้วยหลักเกณฑ์และวิธีการสรรหาประธานกรรมการ และกรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓
  - ระเบียบว่าด้วยหลักเกณฑ์และวิธีการสรรหาประธานกรรมการและกรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (ฉบับที่ ๒) พ.ศ. ๒๕๖๔
  - ระเบียบคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ว่าด้วยการยื่น การไม่รับเรื่อง การยุติเรื่อง การพิจารณา และระยะเวลาในการพิจารณาคำร้องเรียน พ.ศ. ๒๕๖๕
- ข้อบังคับ
- ข้อกำหนด
- ประกาศ
  - ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓ (สิ้นผลใช้บังคับแล้ว)
  - ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (ฉบับที่ ๒) พ.ศ. ๒๕๖๔ (สิ้นผลใช้บังคับแล้ว)
  - ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. ๒๕๖๕
  - ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
  - ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
  - ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. ๒๕๖๕
  - ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง คุณสมบัติและลักษณะต้องห้าม วาระการดำรงตำแหน่ง การพ้นจากตำแหน่งและการดำเนินงานอื่นของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. ๒๕๖๕

https://www.mdes.go.th/law

มาตรการรักษาความมั่นคงปลอดภัย (Security Control)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในระยะแรกที่กฎหมายมีผลใช้บังคับมีความเหมาะสม

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“ความมั่นคงปลอดภัย” หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ข้อ ๔ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้

(๑) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

(๒) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล

(๓) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศ

มาตรการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล
(access control)

มาตรการบริหารจัดการสิทธิ
(right management control)

มาตรการตรวจสอบ
(audit trail)

สร้างเสริมความตระหนักรู้ด้านความสำคัญของ
การคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย
(privacy and security awareness)

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

เหตุผลและความจำเป็น

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ และเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ
ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

เพื่อให้สามารถป้องกันภัยคุกคามดังกล่าวได้อย่างทันท่วงที
โดยไม่ปล่อยให้นานจนเกิดผลกระทบกับประชาชน

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับ ตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา เป็นต้นไป

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

สาระสำคัญ

ประกาศในราชกิจจานุเบกษา
วันที่ 27 พฤษภาคม พ.ศ. 2562

เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที กำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งหน่วยงานของรัฐและหน่วยงานเอกชนที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

ผลใช้บังคับ

28 พฤษภาคม 2562 (ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป)

กลุ่มเป้าหมาย

หน่วยงานกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) และหน่วยงานรัฐ

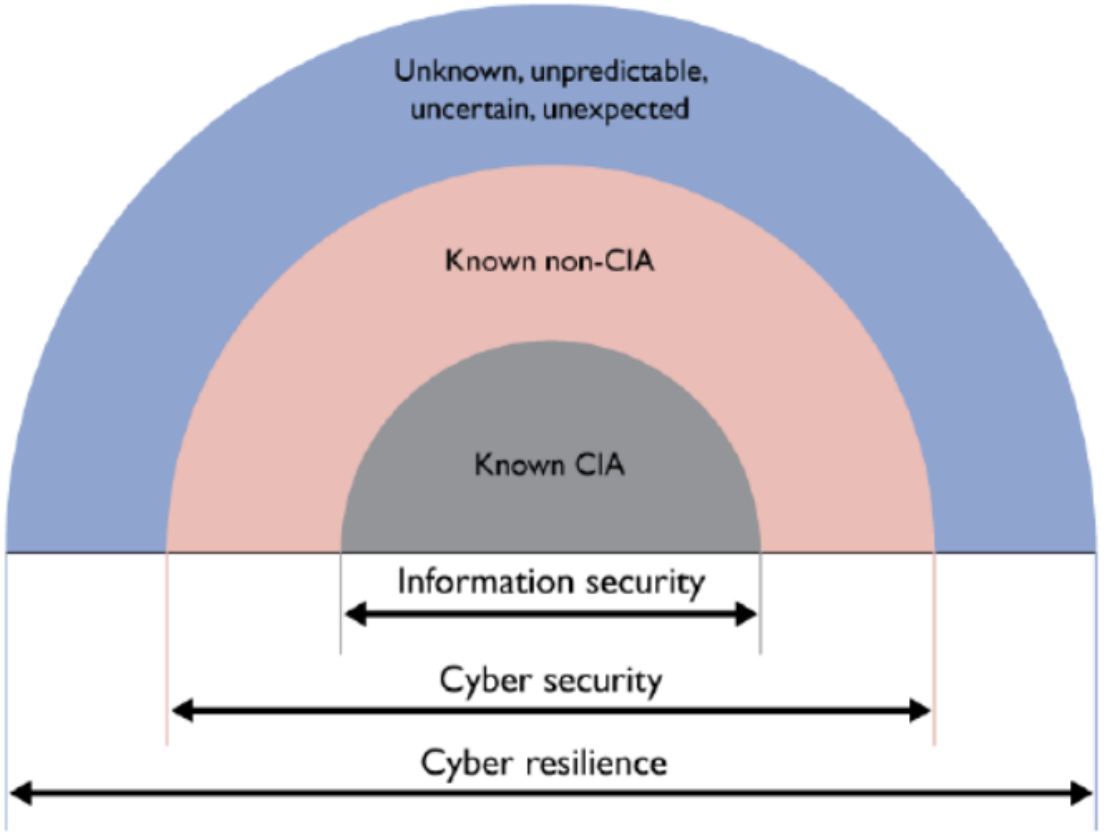
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

- **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒**
  - **(ภาษาไทย)**
    - พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒
  - **(Eng)**
    - Cybersecurity Act B.E.2562 (2019)
  - **(คำอธิบาย)**
    - สรุปสาระสำคัญของกฎหมาย
  - **พระราชกฤษฎีกา**
  - **กฎกระทรวง**
  - **ระเบียบ**
    - ระเบียบ กมช. ว่าด้วยหลักเกณฑ์การสรรหากรรมการผู้ทรงคุณวุฒิในคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๓
    - ระเบียบ กกม. ว่าด้วยการมอบอำนาจให้ปฏิบัติการแทน กกม. พ.ศ. ๒๕๖๕
  - **ข้อบังคับ**
  - **ข้อกำหนด**

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

- ประกาศ
  - ประกาศ กมช. เรื่อง หลักเกณฑ์การแต่งตั้งเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
  - ประกาศ กมช. เรื่อง การแต่งตั้งกรรมการผู้ทรงคุณวุฒิในคณะกรรมการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
  - ประกาศ กมช. ว่าด้วยหลักเกณฑ์และวิธีการสรรหากรรมการผู้ทรงคุณวุฒิในคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์
  - ประกาศ กมช. เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. ๒๕๖๔
  - ประกาศ กมช. เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔
  - ประกาศ กมช. เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. ๒๕๖๔
  - ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
  - ประกาศ กมช. เรื่อง การกำหนดระดับความรู้ความชำนาญฯ เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ พ.ศ. ๒๕๖๔
  - ประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ
  - ประกาศ กมช. เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)
  - ประกาศ กกม. เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖
  - ประกาศ สกมช. เรื่อง หลักเกณฑ์และอัตราค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน และค่าบริการในการดำเนินงาน พ.ศ. ๒๕๖๖

IT/Information Security, Cyber Security and Cyber Resilience



Source: "Cyber security strategies achieving cyber resilience", Information Security Forum (ISF), www.securityforum.org

IT/Information Security, Cyber Security and Cyber Resilience

คำศัพท์	คำอธิบาย
Cyber Resilience	หน่วยงาน Information Security Forum (ISF) แบ่งภัยคุกคามและวิธีรับมือออกเป็น 3 ส่วน ได้แก่ 1. **Information Security** หมายถึง ภัยคุกคามที่ส่งผลกระทบต่อ Confidentiality, Integrity และ Availability การรับมือกับภัยคุกคามนี้เรียกว่า **Known CIA** 2. **Cyber Security** คือ ภัยคุกคามที่ส่งผลกระทบต่อความเสี่ยงอื่น ที่นอกเหนือจาก CIA เช่น Authentication, Authorization การรับมือกับภัยคุกคามนี้เรียกว่า **Known non-CIA** 3. **Cyber Resillience** คือ ภัยคุกคามที่ไม่เคยพบมาก่อน ไม่สามารถทำนายได้ ไม่ชัดเจน หรือไม่คาดคิดมาก่อน เช่น การโจมตีแบบ Zero-day การรับมือกับภัยคุกคามนี้เรียกว่า **Unknown**  **ดังนั้น** Cyber Resilience **คือ** แนวทางในการเตรียมความพร้อมในการรับมือต่อภัยคุกคามทางไซเบอร์ เพื่อป้องกันความเสี่ยง (Protection) การตรวจจับความเสี่ยง (Detection) และการรับมือและฟื้นฟูความเสียหาย (Response and Recovery)

Source: "Cyber Resilience Assessment Framework ภายใต้หลักเกณฑ์การกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Management) ของสถาบันการเงิน" ธนาคารแห่งประเทศไทย

นิยามสำคัญ : ความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ได้บัญญัติคำนิยามไว้อย่างชัดเจน เกี่ยวกับ “ความมั่นคงปลอดภัยไซเบอร์” “ภัยคุกคามทางไซเบอร์” และในส่วนที่เกี่ยวข้อง

- “ไซเบอร์”
- “ภัยคุกคามทางไซเบอร์”
- “เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์”
- “การรักษาความมั่นคงปลอดภัยไซเบอร์”
- “ประมวลแนวทางปฏิบัติ”
- “มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์”
- **“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ”**
- **“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ”**
- **“หน่วยงานของรัฐ”**
- **“หน่วยงานควบคุมหรือกำกับดูแล”**
- **“พนักงานเจ้าหน้าที่”**
- **“คณะกรรมการ”** : คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

National Cyber Security Committee (NCSC)

นิยามสำคัญ : ความมั่นคงปลอดภัยไซเบอร์

"ไซเบอร์" หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

ไซเบอร์

- ข้อมูล / การสื่อสาร
- ที่เกิดจาก
  - (1) การให้บริการ หรือ การประยุกต์ใช้
    - เครือข่ายคอมพิวเตอร์
    - ระบบอินเทอร์เน็ต
    - โครงข่ายโทรคมนาคม
  - (2) รวมทั้ง การให้บริการ โดยปกติของ
    - ดาวเทียม
    - ระบบเครือข่าย
  - ที่คล้ายคลึงกัน
  - ที่เชื่อมต่อกันเป็นการทั่วไป

ภัยคุกคามทางไซเบอร์

- การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ
- โดยใช้
  - คอมพิวเตอร์
  - ระบบคอมพิวเตอร์
  - โปรแกรมไม่พึงประสงค์
- โดยมุ่งหมายให้
  - (1) เกิดการประทุษร้ายต่อ
    - ระบบคอมพิวเตอร์
    - ข้อมูลคอมพิวเตอร์
    - ข้อมูลอื่นที่เกี่ยวข้อง
  - (2) เป็นภยันตรายที่ใกล้จะถึง
    - ที่จะก่อให้เกิดความเสียหาย
    - ส่งผลกระทบต่อการทำงานของ
      - คอมพิวเตอร์
      - ระบบคอมพิวเตอร์
      - ข้อมูลอื่นที่เกี่ยวข้อง

"ภัยคุกคามทางไซเบอร์" หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

นิยามสำคัญ : ความมั่นคงปลอดภัยไซเบอร์

“เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของเครื่องคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

เหตุการณ์	ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบ	ซึ่งกระทำการผ่านทาง	คอมพิวเตอร์	ซึ่งอาจเกิด	ความเสียหาย	ต่อ	การรักษาความมั่นคงปลอดภัยไซเบอร์	เครื่องคอมพิวเตอร์
								ข้อมูลคอมพิวเตอร์
			ระบบคอมพิวเตอร์		ผลกระทบ		ความมั่นคงปลอดภัยไซเบอร์ของ	ระบบคอมพิวเตอร์
								ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

ประมวลแนวทางปฏิบัติ

ระเบียบ	ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนด
หลักเกณฑ์	

Code of practices

“ประมวลแนวทางปฏิบัติ” หมายความว่า ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนด

นิยามสำคัญ : ความมั่นคงปลอดภัยไซเบอร์

การรักษาความมั่นคงปลอดภัยไซเบอร์

"การรักษาความมั่นคงปลอดภัยไซเบอร์" หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

มาตรการ หรือการดำเนินการที่กำหนดขึ้น	เพื่อ	ป้องกัน / รับมือ / ลด	ความเสี่ยง	จากภัยคุกคามทางไซเบอร์	จากภายในประเทศ / จากภายนอกประเทศ	อันกระทบต่อ	ความมั่นคงของรัฐ / ความมั่นคงทางเศรษฐกิจ / ความมั่นคงทางทหาร / ความสงบเรียบร้อยภายในประเทศ

มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

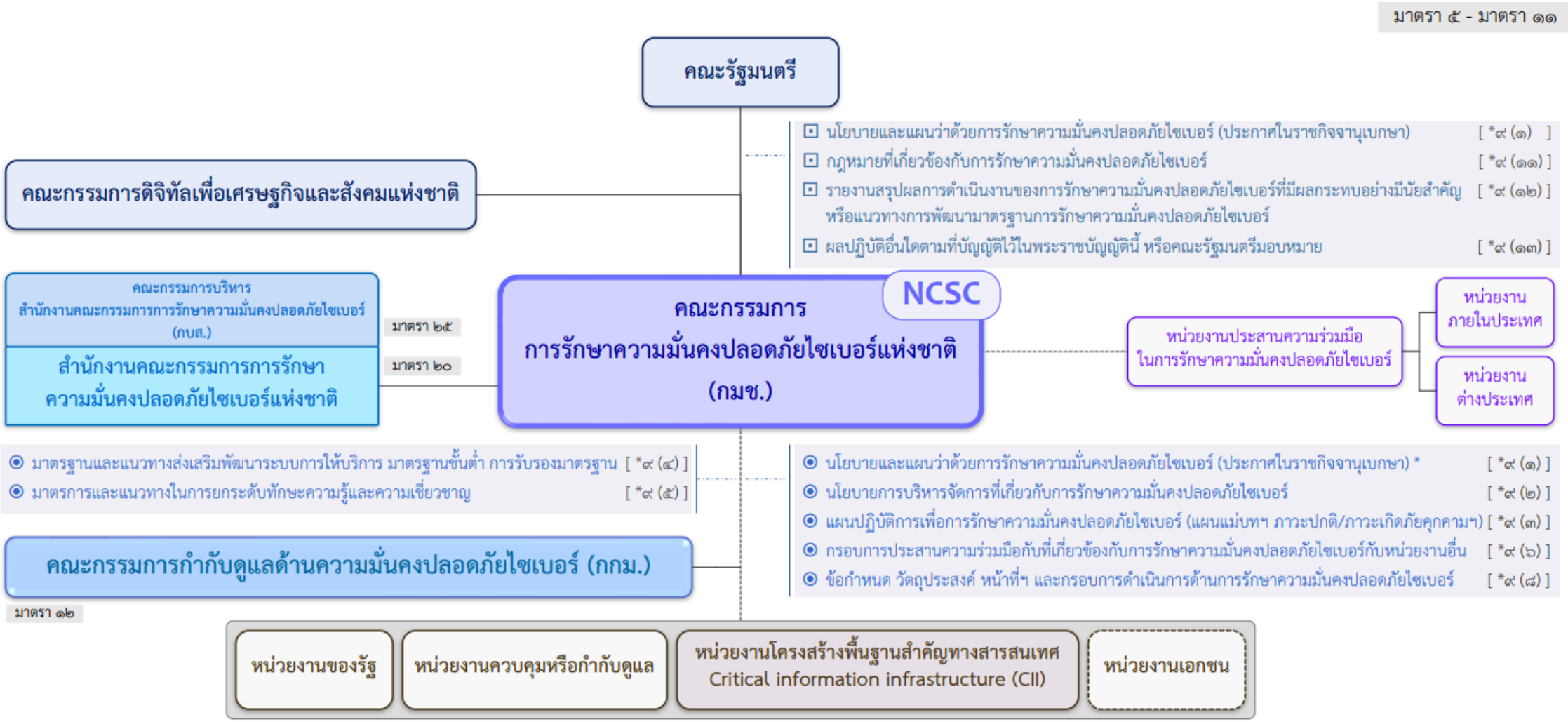
การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์	โดยใช้	บุคลากร / กระบวนการ / เทคโนโลยี	โดยผ่าน	คอมพิวเตอร์ / ระบบคอมพิวเตอร์ / โปรแกรมคอมพิวเตอร์ / บริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ	เพื่อสร้างความมั่นใจและเสริมสร้าง	ความมั่นคงปลอดภัยไซเบอร์ของ	คอมพิวเตอร์ / ข้อมูลคอมพิวเตอร์ / ข้อมูลอื่นที่เกี่ยวข้อง

"มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์" หมายความว่า การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจและเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

หน่วยงานที่มีบทบาทหน้าที่ ตามที่ พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนด

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	หน่วยงานของรัฐ	หน่วยงานควบคุมหรือกำกับดูแล
หน่วยงานของรัฐหรือ หน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ	หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงสร้างที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์



คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

มาตรา ๑๒ - มาตรา ๑๙

หน้าที่และอำนาจ

มาตรา ๑๓ (๓)

กำกับดูแลการดำเนินงาน

เพื่อรับมือกับภัยคุกคามทางไซเบอร์ได้ทันท่วงที กกม. อาจมอบอำนาจให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ผู้บัญชาการทหารสูงสุด และกรรมการอื่นซึ่ง กกม. กำหนด *ร่วมกันปฏิบัติการ* ในเรื่องดังกล่าวได้ และจะกำหนดให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่ถูกคุกคามเข้าร่วมดำเนินการประสานงาน และให้การสนับสนุนด้วยก็ได้

- ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
- การเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์

การปฏิบัติตามวรรคหนึ่ง ให้เป็นไปตามระเบียบที่ กกม. กำหนด

มาตรา ๑๓ (๔)

กำหนด

(ข้อกำหนด)

(มาตรฐานขั้นต่ำ)

- ประมวลแนวทางปฏิบัติ
- กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์(ผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ)

มาตรา ๑๖

มีอำนาจแต่งตั้ง คณะอนุกรรมการเพื่อปฏิบัติการอย่างใดอย่างหนึ่งตามที่ กกม. มอบหมาย

NIST Cybersecurity Framework

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (NCERT)

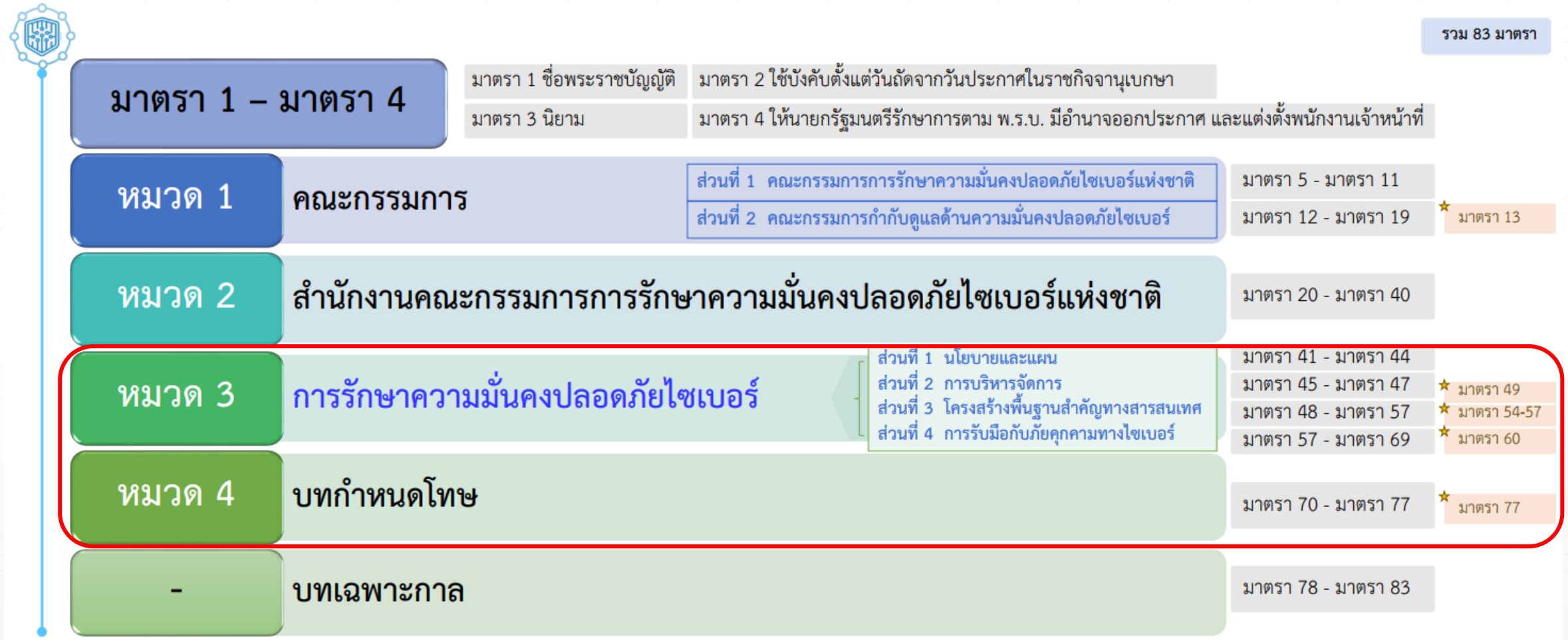
NCERT

National Computer Emergency Response Team

- TB-CERT — Thailand Banking Sector CERT
- TCM-CERT — Thai Capital Market CERT
- TTC-CERT — Thailand Telecommunication CERT
- TI-CERT — Thai Insurance CERT

Thailand Sector-based CERT

สาระสำคัญของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ มีอะไรบ้าง



สาระสำคัญของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ มีอะไรบ้าง

หมวด ๓ • การรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๑ นโยบายและแผน
มาตรา ๔๑ - มาตรา ๔๔

การใช้สัญลักษณ์ : ผู้สั่งการ : ผู้ติดตาม/ผู้ตรวจสอบ : ผู้ปฏิบัติตาม : การรายงานผล

กมช.	กกม.	สนง. กมช.	หน่วยงานของรัฐ	หน่วยงานควบคุมหรือกำกับดูแล	หน่วยงานโครงสร้างพื้นฐานสำคัญฯ

มาตรา ๔๑ การรักษาความมั่นคงปลอดภัยไซเบอร์ต้องคำนึงถึงความเป็นเอกภาพและการบูรณาการในการดำเนินงานของหน่วยงานของรัฐและหน่วยงานเอกชน และต้องสอดคล้องกับ นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

๙(๑)

มาตรา ๔๒ นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีเป้าหมาย และแนวทาง

๙(๑) ๑๓(๑)

มาตรา ๔๓ จัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นตามแนวทางในมาตรา ๔๒ -> ประกาศในราชกิจจานุเบกษา ->ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามที่กำหนดไว้ในแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ดำเนินการให้เป็นไปตามนโยบายและแผนดังกล่าว

๙(๑)

มาตรา ๔๔ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

๙(๑)

สาระสำคัญของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ มีอะไรบ้าง

หมวด ๓ • การรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๒ การบริหารจัดการ
มาตรา ๔๕ - มาตรา ๔๗

การใช้สัญลักษณ์ : ผู้สั่งการ : ผู้ติดตาม/ผู้ตรวจสอบ : ผู้ปฏิบัติตาม : การรายงานผล

กมช.	กกม.	สนง. กมช.	หน่วยงานของรัฐ	หน่วยงานควบคุมหรือกำกับดูแล	หน่วยงานโครงสร้างพื้นฐานสำคัญฯ

มาตรา ๔๕ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ของหน่วยงาน และให้เป็นไปตามประมวลฯ ตามมาตรา ๑๓ วรรคหนึ่ง (๔)

(ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งกำหนดโดย กกม.... กรอบมาตรฐานฯ อย่างน้อยต้องประกอบด้วยวิธีการและมาตรการ... ๑๓ วรรคสอง Identify, Protect, Detect, Response, Recovery)

๙(๒) ๑๓(๔) ๑๓(๕)

มาตรา ๔๖ แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน

๙(๒)

มาตรา ๔๗ ในกรณีที่การปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ต้องอาศัยความรู้ ความเชี่ยวชาญคณะกรรมการหรือ กกม. อาจมอบหมายให้เลขาธิการว่าจ้างผู้เชี่ยวชาญตามความเหมาะสมเฉพาะงานได้

๙(๒)

สาระสำคัญของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ มีอะไรบ้าง

หมวด ๓ • การรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๓ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
มาตรา ๔๘ - มาตรา ๕๗

การใช้สัญลักษณ์ : ผู้สั่งการ : ผู้ติดตาม/ผู้ตรวจสอบ : ผู้ปฏิบัติตาม : การรายงานผล

กมช.	กกม.	สนง. กมช.	หน่วยงานของรัฐ	หน่วยงานควบคุมหรือกำกับดูแล	หน่วยงานโครงสร้างพื้นฐานสำคัญฯ

มาตรา ๔๘ โครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นกิจการที่มีความสำคัญต่อความมั่นคงของรัฐ เป็นหน้าที่ของสำนักงานในการสนับสนุนและให้ความช่วยเหลือ

มาตรา ๔๙ ประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ... เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ...

มาตรา ๕๐ ประกาศกำหนดลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ โดยจะกำหนดให้หน่วยงานของรัฐที่มีความพร้อมหรือหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ๆ ทำหน้าที่ดังกล่าวให้แก่หน่วยงานโครงสร้างพื้นฐานฯตามมาตรา ๔๙ ทั้งหมดหรือบางส่วนก็ได้

๑๓(๓)

มาตรา ๕๑ กรณีมีข้อสงสัยหรือข้อโต้แย้งเกี่ยวกับลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านที่มีการประกาศกำหนดตามมาตรา ๔๙ หรือมาตรา ๕๐ ให้คณะกรรมการเป็นผู้วินิจฉัยชี้ขาด

สาระสำคัญของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ มีอะไรบ้าง

หมวด ๓ • การรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๓ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
มาตรา ๔๘ - มาตรา ๕๗

การใช้สัญลักษณ์ : ผู้สั่งการ : ผู้ติดตาม/ผู้ตรวจสอบ : ผู้ปฏิบัติตาม : การรายงานผล

กมช.	กกม.	สนง. กมช.	หน่วยงานของรัฐ	หน่วยงานควบคุมหรือกำกับดูแล	หน่วยงานโครงสร้างพื้นฐานสำคัญฯ

มาตรา ๕๒ แจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์และผู้ดูแลระบบคอมพิวเตอร์ไปยังสำนักงาน หน่วยงานควบคุมหรือกำกับดูแลของตน และหน่วยงานตามมาตรา ๕๐ ภายในสามสิบวันนับแต่วันที่คณะกรรมการประกาศตามมาตรา ๔๙ วรรคสอง และมาตรา ๕๐ วรรคสอง ในกรณีที่มีการเปลี่ยนแปลง ให้แจ้งการเปลี่ยนแปลงไปยังหน่วยงานที่เกี่ยวข้องตามวรรคหนึ่งก่อนการเปลี่ยนแปลงล่วงหน้าไม่น้อยกว่าเจ็ดวัน

มาตรา ๕๓ ตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน หากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นยังคงเพิกเฉยไม่ดำเนินการหรือไม่ดำเนินการให้แล้วเสร็จภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด ให้หน่วยงานควบคุมหรือกำกับดูแลส่งเรื่องให้ กกม.

มาตรา ๕๔ จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละหนึ่งครั้ง รายงานสำนักงานภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ

สาระสำคัญของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ มีอะไรบ้าง

หมวด ๓ • การรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๓ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
มาตรา ๔๘ - มาตรา ๕๗

การใช้สัญลักษณ์ : ผู้สั่งการ : ผู้ติดตาม/ผู้ตรวจสอบ : ผู้ปฏิบัติตาม : การรายงานผล

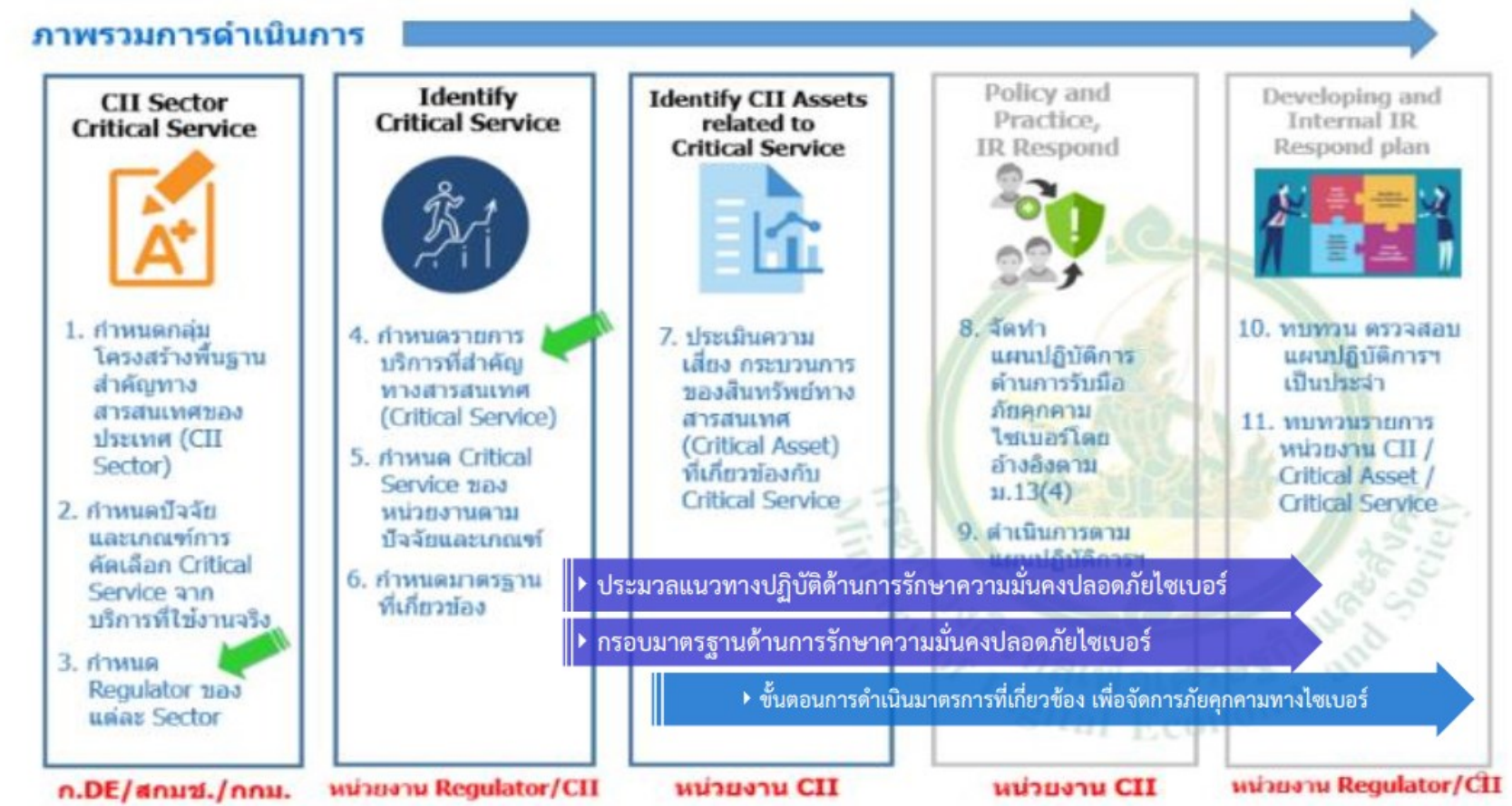
กมช.	กกม.	สนง. กมช.	หน่วยงานของรัฐ	หน่วยงานควบคุมหรือกำกับดูแล	หน่วยงานโครงสร้างพื้นฐานสำคัญฯ

มาตรา ๕๒ แจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์และผู้ดูแลระบบคอมพิวเตอร์ไปยังสำนักงาน หน่วยงานควบคุมหรือกำกับดูแลของตน และหน่วยงานตามมาตรา ๕๐ ภายในสามสิบวันนับแต่วันที่คณะกรรมการประกาศตามมาตรา ๔๙ วรรคสอง และมาตรา ๕๐ วรรคสอง ในกรณีที่มีการเปลี่ยนแปลง ให้แจ้งการเปลี่ยนแปลงไปยังหน่วยงานที่เกี่ยวข้องตามวรรคหนึ่งก่อนการเปลี่ยนแปลงล่วงหน้าไม่น้อยกว่าเจ็ดวัน

มาตรา ๕๓ ตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน หากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นยังคงเพิกเฉยไม่ดำเนินการหรือไม่ดำเนินการให้แล้วเสร็จภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด ให้หน่วยงานควบคุมหรือกำกับดูแลส่งเรื่องให้ กกม.

มาตรา ๕๔ จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละหนึ่งครั้ง รายงานสำนักงานภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ

แนวทางกำหนดหลักเกณฑ์บริการที่จัดเป็น Critical Services สำหรับหน่วยงานควบคุมกำกับดูแลหรือดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ



ขั้นตอนการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

:: ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

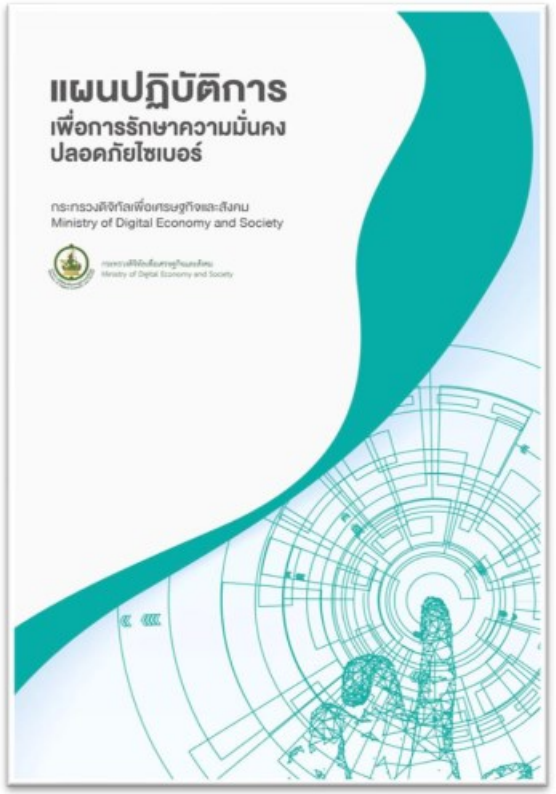
- แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- แผนการรับมือภัยคุกคามไซเบอร์

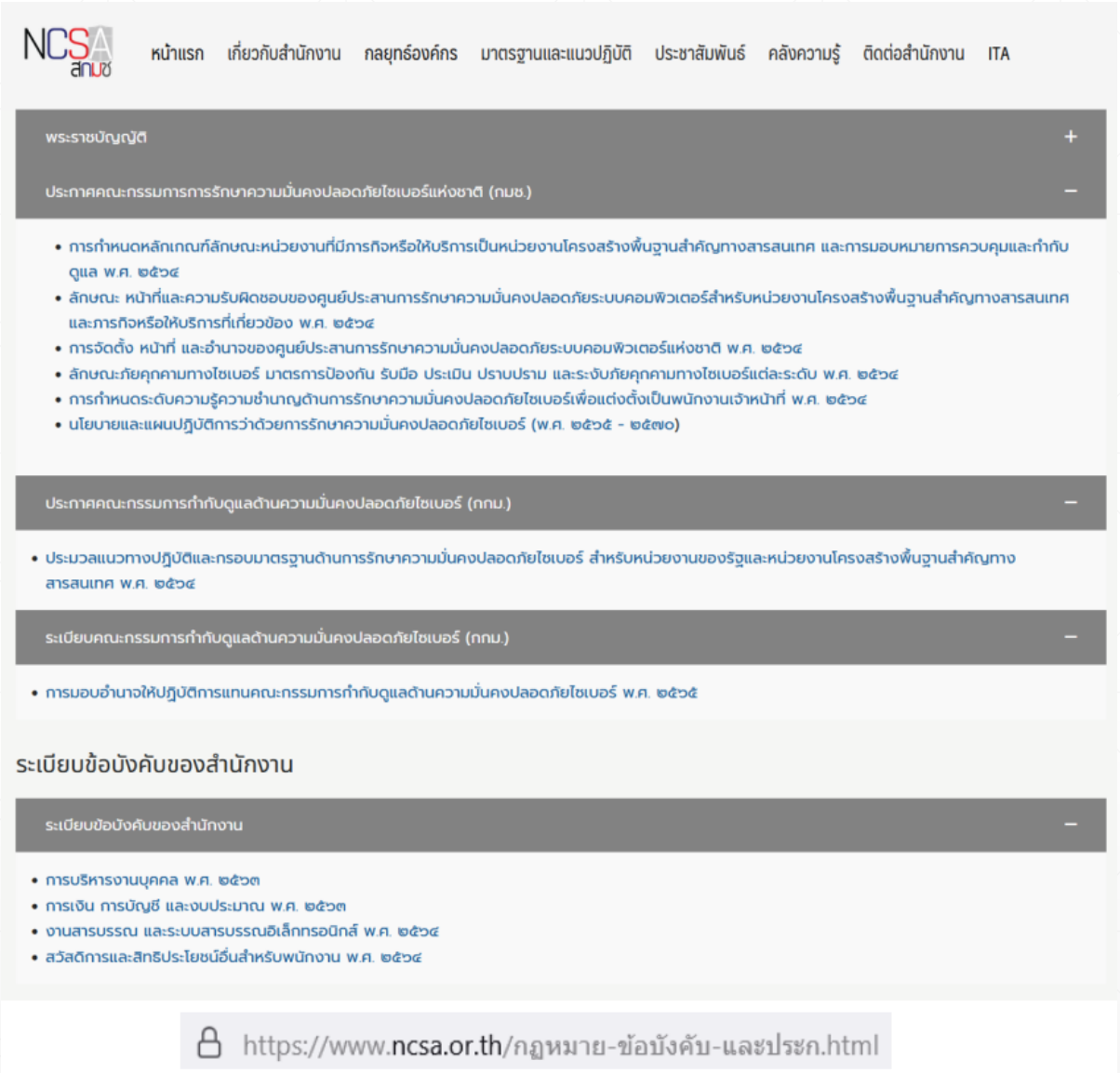
:: กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

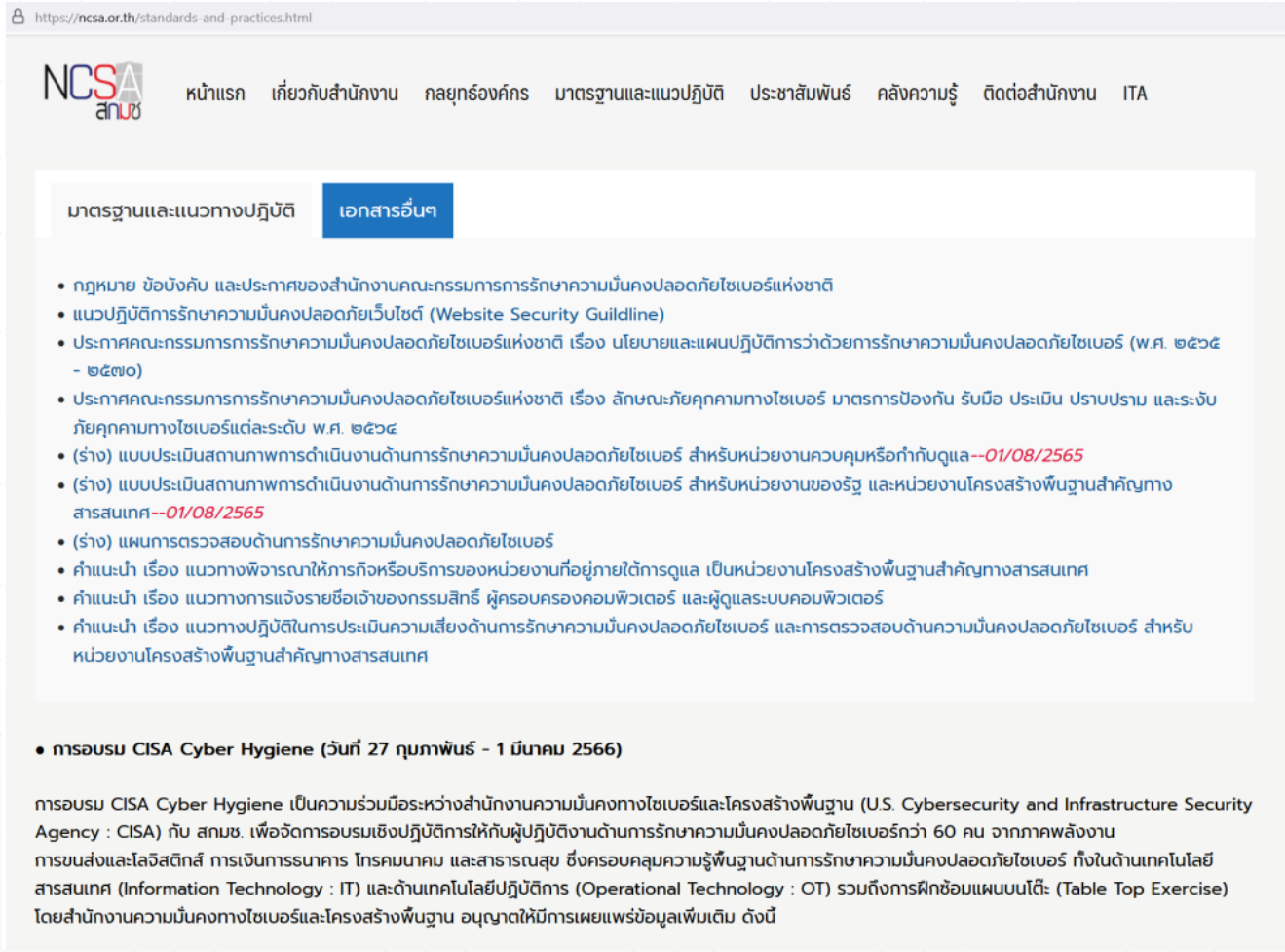
- Identify
- Pretect
- Detect
- Respond
- Recover

สถานะของการประกาศใช้บังคับ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

(ฉบับยกร่าง เพื่อนำเสนอ สกมช. กกม. กมช. ช่วงปี พ.ศ. 2564)

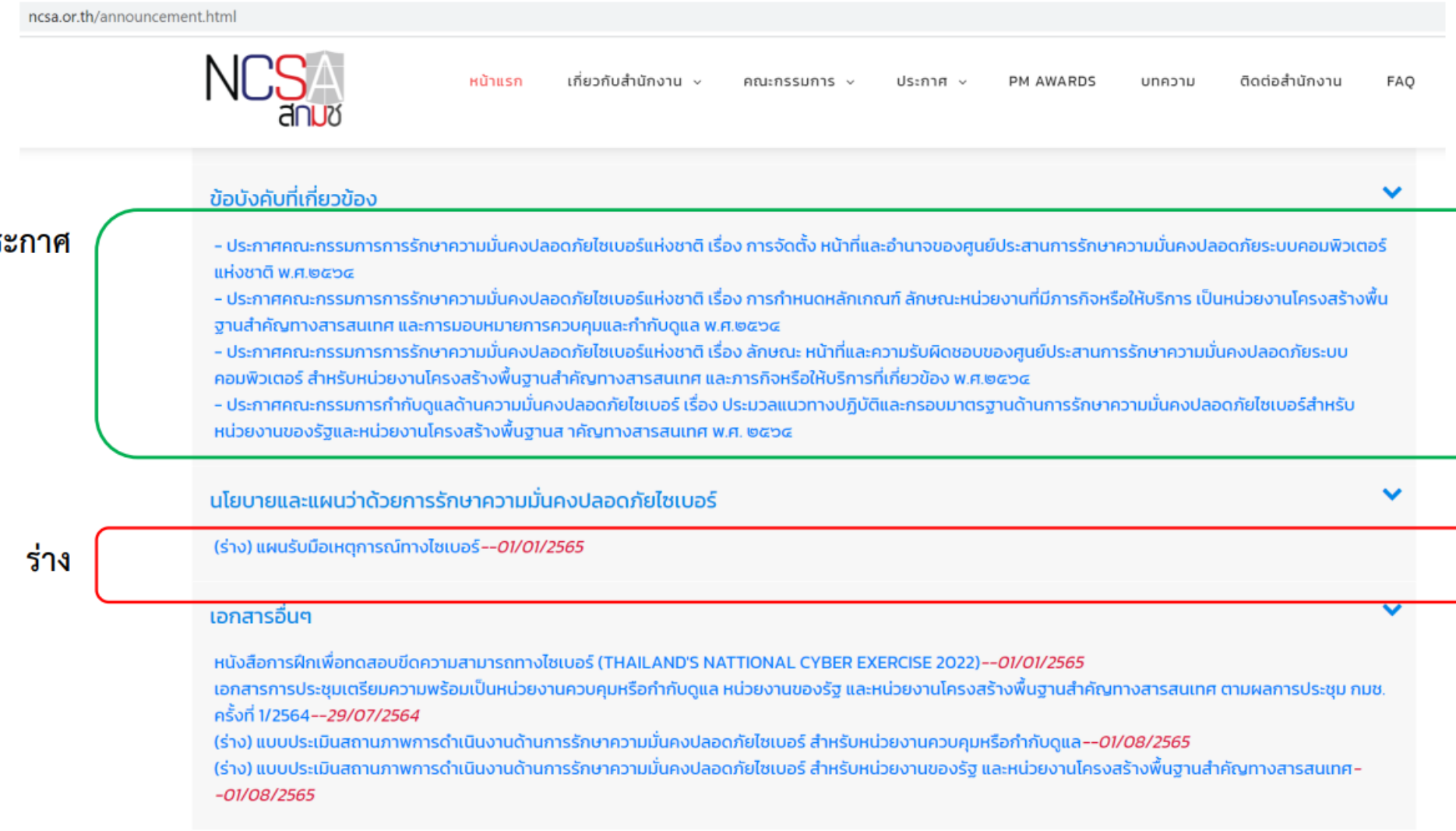






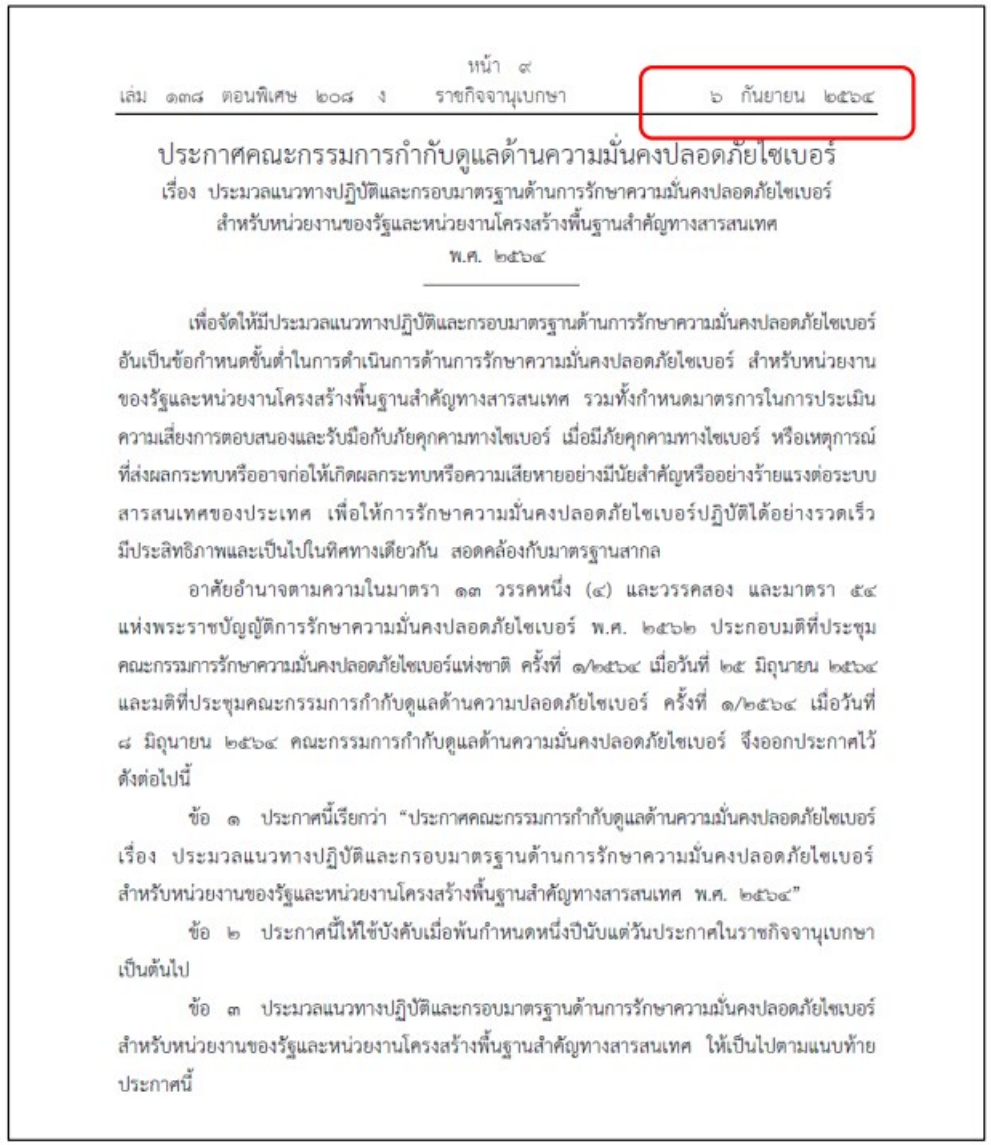
• การอบรม CISA Cyber Hygiene (วันที่ 27 กุมภาพันธ์ - 1 มีนาคม 2566)

การอบรม CISA Cyber Hygiene เป็นความร่วมมือระหว่างสำนักงานความมั่นคงทางไซเบอร์และโครงสร้างพื้นฐาน (U.S. Cybersecurity and Infrastructure Security Agency : CISA) กับ สกมช. เพื่อจัดการอบรมเชิงปฏิบัติการให้กับผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กว่า 60 คน จากภาคพลังงาน การขนส่งและโลจิสติกส์ การเงินการธนาคาร โทรคมนาคม และสาธารณสุข ซึ่งครอบคลุมความรู้พื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งในด้านเทคโนโลยีสารสนเทศ (Information Technology : IT) และด้านเทคโนโลยีปฏิบัติการ (Operational Technology : OT) รวมถึงการฝึกซ้อมแผนบนโต๊ะ (Table Top Exercise) โดยสำนักงานความมั่นคงทางไซเบอร์และโครงสร้างพื้นฐาน อนุญาตให้มีการเผยแพร่ข้อมูลเพิ่มเติม ดังนี้


ncsa.or.th/announcement.html
NCSA สกมช
หน้าแรก
เกี่ยวกับสำนักงาน
คณะกรรมการ
ประกาศ
PM AWARDS
บทความ
ติดต่อสำนักงาน
FAQ
ข้อบังคับที่เกี่ยวข้อง
ประกาศ
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ.๒๕๖๔
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ.๒๕๖๔
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ.๒๕๖๔
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานส าคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
ร่าง
(ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์--01/01/2565
เอกสารอื่นๆ
หนังสือการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ (THAILAND'S NATTIONAL CYBER EXERCISE 2022)--01/01/2565
เอกสารการประชุมเตรียมความพร้อมเป็นหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามผลการประชุม กมช. ครั้งที่ 1/2564--29/07/2564
(ร่าง) แบบประเมินสถานภาพการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานควบคุมหรือกำกับดูแล--01/08/2565
(ร่าง) แบบประเมินสถานภาพการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ--01/08/2565

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564



ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

เพื่อจัดให้มีประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยงการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๑๓ วรรคหนึ่ง (๔) และวรรคสอง และมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบมติที่ประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๑/๒๕๖๔ เมื่อวันที่ ๒๕ มิถุนายน ๒๕๖๔ และมติที่ประชุมคณะกรรมการกำกับดูแลด้านความปลอดภัยไซเบอร์ ครั้งที่ ๑/๒๕๖๔ เมื่อวันที่ ๘ มิถุนายน ๒๕๖๔ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔"

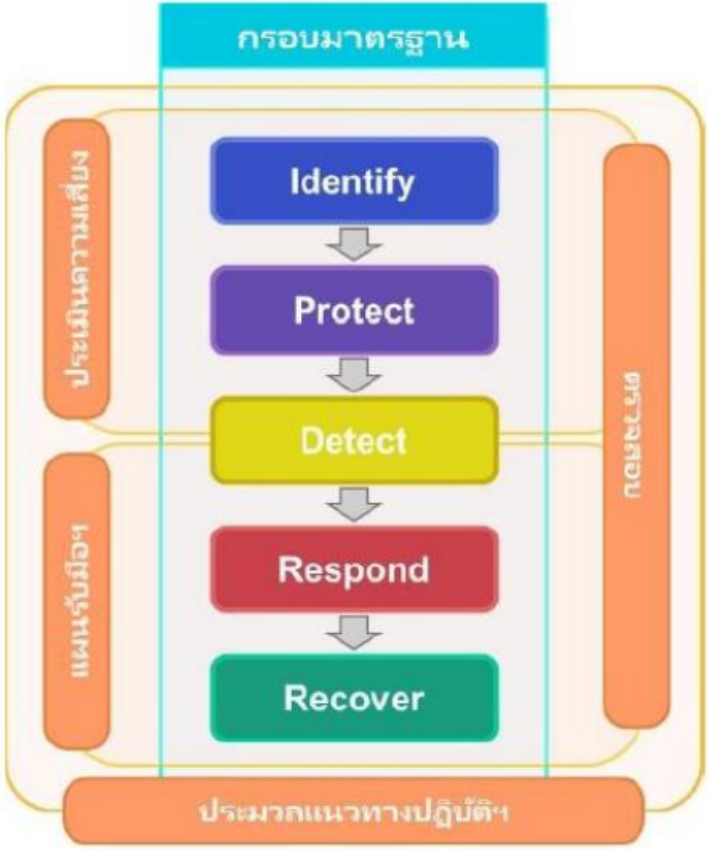
ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้เป็นไปตามแนบท้ายประกาศนี้

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

ประมวลแนวทางปฏิบัติ

- แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- แผนการรับมือภัยคุกคามทางไซเบอร์



แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

17.1 ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง*

โดยมีขอบเขตของการตรวจสอบ ดังนี้

(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

(ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (ก)

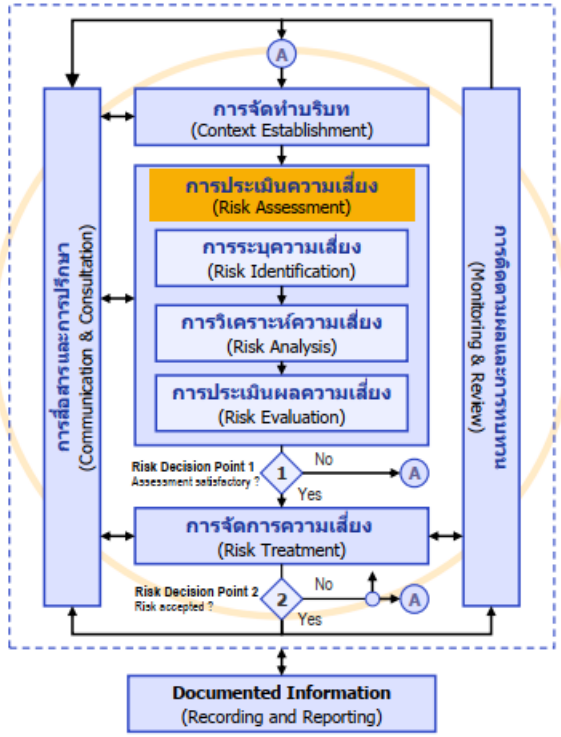
(ค) การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด

*หน่วยงานรัฐ, หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

17.2 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการ ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด 30 วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา 54 พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย

การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้



18.1 การประเมินความเสี่ยง (Risk Assessment)

(ก) การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุ มาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

(ข) การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

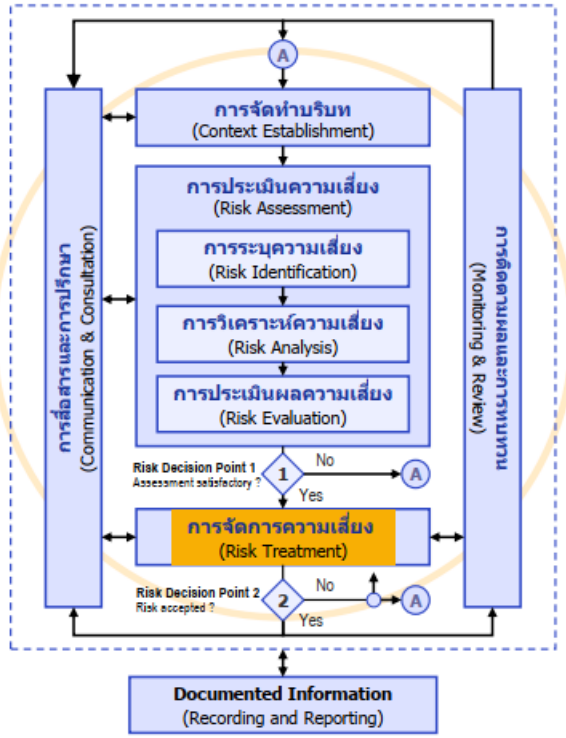
(ค) การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ต่อ)

18.2 การจัดการความเสี่ยง (Risk Treatment)

ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง



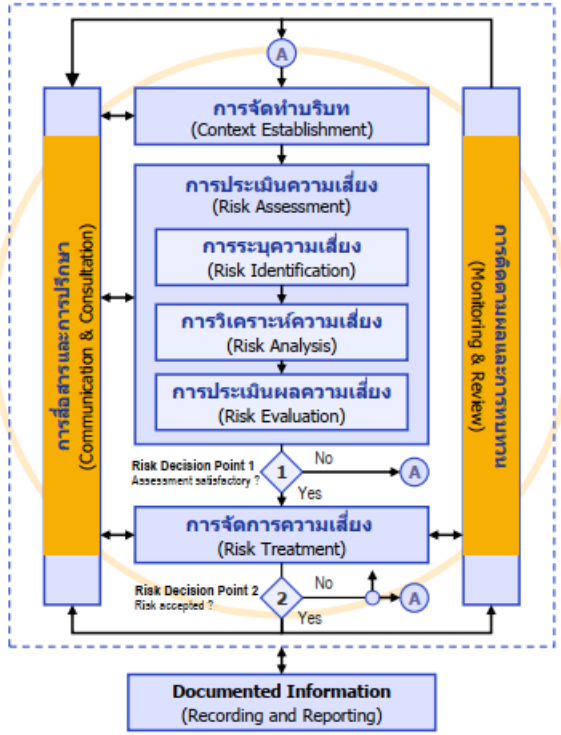
การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ต่อ)

18.3 การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

18.4 การรายงานความเสี่ยง (Risk Reporting)

ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงานที่ได้รับมอบหมายทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น



แผนการรับมือภัยคุกคามทางไซเบอร์

19.1 ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ

(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

แผนการรับมือภัยคุกคามทางไซเบอร์

19.1 ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้ (ต่อ)

(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ

(ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

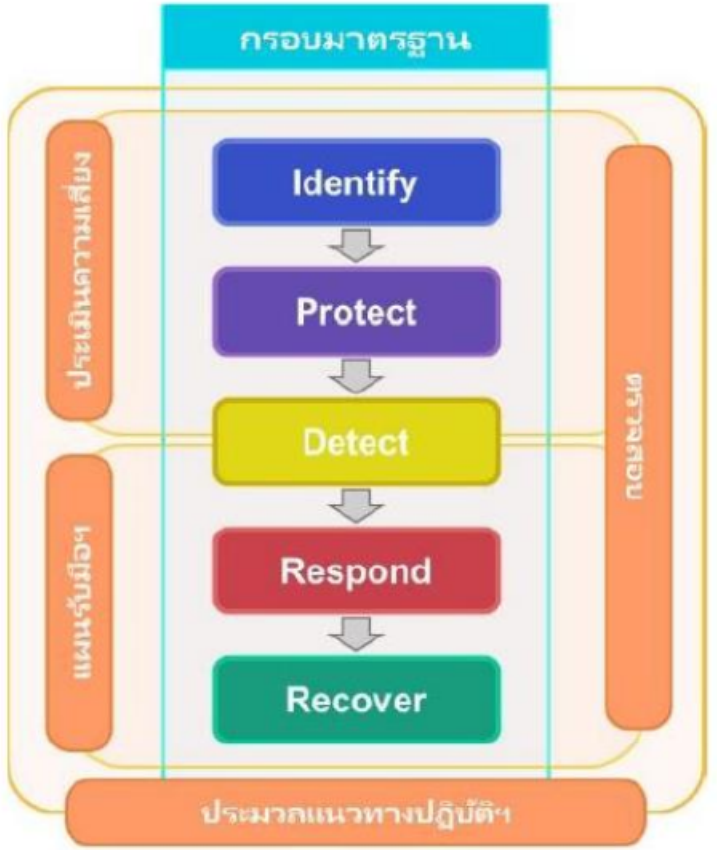
การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)



สารบัญ

เอกสารนี้เป็นเพียงผลการศึกษา อยู่ระหว่างเสนอคณะกรรมการพิจารณา

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

1. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)

2. การบริหารความเสี่ยง (Risk Management)

3. นโยบาย และแนวปฏิบัติ (Policies and Guidelines)

การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์
(Good Governance in Cybersecurity)

2.1.2 การกำหนดให้มีผู้รับผิดชอบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

หน่วยงานของรัฐต้องจัดให้มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่าที่ปฏิบัติหน้าที่ของหน่วยงานโดยบุคคลดังกล่าวต้องเป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือกับภัยคุกคามทางไซเบอร์

2.1.3 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงาน

การบริหารความเสี่ยง (Risk Management)

2.2.1 ต้องจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษรกรอบจะรวมถึง:

(1) ระบุเกณฑ์ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และระดับความเสี่ยงที่ยอมรับได้ (Risk appetite)

(2) วิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และ

(3) การเฝ้าระวังและติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

2.2.2 ต้องเก็บรักษารายการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในทะเบียนความเสี่ยง (Risk register) ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

2.2.3 ต้องติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้อย่างสม่ำเสมอเพื่อให้แน่ใจว่าอยู่ภายใต้เกณฑ์ระดับความเสี่ยงที่ยอมรับได้ที่ระบุไว้ในข้อ 2.2 (1)

นโยบาย และแนวปฏิบัติ (Policies and Guidelines)

2.3.1 ต้องกำหนด และอนุมัตินโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จากภัยคุกคามทางไซเบอร์นโยบาย มาตรฐาน และแนวปฏิบัติจะต้อง:

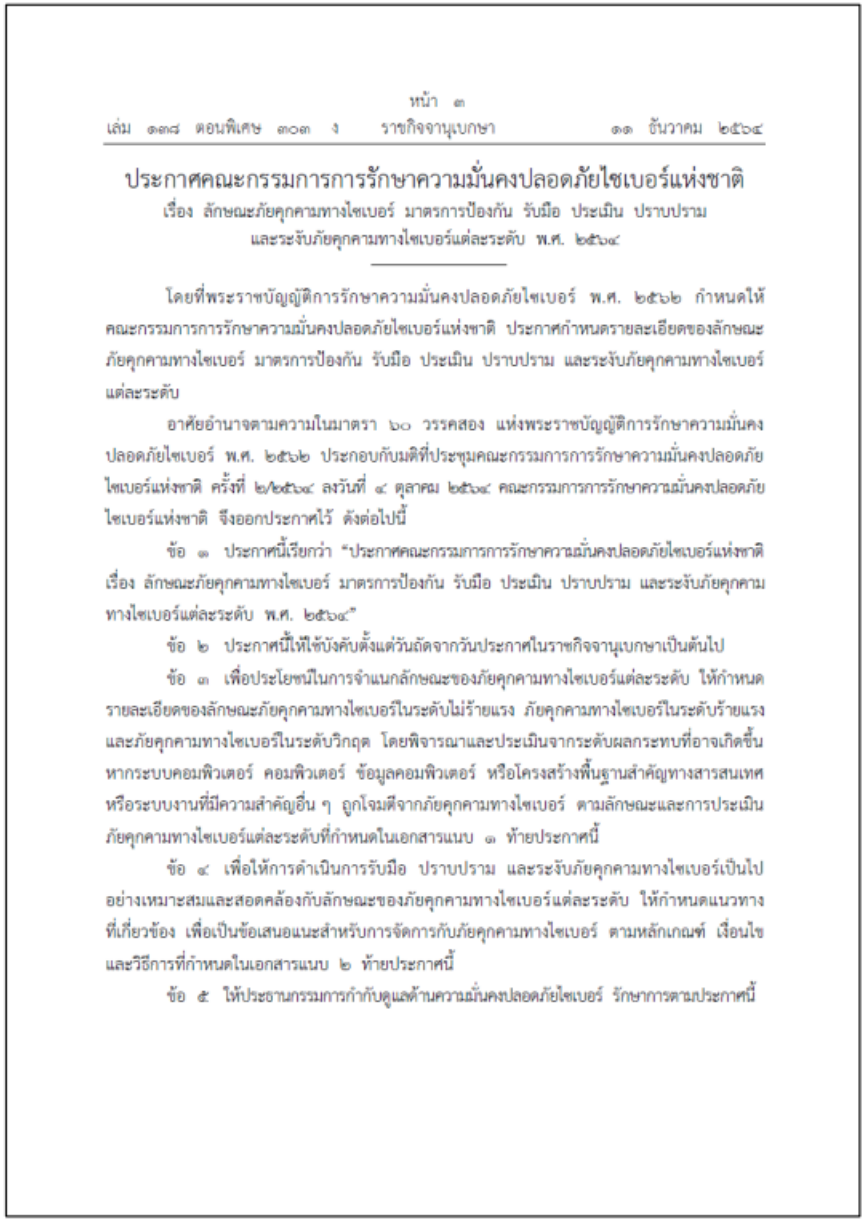
(1) สอดคล้องกับหลักประมวลแนวทางปฏิบัตินี้ ข้อกำหนดการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วน และนโยบาย มาตรฐาน และทิศทางการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับภูมิภาค หรือระดับประเทศ และ

(2) เผยแพร่และสื่อสารไปยังบุคลากรและบุคคลภายนอกทุกคนที่ทำหน้าที่หรือสามารถเข้าถึงบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

2.3.2 ต้องทบทวนนโยบาย มาตรฐาน และแนวทางปฏิบัติกับสภาพแวดล้อมการปฏิบัติการไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภูมิทัศน์ภัยคุกคามทางไซเบอร์ในปัจจุบันอย่างน้อยปีละหนึ่ง (1) ครั้ง โดยนับถัดจากวันที่การทบทวนครั้งสุดท้ายหรือวันที่มีผลบังคับใช้ของนโยบาย มาตรฐาน หรือแนวปฏิบัติแต่ละข้อ

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564



หน้า ๓
เล่ม ๑๓๘ ตอนพิเศษ ๓๐๓ ง ราชกิจจานุเบกษา ๑๑ ธันวาคม ๒๕๖๔

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประกาศกำหนดรายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

อาศัยอำนาจตามความในมาตรา ๖๐ วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๒/๒๕๖๔ ลงวันที่ ๔ ตุลาคม ๒๕๖๔ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ เพื่อประโยชน์ในการจำแนกลักษณะของภัยคุกคามทางไซเบอร์แต่ละระดับ ให้กำหนดรายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤต โดยพิจารณาและประเมินจากระดับผลกระทบที่อาจเกิดขึ้นหากระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือระบบงานที่มีความสำคัญอื่น ๆ ถูกโจมตีจากภัยคุกคามทางไซเบอร์ ตามลักษณะและการประเมินภัยคุกคามทางไซเบอร์แต่ละระดับที่กำหนดในเอกสารแนบ ๑ ท้ายประกาศนี้

ข้อ ๔ เพื่อให้การดำเนินการรับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์เป็นไปอย่างเหมาะสมและสอดคล้องกับลักษณะของภัยคุกคามทางไซเบอร์แต่ละระดับ ให้กำหนดแนวทางที่เกี่ยวข้อง เพื่อเป็นข้อเสนอแนะสำหรับการจัดการกับภัยคุกคามทางไซเบอร์ ตามหลักเกณฑ์ เงื่อนไข และวิธีการที่กำหนดในเอกสารแนบ ๒ ท้ายประกาศนี้

ข้อ ๕ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ รักษาการตามประกาศนี้

ลักษณะภัยคุกคามทางไซเบอร์ และปัจจัยที่ใช้ในการประเมินภัยคุกคามทางไซเบอร์แต่ละระดับ

ในการพิจารณาระบุระดับของภัยคุกคามทางไซเบอร์ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรพิจารณาจากเหตุการณ์ต่าง ๆ ที่เป็นพฤติการณ์แวดล้อม ผลกระทบที่เกิดขึ้น ความเสี่ยงหรือแนวโน้มที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ในกรณีต่าง ๆ เพื่อพิจารณาว่าลักษณะของภัยคุกคามทางไซเบอร์นั้นอยู่ในระดับใด โดยให้พิจารณาจากปัจจัยที่ใช้ในการประเมินทั้ง ๔ ปัจจัย ดังนี้

(๑) ลักษณะผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน

(๒) ลักษณะผลกระทบต่อข้อมูลในระบบ

(๓) แนวโน้มในการกู้คืนระบบ

(๔) ลักษณะผลกระทบต่อลูกค้าหรือผู้ใช้บริการ

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี (ก)	กรณี (ข)
๑. ลักษณะผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ดังนี้ (๑) ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือ (๒) อุปกรณ์หรือระบบงานอื่นใดที่ใช้สำหรับการให้บริการของรัฐ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของรัฐด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงขนาดที่จะทำให้ระบบหรือบริการต้องหยุดชะงักหรือไม่สามารถใช้งานได้	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่ถูกใช้สำหรับให้บริการหลัก ดังนี้ (๑) ระบบคอมพิวเตอร์ (๒) โครงสร้างสำคัญทางสารสนเทศ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว แสดงให้เห็นได้ว่าผู้โจมตีมีความมุ่งหมายที่จะทำให้โครงสร้างพื้นฐานสำคัญของประเทศเสียหายจนไม่สามารถทำงานหรือให้บริการได้	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่รุนแรงในลักษณะที่เป็นวงกว้างต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว ทำให้ (๑) การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือ (๒) การใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ หรือระบบคอมพิวเตอร์ คอมพิวเตอร์ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ	ไม่เจาะจงอุปกรณ์หรือระบบงานที่ได้รับผลกระทบ แต่เมื่อพิจารณาจากพฤติกรรมของผู้โจมตีหรือพฤติการณ์แวดล้อมแล้วมีเหตุอันควรเชื่อได้ว่าการก่อภัยคุกคามทางไซเบอร์นั้นกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี (ก)	กรณี (ข)
๒. ลักษณะผลกระทบต่อข้อมูลในระบบ	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูล ซึ่งส่งผลกระทบทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของรัฐด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงขนาดที่จะทำให้ระบบหรือบริการต้องหยุดชะงักหรือไม่สามารถใช้งานได้	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลที่ใช้สำหรับระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศ ซึ่งส่งผลให้บริการหลักไม่สามารถทำงานหรือให้บริการได้	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลอันมีลักษณะดังนี้ (๑) เป็นข้อมูลที่เกี่ยวข้องกับการทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชน หรือ (๒) เป็นข้อมูลที่เกี่ยวข้องกับชีวิตของบุคคลจำนวนมาก หรือเป็นข้อมูลคอมพิวเตอร์จำนวนมากในระดับประเทศ	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลใด ๆ อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี (ก)	กรณี (ข)
๓. แนวโน้มในการกู้คืนระบบ	สามารถกู้คืนระบบคอมพิวเตอร์ หรือทำให้บริการของรัฐกลับมาได้บางส่วน โดยสามารถดำเนินการได้ตามแผนการกู้คืน	ไม่สามารถกู้คืนระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่ใช้สำหรับให้บริการหลักได้ ตามแผนการกู้คืน	ไม่สามารถกู้คืนการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศได้ตามแผนการกู้คืน ทำให้ (๑) รัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือ (๒) มีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์ คอมพิวเตอร์ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ	ไม่สามารถกู้คืนอุปกรณ์หรือระบบงานที่ได้รับผลกระทบได้ และจำเป็นต้องมีมาตรการเร่งด่วนในการกู้คืนอุปกรณ์หรือระบบงานที่เกี่ยวข้อง

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี (ก)	กรณี (ข)
๔. ลักษณะผลกระทบต่อลูกค้าหรือผู้ใช้บริการ	ส่งผลหรืออาจส่งผลกระทบต่อผู้ใช้บริการในวงจำกัด	อาจส่งผลกระทบต่อผู้ใช้บริการทั้งหมด	ส่งผลกระทบต่อผู้ใช้บริการทั้งหมด หรืออาจมีผลทำให้บุคคลจำนวนมากเสียชีวิต	ส่งผลหรืออาจส่งผลกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม

เอกสารแนบ ๒ ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม
และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔
ว่าด้วยมาตรการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

ภาพแสดงขั้นตอนการดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์
(Incident Handling Cycle)

ภาคผนวก
ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม
และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

ข้อ ๑ การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย
๐	เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises)
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)[๔4]
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

ภาคผนวก
ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม
และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

ข้อ ๒ ตัวอย่างลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ

	หมวดหมู่ภัยคุกคาม						
ประเภทอุปกรณ์เครือข่าย	**๑**	**๒**	**๓**	**๔**	**๕**	**๖**	**๗**
Backbone	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เราเตอร์	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายสำหรับการจัดการเครือข่าย หรือ ดูแลความปลอดภัย	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายที่ไม่ได้ให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง
เครื่องแม่ข่ายที่เปิดให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง
เครื่องเวิร์กสเตชัน	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง

ข้อ ๑ การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย
๐	เหตุการณ์จำลอง และ การฝึกรู้โจม ของหน่วยงานเอง (Training and Exercises)
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)[๔]
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

ภาคผนวก

ข้อ ๓ ตัวอย่างกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

หมวดหมู่ภัยคุกคามทางไซเบอร์	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้หน่วยงานควบคุมหรือกำกับดูแล (ภายในเวลา)	การส่งรายงานให้สำนักงาน (ภายในเวลา)
๑	ทุกเหตุการณ์	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๒	ทุกเหตุการณ์	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๓	ทุกเหตุการณ์	๓๐ นาที	๒ ชั่วโมง	๘ ชั่วโมง
๔	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๕	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๖	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๗	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๑๐ นาที	๑ ชั่วโมง	๑ ชั่วโมง
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๘	-	๒๐ นาที	ตามเวลาที่ต้องใช้ในการสืบสวน	๔ ชั่วโมง
๙	-	-	๔ ชั่วโมง	๑๒ ชั่วโมง


THE NATIONAL CYBER INCIDENT
RESPONSE PLAN OF THAILAND (Draft)
LAW
(ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์

การดำเนินงานให้สอดคล้องกับ พ.ร.บ. ไซเบอร์

- ☑ ประเมินองค์กรตาม **ประกาศหลักเกณฑ์ การกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ** ที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ *(หมายเหตุ ประกาศ กมช. ภายในหนึ่งปี)*
- ☑ ***แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ*** เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน กมช.
- ☑ ***แจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์*** ไปยังสำนักงาน กมช. ฯลฯ ภายในสามสิบวัน นับแต่วันที่คณะกรรมการ (กมช.) ประกาศ
- ☑ รับการ ***ตรวจสอบมาตรฐานขั้นต่ำ*** **เรื่องความมั่นคงปลอดภัยไซเบอร์** ของหน่วยงาน CII โดยหน่วยงานควบคุมหรือกำกับดูแล
- ☑ **ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์** โดยมีผู้ตรวจประเมิน
- ☑ **ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์** โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง ให้หน่วยงาน CII *จัดส่งผลสรุป**รายงานการดำเนินการ*** ต่อสำนักงาน กมช. ภายในสามสิบวัน นับแต่วันที่ดำเนินการแล้วเสร็จ

อ้างอิง ข้อกำหนดที่ต้องดำเนินการสำหรับหน่วยงาน CII

การดำเนินงานให้สอดคล้องกับ พ.ร.บ. ไซเบอร์

☑ มี **กลไกหรือขั้นตอน** เพื่อ **การเฝ้าระวังภัยคุกคามทางไซเบอร์** หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน

[1] ตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และ

[2] ตามประมวลแนวทางปฏิบัติ

รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการ หรือ กกม. กำหนด และ *ต้องเข้าร่วมการทดสอบสถานะความพร้อม* ในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

☑ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบ ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้ *รายงาน* ต่อ สำนักงาน กมช. และ หน่วยงานควบคุมหรือกำกับดูแล และ *ปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์* ตามที่กำหนดในส่วนที่ 4 ทั้งนี้ กกม. *อาจกำหนด* **หลักเกณฑ์และวิธีการการรายงาน** ด้วยก็ได้

อ้างอิง ข้อกำหนดที่ต้องดำเนินการสำหรับหน่วยงาน CII

การดำเนินงานให้สอดคล้องกับ พ.ร.บ. ไซเบอร์

- ☑ จัดทำ ประมวลแนวทางปฏิบัติ และ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
- ☑ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน

ประมวลแนวทางปฏิบัติ

- แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- แผนการรับมือภัยคุกคามทางไซเบอร์

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

- ระบุความเสี่ยง
- มาตรการป้องกันความเสี่ยง
- มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์
- มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์
- มาตรการรักษาและฟื้นฟูความเสียหาย

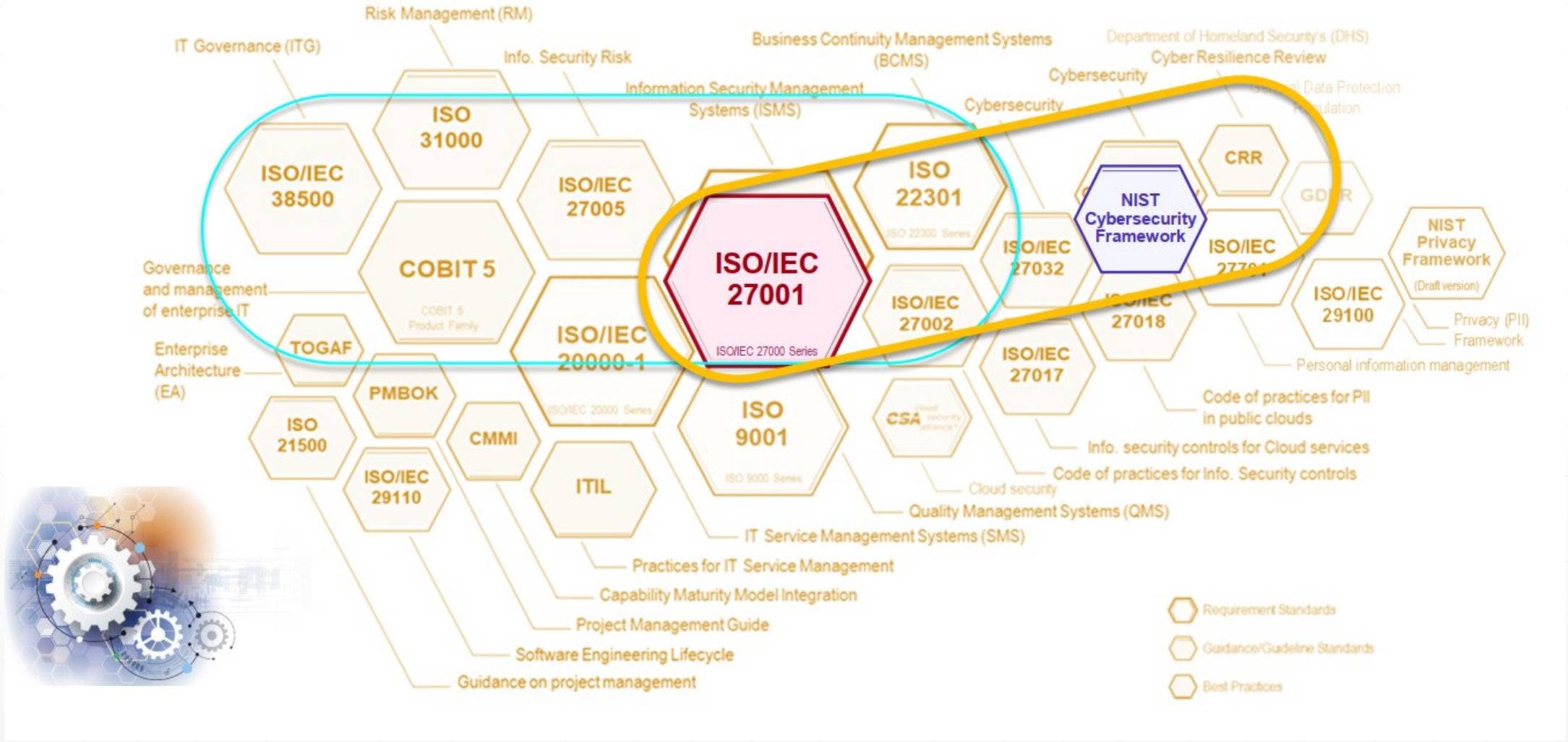
อ้างอิง ข้อกำหนดที่ต้องดำเนินการสำหรับหน่วยงาน CII

Best Practices in Information Technology and Cybersecurity

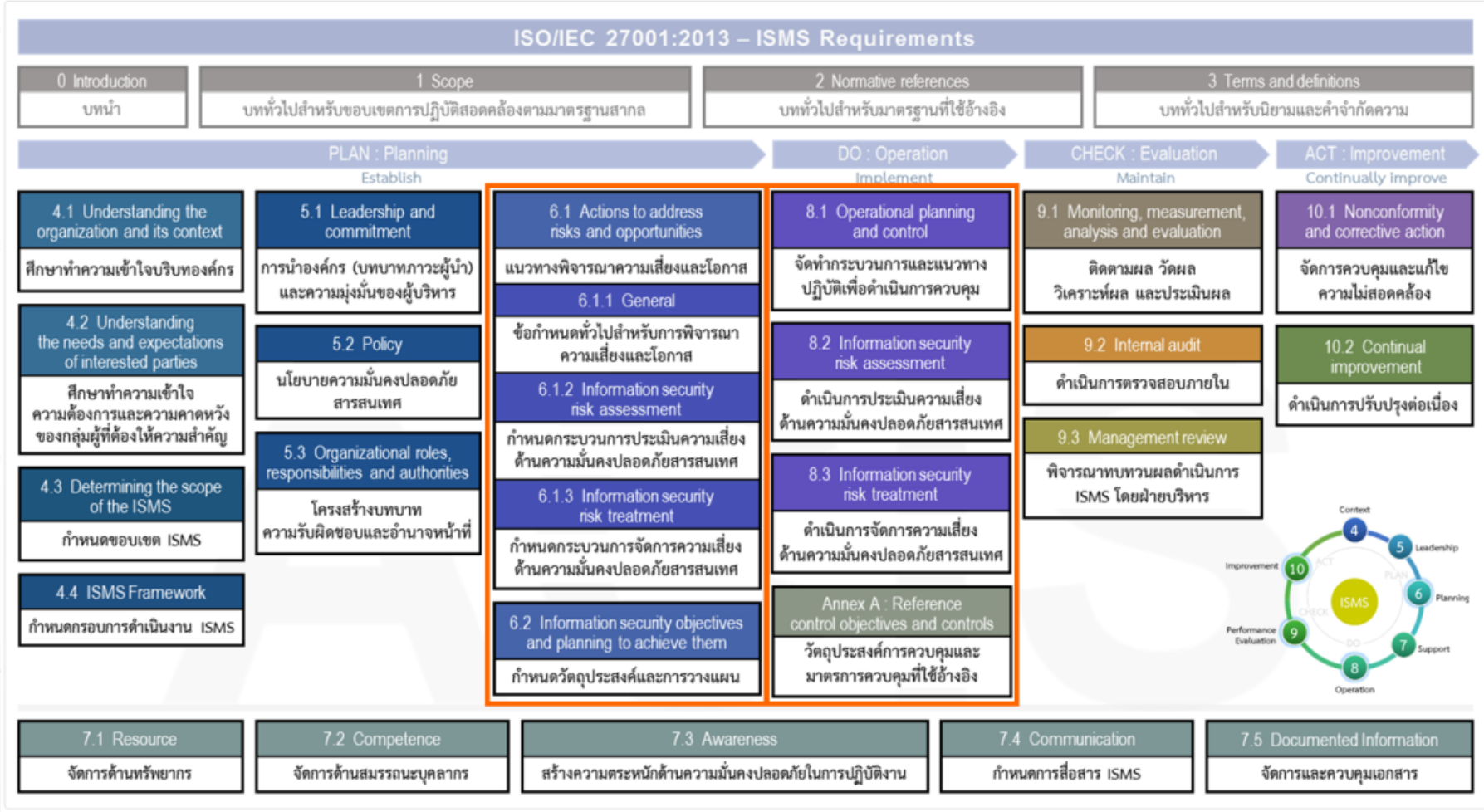
3

แนวปฏิบัติด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์

Reference Risk-based Standards & Best Practices



ISO/IEC 27001:2013
Information Security Management System : ISMS Requirements



ISO/IEC 27001:2013
Information Security Management System : ISMS Requirements

Annex A : Reference control objectives and controls*

Information Security : 14 Domains, 35 Control objectives, 114 Controls

A.5 Information security policy 1 2
- Management direction for information security (2 controls)

A.6 Organization of information security 2 7
- Internal organization (5 controls)
- Mobile devices and teleworking (2 controls)

A.7 Human resource security 3 6
- Prior to employment (2 controls)
- During employment (3 controls)
- Termination and change of employment (1 control)

A.8 Asset management 3 10
- Responsibility for assets (4 controls)
- Information classification (3 controls)
- Media handling (3 controls)

A.9 Access control 4 14
- Business requirements of access control (2 controls)
- User access management (6 controls)
- User responsibilities (1 control)
- System and application access control (5 controls)

A.10 Cryptography 1 2
- Cryptographic controls (2 controls)

A.11 Physical & environmental security 2 15
- Secure areas (6 controls)
- Equipment (9 controls)

A.12 Operations security 7 14
- Operational procedures and responsibilities (4 controls)
- Protection from malware (1 control)
- Backup (1 control)
- Logging and monitoring (4 controls)
- Control of operational software (1 control)
- Technical vulnerability management (2 controls)
- Information systems audit considerations (1 control)

A.13 Communications security 2 7
- Network security management (3 controls)
- Information transfer (4 controls)

A.14 System acquisition, development and maintenance 3 13
- Security requirements of information systems (3 controls)
- Security in development and support processes (9 controls)
- Test data (1 control)

A.15 Supplier relationships 2 5
- Information security in supplier relationships (3 controls)
- Supplier service delivery management (2 controls)

A.16 Information security incident management 1 7
- Management of Information security incidents and improvements (7 controls)

A.17 Information security aspects of business continuity management 2 4
- Information security continuity (3 controls)
- Redundancies (1 controls)

A.18 Compliance 2 8
- Compliance with legal & contractual requirements (5 controls)
- Information security reviews (3 controls)

Organizations can design controls as required, or identify them from any source.
Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.

ISO/IEC 27002:2022 – Information Security Controls

5 Organizational controls — Annex A: A.5

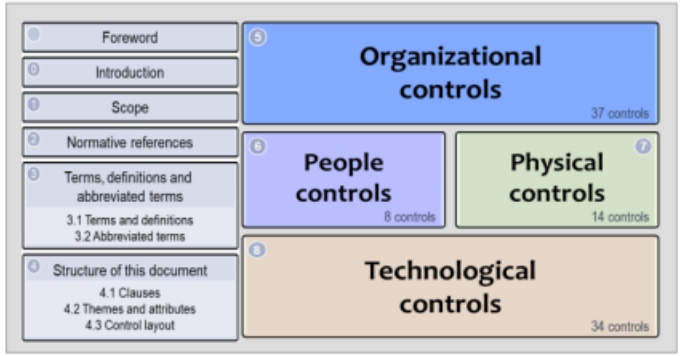
5.1 Policies for information security
5.2 Information security roles and responsibilities
5.3 Segregation of duties
5.4 Management responsibilities
5.5 Contact with authorities
5.6 Contact with special interest groups
5.7 Threat intelligence ★
5.8 Information security in project management
5.9 Inventory of information and other associated assets
5.10 Acceptable use of information and other associated assets
5.11 Return of assets
5.12 Classification of information
5.13 Labelling of information
5.14 Information transfer
5.15 Access control
5.16 Identity management
5.17 Authentication information
5.18 Access rights
5.19 Information security in supplier relationships
5.20 Addressing information security within supplier agreements
5.21 Managing information security in the ICT supply chain
5.22 Monitoring, review and change management of supplier services
5.23 Information security for use of cloud services ★
5.24 Information security incident management planning and preparation
5.25 Assessment and decision on information security events
5.26 Response to information security incidents
5.27 Learning from information security incidents
5.28 Collection of evidence
5.29 Information security during disruption
5.30 ICT readiness for business continuity ★
5.31 Legal, statutory, regulatory and contractual requirements
5.32 Intellectual property rights
5.33 Protection of records
5.34 Privacy and protection of PII
5.35 Independent review of information security
5.36 Compliance with policies, rules and standards for information security
5.37 Documented operating procedures

6 People controls — Annex A: A.6

6.1 Screening
6.2 Terms and conditions of employment
6.3 Information security awareness, education and training
6.4 Disciplinary process
6.5 Responsibilities after termination or change of employment
6.6 Confidentiality or non-disclosure agreements
6.7 Remote working
6.8 Information security event reporting

7 Physical controls — Annex A: A.7

7.1 Physical security perimeter
7.2 Physical entry
7.3 Securing offices, rooms and facilities
7.4 Physical security monitoring ★
7.5 Protecting against physical and environmental threats
7.6 Working in secure areas
7.7 Clear desk and clear screen
7.8 Equipment siting and protection
7.9 Security of assets off-premises
7.10 Storage media
7.11 Supporting utilities
7.12 Cabling security
7.13 Equipment maintenance
7.14 Secure disposal or re-use of equipment



8 Technological controls — Annex A: A.8

8.1 User endpoint devices
8.2 Privileged access rights
8.3 Information access restriction
8.4 Access to source code
8.5 Secure authentication
8.6 Capacity management
8.7 Protection against malware
8.8 Management of technical vulnerabilities
8.9 Configuration management ★
8.10 Information deletion ★
8.11 Data masking ★
8.12 Data leakage prevention ★
8.13 Information backup
8.14 Redundancy of information processing facilities
8.15 Logging
8.16 Monitoring activities ★
8.17 Clock synchronization
8.18 Use of privileged utility programs
8.19 Installation of software on operational systems
8.20 Network security
8.21 Security of network services
8.22 Segregation in networks
8.23 Web filtering ★
8.24 Use of cryptography
8.25 Secure development life cycle
8.26 Application security requirements
8.27 Secure system architecture and engineering principles
8.28 Secure coding ★
8.29 Security testing in development and acceptance
8.30 Outsourced development
8.31 Separation of development, test and production environments
8.32 Change management
8.33 Test information
8.34 Protection of information systems during audit and testing

★ 11 New controls

Total : 93 controls

ISO/IEC 27002:2022 – Information Security Controls

❖ Control Layout

Examples:

Control Title

Attribute table

5.26 Response to information security incidents

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Information_security_event_management	#Defence

Control

Information security incidents should be responded to in accordance with the documented procedures.

Purpose

To ensure efficient and effective response to information security incidents.

Purpose

Control

Guidance

Guidance

The organization should establish and communicate procedures on information security incident response to all relevant interested parties.

Information security incidents should be responded to by a designated team with the required competency (see 5.24).

The response should include the following:

a) containing, if the consequences of the incident can spread, the systems affected by the incident;

b) collecting evidence (see 5.28) as soon as possible after the occurrence;

c) escalation, as required including crisis management activities and possibly invoking business continuity plans (see 5.29 and 5.30);

d) ensuring that all involved response activities are properly logged for later analysis;

e) communicating the existence of the information security incident or any relevant details thereof to all relevant internal and external interested parties following the need-to-know principle;

f) coordinating with internal and external parties such as authorities, external interest groups and forums, suppliers and clients to improve response effectiveness and help to minimize consequences for other organizations;

g) once the incident has been successfully addressed, formally closing and recording it;

h) conducting information security forensic analysis, as required (see 5.28);

i) performing post-incident analysis to identify root cause. Ensure it is documented and communicated according to defined procedures (see 5.27);

j) identifying and managing information security vulnerabilities and weaknesses including those related to controls which have caused, contributed to or failed to prevent the incident.

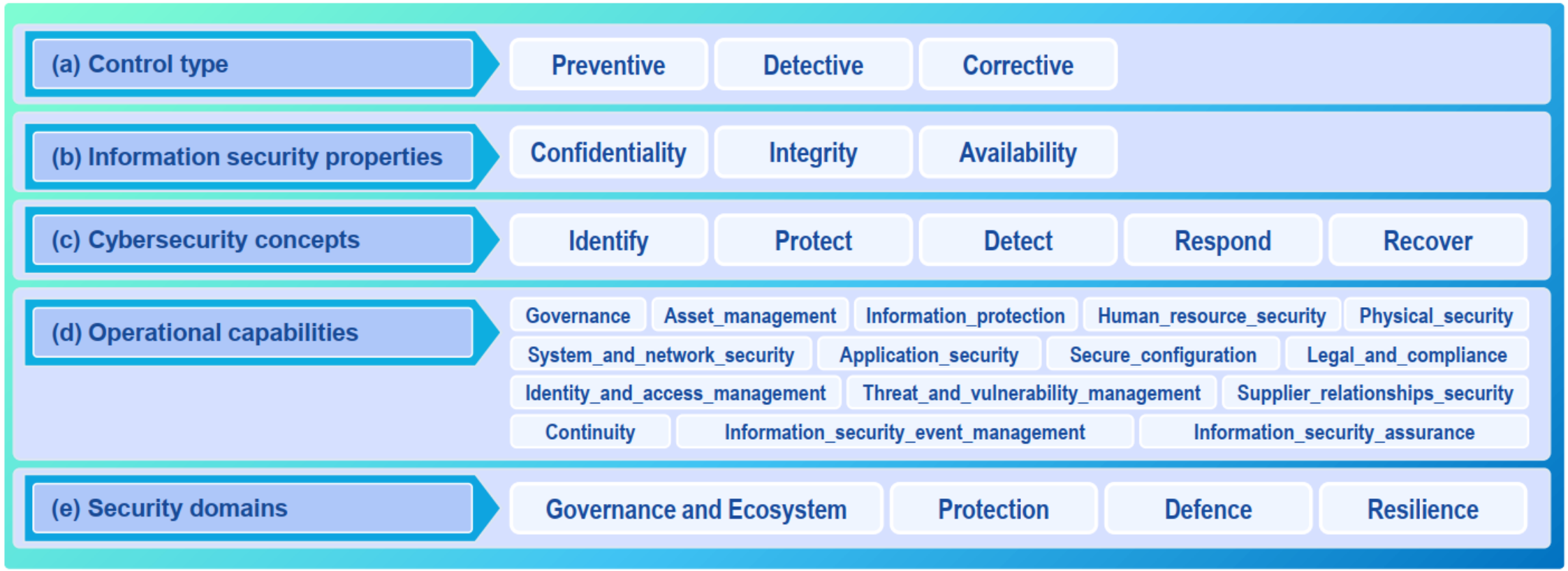
Other information

Other information

The ISO/IEC 27035 series provides further guidance on incident management.

ISO/IEC 27002:2022 – Information Security Controls

Themes and Attributes: Categorization of Controls



ISO/IEC 27002:2022 – Information Security Controls

❖ Themes and Attributes: Categorization of Controls

Examples:

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains

5.24 Information security incident management planning and preparation

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_security_event_management	#Defence

8.20 Networks security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security	#Protection

NIST Cybersecurity Framework

NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018

Overview of NIST Cybersecurity Framework

4

ภาพรวมของ NIST Cybersecurity Framework

What is the cybersecurity framework (CSF)?

CSF คือ หลักการและแนวทางปฏิบัติที่ดีที่สุดในการบริหารจัดการความเสี่ยง เพื่อยกระดับความมั่นคงปลอดภัยขององค์กรทุกระดับ รวมไปถึงช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ ในขณะที่ธุรกิจยังคงดำเนินต่อไปได้อย่างเนื่อง

What is the cybersecurity framework (CSF)?

NIST
National Institute of Standards and Technology
สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ

NIST Cybersecurity Framework version 1.0

Released in Feb 2014

Released in April 2018

NIST Cybersecurity Framework version 1.1

Version ปัจจุบัน

Date Published: August 2023

Initial Public Draft

NIST Cybersecurity Framework version 2.0

อยู่ระหว่างรับฟังความคิดเห็น

NIST Cybersecurity Framework

NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018

NIST Cybersecurity Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Identity Management And Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Strategy	Protective Technology			

พ.ร.บ. ไซเบอร์	การระบุความเสี่ยงที่อาจจะเกิดขึ้น	มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น	มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์	มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์	มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์	มาตรา 13 (4)

Components of NIST Cybersecurity Framework

5

องค์ประกอบของ NIST Cybersecurity Framework

Cybersecurity Framework Components

Defines the activities, outcomes and references.

Consists of five concurrent and continuous functions:

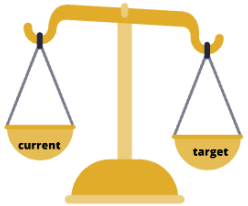
Image: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology

Documents the "current state"

&

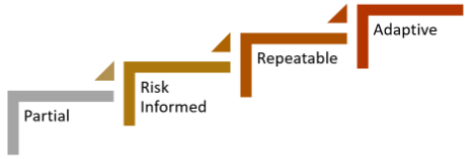
uses risk management processes

to



create the "target state" profile.

Describes the extent of *"rigor & sophistication"* of cybersecurity risk management processes and practices



There are 4 levels from Tier 1 (Partial) to Tier 4 (Adaptive)

***The CSF says the tiers do NOT represent maturity levels. (More about this later)**

Framework Core

Functions	Cybersecurity Framework (CSF) Core Functions:
IDENTIFY	**Identify**—Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.
PROTECT	**Protect**—Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
DETECT	**Detect**—Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
RESPOND	**Respond**—Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
RECOVER	**Recover**—Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

https://www.us-cert.gov/resources/cybersecurity-framework

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

	Function	Category	ID
What processes and assets need protection?	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
What safeguards are available?	Protect	Identity Management & Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes & Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
What techniques can identify incidents?	Detect	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
What techniques can contain impacts of incidents?	Respond	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
What techniques can restore capabilities?	Recover	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

ที่มา: https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components

Subcategories & Informative References

5 Functions

23 Categories

108 Subcategories

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

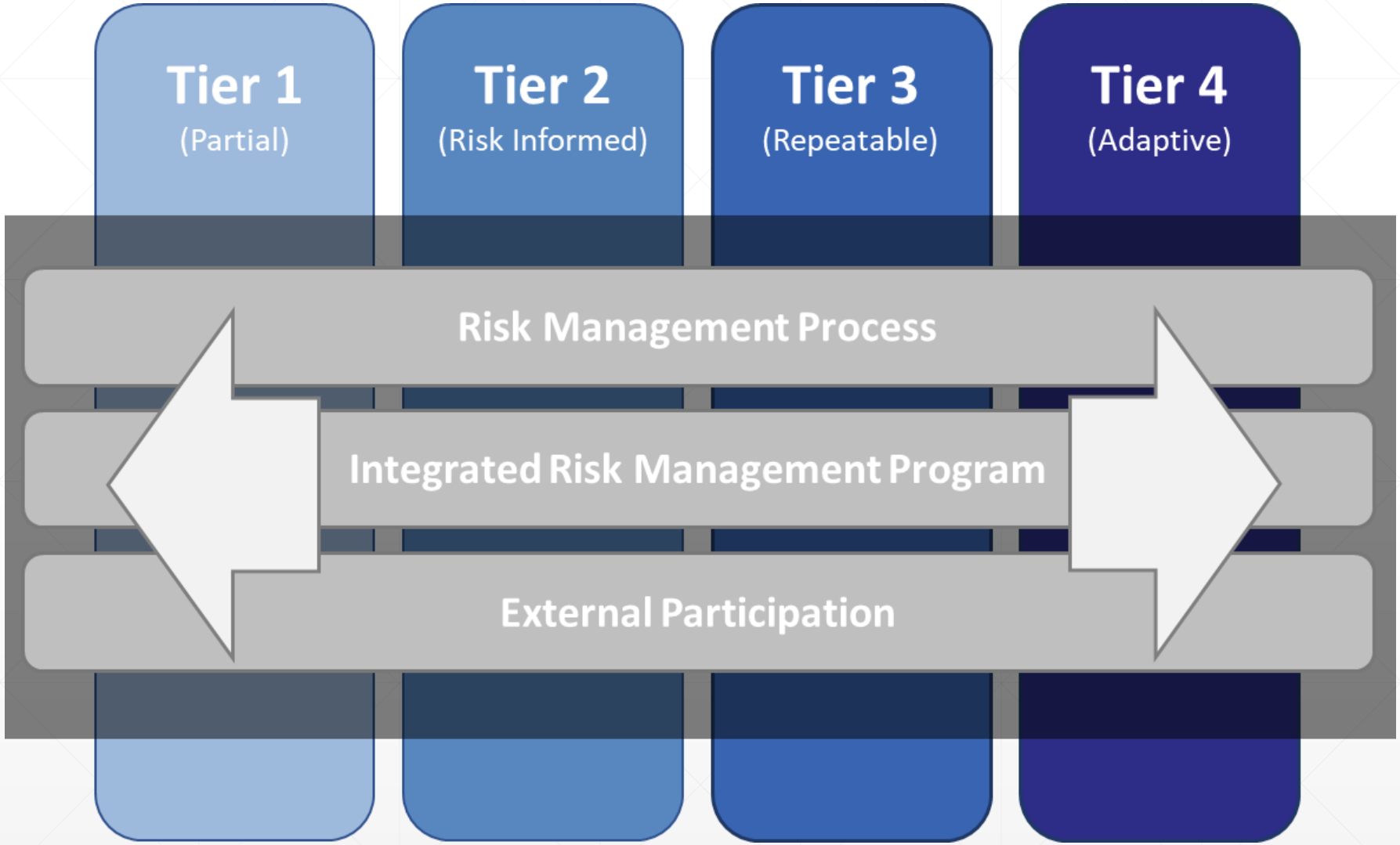
6 informative references

ที่มา: https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components

Mapping CSF Core Functions vs. ISO/IEC 27001:2013

Cybersecurity Framework						ISO/IEC 27001:2013 ISMS		
ID	PR	DE	RS	RC	Summary		Annex A Reference Controls	
✓	-	-	-	-	☑	1	A.5 Information security policies	*
✓	✓	✓	✓	-	☑☑☑☑	2	A.6 Organization of information security	****
✓	✓	-	-	-	☑☑	3	A.7 Human resource security	**
✓	✓	-	-	-	☑☑	4	A.8 Asset management	**
-	✓	-	-	-	☑	5	A.9 Access control	*
-	✓	-	-	-	☑	6	A.10 Cryptography	*
✓	✓	-	-	-	☑☑	7	A.11 Physical and environmental security	**
✓	✓	✓	✓	-	☑☑☑☑	8	A.12 Operations security	****
✓	✓	-	-	-	☑☑	9	A.13 Communications security	**
-	✓	✓	-	-	☑☑	10	A.14 System acquisition, development and maintenance	**
✓	✓	✓	-	-	☑☑☑	11	A.15 Supplier relationships	***
-	✓	✓	✓	✓	☑☑☑☑	12	A.16 Information security incident management	****
✓	✓	-	-	-	☑☑	13	A.17 Information security aspects of business continuity	**
✓	✓	✓	-	-	☑☑☑	14	A.18 Compliance	***

Framework Implementation Tiers



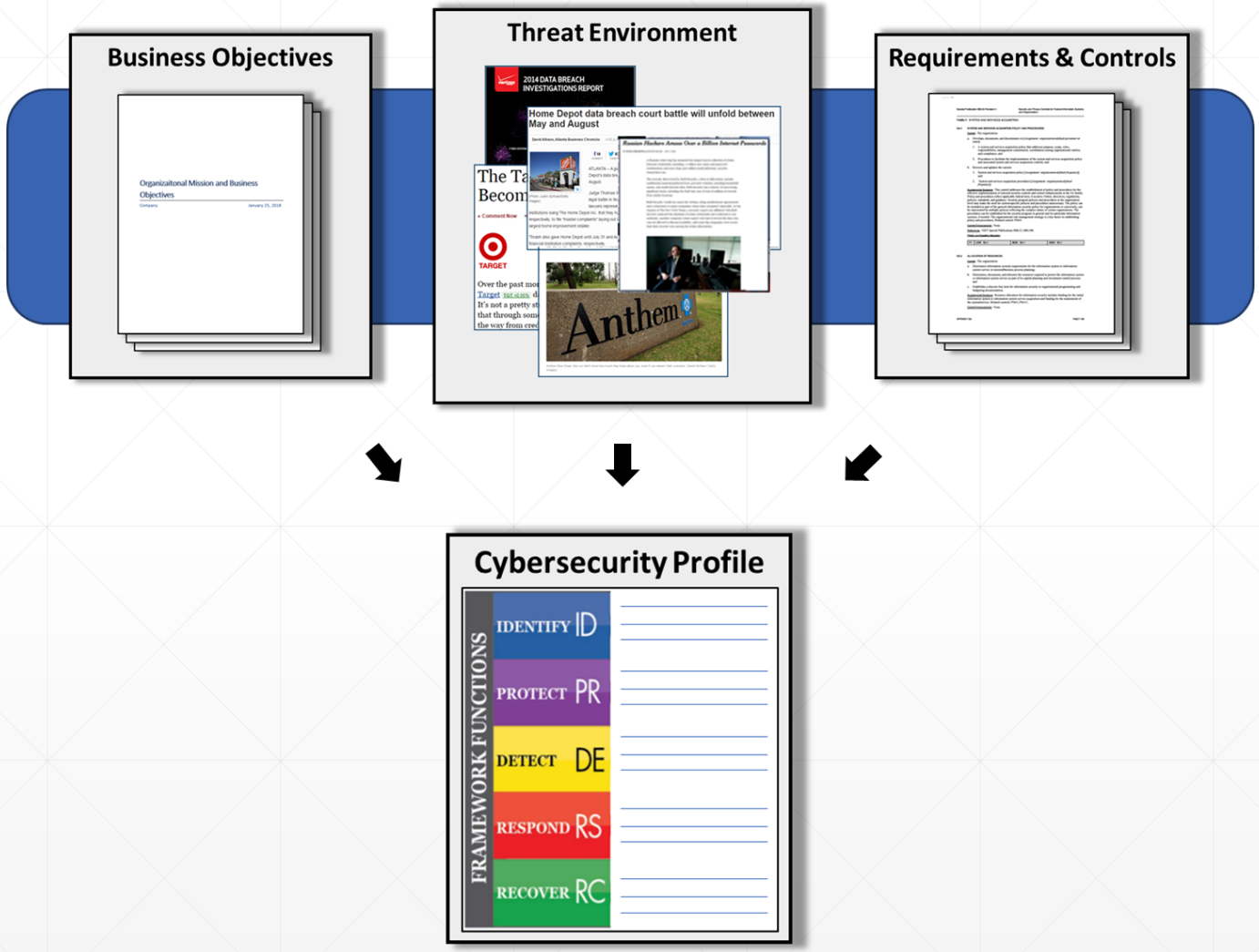
ที่มา: https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components

Framework Profiles

- Alignment with business requirements, risk tolerance, and organizational resources
- Enables organizations to establish a roadmap for reducing cybersecurity risk
- Used to describe current state or desired target state of cybersecurity activities

ที่มา: https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components

Building a Profile



ที่มา: https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components

Resource and Budget Decision Making

Subcategory	Priority	Gaps	Budget	Activities (Year 1)	Activities (Year 2)
1	Moderate	Small	$$$		X
2	High	Large	$$	X	
3	Moderate	Medium	$	X	
…	…	…	…		
98	Moderate	None	$$		Reassess

…and supports on-going operational decisions, too

ที่มา: https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components

Workshop 1

จับคู่ข้อความต่อไปนี้ให้สัมพันธ์กันและถูกต้อง

พ.ร.บ. ไซเบอร์	
NIST Cybersecurity Framework	
CIA Triad	
Risk Management	
ประมวลแนวทางปฏิบัติ	
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)	
ภัยคุกคามทางไซเบอร์	

A	องค์ประกอบสามประการของการรักษาความปลอดภัยข้อมูล
B	การกระทำหรือการดำเนินการใดๆ ผ่านการใช้ระบบสารสนเทศหรือเครือข่ายที่ก่อให้เกิดผลเสียต่อระบบข้อมูลเครือข่ายและ / หรือข้อมูลภายในองค์กร
C	กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
D	ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนด
E	กรอบการดำเนินงานหรือแนวทางการออกแบบความปลอดภัยด้านความมั่นคงปลอดภัยไซเบอร์
F	มาตรการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกของประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ
G	กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลง หรืออยู่ในระดับที่องค์กรยอมรับได้

NIST Cybersecurity Framework version 1.1

6

แนวปฏิบัติตาม NIST Cybersecurity Framework version 1.1

NIST Cybersecurity Framework

NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018

NIST Cybersecurity Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Identity Management And Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Strategy	Protective Technology			

พ.ร.บ. ไซเบอร์	การระบุความเสี่ยงที่อาจจะเกิดขึ้น	มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น	มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์	มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์	มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์	มาตรา 13 (4)

NIST Cybersecurity Framework

NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018

What processes and assets need protection?

IDENTIFY

The purpose of this function is to identify and develop the organizational capability to management cybersecurity risk

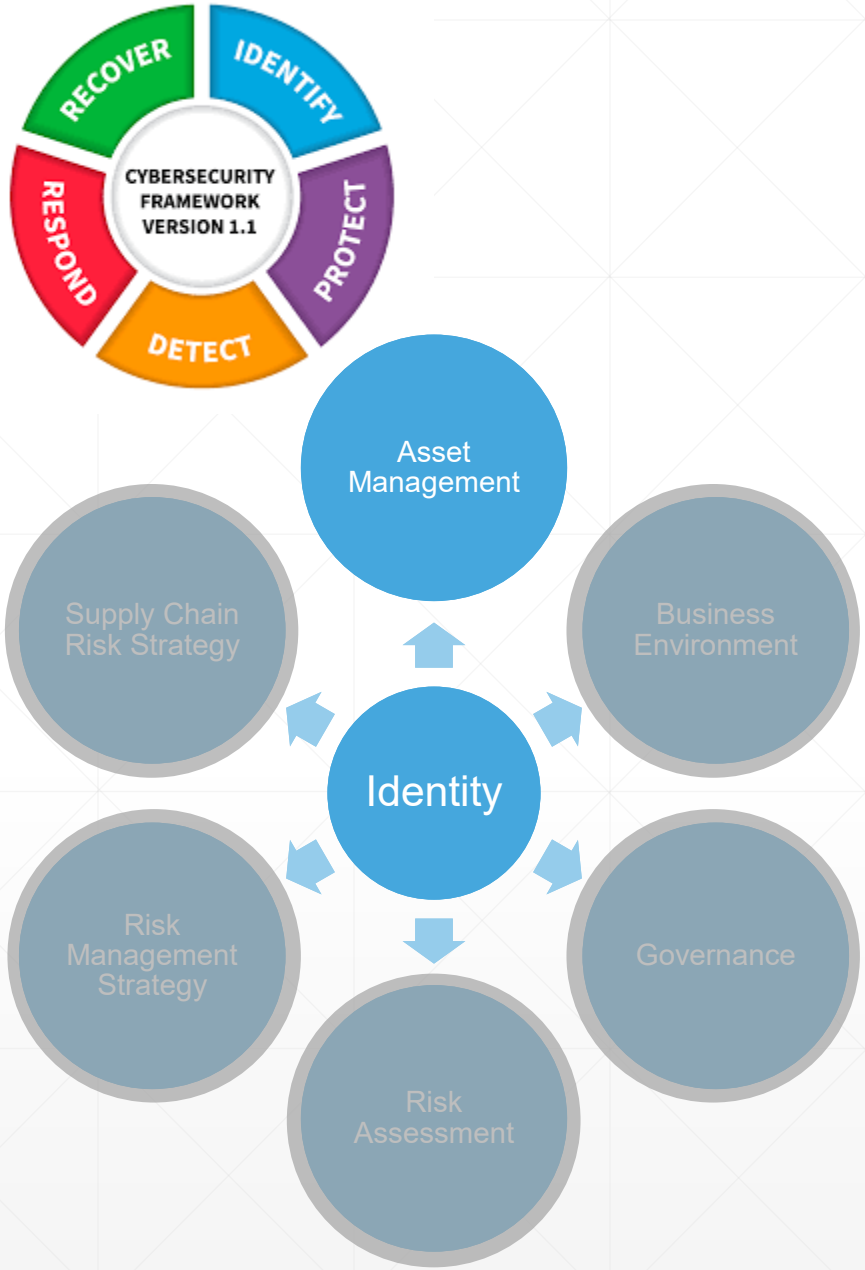

RECOVER
IDENTIFY
CYBERSECURITY
FRAMEWORK
VERSION 1.1
RESPOND
PROTECT
DETECT


Asset Management
Business Environment
Supply Chain Risk Strategy
Identity
Risk Management Strategy
Governance
Risk Assessment

People managed based on their "relative importance…"?

ID.AM

- Asset (hardware; software; facilities; information; people) are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy

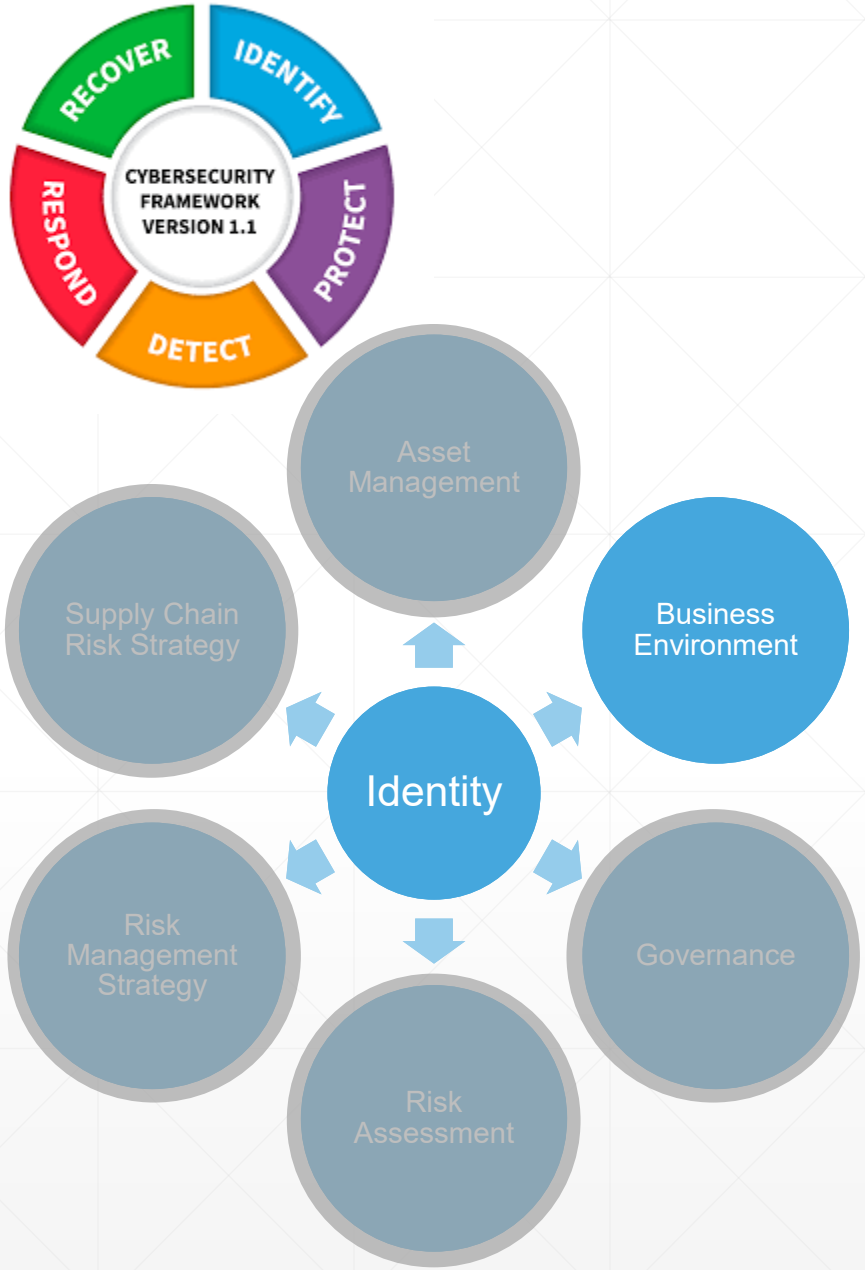


Subcategory	Informative References
ID.AM-1: Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
ID.AM-4: External information systems are catalogued	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	· **CIS CSC** 13, 14 · **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **CIS CSC** 17, 19 · **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

ID.BE

- The organization's mission, objectives, stakeholders and activities are understood and prioritized.

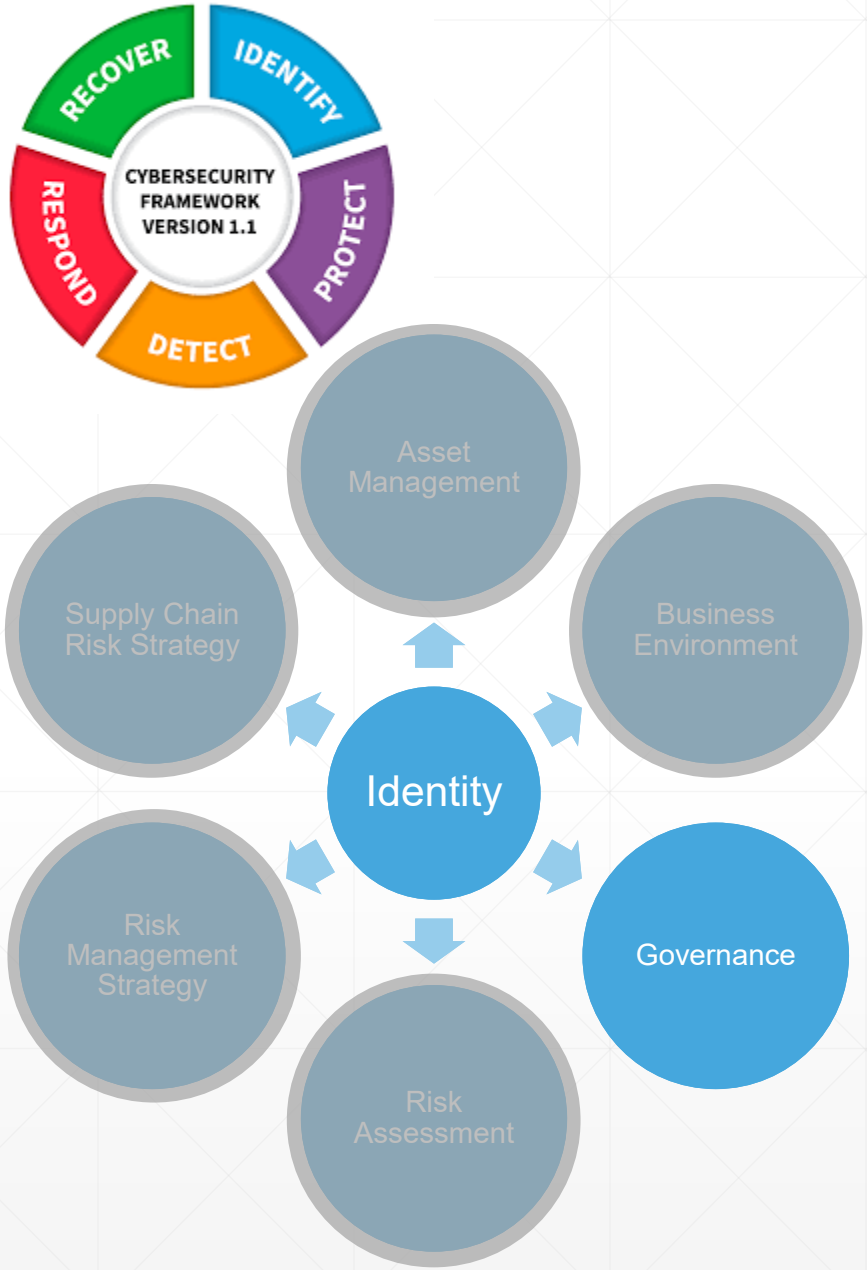
Part of establishing the business context for those familiar with 27001



Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	· **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, · **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	· **COBIT 5** APO02.06, APO03.01 · **ISO/IEC 27001:2013** Clause 4.1 · **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	· **COBIT 5** APO02.01, APO02.06, APO03.01 · **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 · **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	· **COBIT 5** APO10.01, BAI04.02, BAI09.02 · **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 · **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g.	· **COBIT 5** BAI03.02, DSS04.02 · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14

ID.GV

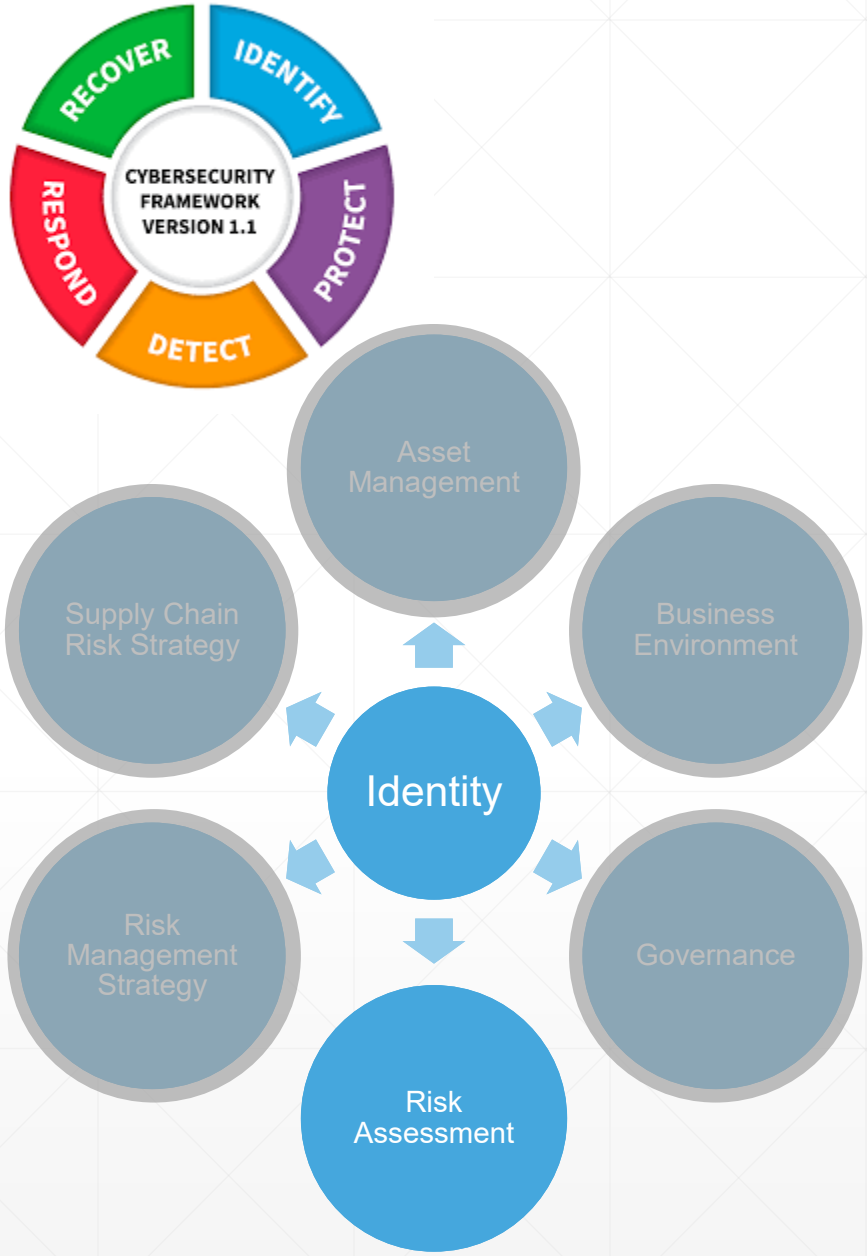
- Cyber security policies are written and communicated;
- Cyber roles and responsibilities;
- Legal / regulatory requirements;
- Governance & risk management processes



Subcategory	Informative References
ID.GV-1: Organizational cybersecurity policy is established and communicated	· **CIS CSC** 19 · **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 · **ISA 62443-2-1:2009** 4.3.2.6 · **ISO/IEC 27001:2013** A.5.1.1 · **NIST SP 800-53 Rev. 4** -1 controls from all security control
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	· **CIS CSC** 19 · **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 · **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· **CIS CSC** 19 · **COBIT 5** BAI02.01, MEA03.01, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.7 · **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, · **NIST SP 800-53 Rev. 4** -1 controls from all security control
ID.GV-4: Governance and risk management processes address cybersecurity risks	· **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, · **ISO/IEC 27001:2013** Clause 6 · **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11

ID.RA

- Threats, vulnerabilities, impacts, likelihood are identified and used to determine the level of risk;
- Risk treatment plans (responses) identified and prioritized



Subcategory	Informative References
ID.RA-1: Asset vulnerabilities are identified and documented	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	· **CIS CSC** 4 · **COBIT 5** BAI08.01 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16
ID.RA-3: Threats, both internal and external, are identified and documented	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
ID.RA-4: Potential business impacts and likelihoods are identified	· **CIS CSC** 4 · **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	· **CIS CSC** 4 · **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
ID.RA-6: Risk responses are identified and prioritized	· **CIS CSC** 4 · **COBIT 5** APO12.05, APO13.02 · **ISO/IEC 27001:2013** Clause 6.1.3 · **NIST SP 800-53 Rev. 4** PM-4, PM-9

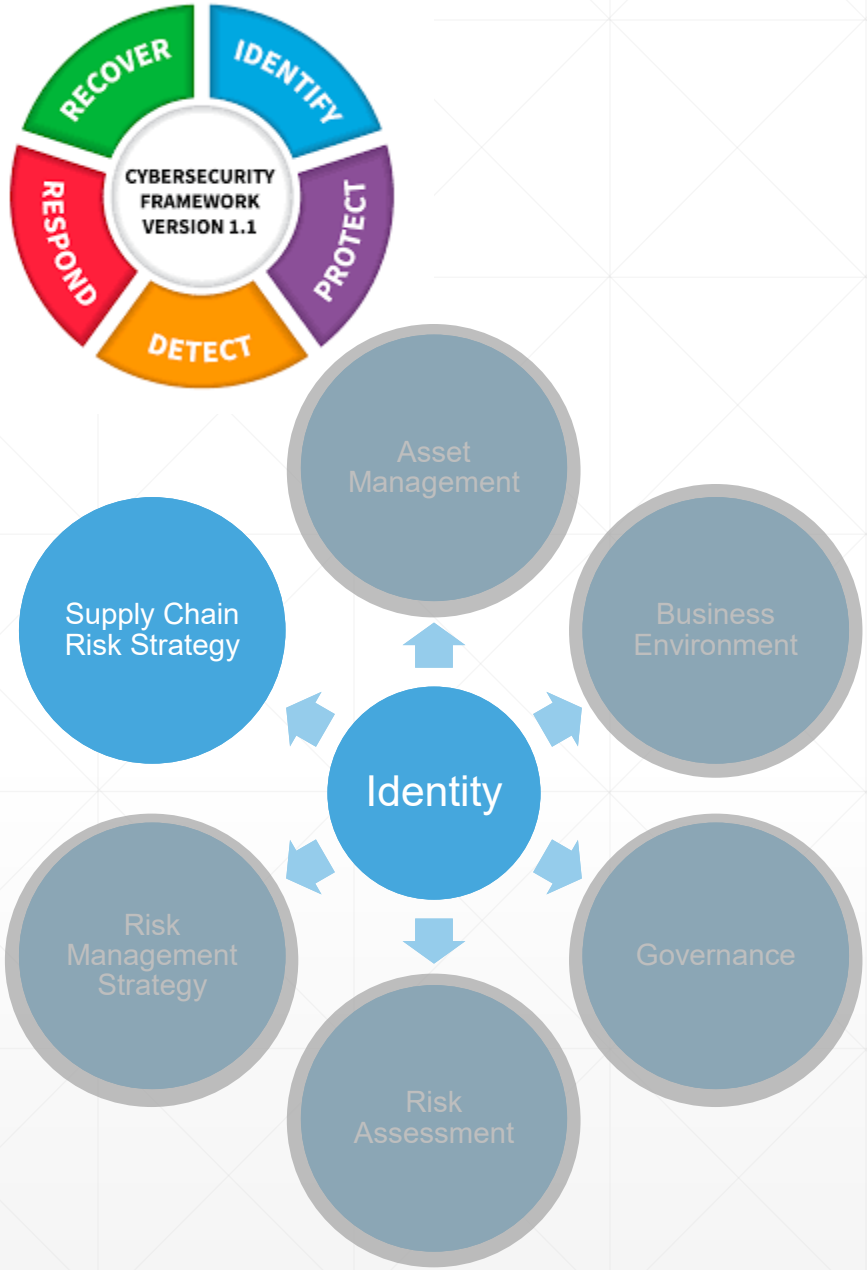
ID.RM

- Risk management process;
- Risk criteria and tolerances;

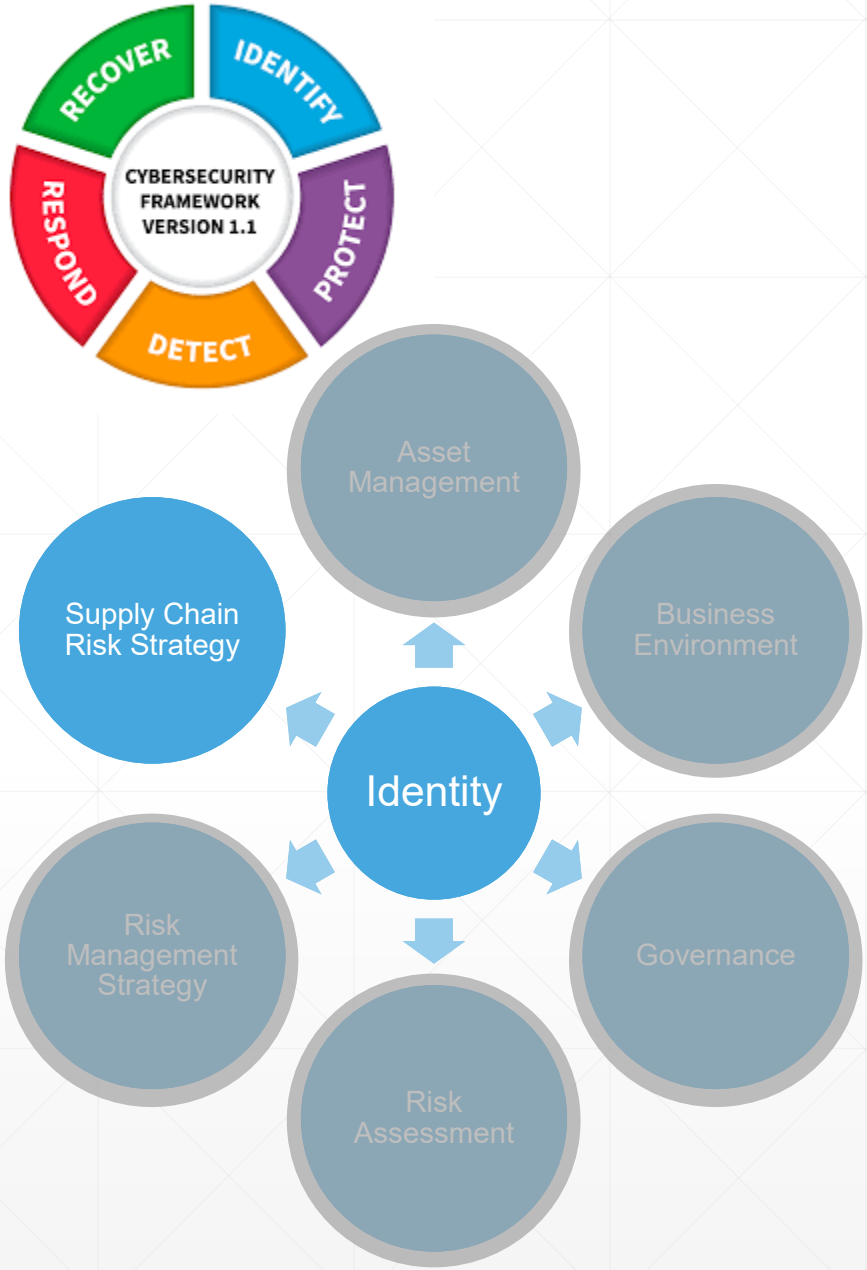
Subcategory	Informative References
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	· **CIS CSC** 4 · **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 · **NIST SP 800-53 Rev. 4** PM-9
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.2.6.5 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 4** PM-9
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector	· **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11

ID.SC

- Supply chain risk management processes;
- Suppliers identified, prioritized & assessed;
- Contracts meet cybersecurity objectives;



Subcategory	Informative References
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	· **CIS CSC** 4 · **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	· **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9



Subcategory	Informative References
ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	· **COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 · **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	· **COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 · **ISA 62443-2-1:2009** 4.3.2.6.7 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

NIST Cybersecurity Framework

NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018

What safeguards are available?

PROTECT

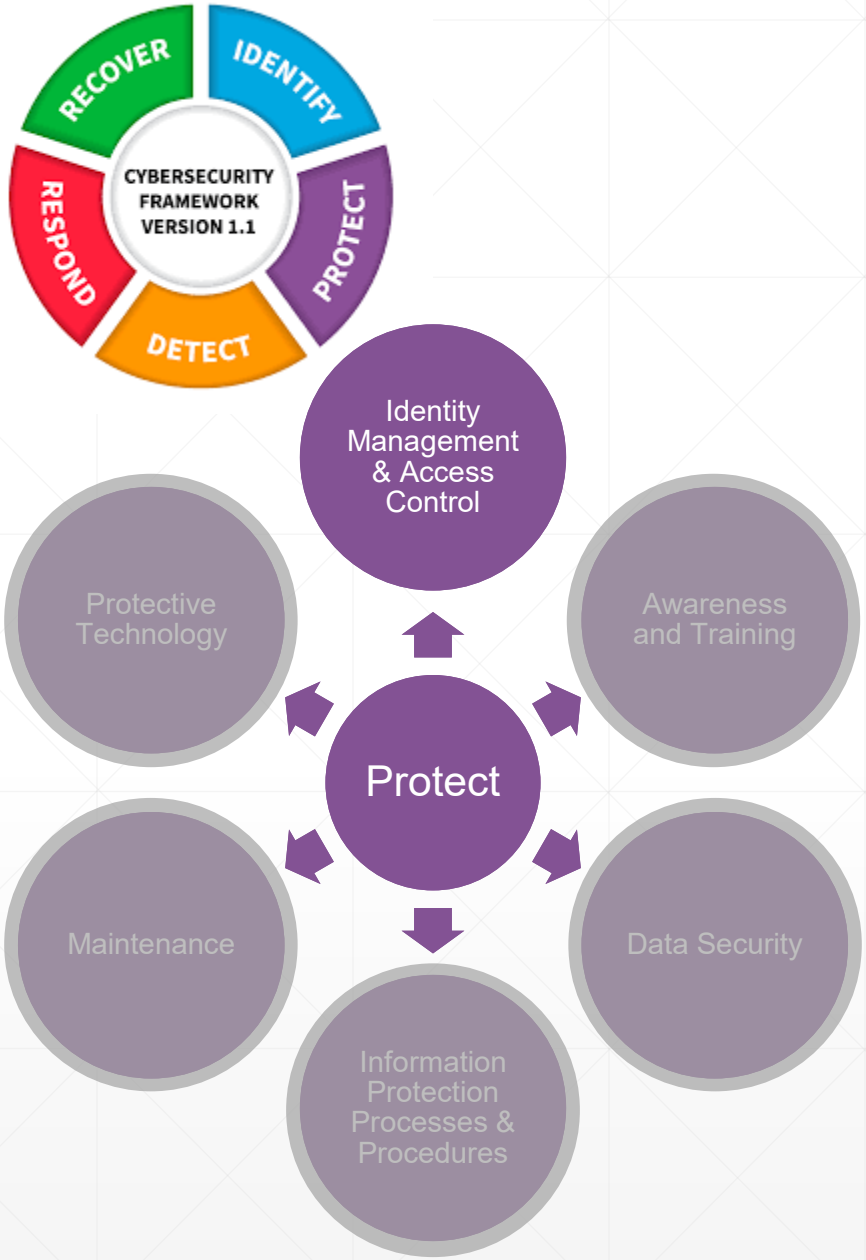
Do what needs to be done to protect the assets by developing and implementing safeguards


RECOVER
IDENTIFY
CYBERSECURITY
FRAMEWORK
VERSION 1.1
RESPOND
PROTECT
DETECT

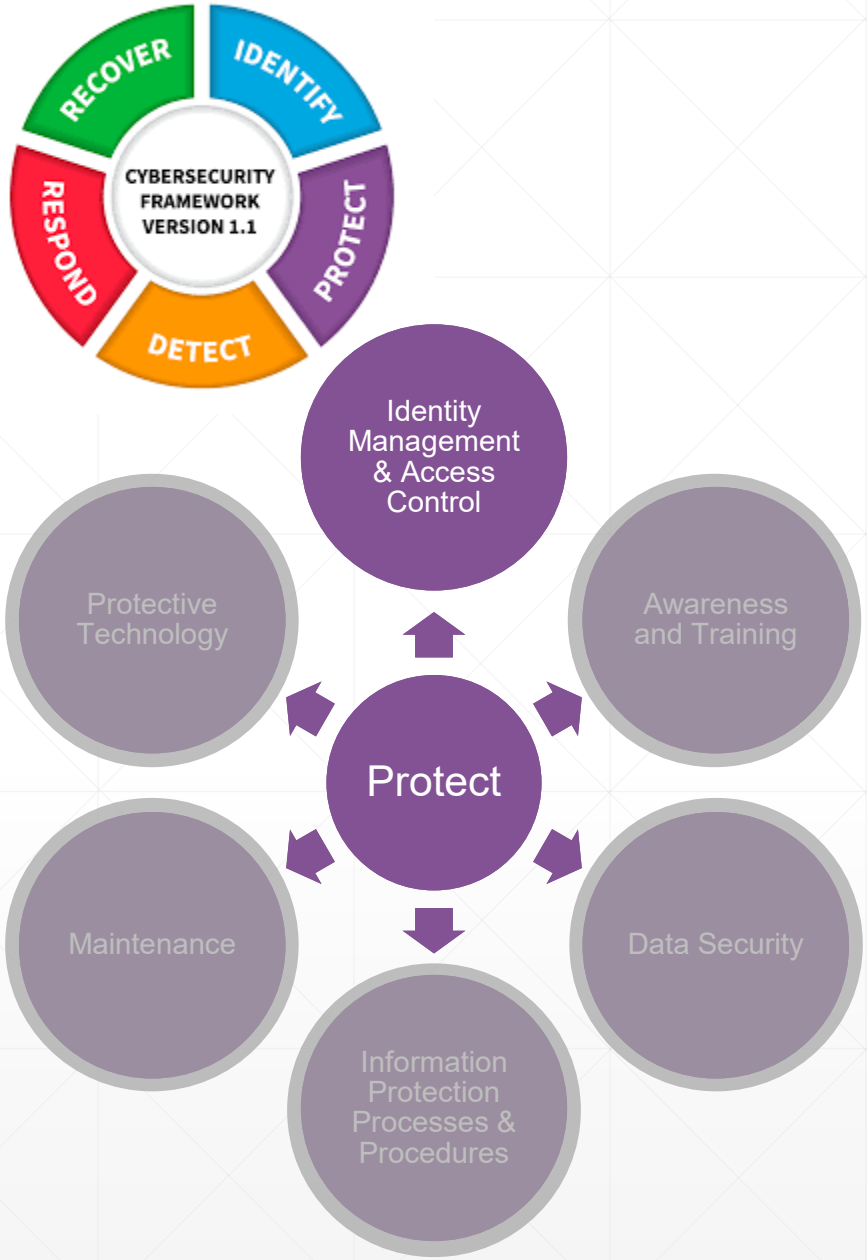

Identity Management & Access Control
Protective Technology
Awareness and Training
Protect
Maintenance
Data Security
Information Protection Processes & Procedures

PR.AC

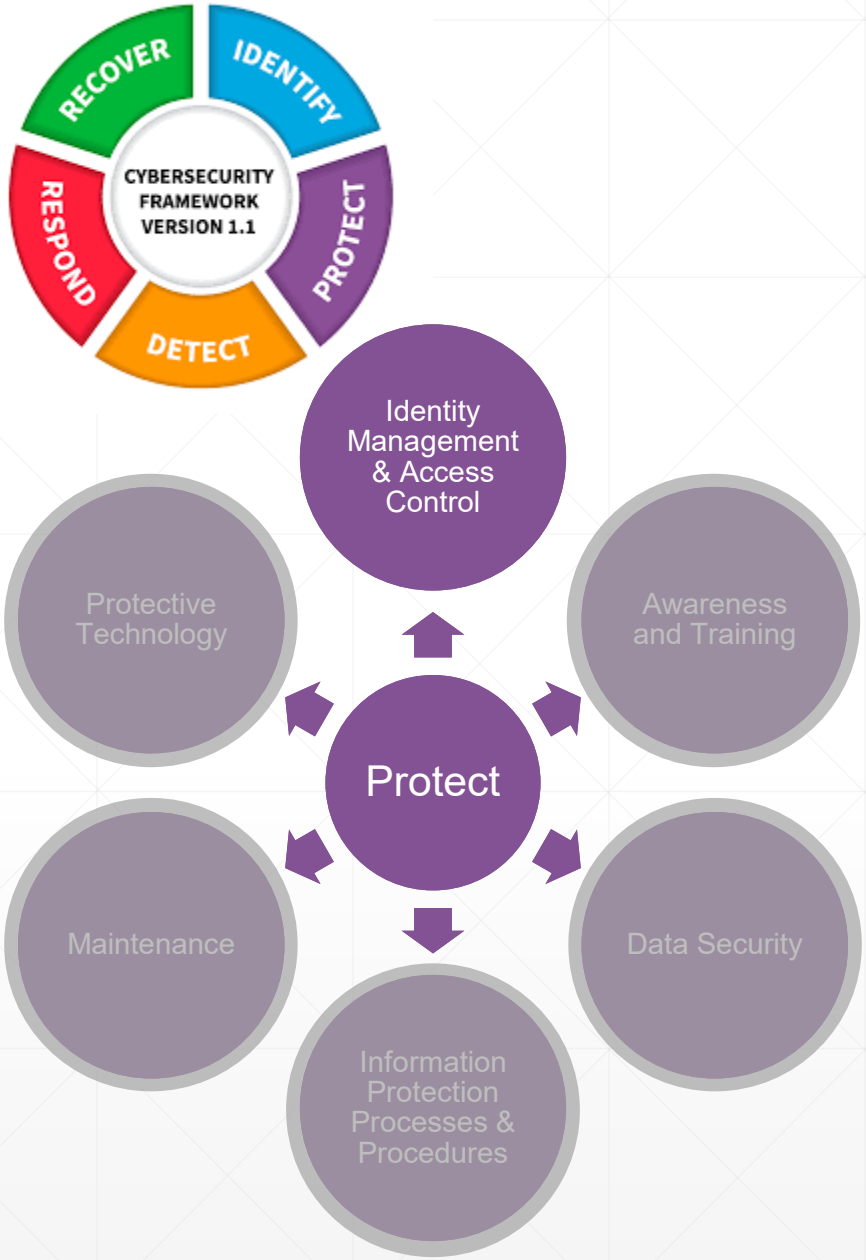
- Identity lifecycle is managed;
- Physical and remote access is managed;
- Access permissions and authorization is controlled; (Least priv / SoD)
- Networks are segmentate;
- IDs are bound to credentials and asserted;
- Authentication mechanisms are relevant to the risk of the interaction / transaction



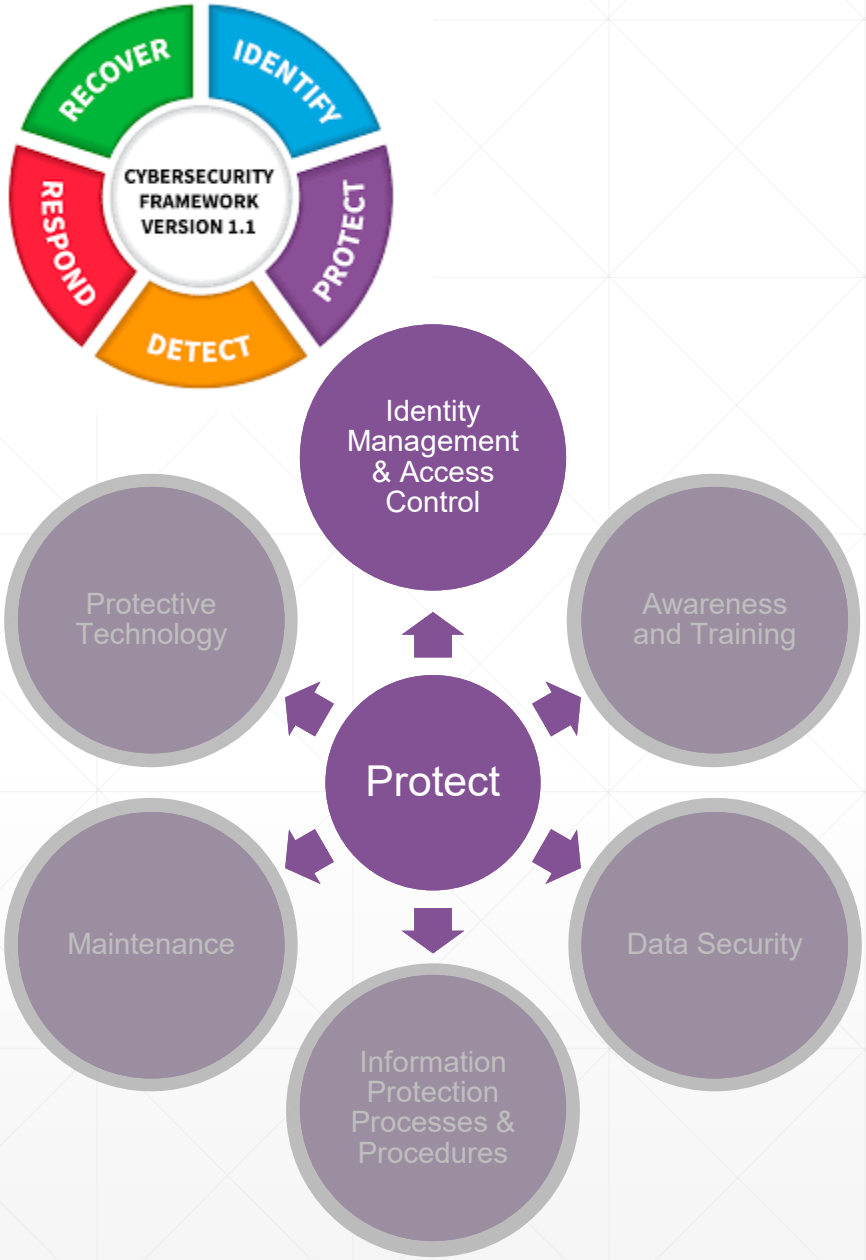
Subcategory	Informative References
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	· **CIS CSC** 1, 5, 15, 16 · **COBIT 5** DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.5.1 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
PR.AC-2: Physical access to assets is managed and protected	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 · **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8



Subcategory	Informative References
PR.AC-3: Remote access is managed	· **CIS CSC** 12 · **COBIT 5** APO13.01, DSS01.04, DSS05.03 · **ISA 62443-2-1:2009** 4.3.3.6.6 · **ISA 62443-3-3:2013** SR 1.13, SR 2.6 · **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	· **CIS CSC** 3, 5, 12, 14, 15, 16, 18 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.7.3 · **ISA 62443-3-3:2013** SR 2.1 · **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24



Subcategory	Informative References
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	· **CIS CSC** 9, 14, 15, 18 · **COBIT 5** DSS01.05, DSS05.02 · **ISA 62443-2-1:2009** 4.3.3.4 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8 · **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	· **CIS CSC**, 16 · **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 · **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3



Subcategory	Informative References
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	· **CIS CSC** 1, 12, 15, 16 · **COBIT 5** DSS05.04, DSS05.10, DSS06.10 · **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 · **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

PR.AT

- All users are informed and trained;'
- Privileged users, 3rd parties, Senior Executives, physical security personnel and cybersecurity personnel understand their roles and (security) responsibilities

Subcategory	Informative References
PR.AT-1: All users are informed and trained	· **CIS CSC** 17, 18 · **COBIT 5** APO07.03, BAI05.07 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 · **NIST SP 800-53 Rev. 4** AT-2, PM-13
PR.AT-2: Privileged users understand their roles and responsibilities	· **CIS CSC** 5, 17, 18 · **COBIT 5** APO07.02, DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	· **CIS CSC** 17 · **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16

Subcategory	Informative References
PR.AT-4: Senior executives understand their roles and responsibilities	· **CIS CSC** 17, 19 · **COBIT 5** EDM01.01, APO01.02, APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	· **CIS CSC** 17 · **COBIT 5** APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13

PR.DS

- Data at rest and in transit is protected;
- Assets are managed when be removed, transferred or disposed;
- Capacity is managed;
- DLP is implemented;
- Software, firmware, hardware and information integrity checking is implemented;
- Dev/Test environments are separated from production

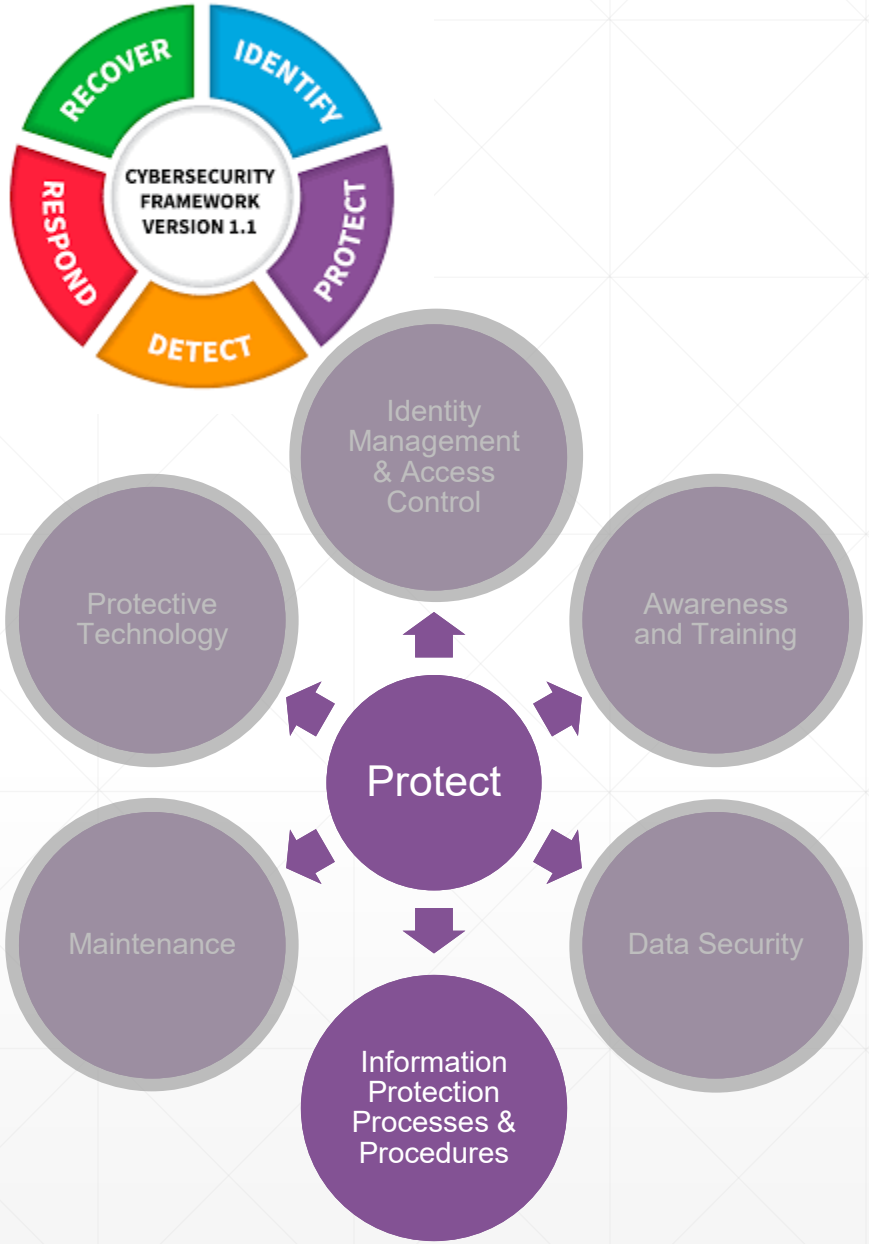
Subcategory	Informative References
PR.DS-1: Data-at-rest is protected	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 · **ISA 62443-3-3:2013** SR 3.4, SR 4.1 · **ISO/IEC 27001:2013** A.8.2.3 · **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
PR.DS-2: Data-in-transit is protected	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, DSS05.02, DSS06.06 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· **CIS CSC** 1 · **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 · **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16

Subcategory	Informative References
PR.DS-4: Adequate capacity to ensure availability is maintained	· **CIS CSC** 1, 2, 13 · **COBIT 5** APO13.01, BAI04.04 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 · **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
PR.DS-5: Protections against data leaks are implemented	· **CIS CSC** 13 · **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 · **ISA 62443-3-3:2013** SR 5.2 · **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4

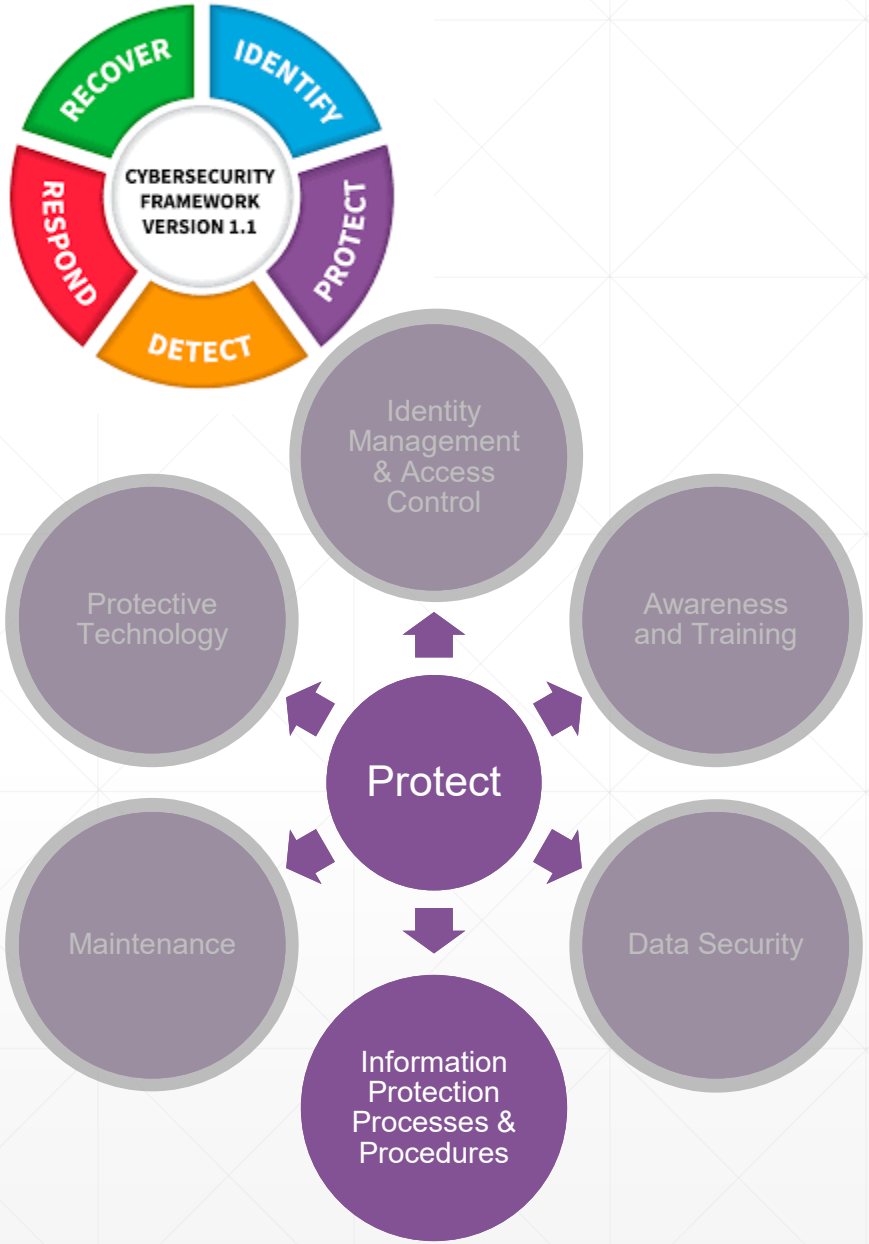
Subcategory	Informative References
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	· **CIS CSC** 2, 3 · **COBIT 5** APO01.06, BAI06.01, DSS06.02 · **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 · **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** SC-16, SI-7
PR.DS-7: The development and testing environment(s) are separate from the production environment	· **CIS CSC** 18, 20 · **COBIT 5** BAI03.08, BAI07.04 · **ISO/IEC 27001:2013** A.12.1.4 · **NIST SP 800-53 Rev. 4** CM-2
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	· **COBIT 5** BAI03.05 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISO/IEC 27001:2013** A.11.2.4 · **NIST SP 800-53 Rev. 4** SA-10, SI-7

PR.IP

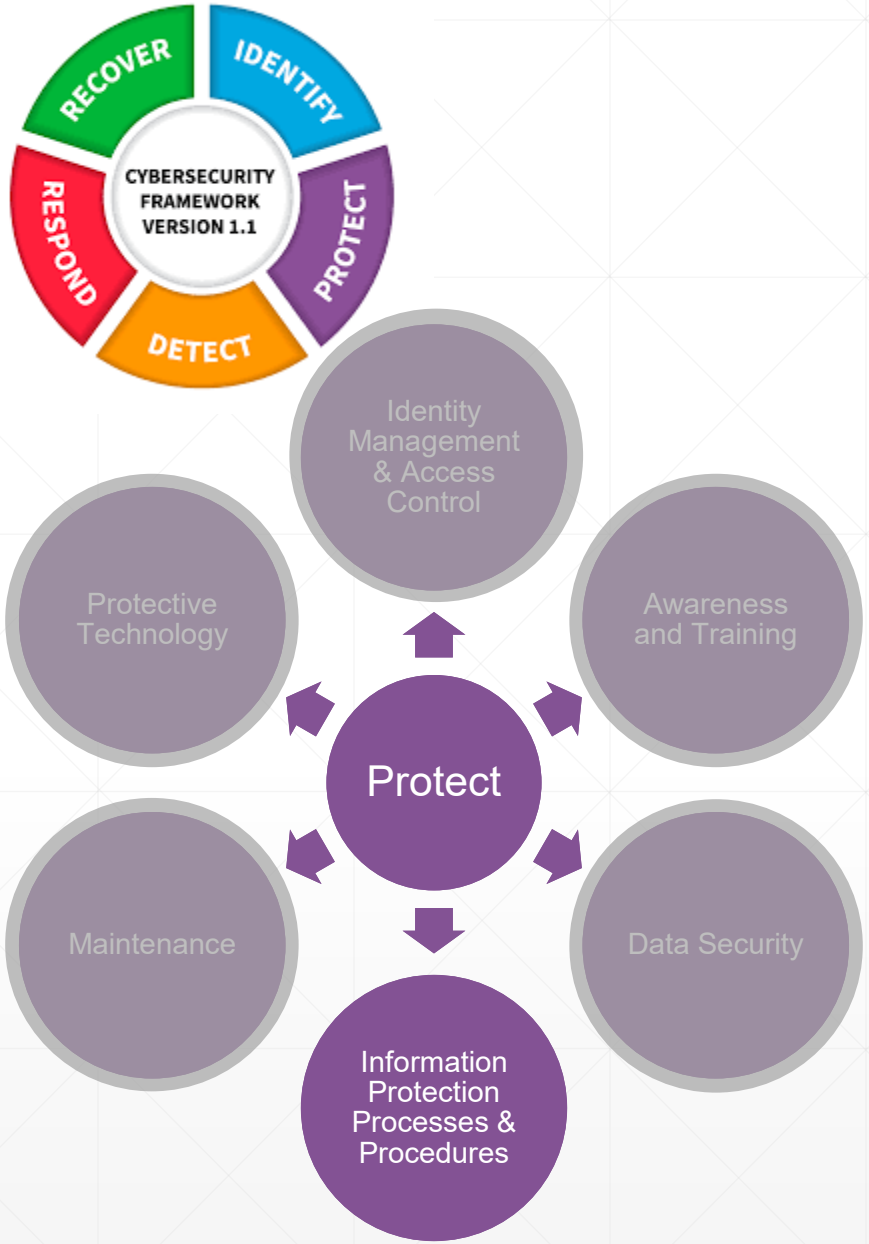
- Secure baselines are developed and maintained;
- An SDLC is implemented;
- Change control is implemented;
- Backups are taken, maintained and tested;
- Physical operation environment for assets is implemented;
- Data disposal / destruction policies are followed;
- Effectiveness of protection technology and lessons for improvement is shared;
- Response and recovery plans are developed, managed and tested;
- HR security policy and processes are developed;
- A VA plan is developed, implemented and updated.



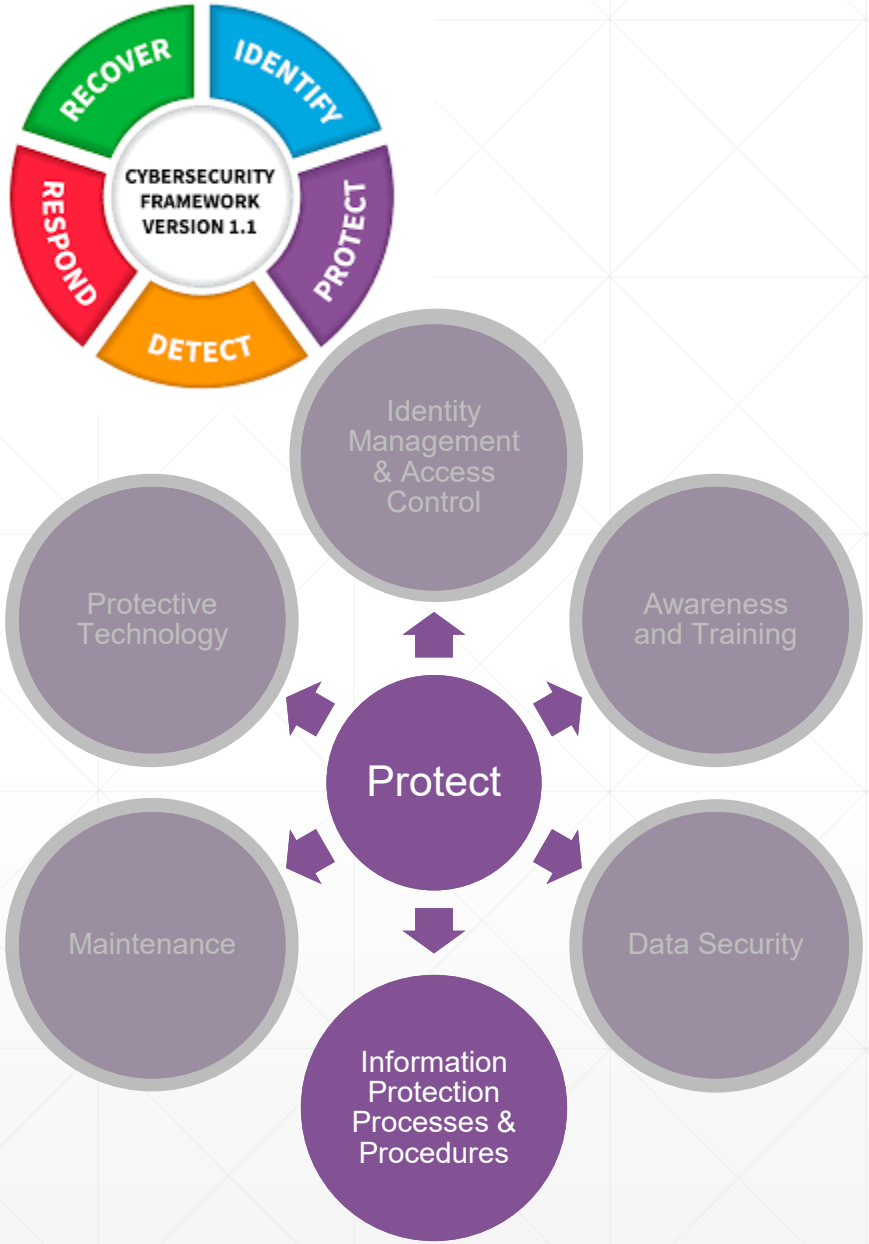
Subcategory	Informative References
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	· **CIS CSC** 3, 9, 11 · **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
PR.IP-2: A System Development Life Cycle to manage systems is implemented	· **CIS CSC** 18 · **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 · **ISA 62443-2-1:2009** 4.3.4.3.3 · **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17



Subcategory	Informative References
PR.IP-3: Configuration change control processes are in place	· **CIS CSC** 3, 11 · **COBIT 5** BAI01.06, BAI06.01 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
PR.IP-4: Backups of information are conducted, maintained, and tested	· **CIS CSC** 10 · **COBIT 5** APO13.01, DSS01.01, DSS04.07 · **ISA 62443-2-1:2009** 4.3.4.3.9 · **ISA 62443-3-3:2013** SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 · **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18



Subcategory	Informative References
PR.IP-6: Data is destroyed according to policy	· **COBIT 5** BAI09.03, DSS05.06 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · **NIST SP 800-53 Rev. 4** MP-6
PR.IP-7: Protection processes are improved	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
PR.IP-8: Effectiveness of protection technologies is shared	· **COBIT 5** BAI08.04, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	· **CIS CSC** 19 · **COBIT 5** APO12.06, DSS04.03 · **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17



Subcategory	Informative References
PR.IP-10: Response and recovery plans are tested	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	· **CIS CSC** 5, 16 · **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 · **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
PR.IP-12: A vulnerability management plan is developed and implemented	· **CIS CSC** 4, 18, 20 · **COBIT 5** BAI03.10, DSS05.01, DSS05.02 · **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 · **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2

PR.MA

- Maintenance / repair of assets is monitored, recorded and conducted with approved and controlled tools;
- Remote maintenance is managed and performed in a way that prevents unauthorized access

Subcategory	Informative References
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	· **COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.7 · **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 · **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	· **CIS CSC** 3, 5 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 · **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 · **NIST SP 800-53 Rev. 4** MA-4

PR.PT

- Audit / log records are determined, documented and implemented;
- Removable media is protected and its use restricted;
- Systems / applications apply “least functionality”
- Communication and control (Management networks) are protected;
- Mechanisms to achieve resilience requirements are implemented.

Subcategory	Informative References
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	· **CIS CSC** 1, 3, 5, 6, 14, 15, 16 · **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · **NIST SP 800-53 Rev. 4** AU Family
PR.PT-2: Removable media is protected and its use restricted according to policy	· **CIS CSC** 8, 13 · **COBIT 5** APO13.01, DSS05.02, DSS05.06 · **ISA 62443-3-3:2013** SR 2.3 · **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8

Subcategory	Informative References
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	· **CIS CSC** 3, 11, 14 · **COBIT 5** DSS05.02, DSS05.05, DSS06.06 · **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 4** AC-3, CM-7
PR.PT-4: Communications and control networks are protected	· **CIS CSC** 8, 12, 15 · **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43

Subcategory	Informative References
PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	· **COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 · **ISA 62443-2-1:2009** 4.3.2.5.2 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

NIST Cybersecurity Framework

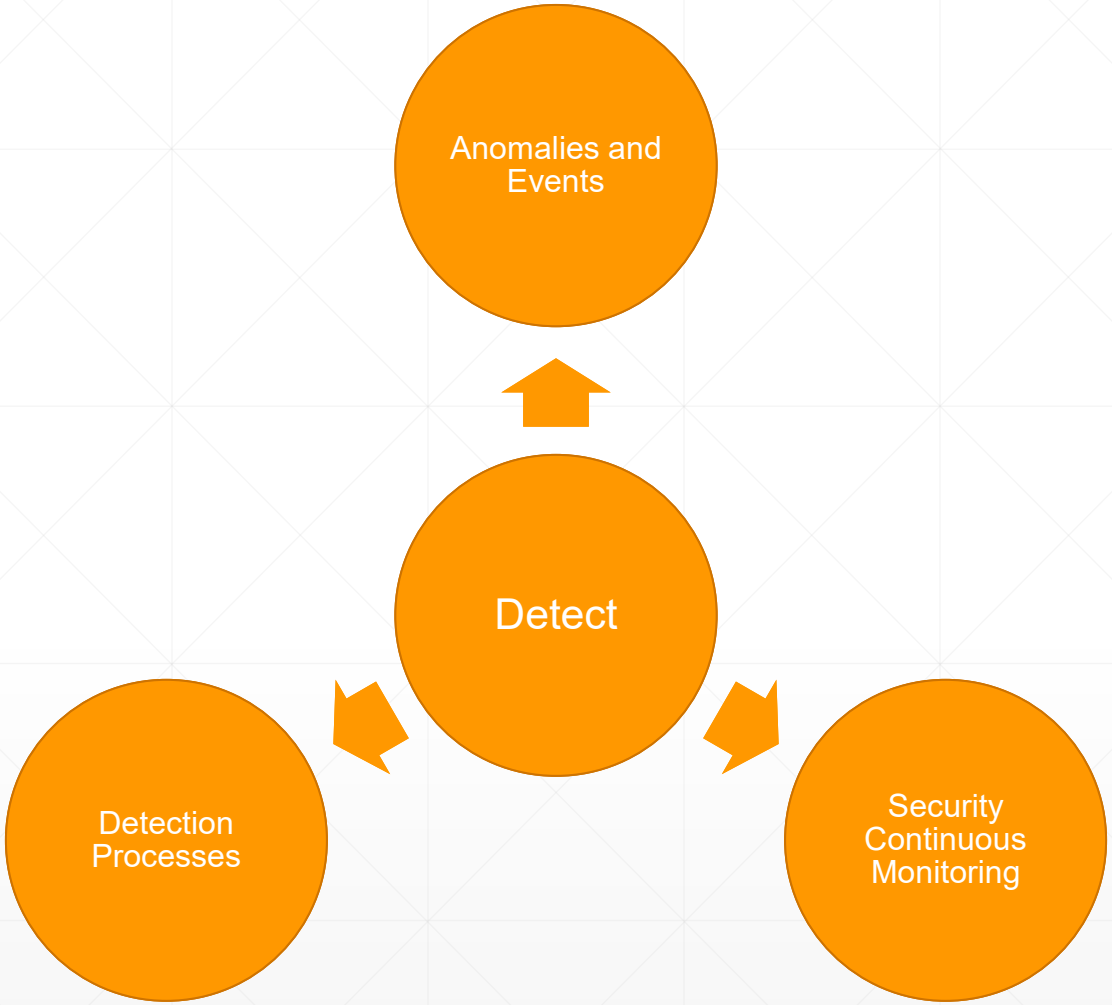
NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018

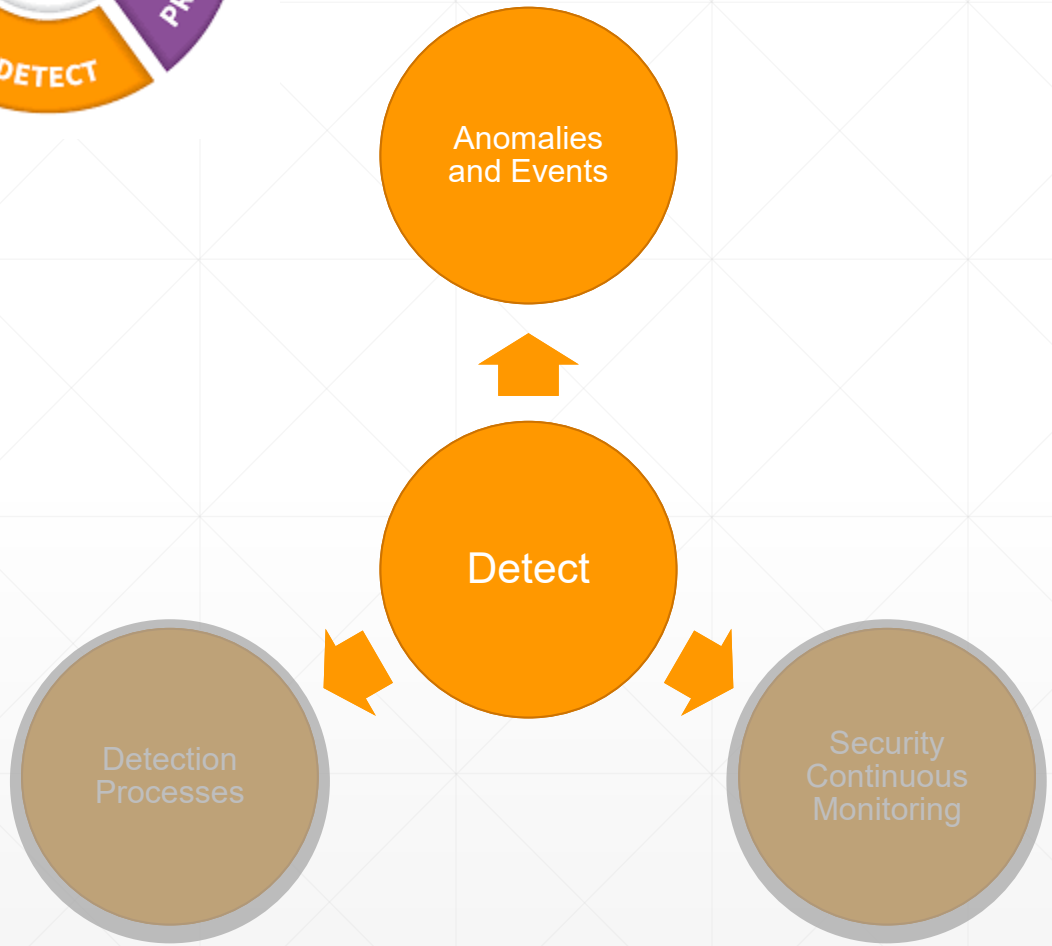
What techniques can identify incidents?

DETECT

Ensure the organization is capable of identifying a cybersecurity event (incident) when it happens

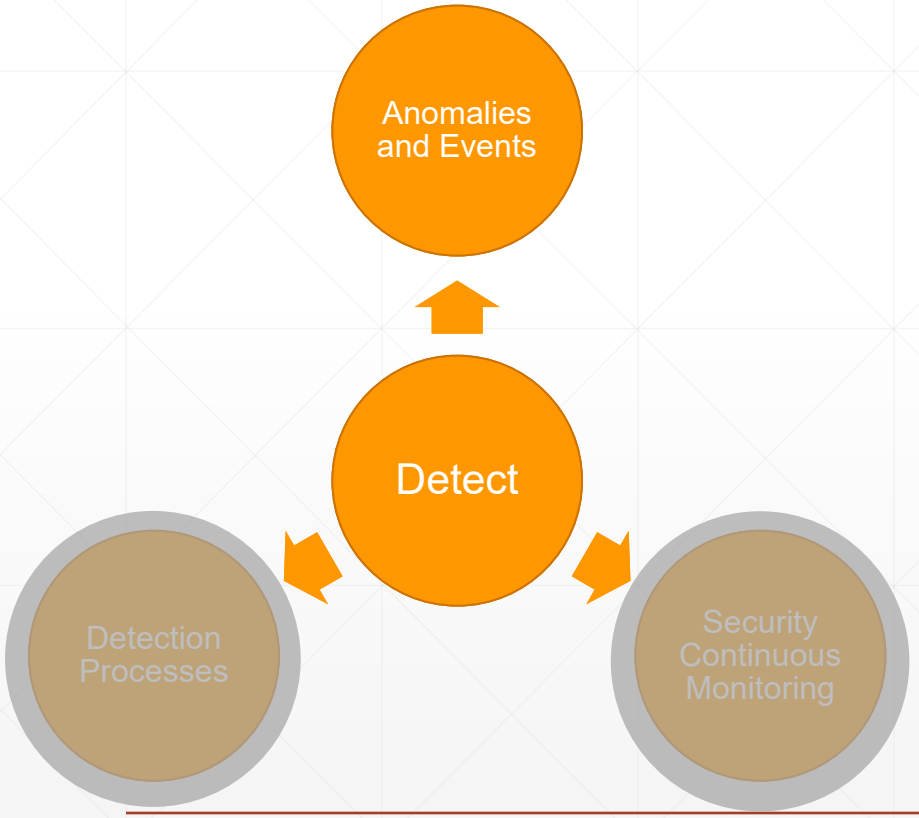

RECOVER
IDENTIFY
CYBERSECURITY
FRAMEWORK
VERSION 1.1
RESPOND
PROTECT
DETECT


Anomalies and Events
Detect
Detection Processes
Security Continuous Monitoring

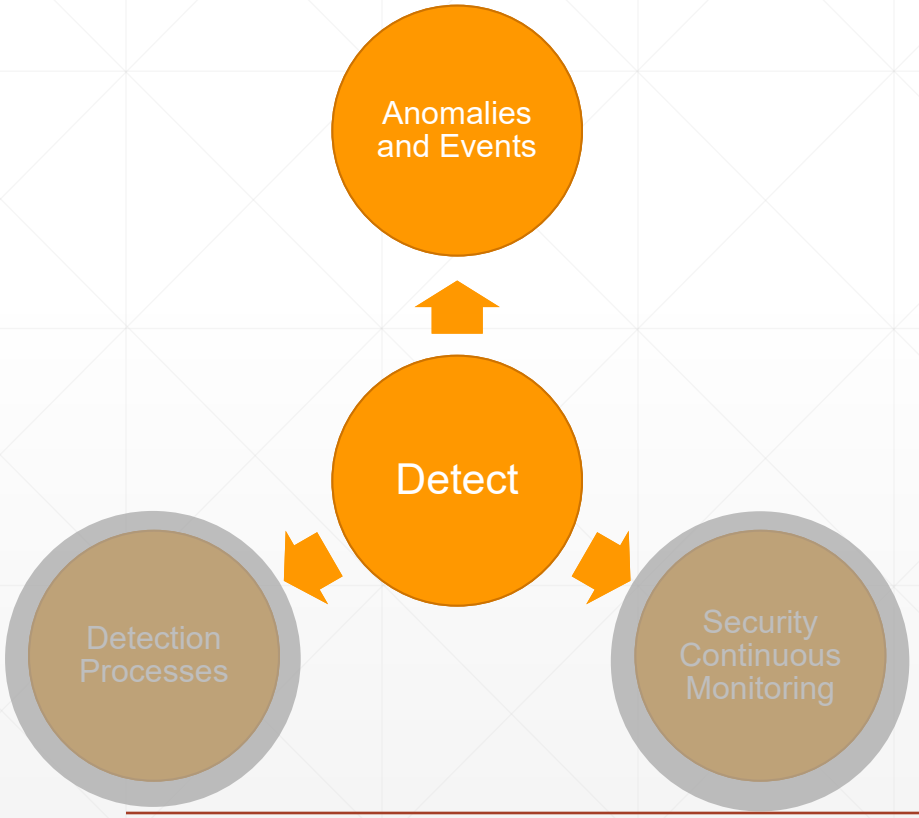


DE.AE

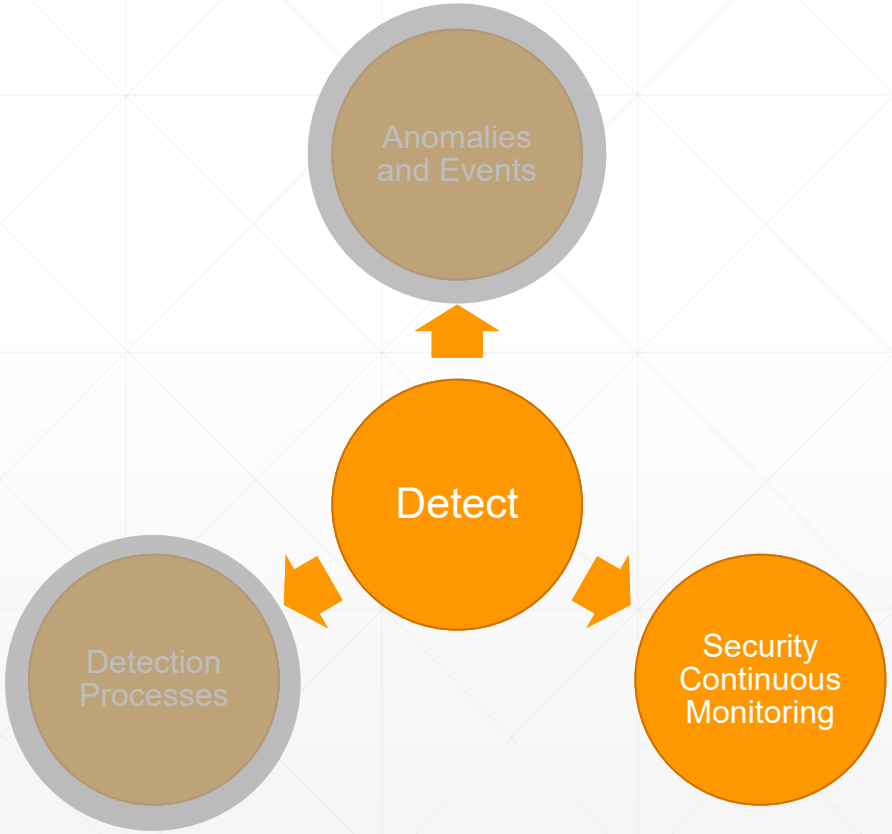
- Data flow baselines are established and managed;
- Detected events are analyzed to understand attack target, methods;
- Event data is collected and correlated from multiple sources;
- Impact of events is determined;
- Incident thresholds are established.



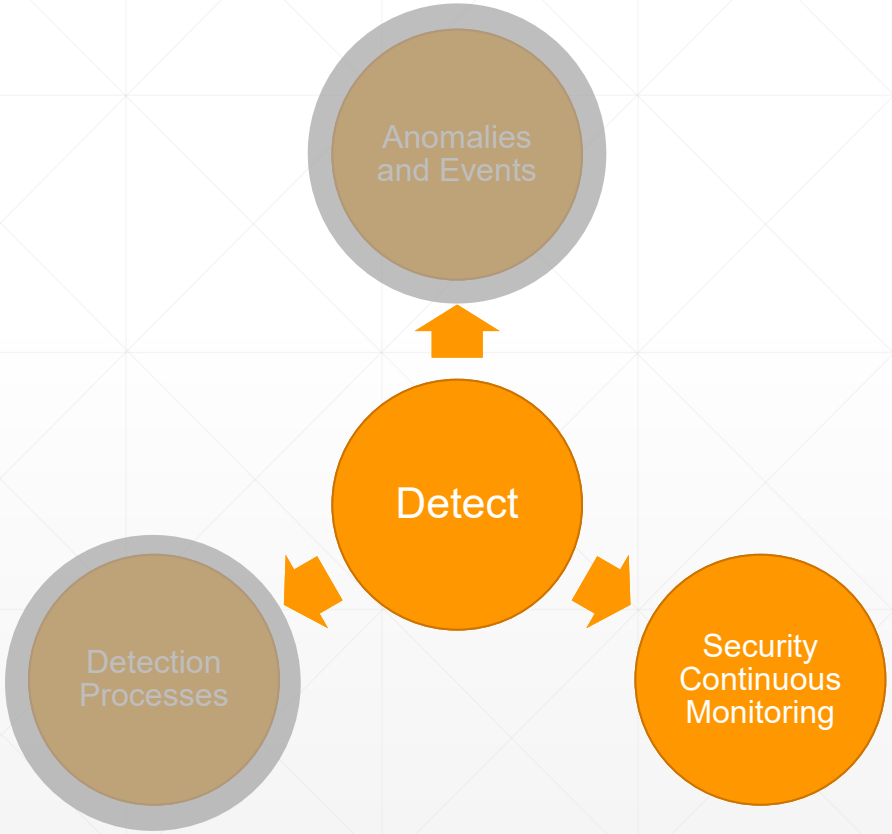
Subcategory	Informative References
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	· **CIS CSC** 1, 4, 6, 12, 13, 15, 16 · **COBIT 5** DSS03.01 · **ISA 62443-2-1:2009** 4.4.3.3 · **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
DE.AE-2: Detected events are analyzed to understand attack targets and methods	· **CIS CSC** 3, 6, 13, 15 · **COBIT 5** DSS05.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
DE.AE-3: Event data are collected and correlated from multiple sources and sensors	· **CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 · **COBIT 5** BAI08.02 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4



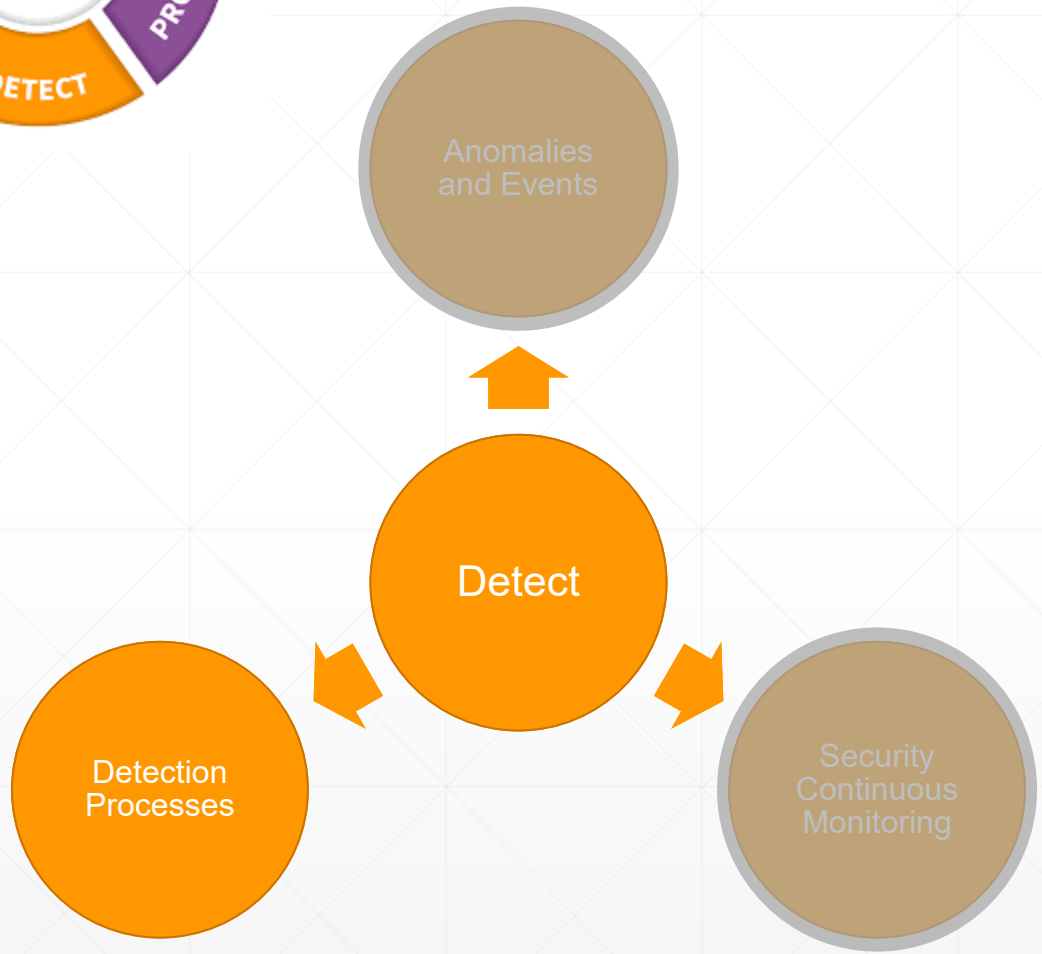
Subcategory	Informative References
DE.AE-4: Impact of events is determined	· **CIS CSC** 4, 6 · **COBIT 5** APO12.06, DSS03.01 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
DE.AE-5: Incident alert thresholds are established	· **CIS CSC** 6, 19 · **COBIT 5** APO12.06, DSS03.01 · **ISA 62443-2-1:2009** 4.2.3.10 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8



Subcategory	Informative References
DE.CM-4: Malicious code is detected	· **CIS CSC** 4, 7, 8, 12 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.3.4.3.8 · **ISA 62443-3-3:2013** SR 3.2 · **ISO/IEC 27001:2013** A.12.2.1 · **NIST SP 800-53 Rev. 4** SI-3, SI-8
DE.CM-5: Unauthorized mobile code is detected	· **CIS CSC** 7, 8 · **COBIT 5** DSS05.01 · **ISA 62443-3-3:2013** SR 2.4 · **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 · **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	· **COBIT 5** APO07.06, APO10.05 · **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4

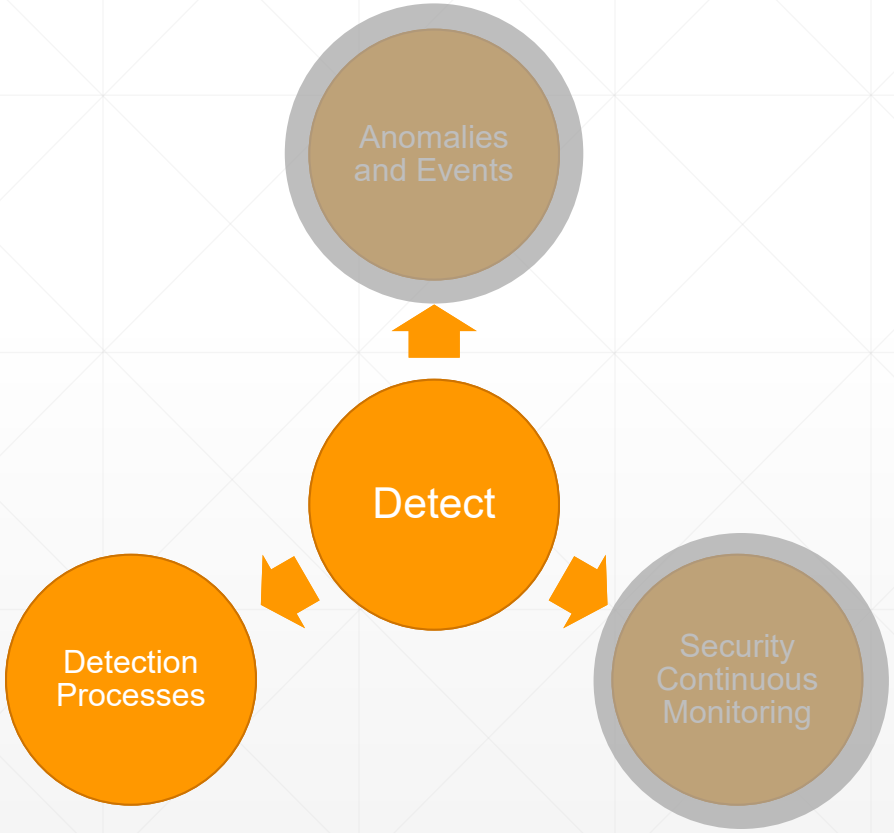


Subcategory	Informative References
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	· **CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 · **COBIT 5** DSS05.02, DSS05.05 · **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
DE.CM-8: Vulnerability scans are performed	· **CIS CSC** 4, 20 · **COBIT 5** BAI03.10, DSS05.01 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-5

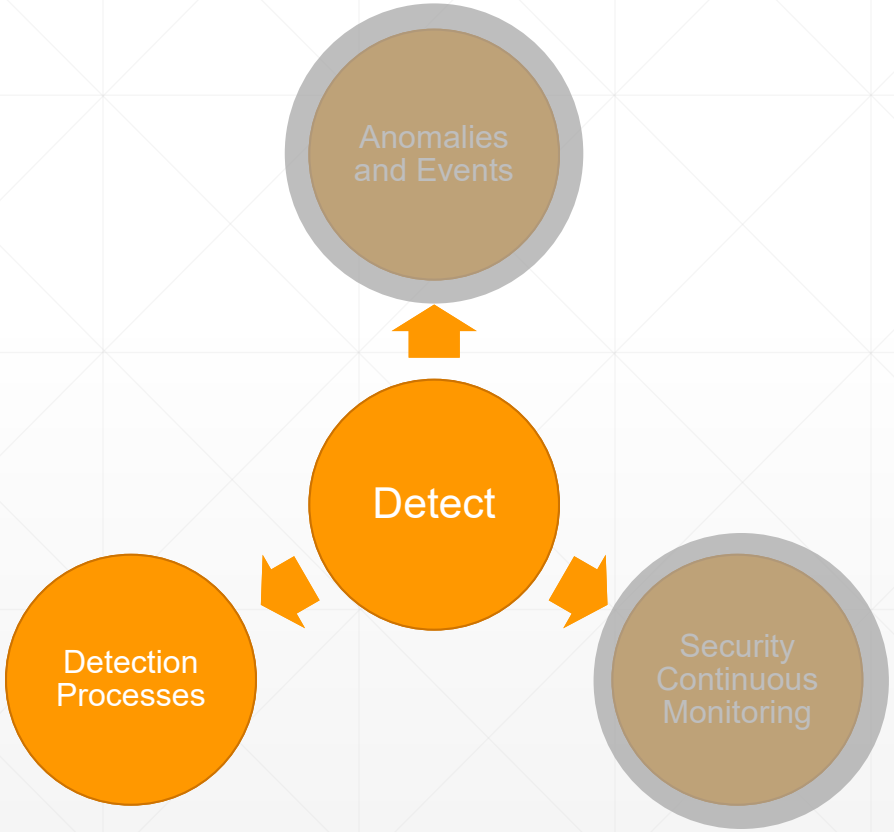


DE.CM

- Detection roles, responsibilities and activities are defined;
- Detection processes are tested;
- Event detection information is communicated;
- Detection processes are improved.



Subcategory	Informative References
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	· **CIS CSC** 19 · **COBIT 5** APO01.02, DSS05.01, DSS06.03 · **ISA 62443-2-1:2009** 4.4.3.1 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
DE.DP-2: Detection activities comply with all applicable requirements	· **COBIT 5** DSS06.01, MEA03.03, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 · **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
DE.DP-3: Detection processes are tested	· **COBIT 5** APO13.02, DSS05.02 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.14.2.8 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14



Subcategory	Informative References
DE.DP-4: Event detection information is communicated	· **CIS CSC** 19 · **COBIT 5** APO08.04, APO12.06, DSS02.05 · **ISA 62443-2-1:2009** 4.3.4.5.9 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 · **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
DE.DP-5: Detection processes are continuously improved	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

NIST Cybersecurity Framework

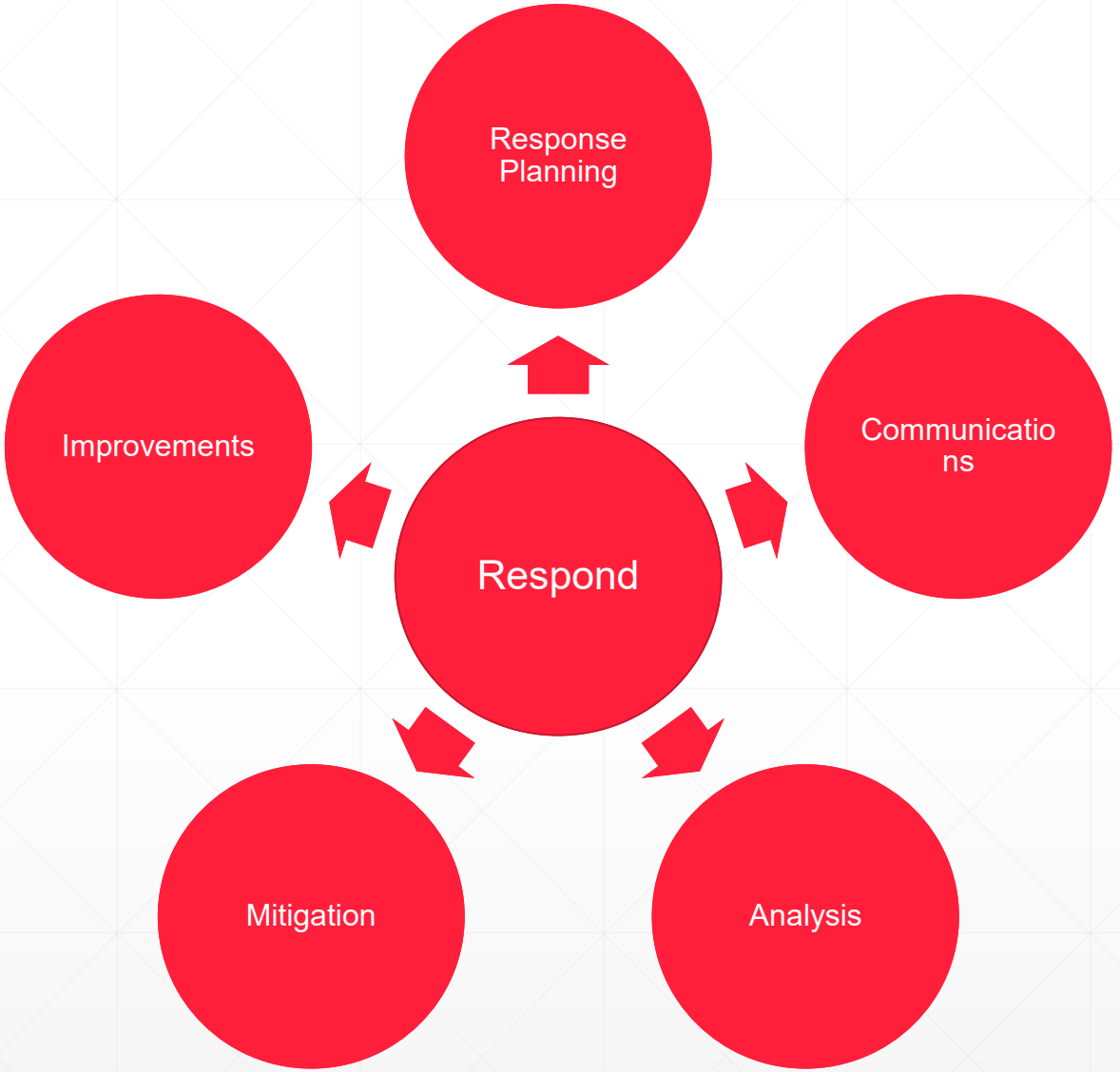
NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018

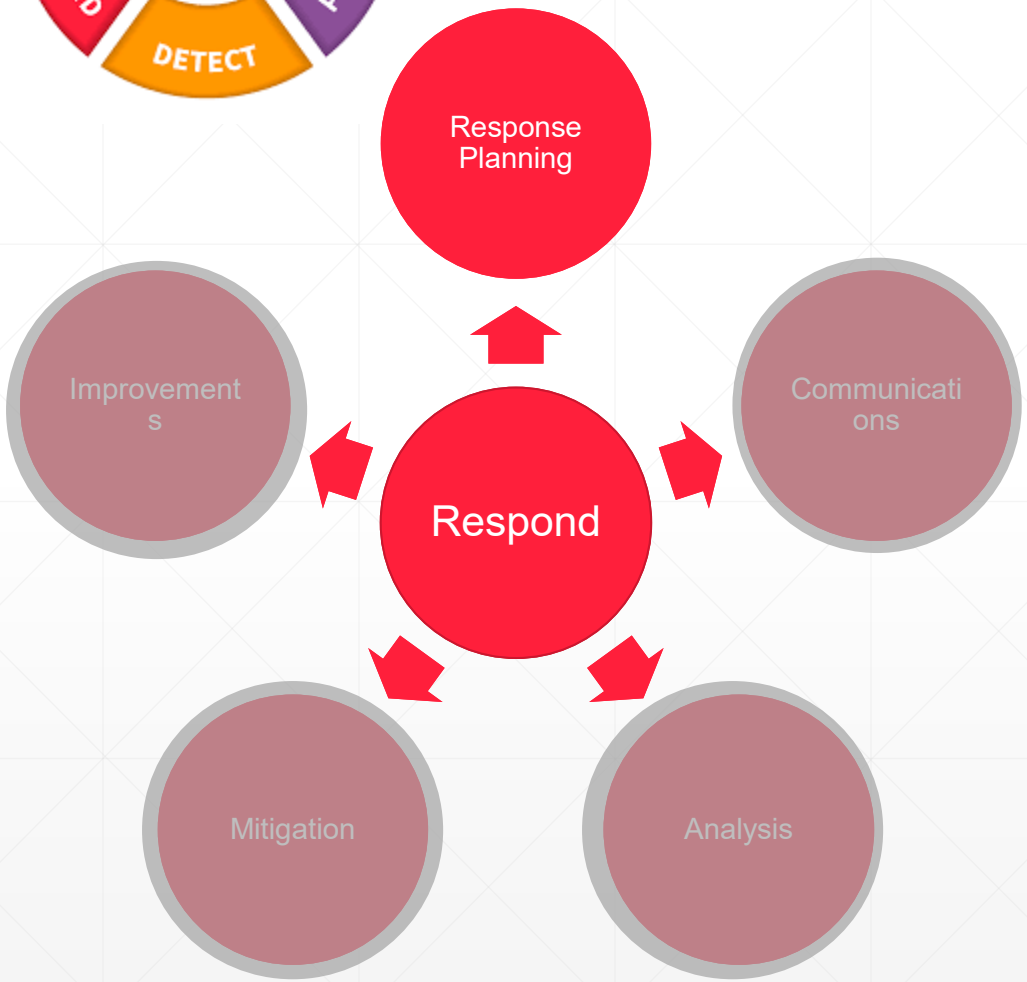
What techniques can contain impacts of incidents?

RESPONSE

Ensure the activities to take action if a cybersecurity event is identified are in place


RECOVER
IDENTIFY
CYBERSECURITY
FRAMEWORK
VERSION 1.1
RESPOND
PROTECT
DETECT


Response Planning
Improvements
Communications
Respond
Mitigation
Analysis



RS.RP

- Response plan is executed after an incident

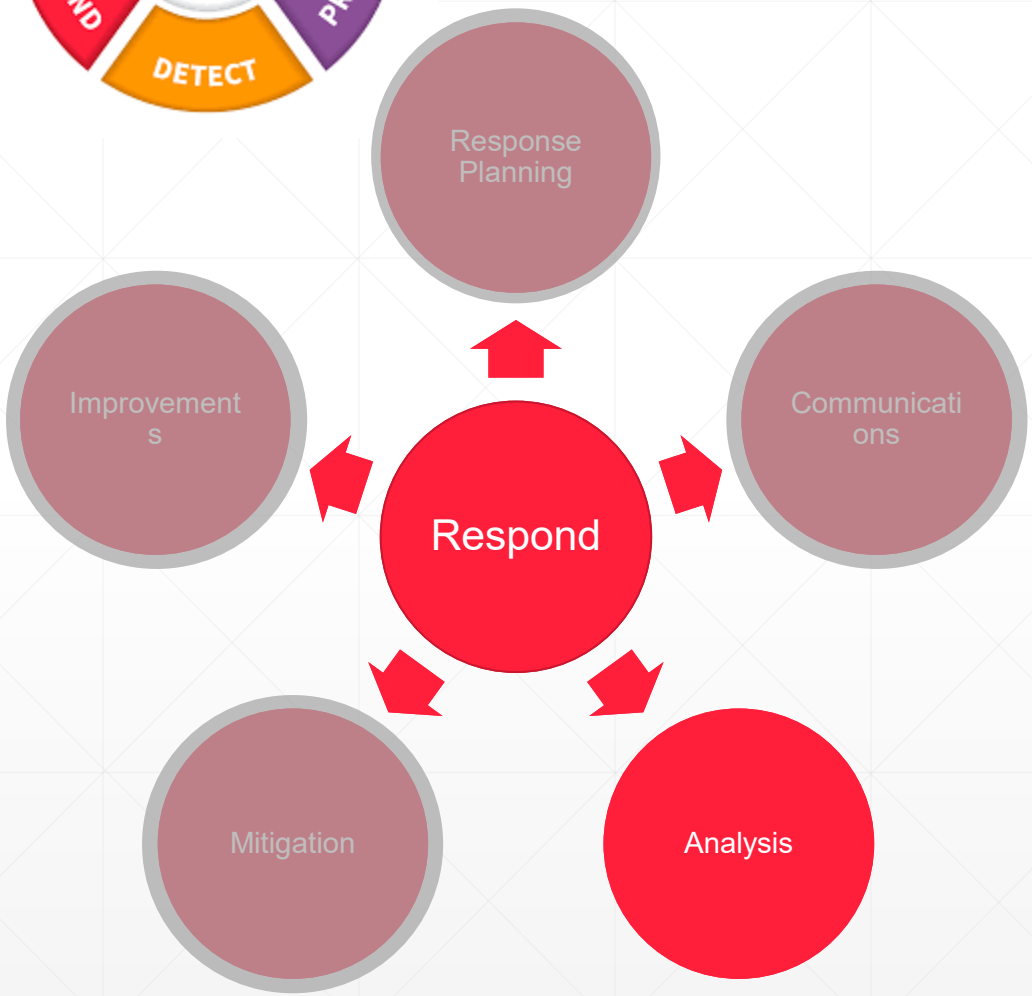
Subcategory	Informative References
RS.RP-1: Response plan is executed during or after an incident	• **CIS CSC** 19 • **COBIT 5** APO12.06, BAI01.10 • **ISA 62443-2-1:2009** 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8

RS.CO

- Response personnel know their responsibilities;
- Incidents are reported based on established criteria;
- Information is shared and coordination with stakeholders managed;

Subcategory	Informative References
RS.CO-1: Personnel know their roles and order of operations when a response is needed	· **CIS CSC** 19 · **COBIT 5** EDM03.02, APO01.02, APO12.03 · **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
RS.CO-2: Incidents are reported consistent with established criteria	· **CIS CSC** 19 · **COBIT 5** DSS01.03 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 · **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
RS.CO-3: Information is shared consistent with response plans	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.2 · **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4

Subcategory	Informative References
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	· **CIS CSC** 19 · **COBIT 5** BAI08.04 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15

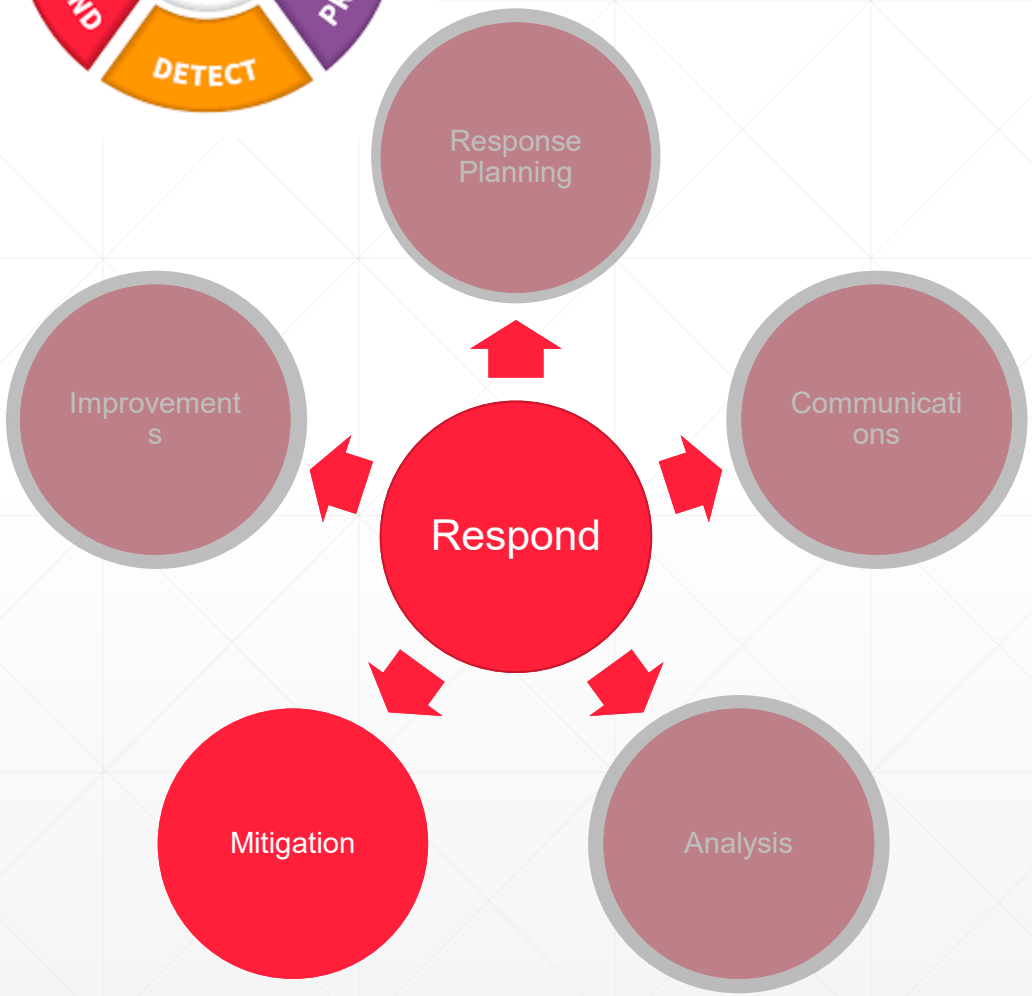


RS.AN

- Alerts from detection systems are investigated;
- Impact of the incident is understood;
- Forensic analysis is performed;
- Incidents are categorized;
- Processes to receive, analyze and respond to vulnerabilities are established.

Subcategory	Informative References
RS.AN-1: Notifications from detection systems are investigated	· **CIS CSC** 4, 6, 8, 19 · **COBIT 5** DSS02.04, DSS02.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
RS.AN-2: The impact of the incident is understood	· **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 · **NIST SP 800-53 Rev. 4** CP-2, IR-4
RS.AN-3: Forensics are performed	· **COBIT 5** APO12.06, DSS03.02, DSS05.07 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · **ISO/IEC 27001:2013** A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-7, IR-4

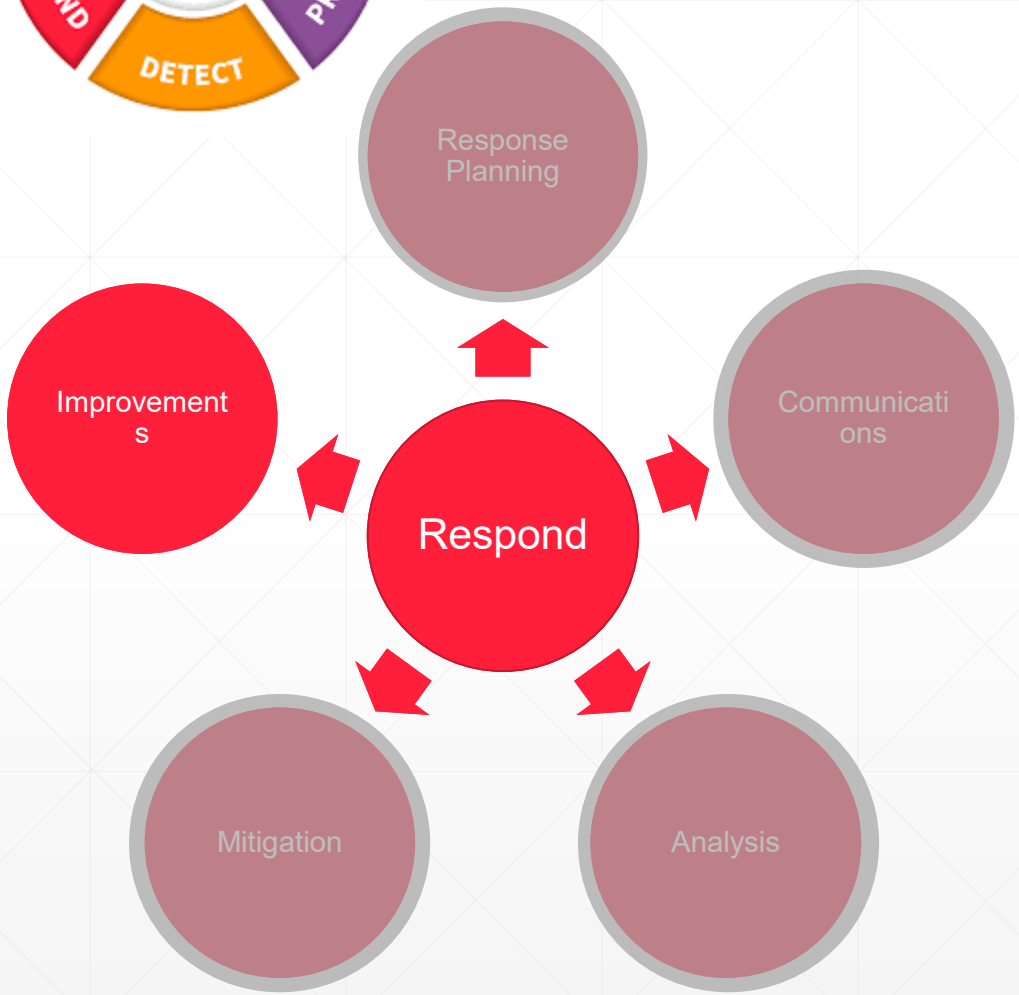
Subcategory	Informative References
RS.AN-4: Incidents are categorized consistent with response plans	· **CIS CSC** 19 · **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	· **CIS CSC** 4, 19 · **COBIT 5** EDM03.02, DSS05.07 · **NIST SP 800-53 Rev. 4** SI-5, PM-15



RS.MI

- Incidents are contained and mitigated;
- New vulnerabilities are mitigated or accepted as risks.

Subcategory	Informative References
RS.MI-1: Incidents are contained	· **CIS CSC** 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4
RS.MI-2: Incidents are mitigated	· **CIS CSC** 4, 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	· **CIS CSC** 4 · **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5



RS.IM

- Response plans incorporate lessons learnt;
- Response strategies are updated.

Subcategory	Informative References
RS.IM-1: Response plans incorporate lessons learned	· **COBIT 5** BAI01.13 · **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RS.IM-2: Response strategies are updated	· **COBIT 5** BAI01.13, DSS04.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

NIST Cybersecurity Framework

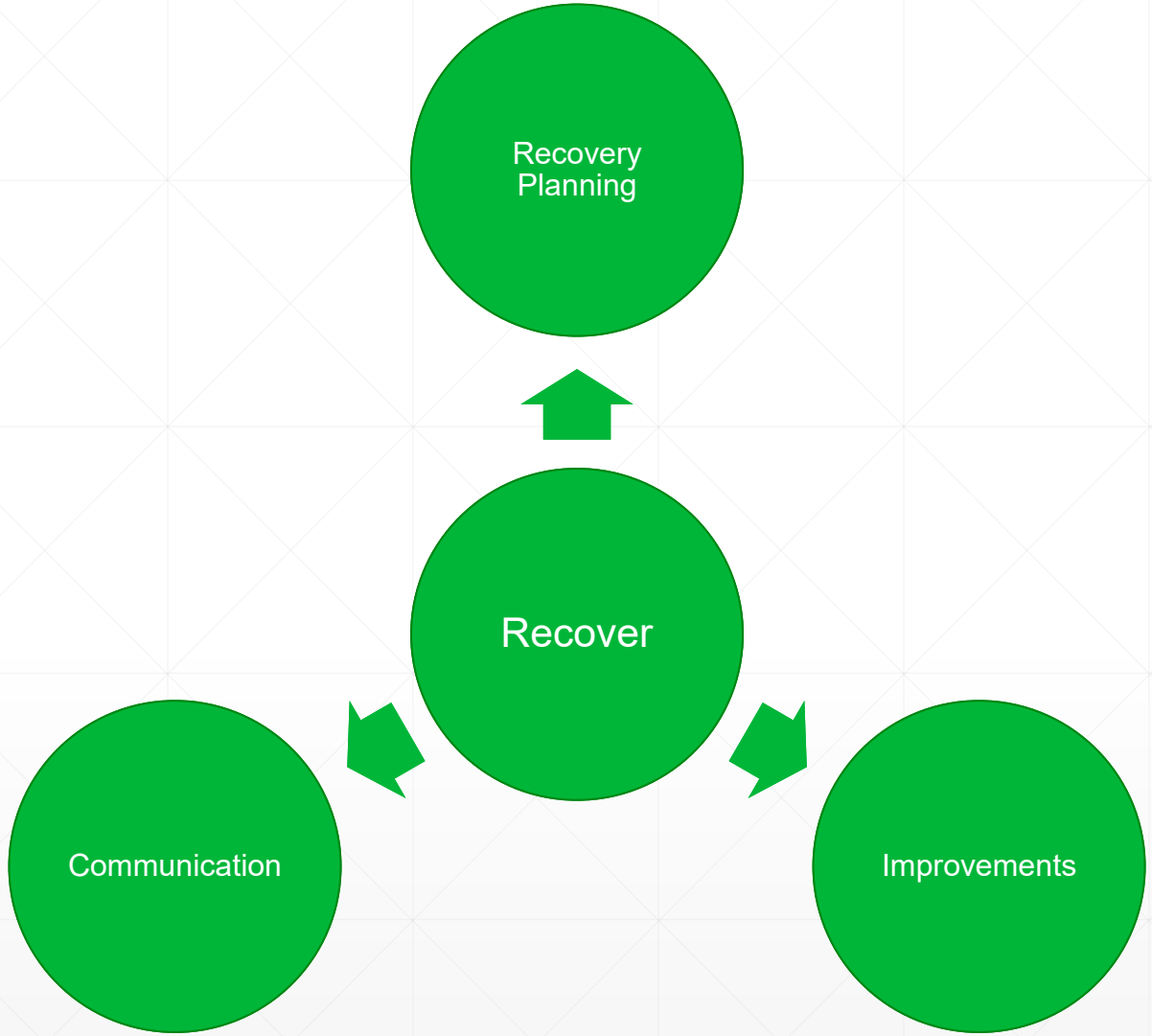
NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018

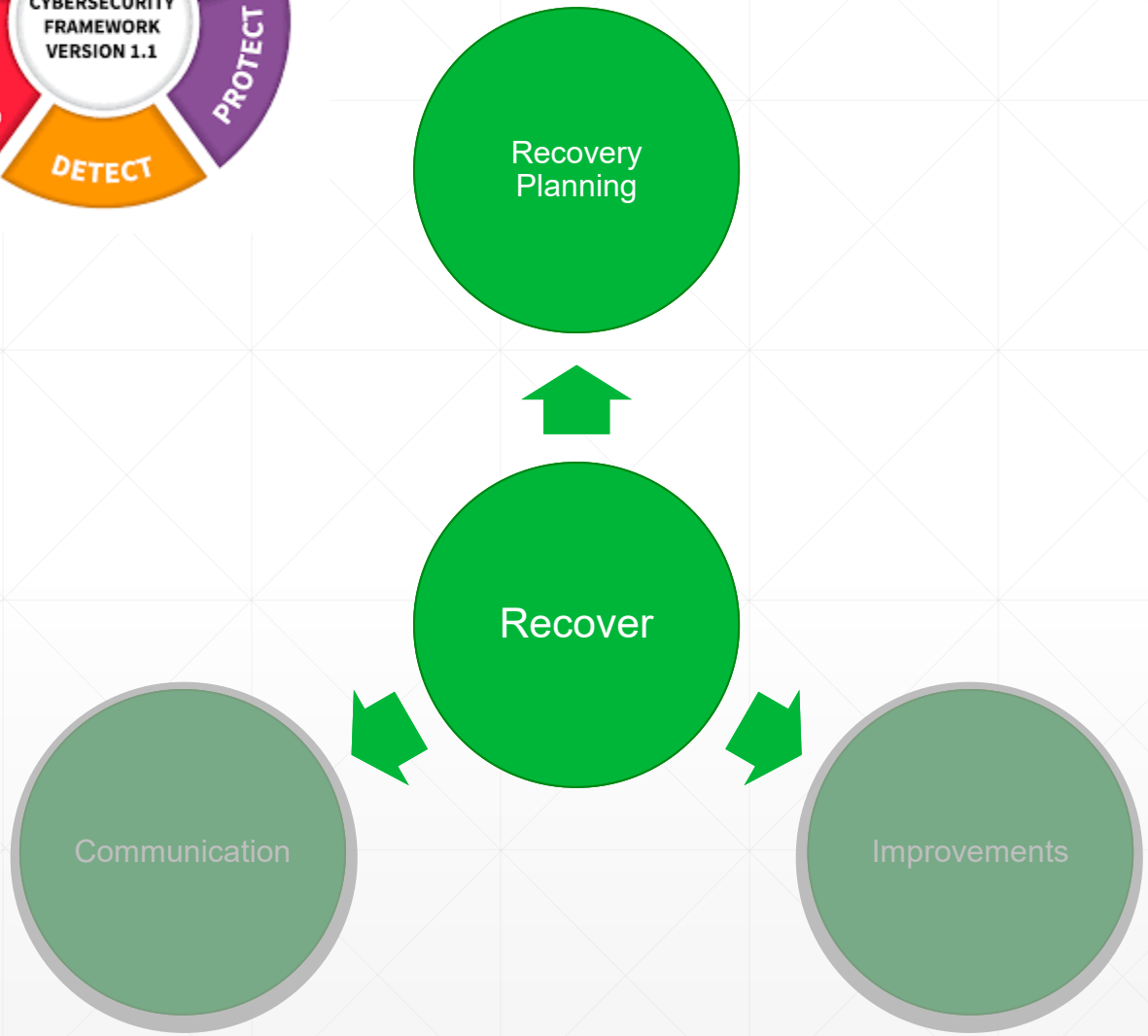
What techniques can restore capabilities?

RECOVER

Develop and implement recovery plans to ensure that the impact of a cybersecurity event can be minimized and normal operations resumed in a timely manner

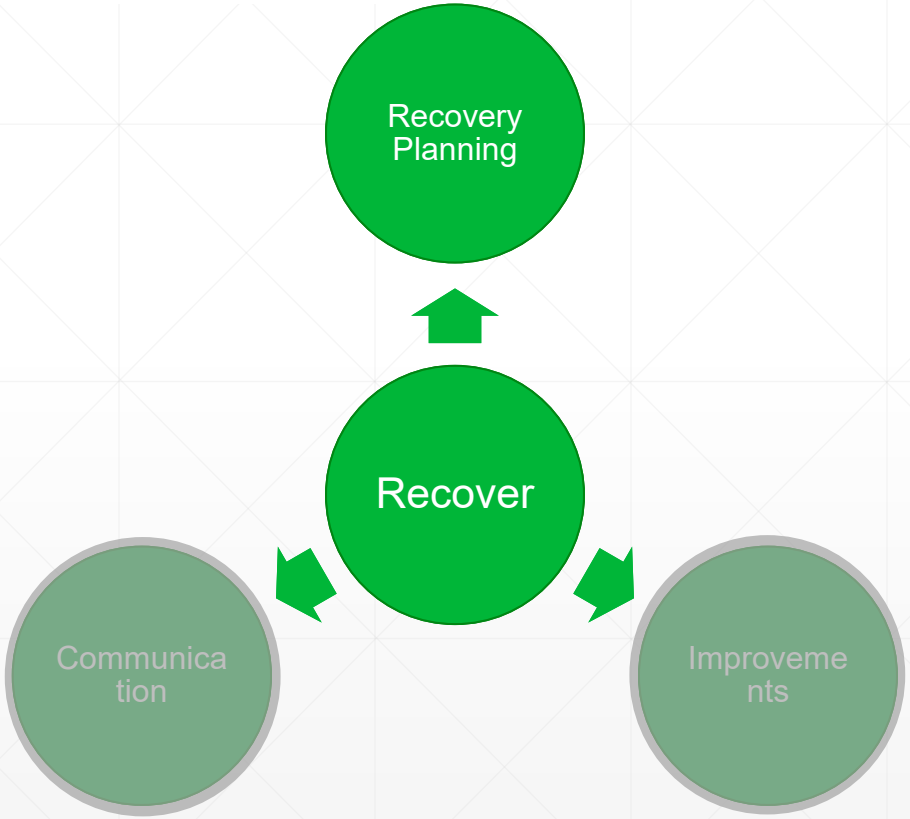

RECOVER
IDENTIFY
CYBERSECURITY
FRAMEWORK
VERSION 1.1
RESPOND
PROTECT
DETECT


Recovery
Planning
Recover
Communication
Improvements

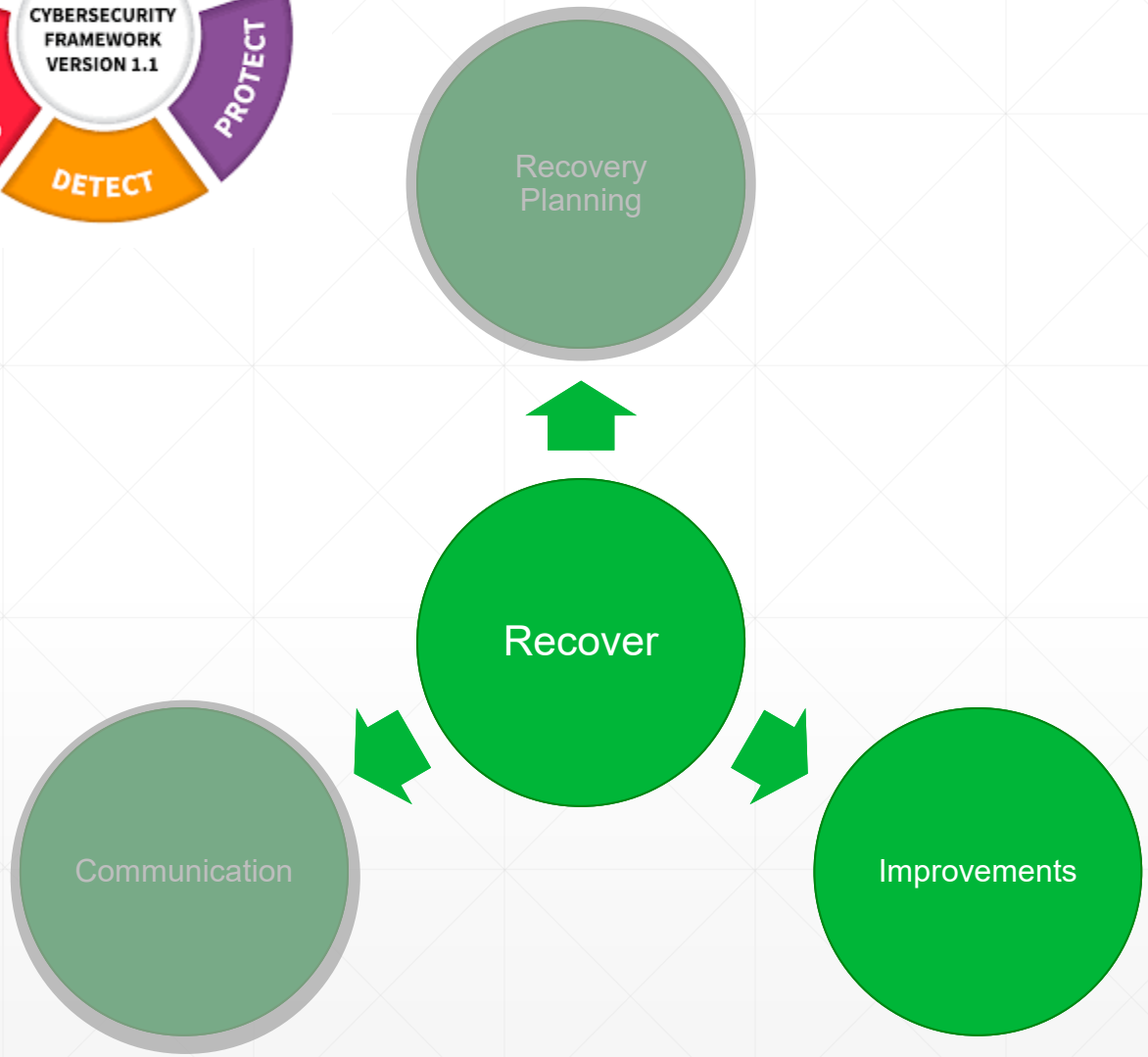


RC.RP

- Recovery plan is executed during or after a cybersecurity incident.

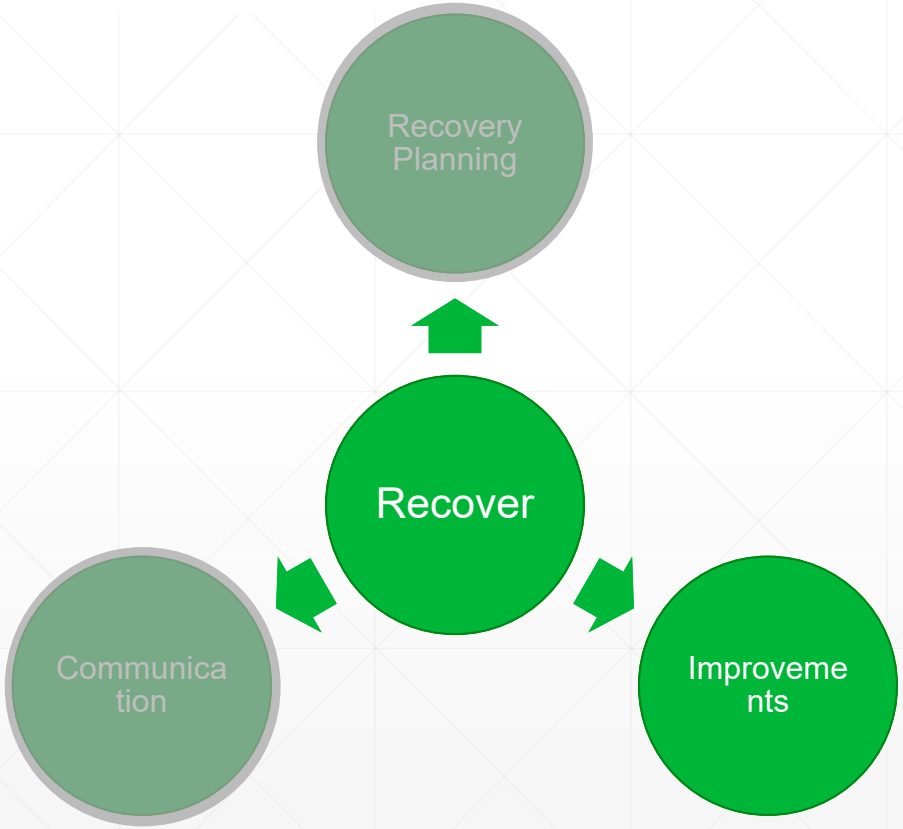


Subcategory	Informative References
RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	· **CIS CSC** 10 · **COBIT 5** APO12.06, DSS02.05, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8

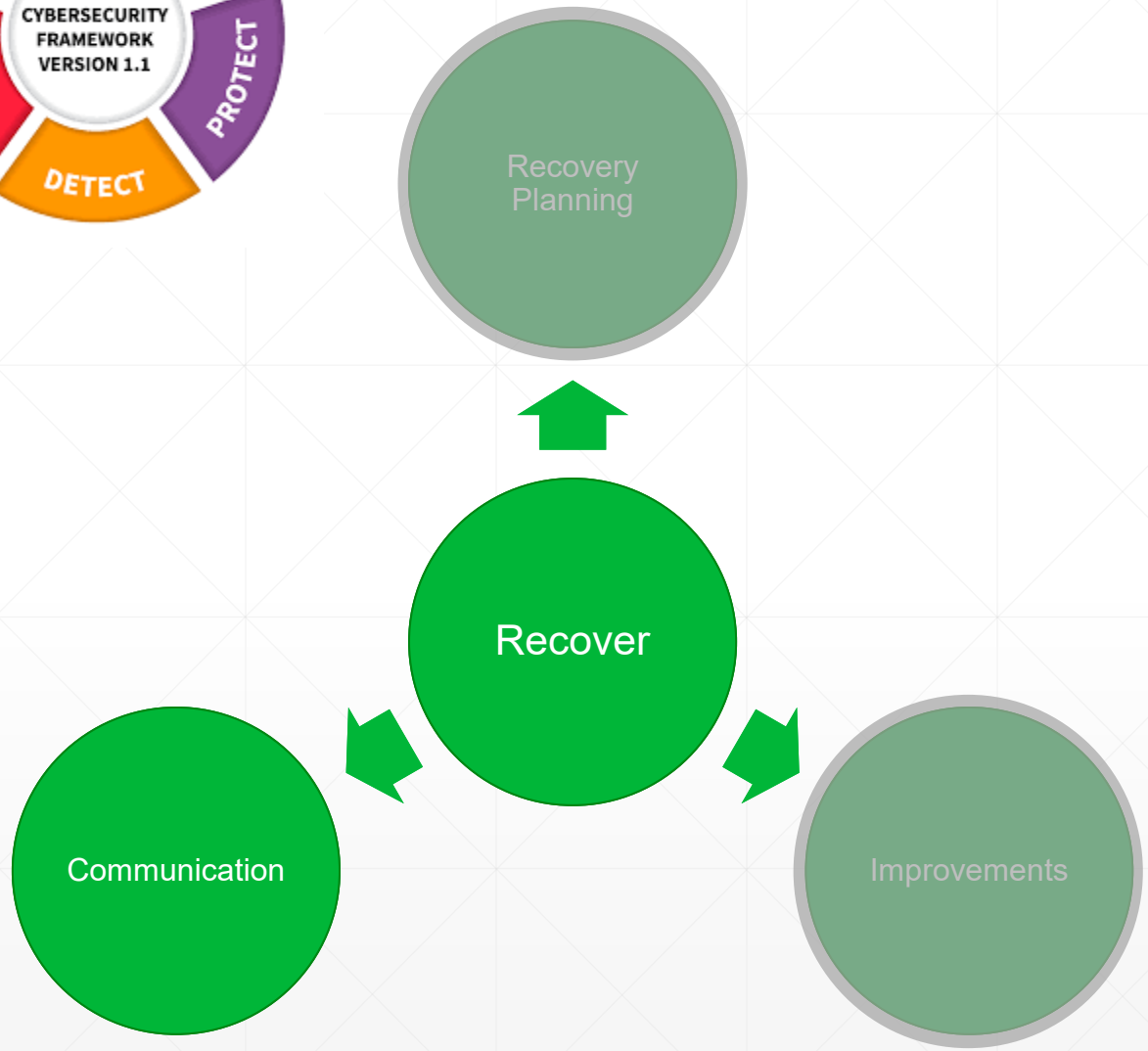


RC.IM

- Recovery plans incorporate lessons learned and strategies are updated.

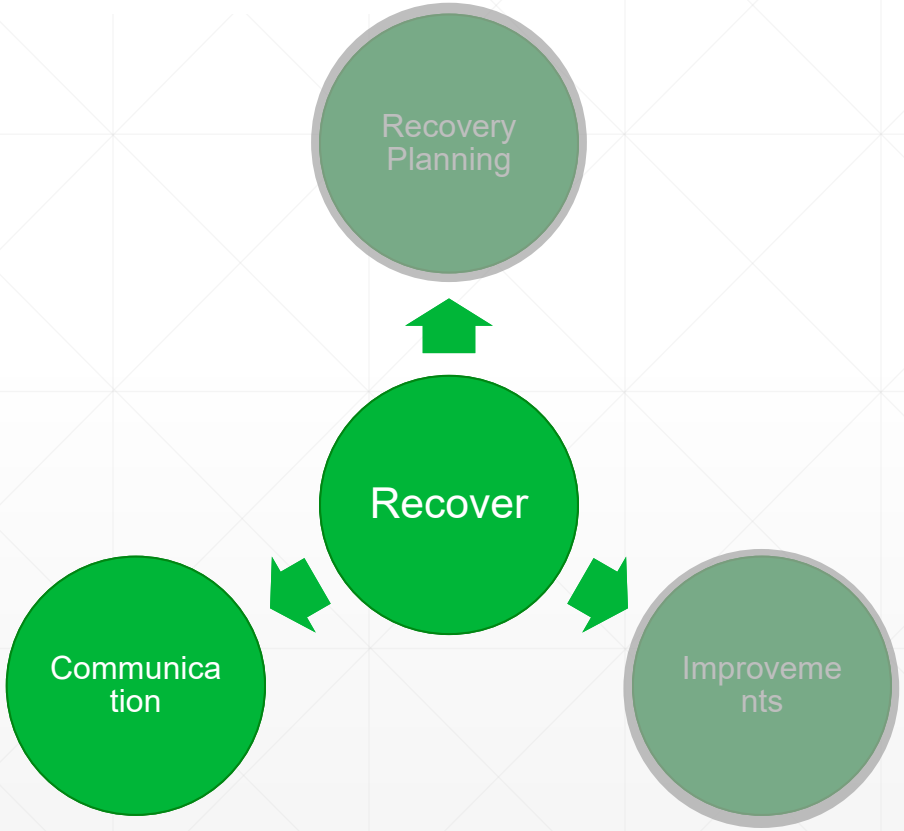


Subcategory	Informative References
RC.IM-1: Recovery plans incorporate lessons learned	· **COBIT 5** APO12.06, BAI05.07, DSS04.08 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RC.IM-2: Recovery strategies are updated	· **COBIT 5** APO12.06, BAI07.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8



RC.CO

- PR is managed;
- Reputation is repaired;
- Recovery activities are communicated.



Subcategory	Informative References
RC.CO-1: Public relations are managed	· **COBIT 5** EDM03.02 · **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
RC.CO-2: Reputation is repaired after an incident	· **COBIT 5** MEA03.02 · **ISO/IEC 27001:2013** Clause 7.4
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	· **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4

Workshop 2

ระบุการดำเนินงานในปัจจุบันขององค์กรให้สอดคล้องกับแต่ละ Function ของ NIST CSF version 1.1

IDENTIFY	- - -
PROTECT	- - -
DETECT	- - -
RESPOND	- - -
RECOVER	- - -

Q&A

Thank you