๗๒
(๒๔๘๕-๒๕๖๐)
ธนาคารแห่งประเทศไทย

แนวทางการบริหารความเสี่ยงด้าน IT และความเสี่ยงด้าน Cyber

โดยผู้แทนจาก
ฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ
สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน ธนาคารแห่งประเทศไทย

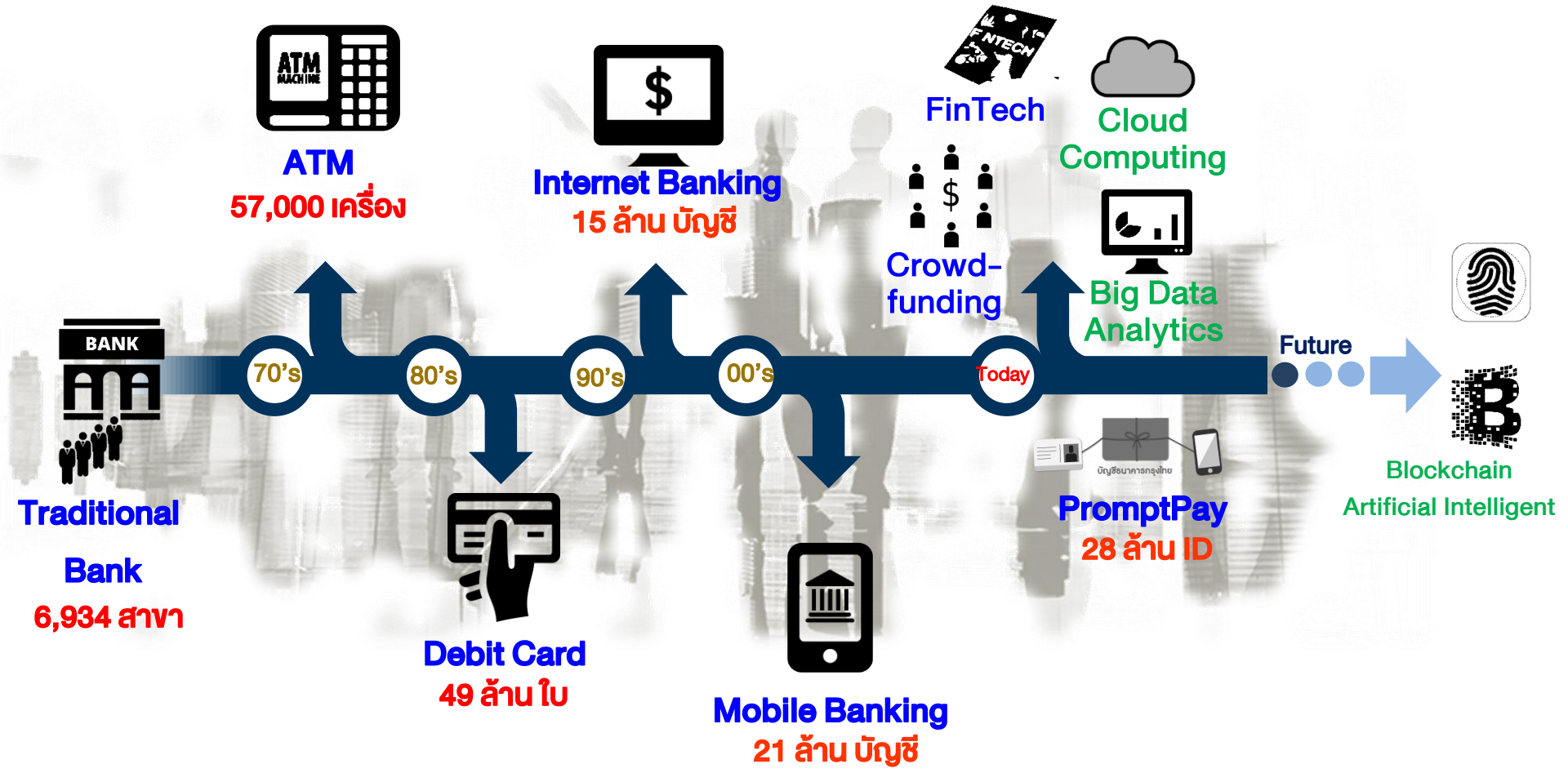
29 กันยายน 2560

สัมมนา “Future of Blockchain and Cybersecurity” ชมรมผู้ตรวจสอบภายในธนาคารและสถาบันการเงิน
ณ โรงแรมแอมบาสเดอร์

ธนาคารแห่งประเทศไทย

1. วิวัฒนาการและบทบาทของผู้ตรวจสอบภายใน
2. ความเสี่ยงด้าน IT and Cybersecurity Risks
3. การกำกับดูแล IT Risk Management และ Cyber Resilience ของสถาบันการเงิน

วิวัฒนาการ Digital Banking ปรับตัวเร็วขึ้น



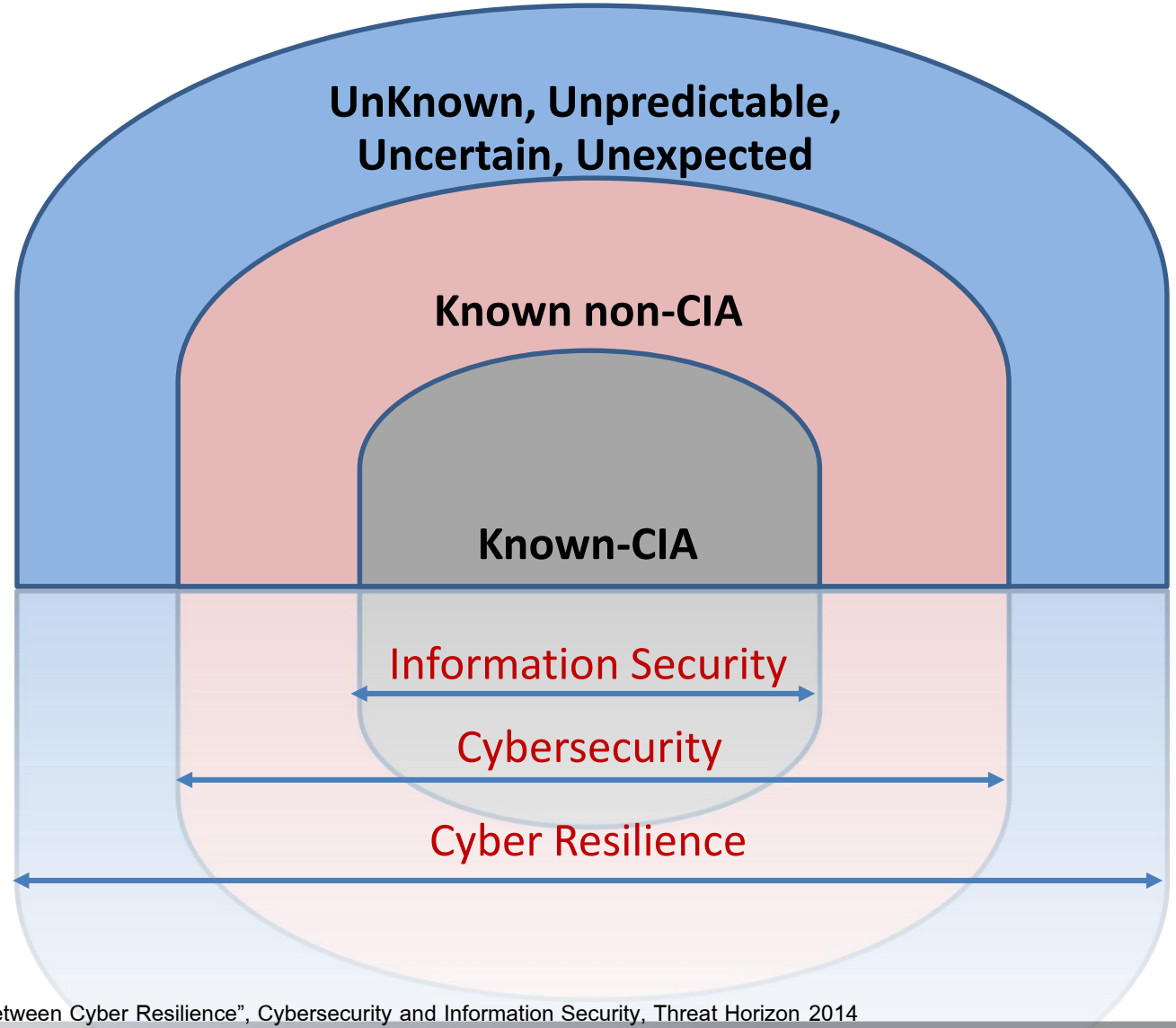
Source: BOT พระสยาม ฉ. 2-3 มี.ค. – มิ.ย. 59

ธุรกิจสถาบันการเงินใช้เทคโนโลยี 99.99%

ระบบธนาคารต้องมั่นคงปลอดภัย

ลูกค้าทำธุรกรรมอย่างปลอดภัย มั่นใจ

IT Security ➡ Cybersecurity ➡ Cyber Resilience



Source: “Relationship between Cyber Resilience”, Cybersecurity and Information Security, Threat Horizon 2014

Top 10 HOT Topics for IT Internal Audit

Rank	2017	2016	2015	2014	2013	2012
1	Cyber Security	Cyber Security	Cyber Security	Large Scale Change	Third-party management	Cyber Threat
2	Strategic Change	Strategic Change	Disaster Recovery and Resilience	IT Governance and IT Risk Management	Identity and Access Management	Complex Financial Models
3	Data Management and Data Governance	Third-Party Management	Large Scale Change	Identity & Access Management and Data Security	Data Governance and Quality	Data Leakage
4	Third-Party Management	IT Disaster Recovery and Resilience	Enterprise Technology Architecture	Data Governance & Quality	Large Scale Change	Data Governance and Quality
5	IT Disaster Recovery and Resilience	Data Management and Data Governance	Third-party management	Third-party management	Cyber Security	Rogue Trader and Access Segregation
6	IT Governance and IT Risk Management	Information Security	Information Security	Cyber Security	Resilience	Regulatory Programmes
7	Information Security	Digital and Mobile Risk	Digital and Mobile Risk	Digital and Mobile Risk	Cloud Computing	Financial Crime
8	Enterprise Technology Architecture	IT Governance and IT Risk Management	Data Management and Governance	Service Management	Mobile Devices	Third-Party management
9	Cloud Computing	Enterprise Technology Architecture	IT Governance and IT Risk Management	Disaster Recovery and Resilience	Complex Financial Modelling	Social Media
10	Digital and Mobile Risk	Payment Systems	Service Management	Cloud Computing	Social Media	Mobile Devices

Source: Storming ahead 2017 Hot Topics for IT Internal Audit in Financial Services An internal audit viewpoint

EXAMPLES OF RECENT INITIATIVES IN ASIA

Aug 2015 (Singapore)
Singapore MAS publishes a circular "**Early Detection of Cyber Intrusions**"

May 2016 (Hong Kong)
HKMA launches "**Cybersecurity Fortification Initiative**"

Apr 2015 (Japan)
Japan FSA revised its financial institutions inspection manual with the creation of a specific section for cybersecurity management and an emphasis on information security governance

Nov 2015 (International)
The Committee on Payments and Market Infrastructures (CPMI) and the board of the International Organization of Securities Commissions (IOSCO) released the "**Guidance on cyber resilience for financial market infrastructures**"

Oct 2016 (Singapore)
MAS launches and a **"national Cybersecurity strategy"** and a new "**Cybersecurity Act**" to be enforced in 2017

Source: Sia Partners, 2016

Dec 2017 (Thailand) BOT launches Cyber Assessment Framework

Oct 2017 (Thailand) BOT launches ITRM

ธนาคารแห่งประเทศไทย

Importance of “IT Internal Audit”

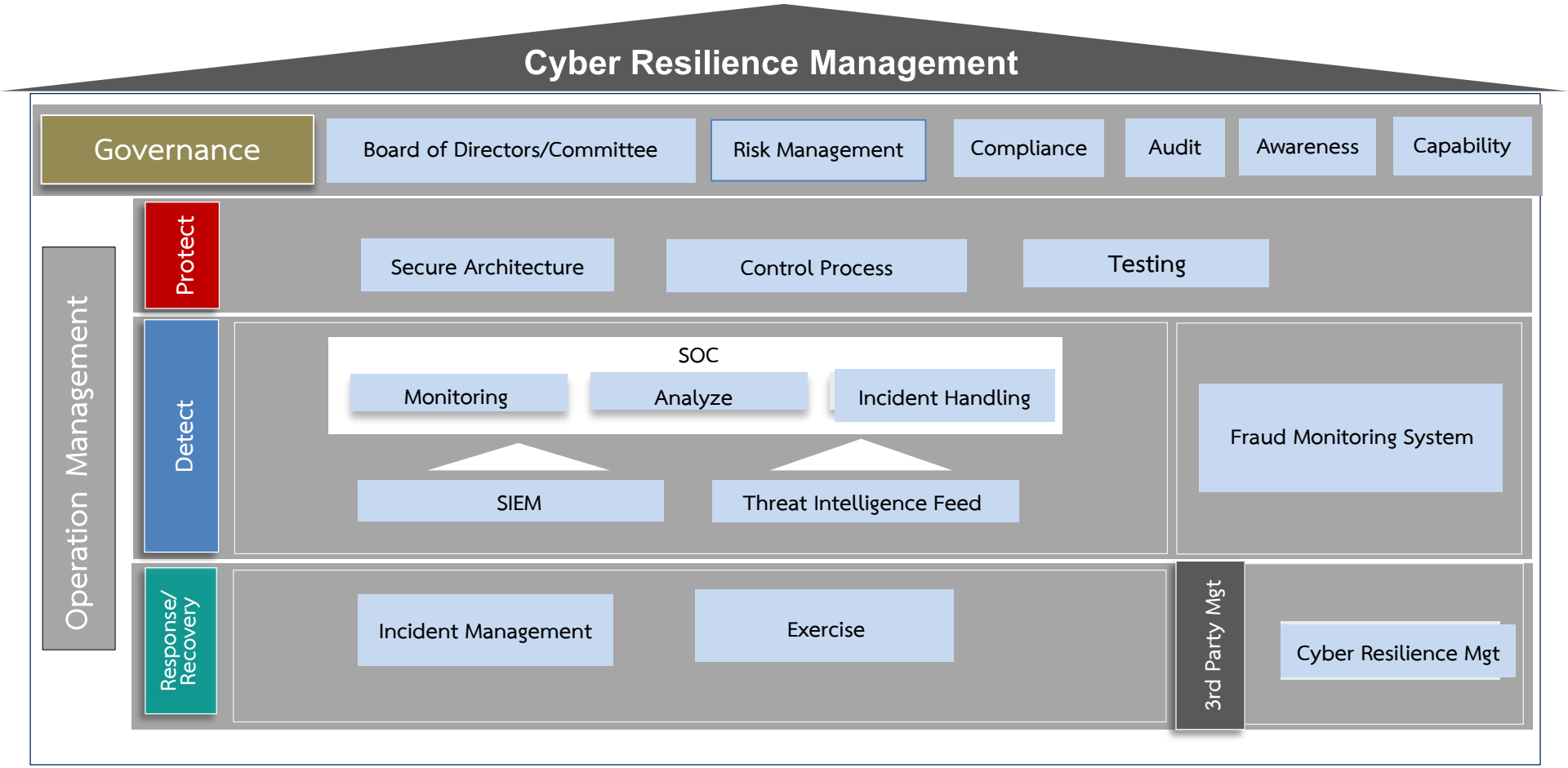
3rd line of defense : IT Audit

ธนาคารแห่งประเทศไทย

Points of your concern

- Know your bank's cyber risk appetise
- Board, Audit Com and Senior Mgt Knowledge/ Awareness and People awareness
- Sufficient and capability of taskforce
- Cyber risk is business risk, business involvement?
- Ready for timely response: plans + exercises
- 3rd party management – cloud computing
- Clear accountability of 3 lines of defense
- Internal Audit Universe cover cyber resilence
- **Is traditional way of doing certain things still work?**

Cyber Resilience Management



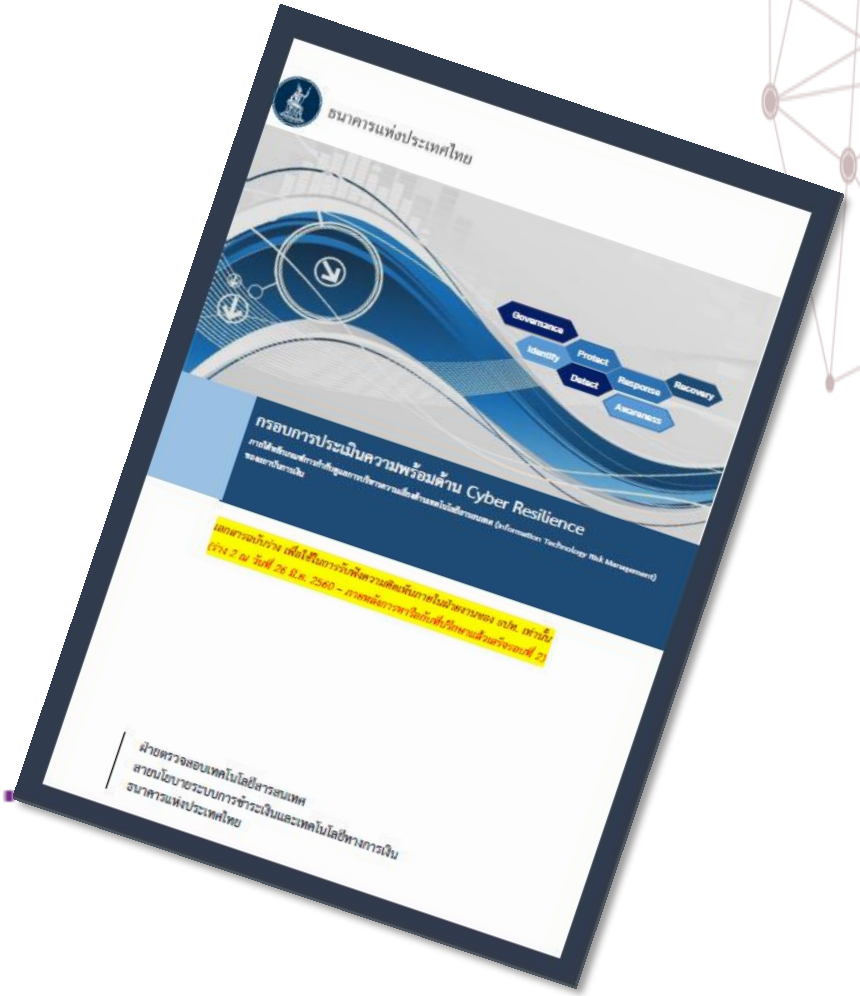
How to handle your challenges

- Rapid Technology Change
- Complexity of Cyber/IT Risk
- Scarce Skills
- Strategic Uncertainty
- New law/regulation

ความเสี่ยงด้าน IT

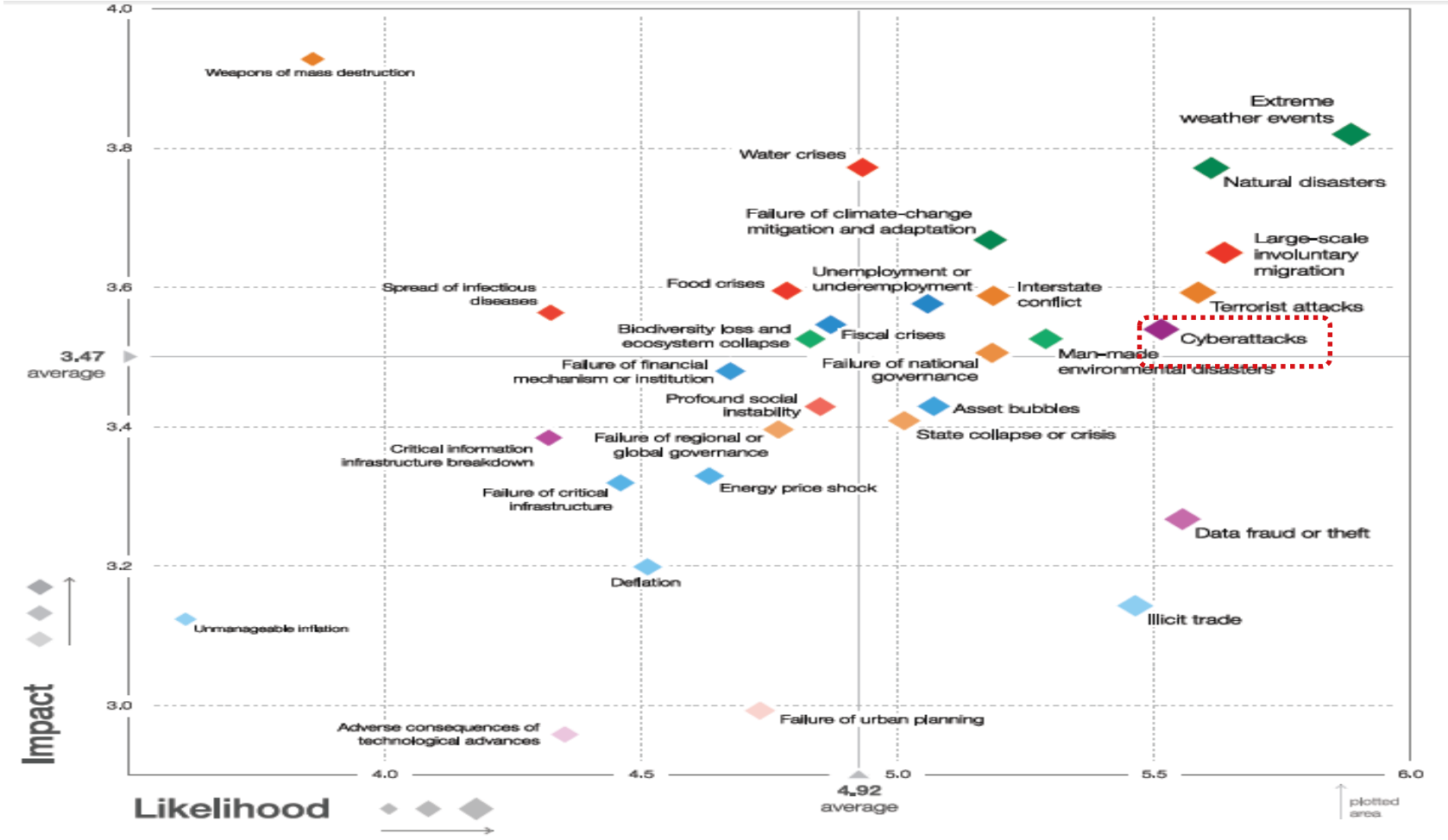
ธนาคารแห่งประเทศไทย

การกำกับดูแลด้าน Cyber Resilience ของสถาบันการเงิน



ธนาคารแห่งประเทศไทย

รายงาน World Economic Forum ปี 2015-2017 จัดให้ Cyberattack เป็นความเสี่ยงสำคัญ ที่มีโอกาสและผลกระทบที่เกิดขึ้นได้มากใน 10 ปีข้างหน้า



1.World Economic Forum (2017), 'Global Risks Report 2017 12th Edition

ธปท. มีแผนยุทธศาสตร์ 3 ปี (ปี 2560-2562) ด้าน Cyber Resilience

ธนาคารแห่งประเทศไทย

Intended Outcome :

ธปท. สถาบันการเงิน และระบบการเงินของประเทศ มีความพร้อม ทั้งด้านระบบ กระบวนการ และบุคลากร สามารถรับมือกับภัยคุกคาม Cyber ได้ ไม่ก่อให้เกิดความเสียหายที่ร้ายแรง ส่งผลกระทบต่อประชาชนในวงกว้าง

ให้ สง. มีการประเมินความพร้อมในการรับมือเทียบกับ Cyber Risk ที่ สง. มี เพื่อปิด gap สำคัญได้ภายในปี 2561 โดยใช้ Cyber Resilience Assessment Framework

สร้างความร่วมมือในภาคการเงิน ระหว่าง สง. Regulators องค์กรรัฐ ทั้งในประเทศ และ ต่างประเทศ

(1) TBA Information Sharing Group (ISG)

(2) ธปท. กลต. คปภ. กสทช.

(3) ETDA ปอท. สรอ.

(4) MAS, HKMA, ASTRI, etc

สร้างความรู้เรื่องภัยคุกคาม และความปลอดภัยในการทำธุรกรรมให้กับประชาชนต่อเนื่อง

ร่วมมือกับภาคการศึกษาสร้างบุคลากรด้าน Cybersecurity ในภาคการเงินให้เพียงพอ และมีความรู้เท่าทัน

ธปท.ประเมิน Cyber Resilience ตามแนวทางมาตรฐานสากล

ธนาคารแห่งประเทศไทย

Inherent Cyber Risk (IR)

ประเมินการเปิด surface ของ สง. ต่อ
ภัยคุกคามทาง Cyber

- Technology Usage & Connection
- Delivery Channels
- Product & Services
- Org. Characteristics
- Cyber Incident Records

→ L / M / H

FI Self Assessment → BOT Review

Cyber Risk Management and Control (Maturity)

ประเมินการบริหารจัดการและควบคุม
ภัยคุกคามทาง Cyber

- Governance
- Risk Identification
- Protection
- Detection
- Response & Recovery
- 3rd Party Management

Baseline + Intermediate + Advanced

PEOPLE → PROCESS → TECH

Risk Based Expected Maturity

- L → Baseline
- M → Intermediate
- H → Advanced

GAPs

Bank's Existing Maturity

Framework
: อ้างอิง NIST,BIS,ISO270032,HKMA
: หารือที่ปรึกษา บ. Deloitte, ผู้เชี่ยวชาญ (ดร.ชัยชนะ ดร.ธนชาติ ดร.รอม ดร.ภูมิ อ.ปริญญา อ.เมธา)

ธปท.ประเมิน Cyber Resilience ตามแนวทางมาตรฐานสากล

Cyber Resilience Assessment Framework

Inherent Risk Profile | Control Principles

Inherent Cyber Risk : ประเมินความเสี่ยงตั้งต้นของ สง. ที่มี surface ในการเผชิญกับ cyber risk

Key Risk Factors

IR 1 — Techology & Connection

- Connections
- Public IPs
- Wireless Network
- BYOD
- EOL Technology
- Open Source S/W
- Platform
- Cloud Computing

IR 2 — Delivery Channels

- ATM
- Internet Banking
- Mobile Banking
- Branchs
- Social Media

IR 3 — Product & Service

- Cards
- Online Transfer
- ATM Service
- Cross Border Service

IR 4 — Org. Characteristics

- IT Enviroment
- Size
- IT Staffs
- Privileged Access
- IT Out. staffs

IR 5 — Cyber Incident Records

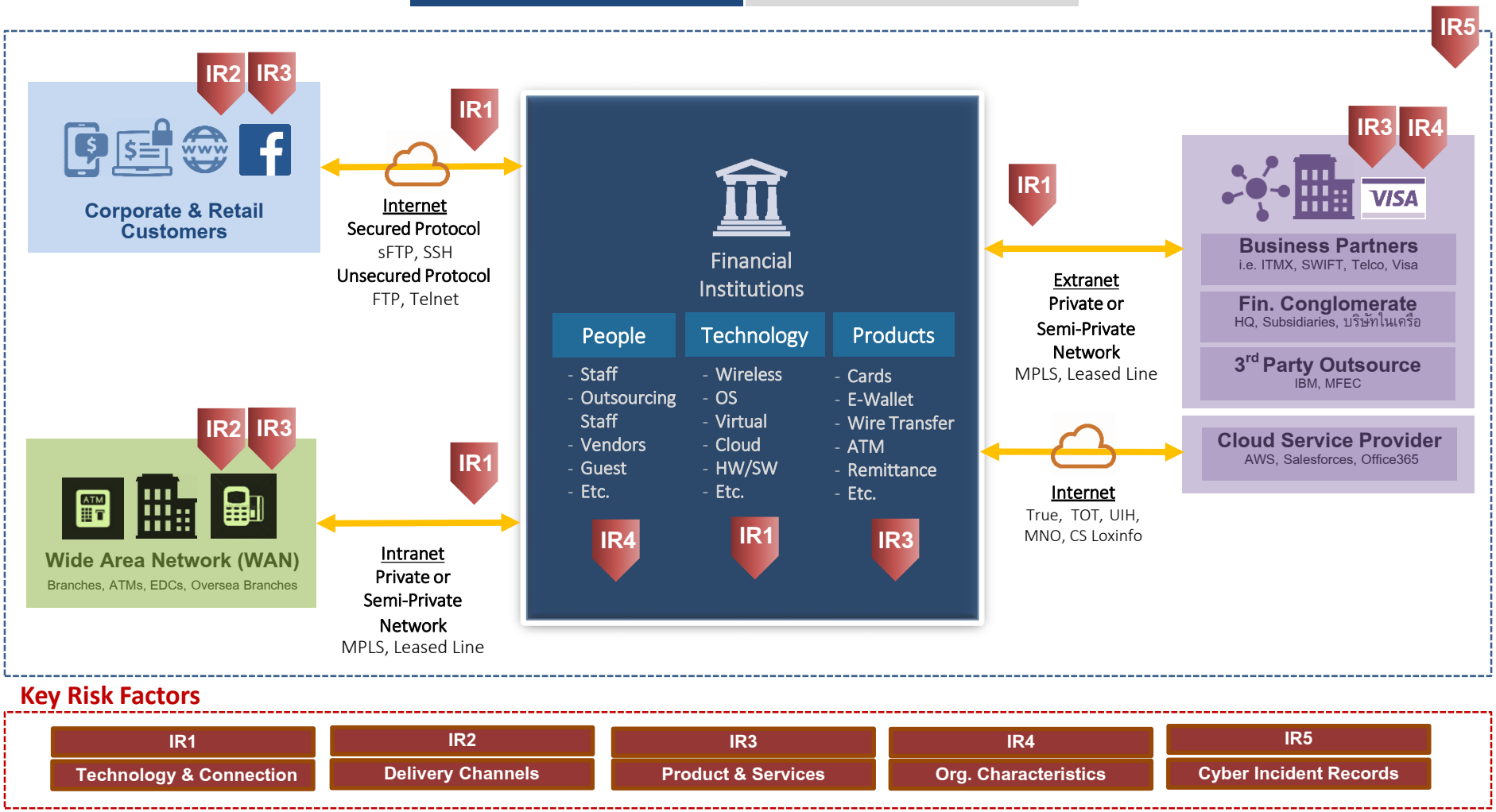
- DDoS
- Phishing
- Social Engineering
- Malware
- Hacking

ธปท.ประเมิน Cyber Resilience ตามแนวทางมาตรฐานสากล

ธนาคารแห่งประเทศไทย

Cyber Resilience Assessment Framework

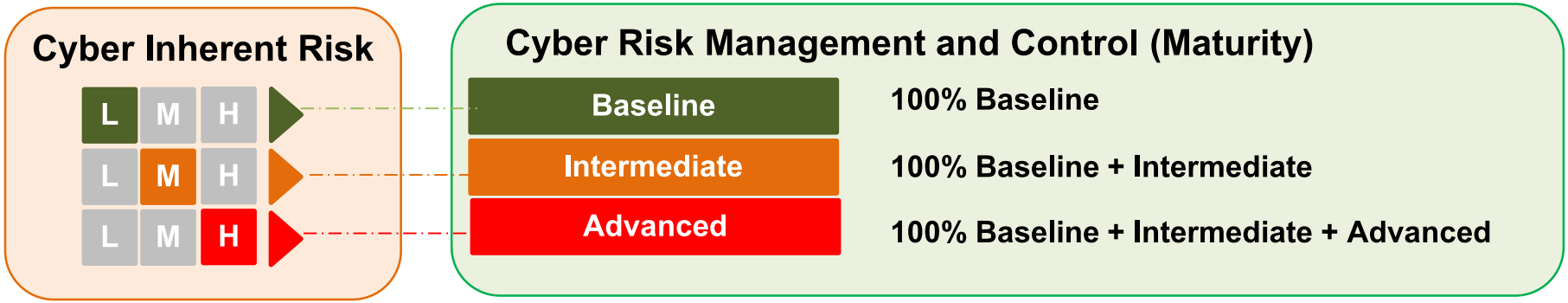
Inherent Risk Profile | Control Principles



Key Risk Factors

IR1	IR2	IR3	IR4	IR5
Technology & Connection	Delivery Channels	Product & Services	Org. Characteristics	Cyber Incident Records

Cyber Inherent Risk → Cyber Risk Management and Control (Maturity)

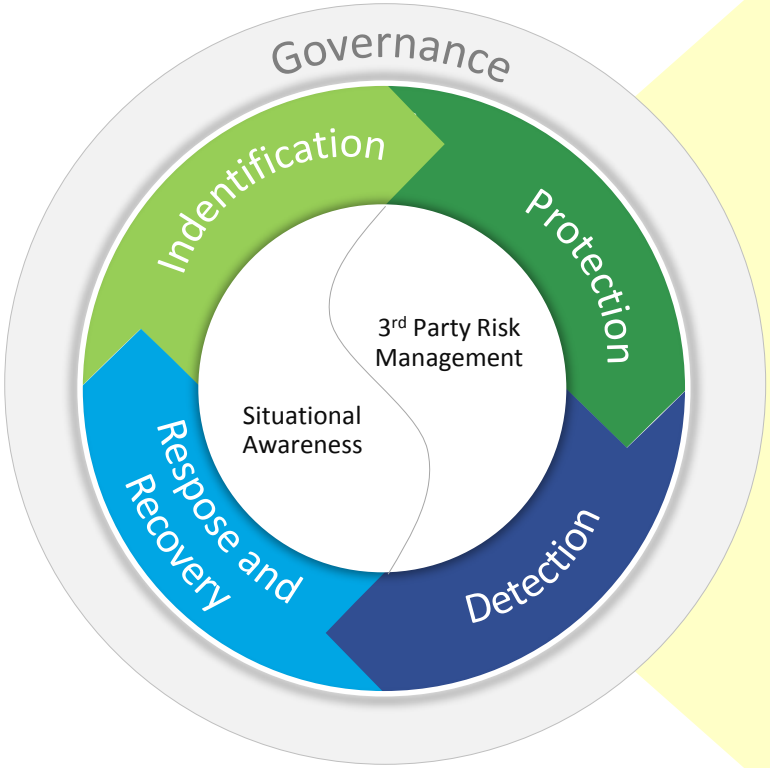


ธปท.ประเมิน Cyber Resilience ตามแนวทางมาตรฐานสากล

Cyber Resilience Assessment Framework

Inherent Risk Profile | Control Principles

Control Principle: การควบคุมความเสี่ยงด้านไซเบอร์ตามระดับ IR ครอบคลุม 6 ด้าน



1. Governance

Cybersecurity Oversight, Strategy and Policies, Cyber Risk Management, Audit, Budgeting, Staffing and Training

2. Risk Identification

IT Asset Identification, Cyber Risk Assessment

3. Protection

Infrastructure Protection, Access Control, Data Security, Secure Coding, Patch Management, Remediation Management

4. Detection

Vulnerability Assessnent(VA)
Penatration Testing
Cyber Incident Detection
Threat Monitoring/Analysis

5. Response and Recovery

Response Planning, Incident Management, Escalation and Reporting

6. 3rd Party Risk Management

External Connections
3rd Party Management
Ongoing monitoring

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | 3. Protection | 4. Detection | 5. Response and Recovery | 6. 3rd Party Management

	Baseline	Intermediate	Advanced
บทบาทหน้าที่ของ Board และ คกก. ที่เกี่ยวข้อง	- Board มีบทบาทและหน้าที่รับผิดชอบชัดเจน กำหนดกลยุทธ์ นโยบายด้าน Cyber		- กำหนด Cyber risk appetite
	- กำหนดบทบาท คกก. ที่เกี่ยวข้อง (IT Steering) ที่ชัดเจนด้าน Cyber	- กำหนดบทบาท คกก. Risk และ Audit ที่ชัดเจนด้าน Cyber	- มอบหมาย BU มีส่วนในการกำกับดูแล Cyber
กลยุทธ์และนโยบาย	- หน่วยงาน IT กำหนดกลยุทธ์ด้าน Cyber	- กลยุทธ์สามารถรองรับภัยคุกคามใหม่ๆ ด้าน Cyber	- กลยุทธ์ Cyber เป็นส่วนหนึ่งของการกำหนดกลยุทธ์ของ BU และ Risk
	- สง. กำหนดนโยบาย Cybersecurity - มีนโยบาย Cyber threat sharing	สอดคล้องกับทิศทางของเทคโนโลยีหรือมาตรฐานการรักษาความมั่นคงปลอดภัยที่ยอมรับโดยทั่วไป	- มีนโยบาย Cyber threat Intelligence (รวบรวม/วิเคราะห์/แชร์)
การบริหารจัดการความเสี่ยง	- Risk owner ใน IT	- มีบุคลากรหรือหน่วยงานที่เป็นอิสระ (อาจอยู่ในสายงาน IT) - รวมภาพและ Challenge สาย IT	- มีหน่วยงานที่เป็นอิสระแยกจากสาย IT - Challenge BU ด้าน Cyber risk
	- สง. กำหนดกระบวนการระบุ วัด ควบคุม ติดตามและรายงาน	- การประเมินผลกระทบครอบคลุมข้อกำหนดทางการ ผลกระทบทางการเงิน หรือ กลยุทธ์	- รายงานและ update Cyber incident / Threat อย่างรวดเร็ว
			- พิจารณาทำ Cyber insurnace

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | 3. Protection | 4. Detection | 5. Response and Recovery | 6. 3rd Party Management

	Baseline	Intermediate	Advanced
การตรวจสอบภายใน	- วางแผนและกำหนดขอบเขตการ ต/ส และรายงานให้ คกก. ต/ส		
	ขอบเขต ครอบคลุม - การจัดเก็บข้อมูล ล/ค - Cyber threat intelligence	ขอบเขต ครอบคลุม - กระบวนการจัดทำ Cyber risk appetite	ขอบเขต ครอบคลุม - ความเหมาะสมค่า Cyber risk appetite
	- การปรับปรุงขอบเขตให้สอดคล้อง IR ที่ ปป.	- สอดคล้องตาม Cyber threat ของ สง. อื่นๆ (Peer)	- สอดคล้องตาม Cyber threat ของหน่วยงานภายนอกอื่น (telco, insurance)
บุคลากร	- กำหนดบทบาทคน/หน่วยงาน ที่รับผิดชอบที่ชัดเจน		
	- พนง. ที่รับผิดชอบมีคุณสมบัติตามที่กำหนด	- C level มีความรู้ ความเชี่ยวชาญ และ ปสก ด้านไซเบอร์	
ฝึกอบรม / Awareness	- จัดหลักสูตรอบรม Cyber ครอบคลุม พนง. ในองค์กร	- ทบทวนและปรับปรุงพร้อมรับมือภัยใหม่ๆ	- Cyber drill
	- ให้ความรู้ สร้าง awareness ให้ลูกค้า และนิติบุคคล		

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | **2. Identification** | 3. Protection | 4. Detection

5. Response and Recovery | 6. 3rd Party Management

	Baseline	Intermediate	Advanced
การจัดการทะเบียนทรัพย์สิน	- กำหนด คน/หน่วยงาน รับผิดชอบจัดทำและดูแลให้ชัดเจน		
	- จัดทำทะเบียนทรัพย์สินครอบคลุม HW, SW, ระบบงานและข้อมูล	- จัดลำดับความสำคัญตามความลับของข้อมูล หรือความสำคัญของบริการ	- ระบบงานที่กำหนดเงื่อนไขให้ต้องประเมิน ค.เสี่ยง - กระบวนการ/เครื่องมือที่ตรวจจับ/ป้องกันการ ปป. แก้ไข - ประเมิน ค.เสี่ยง Supply chain
	- มีกระบวนการพิจารณา อนุมัติ ปป. ทรัพย์สิน	- ประเมิน ค.เสี่ยงด้าน Cyber ในแต่ละขั้นตอน	
การระบุและประเมินความเสี่ยง	- สาย IT มีกระบวนการและจัดทำการประเมิน ค.เสี่ยง ที่สามารถระบุธุรกรรม/ระบบงานสำคัญ และมีแนวทางควบคุม		- กระบวนการประเมิน ค.เสี่ยงด้านไซเบอร์ เป็นส่วนหนึ่งของการประเมิน ค.เสี่ยงขององค์กร
	ขอบเขตการประเมิน ค.เสี่ยง การรักษาความปลอดภัยครอบคลุมในด้าน - ข้อมูลลูกค้า - การใช้เทคโนโลยีใหม่ - EOL/EOS	- ขอบเขตครอบคลุมข้อมูลสำคัญของ สง.	- ปป. ขอบเขตให้รองรับความเสี่ยงรูปแบบใหม่ที่อาจจะเกิดขึ้น

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | **3. Protection** | 4. Detection | 5. Response and Recovery | 6. 3rd Party Management

Infrastructure Protection Controls

	Baseline	Intermediate	Advanced
การป้องกันระบบเครือข่าย	- มีอุปกรณ์ป้องกันเครือข่าย เช่น FW - ทบทวน FW Rules เป็นระยะ ๆ	- ตั้งค่าอุปกรณ์ให้จำกัดและติดตามการรับส่งข้อมูล Trusted VS Untrusted ได้	- มีเทคนิคเชิงป้องกัน Unauthorized code บน network Device
	- มี IPS/IDS เพื่อตรวจจับการบุกรุก - ป้องกันการเชื่อมต่อโดยไม่ได้รับอนุญาต	- พิจารณา ISP ที่มีมาตรการและความเสี่ยงจากการถูกโจมตีทาง Cyber เช่น DDoS	- ป้องกัน IP และ MAC Address ที่ถูกปลอมแปลงไม่ให้เชื่อมต่อ
	- เข้ารหัสเมื่อรับส่งข้อมูลผ่านเครือข่ายไร้สาย - ใช้ DNSSEC ครอบคลุมการให้บริการ สง.	- ควบคุม Remote Access และการกระจายสัญญาน wifi	
	- แบ่งเครือข่ายภายในตามกลยุทธ์ Defense-in-depth		
System Configuration	- มีกระบวนการติดตามการตั้งค่าอุปกรณ์ และต้องกำหนดการตั้งค่าอุปกรณ์ตาม Baseline - สอบทานระบบงานสำคัญที่ใช้เทคโนโลยีที่ล้าสมัย หรือสิ้นสุดการสนับสนุน		ประเมินระบบควบคุมภายในที่อาจถูกใช้เป็นส่วนหนึ่งของ Zero-Day Attack
	- ปิด Port/Service/Protocol ที่ไม่จำเป็นและป้องกันการติดตั้งโปรแกรมที่ไม่อนุญาต	กำหนดให้ Critical Server มี Service หลักService เดียว เพื่อลดความขัดแย้งการตั้งค่า	หมุนเวียนเครื่อง Server กรณีมีความจำเป็นเชื่อมต่อกับสาธารณะ
Device Protection	- Lock การใช้งาน Session เมื่อไม่มีการใช้งานตามเวลาที่กำหนด		

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | **3. Protection** | 4. Detection | 5. Response and Recovery | 6. 3rd Party Management

Access Controls

	Baseline	Intermediate	Advanced
การบริหารจัดการบัญชีผู้ใช้งาน	- มีการพิสูจน์ตัวตนทั้งระดับ Physical และ Logical (System, Application & HW) - ยกเลิกสิทธิ์การเข้าออกระดับ Physical และ Logical ทันทีเมื่อพนักงานโยกย้าย หรือลาออก		มีการป้องการการเข้าถึงอุปกรณ์สื่อสารภายในองค์กร (IoT Device)
	- มีมาตรการควบคุมการเข้าถึงและกำหนดความซับซ้อนของรหัสผ่าน - สอบทานบันทึกการเข้าใช้งาน System หรือ Application สอดคล้องระดับความเสี่ยง		
	มีมาตรฐานการเข้ารหัส Password ทั้งในการจัดเก็บและการรับส่ง		
	กำหนดสิทธิ์ตามหลัก Least Privilege และ Segregation of Duty	- มีระบบแจ้งเตือนเมื่อมีการเปลี่ยนแปลงสิทธิให้ผู้เกี่ยวข้องทราบอัตโนมัติ เช่น SMS	
	แยกบัญชีผู้ใช้งาน Non-production และ Production ออกจากกัน		
การบริหารจัดการผู้ใช้งานสิทธิ์สูง	- จำกัดจำนวนผู้ใช้งานสิทธิ์สูง และควบคุมอย่างเข้มงวด	ควบคุม DB Admin เพื่อป้องกันการนำข้อมูลไปใช้โดยไม่ได้รับอนุญาติ	
	- กำหนดสิทธิ์สำหรับผู้ดูแลระบบไว้ 2 ประเภท คือเพื่อบริหารจัดการ กับ งานทั่วไป	ใช้วิธีพิสูจน์ตัวตนแบบ Multifactor เช่น Tokens, Certificates	

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | **3. Protection** | 4. Detection | 5. Response and Recovery | 6. 3rd Party Management

Access Controls (Cont.)

	Baseline	Intermediate	Advanced
การบริหารจัดการสิทธิ์ของลูกค้า	มีมาตรการควบคุมการพิสูจน์ตัวตนลูกค้าของผลิตภัณฑ์ผ่านระบบ Internet สอดคล้องกับระดับความเสี่ยง		การพิสูจน์ตัวตนลูกค้าสามารถป้องกัน Malware/Man-in-the-Middle
	กำหนดขั้นตอนการพิสูจน์ตัวตนลูกค้าของหน่วยงานด้านการบริการลูกค้าสอดคล้องระดับความเสี่ยงธุรกรรม		นำเทคโนโลยี Tokenization มาใช้ทดแทนข้อมูลที่เป็นความลับ เช่น แทนหมายเลขบัตรเครดิต
Physical Access Mgmt.	มีมาตรการป้องกันทาง Physical เพื่อป้องกันการเข้าถึงห้อง Network และ System และมีบันทึกการเข้าใช้งาน		
Remote Access Mgmt.	ต้องเข้ารหัสช่องทางการเชื่อมต่อและพิสูจน์ตัวตนแบบ Multifactor เพื่อเข้าระบบงานสำคัญ		
Crypto. Key Access Mgmt.	ควบคุมเพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าถึงการจัดเก็บ Encryption Key		
3rd Access Mgmt.	ใช้วิธีการพิสูจน์ตัวตนแบบ Strong Authencation เพื่ออนุญาตให้บุคคลภายนอกเข้าใช้ระบบงาน		

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | **3. Protection** | 4. Detection | 5. Response and Recovery | 6. 3rd Party Management

Data Security

	Baseline	Intermediate	Advanced
End Point Data Security	มีมาตรการควบคุมการใช้ Removable Media ให้ใช้งานได้ผู้ที่ได้รับอนุญาตเท่านั้น		
	- มีมาตรการบันทึกข้อมูลที่เป็นความลับ - มีมาตรการป้องกันการรั่วไหลข้อมูล		การเข้าถึงข้อมูลลับหรือระบบงานต้องทำบน Secure Container
Data Protection	ติดตั้ง Anti-malware บน End-point Device และควบคุมจากส่วนกลาง	มีระบบตรวจสอบ software patch ที่ติดตั้งบน End-point Devices	
	มีกระบวนการทำลายข้อมูลออกจากสื่อบันทึกที่ไม่ได้ใช้งานแล้ว		
	เข้ารหัสข้อมูลลับทุกครั้งเมื่อรับส่งผ่านเครือข่ายสาธารณะ และบนสื่อบันทึกข้อมูล	มีเครื่องมือป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการจารกรรมข้อมูล	เข้ารหัสข้อมูลทุกครั้ง ระหว่างการรับส่งข้อมูลลับผ่านเครือข่าย
	ปกปิดหรือลบข้อมูลในส่วนสำคัญของลูกค้าก่อนนำไปใช้บน Non-production		กำหนดหลักเกณฑ์ในการเข้ารหัสข้อมูลแต่ละประเภทไว้ในนโยบาย
	จำกัดสิทธิ์การใช้งานโปรแกรมที่ใช้ในการตั้งค่า โดยให้สิทธิ์ตามความจำเป็น		
Data Disposal	มีนโยบายและกระบวนการในการยกเลิกและทำลายข้อมูลหรือสื่อบันทึกข้อมูลภายในระยะเวลาที่กำหนด		

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | **3. Protection** | 4. Detection

5. Response and Recovery | 6. Situation Awareness | 7. 3rd Party Management

	Baseline	Intermediate	Advanced
Security Coding			
Secure Development	มีนโยบายควบคุมให้การพัฒนาโปรแกรมปลอดภัยเป็นไปตามมาตรฐานสากล		กำหนดผู้รับผิดชอบด้าน Information Assurance เพื่อประเมินความปลอดภัย
	มีการทดสอบความปลอดภัยของโปรแกรมในแต่ละขั้นตอนการพัฒนา ก่อนใช้งานจริงและทบทวนอย่างสม่ำเสมอ	กำหนดให้มีการทำ VA และ Pen Testing	มีกระบวนการวิเคราะห์ Source Code เพื่อหาและปิดช่องโหว่ก่อนใช้งานจริง
	มีกระบวนการทบทวนความถูกต้องปลอดภัย ของการจัดเก็บ Source Code		
Patch Management			
Patch Management Programme	มีกระบวนการบริหารจัดการ Patch และมีการสอบทานการติดตั้ง	**มีกระบวนการหรือเครื่องมือสอบทานความครบถ้วนของ Patch**	มีระบบติดตามสอบทานความครบถ้วนของ Patch สำหรับ OS DB Middleware และ Software สำคัญ
	มีการรับ Patch ใหม่ๆในทันทีที่ผู้พัฒนาได้ได้ประกาศและเผยแพร่ออกมา		มีกระบวนการสอบทานรายงานการบริหารจัดการเพื่อให้มั่นใจว่า Patch ได้รับการติดตั้งอย่างรวดเร็ว (0-30 วัน)
Patch Assesment and Testing	มีกระบวนการจัดหา ทดสอบ และติดตั้ง Patch ตามระดับความสำคัญ	มีการทดสอบและติดตั้ง Critical Patch อย่างรวดเร็วตามความเสี่ยง	

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | **3. Protection** | 4. Detection | 5. Response and Recovery | 6. 3rd Party Management

Remediation Management

	Baseline	Intermediate	Advanced
Issues Management	มีกระบวนการแก้ไขช่องโหว่ โดยจัดลำดับความสำคัญ และแก้ไขตามเวลาที่กำหนด	ทำ Simulation Test เพื่อสอบทานผลการแก้ไขช่องโหว่	มีการควบคุมผู้ทำหน้าที่ซ่อมบำรุง เครื่องมือที่ใช้ ทำบันทึกและสอบทานรายละเอียดการซ่อมบำรุงอย่างสม่ำเสมอ
Testing after Remediation	ทำ VA Scan เพื่อสอบทานการแก้ไขช่องโหว่		
Incident Forensic		มอบหมายให้ผู้ที่มีความเชี่ยวชาญทำ Security Investigation, Forensic Analysis และ Remediation	มีกระบวนการพิสูจน์หลักฐาน และมีการรักษาวัตถุพยานที่น่าเชื่อถือ

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | 3. Protection | **4. Detection**

5. Response and Recovery | 6. 3rd Party Management

	Baseline	Intermediate	Advanced
★ การตรวจหาเพื่อปิดช่องโหว่			
การตรวจหาและกำจัดไวรัสและมัลแวร์ (Antivirus and Anti-Malware)	มีเครื่องมือปรับปรุง Anti-malware บนเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆให้ทันสมัยโดยอัตโนมัติ		
	มีกระบวนการหรือมาตรการ Filer ภัยคุกคามที่มาจาก Email	มีเครื่องมือที่สามารถ Scan ไฟล์แนบ เพื่อตรวจหา Malware ที่แฝงมากับ Email	
การตรวจหาช่องโหว่และทดสอบเจาะระบบ	ทำ VA/Pentest อย่างสม่ำเสมอตามรอบ รวมถึงก่อนใช้งานจริง และเมื่อมี Change ที่มีนัยสำคัญ	ใช้ข้อมูล Threat Intelligence มาออกแบบ Scenario เพื่อเตรียมการทดสอบ Pentest	ทดสอบ Pentest ตามที่ออกแบบใน Intermediate Level

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | 3. Protection | **4. Detection**

5. Response and Recovery | 6. 3rd Party Management

	Baseline	Intermediate	Advanced
★★ การสอบทานเพื่อตรวจให้พบความเสี่ยง			
การสอบทานและวิเคราะห์ Log	จัดเก็บ / สอบทาน / ติดตามการเข้าใช้งาน / นำ Log มาประกอบการสืบสวนเมื่อผิดปกติ		
การวิเคราะห์ Log เพื่อหาสิ่งผิดปกติ (SIEM)	ประเมิน/กำหนดเกณฑ์ผิดปกติสำหรับ Log เพื่อรายงานและติดตามพฤติกรรมผิดปกติ	มี Tool แจ้งเตือนผู้รับมอบอำนาจเมื่อถึงเกณฑ์ผิดปกติใน Baseline LV	นำการแจ้งเตือนมาเชื่อมโยงกันทุก BU เพื่อตรวจจับการโจมตี MultiFaceted
	มีมาตรการติดตามการเข้าถึงระบบสำคัญจาก 3rd Party เพื่อเช็คการเข้าถึงโดยไม่อนุญาต	กบก.ติดตามกิจกรรมที่เข้าข่ายผิดปกติที่อาจนำไปสู่ Data loss/leak	ทำไฟล์ปลอมดักไว้ เพื่อดูการเข้าถึงของผู้ไม่ประสงค์ดี
Customer Transaction Monitoring	มีการติดตามพฤติกรรมที่น่าสงสัย หรือเข้าข่ายเป็น Fraud Transaction ของลูกค้า	มี Tool แจ้งเตือนลูกค้าเมื่อมีการ Login จากสถานที่ต่างกันเวลาใกล้กัน	มี Tool แจ้งเตือนเมื่อพบการโอนเงินผิดปกติ โดยให้ลูกค้าอนุมัติก่อน

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | 3. Protection | **4. Detection**

5. Response and Recovery | 6. 3rd Party Management

	Baseline	Intermediate	Advanced
การติดตามความเสี่ยงเพื่อแจ้งเตือน			
การติดตามเหตุการณ์ผิดปกติ	กำหนดบทบาทหน้าที่ผู้รับผิดชอบในการติดตาม และรายงานกิจกรรมต้องสงสัย	มีกระบวนการเฝ้าระวังกิจกรรมผิดปกติครอบคลุมทั้ง Physical และ Logical	มีมาตรการตรวจจับการรับส่งข้อมูลผ่านช่องทางต่างๆที่เสี่ยงต่อ Data loss/leak
การตรวจพบและแจ้งเตือน	- Alert ให้ผู้เกี่ยวข้องทราบ และทำการแก้ไข เมื่อพบโอกาสเกิดเหตุการณ์ผิดปกติ - นำ System Report ประกอบการทำ KRI	Detect ความพยายามบุกรุกก่อนที่จะผ่านเข้ามาสร้างความเสียหายต่อข้อมูล และ Alert	Detect การเปลี่ยนแปลงค่าความปลอดภัยของระบบ / เกิดการบุกรุก Network และ Alert
การพัฒนาเพื่อตั้งรับความเสี่ยงใหม่ๆ			
การวิเคราะห์ภัยคุกคาม	- มีหน่วยงาน SOC เพื่อเฝ้าระวัง ติดตาม ประสานงาน และเป็นศูนย์กลางการด้านการรักษาความปลอดภัย - มีระบบรับ Threat Intelligence มาวิเคราะห์เพื่อเป็นข้อมูลในการเฝ้าระวัง	- ระบุแนวโน้ม/ผลกระทบของภัย cyber - Monitor โอกาสเกิดภัยคุกคาม - รายงานผลวิเคราะห์ให้ผู้บริหารระดับสูง - ทำ Risk Profile และ Mitigation Plan - ปรับปรุง IT Security Architecture และทบทวน policy	

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | 3. Protection | **4. Detection** | 5. Response and Recovery | 6. 3rd Party Management

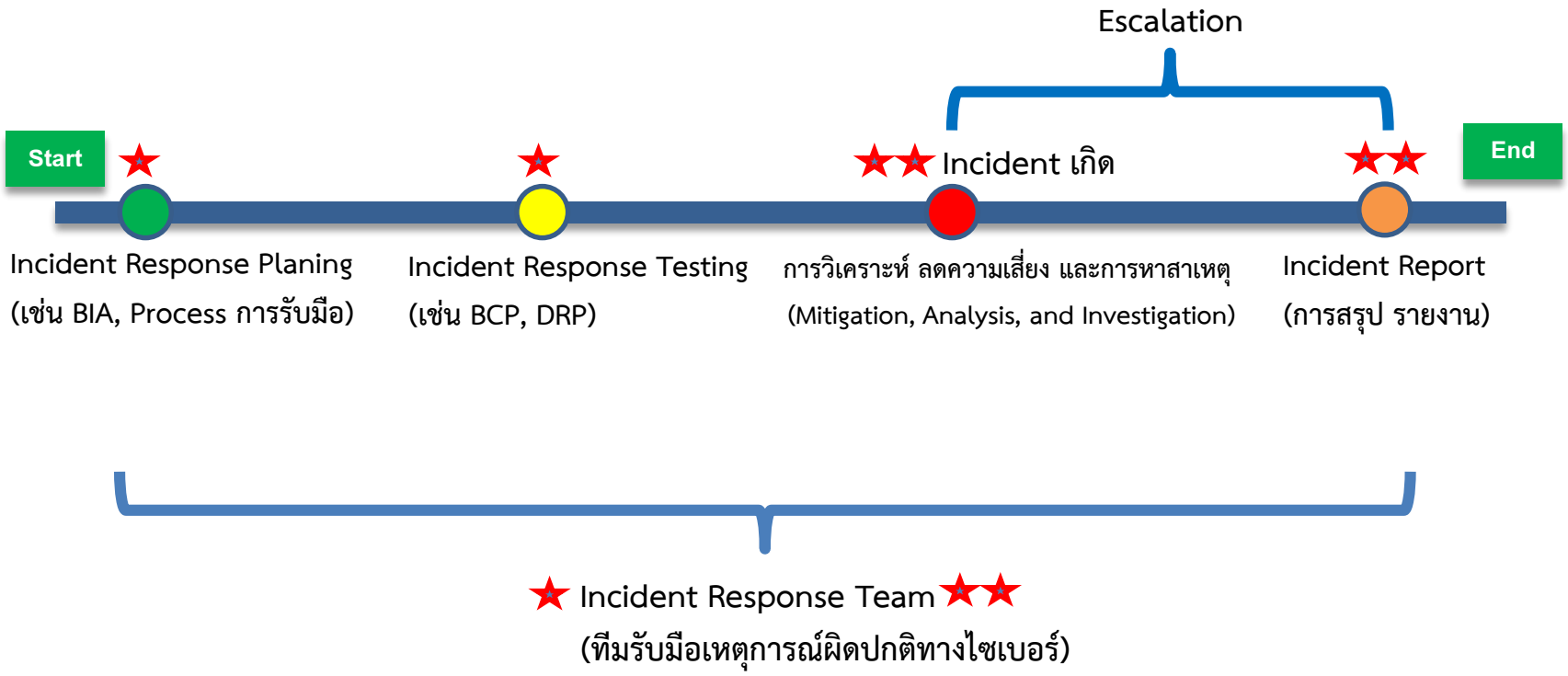
	Baseline	Intermediate	Advanced
การรวบรวมข้อมูลภัยคุกคามทางไซเบอร์	มีหน่วยงานที่รับผิดชอบ และมีกระบวนการวิเคราะห์		
	เป็นสมาชิกของ Cyber Threat Intelligence Platform	วิเคราะห์และจัดทำ Cyber Threat Intelligence เอง	มีระบบอัตโนมัติที่วิเคราะห์เชื่อมโยงข้อมูล แจ้งเตือน และบรรเทา/แก้ไข
	นำ Cyber Threat Intelligence มาใช้ประกอบการเฝ้าระวังและปรับปรุง		
		มีศูนย์กลางจัดเก็บ Cyber Threat Intelligence	มีระบบอัตโนมัติที่รวบรวม Cyber Threat Intel. แบบ Real-time
การแลกเปลี่ยนข้อมูลภายใน	มีกระบวนการสื่อสาร Cyber Threat Intelligence และเหตุการณ์ผิดปกติ	ผู้บริหารสื่อสารและให้ข้อแนะนำเพื่อบริหารจัดการความเสี่ยง	
การแลกเปลี่ยนข้อมูลภายนอก	แลกเปลี่ยนข้อมูลกับหน่วยงานบังคับใช้กฎหมายได้ตามที่กำหนด	มีกระบวนการที่ปลอดภัยในการแลกเปลี่ยนข้อมูล	มีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูล
	มีข้อมูลผู้ประสานงานของหน่วยงานภายนอก และปรับปรุงให้เป็นปัจจุบัน		
		มีตัวแทนเข้าร่วมประชุมแลกเปลี่ยนข้อมูลอย่างสม่ำเสมอ	ผลักดันให้มีเครื่องมีที่ใช้แลกเปลี่ยนข้อมูล

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | 3. Protection | 4. Detection

5. Response and Recovery | 6. 3rd Party Management



ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | 3. Protection | 4. Detection

5. Response and Recovery | 6. 3rd Party Management

★ Response Planing (ก่อนเกิดเหตุ)

	Baseline	Intermediate	Advanced
การวางแผนรับมือเหตุการณ์ผิดปกติทางไซเบอร์ (Incident Response Planning)	มีนโยบาย กระบวนการ ขั้นตอนการรับมือเหตุการณ์ผิดปกติทางไซเบอร์อย่างชัดเจน	ประเมินผู้เชี่ยวชาญก่อนว่าจ้างกรณีช่วยเหลือ สง. เมื่อเกิด Incident	
	จัดทำแผน BIA BCP DRP Crisis Mgt และ Data Recovery	มีการทำสัญญาหรือข้อตกลงร่วมมือ เช่น กับผู้ให้บริการ MOU และอื่นๆ	
	มีแผนรับมือเมื่อเกิดเหตุ เช่น รับแจ้ง ประเมิน ตรวจสอบ และวิเคราะห์สาเหตุ / มีการปรับปรุงแผนอย่างต่อเนื่อง		
การทดสอบความพร้อมรับมือเหตุการณ์ผิดปกติ (Incident Response Testing)	ทดสอบแผน Data Restore จากข้อมูลสำรอง เพื่อมั่นใจว่าสามารถกู้คืนได้	เพิ่ม Scenario ที่คำนึงถึงผลกระทบต่อกระบวนการของ BU	เพิ่ม Scenario ที่ซับซ้อนขึ้น เช่น ผลกระทบทางการเงิน และอื่นๆ
		นำผลทดสอบมาประกอบทำแผนรับมือ พร้อมทั้งกำหนดจุด Trigger	
ทีมรับมือเหตุการณ์ผิดปกติทางไซเบอร์ (Incident Response Team)	มี จนท. ชำนาญงานด้านรับมือไซเบอร์ รวมถึงกำหนดบทบาทหน้าที่ชัดเจน	หน่วยงานด้านรับมือไซเบอร์ ประสานงานและสื่อสารใกล้ชิด	

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | 3. Protection | 4. Detection

5. Response and Recovery | 6. 3rd Party Management

★★ Incident Mgt (ช่วงเกิดเหตุและภายหลัง)

	Baseline	Intermediate	Advanced
การวิเคราะห์ ลดความเสี่ยง และการหาสาเหตุ (Mitigation, Analysis, and Investigation)	มีรายชื่อหน่วยงานที่เกี่ยวข้อง รวมถึงกระบวนการติดต่อขอความช่วยเหลือ	วิเคราะห์เหตุการณ์ทันทีที่พบเหตุผิดปกติ เพื่อลดผลกระทบที่เกิดขึ้น	
	กบก. บริหาร IT Asset ที่กระทบจากภัยไซเบอร์ เช่น ยกเลิก ทำลาย เปลี่ยนใหม่	กบก. ตั้งค่า/ทดสอบ IT Asset อย่างเหมาะสม เมื่อกลับมาใช้ใหม่	
ความร่วมมือระหว่างหน่วยงาน Incident Management and Threat Intelligence			ประสานงานใกล้ชิดระหว่าง Incident Mgt, Threat Int และ Network
การสั่งการและการติดต่อสื่อสาร	มีช่องทางให้พนักงานของ สง. ใช้รายงานข้อมูลเหตุการณ์ไซเบอร์ได้อย่างรวดเร็ว	มีแผนประชาสัมพันธ์ให้บุคคลภายนอกทราบตามเหมาะสม	
	กำหนดขั้นตอนการแจ้งเตือนทุกคนที่เกี่ยวข้อง เช่น ลูกค้า หน่วยงานอื่นๆ		
	กำหนดให้มีการรายงานเหตุการณ์ไซเบอร์หรือช่องโหว่ต่อผู้บริหารตามความเสี่ยง		
การรายงานเหตุการณ์ความเสียหาย (Incident Report)	จัดประเภทของเหตุการณ์ และติดตามเหตุการณ์ผิดปกติที่เกิดขึ้น		
	วิเคราะห์และจัดทำรายงานสรุปคณะกรรมการที่เกี่ยวข้อง		

ธนาคารแห่งประเทศไทย

Control Principles

1. Governanace | 2. Identification | 3. Protection | 4. Detection | 5. Response and Recovery | **6. 3rd Party Management**

	Baseline	Intermediate	Advanced
การเชื่อมโยง/เชื่อมต่อ	- มีนโยบาย และ Security Control - ระบุกระบวนการทางธุรกิจที่สำคัญได้		
	มี Network and System's Data Flow Diagrams แสดงการเชื่อมต่อ	ครอบคลุมถึง Data Repositories ที่สอดคล้องกับ Inventory list	
		มีการสอบทานผลกระทบ ทั้งก่อนที่จะทำการปรับปรุงหรือเปลี่ยนแปลงการเชื่อมต่อ	
			ทำงานอย่างใกล้ชิดกับ 3rd Party เพื่อบำรุงและปรับปรุงการรักษาความมั่นคงปลอดภัย
การบริหารจัดการสัญญา	จัดทำสัญญาให้มีมาตรการในการรักษาความมั่นคงปลอดภัยในส่วนที่ให้บริการกับ สง.		มีมาตรการไม่ต่ำกว่ามาตรฐานของ สง.
	ระบุถึงหน้าที่ความรับผิดชอบในการรับมือต่อเหตุการณ์ผิดปกติที่เกิดขึ้นกับ สง.	ระบุถึงหน้าที่ความรับผิดชอบในการรายงานช่องโหว่ที่เกิดขึ้นกับ สง.	
	ระบุถึงแนวทางการส่งคืนหรือทำลายข้อมูลสำคัญในกรณีที่มีการยกเลิกสัญญา	มีแนวทางรองรับกรณียกเลิกหรือยุติการใช้บริการ	
	ระบุสิทธิเรียกร้องค่าเสียหายในกรณีที่ไม่สามารถปฏิบัติตามที่ สง. กำหนดไว้		

ธนาคารแห่งประเทศไทย

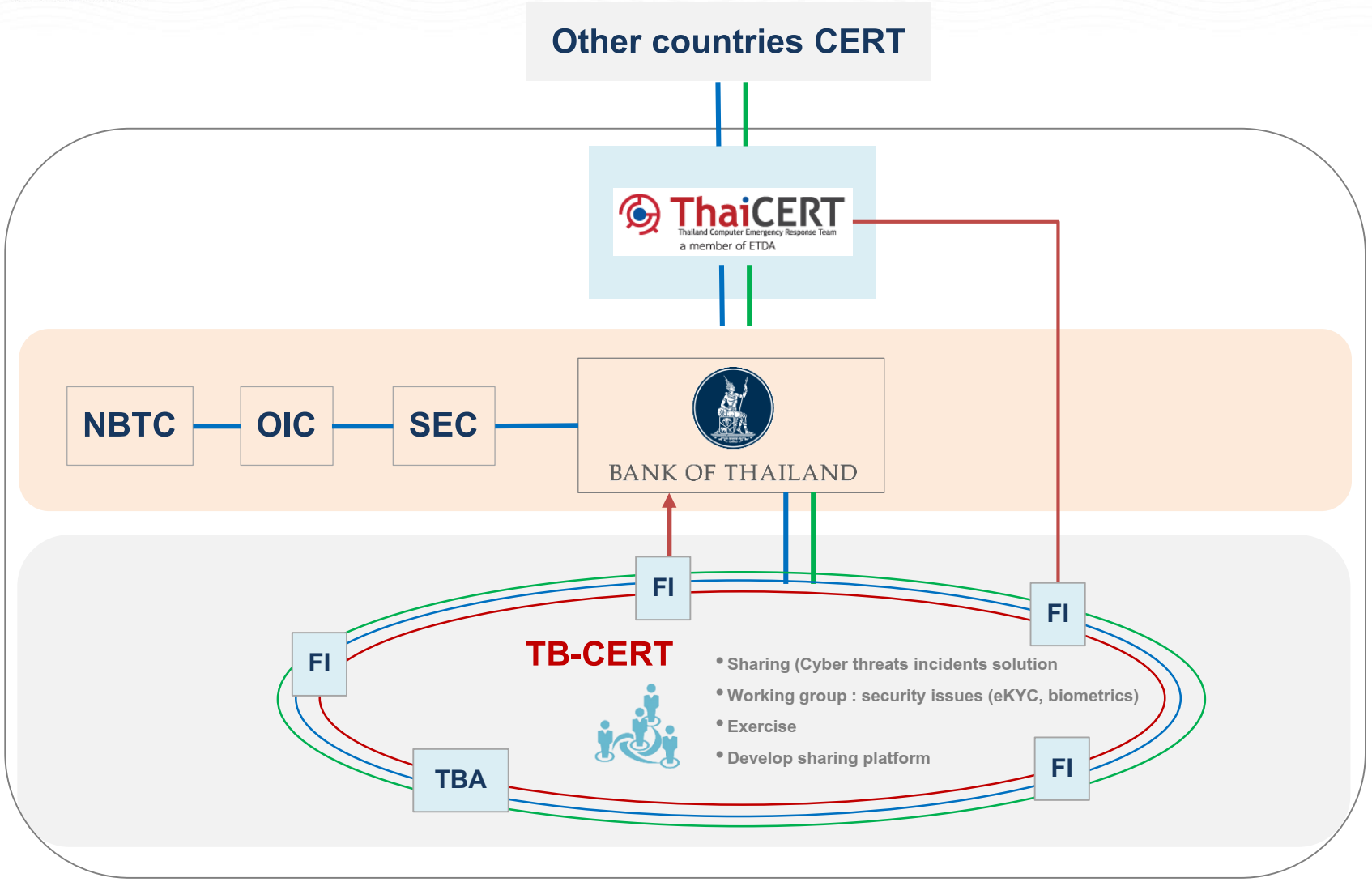
Control Principles

1. Governanace | 2. Identification | 3. Protection | 4. Detection | 5. Response and Recovery | **6. 3rd Party Management**

	Baseline	Intermediate	Advanced
การทำ Due Diligence	ประเมินความเสี่ยงการควบคุมภัยด้านไซเบอร์ก่อนทำสัญญาว่าจ้างทุกครั้ง		
	จัดเก็บและปรับปรุงรายชื่อให้เป็นปัจจุบัน		
การติดตามความเสี่ยงของการใช้บริการ	กำหนดแนวการติดตามการปฏิบัติงานและสอบทานให้เป็นไปตามเงื่อนไขสัญญา	กำหนดขอบเขตและความถี่ในการติดตาม	ติดตามการเข้าถึงข้อมูลที่สำคัญอย่างใกล้ชิดตามหลัก Least Privilege
	ทบทวนและปรับปรุงผลการประเมินความเสี่ยง 3rd Party		
	จัดให้มีการตรวจสอบการบริหารจัดการการเชื่อมต่อ 3rd Party		เข้าตรวจสอบหรือสอบทานรายงานการตรวจสอบของหน่วยงานภายนอก
		มีระบบแจ้งเตือนเมื่อถึงเวลาที่ 3rd Party ต้องนำส่งข้อมูลตามที่กำหนดมาให้ สง.	

Collaboration & Intelligence Sharing

Cybersecurity Information Sharing in Thailand



NBTC - National Broadcasting and Telecommunications Commission
OIC - Office of Insurance Commission
SEC - The Securities and Exchange Commission
TBA - Thai Bank Association

Cyber threats / incident sharing
Knowledge sharing (threats, solutions)
Capability building

พัฒนาบุคลากรในภาคธุรกิจการเงิน

พัฒนาบุคลากรภาคการเงิน

ธนาคารแห่งประเทศไทย

คณะกรรมการและผู้บริหาร

จัดทำกรอบการให้ความรู้ด้าน Cybersecurity แก่คณะกรรมการและผู้บริหารระดับสูง

- จัดประชุม CEO เพื่อให้ความรู้ด้าน Cybersecurity
- หารือ IOD เพื่อวางโครงการอบรมด้าน Cybersecuirty

บุคลากร

- 5 องค์กร (TBA, 3 Regulators, Vendors, มหาวิทยาลัย) ร่วมกับจัดทำกรอบการพัฒนาบุคลากรด้าน Cybersecurity โดยเริ่มต้นวางโครงการอบรมด้าน Cybersecuirty

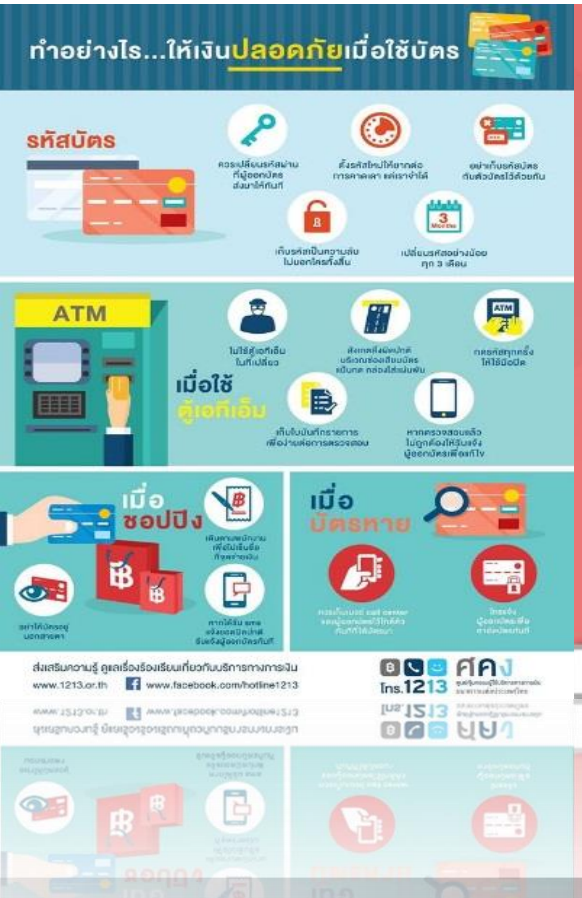
Financial Technology Literacy

ธนาคารแห่งประเทศไทย

การคุ้มครองผู้ใช้บริการทางการเงิน

ศคง
Ins.1213
ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน
ธนาคารแห่งประเทศไทย

- นำเสนอข้อมูลเกี่ยวกับผลิตภัณฑ์ทางการเงิน
- ตอบคำถาม รับเรื่องร้องเรียน
- ดูแลความเดือนร้อนลูกค้า



ธนาคารแห่งประเทศไทย

การกำกับดูแลด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

กฎหมายและหลักเกณฑ์ที่ใช้ในการกำกับดูแลด้าน IT

ธนาคารแห่งประเทศไทย

พ.ร.บ. / พ.ร.ฎ.

- พ.ร.บ. ธุรกิจสถาบันการเงิน พ.ศ. 2551
- พ.ร.บ. ธุรกิจสถาบันการเงิน (ฉบับที่2) พ.ศ. 2558
- พ.ร.ฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551
- ประกาศคณะปฏิวัติ ฉบับที่ 58

ประกาศ ธปท.

- ประกาศ สนส. 26/2551 เรื่อง การให้บริการการเงินทางอิเล็กทรอนิกส์
- ประกาศ สนส. 19/2559 เรื่อง IT Outsourcing
- ประกาศ สรข. 2/2552 และ สรข. 3/2552 เกี่ยวกับการประกอบธุรกิจ e-Payment
- (ร่าง) ประกาศ เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้าน IT ของ สง.
- (ร่าง) ประกาศ เรื่อง เหตุการณ์สำคัญที่ต้องรายงานต่อธนาคารแห่งประเทศไทย

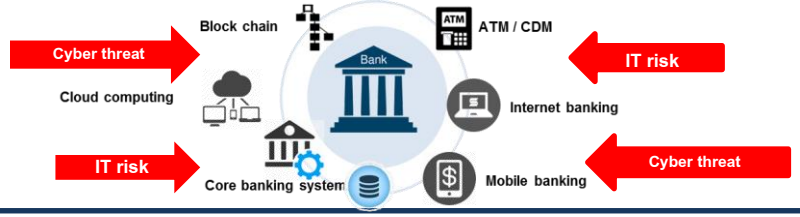
แนวปฏิบัติ ธปท.

- แนวปฏิบัติ ธปท. เรื่อง การบริหารความเสี่ยงด้านปฏิบัติการ
- แนวปฏิบัติ ธปท. เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ของ สง.
- แนวปฏิบัติ ธปท. เรื่อง IT Best Practices I & II
- แนวปฏิบัติ ธปท. เรื่อง การป้องกันความเสี่ยงของระบบ ATM จากโปรแกรม Malware
- (ร่าง) แนวปฏิบัติ ธปท. เรื่อง การกำกับดูแลความเสี่ยงด้าน IT ของ สง.
- (ร่าง) แนวปฏิบัติ ธปท. เรื่อง การประเมินความพร้อมด้าน Cyber Resilience

การยกระดับแนวทางการกำกับดูแลด้าน IT

ธนาคารแห่งประเทศไทย

การเปลี่ยนแปลงการดำเนินธุรกิจ สง.

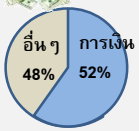


Weakpoint ของการดูแลและการบริหารจัดการด้าน IT ของ สง.

- IT Risk ไม่ถูกยกเป็นความเสี่ยงสำคัญระดับองค์กร (Enterprise-Wide-Risk)
- คณะกรรมการ สง. มีความรู้และประสบการณ์ไม่เพียงพอต่อการกำกับดูแลด้าน IT
- IT risk awareness ในองค์กรไม่เพียงพอ ไม่สอดคล้องกับการใช้เทคโนโลยี
- พบข้อบกพร่องในทางปฏิบัติของ สง. ในบางเรื่อง

ภัยคุกคามทางไซเบอร์และผลกระทบเพิ่มมากขึ้น

Phishing | Ransomware | IOT Botnets | Machine Learning Attacks



ผลกระทบจากภัยคุกคามฯ : 689 ล้านคน 126 พันล้านบาท

DDos attack / ransomware (Wannacry / Petya) / ตู้ ATM ถูก malware

เป้าหมายหลักของ Hacker คือ “ภาคการเงิน”

ไทยมี cyber threat สูงเป็น “อันดับ 11 ของโลก” และ “อันดับ 5 ของเอเชีย”

- หลักเกณฑ์ปัจจุบันอาจไม่เพียงพอรองรับการใช้ IT และความเสี่ยงที่มากขึ้น
- ไม่มีเกณฑ์กำกับดูแลการบริหารจัดการ IT Risk แบบองค์รวม : มีเฉพาะเกณฑ์ IT security ในส่วนของ e-Banking แนวปฏิบัติ BCM & BCP และเกณฑ์ IT Outsourcing

เป้าหมายของการกำกับดูแล

สง. มีการใช้ IT ที่สอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจ และพร้อมรับการเปลี่ยนแปลง

คณะกรรมการ สง. และผู้บริหารระดับสูงมีบทบาทสำคัญในการกำกับดูแลความเสี่ยงด้าน IT

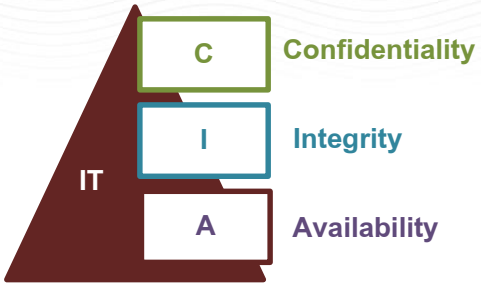
ยกระดับความเสี่ยงด้าน IT ถือเป็นความเสี่ยงที่สำคัญขององค์กร (Enterprise-Wide-Risk)

สง. มีการรักษาความมั่นคงปลอดภัยและการบริหารความเสี่ยงด้าน IT ที่สอดคล้องกับความเสี่ยงที่เพิ่มมากขึ้น

สง. มีการบริหารจัดการโครงการด้าน IT ที่รัดกุมและมีประสิทธิภาพ

ธนาคารแห่งประเทศไทย

ภาพรวมการกำกับดูแล ความเสี่ยงด้าน IT และ Cyber ของ สง.



มาตรฐานสากล

+

หลักเกณฑ์การกำกับดูแลต่างประเทศ

1 ประกาศ ธปท. เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน

สถาบันการเงิน SFIs (อาจพิจารณาบังคับใช้ในอนาคต)

+

2 แนวปฏิบัติในการกำกับดูแลความเสี่ยงด้าน IT ของ สง. (IT Risk Management Implementation Guideline)

สถาบันการเงิน SFIs

3 แนวปฏิบัติในการประเมินความพร้อมด้าน Cyber Resilience (ภายใต้หลักเกณฑ์ IT Risk Management)

สถาบันการเงิน SFIs ผู้ให้บริการ Switching

สาระสำคัญของประกาศ เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของ สง.

1. การกำกับดูแลความเสี่ยงด้าน IT
   - 1.1 IT Governance
     - บทบาทหน้าที่คณะกรรมการ / โครงสร้างการกำกับดูแล / การบริหารจัดการบุคลากร / การส่งเสริมให้ตระหนักถึงความเสี่ยงด้าน IT / นโยบายที่เกี่ยวข้องกับ IT Risk
   - 1.2 IT Security (1st line)
     - Asset management / Information / Access control / Physical and environmental / Communications / IT operations / Acquisition and development / Incident and problem management / Contingency plan / Supplier management
   - 1.3 IT Risk Management (2nd line)
     - Assessment / Treatment / Monitoring and review / Reporting
   - 1.4 IT Project Management
     - Feasibility study / Project management framework
   - 1.5 IT Compliance
   - 1.6 IT Audit (3rd line)
2. การรายงานปัญหาหรือเหตุการณ์ผิดปกติ
3. การขออนุญาตกรณีเปลี่ยนแปลงการใช้เทคโนโลยีที่มีนัยสำคัญ
4. การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

หลักเกณฑ์การกำกับดูแลความเสี่ยงด้าน IT ของ สง.

1 การกำกับดูแลความเสี่ยงด้าน IT

1.1 IT Governance : ธรรมาภิบาลด้าน IT

1

บทบาทและหน้าที่ของคณะกรรมการของ สง.

คณะกรรมการ สง. ต้องมีความรู้หรือประสบการณ์ด้าน IT อย่างเพียงพอที่จะกำกับดูแลและสนับสนุนให้องค์กรมีการบริหารความเสี่ยงด้าน IT ที่เหมาะสมและสอดคล้องกับการดำเนินธุรกิจ

คณะกรรมการต้องได้รับการอบรมให้ความรู้ด้าน IT อย่างเพียงพอเพื่อกำกับดูแล IT อย่างมีประสิทธิภาพ

- มีกรรมการอย่างน้อย 1 ท่านที่มีความรู้ / ประสบการณ์ด้าน IT
- ดูแลการใช้ IT ให้สอดรับกับ **business strategy** และพร้อมรับการเปลี่ยนแปลงทั้งด้าน IT และด้านธุรกิจ
- ดูแลให้มีการบริหารความเสี่ยงด้าน IT โดยถือเป็นส่วนหนึ่งของ **Enterprise risk management : ERM**
- อนุมัตินโยบายด้าน IT ดูแลและติดตามการนำไปใช้อย่างเหมาะสม
  - ✓ นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT (IT security policy) รวมถึงนโยบายการจัดทำแผนฉุกเฉินด้าน IT
  - ✓ นโยบายการบริหารความเสี่ยงด้าน IT (IT risk management policy)
- ดูแลให้มีการติดตาม ตรวจสอบ และรายงานต่อคณะกรรมการ สง. / คณะกรรมการที่ได้รับมอบหมาย / ผู้บริหารระดับสูง
- ส่งเสริม IT awareness ในองค์กรให้ตระหนักถึงความสำคัญของความเสี่ยง IT และใช้ IT ได้อย่างถูกต้อง

หลักเกณฑ์ที่เกี่ยวข้อง

- ประกาศ ธปท. ที่ สนส. 13/2552 เรื่อง ธรรมาภิบาลของสถาบันการเงิน
- ประกาศ ธปท. ที่ สนส. 15/2552 เรื่อง อำนาจหน้าที่ของกรรมการของสถาบันการเงินที่ธนาคารแห่งประเทศไทยให้ความสำคัญสูงสุด

ธนาคารแห่งประเทศไทย (๒๔๘๕-๒๕๖๐)

1 การกำกับดูแลความเสี่ยงด้าน IT

1.1 IT Governance : ธรรมาภิบาลด้าน IT

1

โครงสร้างการกำกับดูแล

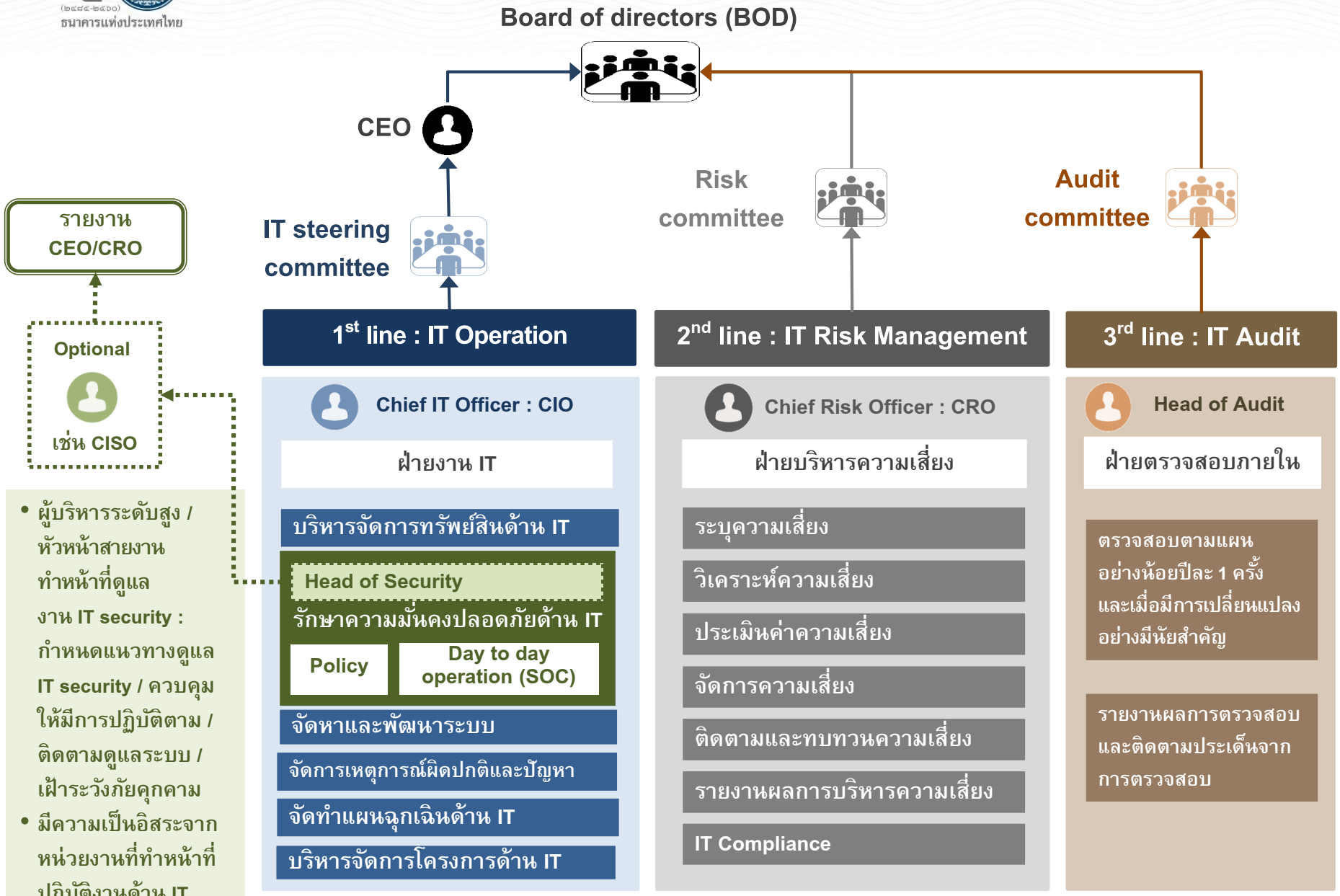
โครงสร้างองค์กรต้องเอื้อต่อการบริหารความเสี่ยงด้าน IT ที่เหมาะสม และสอดคล้องตามหลัก 3 lines of defense

- **3 lines of defense** :
  มีการถ่วงดุลอย่างอิสระ โดยแบ่งแยกหน้าที่ระหว่าง (1) การปฏิบัติงานด้าน IT (2) การบริหารความเสี่ยงด้าน IT และ (3) การตรวจสอบด้าน IT
- **IT committees** :
  (1) คณะกรรมการที่ทำหน้าที่กำกับดูแลการปฏิบัติงานด้าน IT : ดูแลการกำหนดกลยุทธ์ด้าน IT / ดูแลและติดตามการปฏิบัติงานด้าน IT ให้เป็นไปตามกลยุทธ์ที่กำหนด
  (2) คณะกรรมการที่ทำหน้าที่กำกับดูแลการบริหารความเสี่ยงด้าน IT : ดูแลการกำหนดนโยบายการบริหารความเสี่ยงด้าน IT / ดูแลและติดตามให้เป็นไปตามนโยบายที่กำหนด โดยเชื่อมโยงกับความเสี่ยงในภาพรวมของ สง. / ดูแลการปฏิบัติตามหลักเกณฑ์ (IT compliance)
  (3) คณะกรรมการที่ทำหน้าที่กำกับดูแลให้มีการตรวจสอบด้าน IT : ดูแลการตรวจสอบการปฏิบัติงานด้าน IT และการบริหารความเสี่ยงด้าน IT / สอบทานการปฏิบัติตามหลักเกณฑ์

สนับสนุนให้มีผู้บริหารระดับสูง หรือ หัวหน้าหน่วยงานที่ทำหน้าที่บริหารจัดการ IT Security (เช่น CISO)

- ✓ เป็นผู้ที่มีความรู้ความสามารถด้าน IT security
- ✓ มีความเป็นอิสระจากหน่วยงานที่ปฏิบัติงานด้าน IT

โครงสร้างการกำกับดูแลด้าน IT ใน สง.



1. การกำกับดูแลความเสี่ยงด้าน IT (IT Governance)

นโยบายที่เกี่ยวกับการบริหารความเสี่ยงด้าน IT

- สง. ต้องจัดให้มีนโยบายด้าน IT ที่เป็นลายลักษณ์อักษร อนุมัติโดยคณะกรรมการ สง.
- มีการดูแลติดตามการปฏิบัติตามนโยบายอย่างเหมาะสม
- มีการทบทวนนโยบายฯ อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

1 นโยบายการบริหารความเสี่ยงด้าน IT

IT risk management policy

- ระบุความเสี่ยง :
  ครอบคลุมความเสี่ยงที่สำคัญ
- วิเคราะห์ความเสี่ยง :
  เข้าใจความเสี่ยง เพื่อหาแนวทางในการจัดการ
- ประเมินค่าความเสี่ยง :
  โอกาส-ผลกระทบต่อ การปฏิบัติงานและการดำเนินธุรกิจ
- จัดการความเสี่ยง :
  แนวทางในการจัดการ ควบคุม และป้องกัน
- ติดตามและทบทวนความเสี่ยง :
  ให้ความเสี่ยงอยู่ภายใต้ระดับที่ยอมรับได้
- รายงานความเสี่ยง :
  ให้ทราบผลการบริหารความเสี่ยงและแนวโน้ม

2 นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT

IT security policy

1. การบริหารจัดการทรัพย์สินด้าน IT (IT asset management)
2. การรักษาความปลอดภัยของข้อมูล (information security)
3. การควบคุมการเข้าถึง (access control)
4. การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)
5. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)
6. การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security)
7. การจัดหาและการพัฒนาระบบ IT (system acquisition and development)
8. การบริหารจัดการเหตุการณ์ผิดปกติหรือปัญหาด้าน IT (IT incident and problem management)
9. แผนฉุกเฉินด้าน IT (disaster recovery plan)
10. การบริหารจัดการหน่วยงานภายนอก (Supplier management)

3 นโยบายการใช้บริการจากผู้ให้บริการภายนอกด้าน IT

ประกาศ ธปท. ที่ สนส. 19/2559
เรื่อง การใช้บริการ
IT Outsourcing

ธนาคารแห่งประเทศไทย

1 การกำกับดูแลความเสี่ยงด้าน IT

โครงสร้างและหน้าที่ในการดูแลความเสี่ยงด้าน IT

หน้าที่และกระบวนการในการรักษาความมั่นคงปลอดภัยและการบริหารความเสี่ยง แบ่งตามหลักการ 3 lines of defense

หลักเกณฑ์ที่เกี่ยวข้อง

ร่างประกาศ Banking channel

- Branch
- ATM / CDM
- Internet banking
- Mobile banking
- Card (EDC)
- Payment agent

ประกาศ ธปท. ที่ สนส. 19/2559 IT Outsourcing

แนวปฏิบัติ BCM / BCP (3 ส.ค. 51)

1st line - IT Operation

1.2 IT Security

IT security policy

2 Information security

5 Communications security

10 Supplier management

Service provider

IT Outsourcing

Data Center

ศูนย์คอมพิวเตอร์หลัก

Network Equipment เช่น firewall/ router

Servers ประมวลข้อมูลจากระบบต่าง ๆ เช่น Branch / ATM / Internet Banking

Core banking

ศูนย์คอมพิวเตอร์สำรอง

3 Access control

1 IT asset management

2 4 5 Information / Physical & environmental / Communications security

6 IT operations security

7 System acquisition and development

8 IT incident and problem management

9 IT contingency plan

2nd line - IT Risk Management & Compliance

IT Risk Mangement

IT Compliance

3rd line - IT Audit

ตรวจสอบการปฏิบัติงานของ IT Operation และ IT Risk Management

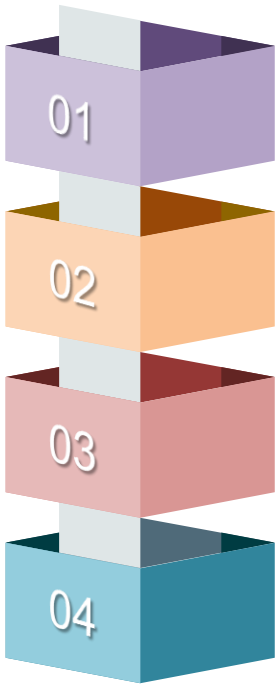
ธนาคารแห่งประเทศไทย

โครงสร้างและหน้าที่ในการดูแลความเสี่ยงด้าน IT

1.3 IT Risk Management

2nd line : IT Risk Management and Compliance

IT Risk Management – มีการบริหารความเสี่ยงอย่างมีประสิทธิภาพตาม IT risk management policy ที่กำหนด



การประเมินความเสี่ยง (risk assessment)

- ระบุความเสี่ยง (risk identification) : ระบุความเสี่ยง ภัยคุกคาม และช่องโหว่ที่สำคัญ
- วิเคราะห์ความเสี่ยง (risk analysis) : เข้าใจและวิเคราะห์ความเสี่ยง เพื่อหาแนวทางจัดการที่เหมาะสม
- ประเมินค่าความเสี่ยง (risk evaluation) : ประเมินโอกาสและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ

การจัดการความเสี่ยง (risk treatment)

- มีแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสม สอดคล้องกับผลการประเมินความเสี่ยง

การติดตามและทบทวนความเสี่ยง (risk monitoring and review)

- ติดตามและทบทวนความเสี่ยง ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ (risk appetite)

การรายงานความเสี่ยง (risk reporting)

- รายงานผลการบริหารความเสี่ยงและแนวโน้มของความเสี่ยงต่อคณะกรรมการ สง.

*** มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการการบริหารความเสี่ยงด้าน IT อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่เปลี่ยนแปลง ***

1.4 IT Compliance

IT compliance

- ปฏิบัติตามกฎหมาย / หลักเกณฑ์ที่เกี่ยวกับ IT เช่น พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ และ พ.ร.บ. ระบบการชำระเงิน

ธนาคารแห่งประเทศไทย

1 การกำกับดูแลความเสี่ยงด้าน IT

1.5 IT Project Management : การบริหารจัดการโครงการด้าน IT

ประเมินความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ

ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อฝ่ายงานอื่นและระบบที่เกี่ยวข้อง และเลือกใช้เทคโนโลยีที่เหมาะสม

จัดลำดับความสำคัญของโครงการ

จัดลำดับความสำคัญของโครงการ และเสนอขออนุมัติต่อคณะกรรมการ สง. / คณะกรรมการที่ได้รับมอบหมาย / ผู้บริหารระดับสูง

จัดทำกรอบการบริหารโครงการ (IT project management framework)

คณะกรรมการกำกับดูแลโครงการ		กำกับดูแลความคืบหน้า ให้คำแนะนำ พิจารณาตัดสินใจการดำเนินงานของโครงการที่สำคัญ
Project management office (PMO)		ติดตามความคืบหน้าและรายงานความคืบหน้าของโครงการต่อคณะกรรมการ สง. / คณะกรรมการกำกับดูแลโครงการ / ผู้บริหารระดับสูง
Project manager		บริหารจัดการโครงการแต่ละโครงการ

ธนาคารแห่งประเทศไทย

โครงสร้างและหน้าที่ในการดูแลความเสี่ยงด้าน IT

1.6 IT Audit

3rd line : IT Audit

IT Audit – มีการตรวจสอบการปฏิบัติงานของ IT operation (1st line) และ IT risk management (2rd line)

ผู้ตรวจสอบด้าน IT

ต้องมีความรู้ ประสบการณ์ ความเชี่ยวชาญ และ มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานและบริหารความเสี่ยง

แผนงานและขอบเขตการตรวจสอบ

สอดคล้องกับความสำคัญและความเสี่ยงของการใช้ IT และ IT risk management policy โดยทบทวนอย่างน้อยปีละ 1 ครั้ง

การตรวจสอบ

- ตรวจสอบด้าน IT ตามแผนงานและขอบเขต อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุการณ์ผิดปกติที่มีนัยสำคัญ

รายงานการตรวจสอบ

จัดทำรายงานผลการตรวจสอบเสนอต่อคณะกรรมการตรวจสอบ และจัดเก็บให้ ธปท. ตรวจสอบหากร้องขอ

การติดตามประเด็นการตรวจสอบ

ติดตามประเด็นจากการตรวจสอบ และรายงานประเด็นสำคัญให้กับคณะกรรมการตรวจสอบและฝ่ายงานที่เกี่ยวข้อง

ธนาคารแห่งประเทศไทย

2 การรายงานปัญหาหรือเหตุการณ์ผิดปกติจากการใช้ IT

เกิดเหตุการณ์ที่ IT ที่สำคัญเกิดปัญหา / ขัดข้อง ส่งผลกระทบต่อผู้ใช้บริการในวงกว้าง หรือเกิดเหตุการณ์ที่ IT ที่สำคัญถูกโจมตีหรือถูกขู่โจมตี เช่น การแพร่กระจายไวรัส / DDos attack / Web defacement

→ รายงานทันทีเมื่อเกิด / รับรู้เหตุการณ์ โดยสามารถแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลังได้

→ ธนาคารแห่งประเทศไทย

3 การขออนุญาตกรณีเปลี่ยนแปลงการใช้เทคโนโลยีอย่างมีนัยสำคัญ

ยื่นขออนุญาตมายัง ธปท. ก่อนเปลี่ยนแปลงการใช้เทคโนโลยี

แผนการเปลี่ยนแปลงการใช้เทคโนโลยีที่มีผลกระทบหรือมีความเสี่ยงอย่างมีนัยสำคัญ +

- รายละเอียดการใช้ IT
- การบริหารความเสี่ยง
- การคุ้มครองลูกค้า
- แผนฉุกเฉินด้าน IT

→ ธนาคารแห่งประเทศไทย

4 การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

- หาก สง. ไม่สามารถปฏิบัติตามหลักเกณฑ์ได้ ให้ยื่นขอผ่อนผันมาเป็นรายกรณี พร้อมแสดงเหตุผลและความจำเป็น และแผนการดำเนินการเพื่อให้ปฏิบัติตามหลักเกณฑ์ได้

ธนาคารแห่งประเทศไทย

4 Principles of IT Risk Management

1. Tone from The Top
2. Enterprise-wide Risk
3. 3 Lines of Defense
4. Building Capabilities

IT Risk Management Implemention Guidelines

1 IT Governance

- **2 IT Project Mgmt.**
- **3 IT Security**
- **4 IT Out-sourcing**

(ร่าง) แนวปฏิบัติ ธปท. เรื่อง การกำกับดูแลความเสี่ยงด้าน IT ของ สง.

1 IT Risk Governance

- บทบาทหน้าที่ของคณะกรรมการ สง.
- โครงสร้างองค์กรในการกำกับดูแลความเสี่ยง
- การบริหารจัดการบุคลากร
- นโยบายที่เกี่ยวกับการบริหารความเสี่ยงด้าน IT

2 IT Project Management

3 IT Security

- IT Asset Management
- Information Security
- Access Control
- Physical and Environmental Security
- Communication Security
- IT Operation Security
- System Acquisition and Development
- IT Incident and Problem Management
- IT Contigency Plan
- Third Party Management

4 IT Outsourcing

- การกำกับดูแลการใช้บริการ IT Outsourcing
- หลักเกณฑ์การแบ่งประเภทการใช้บริการ
- แนวทางการบริหารจัดการความเสี่ยง แนวทางการคัดเลือกผู้ให้บริการ และแนวทางการประเมินประสิทธิภาพ
- แนวทางการรักษาความมั่นคงปลอดภัยของระบบงานและข้อมูล
- การรายงานผลการประเมินความเสี่ยงและประสิทธิภาพการดำเนินงาน
- การตรวจสอบผู้ให้บริการภายนอก
- การคุ้มครองผู้ใช้บริการของ สง. จากการใช้บริการ IT Outsourcing

Questions?