ธนาคารแห่งประเทศไทย
BANK OF THAILAND

Media Briefing

# หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

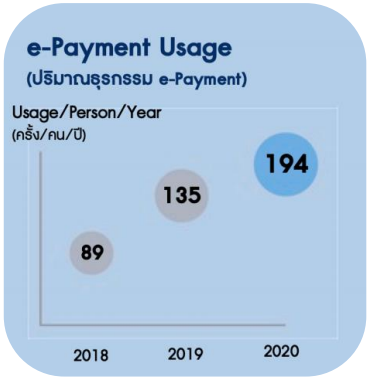
## ผู้ให้บริการและผู้ประกอบธุรกิจด้านการชำระเงิน

15 กุมภาพันธ์ 2564

ธนาคารแห่งประเทศไทย

# เหตุผลและความจำเป็น

- ผู้ใช้บริการและธุรกรรม e-Payment เพิ่มแบบก้าวกระโดด





- ภัยไซเบอร์เพิ่มสูงขึ้น
- เชื่อมต่อภายนอกเพิ่มมากขึ้น

- ผู้ประกอบธุรกิจจำเป็นต้องเพิ่มการระวังป้องกันภัยอย่างต่อเนื่อง ธปท. กำหนดหลักเกณฑ์ปฏิบัติ

ประกาศ
หลักเกณฑ์การ
กำกับความเสี่ยง
ด้าน IT

- ยกระดับความมั่นคงปลอดภัยของระบบและสร้างความมั่นใจให้กับลูกค้า

อ้างอิง ข้อมูลการชำระเงินของธนาคารแห่งประเทศไทย ณ 30 พ.ย. 2563

# หลักเกณฑ์กำกับดูแลด้าน IT Risk สำหรับผู้ประกอบธุรกิจ e-Payment

**2560**

พ.ร.บ. ระบบการชำระเงิน
มีประกาศและแนวปฏิบัติด้าน IT

**2563**

แนวนโยบาย
Mobile Banking Security

**2564**

ประกาศ
หลักเกณฑ์การกำกับความเสี่ยงด้าน IT
(IT Risk)

- Cyber Hygiene
- IT Risk Management

- ขอบเขตการบังคับใช้ :
  ผู้ประกอบธุรกิจ e-Payment
  ทุกแห่งที่มิใช่ สง.
- เทียบเท่ากับหลักเกณฑ์ที่บังคับ
  ใช้กับสถาบันเงิน

## IT Risk and Cyber Management

Governance | Identification | Protection | Detection | Response and Recovery

# สรุปหลักเกณฑ์

**ประกาศ หลักเกณฑ์การกำกับความเสี่ยงด้าน IT**

## 1 หลักเกณฑ์ขั้นต้นที่จำเป็น (Cyber Hygiene)

ผู้ประกอบธุรกิจทุกราย : ภายใน 3 เดือน

**1. การตั้งค่าระบบ ให้มีความปลอดภัย**
(Security Baseline and Hardening)
กำหนดและตั้งค่าให้สอดคล้องกับมาตรฐานสากลและภาพแวดล้อมด้าน IT

**2. การป้องกันระบบจาก Malware**
(Malware Protection)
ตรวจจับและป้องกัน malware ได้เท่าทันภัยคุกคาม

**3. การบริหารจัดการช่องโหว่**
(Security Patch Management)
กำหนดกระบวนการบริหารจัดการ security patch

**4. การจัดการสิทธิสูงของระบบ**
(Privilege User ID Management)
ควบคุมและจำกัดการใช้บัญชีผู้ใช้สิทธิสูงอย่างเข้มงวด

**5. การพิสูจน์ตัวตนอย่างปลอดภัย**
(Multi - Factor Authentication)
มีการพิสูจน์ตัวตนแบบ MFA ในบัญชีผู้ใช้สิทธิสูงและบัญชีผู้ใช้งานที่มีความเสี่ยง

**6. การทดสอบหาช่องโหว่**
(VA & Pentest)
ประเมินช่องโหว่และทดสอบเจาะระบบอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

## 2 หลักเกณฑ์การบริหารจัดการความเสี่ยงด้าน IT (IT Risk Management)

ผู้ประกอบธุรกิจที่มีนัยสำคัญ : ภายใน 1 ปี

**IT Governance**
ดูแลให้มีธรรมาภิบาลด้านเทคโนโลยีสารสนเทศที่ดี มีการบริหารความเสี่ยงด้าน IT ที่เหมาะสมตามระดับความเสี่ยง และจัดโครงสร้างการกำกับดูแลสอดคล้องตามหลัก 3rd line of defence

**IT Security**
รักษาความมั่นคงปลอดภัยด้าน IT อย่างรัดกุมตามกรอบหลักการ Confidentiality Integrity Availability

| | | | | |
|---|---|---|---|---|
| Asset Mgt. | Information Mgt. | Access Control | Physical & Env. | Communication |
| IT operations | Acquisition & Dev. | Incident & Problem Mgt. | IT DRP | Third Party Mgt. |

**IT Project Management**
บริหารจัดการความเสี่ยงของการดำเนินโครงการด้าน IT ที่มีนัยสำคัญอย่างมีประสิทธิภาพ

# กรอบเวลาและการดำเนินการต่อไป

**ประกาศในราชกิจจานุเบกษา**
**29 ม.ค. 64**

**29 เม.ย. 64**
หลักเกณฑ์
Cyber Hygiene
มีผลบังคับใช้

ผู้ประกอบธุรกิจ**ทุกราย**

**29 ม.ค. 65**
หลักเกณฑ์
IT Risk Management
มีผลบังคับใช้

ผู้ประกอบธุรกิจที่มี**นัยสำคัญ**

**ปี 65 เป็นต้นไป**
ผู้ประกอบธุรกิจประเมินตนเองทุกปี

ผู้ประกอบธุรกิจ**ทุกราย**

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

# Q & A

ธนาคารแห่งประเทศไทย

BANK OF THAILAND