Technology Risk Management for Directors

Prevention, Detection, Recovery

Presented by

Surachet Suchaiya,PhD.

Tanawat Tweewat, President of ISC2 Bangkok Chapter

Director’s Briefing 11/2025

www.Mysurachet.com

Part 1
What is Technology Risk?



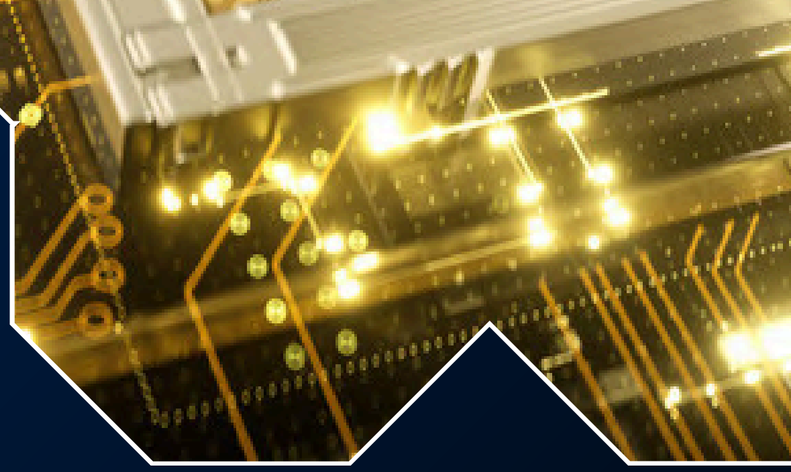
The Board in a Digital Storm

วันนี้ความเสี่ยงไม่ใช่แค่การเงิน
เทคโนโลยีทำให้ “เวลา” กลายเป็นต้นทุนใหม่

โลกธุรกิจเปลี่ยนเร็วกว่าแผนกลยุทธ์ เทคโนโลยีคือ
ทั้ง “โอกาส” และ “ความเสี่ยงใหม่”



Why Directors must care Technology Risk

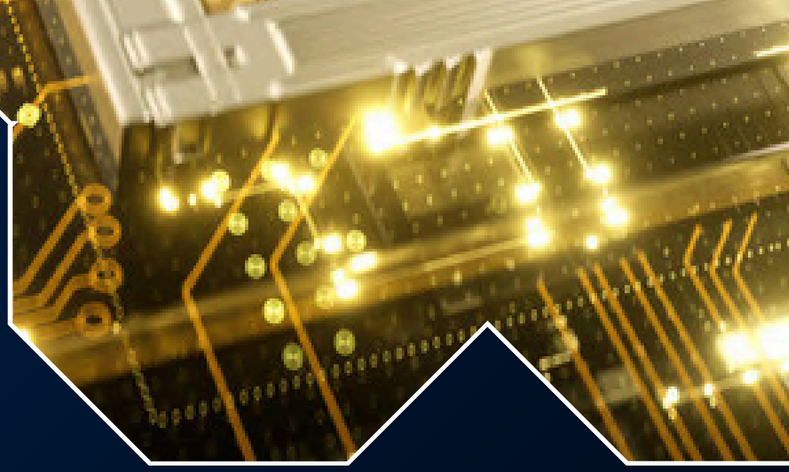


“ความเสี่ยงเทคโนโลยี” ไม่ใช่เรื่องของฝ่ายไอที แต่คือความรับผิดชอบของบอร์ด

ความต่อเนื่องทางธุรกิจ = ความเชื่อมั่นนักลงทุน

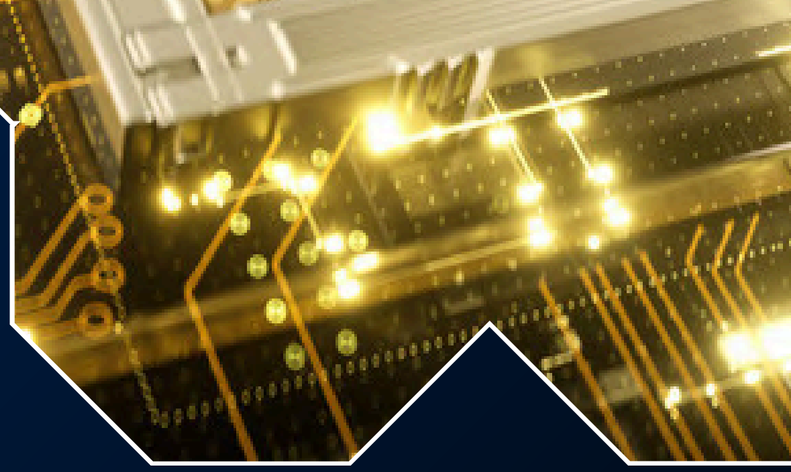


From Traditional Risk to Digital Risk



จาก “ความเสี่ยงการเงิน”
เชื่อมโยงไปสู่ “ความเสี่ยงปฏิบัติการ”
เชื่อมโยงไปสู่ “ความเสี่ยงเทคโนโลยี”





Definition : What is Technology Risk?

ความเสี่ยงจากความล้มเหลวของระบบเทคโนโลยี
หรือข้อมูล ซึ่งกระทบต่อการดำเนินงาน



Definition :
What is Technology Risk?



1

Value Protection
ทำให้รอดจากกฎหมาย

2

Value Creation
ทำได้เกินกฎหมายเพื่อสร้างคุณค่า

3

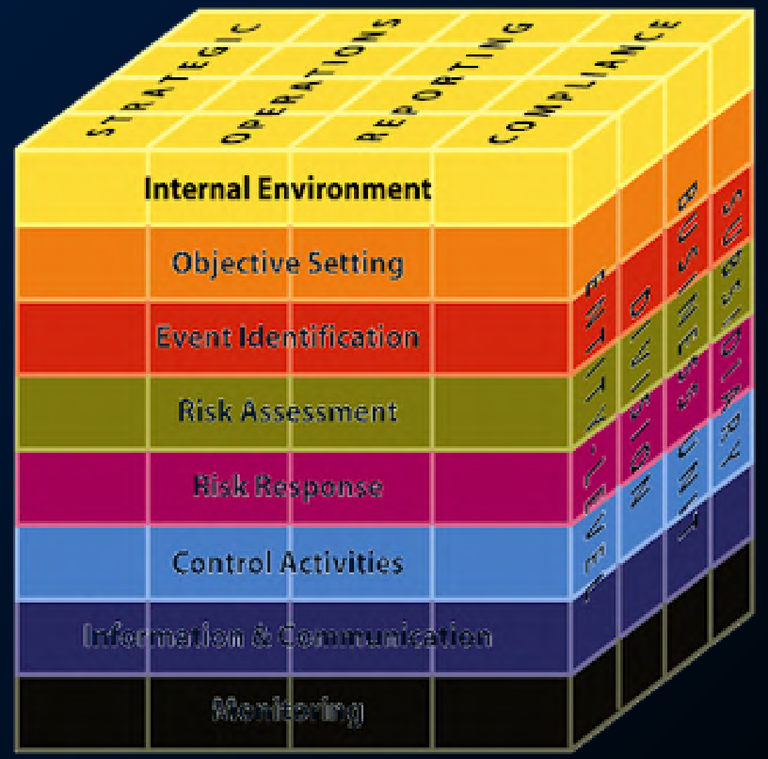
Value Acceleration
คิดนวัตกรรมเพื่อเป็นผู้นำอุตสาหกรรม

Part 2
Risk Framework



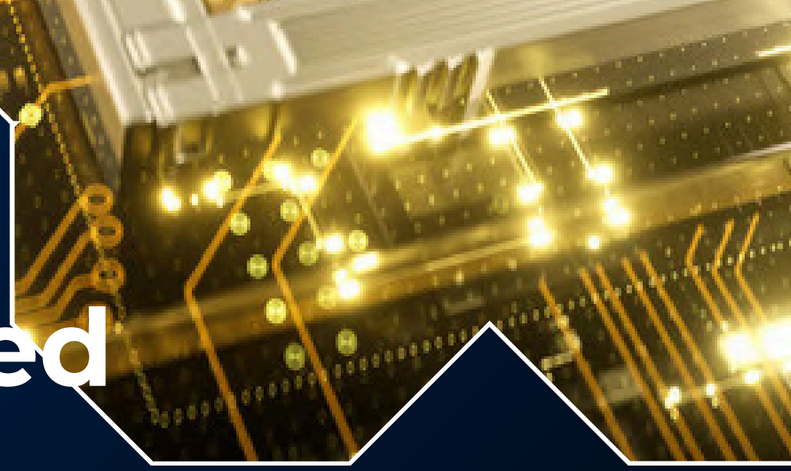
Enterprise Risk Management Overview (COSO)

กรอบ ERM เชื่อม
“กลยุทธ์ – การปฏิบัติ – การควบคุม” เข้าด้วยกัน



COSO Components Simplified



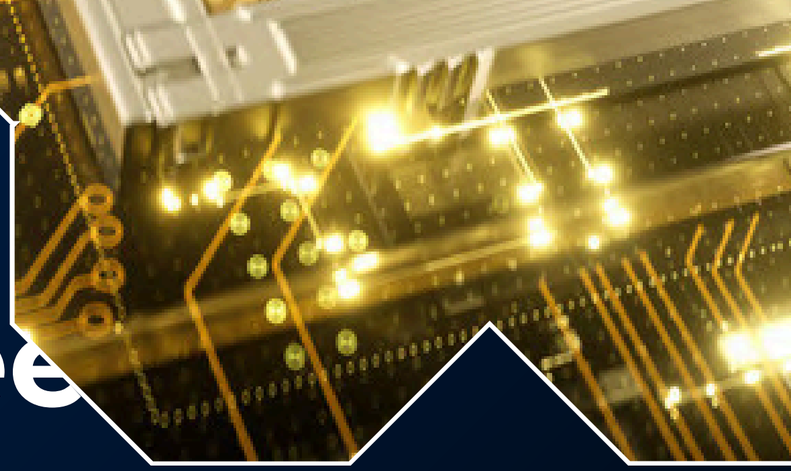


COSO Components Simplified

5 องค์ประกอบหลักของ COSO ERM

1. Governance & Culture
2. Strategy & Objective-setting
3. Performance
4. Review & Revision
5. Information, Communication & Reporting

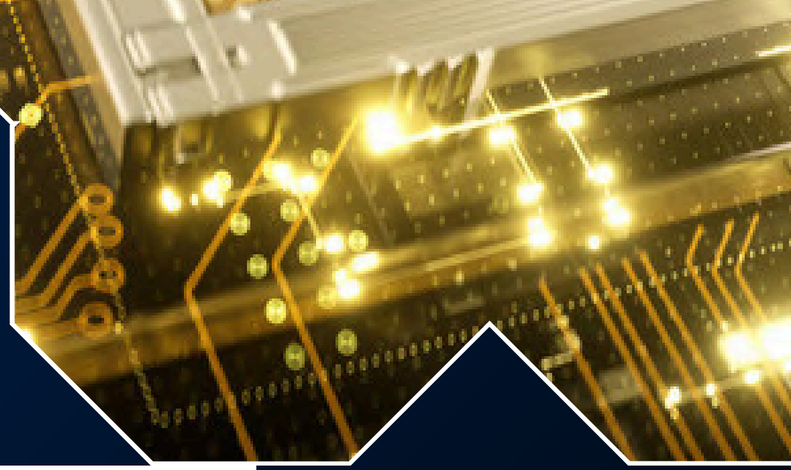
Board & Risk Committee Roles

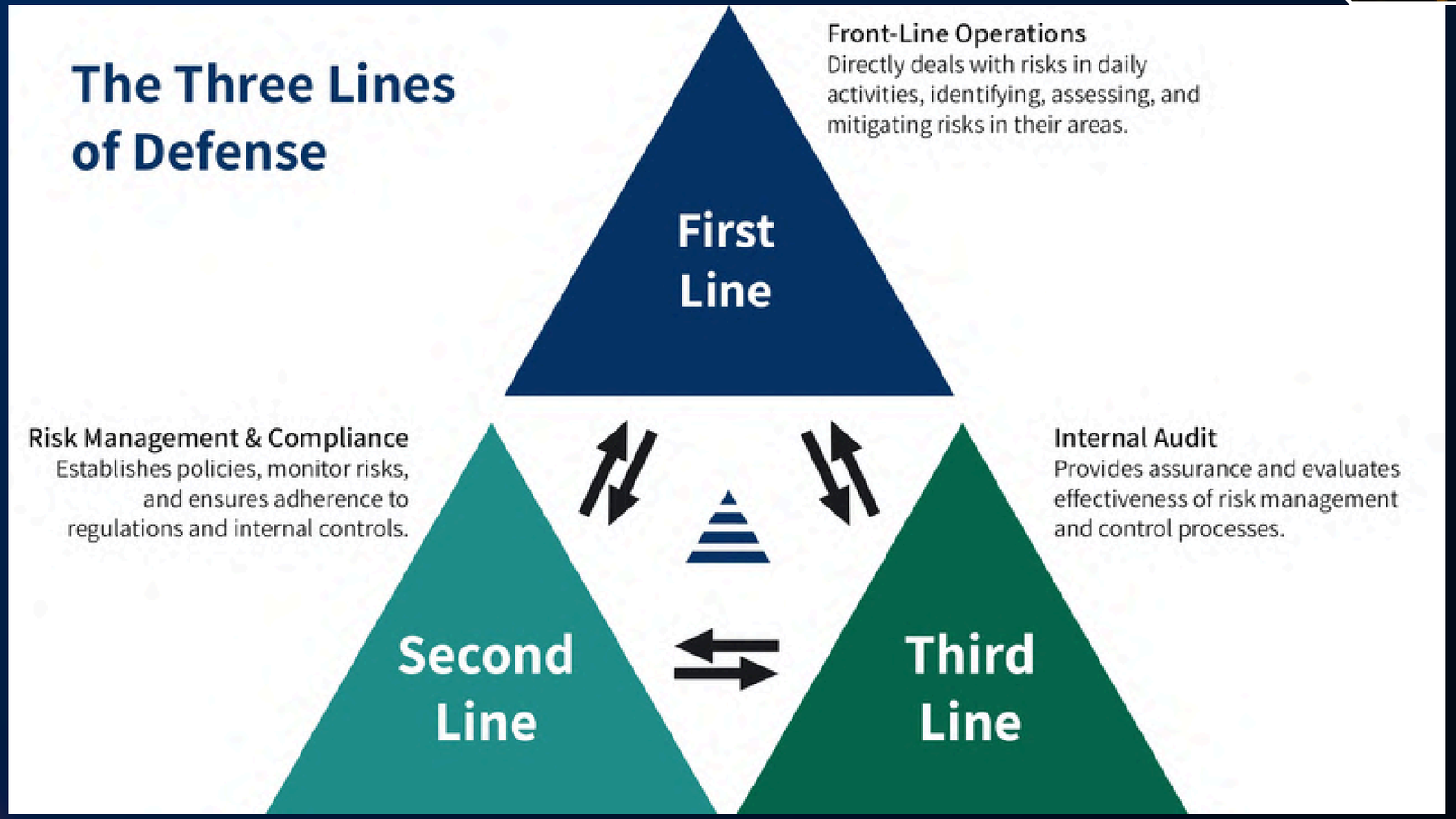


บอร์ดชี้ทิศ คณะกรรมการความเสี่ยงวางกรอบ
ฝ่ายบริหารลงมือ

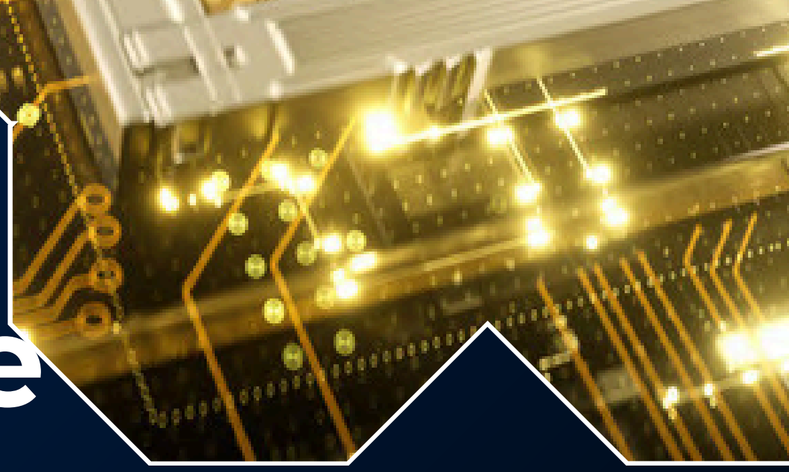


Three Lines of Defense





Integrating Governance with Technology

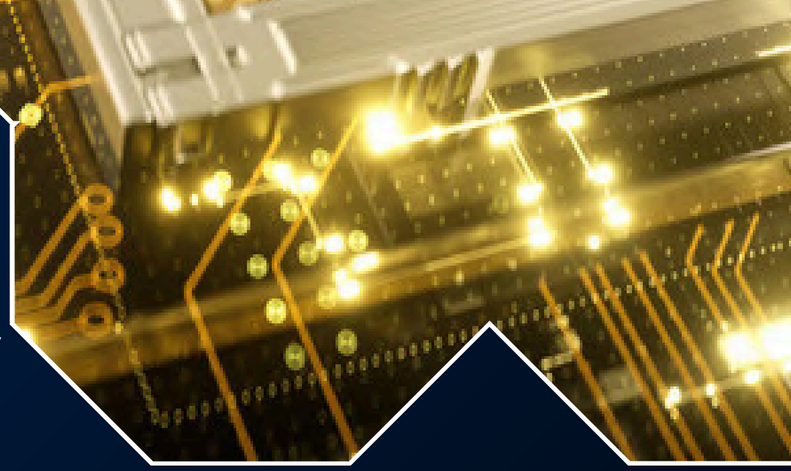


“Technology Risk” ต้องถูกบูรณาการเข้าในโครงสร้างกำกับดูแลของบอร์ด



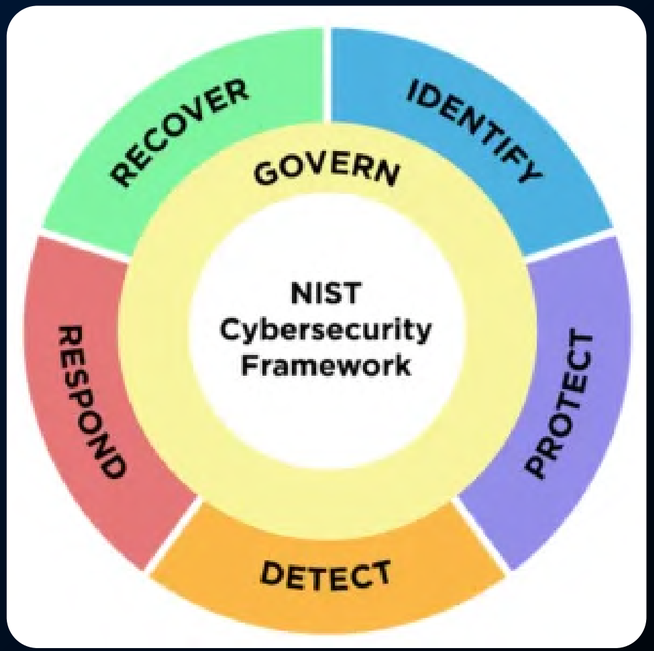
Part 3
Technology Risk Cycle (NIST CSF 2.0)

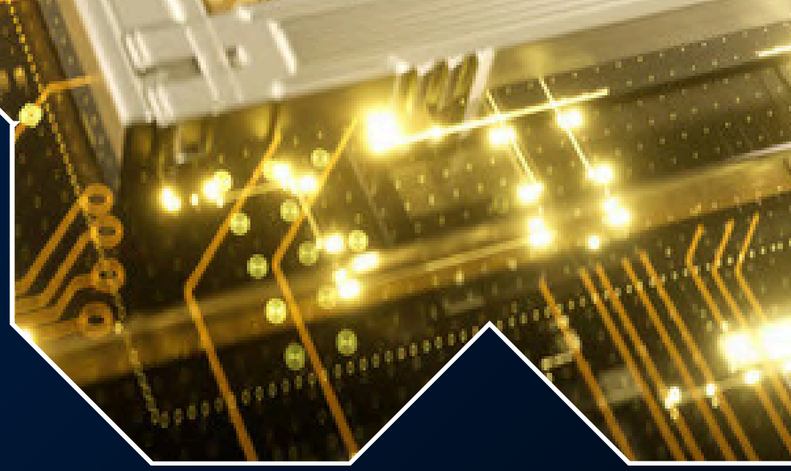




The NIST Cybersecurity Framework 2.0 Overview

NIST CSF 2.0 : กรอบมาตรฐานที่ใช้วัดความ
พร้อมด้าน Cyber Resilience

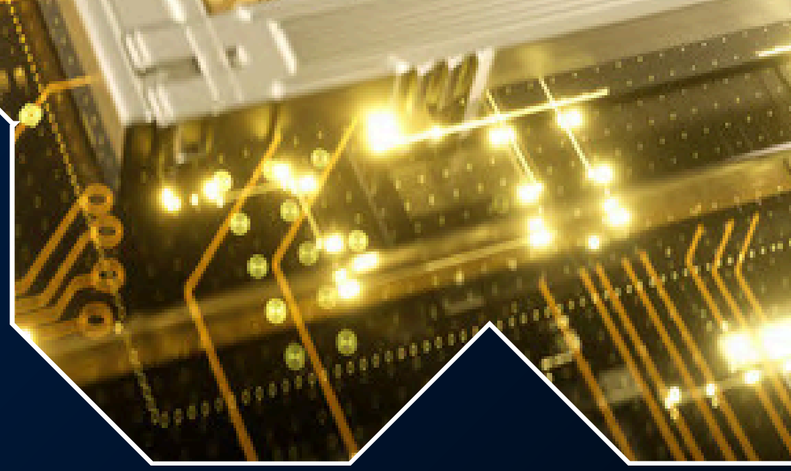




Govern & Identify (Value Protection)

- กำหนด Governance, Policy, Risk Appetite
- ระบุทรัพย์สินดิจิทัลและความสำคัญของข้อมูล

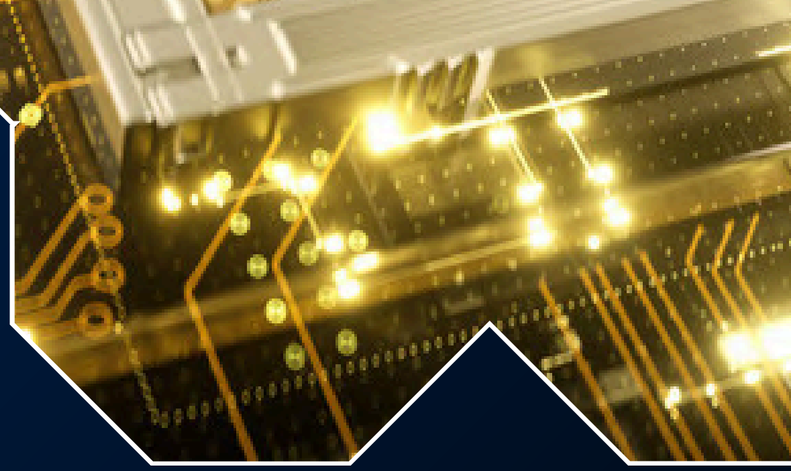
Govern (GV)	Organizational Context
	Risk Management Strategy
	Cybersecurity Supply Chain Risk Management
	Roles, Responsibilities, and Authorities
	Policies, Processes, and Procedures
	Oversight
Identify (ID)	Asset Management
	Risk Assessment
	Improvement



Protect
(Value Protection)

- วางมาตรการป้องกัน : Access Control, Awareness, Patch, Backup

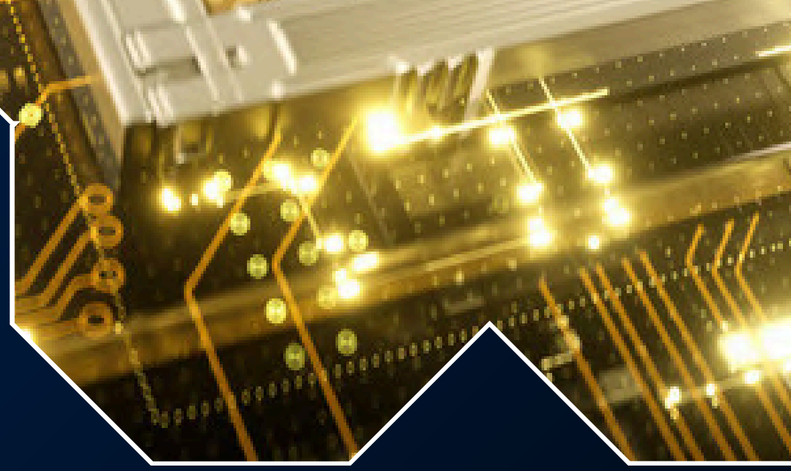
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience



Detect (Monitoring & Response Readiness)

- ใช้ข้อมูลภัยคุกคามและ SOC Dashboard เพื่อ “เห็นก่อน”

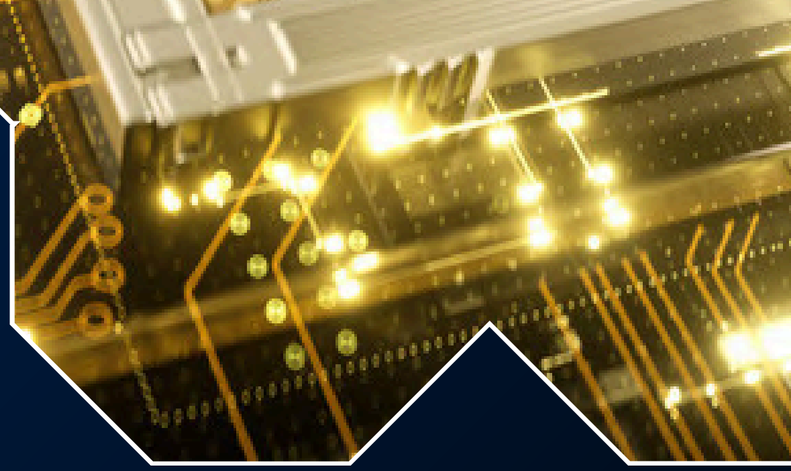
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis



Respond & Recover (Resilience in Action)

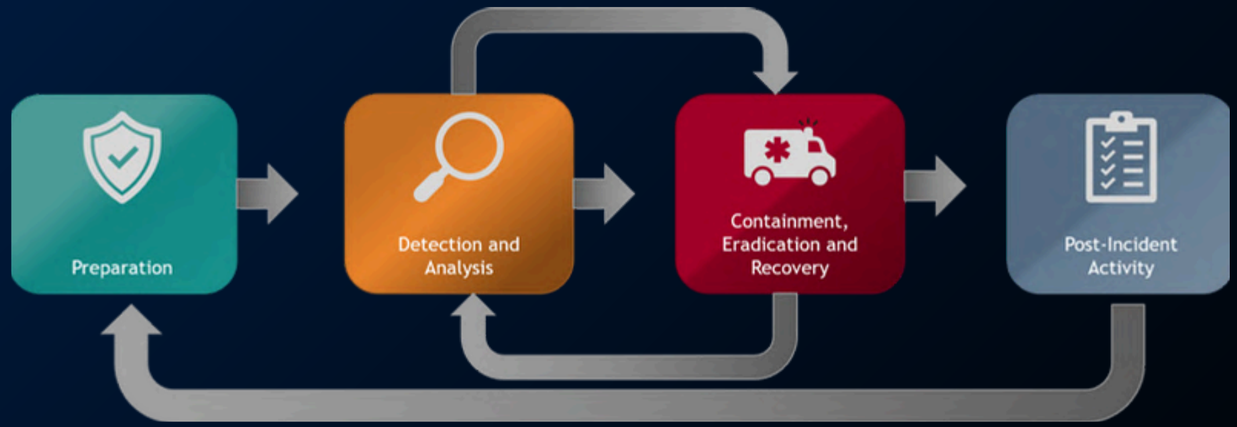
- กำหนดขั้นตอนรับมือเหตุการณ์ / ฟื้นฟูระบบ / สื่อสารกับผู้มีส่วนได้เสีย

Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover (RC)	Incident Recovery Plan Execution
	Incident Recovery Communication



Continuous Improvement

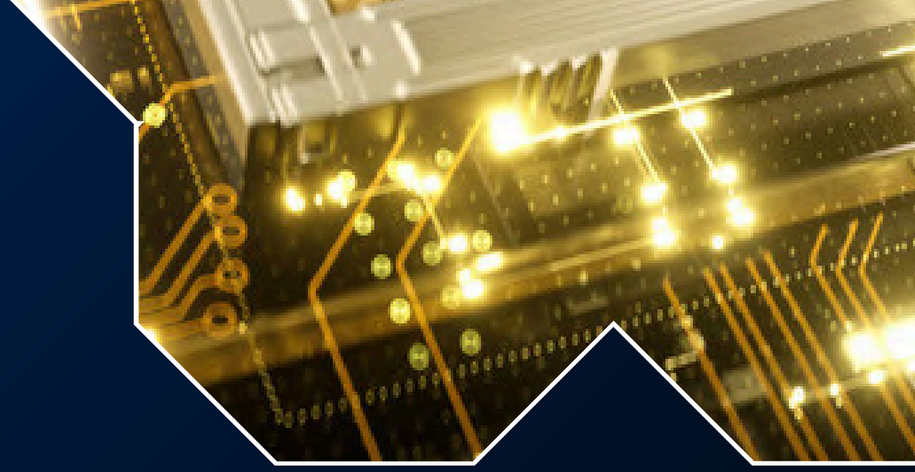
บทเรียนหลังเหตุการณ์ (Lesson Learned) ต้องถูกนำกลับมาปรับกระบวนการ



Part 4
Summary & Reflection



Board Oversight Checklist

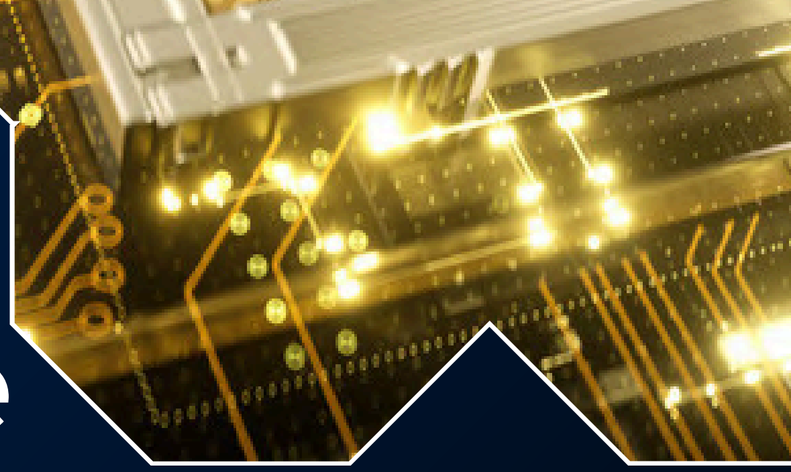


5 คำถามที่บอร์ดควรถามเกี่ยวกับความเสี่ยงเทคโนโลยี

1. เรารู้หรือไม่ว่า “อะไรคือทรัพย์สินดิจิทัลสำคัญ”?
2. ใครเป็นเจ้าของความเสี่ยงระบบนั้น
3. มีการทดสอบแผนกู้คืน (DR Test) บ่อยแค่ไหน?
4. รายงาน Cyber / IT Risk ส่งบอร์ดทุกกี่เดือน?
5. เราวัด “ความพร้อม” ด้วยตัวเลขอะไร?



From Risk to Resilience



“บอร์ดไม่จำเป็นต้องเป็นผู้เชี่ยวชาญเทคโนโลยี
แต่ต้องตั้งคำถามที่ถูกต้อง”



MYSURACHET.COM

Thank You

Thai Institute of Directors

Let’s Connect with Us!

www.MySurachet.com

Biz Card Contact

LINE

