KPMG

Managing technology and cyber risk for insurers - Time to act now

18 May 2021 | 2.00pm – 3.00pm

Housekeeping rules for Webex

Guide on Conf Call

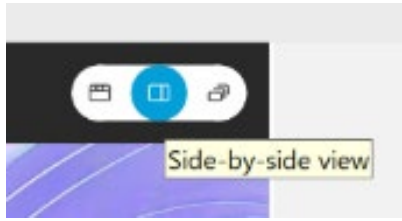
Your microphone is automatically mute.

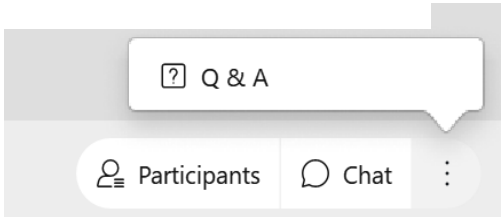
Put your questions in Q&A box or chat box.

Please note: this meeting will be recorded

Webex features

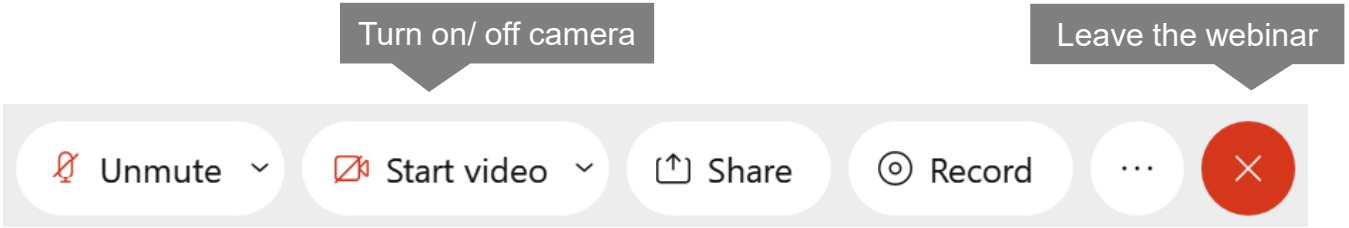
Select ‘Side-by-side view’ at the top right corner as the best viewing experience





Q&A box

Chat box



KPMG with You Today

Itthipat Limmaneerak
Partner, Advisory,
Insurance
KPMG in Thailand

Florian Magin
Partner, Advisory,
Technology Risk
KPMG in Thailand

Natchaon Sunthonlap
Manager, Advisory,
Technology Risk
KPMG in Thailand

Ronachai Laoharawee
Manager, Advisory,
Technology Risk
KPMG in Thailand

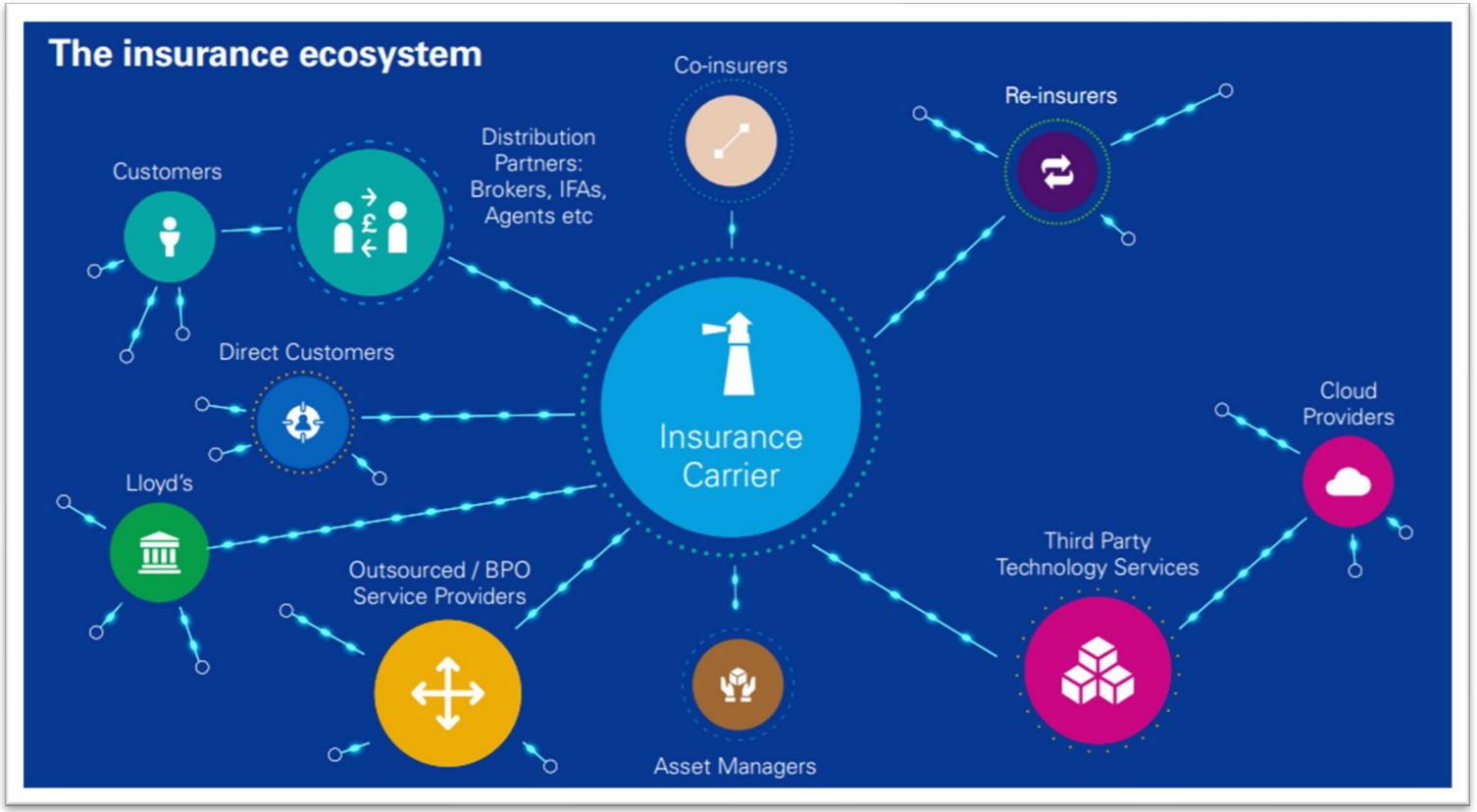
Insurers accelerate to shift their insurance business model to serve better on higher customer expectation and dynamic change post COVID

Three strategic shifts

01 Modular and tailored business models

02 Digital first ways of working

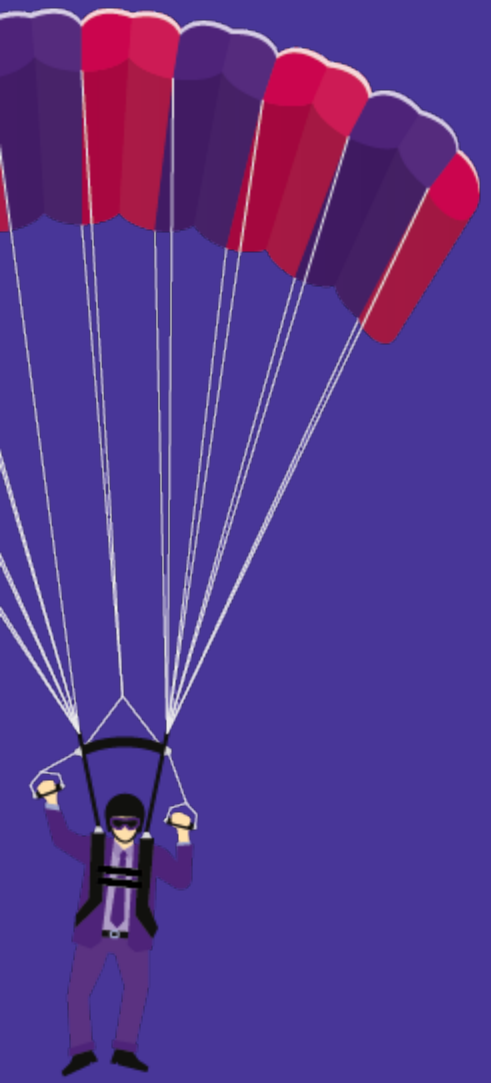
03 Affiliate embedded products & partnership



Reference: KPMG analysis

Digital technology shall be leveraged across the insurance value chain to drive efficiency and create value to customers

360-degree customer profile	Omni-channel management	Technology to support granular products offering	Big data technology
Blockchain technology	Internet-of-thing / 5G	Automated process and tools	AI / machine learning



Strong Digital Governance requires a joint effort across the three lines of defense

1st line readiness

- Business-IT alignment
- Program and project management
- Digitization and technology adoption / Cybersecurity

2nd line readiness

- Technology and cyber risk management framework
- Third party risk management
- Technology risk assessment

3rd line readiness

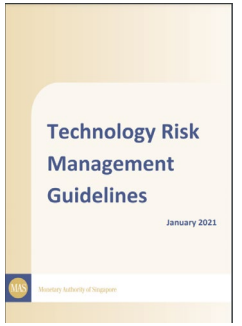
- Assurance on emerging technology solutions
- Digital audit capabilities

Regulatory requirements for technology and cyber risk management are evolving quickly

Bank of Thailand (BOT)
IT Risk Management
Implementation Guideline

Office of Insurance Commission (OIC)
IT Risk Management
Implementation Guideline

Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines



Common Domains

- IT Governance
- IT Security
- IT Risk Management
- Cyber Security
- Third Party Management
- IT Project Management
- IT Compliance
- IT Audit
- Reporting

IT Governance

Increased focus on the board of directors and senior management being able to understand and manage technology risk, including cyber risk

Board of Director

- ✓ Member must have IT knowledge or experience
- ✓ Receive sufficient training in IT and relevant risks

IT Steering Committee

- ✓ Responsible for IT management and oversight of IT operations

Risk Management Committee

- ✓ Oversight of IT risk management

Oversee that:

- ✓ The company uses IT that is appropriate to its business strategies
- ✓ There is IT risk management as part of the ERM
- ✓ IT risk management policy and security policy and are formulated
- ✓ Procedures are setting out
- ✓ There are the appropriate monitoring, auditing and reporting

OIC

IT security policy

(More detail in IT security topic)

IT risk management policy

(More detail in IT risk management topic)

IT Risk Management

IT Risk policy

Should cover the following:

- ✓ IT risk governance structure
- ✓ Roles and Responsibilities
- ✓ IT risk management process
- ✓ IT risk appetite
- ✓ IT risk assessment criteria
- ✓ Methodology or tools
- ✓ IT risk indicator
- ✓ Risk reporting

OIC

- ✓ IT risk policy must be approved by BOD, or designated committee and communicated
- ✓ IT risk policy must be reviewed at least once a year and when there is any significant change

- IT risk definition and scope ✓
- IT risk assessment criteria ✓
- IT risk appetite ✓
- Risk assessment ✓
- Risk treatment ✓
- Risk monitoring and review ✓
- Risk reporting ✓

IT Security

- ✓ IT security policy must be approved by BOD, or designated committee
- ✓ IT security policy must be reviewed at least once a year and when there is any significant change

OIC

IT security policy

At least consist of the following topics:

- ✓ IT asset management
- ✓ Access control
- ✓ physical and environmental security
- ✓ IT operations security
- ✓ IT continuity
- ✓ Cybersecurity

- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Network and communication security
- Third party management
- IT operations security
- IT incident management
- System acquisition and dev.
- IT continuity planning

Evolving area of regulatory focus

Cyber Security

Cyber security governance, cyber risk management and cyber resilience must be set out to manage the risk from the cyber attack, commensurate with the nature of business, volume of transactions, complexity of IT and relevant risks.

Impact Consideration

- Confidentiality
- Integrity
- Availability
- Law & regulation

Cyber Security Governance

Cyber Risk Management

Cyber Resilience

Protection
- ✓ Security controls
- ✓ Security procedures
- ✓ Information gathering

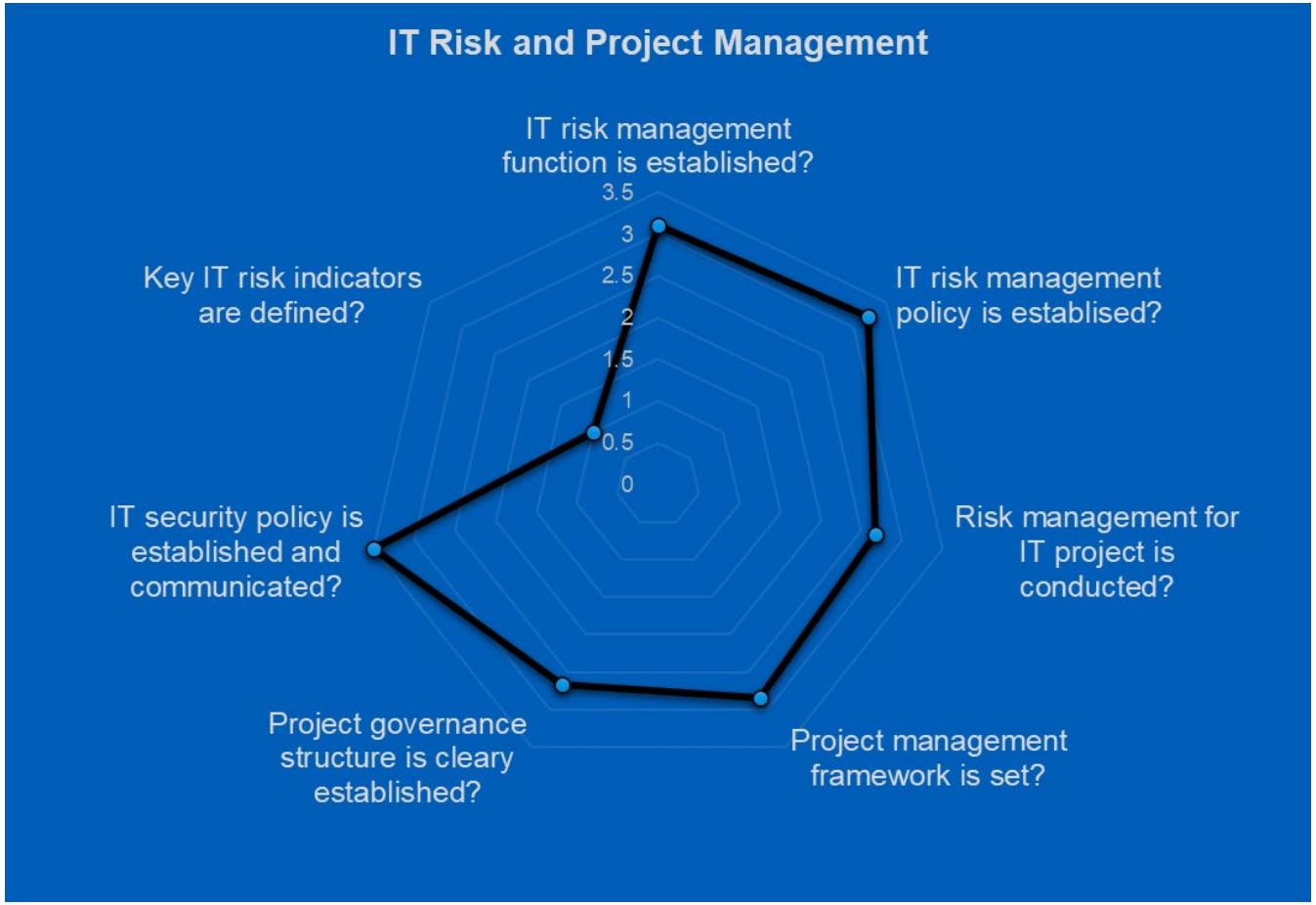
Detection
- ✓ Reporting channel
- ✓ Monitor and alert

Response
- ✓ Incident response
- ✓ Testing
- ✓ Communication

Recovery
- ✓ Recovery plan
- ✓ Recovery communication

Evolving area of regulatory focus

Insight on technology and cyber risk readiness in the Thailand-insurance sector

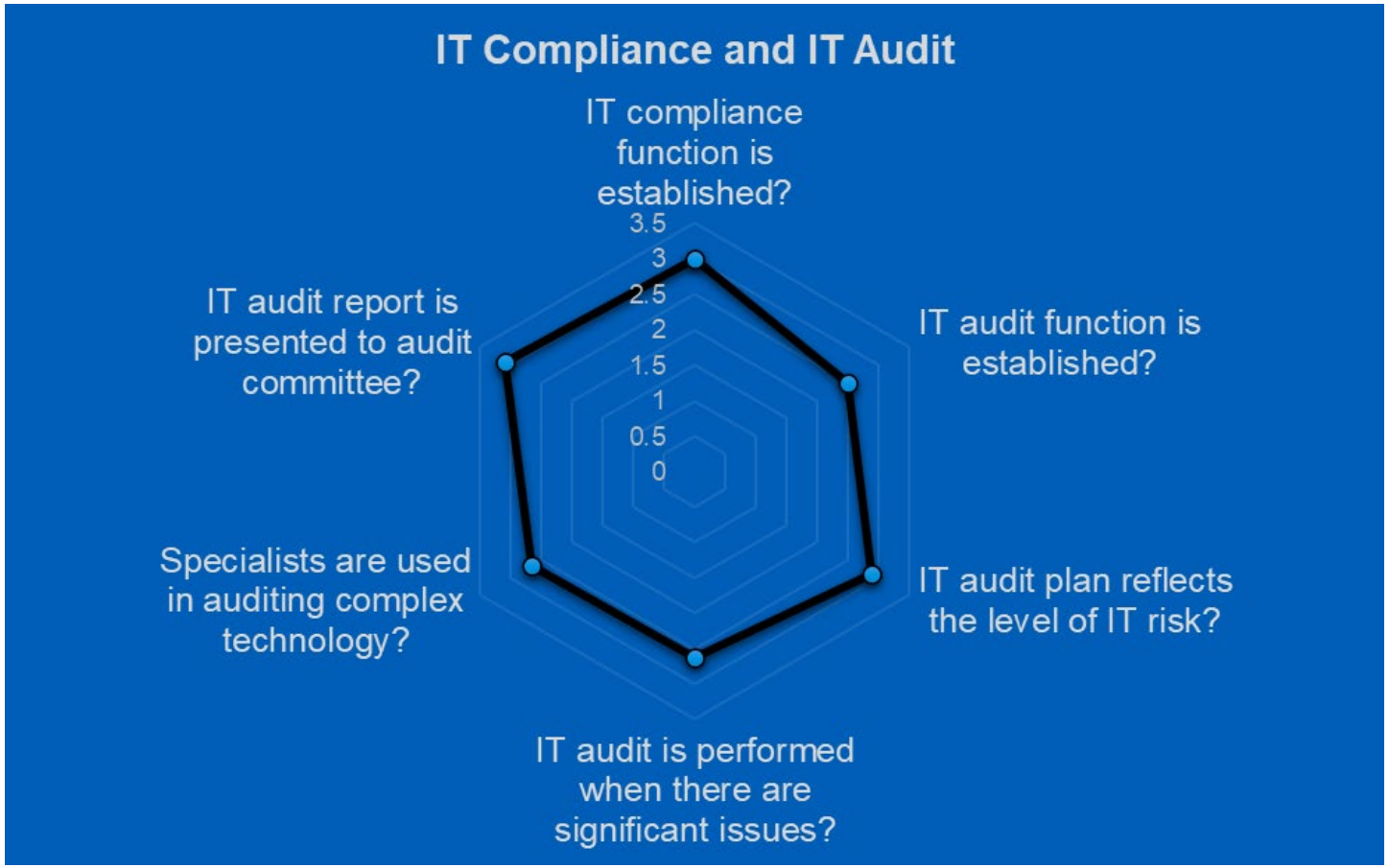


Key Observation

- IT risk management function and policy are established but the implementation of IT risk management is a silo
- Risk assessments are performed in some projects but not in a consistent and standardized way.
- Specific IT KRIs are not defined to monitor the Key IT risks

Based on a survey of 12 insurance companies in Thailand

Insight on technology and cyber risk readiness in the Thailand-insurance sector

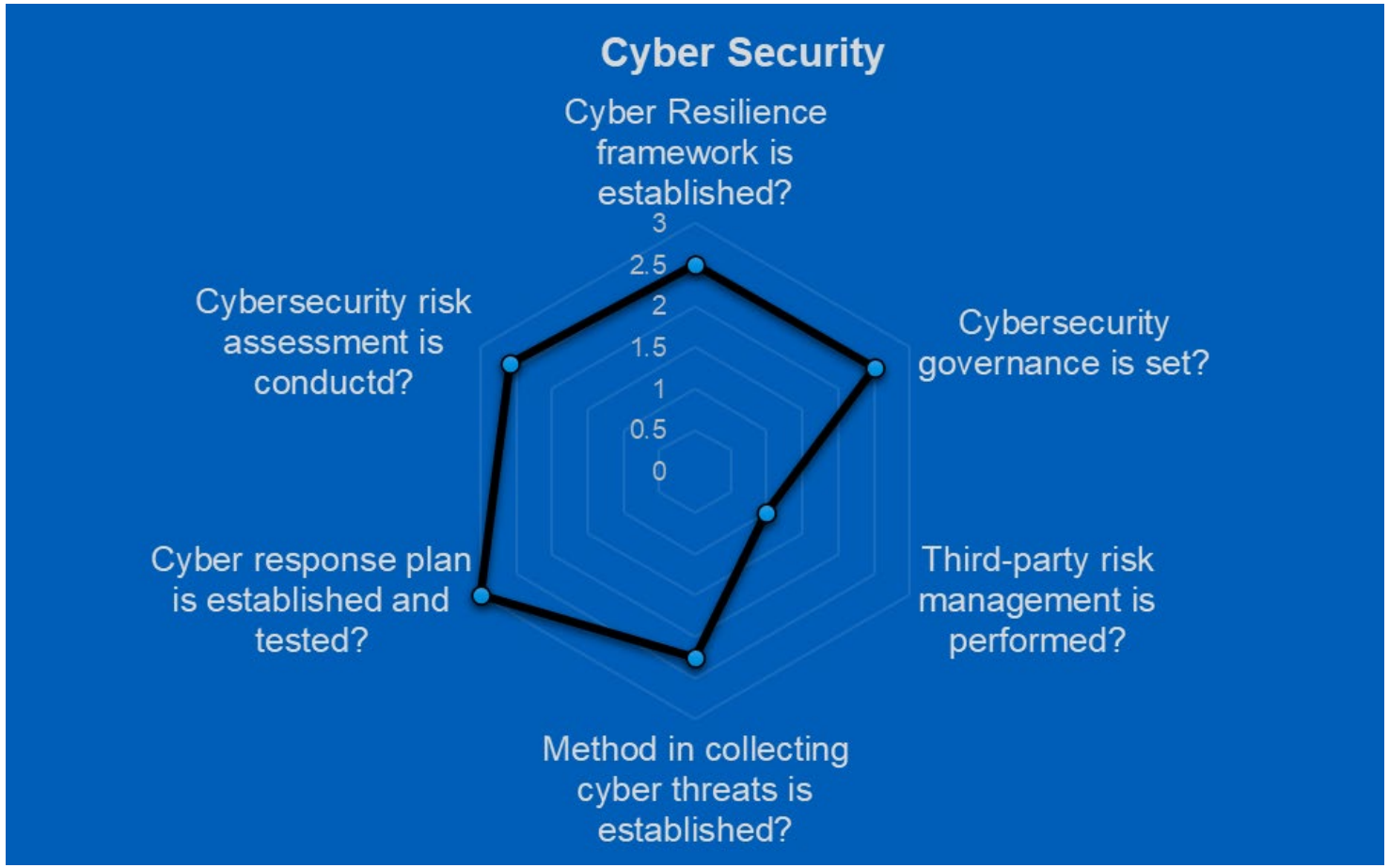


Based on a survey of 12 insurance companies in Thailand

Key Observation

- The supervision of IT compliance is established but operates as a silo
- Auditor has knowledge and experience in IT and the audit plan reflects the level of IT risk and reporting to the audit committee is performed regularly
- Some significant issues/changes are in the audit scope and plan and external auditor (specialists) are used in some case of new or complex technology.

Insight on technology and cyber risk readiness in the Thailand-insurance sector



Based on a survey of 12 insurance companies in Thailand

Key Observation

- Cyber security governance and the cyber security framework are not formally established.
- Cyber security risk assessment is conducted but not consistently.
- Supply chain and third-party risk management is not performed systematically.
- There is no clear method to collect and analyze cyber threat information and collaboration and exchange of such information about cyber threats is limited.
- The cyber response plan, emergency plan are established but not tested or reviewed regularly.

Key takeaways on current state of technology and cyber risk management in the insurance sector

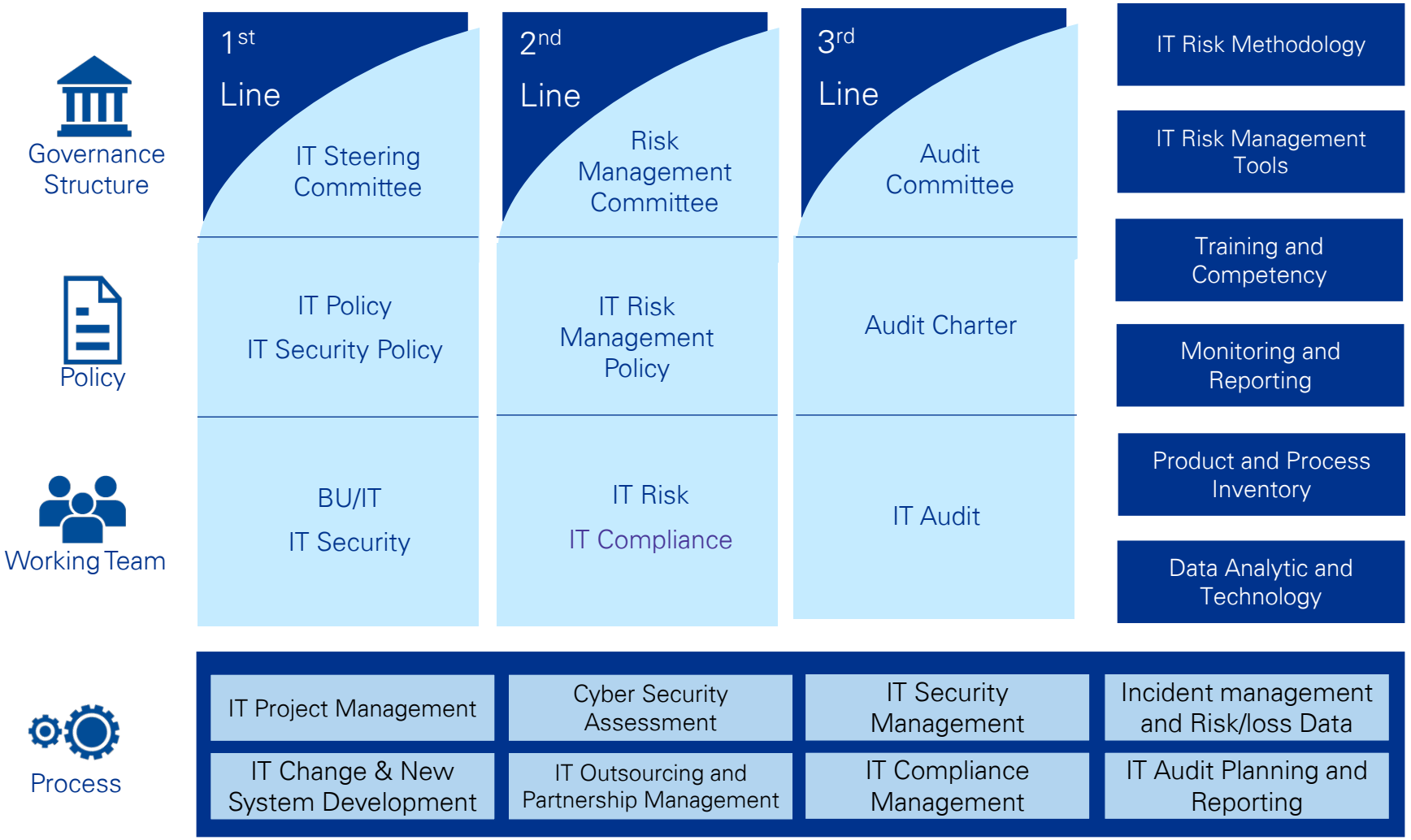
Governance structure for IT risk management is established, while governance of cyber security and projects requires improvement

IT risk and IT security policy are established and communicated to related parties

IT risk and cyber practices are performed inconsistently and with incomplete coverage of relevant risks

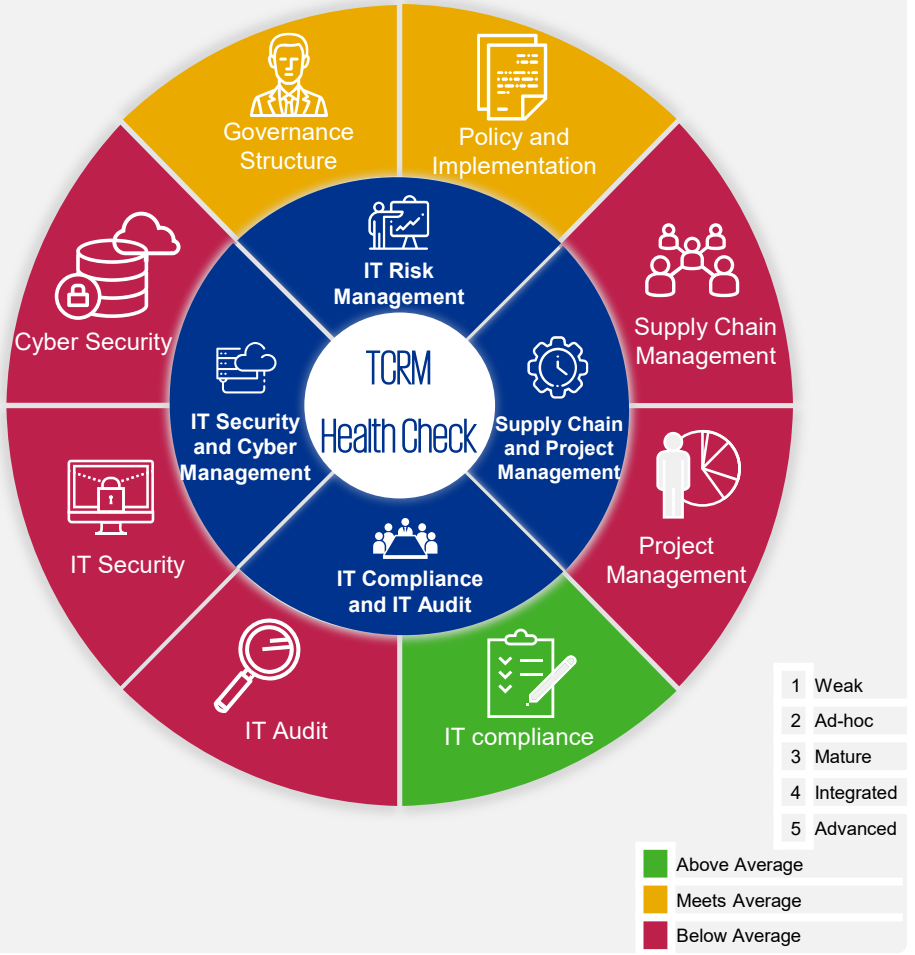
IT compliance and IT audit roles are established, but their focus areas are not always aligned with the key IT risks

Implications for the three lines of defense

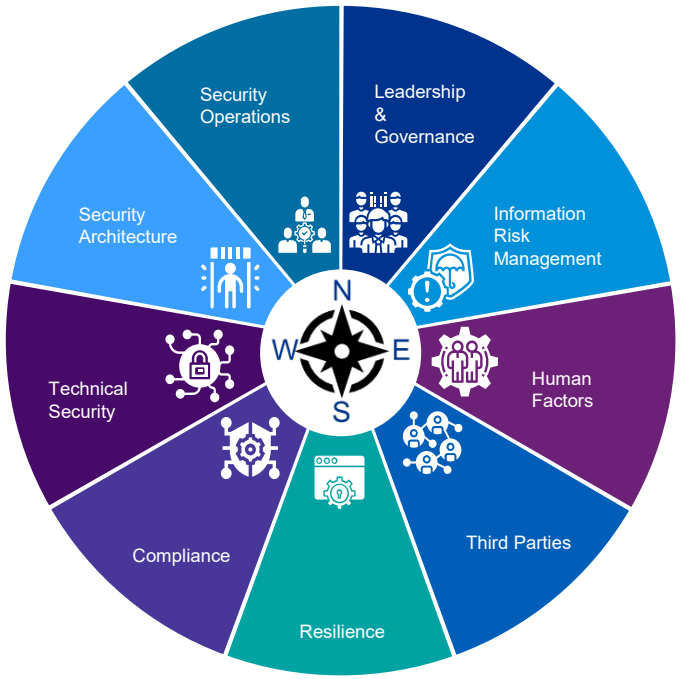


Illustrative TCRM health check to discover current state

	Current State	Sector Benchmark	
IT Risk Management	3.00	3.00	IT risk management structure is setup in accordance with the three lines of defense?
	3.00	3.00	IT risk management policy is established and communicated?
Supply Chain and Project Management	2.50	3.00	Risk management for IT projects is conducted? (considering risk, priority of projects, project management framework, and project oversight)
	2.50	3.00	Project governance structure and framework is established to ensure that the project can be delivered as planned?
	2.50	3.00	Supply chain risk management and third-party service provider management is performed?
IT Security and Cyber Management	3.00	4.00	IT security policy is established and communicated?
	2.50	3.00	Cybersecurity governance and framework is established?
	2.00	3.00	Method in collecting and analyzing cyber threats information, as well as method and channel for exchanging information are established?
	2.00	3.00	Cyber incident response plan, emergency plan are established, tested and presented to board of directors or relevant committee?
IT Compliance and IT Audit	3.00	2.00	The supervision of IT compliance is set?
	3.00	3.00	Auditors who have specialist knowledge, experience, and competence perform IT audits?
	2.00	3.00	IT audit plan and scope reflect the level of IT risks?



Set course for enhancing technology and cyber risk management capabilities across the three lines of defense



START

1

Maturity and Gap Assessment

Current state assessment, future state definition, roadmap development

2

Security, Risk and Assurance Transformation

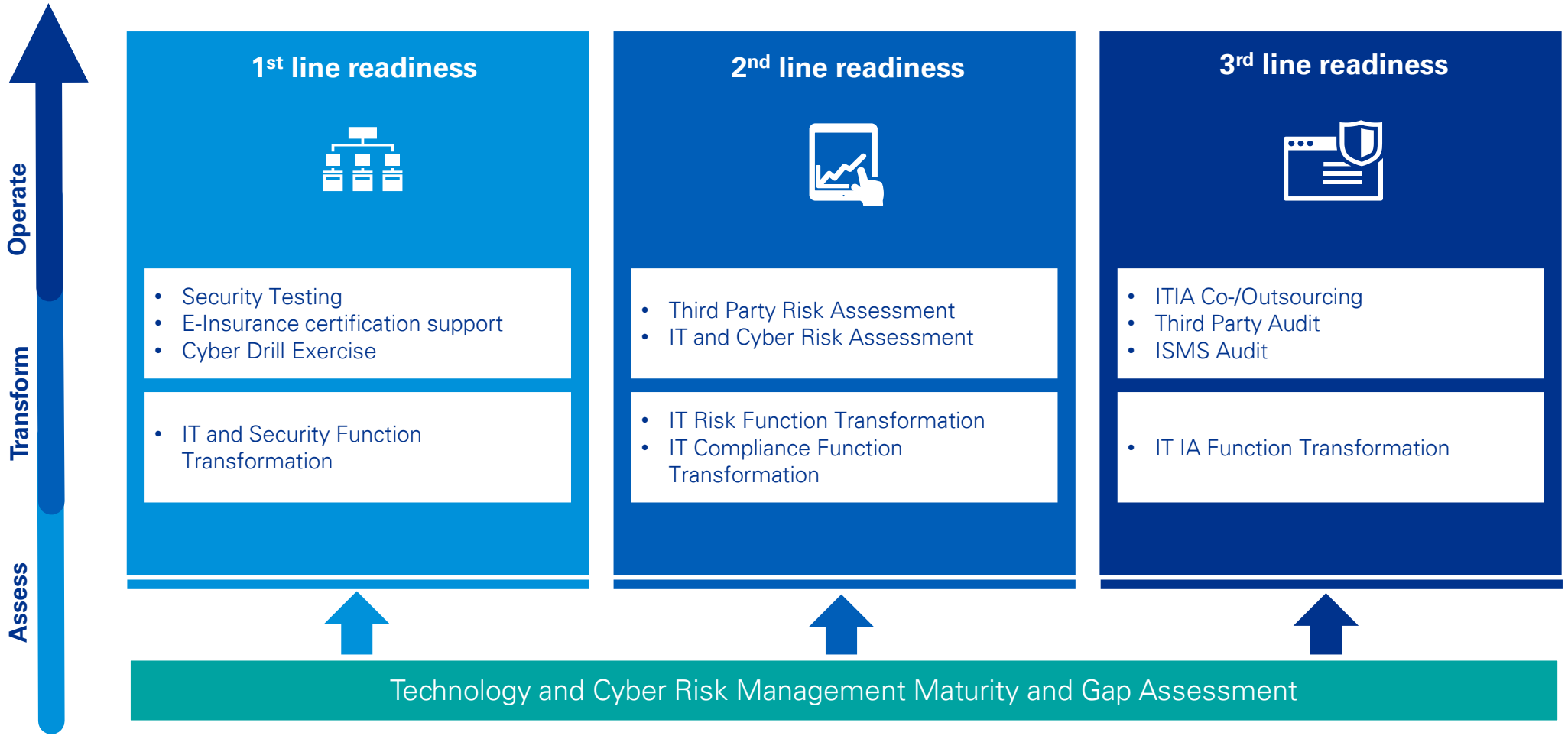
Remediation of maturity gaps, TOM enhancement and capability uplift

3

Continuous delivery and improvement

Transition into BAU and monitor maturity levels

KPMG will support you based on your needs, end to end or focused



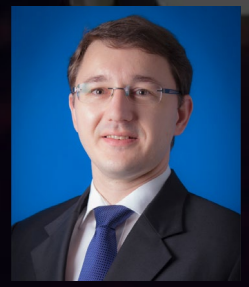
TCRM health check

Event feedback

Thank you

Contact

Itthipat Limmaneerak
Partner, Advisory, Insurance
Email: itthipat@kpmg.co.th



Florian Magin
Partner, Advisory, Technology Risk
Email: florianmagin@kpmg.co.th

Natchaon Sunthonlap
Manager, Technology Risk
natchaon@kpmg.co.th

Ronachai Laoharawee
Manager, Technology Risk
Email: ronachai@kpmg.co.th

KPMG Phoomchai Business Advisory Ltd.
48th Floor, Empire Tower
1 South Sathorn, Yannawa
Bangkok, Thailand
Phone: (66) 2677 2000
Fax: (66) 2677 2222

home.kpmg/th

Twitter: @KPMG_TH
LinkedIn: linkedin.com/company/kpmg-thailand
Facebook: facebook.com/KPMGinThailand
YouTube: youtube.com/kpmginthailand
Instagram: instagram.com/kpmgthailand/