Anticipate Tomorrow

Cybersecurity Control Effectiveness

Introduction

Across industries, companies are trying to quickly leverage new technologies and digitize processes to improve value, productivity, cost and competitive advantage. But as they create new digital channels, business models, remote working capabilities, markets and customer experiences, companies are processing more data in a fast-changing environment, which increases their cyber risk. This risk is keeping many companies from advancing their strategic agenda or launching initiatives quickly.

The universal challenge

Technology makes many things possible, but possible doesn't always mean safe.

Cyber risks are the new reality:

- Does your organization have the confidence and agility to seize these kinds of opportunities, or are cyber threats and regulations holding you back?
- Can you do what you want to do, knowing you have the resilience to withstand a cybersecurity event and continue to serve customers?
- As you exchange more data and become more dependent on interconnected systems, a strategic approach to cybersecurity has never been more critical. Your organization's ability to make brave, agile decisions depends on it.

Use cybersecurity to protect your future:

- As technology becomes essential for meeting the needs of customers, employees, suppliers and other stakeholders, an organization's cybersecurity must build both resilience and trust.
- That is, in addition to protecting your mission-critical assets and ensuring business continuity after a cyber-attack, how can you protect the data that stakeholders entrust to you?
- With cybersecurity and trusted systems, you can protect your future and expand your possibilities.

Where to start?

A natural starting point is to align the cybersecurity strategy with business objectives, adapt to changes in business strategy and to bring assurance and efficiency to their overall cybersecurity management. To achieve this an understanding of the design and operating effectiveness of your existing implemented controls are the first step.

Design Effectiveness:

- Is to measure effectiveness of control design and documentation in order to be implemented sustainably.
- Process focused.
- Risk based design.

Operating Effectiveness:

- To measure the effectiveness of meeting the control objectives post control implementation in accordance with the design.
- People and Technology focused.
- Risk reduction effectiveness.

How can KPMG help?

Cyber Maturity Assessment (CMA):

- Assessment of the maturity of six key dimensions to provide a comprehensive and in-depth view of an organization's cyber maturity.
- Based on international cybersecurity frameworks (NIST; ISO27001, SANS Top 20, etc.).
- Risk based approach.
- Control improvement recommendations.

Scenario Based Control Testing (RED Team):

- Control operating effectiveness validation for People, Process and Technology.
- Mean time to Detect and Respond to emerging threats aligned to industry threat intelligence.
- Technical Playbooks to track and monitor relevant logs in your technology environment.
- Recommendations aligned to strategic initiatives to enhance cybersecurity control implementation and operating effectiveness by improving existing procedures.

At KPMG, we provide an in-depth review of an organization's ability to protect its information assets and its preparedness against a cyber-attack. It is unique in the market in that it looks beyond pure technical preparedness against cyber-attack. It takes a rounded view of people, process and technology, enabling clients to identify critical assets, understand areas of vulnerability, and prioritize areas for remediation, turning information risk to business advantage.

As leading advisors and providers of cybersecurity, KPMG can enable you to:

Anticipate tomorrow…

Confidently seize opportunities – so you know you're protected.

Move faster…

Accelerate your initiatives in an agile world.

And get an edge.

Use cyber security to achieve competitive advantage.

To get an overview of cyber risks in your organization and obtain a proof of concept, call **+603 7721 3388** or reach out to KPMG's cybersecurity professionals below:

Alvin Gan
Head of Technology Consulting &
Executive Director
E : alvingan@kpmg.com.my

Jaco Benadie
Executive Director
Emerging Technology Risk & Cyber
E : jacobenadie@kpmg.com.my

Qadiri, Ubaid Mustafa
Executive Director
Emerging Technology Risk & Cyber
E : ubaidqadiri@kpmg.com.my

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

www.kpmg.com.my/cybersecurity