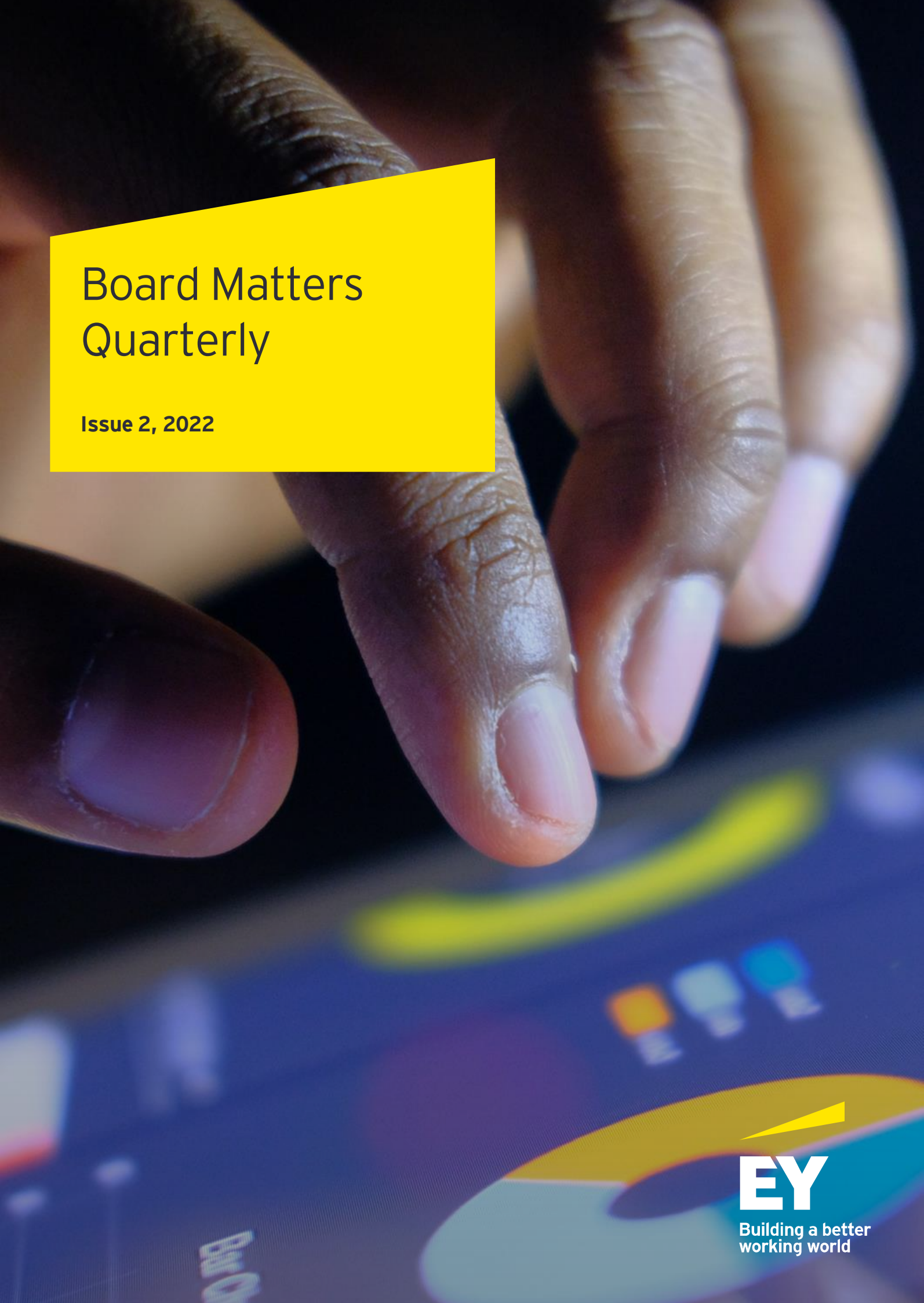

Board Matters Quarterly

Issue 2, 2022

EY
Building a better working world

Issue 2, 2022

Board Matters Quarterly

Board Matters Quarterly offers thought-provoking perspectives and insights into leadership and governance issues for boards and audit committees, supporting them to navigate the increasingly complex business environment.

1

Why tax governance is now a business imperative

2

How organizations can augment their security initiatives with zero trust

Why tax governance is now a business imperative

In the era of tax transparency, with increasing global collaboration and the exchange of information among tax authorities, having good tax governance is vital to any business operation. In fact, many countries have introduced tax governance in their taxation systems to ensure companies follow a set of processes and procedures, that will result in adherence to the stipulated tax rules and requirements.

In Malaysia, the Inland Revenue Board (IRB) introduced the Tax Corporate Governance Framework (TCGF) and Guidelines dated 11 April 2022 to assist companies in designing and operating their tax governance frameworks. Malaysian companies are encouraged to voluntarily participate in the TCGF program to enhance the robustness of their overall corporate governance framework, promote voluntary compliance and minimize tax risks. Taxpayers who participate in the TCGF program will enjoy reduced scrutiny (e.g., fewer tax audits), expedited tax refunds and the appointment of a dedicated tax officer at the IRB as a single point of contact in relation to the taxpayer's tax matters.

Countries, such as Japan and Australia, have a tax governance framework and guidance in place. For example, the Australia Taxation Office (ATO) has established a tax governance benchmark through its Justified Trust Program. In this program, the tax governance of a company is reviewed formally, with greater accountability placed on the board and management team in managing the organization's tax risk. In February 2022, the Singapore tax authorities published its tax governance and tax risk management initiatives to promote the adoption of good tax governance principles and practices among large companies. Subsequently, in March 2022, the Singapore tax authorities introduced the Tax Governance Framework (TGF) and Tax Risk Management and Control Framework for Corporate Income Tax (CTRM) to strengthen tax compliance by large companies.

Good tax governance will help companies:

i. Enhance compliance with tax rules and regulations

Tax rules and regulations change frequently, which means keeping abreast with the latest revisions can continue to be a challenge. A tax governance framework will, therefore, help companies have a formalized structure to prepare for the ever-changing developments in the rules and regulations, allowing them to readily apply the rules to the business transactions as they happen.

Today's digital age means that businesses need to transform their models to stay relevant and competitive. The regulatory environment is also constantly evolving, to stay ahead of the disruptions in the business landscape. Unsurprisingly, there is pressure for businesses to keep up with the rapid changes, capture accurate and relevant data, and ensure the correct treatment is being adopted in their tax computations and in meeting their tax obligations.

ii. Build stakeholder confidence

Successfully managing stakeholders' expectations and building their confidence are key. A tax governance framework enables companies to build the right infrastructure that supports effective risk management and tax decision-making, and ultimately, voluntary compliance. By ensuring the operational effectiveness of their tax governance framework and key internal controls, companies can address their disclosures on tax risk management, and at the same time, demonstrate the sustainability of their business from an ESG (environmental, social and governance) standpoint in their stakeholder communications.

iii. Manage tax risks effectively

Failure to manage tax risks can give rise to legal, as well as financial and reputational risks. A tax governance framework helps companies identify and understand key tax risk areas, including the tax authorities' potential focus areas. By having a good grasp of the tax requirements, companies can better manage the tax risks upfront. At the same time, mitigation actions can be developed and implemented proactively as business transactions happen and as business structures are put in place, rather than during a tax audit.

The tax governance framework will provide boards and senior management enhanced oversight of their tax risks and strategy. With a more comprehensive overview, boards and senior management teams can ask the right questions and obtain the right information to make key business decisions.

iv. Have open, honest engagements with tax authorities

When engaging the tax authorities, having good internal tax governance will ensure effective interactions and clarity in dealing with business transactions. It is important for the taxpayers and the tax authorities to work towards improving tax compliance together, in a transparent and honest manner. This will result in companies meeting their tax obligations and reduce margins of error – a win-win outcome.

v. Reduce compliance costs

An effective tax governance framework can effectively reduce future tax compliance costs. This can be in the form of more efficient processes, better certainty on tax positions, improved tax risk mitigation and a reduction in compliance activities. This means, the manpower time dedicated to compliance activities can then be channeled to more value-adding business activities.

By integrating the necessary internal controls and strategic review mechanisms into the tax governance framework, companies will be able to better gauge the effectiveness of their tax risk management and avoid unnecessary tax costs in the long run.

Conclusion

The complex and ever-evolving business and regulatory environment, coupled with enhanced stakeholder scrutiny and expectations, reinforce the heightened focus on and the importance of good tax governance for businesses. It is vital that businesses demonstrate to all stakeholders a visible and robust tax governance framework, to minimize the financial, regulatory and reputational risks, today and beyond.

Author

Farah Rosley
Malaysia Tax Managing Partner,
Ernst & Young Tax Consultants Sdn. Bhd.

How organizations can augment their security initiatives with zero trust

Modern businesses have been renewed by the pandemic. The move to remote and hybrid work has necessitated organizations to accelerate their digital transformations to convert an office-centric workplace into a complete homeworking space almost overnight.

Digital technologies, software-as-a-service (SaaS) and cloud computing were the enablers in altering workspaces to ensure businesses survive in a challenging environment. As the Internet of Things (IoT) expanded to accommodate and provide seamless processes in our lives and in the jobs we do, IT systems became relatively complex. This has inadvertently paved the way for vulnerabilities to sophisticated threats of cybercrimes in the digital sphere.

According to the *Digital Crimes Unit of Microsoft Asia 2019*, around 720 people fell prey to cyber criminals across the globe every minute – translating to one million victims every day. In 2018, the Royal Malaysia Police dealt with 10,742 cybercrime cases with an estimated loss amounting to RM400 million. The total number of cases increased to 11,875 in the following year with an estimated loss of RM500 million.

2018	2019
10,742	11,875
Total cybercrime cases	Total cybercrime cases
RM397,944,265	RM497,719,498
Estimated loss	Estimated loss

Source: Royal Malaysian Police

With the rise of hybrid and remote work, the continuous shift to cloud servicing, the growth in the adoption of mobile devices and an onslaught of cyber-attacks that could potentially damage supply chains, zero trust is set to take center stage in the world of cybersecurity.

Never trust, always verify

Organizations have never been faced with as many challenges in protecting their data resources, and never was there a need to be more suspicious of users and devices accessing their networks. The zero-trust model, in layman's terms, means trusting no one even when connected to a permissioned network.

For organizations, there is too much at stake to trust anyone or anything outside their entity. The most notable effect of the shift to zero trust is the realization that traditional virtual private networks (VPNs) are no longer fully capable of securing remote access to corporate networks.

When the COVID-19 pandemic hit, the work-from-home concept became inevitable. Organizations relied on VPNs to support their distributed workforces – with results that fell short of expectations. VPNs may not be ideal to provide completely secure access for many users relying on devices that, in many instances, are not as secure as they could or should be.

As such, VPNs will not provide the sufficient defense mechanism against threats. Companies with a sizeable hybrid workforce will need to support a significant volume of VPNs, which will trickle the burden to the IT or cybersecurity team to manage and maintain.

Zeroing on trust

There is no silver bullet when it comes to adopting zero trust. Zero trust is a framework that requires focus on people, process, and technology aspects to be effective. It drives a change in how cybersecurity is managed to strengthen the organizations' cybersecurity posture.

It begs the question – where should organizations start this journey? The emphasis is on the journey and any journey starts with the first step followed by others.

The most effective approach is to adopt zero trust using a piecemeal and not 'big-bang' approach. Focus on the most critical and sensitive data first – the data that is if compromised, lost, or exposed will have a detrimental impact on the organization. Where is this data hosted? Who has access to this data? What is the business justification for needing access to it? Start the adoption at this point and build it out over time.

Don't underestimate the impact of culture. It is better not to call it zero trust as it is a nomenclature that is widely misinterpreted as a solution used when organizations do not trust their employees. This is of course opposite to the objective. It indicates that we do not trust our internal IT network.

See the adoption of zero trust as an opportunity to engage and collaborate with stakeholders. Build internal relationships to protect business data assets to provide access more efficiently to data that is needed by the right people at the right time to drive the business forward.

Zero trust is about eliminating dangerous trust assumptions of a technical nature in security architecture and establishing a singular security strategy to support the business.

> VPNs will not provide sufficient defense mechanism against threats. Companies with a sizeable hybrid workforce will need to support a significant volume of VPNs, which will trickle the burden to the IT or cybersecurity team to manage and maintain.

Six foundational assumptions of the zero trust model

1 The network is always assumed to be hostile, and all communication is secured regardless of the network location.

2 External and internal threats exist on the network and network locality is not sufficient for deciding trust in a network. Any person or device cannot be trusted just because they are part of the company with the assumption that the person is already dealing with both outside adversaries and malicious insiders.

3 All data sources and computing services are considered resources that need to be protected.

4 Every device, user, network, and data flow are authenticated and authorized. The former means positive confirmation that an entity is who or what they say they are. The latter means the entity has the need, rights, and reasons to do what they're doing.

5 Any access to resources is granted on a per-session basis.

6 All security policies are dynamic and incorporate as many sources of contextual data as possible.

The zero trust approach is most effective when it's extended throughout the entire digital landscape and used as an integrated security strategy. This is done by implementing zero trust controls and technologies across six foundational elements:

People

Applications and services

Networks

Devices

Infrastructure

Data

In a nutshell, zero trust is a new model and general philosophy around cybersecurity. It is an approach that more effectively adapts to the complexity of the modern environment, embraces the mobile workforce; and protects people, devices, applications, and data wherever they are located.

Questions for organizations to consider

One of the conundrums faced by organizations to establish zero trust model is whether it can be implemented fully. Because zero trust is not just a product, but a framework or an architecture that can take many forms, here are some questions to consider:

1. How can I leverage my existing cybersecurity infrastructure in the transition to adopt zero trust?
2. What are the business goals that I could achieve through the adoption of zero trust?
3. How do I plan to manage identity and apply it to the security controls across my network?
4. How will the zero trust vendor give emphasis on what data needs to be prioritized and managed continuously?
5. How should granular access to individual users be given?
6. What is the breach notification and back-up plan if the platform goes down?

Author

Jaco Benadie
Partner,
Ernst & Young Consulting Sdn. Bhd.

Contacts

Dato' Abdul Rauf Rashid
Malaysia Managing Partner,
Ernst & Young PLT

Tel: +603 7495 8728
abdul-rauf.rashid@my.ey.com

Ong Chee Wai
Malaysia Assurance Managing Partner,
Ernst & Young PLT

Tel: +603 7495 8776
chee-wai.ong@my.ey.com

Farah Rosley
Malaysia Tax Managing Partner,
Ernst & Young Tax Consultants Sdn. Bhd.

Tel: +603 7495 8254
farah.rosley@my.ey.com

Preman Menon
Malaysia Strategy and Transactions Leader,
Ernst & Young PLT

Tel: +603 7495 7811
preman.menon@my.ey.com

Chow Sang Hoe
EY Asean Consulting Leader
Malaysia Consulting Managing Partner,
Ernst & Young Consulting Sdn. Bhd.

Tel: +603 7495 8696
sang-hoe.chow@my.ey.com

Ismed Darwis
Malaysia Markets Leader
Ernst & Young PLT

Tel: +603 7495 8749
ismed.darwis@my.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

APAC no. 07009004
ED None

ey.com/my