IIA Malaysia e-techline
December 2019 Issue 05/19

BURSA MALAYSIA AMENDS MAIN AND ACE MARKET LISTING REQUIREMENTS IN RELATION TO ANTI-CORRUPTION MEASURES

In an effort to enhance the quality and integrity of listed issuers on Bursa Malaysia Berhad ("Bursa Malaysia" or the "Exchange"), the Exchange has amended the Main and ACE Market Listing Requirements (collectively "Listing Requirements") to encapsulate anti-corruption measures ("**Anti-Corruption Amendments**") in support of the National Anti-Corruption Plan 2019-2023.

To take effect on 1 June 2020, the Anti-Corruption Amendments will require listed issuers to establish and implement policies and procedures to prevent corrupt practices, thereby providing them with a measure of assurance and defence against corporate liability for corruption under section 17A of the Malaysian Anti-Corruption Commission Act 2009.

Datuk Muhamad Umar Swift, Chief Executive Officer of Bursa Malaysia said, "Given the serious threat that corruption poses to corporates and the economy, Bursa Malaysia is supporting government's battle against corruption by amending the Listing Requirements to encapsulate anti-corruption measures which are in addition to the statutory provisions under the law. The amendments will not only promote better governance culture and ethical behaviour within the listed issuer group, but will also provide greater accountability and transparency to investors."

The Anti-Corruption Amendments include the following:

(a) Requiring a listed issuer and its board of directors to ensure that –

(i) the policies and procedures on anti-corruption and whistle-blowing are established and maintained for the listed issuer and its subsidiaries ("group");

(ii) such policies and procedures are reviewed periodically to assess their effectiveness, and in any event, at least once every 3 years; and

(iii) corruption risk is included in the annual risk assessment of the group; and

(b) Requiring a listed issuer to publish anti-corruption policy as well as whistle-blowing policy and procedures on its website.

Reference:

For further information, please visit Bursa Malaysia's website at www.bursamalaysia.com.

TONE AT THE TOP – THE GOVERNANCE BENCHMARK

There is a significant disconnect between our assessments of governance and true governance effectiveness. It is time to determine why our governance evaluations are often wrong and what we can do to fix the problem.

1. The Measurement Challenge.

It is difficult to measure corporate governance. It encompasses all the systems by which organisations are directed and controlled, and some of those systems are difficult to quantify. Governance is more than policies and procedures. It's about how we make decisions, establish objectives, and monitor their achievement.

2. Ranking our Governance: Success or Failure?

The lesson from Enron is that doing well on subjective scoring does not guarantee sound corporate governance or continued success. According to a 2018 report published in Queen's Law Journal, "When the empirical research is examined, there appears to be no relationship between corporate governance scores or ranking schemes and future corporate performance. These schemes also fail to identify companies that are likely to experience scandals or even terminate underperforming executives.

The answer is not to stop benchmarking corporate governance. Running a business without performance measurement means trying to run a business blind to the facts. Instead, it is time to determine why our governance assessments are often wrong and what we can do to fix the problem.

3. Why Governance Rating Systems Fail?

Publicly available governance scores are determined primarily by comparing governance disclosures to a well-known code of governance. At first glance, this approach makes sense, but there are several reasons why it may be prone to failure.

First, the information gleaned from governance disclosures is incomplete. Second, governance disclosures describe specific governance characteristics, but they do not shed much light on governance effectiveness. To make matters worse, many assessments simply compare disclosures to a well-known code of governance. Governance codes are vitally important for establishing minimum expectations, but it's impossible to achieve world-class governance merely by complying with one-size-fits-all minimum expectations.

Perhaps, and most importantly, we have been evaluating governance characteristics rather than how we compare to the principles that are the basis of effective governance.

4. A New Alternative?

The good news is that a new scorecard is available that makes governance evaluation easier for U.S. public companies. The American Corporate Governance Index goes beyond publicly observable measures of corporate governance such as the number of board meetings or executive compensation disclosures. The index is based on governance principles that reflect viewpoints at leading organisations such as the National Association of Corporate Directors, Business Roundtable, Committee of Sponsoring Organisations of the Treadway Commission, New York Stock Exchange, Organisation for Economic Cooperation and Development, and King Commission. Developed by The Institute of Internal Auditors and the Neel Corporate Governance Center at the University of Tennessee in Knoxville, the Guiding Principles of Corporate Governance are intended to describe the basis of good governance.

5. The Path Forward

What is measured improves. However, meaningful improvement requires that we measure the right things systematically, thoroughly, and most importantly, using appropriate measurement criteria.

What CAE should do?

To understand and know how to compare to the Guiding Principles of Corporate Governance that are the basis of effective governance.

Reference:

https://dl.theiia.org/AECPublic/Tone-at-the-Top-December-2019.pdf

CYBERSECURITY, DATA GOVERNANCE CONTINUE TO CHALLENGE IT AUDIT

According to the "2019 Global IT Audit Benchmarking Study" which the survey consists of 2,252 participants who are chief audit executive, internal audit professionals, IT audit vice presidents and directors worldwide, the result then be summarised into the top 5 technology challenges as below:

1. IT security and privacy/ cybersecurity
2. Data management and governance
3. Emerging technology and infrastructure changes – transformation/ innovation/ disruption
4. Staffing and skills challenges
5. Third-party/ vendor management

Losing the Cybersecurity Battle?

According to another study, "Costs and Consequences of Gaps in Vulnerability Response", it found that despite a 24 percent average increase in annual spending on prevention, detection and remediation in 2019 compared with 2018, there was a 17 percent increase in the number cyber-attacks over the past year and a nearly 27% increase in cyber-attack severity compared to 2018.

According to Mr. Sean Convery, general manager of ServiceNow's security and risk unit, he mentioned that "many organisations have the motivation to address this challenge, but struggle to effectively leverage their resources for more impactful vulnerability management."

Nonetheless, he also added "teams that invest in automation and maturing their IT and security team interactions will strengthen the security posture across their organisations."

Ransomware Attacks on the Rise, Too

Another survey was also showing cyberattacks leveraging file-locking malware known as ransomware have more than doubled this year.

A cybersecurity firm McAfee finds that ransomware incidents increased by 118 percent during the first quarter of 2019 across all sectors. Malware led disclosed attack vectors, followed by account hijacking and targeted attacks. Cybercriminals also continue to leverage lax security in the Internet of Things (IoT) devices. While new malware samples increased 10 percent, total IoT malware grew 154 percent over the past four quarters.

Data Management and Governance

The Protiviti study indicated that data management and governance pose the second most critical challenge to their organisations, a significant jump from its number ten spot in the 2018 survey.

As organisations seek to leverage data with technologies such as Robotic Process Automation (RPA), Artificial Intelligence (AI), machine learning and continuous auditing and monitoring, IT audit functions are becoming increasingly focused on evaluating risks associated with data collection, processing and reporting.

Growing Importance of IT Partnerships

IT audit functions have significantly increased exposure to strategic activities within the organisation, including being invited to participate in key IT department committees (e.g., IT governance and risk management, information security, IT strategy). Leaders also assess and identify technology risk on a more frequent, even continual, basis.

Leaders to include cybersecurity in their plans on a more frequent basis than those who have lower levels of engagement and interaction with the IT department.

According to Robin Lyons, ISACA technical research manager, he states that "the importance of the partnership between audit and the IT function, which is particularly essential in the area of risk management." As these two groups work together, risk management becomes a shared, real-time effort that reduces guesswork by IT audit as to which project challenges and risks truly exist.

Lack of Skills and Resources

The survey result revealed that nearly a third (32%) organisations are unable to address specific areas of the annual IT audit plan due to a lack of resources and skills. The survey revealed the top 5 skills most in demand are:

- Expertise in advanced and enabling technologies
- Critical thinking
- Data science
- Agile methodology
- Communications expertise

What Internal Auditors should do?

As businesses continue their digital transformation journeys, the importance of focusing on data and technology by internal audit grows. Auditors need to continuously engage and partner with their stakeholders, the skills they develop and deploy as part of their activities, and the tools and technologies they are familiar with and adopt are all critical areas that require focus.

Reference:
https://misti.com/internal-audit-insights/cybersecurity-data-governance-continue-to-challenge-it-audit

HOW EFFECTIVE IS YOUR INTERNAL AUDIT FUNCTION?

The Institute of Internal Auditors (IIA) recommends that a quality assessment of the internal audit function be made at least every five years, but most chief audit executives want to know how well they are doing every year.

External Quality Reviews

One approach is to have an external quality assurance review (QAR). That can be done through the IIA, who will assign a team of experienced auditors to follow IIA QAR guidance and methodologies. The primary focus is typically compliance with IIA Standards and the Code of Ethics, although the better review leaders will also interview stakeholders and provide more of a qualitative assessment of performance. You can also engage one of the consulting firms to perform a QAR. The value of external reviews is limited to the experience and quality of the QAR team. If team members are conversant with leading practices, then you may get a review of high quality.

If you engage a consultancy firm, they may focus unnecessarily on the quality of your tools (such as analytics and RPA) instead of the value of your assurance and insight. They often rely on a list of so-called best practices rather than taking the time to understand the needs of your organisation and the potential value internal audit can deliver.

Using a Maturity Model

It is immensely valuable to use a maturity model. The IIA has a practice guide on how to use one for other processes. One of the values of a maturity model is that it helps both CAEs and audit committees understand and then discuss leading practices.

One of the values of a maturity model is that it helps both CAEs and audit committees understand and then discuss leading practices. Many audit committees are complacent and accept what they are receiving because they don't realise more value can be obtained.

The guidance can (and probably should) be used in any QAR but can also be used by CAEs and their audit committees simply to see where they stand on an annual basis.

Knowing how you compare to world-class practices and understanding the added value of moving up the maturity curve can, itself, have great value.

What Internal Auditors should do?

The maturity model can be used by the CAEs and their audit committees simply to see where they stand on an annual basis. If a team of reviewers is engaged to perform a QAR, it is suggested to ask them to use the maturity model.

Reference:
https://internalaudit360.com/how-effective-is-your-internal-audit-function/

HOW TO TAKE YOUR DATA ANALYTICS PROGRAMME TO THE NEXT LEVEL?

Internal audit departments that pursue data analytics without fear will soon be expanding their capabilities and unlocking the powerful potential of what it can do. By now, most internal audit departments have at least dipped a toe in the waters of data analytics.

So how can companies leverage data analytics to take their internal audit functions to the next level? Here are seven steps that can help supercharge a data analytics programme.

1. Demonstrate the potential. Provide even modest demonstrations of analytics capabilities that can win over skeptics and build support in the organisation. When senior executives see the potential of what advanced data analytics can do, they will become more likely to provide increased budgets to fund the effort and managers may become less possessive of the data, which can be a big barrier to getting a data analytics programme to the next level.

2. Name a data analytics champion. Internal audit functions with one or more dedicated analytics champions and dedicated analytics functions in place deliver more value, experience higher demand for their analytics services, and obtain better access to higher-quality data.

3. Get board and management support for data sharing. One of the biggest barriers to improving a data analytics programme is getting access to quality data. Business and function owners can be particularly protective of their data and may not provide access or will guard parts of the best data sets. CAEs should explore avenues to expand internal audit's access to quality data. That may include appealing to senior executives and even the board to push the importance of providing access to data throughout the organisation.

A mandate from the CEO can do wonders to loosen the tight grip some process owners maintain on their data.

4. Don't get caught up on data analytics tools. Some internal audit departments get sidetracked on what data analytics package to select. Making that decision too early can harm a data analytics initiative. Placing too much focus on learning the tools can intimidate internal auditors and keep them from advancing. Most data analytics experts say to start with something

as simple as Excel and move on when it becomes limiting to what you want to accomplish. There's no reason to increase the complexity with advanced tools before your team has a good understanding of the data and what it can tell you.

5. Think creatively about data sources. The answers you seek may not lie in the data that is right in front of you. Data analytics practitioners must identify new data sources, both internal and external, that can enhance internal audit's view of risk across the organisation. This can ensure that the organisation will be able to supplement data analytics procedures with a supply of quality data. Getting benchmark data from sources that aggregate it, for example, can provide a good baseline and comparison for analysing the internal data.

6. Get stakeholder input. CAEs should seek ways to increase the level of input stakeholders provide when building and using data analytics models and continuous auditing tools. Process owners have the best understanding of the data and can be vital in helping to determine what data should be monitored. While many different stakeholders have important insights to help determine areas of focus, it is critical that the effort is focused on building tools that internal audit can leverage to monitor risk in the business.

What Internal Auditors should do?

The maturity model can be used by the CAEs and their audit committees simply to see where they stand on an annual basis. If a team of reviewers is engaged to perform a QAR, it is suggested to ask them to use the maturity model.

Reference:
https://internalaudit360.com/how-effective-is-your-internal-audit-function/

THE RISKS IN SUPPLY CHAINS

Over the last couple of years, supply chain risk has become a key concern for the U.S. government. For example, in 2018, the U.S. Senate passed the Federal Acquisition Supply Chain Security Act of 2018, which contains powers to establish a security council specifically charged with supply chain risk.

Further legislation with ramifications for supply chain management — such as the Manufacturing, Investment, and Controls Review for Computer Hardware, Intellectual Property, and Supply Act — has been tabled at a federal level.

The hazards are many, but all point to a recognition that with increasing globalisation and digitalisation, supply chains have become longer, less transparent, and open to a range of threats. That means a business anywhere in the chain with weak security and controls is a potential target.

Dan Shoemaker, director at the University of Detroit Mercy Center for Cyber Security and Intelligence Studies shared that this exposes organisations that build and use complex systems to two key risks:

- malware can be injected into components at the bottom of the supply chain where transparency tends to be lowest
- poor-quality counterfeit products can slip into a system because of cost-cutting pressures.

Complex Contracts

Supply chain documentation is often ignored or badly managed by the purchasing organisation. Without a solid understanding of the contracts upon which agreements to buy are based, organisations run the risk of being arbitrarily overcharged by suppliers.

According to Christopher Kelly, complex supply chains that entail huge, ongoing projects subject to multiple amendments can be daunting. But internal auditors typically can get to grips with the structure of their supply chains by mapping what it looks like. That will help flush out conflicts of interest between related party companies, directors, and shareholders who may sit on both sides of a procurement deal, as well as reduce the risk of compounding overhead costs, for instance, within the project.

Failing to understand the contractual intricacies is the No. 1 mistake internal auditors make. Internal auditors trained in financial accounting, for instance, cannot assume that they will be able to apply Generally Accepted Accounting Principles to any items of expenditure.

Building Resilience

New supply chain risks are not as easy to detect and deal with. According to Jonathan Eaton, rapid change requires a flexible strategy from internal audit teams. “It is important to look at the supply chain through the lens of risk and resilience. “That means digging into the operating model to identify the potential failure points.”

Internal auditors can do that by using a Six Sigma tool called failure mode and effects analysis (FMEA), or instance, or a host of other tools. But the questions need to be addressed. A deep dive into the processes using FMEA is a great place to start.”

In addition, the internal audit leaders to ensure they are positioned as a trusted advisor to the business; otherwise, helping the business deal with supply chain risk is going to be virtually impossible. That is why having a good relationship with the business is important for internal auditors because the people who manage the the supply chain has to be forthright with internal audit about what the risks are and the triggers that make them real."

Eaton added that managing risk in the supply chain in this scenario becomes a way of protecting against the potential erosion of profitability, and internal audit needs to have an in-depth knowledge of the business’ operations to be able to truly assist the organisation in this area. He sees that the ability to track, manage, and measure risk as an internal audit's central role when it comes to supply chain resilience — particularly because those processes should be aligned to the biggest financial supply chain risks the business faces.

Eaton describes robotic process automation (RPA) as a brilliant tool once the audit understands the business' failure modes and its strategy for tracking, managing, and measuring risk. RPA deals with high-volume, repetitive processes, so it can continually scan supply chain transactions in real-time and be programmed to alert for weaknesses and red-flag events. He says too few businesses have made this move.

The internal auditor can introduce thought leadership into an organisation by bringing in the advanced technologies to mitigate the risk and build supply chain resilience. overdependence on technology and analytics can equally make internal audit blind to the more complex interrelated risks in the supply chain. For supply chain technology to work well, it needs to be aligned strategically with the business’ objectives for supply chain risk management.

Preventing Crime

Supply chains are also open to bribery, corruption, money laundering, and human trafficking risks. According to Samar Pratt, internal auditors should expect their organisations to do solid due diligence checks, it will help the organisation demonstrate to internal audit it is taking appropriate steps. As part of this process, organisations are increasingly using artificial intelligence-powered, automated due diligence technology to detect red flags while onboarding new suppliers, or to monitor third parties on an ongoing basis.

The due diligence needs to be proportionate to the risk and reflect the risk appetite of the organisation. While internal auditors are not specialists in investigating fraud in the supply chain, IIA standards require them to look for fraud indicators. That involves coming back in post-investigation to examine what went wrong in the supply chain and add significant value to the business by focusing on the lessons learned and whether controls need to be strengthened.

Making an Impact

The direct impact of mishandling a contract is the reputational damage can be equally long-lasting and harmful.

And as geopolitical risk increases and digitalisation gathers speed, supply chain resilience is likely to become even more important. It requires wide-ranging knowledge of different types of contracts, the business, and its supply chain structure — as well as keeping up to date with fast-changing threats

2019 Supply Chain Trends

The five themes impacting supply chains most in 2019:

- Revision of the Minimum Security Criteria under the U.S. Border Protection's Customs-Trade Partnership Against Terrorism (CTPAT).
- Supply chain growth in Africa, which increases exposure to risks.
- Ongoing mass migration, which poses both security and corporate social responsibility risks.
- Dramatic shifts in politics, such as elections in Brazil, the U.S.-China trade dispute, and uncertainty over Great Britain's departure from the European Union.
- The continued threat to supply chains posed by cybersecurity issues.

Source: BSI's Supply Chain Risk Insights 2019 report.

What Internal Auditors should do?

- To suggest processes to reduce such supply chain risk and insist the organisations to follow procedures established by the U.S. National Institute of Standards and Technology (NIST), and also ISO standards such as ISO 27000 dealing with information security.

- Internal auditors who can play a central role in helping their organisations build robust supply chains will enable them to compete globally and successfully integrate new products and services into their offerings.

Reference:

https://iaonline.theiia.org/2019/Pages/The-Risks-in-Supply-Chains.aspx