KPMG

Kundu

July 2020

Foreword

It's all about risk in this month's issue! We share with you some of the outcomes from our recently conducted pandemic fraud risk survey, with a PNG-specific focus. Some guidance on how to build cyber-resilience is provided by Happymabel who was one of the judges at last weekend's hackathon. The changing risk environment requires risk managers to be flexible in dealing with those risk and how to remain competitive. As always we also update you on recent IRC news.

KPMG is a professional services firm in PNG with dedicated in-house specialists in all of the following areas: internal audit/risk, visa migration, corporate finance, management consulting, IT advisory, fraud investigation as well as tax and assurance, we are well placed to provide a truly multi-disciplined approach to business advisory.

Please enjoy this month's Kundu and reach out to us at +675 321 2022 if you would like to see KPMG cover specific topics in future editions.

Zanie

KPMG PNG pandemic fraud risk management survey by Raymond Conchina, Manager, Advisory Services

We recently conducted the KPMG Pandemic Fraud Risk Management Survey where PNG businesses shared their experience across critical areas of their businesses during the pandemic period.

The survey focused on the following major key risks areas:

- Pandemic fraud risk governance.
- Organisational capacity management during the pandemic.
- Tracking of dependencies within the organisation.
- Maintenance of access controls.
- Supplier management.

The following are some of the key takeaways from our survey:

- 80% of the respondents agree that they take a holistic view when it comes to managing emerging fraud and financial crime risks within their organizations during the pandemic.
- 95% of the respondents said their organizations have implemented short-term controls to ensure that staff are adhering to the organization's policies and procedures.
- 100% of the respondents are keeping track of their team member's health.

Whilst we are facing this pandemic with its unimaginable consequences for our society, your organisation may consider the following to mitigate your fraud risks:

- Performing fraud risk assessment, considering the impact of COVID-19 on key risk indicators, leading to specific areas of focus and relevant action items.
- Data privacy and security assessment to identify any data breaches and to identify gaps to curb future incidents.
- Pro-active monitoring of data by data analytics tools to identify red flags.
- Assessment of servers, networks and firewalls to ensure cybersecurity and to detect cyber-attacks, if any.
- Carry-out investigation into red flags/fraud/suspicious matters and identify any gaps and wrong doers.
- Creating awareness among the workforce on topics related to cyber-security, data privacy and regulatory compliance, in order to prepare them to respond to present and future incidents.
- Strengthening the IT infrastructure and policies to minimize the risk of data breach and cyber-attacks.

Please follow our KPMG PNG LinkedIn page for more details on our Pandemic Fraud Risk Management Survey results. We have been providing key insights that can be helpful to your organisation in navigating this pandemic period.

How risk managers can cope with the changing risk management landscape

by Eugene Michelo, Manager, Advisory Services

When thinking about risk management and how it can help you meet your strategic goals, a good correlation could be to a soccer match. When the team is attempting to score a goal, the teams focus is shifted towards offensive leaving its defence more exposed to counter attacks. Not too dissimilar in organisations there needs to be a good balance of offensive and defensive controls. For example, when an organisation focuses its resources on generating sales (risk taking activity), the more it is exposed to costs and losses reducing its revenue gains (i.e. loss from operations, competitors, fraud, etc.)

As a Risk Manager, taking a balanced view of risk management activities would ensure that its defences are not left vulnerable as the organisation takes on risks to remain competitive. This could be hard, particularly in emerging markets where risks can be more volatile and unexpected.

Organisations could benefit from committing sufficient resources to risk management which would proportionally increase as the organisation expands its sales and its geographic footprint.
To cope with the changing risk landscape, Risk Managers should;

- **Utilize available information systems and other informal channels** to collect and monitor data on current and emerging risks. Although not always credible, informal channels such as Facebook, Twitter and other social media sites are a good source of information on emerging risks and they enable the organisation to be more prepared.

- **Consider having risk oversight across all functions** of the business through formal and informal collaboration with staff from other functions. Casual conversations with staff about how certain processes are being handled or possible product launches could provide more insights on potential risks for the organization.

- **Consider having regular risk awareness training** for all staff in the organisation as risk management is the responsibility of all staff. This would normally be built into the new staff induction process with periodic refresher short training. Having this would help improve the risk culture within the organisation and move risk management from a reactive to a proactive approach.

- **Make risk information, including policies and procedures available** to all staff. This can also include regular short risk bulletins through email and notice boards with specific themes such as fraud, money laundering, cyber security etc. for all to read.

As a Risk Manager, consider looking at how you are addressing the above focus points and being creative in your approach to risk management. This can be done through either your own self-assessment or through another expert's viewpoint to enable you support the organisation reach its goals and concurrently to improve its risk management practices.

Building cyber resilience

by Happymabel Ketias-Zingunzi, Manager, Advisory Services

Cybercrime is a growing global industry with cyber attackers becoming more determined and more skilled than ever. Highly professional and highly motivated, they are continually developing new techniques and seeking new targets to attack. The global regulatory environment for cyber security and privacy is becoming more complex and fragmented and technology is transforming the PNG business community at a speed and scale never seen before. This, combined with the regular cases of high profile breaches being reported in the media, creates an issue that requires attention in the Board room. Now is the time for the PNG business community to act decisively to protect their data, their clients' data and their own reputations.

What are some of the key messages you should consider?

- **Cyber Security Threat Landscape** - Cyber-attacks are most likely to come from organised crime groups or from a malicious insider. Malicious data disclosure, CEO fraud / business email compromise and ransomware are particular threats. Risks can materialise across the organisations entire value-chain, with particular risks around the theft of client data as well as payment fraud. There are also risks to client data processed by third party administrators and custodian banks, while the use of cloud service providers needs to be carefully managed. Criminals are becoming more creative in how they attack systems including using increasingly automated methods to attack large numbers of organisations using customised malware.

- **Building a Cyber Resilient Business** - There are key actions which help build an effective cyber security capability. The Board must be fully engaged and have an understanding of cyber security issues, and establish clear accountability for action. It is vital to map the cyber security risks facing the business, check whether the current cyber security capabilities deal with those risks and agree the organization's cyber security risk appetite and tolerance levels. There should be the technical ability and processes to detect, respond and recover from incidents; and cyber security risks should be managed effectively across the supply chain. But most

importantly of all, employees should be educated around cyber security risks and good behaviours.

- **Collaborative Action** - The PNG business community needs to work more collaboratively as a community and benefit from the economies of scale and pooling of expertise across the region. By sharing threat intelligence, collaborating to create solutions and working together on response and recovery best practices, we can help everyone improve.

- **Future Technology Disruptors** - The PNG business community is becoming increasingly dependent on technology at the core of its business. This creates fantastic ways for your organisation to differentiate their business, grow revenues and increase profits but also creates opportunities for cyber criminals. The potential cyber security risks need to be understood, managed and mitigated. In some cases, this will require new and innovative approaches to security controls.

Cyber security and its implications can no longer be overlooked by the PNG business community. Whether you are just beginning on your cyber security journey, or whether you are an organisation with a significant annual cyber/technology security budget, it is key that you are acknowledging the growing importance of cyber security risks to your organisation and taking steps to make sure you can operate securely in an increasingly digital world. As a result, KPMG believe these are 10 steps that all PNG organisations should consider to make this happen:

1. Allocate accountability for cyber security risk to a Board member.
2. Appoint a person into a senior role with responsibility for managing cyber security.
3. Develop a cyber-security strategy and seek board approval.
4. Implement a relevant international cyber security framework.
5. Perform regular cyber security risk assessments of your business.
6. Educate all staff on their cyber security responsibilities and train those in high-risk roles.
7. Implement controls to protect privileged user accounts.
8. Implement logging and monitoring on your network and critical systems.
9. Document your cyber incident response plans and perform regular simulation exercises.
10. Identify and assess the cyber security risks in your value-chain.

We are currently working with many PNG clients to address their cyber security needs.

IRC and work permit updates

Penalties

IRC had put out some notifications recently advising that penalties would be imposed from July for the late payment of SWT and GST. Prior to this the IRC had been giving taxpayers an undisclosed grace period. We have seen a case of a client being hit with substantial penalties in July for being one day late with their GST payment. Given penalties are 20% flat tax plus 20% interest per annum for SWT and 10% flat tax plus 20% interest per annum for GST we strongly recommend that taxpayers ensure their monthly taxes are paid on time.

Provisional tax

A reminder that the second instalment of provisional tax for 2020 is due for payment by 31 July 2020. Taxpayers may lodge a variation if they believe the amount assessed by the IRC for 2020 is overstated.

Income tax deadlines

Also a reminder that the IRC extended deadline, due to Covid, for taxable 2019 corporate income tax returns is 31 August 2020. For those who have not already lodged their returns it would be important that this deadline is met.

Budget 2020 legislation

The 2020 Budget Bills have recently been certified and gazetted bringing the legislation into force of law. Unfortunately, there were a number of technical errors with the legislation which have not been rectified including the carry forward of losses, the provisional tax payment dates and uncertainty around thin capitalisation. See our KPMG 2020 Budget Review for more details.

IRC scale down

IRC are temporarily scaling down to essential staff providing essential services. IRC's preference is that lodgements are made by email rather than in person although it is still possible to hand deliver documents.

Work permit updates

New work permit applications will not be accepted by the Department of Labour and Industrial Relations during the fourteen-day lockdown period unless they are for essential services. They will however accept work permit renewals, bridging and cancellations. Contact by email rather than in person is encouraged as much as possible although it is still possible to visit their office in person but maintain social distancing measures.

Contact us

Advisory
Zanie Theron
Managing Partner
ztheron@kpmg.com.au

Audit
Herbert Maguma
Partner
hmaguma@kpmg.com.au

Tax, Transactions & Accounting
Karen McEntee
Partner
kmcentee@kpmg.com.au
