KPMG Kundu

February 2025

Foreword

Welcome to the February 2025 edition of KPMG PNG Kundu. This month, we explore key topics impacting Papua New Guinea.

We discuss the potential consequences of PNG's grey-listing by the Financial Action Task Force (FATF), highlighting the challenges and long-term effects on the economy and banking sector.

We also address the importance of cyber security in PNG, emphasizing proactive measures to protect sensitive data and avoid financial and reputational damage.

Additionally, we provide updates on tax matters, including the IRC's new circular on Section 65A and the upcoming Income Tax Act.

We hope you find this edition insightful and welcome your feedback.

Ces Iewago
Managing Partner

Enjoy the read this month and reach out to kmcentee@kpmg.com.au if you have any enquiries or would like to see KPMG cover specific topics in future editions.

The likelihood and consequences of PNG's grey-listing by FATF by Karen McEntee

It seems there is one certainty in the Land of the Unexpected and this is the inevitability of the grey-listing of PNG by The Financial Action Task Force (FATF).

FATF is the global money laundering and terrorist financing watchdog. More than 200 countries and jurisdictions have committed to implement the FATF's Standards. A country is subject to assessment every ten years whereby FATF assess the effectiveness of the country's measures to combat money laundering and terrorist financing (AML/CFT). If the country does not pass the mutual evaluation assessment, it enters a one-year observation period during which the country works with FATF or its regional body to address deficiencies. If the country's measures are found to be ineffective after the one year observation period, the country will be included in a public list of jurisdictions requiring increased monitoring – this is known as a grey list. Being on this list signals to the global financial community that a country poses a higher risk for financial crimes, which can lead to increased scrutiny and reduced confidence from international investors and financial institutions. Once listed, the country is given an action plan and has 2 to 3 years to complete the plan. Some countries come off the list within that timeframe but many do not. To be removed from FATF monitoring, a jurisdiction must address all or nearly all the components of its action plan, implement the necessary legal, regulatory, and/or operational reforms and it must have the necessary political commitment and institutional capacity to sustain implementation.

In terms of PNG's journey, it was first assessed by FATF in 2010 and then again, after a delay due to Covid, in 2023/2024. Although PNG was previously grey listed, between 2014 and 2016, the hurdle for removal from the grey list was much lower at that time as to be removed PNG had to pass the required legislation into law, which it did. The 2023/2024 assessment posed a higher hurdle as this time PNG had to demonstrate that the legislation was actually effective and being enforced. Due to deficiencies in its AML/CFT measures, PNG was put into a one-year observation period from October 2024 to October 2025. It is expected that FATF will run an assessment in October 2025, privately announce the results to PNG in February 2026 and then publicly announce the results in March 2026.

The outcome looks bleak. Only four countries have ever made it out of the observation period without being grey listed – the common denominator was they were small and rich and had the will and the resources to quickly make the reforms required. FATF want to see action on the extensive list of deficient measures, this includes prosecutions and confiscations. Even if PNG had the will to launch prosecutions and confiscations, the likelihood of being able to do so by October, and make the other required legislative and structural reforms, is low.

So PNG's grey listing seems inevitable.

So what does it mean for PNG?

Unfortunately, the longer PNG is on the grey- list, the more pressure will be placed on the banking system and the economy. Given the extent of the reform and actions to take place, it is likely PNG will remain on the list for a number of years. This time round will be harder than the last time and will be dependent on how well the PNG banks can negotiate with correspondent banks. The possible implications for PNG could include:

- **Increased risk premium:** Grey listing often results in higher risk premiums for the affected country. Borrowing costs for PNG could rise, making it more expensive for the government and businesses to access international capital markets.
- **Impact on banking sector:** Banks could face increased compliance costs as banks implement more stringent AML/CFT measures to align with international standards. This could also lead to delays in international transactions and reduced correspondent banking relationships. This will be a tricky time for new PNG banks entering the market.
- **Reduced foreign investment:** As investors typically seek stable and low-risk environments grey-listing could deter foreign direct investment as investors may perceive PNG as a riskier destination for their capital.
- **Reduction in ratio of foreign direct investment to GDP:** There is on average a 2% reduction which can increase the longer the country remains on the list.
- **Reduction in inward receipts:** Analysis indicates a reduction of up to 10% in payments received by grey listed countries from the rest of the world. The study did not show any notable reduction in money leaving the listed countries.
- **Reduction in cross border liabilities:** Studies of bank inflows show a decrease of c. 16% in cross border liabilities.
- **Impact on capital inflows:** Capital inflows decline an average of 7.6% of GDP.
- **Impact on new resource projects:** Grey-listing will make it more challenging to get the new resource projects off the ground. This could impact Papua LNG, P'nyang, Pasca etc.
- **Use of visa debit cards overseas:** The longer PNG remains on the grey list, the greater the pressure on PNG banks and their correspondent banks and therefore the greater the risk that PNG visa debit cards may not work overseas.
- **Impact on fisheries industry and other sales into EU:** A substantial portion of PNG fish is sold into the European market. If PNG is put on FATF's grey list, there is a high risk PNG will be added to the EU's equivalent listing. This could result in significant pressure on EU countries not to trade with PNG.
- **Reputational damage:** PNG's international standing and reputation can be damaged.

At this stage PNG's best hope is to put itself on the right track to secure an early removal from the grey list.

Don't wait for a breach to act: address the low-hanging fruit

By Happymabel Ketias-Zingunzi

In today's rapidly evolving digital landscape, cyber security remains a top priority for organizations worldwide and Papua New Guinea is no exception. Despite the increasing sophistication of cyber threats, many of the risks we encounter are surprisingly simple to mitigate. These low-hanging fruit, such as regular patching, keeping track of updates, implementing strong access controls and performing regular vulnerability assessments, are often overlooked, leaving organizations vulnerable to attack.

Board members and staff should be acutely aware of the importance of addressing security vulnerabilities. Protecting sensitive data is paramount, as a single data breach can expose confidential information, leading to legal repercussions and a loss of trust among stakeholders. Financial implications are also significant; cyber-attacks can result in substantial financial losses due to operational disruptions, ransom payments, and remediation costs.

Ransomware attacks are rising in PNG. Despite these high-profile cases, many organizations still struggle with basic cyber hygiene. The reasons vary, from a lack of resources to complacency, but the consequences are often severe.

Addressing these low-hanging fruit is therefore crucial:

- **Regular software updates and patch management are essential:** Cybercriminals often exploit known vulnerabilities that could have been patched. Regular updates ensure these vulnerabilities are addressed promptly.
- **Employee training and awareness are vital:** Human error is a significant factor in many cyber breaches. Regular training sessions can educate employees about phishing scams, social engineering tactics, and safe online practices. Awareness programs help employees recognize and avoid potential threats.
- **Implementing strong access controls:** This ensures that only authorized individuals have access to sensitive information. This can include multi-factor authentication (MFA), role-based access controls, and regular audits of access permissions.
- **Data encryption adds an extra layer of security:** Encrypting sensitive data both in transit and at rest ensures that even if cybercriminals manage to access the data, they cannot read or use it without the decryption key.
- **Regular security audits and vulnerability assessments:** Help identify potential weaknesses in your systems. These penetration tests and assessments should include scans for security vulnerabilities in devices, applications, operating systems, cloud services, and other network resources. Addressing these vulnerabilities proactively can prevent breaches before they occur. Once identified, organisations must ensure the recommendations are actually implemented in a timely manner and tracked.

To address this growing concern, we have established a PNG Cyber Security Centre of Excellence platform. This initiative aims to share knowledge and best practices on cyber security, focusing on simple yet effective measures like patch management and update tracking. Our resources are available free of charge, but the value they provide is immeasurable. By leveraging these tools and insights, organizations can fortify their defences and stay ahead of emerging threats.

The cost of inaction is too high—do not wait for a breach to act. Proactive measures today can save your organization from devastating financial losses, reputational damage, and operational disruptions tomorrow.

Our Cyber Team is here to support you every step of the way. With our monthly vulnerability checks, you can ensure your organization is well-protected against cyber threats. This comprehensive assessment, which takes just 24-48 hours, provides timely and actionable insights through a scan for security vulnerabilities in devices, applications, operating systems, cloud services, and other network resources providing timely and actionable insights to fortify your organization's defence.

Remember, a robust cyber security strategy is invaluable. Act now to prevent your organization from becoming the next victim of a cyber-attack.

Section 65A update

IRC has issued a tax circular on Section 65A however it is not yet available on their website. The Section 65A process requires the withholding of 10% GST from payments to suppliers by certain government departments, certain state-owned enterprises, and certain coffee and cocoa suppliers. Notably the tax circular states that Section 65A has been expanded to other industries such as, but not limited to, the Mining, Wholesale/Retail and Banking and Finance sectors.

The withholder is then required to remit this GST directly to the IRC. The supplier would include the sale as usual in its GST return and it would also include the Section 65A amount withheld as a credit in a specific Section 65A line item in its GST return. The tax circular specifically states that the supplier should include the sale based on the tax point for GST (usually the date of the invoice) but can only include the Section 65A credit in the period in which it receives payment from the customer. There may therefore be a mismatch.

As it can take IRC many months to process and allocate the Section 65A credits, it is critical that suppliers keep an accurate track of their credits allocated. With the expansion of this system to encompass customers in the private sector, the administrative and cash-flow burden around this process will undoubtedly further increase for taxpayers.

IRC and tax matters

The Tax Agent Bulletin which lists the income tax deadline dates for the 2024 income tax returns has not yet issued. The IRC has however posted the updated 2024 tax return forms on its website.

In other news the new Income Tax Act is still on track to be handed down in Parliament in March.

Gazettal of the increase in the tax clearance threshold

The increase in the tax clearance threshold to K1.5m was gazetted this month. This is welcomed by all overseas remitters.

Our social media presence

As usual, you may access our regular multi-disciplined thought leadership pieces, newsletters, and updates on our KPMG PNG LinkedIn page. Also, connect via our webpage www.kpmg.com.pg and Facebook https://www.facebook.com/pngkpmg/

Contact US

Zanie Theron

SPP PIC
ztheron@kpmg.com.au

Karen McEntee

Partner
kmcentee@kpmg.com.au

Pieter Steyn

Partner
psteyn@kpmg.com.au

Ces Iewago

Managing Partner
ciewago@kpmg.com.au

Brett McDermott

Partner
bmcdermott@kpmg.com.au

Christian Angelopoulos

Partner
cangelopoulo@kpmg.com.au

Wayne Osterberg

Partner
wosterberg@kpmg.com.au

kpmg.com.pg