Public Sector and Infrastructure Insight

November 2024

pwc

www.pwc.com/ke

Contents

Introduction

Welcome to our publication, themed **"Resilient Governance: Navigating Challenges while Shaping a Better Tomorrow,"** thoughtfully curated by PwC's subject matter experts in the public and infrastructure sectors. In a rapidly evolving global landscape, the ability to navigate complex challenges while fostering sustainable development is crucial for African nations.

This collection of articles aims to provide insights and actionable recommendations that can empower public sector leaders and stakeholders in their pursuit of resilience and fiscal sustainability.

The first article focuses on tax policy reforms for non-profit organizations (NPOs) in Tanzania, shedding light on the often-overlooked tax obligations that these entities face. Contrary to common assumptions, NPOs are not universally exempt from income tax; instead, they must navigate a complex landscape of compliance requirements.

The discussion highlights the necessity for NPOs to secure Government Notices (GNs) for tax exemptions and to understand the intricacies of their agreements with the government.

In the context of technological advancement, our publication delves into the transformative potential of artificial intelligence (AI) in the African public sector.

Dr. Benson Okundi

Partner, Government and Public Sector Leader, PwC, East Market Area

benson.okundi@pwc.com

Highlighting initiatives from countries such as Kenya, Uganda, Tanzania, and Rwanda, the article emphasizes how governments are beginning to leverage AI to improve public services and operational efficiency.

However, the widespread adoption of AI is hampered by several challenges, including inadequate data, insufficient regulatory frameworks, and a lack of investment and expertise. The piece advocates for responsible AI practices that prioritize fairness, transparency, and accountability, ensuring that the benefits of technology are maximized while minimizing risks such as bias and privacy concerns.

As governments increasingly embrace digital transformation, the demand for robust cybersecurity infrastructure has never been more pressing. Our article on this topic examines the escalating cyber threats targeting sensitive data and critical systems, spurred by initiatives like e-portals and online tax systems.

Despite the urgency, public sector investment in cybersecurity remains inadequate, leaving governments vulnerable to attacks. The piece outlines a multifaceted strategy to enhance cybersecurity, emphasizing the importance of education, increased funding, and cross-sector collaboration.

Data protection and privacy compliance is another critical focus area, particularly in the public sector. With vast amounts of personal data collected for essential services, safeguarding this information is both a legal obligation and an ethical imperative.

The widespread adoption of AI is hampered by several challenges, including inadequate data, insufficient regulatory frameworks, and a lack of investment and expertise

Our article provides practical measures that public organizations can adopt to enhance compliance, such as adhering to the Data Protection Act 2019, establishing privacy governance frameworks, and conducting gap assessments.

By fortifying their privacy practices, public entities can protect individual rights and navigate the evolving regulatory landscape effectively.

Infrastructure development is also highlighted, particularly the financing challenges facing power transmission in Africa. Despite the continent's vast renewable energy potential, inadequate investment in transmission networks hampers rural development and access to essential services.

This article argues for increased public and private sector investments, exploring models such as Independent Power Transmission (IPT) and privatization as potential solutions to attract financing and ensure that projects are bankable.

Finally, the publication addresses the serious threats posed by money laundering and terrorism financing to African economies. With many countries in Africa ranking among the highest risk globally, the ramifications extend beyond financial integrity to foreign investment and political stability. However, there is hope: a coordinated continental approach, along with strengthened national regimes, can effectively combat these threats.

By fostering collaboration among governments, international organizations, and the private sector, we can promote sustainable economic growth and resilience.

We hope that these articles not only inform but also inspire action toward resilient governance in Africa. By confronting challenges head-on and exploring innovative solutions, we can work together to shape a better tomorrow.

Enjoy the read!

Foreword

Welcome to our 2024 Public Sector & Infrastructure insights. This publication reflects our progressive approach, with a particular emphasis on resilient governance.

Aligned with the theme, 'Resilient governance: Navigating Challenges while shaping a better tomorrow', the contributors to this publication shed light on how resilient leadership plays a critical role in driving success by fostering innovation, managing crises effectively, and inspiring high-performing teams.

In this publication, we highlight how in many cases Not-for-profit organisations (NPO's) enter into an agreement or memorandum of understanding with the Government, through the host Ministry responsible for the relevant cause - i.e. education, health, etc. These agreements sometimes include the Government's commitment to certain tax exemptions, that are not necessarily provided for under the tax law.

However, the law requires exemptions to be explicitly provided in the relevant legislation and where it is not the case, there has to be a Government Notice (GN) published by the Minister for Finance to give such exemptions effect into law.

Creating a resilient cybersecurity infrastructure demands a multifaceted strategy. As an initial step, there must be a concerted effort to enhance the appreciation of cybersecurity in the sector. Comprehensive educational programs, workshops and awareness campaigns focused on cybersecurity would need to be curated and implemented to cover all officials relevant and necessary to support the drive for maturity.

Secondly, there should also be a concerted effort to prioritize cybersecurity funding and budget allocation within the public sector to mirror digital transformation investments as a key attribute of security and privacy by design.

Additionally, collaboration among government agencies and regulatory bodies is essential to establish policies, frameworks and standards mandating security and privacy considerations in all tech projects and ensuring

Isaac Otolo

Infrastructure Industry Leader,
Partner,
Deals - Transaction Advisory,
PwC Kenya

isaac.otolo@pwc.com

that cybersecurity is integrated from the outset or at worst retrospectively for existing infrastructure.

Transmission line development in Kenya is dominated by the public sector with limited private sector investment. The historical investment in generation has been approximately four times more than transmission and distribution combined. Construction of these transmission networks are highly capital intensive. Fiscal constraints in most African governments limit their ability to invest in these transmission projects resulting in a major infrastructure deficit.

According to the World Bank, an average annual investment of between USD 3.2 billion to USD 4.3 billion is required in the power transmission sector between 2015 and 2040. To meet the required investment, and borrowing from the track record in generation, private sector financing will be required and should be considered to ease the financial constraints and bring their experience in project implementation and operation.

Each article invites us to navigate the infrastructure sector landscape, uncovering opportunities and strategies that can shape a more resilient and sustainable future for East Africa. We hope you find the topics covered in these articles insightful and valuable. Your comments and feedback are highly appreciated. Please feel free to reach out to any of the PwC contributors featured in this publication for further clarification or discussions.

1 The AI Revolution in Government: Unlocking the Future, Navigating the Challenges

Artificial intelligence (AI) is rapidly becoming a reality that will transform governments and public sector players across the world. In Africa, major tech companies like Google, Microsoft, and Amazon are establishing technology hubs focused on using AI to address local challenges.

We are already witnessing flashes of AI's potential in government. In Kenya, the Office of the Data Protection Commissioner (ODPC) launched an innovative AI chatbot to enhance data privacy awareness and support among citizens and businesses. The Kenya Revenue Authority (KRA) in its newsletter indicated it had plans to leverage AI to automate repetitive tasks and improve tax collection. International donors use AI to avoid waste and hasten the achievement of development targets. Use cases include analyzing health data with AI for early detection of disease outbreaks.

In Uganda, the Ministry of ICT and National Guidance have recently engaged in partnerships geared towards leveraging Artificial Intelligence Systems to increase the use of ICT services for Uganda's social and economic development.

Tanzania's government, through the Government Enterprise Service Bus (GovESB) initiative, is actively digitizing its administrative functions and this presents opportunities to integrate AI into these centralized e-government platforms for efficiency and transparency.

Rwanda has also been on the forefront with the launch of Centre for the Fourth Industrial Revolution (C4IR Rwanda) that focuses primarily on artificial intelligence (AI), machine learning, and data governance. Other countries like Egypt and Mauritius have also designed national AI strategies that cover adoption of AI in government and national development.

At the regional level, the African Union (AU) has established a working group to develop a capacity-building framework and an AI think tank.

Jamila Aroi
Consulting & Risk Services Partner,
PwC Kenya
jamila.aroi@pwc.com

Brencil Kaimba
Alumni

Despite these initiatives, AI applications have not yet been widely adopted throughout Africa. The public sector, in particular, is still lagging behind in AI innovation.

This lag is due to factors such as:

1. Lack of relevant data to train AI algorithms.
2. Absence of a regulatory framework and policies to govern ethical AI use.
3. Lack of investment by the government and public sector in AI research and development.
4. Lack of skills/expertise in AI due to the low uptake of STEM education.
5. Need to carefully apply data protection principles without stifling innovation.

Realizing AI's full transformative power requires embracing innovation while navigating serious risks and challenges. These risks include:

1. AI bias leading to unfair and discriminatory outcomes, especially against marginalized groups. For example, an AI-based resume screening tool can disproportionately reject applications from say women when the training data used contained historical gender biases.
2. Weaponization of AI to spread or automate cyber-attacks. This can be in the form of phishing attacks, malware, sophisticated nation state attacks and deep fakes, where AI generates realistic but fake audio/video content us used to spread disinformation against individuals and entities.
3. Data protection concerns ranging from mass collection and use of Citizen's personal data to train AI surveillance systems like facial recognition to unfair automated decision making processes in functions like loan approvals.

Building trustworthy AI systems requires diverse teams of experts and closely following principles like fairness, accountability, and ethical data practices. The concept of "Responsible AI" has therefore emerged, which involves defining policies and establishing accountability to guide the ethical creation and deployment of AI systems. Without these, AI adoption will be curtailed.

It is important to acknowledge these challenges and consider the risks posed by AI. Key questions to ask ourselves are:

1. Does AI genuinely solve core problems better than existing methods?
2. What safeguards are needed to prevent biased, discriminatory AI outputs?
3. Do we have the technical capabilities to implement AI effectively and responsibly?

Key ethical principles for responsible AI for public sector players to consider include:

- **Human Rights and Dignity:** AI must uphold human rights laws and standards, safeguarding freedoms like expression and information access.
- **Fairness and Non-Discrimination:** AI systems should be designed to prevent biases and discrimination that could reinforce societal inequalities. For example, AI recruitment tools must avoid discriminating based on gender, race or age.
- **Privacy and Data Protection:** Strong data governance is crucial for AI handling personal data. AI surveillance systems like facial recognition must have strict privacy safeguards limiting data collection.
- **Transparency and Explainability:** AI decision-making systems, like those for loan approvals, must provide clear explanations to allow scrutiny of potential biases.
- **Human Oversight:** Humans must maintain control, able to intervene in high-stakes AI decisions. For example, medical AI diagnosis tools should allow expert validation before treatment.
- **Accountability:** Clear lines of responsibility are needed, with corrective options for AI failures. Critical AI deployments like in infrastructure must have mechanisms to hold developers/operators accountable.

In conclusion, optimism must be balanced with realism about the potential benefits, risks, and challenges.

Governments, public sector players and policymakers must take a strategic, ethical, and human-centered approach, when adopting AI to elevate the public sector to new heights of efficiency, accountability, and public service.

2 Enhancing data protection and privacy compliance in the public sector

Herbert Njoroge
Manager, Legal Business Solutions
PwC Kenya
herbert.njoroge@pwc.com

Tracy Odipo
Manager,
Legal Business Solutions
PwC Kenya
tracy.odipo@pwc.com

Entities in the public sector collect vast amounts of personal data and information to provide critical services to individuals. This includes personal data relating to health records, social security numbers, education records, financial data, criminal records, identification information, biometric data and images among others.

Ensuring the confidentiality and integrity of this information is not only a legal requirement but also a fundamental ethical and human rights obligation.

Public entities now have the obligation to implement strict privacy measures particularly in respect of data subject rights, determining the disclosure requirements to data subjects prior to processing their personal data, implementing robust technical and organisational measures, and putting in place safeguards for cross border transfers of personal data to cultivate a sense of security in the services they provide.

In this article, we delve into the key data protection compliance considerations for public entities engaged in the infrastructure industry. Their compliance efforts can enhance positive impact on society especially on matters data protection and privacy.

What is the public sector basis for processing personal data?

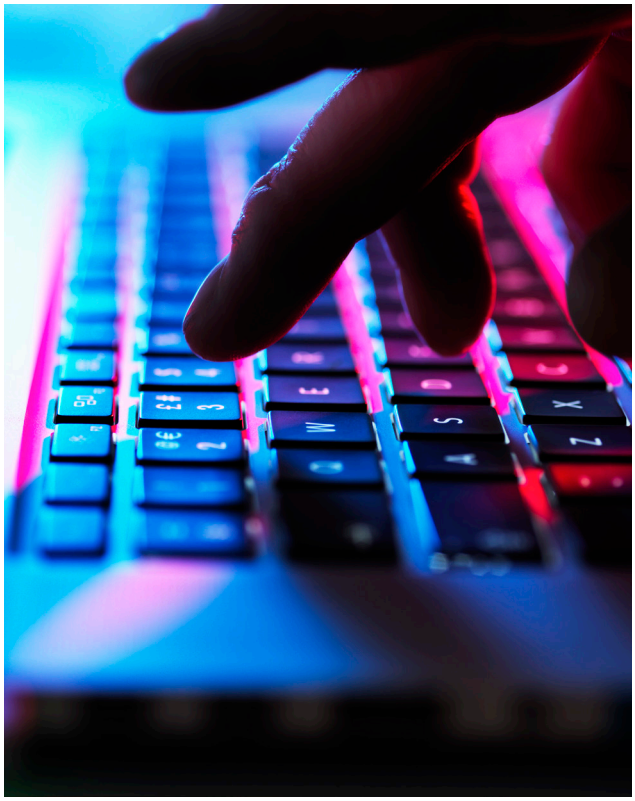
The Data Protection Act, 2019 (DPA) provides for various lawful basis which organisations are required to rely on when processing personal data. The most relevant lawful basis for processing personal data by the public sector is the public interest basis where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

This lawful basis covers public functions and other public interest functions done by non-governmental agencies. Neither the DPA nor the supplementing Data Protection General Regulations, 2021 (Regulations) provide for the specific processing activities that would be considered public. Public entities in various sectors hold large amounts of personal data. The most important consideration when relying on this particular lawful basis is identifying the nature of the function being exercised by the controller and not the nature of the organisation performing the function.

What other lawful basis can be relied upon by the public sector?

The DPA provides for other lawful basis that public sector organisations can rely on. This includes processing individuals' data to comply with any legal obligation to which the controller is subject. Organisations whose mandate is established under statute to offer services to the public may rely on this legal basis to process personal data. For instance,

The Data Protection Act, 2019 (DPA) provides for various lawful basis which organisations are required to rely on when processing personal data



the Kenya Revenue Authority which is established by the KRA Act can rely on this lawful ground as a basis for assessing, collecting and administering taxes to individuals and corporate entities in Kenya.

Public sector entities may also rely on consent and legitimate interest as grounds for collecting personal data. These legal bases may be quite limiting to rely on but may be available in certain circumstances. In particular, consent and legitimate interest may still be available for processing which falls outside the tasks of a public entity.

An example will be when a specific public body f sets out to run a research study to establish the number of female students in rural areas that dropped out of secondary school due to teenage pregnancies. This would require the body to first obtain parental consent due to the sensitive nature of the data involved and the processing of large amounts of personal data.

How can public sector organisations comply with cross-border transfers?

Public sector organisations may find themselves sub-contracting third party cloud-based system providers to manage their data storage needs. In many instances, these third parties are located outside Kenya, and they have access to the personal data which is stored and processed on their systems. The DPA provides for conditions which must be fulfilled by organisations prior to transferring personal data outside Kenya.

This includes transfers which take place on cloud-based systems. Prior to transferring personal data on cloud, public sector entities must comply with the following:

- **Proof of appropriate safeguards with respect to the security and protection of the personal data;**
  Appropriate safeguards include legal instruments such as a single data transfer agreement which sets out the rules of processing personal data between public authorities or agencies, their compliance with the principles of processing data, how they will manage data subject rights access requests among other things. Organisations may also consider entering into data processing and data sharing agreements with third parties providing cloud storage/hosting services.

- **Adequacy decision made by the Data Commissioner;**
  The transfer of personal data to another country or relevant international organisation is based on an adequacy decision where the data commissioner makes an adequacy decision that the other country or organisation ensures an adequate level of protection of personal data. The Kenya data commissioner is yet to issue any guidance on countries whose data protection laws provide an adequate level of protection.

- **Transfer as a necessity and obtaining consent of the data subject;**
  The DPA and the Regulations do require public organisation to obtain consent from data subjects prior to transferring their sensitive personal data outside Kenya. Public entities must ensure that the consent obtained is explicit from the data subject and that the data subject is informed of the purpose for transferring their personal data before consenting. Public entities can also rely on necessity as a ground for transferring personal data. Necessity may include contractual agreement between the data subject and the public entity for purposes of exercising or defending a legal claim, for vital interest, legitimate interest or the public interest of the organisation.

How can public sector organisations build a privacy governance framework?

The DPA provides various obligations for organisations processing personal data. Public sector organisations have a mandatory duty to notify individuals before collecting their personal data about their data subject rights and how they can exercise those rights, the purpose for which they are collecting their personal data, the fact that their data is being collected, third parties with whom their personal data will be shared with and a description of the technical and security measures implemented to protect the personal data.

Public sector organisations are also obligated to put in place other critical privacy policies such as a data retention policy which discloses the organisations data retention periods.

What are some key strategies for compliance by the public sector?

1. **Gap assessment:** A gap assessment is a critical part of a data privacy compliance program. It helps organisations to evaluate the maturity of the privacy program compared to regulatory and legal obligations. By identifying problem areas and showing progress to close gaps over time, organisations in the public sector can strategically improve their privacy posture and comply with evolving requirements.
2. **Develop data inventories:** Documenting the processing activities which are necessary for public interest or for reasons to exercise official authority is critical to demonstrate compliance with the DPA. This also helps public entities to understand their data processing activities.
3. **Policy Management:** The creation of policies aligned to applicable laws and regulations. These policies cover key topics such as data collection, usage, storage/retention, transfers, individual rights and establish review cycles to update for new requirements.
4. **Privacy incident management:** An incident response plan is a good strategy for compliance in the public sector. It would incorporate a breach notification procedure that swiftly identifies, escalates, investigates and finally fixes the data security breach to mitigate all potential losses.
5. **Data protection and privacy audit:** This encompasses a comprehensive review process undertaken by an organisation to assess its handling of personal data. Structured data discovery and risk analysis is key in building privacy programs, target areas of high risk and impact, and demonstrate due diligence.

Public sector organisations are obligated to put in place other critical privacy policies such as a data retention policy which discloses the organisations data retention periods

3 Money Laundering & Terrorism Financing| Ramifications on African Economies

The ML/TF risk landscape in Africa

Money laundering, terrorism financing and recently spotlighted, proliferation financing, are risks that continue to have far reaching consequences on the global financial system and African economies have not been spared. According to the 2023 Basel AML Index which measures the risk of money laundering and terrorism financing in jurisdictions around the world, 6 of the top 10 countries with the highest money laundering and terrorism financing risk levels are from Africa.

Further to this, of the 19 countries currently grey listed by the Financial Action Task Force (FATF), 11 are African countries including Kenya, Tanzania, South Sudan, South Africa and the Democratic Republic of Congo. This is a clear indication that money laundering, terrorism financing and proliferation financing continue to be pervasive and that more concerted efforts are required to curb and mitigate these risks both at a country and continent level.

Impact of ML/TF on African economies

The direct and indirect costs of these financial crimes on African economies can be quite lofty. The financial system integrity of countries with heightened risks of money laundering and terrorism financing is significantly compromised, potentially resulting in decreased foreign investments as they are less attractive to foreign investors. This could further result in sanctions, lost financial services and even financial instability.

Corruption, one of the top predicate offenses continues to be widespread in Africa and is on its own detrimental to foreign trade and investment. In a recently published report by the Office of the United States Trade Representative on foreign trade barriers, bribery and corruption was cited as one of the main barriers to doing business in several African countries including Kenya, Ethiopia, Nigeria and Angola, resulting in reduced investment flows, and lost development opportunities.

John Kamau
Deals - Forensics Partner,
PwC Kenya

john.kamau@pwc.com

Bridget Kayondi
Alumni

According to a study published in 2020 by the Africa Growth Initiative at Brookings Institution, Africa is reported to have exported an estimated USD 1.3 trillion between 1980 and 2018 in illicit flows out of the sub-Saharan part of the continent, a consequential loss and drainage of domestic resources that could have been rightly channeled into development and savings.

According to the 2023 Basel AML Index which measures the risk of money laundering and terrorism financing in jurisdictions around the world, 6 of the top 10 countries with the highest money laundering and terrorism financing risk levels are from Africa

This indirectly has possibly further contributed to the observed reduced opportunities as well as increased financial inequality.

On an even larger scale, persistent and widespread financial crimes that go unabated and with no consequences to match erode public confidence and trust in the government structures in place, hindering proper governance and in extreme cases, leading to political instability.

Terrorism financing heightens the risk of actual terrorism which poses a significant threat to life, national security and ultimately the country's economic performance.

Having inadequate anti-money laundering, counter terrorism and proliferation financing regimes, which is evident across many African countries, exacerbates the problem, providing an environment where predicate offenses such as corruption take root and are rife.

A glimmer of hope; there are efforts underway to address this problem

In spite of the current landscape, there are many ongoing efforts across the continent by various stakeholders to address this problem through different approaches. Through governmental institutions, inter-governmental institutions, international development partners and private sector players, there are many programs aimed at mitigating money laundering, terrorism financing and proliferation financing risks as well as corruption.

An example of this is Uganda, which recently exited the FATF grey list, a testament of the country's efforts to address the deficiencies in its anti-money laundering and counter terrorism financing regime.

Call to action: So what?

It is important that the full breadth of the consequences of these financial crimes to our continent's financial systems and economic growth are well understood and articulated. This will be key to driving the necessary change required to curb these risks, including enhancement of the country's technical capacity as well as political will.

Given these risks are cross-border in their very nature, adopting a continental approach to addressing these risks will be pivotal in the fight against money laundering, terrorism financing and proliferation financing.

Intelligence sharing, pooling of resources, setting regulatory standards, establishing a geo-political authority that can enforce sanctions and protect the continent are but a few of the benefits that can be realized from such an approach.

Individually, African countries should make the necessary efforts and investments required to ensure their anti-money laundering and counter terrorism and proliferation financing regimes in place are robust, commensurate to the country's risk levels and in line with global standards such as the FATF recommendations.

Information sources

https://www.imf.org/en/Blogs/Articles/2023/12/07/financial-crimes-hurt-economies-and-must-be-better-understood-and-curbed
https://www.brookings.edu/wp-content/uploads/2020/02/Illicit-financial-flows-in-Africa.pdf
https://www.brookings.edu/articles/new-trends-in-illicit-financial-flows-from-africa/
https://sanctionscanner.com/blog/negative-effects-of-money-laundering-on-the-economy-132
https://www.unodc.org/documents/NGO/AU_ECA_Illicit_Financial_Flows_report_EN.pdf
https://index.baselgovernance.org/ranking
https://baselgovernance.org/basel-aml-index
https://www.ojp.gov/ncjrs/virtual-library/abstracts/consequences-money-laundering-and-financial-crime
https://www.unodc.org/documents/NGO/AU_ECA_Illicit_Financial_Flows_report_EN.pdf
https://www.fatf-gafi.org/content/fatf-gafi/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-february-2024.html
https://www.businessdailyafrica.com/bd/economy/us-flags-kenya-over-bribes-extortion-in-public-tenders--4576806
https://ustr.gov/about-us/policy-offices/press-office/press-releases/2024/march/ustr-releases-2024-national-trade-estimate-report-foreign-trade-barriers

4 Building Cyber Security Infrastructure in the public sector in the age of digital transformation

Dorothy Nansubuga
Consulting & Risk Services,
Senior Associate,
PwC Kenya

dorothy.nansubuga@pwc.com

Jamila Aroi
Consulting & Risk Services
Partner,
PwC Kenya

jamila.aroi@pwc.com

In today's digital era, the public sector is undergoing a profound transformation driven by technology. From local councils to central government agencies, the adoption of digital initiatives has become imperative to enhance service delivery and adapt to citizens' changing expectations. Moreover, the COVID-19 pandemic underscored the criticality of digital resilience, prompting governments worldwide to expedite their digital agendas to ensure uninterrupted services amidst unprecedented disruptions.

Take Uganda, for example, where a host of digital initiatives have been deployed to modernize governmental functions. These range from national payment switches to self-service government e-portals enabling citizens to conduct tasks such as online driving permits and passport applications and renewals.

Notable open data platforms like the Government Citizen Interaction Centre (GCIC) and the online tax-filing system (EFRIS) have further facilitated citizen engagement and transparency. Additionally, initiatives such as public safety and emergency response alert systems have enhanced the government's ability to ensure the welfare of its citizens.

However, despite the immense potential of digital transformation, this journey is not without its challenges, notably in the realm of cybersecurity. Given the abundance of sensitive data processed, such as citizens' personal information, classified government data, and critical infrastructure details, the sector has become an attractive target for various cyber threats.

These threats extend beyond common cybercriminal activities to encompass sophisticated espionage and sabotage schemes orchestrated by nation-states and terrorist groups. Between September 2020 and August 2021, 40% of the threats managed by the National Cyber Security Centre (NCSC) targeted the public sector.

A 2023 report by the National Cybersecurity Agency of France (ANSSI) also highlighted a significant increase in cyber threats, particularly ransomware attacks, with 23% affecting the public sector. These statistics underscore the gravity of the danger posed to the public sector by cyber threats.

Yet, despite a growing awareness of the risks, investment in cybersecurity in the public sector remains significantly underfunded. In 2022, only 6.6% of the public sector budget was allocated to cybersecurity, while the level of technological maturity exceeded 36.9% (source: Wavestone, March 2022).

6.6%

of the public sector budget was allocated to cybersecurity, while the level of technological maturity exceeded 36.9% in 2022

This mismatch in budget allocation has over the years reflected a lack of maturity in cybersecurity considerations. To highlight a few, here is a shortage of skilled cybersecurity personnel employed by the public sector. Furthermore, many government agencies operate outdated systems which have reached end of life, are no longer supported and contain common vulnerabilities with known exploits.

These legacy technologies lack the robust security features of modern counterparts, providing cybercriminals with numerous entry points. Not only are these legacy systems vulnerable, they are also ill-prepared to leverage emerging technologies and meet evolving public expectations. At the core of the problem lies the challenge of "red tapes" and bureaucracies in responsibility mapping and performance measurement. As such, cyber risks are often poorly identified and owned and lead to sluggish action plans and decision-making challenges.

From a broader perspective, it is important to also note that the interconnected nature of government systems and public sector services in a complex value chain amplifies the impact of successful cyberattacks as they can potentially spread across multiple agencies and systems and become a systemic issue.

As the sector steadily advances in digital maturity, the imperative for a robust cybersecurity infrastructure becomes increasingly crucial and is a pivotal cornerstone in the collective defense against the ever-evolving landscape of cyber threats.

The alarming frequency of attacks, increasing sophistication of the exploit approach and the impact it leaves on critical public infrastructure calls for urgent action towards cybersecurity policies, programmes and practices which promote the objectives of safeguarding national security, upholding public trust, and guaranteeing the seamless provision of essential services to citizens.

Creating a resilient cybersecurity infrastructure demands a multifaceted strategy. As an initial step, there must be a concerted effort to enhance the appreciation of cybersecurity in the sector. Comprehensive educational programs, workshops and awareness campaigns focused on cybersecurity would need to be curated and implemented to cover all officials relevant and necessary to support the drive for maturity.

Secondly, there should also be a concerted effort to prioritize cybersecurity funding and budget allocation within the public sector to mirror digital transformation investments as a key attribute of security and privacy by design. Additionally, collaboration among government agencies and regulatory bodies is essential to establish policies, frameworks and standards mandating security and privacy considerations in all tech projects and ensuring that cybersecurity is integrated from the outset or at worst retrospectively for existing infrastructure.

Facilitating collaboration between public and private sectors is equally vital, as a means for information sharing, joint threat intelligence analysis, and coordinated response efforts. To ensure that these programmes are indeed delivering on the target objectives of cybersecurity, resilience and privacy, mechanisms would also need to be designed and implemented for periodic review of the programmes to assess its effectiveness, identify issues and chart a resolution plan for implementation.

In conclusion, as the public sector strides forward into the digital age, the blueprint for cybersecurity in the public sector must adapt—becoming more agile, scalable, elastic, and flexible to safeguard sensitive data, critical systems, and citizen trust.

5 Strategies for fiscal sustainability in African countries through Tax Policy Reforms in the Public Sector

Tax challenges and Reform opportunities for Tanzania

Tax is one of the two main aspects of fiscal policy of a country, the other being spending. As a not-for-profit organisation (NPO) or non-governmental organisation (NGO) you may wonder: of what relevance is tax to me? Well - very relevant! Whilst there is often an expectation that NPO's are automatically exempt from income tax, this is not so, certainly at least for Tanzania.

In addition, even in cases where the entity does have an income tax exemption, there are other taxes that require compliance with. Hence sustainable tax policies are as important to NPO's as they are for private companies. In any case, NPO's should ensure they understand the applicable tax legislation and its relevance to their activities.

In many cases NPO's enter into an agreement or memorandum of understanding with the Government, through the host Ministry responsible for the relevant cause - i.e. education, health, etc. These agreements sometimes include the Government's commitment to certain tax exemptions, that are not necessarily provided for under the tax law. However, the law

Redempta Maira
Associate Director
Tax Services
PwC Tanzania
redempta.maira@pwc.com

Not-for-profit organisations are exempt from paying skills and development levy, to the extent the organisation is considered to be a charitable organisation

requires exemptions to be explicitly provided in the relevant legislation and where it is not the case, there has to be a Government Notice (GN) published by the Minister for Finance to give such exemptions effect into law.

As the NPO sees the Government as one institution, the requirement to get exemptions gazetted is often overlooked on the basis that the coordination between the two ministries (host ministry and Ministry for Finance) should naturally be handled by the Government. What to do? Well, to avoid disputes with the revenue authority, NPO's should ensure a GN is procured before the beginning of the relevant project activities.

Where exemptions are in respect of income tax and provided for in an agreement concluded between the Government of Tanzania and a foreign Government by which the relevant project is funded, then in practice such an agreement is interpreted to qualify as an "international agreement" under the income tax law

(similar to a double tax agreement) such that the provisions of the agreement take precedence over the local legislation in the event the two are inconsistent, and so there is no need for a GN to enforce such exemptions.

Where there is no income tax exemption applicable, an NPO can apply for a private ruling to be issued by the Commissioner of the Tanzania Revenue Authority (TRA) to be considered as a charitable organisation, provided it is a resident entity of a public character that was established and functions as an organisation for poverty relief, advancement of education, or provision of general public health, education, water or road construction or maintenance.

Where such a private ruling is issued, although it does not automatically amount to exemption, in practical terms it provides for exemption so long as a charitable organisation spends at least 75% of its funding in the relevant year.

As NPO's in Tanzania are required to register with the NGO's Registrar, the policy makers may consider streamlining the private ruling approval process with the Registrar's office registration process, so that the two run in parallel with the TRA given a right to revoke the charitable status should it in future (for example, following a tax audit) not be satisfied that the organisation carries out the relevant charitable activities.

In terms of existing tax exemptions in the law, NPO's are exempt from paying skills and development levy (SDL), to the extent the organisation is considered to be a charitable organisation. Even though the definition of a "charitable organisation" under the Vocational Education and Training (VETA) Act (the charging legislation for SDL) is similar to that provided under the Income Tax Act, the VETA Act does not require a private ruling for an entity to obtain such status.

However, the Commissioner of the TRA has to be satisfied that the entity meets the relevant criteria after conducting a due diligence. Whilst there is no mechanism set out in the law for such a due diligence to be conducted, available case law contemplates that the burden of proof lies with the taxpayer and so the taxpayer needs to provide the TRA with all relevant information necessary to conduct the due diligence.

There is therefore a need for legislative amendment to clearly articulate the due diligence process contemplated in the law. Again, as with the proposal on income tax, ideally once the NGO Registrar is satisfied that the organisation carries out its activities as an NPO, the SDL exemption should apply, with TRA given the right to disapply the exemption in the event they become aware of the organisation not conducting its activities as such.

Other compliance obligations for NPO's include compliance with taxes for which the NPO is an agent such as withholding tax (which PAYE also forms part). Non-compliance to tax obligations leads to penalties and interest that may be highly punitive and hence affect the NPO's ability to cater for its important causes, and so tax compliance even if not operating for profit is a necessary evil.

6 Neglected Chain: Financing Power Transmission in Africa

Kenya has a huge untapped potential for renewable energy. This potential has however been largely hindered by the challenges around supply and transmission of power. A lot of investment has been made towards the generation and distribution of energy relative to power transmission.

The inadequate investment in electricity transmission has resulted in an uneven development especially in rural areas affecting provision of health services, access to quality education and growth of businesses. As such, significant public and private investment is required to develop an extensive transmission network through building and upgrading the transmission infrastructure and capacity.

A well-planned and reliable transmission network is beneficial in the long-term resulting in; reduced electricity costs by ensuring economies of scale in power generation, cross-border power transmission, therefore, providing access to cost-efficient energy resources & connecting power to the unserved demand, reduced power reserve required to ensure the security of power supply, and enhanced integration of renewable energy into the energy system.

Transmission line development in Kenya is dominated by the public sector with limited private sector investment. The historical investment in generation has been approximately four times more than transmission and distribution combined. Construction of these transmission networks are highly capital intensive.

Isaac Otolo
Infrastructure Industry Leader,
Partner,
Deals - Transaction Advisory
PwC Kenya

isaac.otolo@pwc.com

Peter Kiprono
Senior Associate,
Deals - Transaction Advisory,
PwC Kenya)

peter.kiprono@pwc.com

Fiscal constraints in most of the African governments limits their ability to invest in these transmission projects resulting in a major infrastructure deficit.

According to the World Bank, an average annual investment of between USD 3.2 billion to USD 4.3 billion is required in the power transmission sector between 2015 and 2040. To meet the required investment, private sector financing will be required to ease the financial constraints and bring their experience in project implementation and operation. Globally, several models have been adopted to attract

private sector investment in power transmission. The use of Independent Power Transmission in Brazil, Peru, Chile, and India enabled the development of approximately 100,000Km of new transmission lines by 2016. Additionally, many OECD member countries have privatized transmission and have since relied purely on private finance for new investment. These models include:

Independent Power Transmission (IPT)

IPT model provides rights and obligations associated with a single transmission line or a package of a few transmission lines for a period between 25-45 years. Africa can easily adopt the IPT model which is similar to the Independent Power Producers (IPP) model that has been used historically to finance power generation.

Currently, Kenya has adopted the IPT model for the development, financing, construction, and operation of the 400kV Lessos – Loosuk and the 220kV Kisumu – Musaga transmission lines. The Government of Uganda and Gridworks have also agreed to support the development of Uganda's transmission sector through private investment support. This will involve the upgrade of substations, which will solve capacity constraints at Tororo, Nkenda, Mbarara and Mirama.

Whole-of-grid concessions

Whole-of-grid concessions involve the transfer of rights and responsibilities from the state-owned transmission company to the private company for a period between 20-30 years. The winning bidder will be responsible for operations and management of the existing network and any investments relating to the transmission network.

Whole-of-grid concessions is applicable in countries that have a regulatory framework that allows for third parties to hold a transmission license. Although most African countries have not established an independent electricity regulator, they can adopt this model through regulation by contract where the government monitors the performance of the operator against the regulatory methodology and key performance indicators. This model has been used in Cameroon, Mali, and Senegal where the government retained a considerable share of ownership.

Merchant investments

Under merchant investments, investors build and operate one transmission line, which in many cases is a high voltage direct current (HVDC) transmission line. Compared to IPT where the concession term is between 25 to 45 years, merchant investments concession term is indefinite.

Despite the private ownership, merchant lines are still subject to technical compliance with grid code and regulations in the same manner as all power system assets. The commercial viability of a merchant line is dependent on its ability to capture value through power pricing arbitrage across markets or by selling its capacity to third parties. African countries with high power generation can adopt this model for inter-country transmission links to countries with high demand. There have been a limited number of merchant transmission lines globally since regulatory certainty is required for long-term investments.

Privatization

Under this model, the government transfers the ownership of the state-owned transmission company to the private sector within a defined geographic area. The government achieves this by privatizing all or part of the state-owned transmission company through a trade sale or a public flotation. The private party will then oversee the operations and management of the existing network and financing of new transmission investments. Full privatization of transmission networks is less common in developing economies.

Following the successful implementation of these models in different countries, Kenya can also adopt them to improve their transmission system.

For these models to work, the projects have to be bankable to attract private sector investments. A project is considered to be bankable when it's risk-return profile aligns with the investors' criteria and also the project can secure funding for development and implementation.

When assessing for project's bankability some of the key criteria's to be considered includes the project's probability of meeting the financial, environmental and social goals; whether the projected cash flows can cover the project costs and realize returns to meet the investors' expectations; the regulatory aspects of the project development and implementation; the value for money and affordability of the project both from the public entity's and end consumer point of view especially with rising interest rates and the resultant benefits of the project including ancillary positive impacts such as employment creation.

Designing an optimum risk-sharing matrix between the different parties in the project development is key in ensuring the bankability of these infrastructure projects. Credit enhancement mechanisms can assist to enhance the projects bankability and attractiveness to the private sector which can be from either the Government or financial institutions. These credit enhancement mechanisms include:

Short term liquidity support which lowers the credit risk borne by lenders and improve funding conditions by encouraging lower pricing and longer debt tenors. Examples include demand/revenue guarantees, partial risk guarantees (PRG's) and partial/full credit substitution.

Government support measures (GSMs) to mitigate against political and commercial risk, as well as deal with issues such as termination compensation. Example of these GSMs are Government's letter of support, escrow arrangements, letter of credit arrangements, ring-fenced funds, and political risk insurance.

The Government of Kenya is keen in introducing project preparation facilities (PPF) to provide support and enhance the bankability of infrastructure projects in Kenya.

Ultimately, the private sector plays a crucial role in bridging the financing gap for the transmission of power in Africa. Despite most governments opening the power generation to the private sector, transmission has been neglected leading to an unreliable power supply. Involving private operators could lead to significant cost efficiencies and improvement of power quality for utility networks that need massive upgrades and improvements.

Sources- World Bank, The United States Department of Commerce, Energy for Growth Hub

www.pwc.com/ke