

# COVID-19: A Business Impact Series

## Navigating the Pandemic: Top 10 Considerations for Business Assurance Leaders

Issue 7 | 11 May 2020

*There is a global effort to reduce the spread of COVID-19 and these efforts are impacting organisations regardless of industry and geography - some more than others. While we are hopeful that Nigeria and the world at large will emerge stronger from this significant challenge, we recognise the top 10 considerations for Business Assurance Leaders to prioritise in the review of their strategy during and beyond this pandemic.*

### Top 10 Considerations

Assurance Leaders should take into consideration the impact of the pandemic on businesses and adjust their strategy to respond to emerging risks triggered by COVID-19. The following are the top 10 considerations, their respective drivers and how business assurance leaders can respond to them.



### 1. Health and Safety

#### Drivers:

COVID-19 has raised concerns about how organisations are handling the safety of the workforce. While some companies are in total shut down due to the regulatory enforced lockdowns, other organisations for example in the retail sector, consumer markets, health sector, etc. have continued to carry on work albeit in skeletal arrangements in most cases.

The primary objective of assurance functions in providing assurance over Health, Safety and Environment should be to proactively drive business continuity and sustainability. The organisation could be exposed to a prolonged shut down and inactivity in the event of a staff being infected with the virus and is exposed to other staff. Consequently, organisations must ensure that safety is not compromised, by putting in place adequate safety measures amongst its employees in the work environment.

#### Response:

- Develop and execute an assurance program to periodically provide assurance that controls and procedures are operated in line with guidance from medical experts such as the Nigeria Centre for Disease Control (NCDC) and World Health Organisation (WHO).
- Evaluate the adequacy and effectiveness of the company's health and safety policies including hygiene programs, travel restrictions, social distancing practices, remote working policies and healthcare.
- Evaluate the adequacy of health and safety equipment including personal protective equipment, hand sanitisers, etc. and compliance of staff and all visitors with the Company's requirements.
- Identify health and safety improvement opportunities

### 2. Business Continuity and Crisis Response

#### Drivers:

While some organisations in Nigeria have a business continuity and crisis management plan, it is challenging to be fully prepared for a pandemic of this scale for various reasons as follows:

- Business continuity plans often focus on the impact of shorter-term scenarios, with the expectations that there is a known recovery timeframe.
- The underlying assumptions for many business continuity plans did not consider a pandemic of this scale; where there is a total lock down and restriction of



movement locally and internationally.

- Some of the business continuity plans do not cover all business operations and are limited to information technology. Consequently, a business impact analysis has not been done to identify all mission-critical activities across all departments and what needs to be done in the event any of the operations default.
- The business continuity plans have been rarely put to the test in a real crisis situation. Hence, some of the designed business continuity plans may not work at the scale it is required to in practice. For example, there are institutions whose information technology infrastructure are inadequate for the significant surge in remote working by its staff.
- Many business functions initially deemed “noncritical” as part of business continuity plans quickly become critical to the ability of the organisation to function, or even survive.

Currently, the pandemic situation is evolving and businesses are still grasping with the realities of the extent to which their operations may have been temporarily or permanently disrupted. This is not in consonant with the nature and profile of the crisis envisaged. For example, in more recent times, there has been an increased exposure to:

- Cyber crisis, including cyber security attacks or IT system outages due to greater connectivity and reliance on IT-systems.
- Government actions, for example, the enforced lockdowns that has reduced movement of goods and people, and consequently led to an increase in business disruptions especially for manual processes.
- Lower demand and purchase capability
- Data breaches and software errors that may cause irreparable damage to an organisation.
- Social issues, including unrest and looting of trucks on highway
- Foreign exchange crisis and a potential economic crisis as a result of the crash in oil prices

For these reasons, organisations require adequate planning covering immediate response, decision-making, recovery, communications and contingency plans for various scenarios which may suddenly arise. Assurance Functions have an important role to play in this regard as it has a bird’s eye view of all the company’s operations and their interdependencies. As a role that is independent of operations, assurance functions have the objectivity required to perform a professional assessment of the adequacy of the business continuity plan and advise accordingly.

#### **Response:**

- Facilitate or provide input into an enterprise risk and impact assessment to understand the company’s overall risk profile and determine the potential exposure and opportunities triggered by the current crisis. The extent of involvement of the assurance functions will vary based on the maturity of the function within the organisation.
- Conduct an independent review of the entire business continuity plan and crisis management system, including governance, processes and risks; and evaluate the quality and extent of coverage to meet the current crisis.
- Conduct a review of the effectiveness of business continuity and crisis responses plans against expected outcomes.

- Assess the leadership’s readiness for crisis situations by conducting a survey with key questions to determine the level of preparation for crisis situations.
- Evaluate the business impact analysis to provide reasonable assurance that the recovery time and point objectives are realistic.
- Using recent events in the media, knowledge of emerging risks and understanding of the business, facilitate or provide input into scenario planning workshops with senior management on the various situations that may arise.
- Identify opportunities for improving the business continuity plan. In time of need, assurance functions can also offer to play an active business continuity role where the roles that need to be occupied are understaffed. All pandemic-related activities conducted by assurance functions and the potential impact on the independence of the assurance function should however be disclosed to the audit committee.

### **3. Cash Flow Management**

#### **Drivers:**

The effective management of cash flow is considered to be critical during this period as organisations are facing issues such as; dwindling revenues, escalating costs, customers default in making payment when due, reduced production capabilities, low customer purchases and increased inventory lead times.

Given the rapidly changing economic circumstances arising from COVID-19, the 2020 cashflow budgets and forecasts prepared in 2019 may now be of limited relevance and requires a revision. It will be critical for companies to assess the impact of the current events and conditions on the company’s cashflow forecast, some of which may include:

- whether the company will have sufficient liquidity to continue to meet its obligations as they fall due
- whether it has sufficient cash and unused credit lines/ borrowing facilities to meet short-term needs.
- whether debt covenants are being met, to reduce the risk of lenders demanding immediate repayment
- re-negotiating with lenders to restructure and/or increase borrowing facilities.
- restructuring operations to reduce operating costs.
- deferring capital expenditure

Beyond the pandemic, other reasons for a renewed focus on cash and net working capital efficiency include:

- Rising finance costs;
- Pressure to meet market analysts’ expectations;
- Growing bargaining power of customers to improve payment terms in their favor;
- Increasing use of supply chain finance by large multinationals;
- Renewed focus of Senior Management on cash generation as a measure of success; and
- Growing use of net working capital measures in incentive or bonus schemes for management



## Response:

- Perform a review of the processes for managing, monitoring and reporting of cashflow.
- Review the basis of cash flow forecasts and predictions of supply and demand, taking into account the risk factors identified and the different possible outcomes.
- Conduct an independent stress test of the cashflow to evaluate whether the company can meet its debt obligations and debt covenants over the next 12 months, based on risk adjusted scenarios for operating, investing and financing activities.
- Review and assess periodic monitoring and reporting of key net working capital measures to enable decision making.
- Perform benchmarking of key cashflow and net working capital metrics against organisations of similar size, industry and location.
- Review the existence, adequacy and effectiveness of the company's contingency funding plan to ensure its liquidity risk triggers are adequate in light of the pandemic, and the sources of liquidity can sufficiently fund normal operations in the event of a liquidity crisis. The funding plan comprises the policies, procedures, projections and action plans designed to manage liquidity risk.
- Review the adequacy and effectiveness of controls in place to improve cashflow during the pandemic such as; the collection of account receivables, extension of account payable days, minimum cash balance, optimal banking of excess/idle funds, etc.
- Identify cashflow improvement opportunities.

## 4. Cost Optimisation

### Drivers:

The twin shocks of the coronavirus outbreak and drastic fall in crude oil price have caused a significant decline in the productivity and gross domestic product (GDP) of Nigeria alongside other economies. This has inevitably led to a fall in revenues and the need for most businesses to start reducing their cost in order to ensure survival and profitability of their business. Currently, organisations are trying to contain or reduce their costs through several means including:

- Reduction of expenditure budgets
- Renegotiation of contracts with third party vendors
- Conversion of fixed costs inputs to variable costs
- Tighter expenditure related policies and controls
- Integration and increase in weight of cost saving metrics into senior management's performance
- Downward review of payroll and other administrative expenses

### Response:

- Review the operating effectiveness of cost optimisation to identify if the designed mechanisms are functioning and verify that the current practices adhere to company policy.
- Conduct an independent review of the performance of each cost reduction initiative against set targets.
- Perform an independent supply chain optimisation review, evaluating various supply and logistic options,

and analysing the impact of changes in supply channels on costs.

- Conduct a value for money review on the top expenditures of the organisation. This may include benchmarking the amount paid for services against other competitive bids received by the company or within the industry.
- Review the adequacy and effectiveness of the organisation's procurement process, with a view to ensuring that goods and services can be efficiently procured at the most competitive cost in a transparent manner.
- Conduct an independent review of the company's recurring expenditures and their business case. For instance, the company may be incurring annual renewal fees for services that are not being enjoyed.
- Review the company's direct consumption (in terms of direct materials, labor, energy) to its productivity, with a view to identifying cost saving opportunities.
- Review the company's operational losses (particularly for those in manufacturing or mining) against permissible limits, with a view to identifying any excesses and ensuring the allowable losses are in line with industry standards.

## 5. Cyber Security & Data Privacy

### Drivers:

In a bid to control the spread of COVID-19, various governments have had to respond by restricting movement and enforcing lockdown measures across different locations. This has compelled both businesses and customers to opt for digital channels in carrying out their day-to-day operations and transactions which in turn increases the risk of cyber insecurity and data breaches. Some of the risk triggers may include:

- **A surge in internet and mobile app adoption**  
Many businesses have adopted remote working, which prior to now was an uncharted territory for many organisations and their employees. Hence, fewer security defences on home networks of employees working remotely and use of insecure virtual meeting platforms can create vulnerabilities in the systems.
- **An increase in social engineering susceptibility**  
The current pandemic is expected to increase anxiety and people are more likely to fall for malicious spams and phishing scams. Data analysed across several threat intelligence platforms show that there has been an upward trend in attempted COVID-19 themed malware and spam campaigns.
- **An increase in interconnectivity**  
In today's world of constant connectivity, hackers target organisations not only through networks directly but also through connections with third parties such as key suppliers and technology partners. Cyber security breaches can have dire consequences on an organisation's bottom line and reputation including:
  - Loss of cash assets
  - Loss of intellectual property and theft of confidential corporate.
  - Loss of new or existing business



Where the cyber insecurity results in a personal data breach, the risk further escalates into a regulatory one with potential sanctions due to the release of the Nigeria Data Protection Regulation (NDPR) by the National Information Technology Development Agency (NITDA) on 25 January 2019. The NDPR is a fundamental game changer which introduces guidelines on the use of personal data by organisations who collect and/or process such data. The NDPR also requires organisations to perform a Data Protection Audit and file a report with NITDA within a stipulated timeline. The potential impact of a breach of data privacy rights on an organisation's bottom line can be as high as 2% of a Company's gross revenue or N10 million (whichever is greater).

It is therefore not surprising that Executives assessed cybersecurity to be the No. 4 risk for businesses in Nigeria in 2020-2021. Based on the foregoing, there is a need for organisations to continually surpass the growing sophistication of capabilities and techniques used by hackers.

#### Response:

- Perform risk assessment of the organisation's information technology general and application controls with reference to leading practices and provide process improvement recommendations.
- Assess the cyber exposure of new and existing systems being used for remote access.
- Evaluate the adequacy and periodicity of company's information security awareness program to the employees within the company.
- Conduct anonymous surveys and simulate phishing activities to assess staff awareness of their information security responsibilities.
- Conduct penetration testing of the company's information technology network infrastructure.
- Assess adequacy and effectiveness of antivirus controls, security patches and firewall systems to ensure information systems within its network are reasonably protected from virus threats and up-to-date.
- Evaluate implementation of leading cyber security models such as multi-layered defense mechanisms, multi-factor authentication, enhanced security breach detection and data encryption methods.
- Evaluate the company's framework for ensuring third parties comply with minimum cybersecurity control requirements. This involves inclusion of information security policy and other required information in tender submissions, inclusion of cybersecurity requirements in relevant third-party contracts, etc.
- Evaluate the ability of third-party security providers to adequately address emerging cyber security risks. Assess third-party risks of vendors who provide support for critical systems, digital interfaces and channels.
- Evaluate the back-up of all critical systems and the integrity of back-ups in the event of a security breach or ransomware.
- Integrate NDPR requirements into the annual assurance program to assist the organisation in improving compliance, prior to external review and validation.
- Get connected to the organisation's NDPR response program, in order to provide input into its governance and implementation activities.
- Assess the impact of the NDPR on the organisation's

strategic goals and more specifically on the information governance strategy and budget.

- Identify cybersecurity and data privacy improvement opportunities.

## 6. Fraud

#### Drivers:

The increased adoption of remote working during this pandemic, is an uncharted territory for many organisations and their employees. Fraudsters can consequently leverage and exploit certain opportunities and loopholes created with the increased uncertainty induced by the COVID –19 pandemic. Some of the triggers for increased fraud during this period include:

- Increased reliance on virtual meeting platforms, due to the need to communicate while working remotely. These platforms may contain vulnerabilities that can be exploited by fraudsters.
- Increased use of e-signature, electronic letter-heads and emails to authorise contracts, invoice payments and other sensitive documents that are usually printed and physically signed; thereby reducing ability to authenticate documents.
- Use of personal devices and email accounts for business communication, which could be vulnerable to phishing attacks.
- Relaxed segregation of duties and controls, payment controls etc.
- Possible increase in falsification of records.
- Financial pressure on staff arising from pay cuts or job uncertainties, in light of the looming recession.

#### Response:

- Raise periodic awareness on fraud within the organisation, warning of the heightened risk of COVID-19 themed phishing attacks.
- Provide input into the policies and controls required to manage the new risks arising from flexible remote working such as the use of electronic approvals, e-signatures, use of personal devices.
- Review the effectiveness and compliance of the new policies and procedures developed as a result of changes to the working arrangements, triggered by the COVID-19 situation.
- Review the adequacy and effectiveness of controls surrounding electronic processing of invoices and payments. This includes segregation of duties, multi-factor authentication, additional confirmation by finance teams & banks to confirm any request for payments above a certain limit, etc.
- Review the adequacy and effectiveness of controls surrounding electronic collection and processing of documents from third parties. This can include testing to ascertain that invoices and sensitive information received from third-parties were not received from personal email addresses and were confirmed against previous communication with the third-parties before they are treated.
- Review the adequacy of the process in place for confirming e-signatures and conduct a sample verification of e-signatures by comparing them against signature mandates or seeking confirmation from the supposed authorisers.



- Conduct an independent review of changes in third parties' bank account details or email addresses within the ERP database.
- Review establishment of daily payment limits with each bank to ensure that they are in line with the Board's current risk appetite and economic realities.
- Evaluate segregation of duties controls for electronic operations to ensure that it is not too relaxed.
- Conduct an independent review of payment systems to determine whether fraud and cyber risks are adequately managed, and identify any opportunities for automation and centralisation.
- Test the whistleblowing channels to ensure that they are active, operational and available for stakeholders to report any form of fraud or misconduct.

## 7. Digitisation

### Drivers:

Digitisation and emerging technologies are allowing organisations to operate more effectively and are impacting the way people live and work. These technologies are increasingly becoming the new means of doing business during the pandemic and beyond.

Growing pressure on the efficiency, effectiveness and the need to give customers improved user experience continues to drive organisations towards digitisation and automation. Consequently, the increasing use of robotics, machine learning, artificial intelligence, advanced analytics, internet of things and other elements of industry 4.0 are driving a new form of business transformation.

Organisations now face a wealth of opportunities to identify and capitalise on these technological advances to drive change and innovation across markets and industries. However, with each evolution in technology comes challenges that companies need to stay on top of to optimise the impact and mitigate any risk surrounding its implementation and use. Some of the associated risks include:

- Business exposure to cyber fraud
- Non-reconciling items with digital payment channels
- Protection of personal data and intellectual property
- Operational downtime and disruption
- Skill shortage of experienced personnel to implement and operate highly automated processes
- Poor customer satisfaction due to delayed deliveries, poor customer service, questionable return policies,

Without proper understanding of these technologies and security measures, the full benefits of such technologies, may not materialise and thus lead to increased exposure to operational, financial and compliance-related risks.

### Response:

- Evaluate the existence and adequacy of a digital transformation strategy to enable the organisation digitally transform its processes and service offerings over time. Where a strategy exists, assess the value realisation from the program.
- Provide input into the design and implementation of digital processes and systems from a governance, risk and control point of view.
- Assess the adequacy of governance and control frameworks over the implementation and periodic

updates of digital processes and systems.

- Review policies and procedures around the management of technology, including governance and controls, data integrity, security, privacy and third party service providers' compliance.
- Conduct a post implementation review of newly implemented digital systems and processes.
- Ensure that digital processes are functioning optimally with the minimum amount of human intervention by conducting periodic tests to assess the effectiveness and accuracy of automated processes.
- Leverage data and analytics using the increased availability of electronic data from the organisation's digital systems to conduct reviews and provide a higher level of insights.
- Conduct an assessment of the organisation's existing and emerging technology systems usage in relation to industry standards.
- Evaluate changes in the business model and related changes in the control structure, that may result from adopted technologies.
- Identify opportunities for improving the company's use of technology and digitisation processes.
- Review the ordering and delivery system to ascertain compliance with laid down policies.
- Review the mechanisms put in place for effective customer engagement and monitor social media risks.

## 8. Foreign Exchange

### Drivers:

Based on the top 10 business risk survey conducted by KPMG Nigeria in December 2019, foreign exchange volatility was assessed by executives to be the third most significant risk for businesses in Nigeria in 2020- 21. Executives are significantly concerned about foreign exchange volatility and its impact on profitability. Following a decline in crude oil price, the ravaging impact of the coronavirus pandemic on the global economy and the recent currency adjustment of the Nigerian Naira; uncertainty about a further devaluation continues to weigh on corporates. Some of the key drivers for an increased risk of foreign exchange volatility include:

- Oil price, which is expected to remain weak throughout the year, as pressures continue to build in the global market due to the low demand triggered by the COVID-19 and oil price war between Saudi Arabia and Russia.
- The continuous decline in the country's foreign reserves.
- Collapse in investor confidence in the wake of the COVID-19 crisis, global financial conditions and decline in foreign portfolio investment to emerging markets.

### Response:

- Provide independent input into the scenario planning exercises where different exchange rates are simulated for transactions prior to decision making. This is to ensure that the scenarios are adequately risk adjusted and reflect the potentials of currency devaluation.
- Provide independent input into the cost-benefit analysis conducted by management, prior to the adoption of hedging instruments such as futures and forwards.
- Review the adequacy and effectiveness of controls.



- Review the company's exposure to foreign exchange and evaluate adequacy/effectiveness of controls designed to mitigate them. The company's strategies can include exportation of products, local sourcing, conversion of foreign denominated loans, etc.
- Identify opportunities for reducing the company's exposure to foreign exchange volatility.

## 9. Credit Management

### Drivers:

During this period, effective credit management will be critical. Debtors may delay payments as much as possible to boost working capital while others may default due to deteriorating business conditions. Some critical drivers that makes credit an important consideration during this pandemic include:

- Increased risk of debtors' default thereby increasing bad debt to a company.
- Increased risk of non-compliance with internal policies for approving credits in a desperate effort to grow business and revenues amidst a receding economy .
- Increased risk of non-compliance with internal policies and regulatory requirements in the course of restructuring debts. Customers with sufficient business case may be availed longer debtors' days, additional facilities etc. during this period.

### Response:

- Provide input into the development of an objective criteria for restructuring existing credit facilities with customers or revising the process for granting new credits.
- Review the process for approving and extending credits to ensure compliance with the existing or revised terms of the organisation.
- Review the adequacy and effectiveness of credit recovery and collection process.
- Ascertain the existence of sufficient collateral (where applicable) and the state of their perfection.
- Review the applicability and adequacy of existing credit agreements. Are there legacy customers that do not have agreements in place? or who have agreements with outdated terms and conditions?
- Review the process of writing-off receivables from the books to ensure compliance? Are there impairments that are yet to be made in line with IFRS 9 and other requirements? On the other hand, are there loans that have been written-off that do not meet write-off requirements?
- Assess compliance with the regulatory process put in place for restructuring credits.
- Analyse the critical credit exposures of organisations and approved credit concentration limits, and make recommendations to management.
- Identify opportunities for improving the Company's credit management process.

## 10. Financial Reporting

### Drivers:

The COVID-19 coronavirus pandemic has evolved rapidly in 2020 and the impact not only affects business operations but also extends to financial reporting. Many organisations will want to know the impact of the pandemic on their financial position, and what adjustments or disclosures will need to be made in periodic financial reports. Depending on a company's reporting date, the impacts of the COVID-19 outbreak could be adjusting or non-adjusting events. Examples of financial reporting issues that may come up for organisations include:

- Financial and non-financial assets may be impaired, as a result of parties not meeting the payment requirements when due, liquidity constraints, or a fall in fair value of the asset based on market conditions for non-financial assets.
- Restrictions of movement arising from COVID-19 has caused disruption to manufacturing, workforce, supply chain facilities, among others and these could have an impact on the carrying value of company's inventory items.
- Revenue forecast may be unrealistic post COVID-19.
- Valuation of associates and subsidiaries in areas severely affected with COVID-19 may need to be relooked. A number of investments may be impaired.
- Fair value measurements may have been based on forecast cashflows, which will need to be reassessed.
- The need to assess whether events or conditions triggered by the pandemic, cast significant doubt on the company's ability to continue as a going concern. In severe cases, the appropriateness of using a going concern assumption as a basis for the preparation of the company's financial statements will need to be evaluated.

### Response:

- Review the impact of changes in the business environment on the financial statement, highlighting areas that need to be adjusted for in line with IFRS.
- Provide professional advice on the impact of the pandemic on accounting treatments and financial statements of the organisation.
- Provide input into impairments of financial and non-financial assets to ensure they are fair and reasonable.
- Review the financial reporting process with a view to ensuring compliance with international financial reporting standards.
- Assess how realistic and achievable the plans to mitigate events or conditions that may cast significant doubt on the company's ability to continue as a going concern are.



## Economic and Regulatory Updates

### CBN Restarts Dollar Sales to SMEs, Students, PTA

The Central Bank of Nigeria (CBN) said it has resumed sales of dollars to SMEs who need foreign exchange for essential imports, as well as Nigerian students in foreign schools who need to pay their school fees. This comes as the world-wide COVID-19 lockdown begins to ease up, even as business activities are expected to gradually return to normal.

### Naira Drops to ₦387.25 at Investors' and Exporters' Window

The exchange rate between the naira and dollar depreciated to ₦387.25 at the Investors' and Exporters' (I&E) window closing the week lower as investors scrambled for forex supplies. The exchange rate at the I&E window differs from the CBN's published exchange rate which is currently stated at ₦360/\$1. It is also different from the exchange rate at the black market which is closed at ₦445/\$1 according to other media sources.

### Analysts Forecast When Nigeria's Bonny Light Could Hit \$50

If the surge in oil prices continue, oil experts expect the price of Nigeria's crude oil, the Bonny light, to stay above \$35 for Q3 and Q4, 2020. According to Professor Adeola Adenikinju, Director, Centre for Petroleum, Energy Economics and Law (CPEEL), University of Ibadan, "It will pick up to mid-\$40s or low \$50s in 2021. However, Nigeria may not be able to fully take advantage of the increase because of production cuts that OPEC would need to maintain to sustain the market."

### NSE Ranks Second in Bloomberg's Best Performing Indexes Over the Past Month

The Nigerian Stock Exchange has enjoyed significant rallies in recent weeks, even amidst the global Coronavirus (COVID-19) pandemic. As the Exchange sustains remote trading, free flow of information and vibrant market activity, the index has accelerated +16.39% in the past month and ranks second in Bloomberg's best performing indexes within the period. Total Market capitalization at the NSE now stands at ₦12.6 Trillion as at 07 May 2020.

## Our Latest Publications



### COVID-19: The Central Bank of Nigeria (CBN) Support Measures

COVID-19 pandemic has put pressures on policy makers and supervisory institutions across the globe, sparking off a number of mitigating initiatives by government agencies to combat the potential negative social-economic impacts on households and businesses. For more details, please follow this link: <https://bit.ly/2WDKx0E>



### COVID-19 and the Nigerian Telecommunication, Media and Technology (TMT) Sector

With over 3 million cases of the Coronavirus disease (COVID-19) and staggering casualty figures globally, the pandemic has indeed reached dreadful proportions, leaving trails of economic woes, even in the most advanced countries. The pandemic has indeed affected every sector of the Nigerian economy including the telecommunications, media and technology (TMT) sector. For more details, please follow this link: <https://bit.ly/2WHGkVa>



For feedback and enquiries, please contact:

**Tomi Adepoju**

T : +234 1 271 8950

E : [tomi.adepoju@ng.kpmg.com](mailto:tomi.adepoju@ng.kpmg.com)

**John Anyanwu**

T : +234 803 975 4061

E : [john.anyanwu@ng.kpmg.com](mailto:john.anyanwu@ng.kpmg.com)

**Tolu Odukale**

T : +234 1 280 5976

E : [tolulope.odukale@ng.kpmg.com](mailto:tolulope.odukale@ng.kpmg.com)

**David Okwara**

T : +234 708 383 3853

E : [david.okwara@ng.kpmg.com](mailto:david.okwara@ng.kpmg.com)

**Seun Olaniyan**

T : +234 1 280 9212

E : [oluwaseun.olaniyan@ng.kpmg.com](mailto:oluwaseun.olaniyan@ng.kpmg.com)

[home.kpmg/ng](http://home.kpmg/ng)

[home.kpmg/socialmedia](http://home.kpmg/socialmedia)

