DATA-FIRST THINKING

FINANCIAL CRIME IN SUB-SAHARAN AFRICA 2020
World-Check®

Uncover risk. Take action.

A powerful combination of data, technology and trusted human expertise to help:

• Simplify and accelerate risk screening
• Meet regulatory obligations
• Protect against financial crime risk

refinitiv.com/world-check
CONTENTS

Introduction ......................................................................................................................................4
Industry voice ..................................................................................................................................6
About the report .............................................................................................................................8
Trends ................................................................................................................................................9
1. Go beyond ticking the boxes ................................................................................................ 11
2. The constant threat of de-risking ............................................................................................... 15
3. Sanctions: A fast-moving situation ............................................................................................. 21
4. Opportunity and risk in African supply chains .............................................................................. 29
5. Innovative technology: Change is coming ..................................................................................... 34
Survey results ................................................................................................................................ 41
Welcome to Refinitiv’s inaugural Financial Crime in Sub-Saharan Africa Report, part of our ongoing commitment to bring the latest insight and intelligence relevant to compliance practitioners and senior executives in the region.

This report is based on a survey of well-informed and experienced individuals across the region. More than 60% of our sample has experienced some form of financial crime in the past five years and 52% work in a multinational organization. The insight gained from their responses will prove invaluable as you look to benchmark and enhance your own risk and compliance programs.

As our report highlights, the threat landscape continues to evolve, and the techniques used by organized crime groups and fraudsters are becoming more diverse and more sophisticated. Identity theft and, what we term, “green crime” are fast growing criminal markets. These are unwelcome threats for many countries in the region; which are not only embracing mobile technology but also home to a variety of wildlife and natural resources.

Indeed, Africa is at the forefront of embracing mobile technology and is host to more than half the world’s mobile money services. With this increased mobile access comes the threat of identity theft and money-laundering. In response, digital identity technologies, including those of Refinitiv, are quickly evolving to meet this need and as our survey reports, a quarter of respondents have already adopted digital identity solutions.

The region is home to a diverse range of wildlife and plants, as well as natural resources and this has increasingly become the target of organized crime. We are seeing a robust regulatory response to the increasing threat of “Green Crime” the European Union has included environmental crime as a predicate offence under the 6th EU Anti-Money Laundering Directive (6AMLD); and the Financial Action Task Force (FATF) priorities for 2020 will focus on illegal wildlife trade.

Green crime will inevitably become a growing focus for the compliance and risk functions. Technology and data have a crucial role to play in disrupting green crime networks, but the problem also requires a concerted effort to bring big companies, regulators, politicians, and charities together in order to meet the challenge.

I am acutely aware that Refinitiv has released this report at a time when the world finds itself grappling with a new and rapidly growing threat in the form of the COVID-19 virus. While our survey was conducted prior to the crisis, I have little doubt that the trends we have identified remain highly relevant.

With the arrival of COVID-19, the threat landscape has changed significantly, increasing the risk of financial crime and in particular supply-chain fraud and cybercrime.
In response to the crisis, regulators have shown a greater degree of flexibility concerning the adoption of technology to help combat the criminals seeking to profit from the pandemic and to support continuing access to critical services during a period of social distancing.

FATF has issued guidance encouraging the use of digital customer onboarding and simplified due diligence in the delivery of digital financial services given the social distancing measures being enforced around the world. We have since seen numerous regulators around the world follow suit, issuing their own statements supporting such action, including the including the UK’s Financial Conduct Authority (FCA), Hong Kong’s Monetary Authority (HKMA) and The Financial Crimes Enforcement Network (FinCEN) in the U.S.

Much of the regulatory guidance points to the use of robust technology and trusted data for Know Your Customer (KYC) and identity verification of customers, to help streamline client onboarding and screening aligned to the organizations risk policy.

The shift towards digitalization is a theme that comes through very clearly in our report. The pace of this transformation is likely to have accelerated in response to COVID-19 and it is unlikely to diminish once we exit the pandemic.

Forward-thinking compliance functions will be focussed on how they can best make the transition towards digital channels and tools, while ensuring the needs of their business and customer base are accounted for and their regulatory requirements are fully addressed. With 66% of SSA respondents embracing innovative technology and 90% expecting their financial crime technology to change in next two years, this will be an interesting trend to track.

I highly recommend that you review the findings of this report and I am confident the insights it offers will usefully enable you to evaluate your compliance program against a background of new and emerging threats.

Join the conversation #FightFinancialCrime
Shifting from a rule-based to a risk-based approach created quite an uproar in the non-banking financial industry. Understanding the impact on systems, processes and doing business was enormous.

Obtaining buy-in from the board and senior management required extensive communication. This was a vital starting point to embark on a huge challenge. At the beginning, it was not completely clear how big this challenge was. Since limited research was available on the ‘how to’ of a risk-based approach for the non-banking financial industry, each organization was left to make its own difficult decisions.

Building a culture of guarding against financial crime in a large international organization must start with the board and senior management. They should understand the regulatory requirements, penalties for non-compliance, personal liability, and their organization’s unique money laundering and terrorist financing risks. These leaders are required to advocate that complying to the organization’s Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) obligations is in the interest of the organization and its shareholders, and should be embedded into all its operations.

Management that understands the requirements support the need for tools and resources to implement effective controls to manage the risk of money laundering and terrorist financing. The organization’s internal audit and compliance monitoring departments should support compliance with its AML/CFT obligations. They must also give regular feedback to the board and senior management. Establishing a risk-based culture takes time and requires ongoing awareness.

Innovative technology has been incredibly helpful in implementing the requirements for fighting financial crime in our organization. However, this comes at a cost. Identifying a system and finding the right software package has its challenges, especially in a non-banking environment. Most solution providers are acquainted with banking requirements but not other financial industries’ requirements. You need to be very clear on your requirements, expected results and find out if the system you’re looking into is flexible enough to be customised to meet your requirements. Otherwise, your money laundering and terrorist financing risks might not be mitigated adequately. Developing ‘tuning scenarios’ requires several testing iterations to illuminate the possibility of missing risks or getting too many false positive alerts. To identify ‘red flags’ requires extensive understanding of your business, trends and typologies. This list will never be an exhaustive list of tried and true indicators in identifying suspicious scenarios.
It is all good and well to set up a system that produces the expected outcome, but do not underestimate the importance of the ongoing monitoring and analysis of the system. It is important to use data analytics, machine learning, and process automation to improve the efficiency and effectiveness of screening, risk rating and transaction monitoring. Your system is only as good as its ability to adapt to the emerging and identified money laundering and terrorist financing risks.

Digital identification and verification have become a significant part of the customer onboarding process across all industries. This speeds up the client experience. By using independent data sources, it also minimises the risk of accepting a fraudulent identification document. Furthermore, it is of great value to validate previously obtained information if the data or documents are questionable.

Finding a reputable service provider requires a bit of exploration to ensure they can meet your requirements and have effective back-up data sources in the event of a data source not being available. You should have a clear understanding of their matching criteria to prevent getting more failures than confirmations. It is advisable to make use of ‘golden sources’. Ensure that the required data security is in place when using a third-party provider.

Managing the risk of money laundering and terrorist financing in a non-banking financial industry has its challenges. But with a good understanding of your risks, ongoing analysis to assess the impact and likelihood of financial crime, robust controls embedded in operational processes, and staying abreast with trends and typologies, makes this task possible.

This is why survey reports such as this one, the Financial Crime in Sub-Saharan Africa 2020 report, is so interesting to read. It presents a good opportunity for senior managers and business leaders to understand industry norms and standards in a dynamic and ever evolving regulatory situation, and allows them to benchmark their own processes.
ABOUT THE REPORT

Typical respondent

44% RISK PROFESSIONAL

25% BUSINESS OWNER/MANAGERS/BOARD MEMBER

50% IN A COMPANY WITH 250+ EMPLOYEES

52% IN A MULTI-NATIONAL ORGANIZATION

66% HAVE EXPERIENCED FINANCIAL CRIME OVER THE PAST FIVE YEARS

First survey report in a longitudinal series on financial crime in Sub-Saharan Africa.

Survey responses reveal that Africa-based executives face the same issues that concern compliance departments around the world – how to cope and make sense of an overwhelming flow of data while the regulatory environment bends, shifts and grows ever more complex and demanding. Fighting financial crime has become a global priority, and meeting the compliance challenge is a demanding task.

As the pressure to meet compliance obligations increases, many respondents are looking to technology for help: 90% expect their investment into technology to increase over the next two years, and 62% say that they are seeking better management and analytical capability from their technology. Innovative technology, including cloud computing, artificial intelligence and digital identity, has been widely embraced. Only 9% of respondents, however, focus on the issue of data quality, a vital element in the fight against financial crime.

61% expect a substantial increase in compliance investment

90% expect their financial crime technology to change in the next 2 years

62% desire better data management and analytical capabilities from their technology

28% say reputational degradation is their biggest concern

28% say internal behavioral change is their biggest challenge
5 TRENDS AND HIGHLIGHTS

The constant threat of de-risking
61% expect a substantial increase in compliance investment
An unfortunate by-product of increasing regulatory pressure is the redlining of correspondent banking relationships in sensitive geographic locations. There are, however, concrete steps that can be taken to signal a serious commitment to compliance to the international banking community, and therefore, reduce the risk of relationship breakdown. While there is an increase in compliance activity and investment, there also appears to be a lack of commitment to compliance obligations. For example, asked where their focus would be in terms of compliance activity over the next two years, only 14% of respondents chose regulatory monitoring, which potentially exposes the organization to heightened risk.

Sanctions: a fast-moving target
43% have a sanctions program
Failure to have a comprehensive sanctions program potentially exposes Africa-based organizations to risk of sanction breaches and potentially significant fines as a result of enforcement actions.
Sanctions are complicated, fast-evolving, contradictory and globally fragmented, and non-compliance risk has increased substantially. The results of our survey showed a weak response in this area, yet Africa-based organizations can be especially vulnerable and exposed due to the emergence of green crime, such as wildlife trafficking and illegal logging, as a growing global concern.

Opportunity and risk in African supply chains
74% have a KYC program
Bribery and corruption emerged as a top concern for respondents. As trade barriers fall and economic opportunities become increasingly accessible, we will see a growth of supplier networks. While this creates considerable opportunities, there should also be an awareness of the inherent risks that lurk in supply chains, and the increasing focus of regulators on money laundering and related risks. Supply chain risk management requires a rigorous response.

Go beyond ticking the boxes
28% say driving internal behavior change is their main challenge
Regulatory compliance has become so complex that it demands a comprehensive response. Compliance executives should not be lulled into a false sense of security because they have invested into the most up-to-date, sophisticated technology. Regulators expect so much more.

Innovative technology: change is coming
66% have embraced innovative compliance technology
The search for smart technology that can greatly reduce the increasing burden of compliance, is a focus of compliance executives around the world. Africa-based organizations have been hampered in the past by a lack of telecommunication infrastructure, but this lack of infrastructure may also present an opportunity to leapfrog the many developmental phases of technology. Of particular interest is digital identity, a potential game changer that over a third of respondents have already embraced. The entrepreneurial spirit is strong in Africa, and there is reason to be positive.
Without insight and careful consideration, committing a substantial portion of the compliance budget to technology may fail to produce a good return on investment.
Awareness of the need for regulatory compliance has grown in Sub-Saharan Africa. The impact of global bodies such as the FATF, one of the most influential anti-money laundering and counter terrorism financing agencies, is growing across the continent.

The FATF recommendations and regular policy guides have been instrumental in guiding policy makers throughout the world, influencing not only its membership base but other governments that seek to integrate their economies. Many Sub-Saharan African countries are members of the FATF, indicating a commitment to good governance. South Africa has been a member since 2003 and over a third of Sub-Saharan African countries have been members since 2010 due to their membership in the Eastern and Southern Africa Anti-Money Laundering Group (ESAMLG).
Recent trade agreements such as the African Continental Free Trade Area (AfCFTA) facilitates trade between its 28 signatories¹ and this growth in trade will help to promote the spread of governance norms and standards promoted by FATF and other global bodies. The drive to integrate economies will greatly encourage the achievement of norms and standards that have long been accepted practice in major financial centres around the world.

We see this increasing regulatory pressure reflected in a number of responses:

- 90% expect their financial crime prevention technology to develop over the next 2 years (Q12)
- 62% said the main reason they would invest in a technology upgrade is for better data management and analytical capabilities (Q25)
- 66% have embraced innovative technology to help them meet their compliance obligations (Q14)

The increasing use of technology in compliance, however, implies a possible risk of over reliance on software to solve compliance challenges. Sophisticated technology helps to reduce repetitive tasks and supports, but should not replace, decision making. Human intervention is a critical element of an effective compliance policy and many organizations have fallen foul of regulations due to complacency, a false sense of assurance that the compliance task is complete due to costly compliance technology. 

### Box ticking heightens risk

Indeed, the challenge of meeting regulators’ expectations has grown increasingly complex in recent years, and costs have increased substantially. It’s been a long time since compliance was a back room, tick box function, a task completed by a junior accounting or auditing professional. Today, meeting regulators’ expectations requires a combination of skill, constant scrutiny, human intuition and appropriate software.

### Consider policy carefully

Choosing compliance technology that can cope with an evolving regulatory focus is challenging and should take into account organizational risk appetite, as well as current and future goals. Without insight and careful consideration, committing a substantial portion of the compliance budget to technology may fail to produce a good return on investment.

We note, for example, that only 9% of respondents said that data quality was their focus of investment to meet compliance objectives (Q13). The quality of data can make a substantial difference to the number of false positives produced during screening and therefore the amount of time, and money, spent on remediation. Without data that has been de-duplicated, carefully checked for error and networked to reveal relationships, sophisticated technology that promises faster processing speeds will probably produce a high volume of false positives, and any time saved will be lost to the burden of remediation. Investing time to carefully research rather than money when choosing compliance technology can substantially reduce the burden of cost in the long term.

---

¹ Forty-four African countries sign a free-trade deal, The Economist, 22 March 2018
**Build consensus**

Best practice compliance requires a company wide approach, and this may require a mental shift for senior managers. Responses indicate a resistance to transformation – when asked what their main challenge was in terms of compliance management over the next two years (Q19), the majority, 28%, said that it is “driving internal behavior change”. It is helpful if employees and stakeholders understand the organizations’ commitment to compliance and their role in achieving regulatory obligations. Without a holistic, company wide approach, the compliance task will remain the responsibility of a single department only. The task of uncovering risk will rely on specific, basic compliance processes, and today, regulators expect more from organizations.

**Create a supportive culture**

A company wide approach and a shift in mind set requires visible leadership, however. Responses show that there is a perception of a lack of support from senior management. Questions about confidence levels (Q21, 27) revealed a large proportion of respondents lack confidence in their compliance systems in general, and specifically their technology solutions. When asked for reasons for a lack of confidence (Q22), the number one reason given by nearly half of all respondents was ‘lack of management support’.

A ‘lack of specialist resources’ was also frequently cited, the second most common answer. There is a sense of frustration around the challenge of managing data in the pursuit of compliance obligations, and responses (Q10) reveal that the most challenging aspect of onboarding and monitoring business relationships is data management and knowing their customers.

A crucial element of a best practice compliance policy is the role played by senior management. Their attitude towards compliance, their daily actions both in and out of the office, their communication around the issue of compliance, all contribute towards a ‘tone’ within a company. With the task of compliance shifting to a more central position within organizations, setting the right tone has become a critical factor to the success of compliance, and overall success.
Deliberate steps on this issue demonstrates a visible commitment to compliance, and it is increasingly recognized by regulators as a critical element of a successful compliance policy. Setting the right tone starts with the board and includes the senior management team. A leadership team has the ability to signal a commitment to ethical governance and adherence to the spirit of ABC/AML compliance through the composition of its board, ensuring that its members are fit and proper to govern.

An organization can have a gold-plated compliance policy that reads well and looks good on paper, but unless there is visible, demonstrable commitment to this policy from the top, it may not reduce their exposure to risk as much as expected. Compliance is central to the health of an organization; it is a passport to other opportunities further afield. In a time when de-risking is rife, the need for a visible commitment and ethical behavior cannot be understated.

HOW TO BUILD AN APPROPRIATE TONE:
REINFORCE THE MESSAGE

Define it – an important first step as it cannot be assumed that values and priorities are always shared, regardless of how homogeneous the community. Companies often operate across jurisdictions and may have stakeholders in remote locations with values that are not always aligned with those of the host organization. While not wrong, it is important to set the standard of behavior according to the context in which the organization will be judged by regulators.

Create a reward system for appropriate behavior – look for opportunities to put a spotlight on principled behavior and reward this in the same way a sales team that hits its target is rewarded.

Emphasize specific ethical behavior in succession planning – ensure that employees who are being groomed for future leadership positions understand that ethical behavior is an important component of the corporate ladder.

Escalation policy – consider how issues and complaints are dealt with internally and ensure that employees feel safe to escalate an issue. Consider how dissenting views are handled. If there is some kind of wrongdoing that has occurred, it is beneficial to the organization that this information reaches the senior management team sooner rather than later.

Communication – regular information session and workshops on the topic of compliance will help to support the message from senior management and ensure that the topic is kept front of mind.
Non-compliance or weak compliance carries substantial risk for banks and financial institutions. Not only is there a risk of losing clientele and business, reputational degradation, and censure and financial loss, but there is a credible risk of loss of correspondent banking relationships. This phenomenon, known as de-risking, has become a reality for many banks around the world, especially those located in geopolitically sensitive regions.

SWIFT data from 2011 to 2019 shows a decline in active relationships in the global correspondent banking network by about 20%, and a decline in active corridors of 10%. An active corridor is defined as a country pair that processes at least one transaction\(^2\).

\(^2\) *New correspondent banking data - the decline continues, BIS, 2019*

The pressure on banks to conduct a high level of due diligence on a broader section of their client data has grown significantly.
Banks in various regions around the world are experiencing a decline in correspondent banking, but some regions are more vulnerable than others. The loss of a correspondent banking relationship has the potential to substantially impact operations and could result in a loss of banking license and eventual closure.

**Pressure builds to reduce risk**

The pressure on banks to conduct a high level of due diligence on a broader section of their client data has grown significantly. For some compliance departments, this task has become overwhelming, so much so that instead of putting appropriate controls in place, they have preferred to draw a red line under any organization in a location within a high-risk geographical location.

Africa-based financial institutions will understand this risk due to a persistent perception of the continent as a high-risk location. We have witnessed a growing number of financial institutions, lacking the necessary resources to cope with the onboarding process, opting for this blanket ‘de-risking’ approach. This is unfortunate, instead of controlling money laundering and financial terrorism risk on a case-by-case basis, these banks simply avoid risk by restricting business relationships with entire categories of customers, industries and regions.

Should a financial institution lose a correspondent relationship, it goes without saying that its operations may be severely curtailed.

Some of the responses to question 7 show a mixed response to compliance and in some places a lack of urgency.

For example, only:

- 32% have a policy to understand Ultimate Beneficial Ownership (UBO)
- 43% have a sanctions policy
- 54% have a whistleblower protection policy

The highest rated compliance policies include:

- 74% know your customer
- 73% anti-money laundering
- 70% anti-bribery and corruption

Asked (Q9) what their concerns were in terms of financial crime, they chose fraud, ABC and cybercrime. The bottom three choices included CFT, sanctions and trade based money laundering.

**Developing economies are vulnerable**

Many countries in Africa have seen a reduction in the number of foreign correspondent banking relationships. According to a report published in 2016, ‘Addressing the unintended consequences of de-risking – Focus on Africa’, the number of foreign counterparties fell by over 10% across the continent between 2013 and 2015.

Not only is de-risking disastrous for individual organizations, it is harmful to the global financial system in general.

In a keynote speech in March 2015, the FATF Vice-President Je-Yoon Shin warned that “de-risking can itself introduce risk and opacity into the global financial system, as the termination of account relationships has the potential to force entities and persons into less regulated or unregulated channels”.

---

3. *Addressing the unintended consequences of de-risking – Focus on Africa*, 2016, SWIFT.COM
Unfortunately, financial exclusion has a habit of pushing marginalised individuals and organizations to look outside legitimate channels for relationships that will facilitate financial products and solutions. This works against the goals of the regulation that led to the de-risking in the first place.

It is therefore a situation best avoided.

**Derisking can be avoided through action**

Proactive institutions will make choices that signal to the international banking community that they have strong controls and a robust compliance framework in place. We see encouraging signs amongst some of the responses that there is a growing awareness of the importance of committing to an effective compliance policy.

Responses point to an awareness of the importance of meeting regulatory obligations. When asked what poses most risk to their organization (Q18), the most popular choice was ‘failure to meet regulatory obligations’ and the second ‘failure to invest in advanced technology’.

When asked if compliance activity has increased, what has been the focus (Q15), and what will be the focus (Q16), both questions had the same top two responses; investment technology and training and staff resources. Responses to earlier questions (Q11 & 12) also reflected an awareness of the need to invest in compliance systems in general:

- 55% said there had been an increased investment in compliance
- 61% said they expect an increase of over 25% in investment over the next two years

---

**FATF STATEMENT ON DE-RISKING, OCTOBER 2014**

“The FATF Recommendations only require financial institutions to terminate customer relationships, on a case-by-case basis, where the money laundering and terrorist financing risks cannot be mitigated. This is fully in line with AML/CFT objectives.”

“What is not in line with the FATF standards is the wholesale cutting loose of entire classes of customer, without taking into account, seriously and comprehensively, their level of risk or risk mitigation measures for individual customers within a particular sector.”

The impact of de-risking in any country can be significant, in developing economies, however, such as the economies of Sub-Saharan Africa, it can be devastating. It can result in the exclusion of entire communities and business sectors from the regulated financial system. This may not stop the flow of money but may push it underground, an entirely different result from what regulators envisioned.
Technology, skills, processes are key

While financial institutions tend to lead the way in terms of innovative technology, ideally, a bank would have key compliance skills at every level of the organization to ensure that sufficient information is gathered on the potential client’s business and AML/CFT controls, as well as the client’s commercial and personal relationships, reputation, history of regulatory action and association with money laundering or terrorist financing investigations.

Training and skills are key to the quality of supervision and AML/CFT controls, and therefore impact on the reputation of the institution as well as the potential for any regulatory action.

For AML/CFT policies and procedures to be effectively applied, employees need to understand the bigger picture. This involves explaining the reasons why these processes are in place and the possible consequences of a breach. Compulsory AML/CFT training is a way to achieve this, but only if the training is high quality, relevant and in line with evolving regulatory developments. Once a culture of compliance has been entrenched, relevant staff can be given specialized training that helps to equip them to deal with money laundering and terror financing risks specific to their lines of business.

Ultimately, an Africa-based organization with strong compliance resources in place is better-equipped to navigate risk on a case-by-case basis and is therefore more attractive to potential relationships and less likely to fall victim to a de-risking strategy. Or, if they should fall victim to such a strategy, they are better placed to appeal the situation.

To help avoid de-risking:

- Ensure robust controls are in place that at least match, if not better, those of international peers
- Document all associated activity to show that policies are not only good on paper, they are put into practice
- Regularly review policies to ensure that they remain recent and review activity to ensure that complacency does not creep in
THE WOLFSBERG CORRESPONDENT BANKING QUESTIONNAIRE

In 2018, The Wolfsberg Group published a Correspondent Banking Due Diligence Questionnaire (CBDDQ) as well as associated guidance material. This was aimed at setting a standard for cross-border and/or other high-risk correspondent banking due diligence, and Wolfsberg members are encouraged to use the material as a guide in their respondent relationships. A standardized, reasonable CBDDQ should help to reduce the compliance challenge and result in a time and cost saving for financial institutions, as well as set a due diligence standard. In the long term this may support the objectives of the G20 and other supranational organizations to create more harmonized regulatory standard in correspondent banking, and thus create long term positive effects that will reduce de-risking and increase access to finance, the development of trade and financial inclusion.

5 Wolfsberg CBDDQ, The Wolfsberg Group, 2018
22% responded that they assessed their risk infrequently or not on a regular basis.
Several responses reveal that, for many Sub-Saharan African organizations, sanctions compliance has a relatively lower profile than other regulatory issues. Asked about their financial crime programs (Q7), over 70% said they had an ABC and AML program, yet only 43% have a sanctions program.

Asked about their major concerns (Q9), sanctions were rated among the bottom three along with CFT and trade based money laundering, while the top three concerns are fraud, ABC and cybercrime.

This could be due to a perception of weak enforcement on this issue. When asked what crimes their organization had fallen victim to (Q6), only 7% pointed to a sanctions breach. However, perceptions can be misleading, and it is risky for organizations to discount the issue of sanctions compliance.
**Fragmentation in global approach**
Sanctions regimes have become incredibly complex and difficult to forecast. Recent political activity has encouraged, in some quarters, the pursuit of national interests and a growth in geopolitical competition, and this growing polarization reflects in global sanctions activity. We have noted little sanctions activity from the United Nations (UN) in recent months and only slightly more activity from the European Union (EU). The U.S. Office of Foreign Assets Control (OFAC) and Treasury, on the other hand, have both been highly active in terms of issuing new and updating existing sanctions. This growing divergence in approach to the application of sanctions, while it may reduce the efficacy of a sanction’s regime, is contributing to an increase in complexity and risk for organizations that operate across borders.

OFAC is frequently updating its sanctions lists and issuing sanctions on oligarchs, kleptocrats, individuals in many countries, entities, and governments. The U.S. administration is also making use of secondary sanctions to put pressure on non-U.S. companies to stop doing business with countries that are under U.S. sanctions.

**Increased cooperation between authorities**
Given the rising profile of green crime and the transnational nature of many crimes, we expect to see an increase in cooperation between global authorities in terms of intelligence gathering and enforcement activity. A recent example of this is the recent combined operation between Europol and INTERPOL to combat the illegal trade of reptiles which involved a number of European countries and South Africa in an intelligence gathering operation. It resulted in hundreds of seizures and 12 arrests in the EU in June 2019, as well as the identification of almost 200 suspects around the world.

UNEP and Interpol estimate that the cost of environmental crime is around USD 258 billion annually, and growing steadily. Many crimes that fall under the banner of “environmental” are attractive to organized criminal groups due to relatively low input and high returns, as it’s easier to move fauna, flora and animal parts than human beings, for example. However, in 2015 the EU Commission linked environmental crime to other forms of organized crime such as money laundering and terrorism, and this will result in an increase of resources to combat the problem.

The degradation of the environment along with the very real threat of species extinction has brought a certain urgency to the task, and we note an increase in the number of sanctions that have been instituted against individuals and entities that are involved in this illegal practice, and the potential for more.

**Increasing risk of environmental crime**
Over the past five years, as a result of the work of international agencies such as the United Nations Environment Program (UNEP), environmental or green crime has become an increasing focal point for regulators and enforcement authorities.

UNEP and Interpol estimate that the cost of environmental crime is around USD 258 billion annually, and growing steadily. Many crimes that fall under the banner of “environmental” are attractive to organized criminal groups due to relatively low input and high returns, as it’s easier to move fauna, flora and animal parts than human beings, for example. However, in 2015 the EU Commission linked environmental crime to other forms of organized crime such as money laundering and terrorism, and this will result in an increase of resources to combat the problem.

The degradation of the environment along with the very real threat of species extinction has brought a certain urgency to the task, and we note an increase in the number of sanctions that have been instituted against individuals and entities that are involved in this illegal practice, and the potential for more.

---

7 Global action against wildlife crime: 4,400 reptiles saved from criminal hands, Europol, 03 June 2019
THE UNEP IDENTIFIES THREE AREAS OF CONCERN:
environmental quality; biodiversity and natural resources,
and the underpinnings of the global ecosystem.

Africa is a known hotspot for certain illegal activities in the area of biodiversity and natural resources. Some regions across the continent are subject to the problem of illegal logging and timber trafficking along with an associated crime of charcoal trafficking. Illegal logging is a particular problem for Cameroon and the shipment of illegal wood is easily mixed with legally shipped wood, making it difficult to detect. Main destination markets include China, the EU and the U.S.

Charcoal, created by burning wood at a high temperature without oxygen, is a popular product in Africa and the Gulf countries. The main source of charcoal is countries such as Eritrea, Ethiopia, Kenya, Somalia, South Sudan, Tanzania, Uganda and its destination markets include Burundi, Rwanda, Uganda and the Gulf countries.

Illegal mining is flourishing in areas across the continent where mineral resources are plentiful and it is difficult to police. Any mining that is conducted in a prohibited zone or without the required licences is illegal and it is usually characterized by the use of heavy machinery. Countries in the front line include the Democratic Republic of Congo, South Africa, Uganda and Zimbabwe and main destination markets include China, the EU, the U.S., Japan and South East Asia.

While illegal logging, charcoal and mining are pressing issues for Africa, it is the subject of wildlife trafficking that is perhaps the most sensational, and for good reason. There is a very real danger of species extinction for elephants, rhinoceroses and pangolins, and this is where we would expect to see the most regulatory attention and enforcement activity.

The elephant population has dropped dramatically due to human intervention. Estimates put 26 million elephants in Africa in 1800, while now the population is around half a million. A ban on ivory sales in the late 1980s saw a healthy return of elephant stock but with the infiltration of organized crime after 2008, numbers have dropped dangerously low.8

Rhinoceroses are in a similar situation with poaching incidents at catastrophic levels. The level of rhino-poaching is estimated to have risen substantially since 2008 and peaked in 2015, although levels remain uncomfortably high. While there are a number of vulnerable areas for the poaching of rhino, South Africa is the main source market. Nearly 80% of the global rhino population reside in the country and there has been a significant battle against the scourge over the past few years, with over 1000 rhinos killed each year between 2013 and 2017.9

Rhinos are now among the most endangered species in the world with some species under particular stress. Destination markets for elephant ivory and rhino horn include China, Hong Kong, Malaysia, Singapore, Sri Lanka, Thailand, the United Arab Emirates, and Vietnam.

Pangolins are another animal in the news a lot recently. As the world’s most trafficked mammal, this species is definitely on the endangered list and is already extinct in some regions. Their parts and derivatives are much sought after by the luxury goods market, and pangolin meat can command several thousands of dollars on the black market. Source markets include Cameroon, Kenya, Mozambique, Nigeria, Sierra Leone, South Africa, Togo and Uganda and destination markets include China, Singapore, Thailand, and Vietnam.

8 Elephants on the path to extinction - the facts, The Guardian, 12 August 2016
9 Savetherhino.org
THE INTERNATIONAL SANCTIONS SITUATION

There have been recent cases of individuals and entities on the continent who have been sanctioned due to their involvement in illegal logging, mining and wildlife trafficking.

Moving illicit minerals and animal parts across great areas of continents requires a serious effort, a vast network and many touchpoints. It is advisable that financial institutions and multinational organizations take care to ensure they conduct effective due diligence.

**Iran**

The most high-profile sanctions news, over the past couple of years, is the Iran snapback following the withdrawal of the U.S. administration from the Joint Comprehensive Plan of Action (JCPOA). Now that previously held sanctions have been reinstated by the U.S., it has created a complex situation for organizations that have already embarked on commercial relationships under the JCPOA. The other JCPOA signatories, which include the EU, China, Russia, and the United Kingdom, continue to honor their commitment to the plan and have developed a Special Purpose Vehicle for investors in an effort to protect them from U.S. secondary sanctions.

**Russia**

The sanctions that will probably have more of an impact on Africa-based organizations are those directed at Russia, and sanctions that impact China and North Korea.

There has been an increase in interest on the African continent for Russian investors, driven by several factors including oil reserves, gold, chromium, and other resources. As the middle class grows, it is attracting competition between financial organizations, and there has also been several military cooperation and arms deals signed across the continent in recent months. Seven African countries, Egypt, Algeria, Morocco, South Africa, Tunisia, Nigeria and Sudan, account for nearly 90% of Russia’s trade.

Both the U.S. and the EU extended sanctions against Russia in 2019, after their original imposition in 2014 during the Ukrainian crisis. These sanctions have targeted individuals and entities in Russia and the focus has been on alleged human rights violations and corruption. The relatively new Magnitsky Act in particular targets Russian oligarchs in an effort to stop the movement of goods and assets abroad. Signed into law in 2012, the original focus of the Magnitsky Act was Russian oligarchs and officials.

Since 2016, it has had an increasingly global application and it allows the U.S. government to sanction alleged human rights offenders by freezing their assets and banning them from entering the U.S. Today, the list includes people from numerous countries. A group of NGOs and anti-corruption agencies submitted a list of names for inclusion in 2017, including several from the African continent, and as of October 2019, the Department of the Treasury had designated a total of 118 individuals and entities.

**China**

OFAC lists also designate a number of Chinese individuals and entities. China has been incredibly competitive across the African continent and overtook the U.S. as Africa’s largest trading partner some years ago. Much of the investment has been directed towards building infrastructure, particularly ports. The massive Chinese international infrastructure project, known as the Belt and Road project, links Kenya’s capital Nairobi, to the city of Mombasa by rail, a distance of nearly 500 km. There are plans to extend this project to include South Sudan, Uganda, Rwanda and Burundi.
North Korea

OFAC has increasingly listed Chinese individuals and entities as part of the U.S. administration’s response to North Korea’s ongoing development of weapons of mass destruction. There have also been long standing relationships between certain African states and North Korea. A recent UN investigation uncovered North Korean military radio equipment headed to Eritrea, automatic weapons arriving in Congo and military trainers landing in Angola and Uganda. In Namibia, the national history museum, presidential palace, defense headquarters and munitions factory were built by North Korea. It is believed that Yoweri Museveni, President of Uganda, was taught basic Korean by Kim Il Sung, the grandfather of North Korea’s current leader, Kim Jong Un. Former Zimbabwean leader, Robert Mugabe, once sent a gift of two rhinoceros to Pyongyang in the 1980s and in Maputo, Mozambique, there is a street named Avenida Kim Il Sung.

Nikki Haley, the former U.S. ambassador to the UN (2017 to 2018), warned that countries could lose their right to trade with the U.S. if they were caught violating sanctions against North Korea. Sensitive to such criticism, Namibia released a statement in 2016 that said it ‘remains committed to the implementation of all UN sanctions resolution,’ but added that the warm diplomatic relations with the Democratic People’s Republic of Korea (DPRK) will be maintained.

The status of relationships between other African states and North Korea is less clear. UN member states are obliged to document and report their efforts to enforce sanctions, however in 2016 the UN panel of experts noted ‘an extremely high number of non-reporting and late-reporting States’ and the ‘poor quality and lack of detail of the reports received.’ Despite this, some countries have taken steps to distance themselves from North Korea. In 2017, for example, Uganda’s foreign minister, Sam Kutesa, said on state television that the country is in the process of ‘disengaging the cooperation we are having with North Korea as a result of UN sanctions.’
Identify sanctions risk exposure and close the gaps

To reduce their exposure to the risk of sanctions transgressions, the first step would be a review of all systems and policies. The good news is that survey responses show that over 70% of organizations have a compliance policy in place (Q7), and while this is mostly to address ABC or AML, it means that there is existing infrastructure on which to build a sound sanctions compliance program.

OFAC released its Sanctions Compliance Program (SCP) advisory in 2019, in which five pillars are recommended:

1. Commitment from senior management through
   a. A review and approval of SCP
   b. Ensuring sufficient authority and autonomy to implement the SCP
   c. Ensuring adequate resources
   d. Promoting a culture of compliance throughout the organization
   e. Responding adequately to any violations or SCP deficiencies.
2. Conduct an OFAC risk assessment that accounts for potential sanctions risks relevant to business objectives
3. Build internal risk-based controls that are appropriate and relevant
4. Test and audit the SCP
5. Provide training to all appropriate employees on a regular basis

A number of deficiencies are likely to result in an SCP failure, such as:

- the absence, or inconsistent application, of a formal SCP
- failure to understand the scope of OFACs jurisdiction and how it impacts on non-U.S. citizens
- failure to appropriately update screening software
- ineffective due diligence on clients and commercial relationships

This last point is of interest. According to responses, very few organizations have an effective program for establishing the UBO, a key element to a sanctions program. When asked if compliance activity has increased over the past two years, what was the focus (Q15), understanding UBO scored 2%. Asked where they expected focus to increase (Q16), UBO scored only 3%

Another potential weak spot was revealed when respondents were asked how regularly risk was assessed (Q20), 22% responded that they assessed their risk infrequently or not on a regular basis. That’s a sizeable group of organizations that have probably experienced a change in status in some of their commercial relationships without any idea of the potential impact on that organization’s risk profile, which may well have a bearing on an overall risk profile.

12 OFAC Issues a Framework for Compliance Commitments, U.S. Department of the Treasury, May 2, 2019
ENFORCEMENT ACTIVITY

The OFAC advisory points to recent enforcement activity as a guidance to two specific areas of vulnerability when conducting international trade:

• Cross border mergers and acquisitions – should an organization acquire an interest in a non-U.S. subsidiary and the subsidiary is trading in a high-risk location such as Cuba or Iran, even if that subsidiary is folded due to its high-risk potential, the mother organization is exposed to risk.

• International supply chains – international trade is considered high-risk activity by OFAC and suppliers that operate in geopolitically sensitive areas should receive heightened due diligence.

Ignorance has not been accepted as a defense for several years now and both of these themes underline the need for strong due diligence and internal controls.

OFAC also point out that although it has not often taken action against an individual in a position that is responsible for compliance, there is always the possibility of individual liability.
Enhanced due diligence

Enhance. Simplify. Protect.
Advanced background and integrity checks on any entity or individual, anywhere in the world. Protect your reputation, meet regulatory obligations and understand exactly who you are doing business with.

refinitiv.com/edd
OPPORTUNITY AND RISK IN AFRICAN SUPPLY CHAINS

Bribery and corruption are a major concern to Africa-based businesses. We see this in responses to a question about their financial crime experience (Q6), with over a quarter of respondents saying that they have fallen victim to bribery and corruption, second only to fraud as an issue. Asked about their major concerns, (Q9) it is not surprising to see fraud and ABC listed as priorities. In terms of financial crime programs (Q7), responses also show that ABC is a priority, 74% said they have a KYC program and 70%, higher than other developing countries, have an ABC policy.

With bribery and corruption such a major vulnerability, close attention should be paid to supply chain relationships, especially in a time when trade barriers are falling across the continent, and foreign investors are looking with interest at Africa.
Africa: an increasingly attractive investment destination

Africa is now the world’s second most attractive investment destination, according to the World Economic Forum\(^\text{13}\). The growth of the middle class is driving expectations, especially in the increasingly connected, increasingly urban youth market. Common to other emerging markets, much of the energy comes from small to medium enterprises, all keen to meet the growing demand and establish themselves as regional players, able to compete with the world’s best brands. To do this, however, they will need the support of supply chains that are of a standard that meets international regulations.

This growth in supply chains, while full of opportunities and benefits for business and social needs, will also represent heightened risk. Due diligence of a supply chain may require scrutiny of each link, depending on the risk profile of the individuals and entities involved.

Supply chain risk set to grow

As businesses respond to an expanding commercial environment, supply chains will grow increasingly complex and geographically diverse. At the same time, the regulatory environment has become more constrained and senior executives will find ABC compliance even more challenging.

In today’s regulatory environment, organizations are being held responsible for not only their activities but the actions of their clients, suppliers, vendors and partners. The management of third-party data has become a demanding task which often requires time consuming and detailed reporting based on risk appetites and profiles.

The regulatory burden for small organizations operating from a single location can be relatively straightforward, but for those organizations with operations that cross borders and are subject to different jurisdictions, the necessary documentation and resources is significant. KYC routines

THE AFRICAN CONTINENTAL FREE TRADE AREA

Signed in 2018, ACFTA has created the largest free trade area in the world in terms of participating countries since the launch of the World Trade Organization in 1995. Covering 54 nations, it is estimated that it will create a market of 1.2 billion people with a combined GDP of USD 2.5 trillion. A multi-state deal of this size should be of benefit to even the smallest of states and will likely encourage the growth of production and assembly operations across many African countries. This will bring development to various sectors such as electronics, chemicals, textile production and processed foods amongst others. This will boost the growth of greenfield investment and help to create a diversity of supply chains, some of which will link across borders, involve hundreds of actors and be incredibly complex.

\(^{13}\) Africa is ready for long-term investment. Here’s why, World Economic Forum, 8 November 2018
\(^{14}\) FCPA enforcement report for Q3 2019, The FCPA Blog, October 1, 2019
can differ from country to country and organizations will have their own risk management processes that do not always conveniently match those of the jurisdiction. Language differences also greatly impact the process and some countries are better than others at providing access to public documentation. The ability to collect and analyze KYC documentation is key to third-party management, and the more obstacles to this task the higher the time and cost. We see this difficulty reflected in responses to a question about their most challenging aspect of onboarding and monitoring of business relationships (Q10) with the top two choices being data management and KYC.

**Important anti-bribery and corruption regulation**

ABC regulation tends to have a long extra-territorial reach, a trend that began with the introduction of the U.S. Foreign Corrupt Practices Act (FCPA) in 1977, with its focus on prohibiting the bribery of foreign officials. Given that the U.S. is the dominant economy, the FCPA has a significant extra-territorial reach and its impact is felt around the world. In recent years it has led a global push back against corruption, with other countries enacting similar regulations. The U.S. Department of Justice and Securities and Exchange Commission, the bodies responsible for enforcing the FCPA, recently strengthened its enforcement capabilities by increasing its investigative team as well as its coordination with foreign counterparts.

It should also be noted that in recent years FCPA enforcement activity has targeted more non-U.S. companies than U.S. companies, which means it poses a strong regulatory risk to Africa-based organizations. In the third quarter of 2019, the most recent enforcement activity results that were available during the writing of this report, we noted that five U.S. based corporates, three foreign-based corporates and two foreign banks were subject to penalties.

Other regulations that impact on supply chain management include the Conflict Minerals Rule of the U.S. Dodd Frank regulation and in the UK the Bribery Act and Modern-Day Slavery Act.

While some compliance executives may feel their location, far away from global financial centers, provides an extra layer of protection from scrutiny, it only takes one well-placed whistleblower to draw an unwelcome focus on their operations.
Are your anti-bribery and corruption protocols up-to-date?

Regulators favor organizations with proactive compliance policies. OFAC, for example, in their guidance on sanctions, advise organizations that do business with a U.S. nexus should review and assess their processes against the OFAC baseline expectations because doing so will ‘reduce the potential liability should an apparent sanctions violation occur (particularly if the firm can demonstrate that the violations occurred notwithstanding best efforts to follow OFAC’s SCP Guidance).’

So, while the environment is favorable to investment, it is a good time to review compliance strategies and policies.

These are a few steps to consider in creating a best practice supply chain due diligence routine:

1. Compare existing processes with those outlined in official guidance
2. Understand the weak spots and develop appropriate processes to mitigate risks
3. Introduce controls that will create automated alerts
4. Test
5. Monitor and report
6. Continually review and align
7. Train and educate compliance staff as well as staff in other functions

Responses to question 20 show us that 22% of respondents only assess risk every two years or more, or not at all, leaving them incredibly exposed and vulnerable. Any one of their commercial relationships could have a dramatically altered risk profile from when the relationship was originally onboarded, and with such a weak assessment protocol this risk could lie hidden for two or more years, if it is discovered at all. Responses to question 21 also reveals that less than 53% of respondents have confidence in their compliance policy to do the job. Change is coming, however, with over 90% of respondents expecting some change in their technology over the next two years (Q24).

Less than 53% of respondents have confidence in their compliance policy.
FACTORS THAT PERSUADE PROSECUTORS WHEN PURSUING A CHARGE - DOJ GUIDANCE

Factors include:

- “the adequacy and effectiveness of the corporation’s compliance program at the time of the offense, as well as at the time of a charging decision”
- “the corporation’s remedial efforts to implement an adequate and effective corporate compliance program or to improve an existing one”
- “whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine”
- “whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems”
- “whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future” to determine whether a monitor is appropriate”

Evaluation of Corporate Compliance Programs Guidance Document, U.S. Department of Justice Criminal Division, April 2019
INNOVATIVE TECHNOLOGY: CHANGE IS COMING

Responses to the survey tell the tale of an increasing need for robust analytical support and sophisticated technology to increase the effectiveness of data management.
57% indicated that they expect significant change in their financial crime prevention technology over the next two years.
When asked what is the most challenging aspect of onboarding and monitoring of business relationships (Q10), the top two options chosen were data management and KYC. Responses to questions 11 and 12 reveal a substantial increase in investment into compliance systems, with 55% of respondents indicating a substantial increase in investment over the past two years, and 61% of respondents indicating they will invest substantially into their compliance systems over the next two years. Asked where the main focus of their investment would be (Q13), the top answer was technology.

We also see this need reflected in responses elsewhere:

- 40% indicated significant change when asked how much their financial crime prevention technology had developed over the past two years (Q23)
- 57% indicated that they expect significant change in their financial crime prevention technology over the next two years (Q24)

These responses indicate a growing concern over current compliance processes. Asked how confident they are that their technological financial crime solutions are operating as required and that staff members understand how the solutions operate (Q27), 39% of respondents revealed a lack of confidence in their systems.

### Coping with increasing levels of data and complexity

Compliance executives everywhere are feeling the impact of increasing regulatory volume and complexity, but for organizations in developing countries the impact is arguably more acute as they work towards aligning their processes with the regulatory standards of destination markets. The flow of regulatory information has increased considerably over the past 12 years – in 2008 there used to be around ten updates to regulatory information daily, ten years later, in 2018, there were around 200 updates a day. Not only has the volume increased substantially, so has the complexity of regulation, as well as the consequences of transgression.

It is therefore not surprising to see that compliance executives in developing countries are challenged by the pressure of meeting regulatory expectations. The task of screening and remediation can be overwhelming, compliance technology that was developed ten or twenty years ago simply cannot keep up with the volume of screening and monitoring of relationships that is required today and it is often no longer fit for purpose. We see this reflected in responses to question 25 which asked respondents what the main reason is for investing in a technology upgrade. A sizeable majority of respondents, 62%, cited data management and analytics. There is a demand for sophisticated, innovative technology that will reduce the remediation workload and allow executives to focus their attention on high-risk cases.

### The advantage of lagging behind the curve: learning from others’ experience

The good news is, however, it appears that Africa is more than ready to engage with innovation. Many African states are disadvantaged due to a lack of telecommunications infrastructure yet in the midst of these constraints, or perhaps because of these constraints, there is a higher level of entrepreneurial activity. The World Economic Forum reports that early-stage entrepreneurial activity is 13% higher than the global average16.

---

16 Africa’s future is innovation rather than industrialization, 1 September 2019, World Economic Forum
There is an advantage to being behind the technology curve. Africa-based businesses are able to learn from experimentation and experience of their foreign-based peers and this helps them to leapfrog various development phases. We see this in the rapid uptake of the mobile phone across African markets for example, which has become a powerful tool for millions of people that goes beyond simple communication. A mobile phone allows the user to access the internet, and a stable connection provides an excellent platform for goods and services that otherwise would be out of reach. In particular, the spread of the smart phone across Africa provides a great opportunity for financial institutions to gain access to a mass market of unbanked consumers, desperate for options.

Indeed, Africa’s estimated population is around 1.2 billion, 60% of which are under 24. By 2050, the UN estimates the population will double to 2.4 billion. In 2015, 350 million people in Africa were unbanked according to the World Bank. While only 2% of adults worldwide have a mobile money account, in Sub-Saharan Africa 12% use a mobile account, and for half of these people this is their only account. These numbers provide a snapshot of the potential for growth of financial inclusion across the continent using technology that will continue to produce innovative solutions and grow more sophisticated every year. Young Africans are actively pursuing solutions to challenges and barriers to trade and access to capital and this will include the removal of barriers to financial products.

Global tech giants have recognized the potential in this market and over the past couple of years have begun to build data centers and cloud infrastructure in several African markets. They have also made a significant commitment to developing the necessary skill set in the communities in which they are based.

Not only has there been external interest, certain communities have begun to invest in themselves. The continent now hosts more than 400 tech hubs, and ambitious tech centers have emerged in major cities such as Lagos, Nairobi and Cape Town. Thousands of start-ups now thrive in the network of incubators, accelerators, innovations hubs and technology parks across the continent and there is an appetite for innovative technology that will be able to not only address the issue of financial exclusion but also promote development in all sorts of other areas.

There is a multitude of Africa-based organizations that are primed, ready to grow, ambitiously searching to move into other markets and that desperately need the channels in which to do this. Many recognize that digital innovation will be a bridge for them to connect to the markets that they seek out. We see this in the responses to the question of what, if any, innovative technology their organization had embraced (Q14). Two thirds of respondents indicated that they were employing some sort of advanced technology in the pursuit of their goals, with digital identity the most commonly embraced innovative technology. This shows an appetite for complying with regulatory obligations such as KYC and UBO.

---

17 Silicon Valley eyes Africa as new tech frontier, Fin24, 15 July 2018
18 The Global Findex Database 2017, The World Bank, 2018
Research shows that digitalization of identification will assist in the provision of services, reduction in corruption and a boost to welfare for many citizens, especially those who are vulnerable.
**Digital identification: a potential game changer**

The path to full digital identification for businesses and financial institutions across the African continent will be challenging, but once achieved, it is likely to be a game changer. Many African states are working to reduce barriers to starting and maintaining a business, the ability to identify customers, partners, vendors, and other stakeholders almost immediately through the process of digital identification will substantially impact on the ease of doing business, regardless of how patchy infrastructure is or how many other barriers exist.

Ambitious African states recognize this, and a growing number have begun to pursue digitalization of select Government to Person (G2P) payments as well as integrated access to services using a biometrically authenticated ID system.

Research shows that digitalization of identification will assist in the provision of services, reduction in corruption and a boost to welfare for many citizens, especially those who are vulnerable. Digital ID can also help to catalyze private markets.

Banks in other regions have begun to use facial recognition technology as part of the onboarding process where customers are deemed low risk, but this risk-based approach will not be suitable or permissible for banks in many other areas.

There are many challenges to overcome, however. In FATF’s statement about digital ID systems, digital transactions require a ‘better understanding of how individuals are being identified and verified in the world of digital financial services. Digital ID technologies are quickly evolving to meet the need, and this will produce a number of different systems. FATF’s guidance is intended to assist governments, regulated entities, and other stakeholders to determine how best to create a system that can be used to conduct key elements of customer due diligence under FATF Recommendation 10.

Moving towards digital ID is likely to be a frustratingly slow process to begin with for many businesses, especially so for those based in Africa. The fact that so many people have been excluded from the formal financial system for so long will mean that the task of formal identification to enable digital identification will be fraught with problems and obstacles. Once these issues are overcome, however, there is little doubt that many of the remaining obstacles to doing business will be eradicated. The digital identification project has great potential.
SURVEY RESULTS

Q1. Please choose the option that is the closest fit to your role.

- Board member: 2.22%
- Business owner: 8.00%
- Employee: 8.02%
- External audit professional: 3.56%
- External professional consultant: 6.67%
- Finance manager: 0.44%
- General counsel: 0.44%
- Internal audit professional: 8.44%
- IT manager: 1.33%
- Middle management: 7.56%
- Risk/AML/Compliance/Financial crime officer: 43.56%
- Senior management at C-suite level: 5.78%
'20% of respondents indicated they have less than 25 employees in their organization.'

**Q2. Please indicate the number of employees in your organization.**

- Less than 25: 20.00%
- 25-100: 15.56%
- 101-250: 14.22%
- 251-500: 12.89%
- 501-1,000: 12.44%
- 1,000+: 24.89%

**Q3. How many countries within Africa does your organization operate in?**

- Has a presence exclusively in one country: 48.44%
- Has a presence in 2-5 countries: 22.22%
- Has a presence in 6-10 countries: 13.33%
- Has a presence in greater than 10 countries: 16.00%
Q4. Please indicate the closest fit to the primary industry in which you operate.

- Charity/Not for profit: 1.33%
- Construction/engineering: 1.78%
- Consultancy: 7.56%
- Financial services: 66.22%
- Government: 4.89%
- Healthcare: 0.44%
- Legal: 1.78%
- Manufacturing: 1.78%
- Media: 1.33%
- Oil and gas/Energy: 3.11%
- Professional services: 6.22%
- Retail: 1.78%
- Transport and logistics: 1.78%
**Q5. In which country are you based?**

<table>
<thead>
<tr>
<th>Country</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Angola</td>
<td>2.22%</td>
</tr>
<tr>
<td>Benin</td>
<td>0.89%</td>
</tr>
<tr>
<td>Botswana</td>
<td>5.78%</td>
</tr>
<tr>
<td>Burkina Faso</td>
<td>0.00%</td>
</tr>
<tr>
<td>Burundi</td>
<td>0.89%</td>
</tr>
<tr>
<td>Cameroon</td>
<td>1.78%</td>
</tr>
<tr>
<td>Cape Verde</td>
<td>0.89%</td>
</tr>
<tr>
<td>Central African Republic</td>
<td>0.00%</td>
</tr>
<tr>
<td>Chad</td>
<td>0.44%</td>
</tr>
<tr>
<td>Comoros</td>
<td>0.00%</td>
</tr>
<tr>
<td>Cote D’Ivoire (Ivory Coast)</td>
<td>0.89%</td>
</tr>
<tr>
<td>Djibouti</td>
<td>0.00%</td>
</tr>
<tr>
<td>Equatorial Guinea</td>
<td>0.00%</td>
</tr>
<tr>
<td>Eritrea</td>
<td>0.00%</td>
</tr>
<tr>
<td>Ethiopia</td>
<td>2.67%</td>
</tr>
<tr>
<td>Gabon</td>
<td>0.00%</td>
</tr>
<tr>
<td>Gambia</td>
<td>1.78%</td>
</tr>
<tr>
<td>Ghana</td>
<td>4.89%</td>
</tr>
<tr>
<td>Guinea</td>
<td>1.33%</td>
</tr>
<tr>
<td>Guinea Bissau</td>
<td>0.00% (0)</td>
</tr>
<tr>
<td>Kenya</td>
<td>14.67%</td>
</tr>
<tr>
<td>Lesotho</td>
<td>1.33%</td>
</tr>
<tr>
<td>Madagascar</td>
<td>0.00%</td>
</tr>
<tr>
<td>Malawi</td>
<td>0.89%</td>
</tr>
<tr>
<td>Mali</td>
<td>0.00%</td>
</tr>
<tr>
<td>Mauritania</td>
<td>0.00%</td>
</tr>
<tr>
<td>Mauritius</td>
<td>3.11%</td>
</tr>
<tr>
<td>Mozambique</td>
<td>0.89%</td>
</tr>
<tr>
<td>Namibia</td>
<td>0.89%</td>
</tr>
<tr>
<td>Niger</td>
<td>0.00%</td>
</tr>
<tr>
<td>Nigeria</td>
<td>14.67%</td>
</tr>
<tr>
<td>Country</td>
<td>Percentage</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Republic of the Congo</td>
<td>0.00%</td>
</tr>
<tr>
<td>Reunion</td>
<td>0.00%</td>
</tr>
<tr>
<td>Rwanda</td>
<td>2.22%</td>
</tr>
<tr>
<td>Saint Helena</td>
<td>0.00%</td>
</tr>
<tr>
<td>Sao Tome &amp; Principe</td>
<td>0.00%</td>
</tr>
<tr>
<td>Senegal</td>
<td>1.33%</td>
</tr>
<tr>
<td>Seychelles</td>
<td>0.00%</td>
</tr>
<tr>
<td>Sierra Leone</td>
<td>0.89%</td>
</tr>
<tr>
<td>Somalia</td>
<td>0.89%</td>
</tr>
<tr>
<td>South Africa</td>
<td>15.11%</td>
</tr>
<tr>
<td>Swaziland</td>
<td>1.33%</td>
</tr>
<tr>
<td>Tanzania</td>
<td>0.89%</td>
</tr>
<tr>
<td>The Democratic Republic of Congo</td>
<td>0.00%</td>
</tr>
<tr>
<td>Togo</td>
<td>0.00%</td>
</tr>
<tr>
<td>Uganda</td>
<td>5.78%</td>
</tr>
<tr>
<td>Zambia</td>
<td>5.33%</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>4.00%</td>
</tr>
<tr>
<td>None of the above</td>
<td>1.33%</td>
</tr>
</tbody>
</table>
Levels of crime awareness

Q6. Has your organization fallen victim to any of these crimes over the past five years? (Please select all that apply.)

<table>
<thead>
<tr>
<th>Crime Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bribery and corruption</td>
<td>28.73%</td>
</tr>
<tr>
<td>Cyber breach</td>
<td>14.92%</td>
</tr>
<tr>
<td>Fraud</td>
<td>51.38%</td>
</tr>
<tr>
<td>Identity theft</td>
<td>19.34%</td>
</tr>
<tr>
<td>Money laundering</td>
<td>18.78%</td>
</tr>
<tr>
<td>Regulatory breach</td>
<td>26.52%</td>
</tr>
<tr>
<td>Sanctions breach</td>
<td>7.18%</td>
</tr>
<tr>
<td>None of the above</td>
<td>34.25%</td>
</tr>
</tbody>
</table>

Over 50% of respondents said that their organization had fallen victim to fraud in the past five years.
Financial crime programs

Q7. Which of the following financial crimes programs does your organization currently have in place? (Please select all that apply.)

- Anti-bribery and corruption: 70.17%
- Anti-money laundering: 73.48%
- Counter-threat financing: 32.04%
- Cybercrime: 45.03%
- Digital identity: 25.41%
- Fraud: 64.64%
- Know your customer: 74.03%
- Sanctions: 43.09%
- Trade-based money laundering: 28.18%
- Understanding ultimate beneficial ownership (UBO): 32.04%
- Vessel screening: 16.02%
- Whistleblower protection: 53.59%
- None of the above: 3.87%

Q8. If your company does not have an anti-bribery and corruption program, why not? (Please select all that apply.)

- Associated costs: 73.48%
- Lack of awareness: 13.26%
- Lack of management support: 4.97%
- Lack of specialist resources/skills: 13.81%
- Not applicable – my company has an anti-bribery and corruption program: 7.3%
Which financial crime issues are the most concerning?

Almost 50% of respondents were extremely concerned with cybercrime issues.

High concern – fraud, ABC, cybercrime
Low concern – CFT, sanctions, digital ID. Sanctions will probably pose a higher risk than respondents realize.
What is the biggest challenge during onboarding and monitoring of business relationships?

Q10. What, in your opinion, is the most challenging aspect of onboarding and monitoring business relationships?

- Data management: 27.07%
- EDD: 8.84%
- KYC: 27.07%
- Robust digital identification: 15.47%
- Screening: 8.29%
- UBO: 13.26%

Over 27% percent feel that data management and KYC are the most challenging aspects of onboarding and monitoring business relationships.
### Increase and anticipated increase in compliance investment

**Q11. How has your investment in compliance increased compared to two years ago?**

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over 50%</td>
<td>28.49%</td>
</tr>
<tr>
<td>Over 25%</td>
<td>27.33%</td>
</tr>
<tr>
<td>Over 10%</td>
<td>17.44%</td>
</tr>
<tr>
<td>Less than 10%</td>
<td>13.37%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>13.37%</td>
</tr>
</tbody>
</table>

**Q12. What do you anticipate the increase in your compliance investment will be over the next two years?**

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over 50%</td>
<td>32.56%</td>
</tr>
<tr>
<td>Over 25%</td>
<td>28.49%</td>
</tr>
<tr>
<td>Over 10%</td>
<td>19.19%</td>
</tr>
<tr>
<td>Less than 10%</td>
<td>10.47%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>9.30%</td>
</tr>
</tbody>
</table>
Q13. Where is the main focus of investment to meet compliance objectives in your organization?

- Data quality: 8.72%
- Outsourcing: 2.91%
- Processes – internal business change and reorganization: 19.77%
- Technology: 37.79%
- Training: 27.33%
- Don’t know: 3.49%

Over 37% of respondents said that the main focus of investment to meet compliance objectives in their organization was technology.
### Innovative technology

**Q14. What, if any, innovative technology has your organization embraced as a way of meeting compliance obligations? (Please select all that apply.)**

<table>
<thead>
<tr>
<th>Technology</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artificial intelligence</td>
<td>25.00%</td>
</tr>
<tr>
<td>Blockchain</td>
<td>8.14%</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>26.74%</td>
</tr>
<tr>
<td>Data lakes and analytics</td>
<td>25.48%</td>
</tr>
<tr>
<td>Digital identity</td>
<td>26.52%</td>
</tr>
<tr>
<td>Machine learning</td>
<td>18.02%</td>
</tr>
<tr>
<td>None of the above</td>
<td>34.30%</td>
</tr>
</tbody>
</table>
### Compliance activity – where’s the focus?

**Q15. If compliance activity in your organization has increased in the past two years, what is the focus?**

<table>
<thead>
<tr>
<th>Area</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data quality</td>
<td>9.88%</td>
</tr>
<tr>
<td>Digital identity</td>
<td>6.40%</td>
</tr>
<tr>
<td>Investment in technology</td>
<td>20.35%</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>4.65%</td>
</tr>
<tr>
<td>Processes</td>
<td>11.5%</td>
</tr>
<tr>
<td>Regulatory monitoring</td>
<td>15.70%</td>
</tr>
<tr>
<td>Training and staff resources</td>
<td>24.22%</td>
</tr>
<tr>
<td>Understanding ultimate beneficial ownership</td>
<td>1.78%</td>
</tr>
<tr>
<td>There is no difference from before</td>
<td>5.81%</td>
</tr>
</tbody>
</table>

**Q16. If you expect compliance activity to increase in the next two years, what will be the focus?**

<table>
<thead>
<tr>
<th>Area</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data quality</td>
<td>12.79%</td>
</tr>
<tr>
<td>Digital identity</td>
<td>4.07%</td>
</tr>
<tr>
<td>Investment in technology</td>
<td>30.81%</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>1.74%</td>
</tr>
<tr>
<td>Processes</td>
<td>10.47%</td>
</tr>
<tr>
<td>Regulatory monitoring</td>
<td>13.95%</td>
</tr>
<tr>
<td>Training and staff resources</td>
<td>20.35%</td>
</tr>
<tr>
<td>Understanding ultimate beneficial ownership</td>
<td>2.91%</td>
</tr>
<tr>
<td>There will be no difference</td>
<td>2.91%</td>
</tr>
</tbody>
</table>
### Q17. In your organization, what do you believe is the key concern in terms of financial crime and compliance?

<table>
<thead>
<tr>
<th>Concern</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforcement action - financial loss</td>
<td>23.03%</td>
</tr>
<tr>
<td>Enforcement action - threat to trading activity</td>
<td>9.21%</td>
</tr>
<tr>
<td>Lost revenue/customers and/or relationships</td>
<td>22.37%</td>
</tr>
<tr>
<td>Reputational degradation</td>
<td>28.29%</td>
</tr>
<tr>
<td>Risk of personal liability</td>
<td>5.92%</td>
</tr>
<tr>
<td>Slowdown of customer onboarding</td>
<td>1.97%</td>
</tr>
<tr>
<td>Threat to correspondent banking relationship</td>
<td>6.58%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>2.91%</td>
</tr>
</tbody>
</table>

### Q18. What, in your opinion, currently poses the most risk to your organization?

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to invest in advanced technology</td>
<td>21.05%</td>
</tr>
<tr>
<td>Failure to invest in good-quality data</td>
<td>9.87%</td>
</tr>
<tr>
<td>Failure to meet business objectives</td>
<td>17.11%</td>
</tr>
<tr>
<td>Failure to meet regulatory obligations</td>
<td>25.00%</td>
</tr>
<tr>
<td>Loss of correspondent banking relationship</td>
<td>7.89%</td>
</tr>
<tr>
<td>Restriction of trading activity</td>
<td>3.95%</td>
</tr>
<tr>
<td>Regulatory fine</td>
<td>7.24%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>7.89%</td>
</tr>
</tbody>
</table>
**Confidence and assurance levels**

**Q20. How regularly do you assess the risks that financial crime poses to your organization?**

- Two to four times a year: 44.74%
- Once a year: 33.55%
- Once every two years: 3.29%
- Once every two to five years: 3.29%
- Not on a regular basis: 15.13%

**Q21. How confident are you that your financial crime program is compliant with regulatory requirements?**

- Not at all confident: 7.89%
- Not very confident: 9.21%
- Somewhat confident: 35.53%
- Very confident: 40.79%
- Extremely confident: 6.58%

**Q22. Where there is a lack of confidence in your financial crime program, what are the main reasons? (Please select all that apply.)**

- Lack of management support: 46.15%
- Competing business goals and objectives: 0.00%
- Lack of specialist resources: 38.46%
- Lack of strategy: 26.92%
- Lack of understanding of technology: 24.36%
- Regulatory complexity: 28.18%
- Don’t know: 10.26%
- Standard of compliance competency amongst team: 0.00%
- Don’t know: 0.00%
- Other (please specify): 0.00%
The role of technology

40% stated that their financial crime prevention technology developed significantly over the past two years.

Q23. How has your financial crime prevention technology developed over the past two years?

- Significantly: 40.28%
- Slightly: 34.72%
- No change: 22.22%
- Don’t know: 2.78%

Q24. How do you expect your technology to change in this regard over the next two years?

- Significantly: 56.94%
- Slightly: 33.33%
- No change: 5.56%
- Don’t know: 4.17%
Q25. What is the main reason you would invest in a technology upgrade?

- Better data management and analytical capabilities: 61.81%
- Faster processing times: 6.94%
- Reduced operational costs: 9.72%
- Standardization and consistency: 18.06%
- Don’t know: 3.47%

Q26. What, in your opinion, is the biggest disadvantage of an advanced technological solution?

- Cost: 52.78%
- Need for training: 12.50%
- Risk of over-reliance: 23.61%
- Time to implement: 7.64%
- Don’t know: 3.47%
Q27. How confident are you that your technological financial crime solutions are operating as required and that staff members understand how the solutions operate?

- Very confident: 20.14%
- Fairly confident: 40.97%
- Limited confidence: 28.47%
- Not at all confident: 10.42%

Q28. What is the main cause of your concern?

- Integrity of screening data: 10.71%
- Lack of specialist resources: 28.57%
- Lack of support from the solution provider: 8.93%
- Lack of training: 23.21%
- Regulatory complexity: 23.21%
- Don't know: 5.36%
A powerful combination of digital identity verification, document proofing and risk screening all via API technology

- Secure digital identity verification and screening
- Seamless delivery via API
- Delivers a frictionless customer experience
- Reduces customer abandonment rates
- Decreases fraud and enhances compliance

HOW DO YOU KNOW YOUR CUSTOMER IF YOU DON'T KNOW YOUR CUSTOMER?

refinitiv.com/qual-id
Refinitiv is one of the world’s largest providers of financial markets data and infrastructure, serving over 40,000 institutions in approximately 190 countries. It provides leading data and insights, trading platforms, and open data and technology platforms that connect a thriving global financial markets community – driving performance in trading, investment, wealth management, regulatory compliance, market data management, enterprise risk and fighting financial crime.

Visit refinitiv.com

@Refinitiv  LinkedIn  Refinitiv

REFINITIV®
DATA IS JUST THE BEGINNING®