COMPLIANCE INSTITUTE
SOUTHERN AFRICA

ANNUAL COMPLIANCE CONFERENCE

2021 HOW?

2021 CONFERENCE THOUGHT LEADERSHIP

18th & 19th AUGUST 2021

LexisNexis

TABLE OF CONTENTS

COMPLIANCE INSTITUTE
SOUTHERN AFRICA

A MESSAGE FROM THE CHIEF EXECUTIVE OFFICER

Between stimulus and response there is a space. In that space is our power to choose our response. In our response lies our growth and our freedom.
Viktor Frankl

2020 was a year of stimulus. We were called upon to be resilient, to make plans and to execute them within timelines hitherto thought impossible. We had to learn new responses and unlearn the old. 2020 was a year of introspection, learning and adapting.

We expected and hoped that things would return to normal in 2021, but the coronavirus is still with us, and the year brought new challenges. As unexpected as the pandemic was, there were warning signs. Hence our choice of this year's conference theme, 'How?'

How do we make sure that we are better prepared for the next disruptor(s)? How do we equip ourselves with pre-knowledge and new skills? How do we think like futurists when our daily job is to keep the ship afloat and build our own careers? How do we make compliance matter in the hearts and minds of those who manage it? How do we win the fight against corruption? How do we understand the developing next global risk, climate change, and protect our world against it? How do we survive and thrive in the new world of crypto currencies that is emerging and entering our lives as we speak?

The answers lie in observing excellence (as we saw with the Forensic Risk Alliance team and their Airbus investigation), absorbing lessons from mentors and experts (our speakers) and bringing it onboard in our daily lives. We must work closely with the innovators and those who think about tomorrow's world and develop solutions that re-imagine the future. You saw them at the conference – they were there in the guise of sponsors and exhibitors.

We have the power to choose our response. What is yours going to be?

Thank you to our speakers for sharing their expertise with us. Thank you to our sponsors and exhibitors for showing us what is possible and how they can make us more effective and efficient. And thank you to you, our delegates for participating and engaging with us as we continue on our journey to elevate compliance in Southern Africa.

Rianné Potgieter
Chief Executive Officer
Compliance Institute Southern Africa

HOW CAN THE RULE OF LAW AND COMPLIANCE CREATE SUSTAINABLE BUSINESSES?

Videsha Proothveerajh, CEO and Chairman of the Board of LexisNexis South Africa (LNSA), discusses the rule of law, the ever-evolving compliance space and its demands on the compliance professional, explaining how proactive compliance delivers resilience and sustainability.

In its simplest form, the rule of law means that "no-one is above the law." No society can function in the absence of the rule of law. It is the foundation for the development of peaceful, equitable and prosperous societies. However, for the rule of law to be effective, there must be equality under the law, transparency of law (law written down and accessible to all), an independent judiciary and access to legal remedy. When these four factors are in place, a government is building its society on a stable base. If any of these factors is missing or damaged, the foundation is weakened.

When the rule of law in a country is strong, GDP and life expectancy rise, child mortality decreases, corruption drops and through the growth of sustainable businesses, countries move up on the competitive index. The rule of law provides business and commercial activity with security, stability, good governance, consistency, accountability and helps safeguard against corruption - all of which are essential to reduce threats to investment and to promote economic activity. As business we have to be committed to advancing the rule of law and this is not possible without compliance as the empowering and enabling force behind it. But why would this commitment be such an important underpinning for a private sector entity? The answer is simple. Advancing the rule of law is not only the right thing to do—it is good for business and when done well, creates trust, customer loyalty and improves the triple bottom line which equals sustainability.

Compliance Interrupted

Compliance is a space that is changing constantly and the 4th Industrial Revolution has not made it any easier.

Technology enables business models to be created and scaled at a phenomenal pace, but as companies explore social, mobile, analytics and cloud opportunities to increase their digital footprint, the surface area for crime as a service and non-compliance increases exponentially.

Cyber-attacks are increasingly sophisticated and the rewards are great for the perpetrators. For any company on the receiving end, it means their security was not good enough. Voya Financial was fined $23,9m million by the Securities and Exchange Commission (SEC) for its failures in cybersecurity policies and procedures surrounding a cyber intrusion that compromised the personal information of thousands of customers. Add to this cost the loss of trust and reputation. Usually its large brand names that make the headlines when they suffer a breach or loss of customer data, but it's not just the large corporations that are at risk. According to Microsoft, a large percentage of small to mid-sized businesses have been targets of cybercrime. The myriad of emerging tech, such as distributed ledgers known more commonly as blockchain, drones, the Internet of Things (IOT) and automated machines, such as self-driving cars, brings the possibility to leapfrog and evolve faster. It also brings much more complexity and many unknowns for compliance officers.

An unexpected disruptor is the Covid-19 pandemic which has brought compliance challenges around remote working, access and security issues, Work from Home policies, productivity tools and measurements. At the same time, it has created great opportunities for companies like LexisNexis that provide online tools and platforms that secure accessibility and productivity, adding value and reducing economic risk. We are now re-imagining the Future of Work and the workforce of the future as traditional models have been forced to evolve.

We also can't ignore the macro factors that test the compliance function daily. I had the misfortune to be caught in the looting and rioting that rocked our country in July. Those actions undermined the Rule of Law and the compliance function failed dismally. The cost is billions of rands in damage to infrastructure and the economy and the deeply concerning loss of life and livelihoods. Business and compliance were front and centre in dealing with the collateral damage.

Other macro factors such as rolling blackouts, water shortages, high levels of unemployment and inequality all have compliance consequences. Then there are new laws, such as the Protection of Personal Information Act (POPIA), which has kept many business, legal and compliance professionals awake at night.

Compliance with regulations and customer requirements will continue to become increasingly difficult to manage. I believe that over the next four to five years, we will see around half a million audits that don't currently exist, and in the next decade, we are likely to see a steady stream of significant new lawsuits around access to data.

What does the role of a compliance professional look like today?

Compliance, in the form of the institutionalized profession that it is today, is a relatively new area of specialization. Yet within

the span of a few decades, due to the confluence of various economic, social, and regulatory trends, the compliance profession has made impressive strides in establishing itself as a full-blown specialty, fundamental to the success of any business organization.

As a compliance professional today, one needs the skills of a lawyer to interpret and understand the context around laws and regulation and the skills that one would expect from a business leader. A compliance professional is accountable and needs management and leadership skills to influence others, often in the absence of line authority. You have to navigate complex organizations and drive concrete outcomes, as opposed to the more classic lawyer role, which focuses on giving advice.

Based on its surveys on the state of compliance, Pricewaterhouse Coopers (PWC) predicts that by 2025, the CCO will be 'the star' of the C-suite. Compliance professionals will need tool kits that span law, compliance, technology, HR, and other critical functions to address the most fundamental problems. To realize the fruits of fairness, justice, and ethics in society, we need strong leaders with management skills, to transform the vision of justice that is written in the law into reality. We need people who understand ethics, who recognize when adherence to the black letter law is not sufficient. As compliance professionals, you contribute to the solutions necessary not only to build sustainable businesses, but what the rule of law envisions: peaceful, equitable and prosperous societies.

Building a compliance culture

Having the right compliance talent on hand, we must build and embrace a culture of compliance. For all employees to own the compliance culture, you need a values- versus a rules-based compliance culture, because in a values-based culture, employees get to know what feels right.

One way that LexisNexis has ensured its ongoing compliance is through what we call a circle of compliance. It starts with a review of the laws. We examine the laws to understand the compliance needs. We then audit our activities and reporting mechanisms to determine if we are doing what the law requires. If not, we assess how we can meet the gap between the law and our activities. We then look to train our employees to meet the new standards which form the change between our old practices and the new practices (the compliance structure). We then audit our compliance. We have mechanisms in place to report transgressions anonymously and otherwise, and then the circle begins again, as laws change and as people join the company. This process has led to a world class, sustainable business.

The cost of non-compliance

"An investment grade company has high brand equity, low cost of doing business due to low risk, enjoys a lucrative share price, is known for its culture of ethics and compliance as it has its foundational pillars and documentation in place which is like the business's constitution.

"Compliance is at the heart of this recipe for success and sustainability. " - *Siemens Senior Executive*

As compliance professionals you understand the colossal risks and cost of non-compliance. The past decade has been marred by a series of compliance scandals in South Africa's private sector. We have all borne witness to the corporate reputational graveyard littered with well-known brands that failed to place compliance firmly at the core of the Company Culture and Code of Conduct.

In addition to penalties such as hefty fines and trade sanctions, other consequences of non-compliance with applicable laws can include:

- **Criminal Charges**
  No director/ board member or executive wants to face criminal charges for not ensuring that their enterprise adheres to the law. However, criminal charges and jail time are a very possible consequence for regulatory non-compliance.
- **Reputational woes**
  A business's public image is key to its success. When a company is thrust into the public eye for failing to comply with regulations it inevitably leads to a loss of trust. I always say that trust is earned in drops and lost in buckets.
- **Loss of lucrative opportunities**
  Businesses are required to meet a host of regulations if they wish to do business with government, parastatals or other law-abiding companies. Non-compliance across your enterprise and business network could result in exclusion from the tendering process and supplier database. In addition, companies that place value on corporate compliance may avoid doing business with you as they would want to ensure that they meet their own regulatory obligations.

Rule of law – a framework for how to act

The rule of law provides a legal foundation for conducting business in a reliable and predictable manner. It promotes economic investment by increasing the protection of property rights and contracts, allows for the timely and predictable resolution of disputes, lowers levels of corruption and bribery. and ensures the legal identity of individuals and organisations, providing greater security. The Rule of Law holds people, business and government accountable for their actions, providing much-needed stability, consistency and certainty in

a potentially volatile landscape. Increased expectations of transparency, an ever-changing regulatory environment and social movements are all impacting the way businesses operate. Now more than ever – Integrity matters.

Triple bottom line compliance ensures sustainability

As companies evolve and transform their business models, they are changing the way they measure success. In our rapidly changing world with an increasingly large middle class and swelling population of millennials, aspects like social and environmental impact have become critically important metrics.

Triple bottom line - a tool for evaluating the economic, social and environmental impact of corporate actions on people and the planet over time – has become standard practice. To ensure business sustainability, compliance must lie at the heart of all three legs of the triple bottom line.

Confronting the dark side

Compliance professionals are dealing with growing business risk (South Africa has the third highest number of cyber victims globally), social risk (think of digital social movements such as #Black Lives Matter and #Me too) and in a regulatory environment where technology is advancing faster than regulation and control.

The sheer size and reach of social media and the way in which they overlap with rights of freedom of speech and privacy, have created complex ethical issues, as have innovations such as bioengineering that take us beyond the level of humanity.

Legislation often struggles to keep up with the rapid pace of change of technology, which can lead to frustration as businesses drive new models. On one hand we need to be agile and flexible and take risks while on the other, we have to balance the compliance requirements in order to ensure sustainability.

We speak about Uber as a positive example of disruptive change, but they have had their fair share of challenges from existing taxi drivers and have been challenged in court over the rights that they must provide drivers in the Uber network. With the rapid adoption of Cloud Computing, the topic of data sovereignty is yet another concern.

In the face of these new risks and concerns, it can seem like the safest option to do nothing or to stick to the traditional model of preventative or reactive law, but is this the best course of action?

I believe Proactive law which regards the law as an enabling instrument, which fosters the creation of economic value and successful relationships, is key. If you combine this with taking advice and seeking out best practice from experienced and trusted partners like LNSA – you cannot go wrong!

Building resilience through partnership

Covid-19 and the unrest have shown us that business as usual can be turned on its head overnight and we have to future-proof our businesses to ensure sustainability. No society can function in the absence of the rule of law. At LNSA, our north star is Advancing the Rule of Law. As compliance professionals, you are also custodians of the rule of law.

Together, we can play a powerful role in helping to drive change. By harnessing the innovation, creativity and energy companies display every day in their commercial activities, we can open up new markets and opportunities through supporting the rule of law.

Videsha Proothveerajh
CEO and Chairman of the Board
LexisNexis South Africa (LNSA)

THE CHALLENGES OF CRYPTO ASSETS

According to a Statista Global Consumer Survey, South Africa is among the top five countries in terms of cryptocurrency ownerships with 17.8% of respondents indicating they owned or used crypto assets in 2020.

In addition, South Africa is in the top four of the 55 countries surveyed for their adoption of crypto assets. There are around 12 different crypto asset trading platforms operating in South Africa with a market capitalisation value of approximately R6.5 billion.

South Africa's increasing adoption of crypto assets has the potential to boost financial innovation and efficiency, but the lack of a regulatory framework and the potential opportunity for anonymity around it, is an especially attractive option that creates new opportunities for money launderers, terrorist financiers, and other criminals to launder their proceeds or finance their illicit activities. To support this, a recent report by CipherTrace stated major crypto thefts, hacks and frauds were found to total $681 million.

As DeFi (Decentralized finance) crimes continue to grow, the Financial Action Task Force (FATF) have tried to address this growing concern by introducing amendments to its recommendations by firmly placing Anti-Money Laundering (AML) and terrorist financing requirements on virtual assets (VAs) and virtual asset service providers (VASPs).

These amendments place obligations on FATF member countries to "assess and mitigate their risks associated with crypto asset activities and service providers; license or register service providers and subject them to supervision or monitoring by competent national authorities" and includes a requirement under Recommendation 16 ('the travel rule') for VASPs to collect and hold information of both the originator and the beneficiary involved in a crypto asset transaction.

While crypto assets are not currently regulated in South Africa, plans are already in motion to bring the country's AML/ Combating the Financing of Terrorism (CFT) regime in line with the FATF's recommendations related to the acquisition, custody, trading and use of crypto assets.

Among the proposed amendments is to include VASPs in the list of Accountable Institutions under Schedule 1 to the Financial Intelligence Centre Act (FICA) , subjecting VASPs to the full weight of FICA regulatory obligations and non-compliance penalties. Once the amendments are approved and published by Parliament, it will bring South Africa's AML/CFT regime more in line with the latest FATF standards. To assist with implementation, the FATF recently completed a cross-jurisdictional study into the use of virtual assets based on more than one hundred cases brought forward by member financial intelligence units from 2017 to 2020. The study highlighted that the types of offences reported include money laundering, the sale of controlled substances and other illegal items (including firearms), fraud, tax evasion, computer-based crimes (e.g. cyberattacks and ransomware), child exploitation and human trafficking.

More recently, professional criminal networks have also started exploiting VA's as one of their means to transfer, collect, or layer illicit proceeds and in some cases to evade financial sanctions and raise funds to support terrorism.

Following this study, the FATF published their guide to 'red flags' of suspicious transactions and activities, to assist member countries with identifying indicators of potentially illicit activity.

These indicators cover a range of specific VA and VASP activities and transactions that may give rise to suspicion, some of which include:

- Red flags related to transactions
- Red flags related to new clients
- Red flags related to senders/recipients

If you work with virtual assets, its vital to keep up to date with the potential risks associated with them and whilst many of these indicators are red flags traditionally found in fiat environments, but with a VA or VASP 'twist' as technology advances, newer, more creative approaches to transfer value will continue to arise.

Want to know more?

For more information, have a look at the FATF Virtual Assets Red Flag Indicators publication here. You can also keep up to date with the latest in FICA and Anti-Money Laundering news by signing up to our newsletter.

Hawken McEwan
Head of Compliance
DocFox Africa

When assessing your compliance function through the lens of strategic foresight, it becomes apparent that the futures of compliance are complex, dynamic, and uncertain. Viewing compliance in the context of futures (plural) allows us to imagine the multiple possible future states of compliance. This empowers us to transcend limitations of traditional thinking and move into a mindset of opportunity, possibility, plausibility, and preparedness.

Adopting this approach, you will find that the business case for manual processes is significantly diminished. Compliance functions, practitioners and professionals will need to arm and elevate themselves. Not only to survive the exponential complexity of regulation but to be able to leverage a proactive approach for compliance as a business enabler.

Align with strategy:

A strategic approach to compliance is vital. Identifying the connection between compliance obligations and their effect on business objectives enables you to assess and manage these obligations holistically. The systemic nature of business means that organisational silos, while convenient, lack the integration needed for compliance to be a business enabler.

A mindset shift is needed to move away from standard connotations of compliance as a preventive "grudge purchase". A compliance function that is not only on top of but ahead of their obligations can be a great source of opportunity for a business.

With strategic alignment and a futures focus, your compliance function can begin to identify and act on early indicators, conduct meaningful environmental scanning, and recognise patterns in regulatory developments.

Optimising compliance processes

Manual processes are often necessary to get started but won't contribute towards business efficiency initiatives and may also pose significant risk with human error. The costs that can be incurred due to non-compliance could be debilitating for an organisation.

Increased complexity, compliance landscape transformation and regulatory scrutiny have created a melting pot of new responsibilities for compliance practitioners. In a poll conducted at the Compliance Institute Southern Africa's annual conference, when asked what their biggest compliance challenge is, 52% of respondents said, "keeping up with legislative changes" followed by 37% who said, "monitoring and assessing your compliance status".

Compliance professionals are feeling greater pressure to do more and do better with fewer resources, forcing an operational re-think. A logical next step is to move away from mundane tasks (where possible and appropriate) that can be optimised by technology, automation, or outsourcing. Shifting into more automated and streamlined compliance processes opens spaces and cultivates conditions for opportunity creation from your compliance function. Compliance practitioners can focus on core responsibilities that add value, instead of being inundated with time-consuming manual or administrative tasks.

Assessing your needs

Taking the leap to automate or outsource compliance activities can often be daunting. A baseline assessment of your current processes and future requirements is a good first step.

1. ***Conduct a Gap Analysis:*** identifying gaps in your compliance processes will enable you to target areas where support is most needed. You can also use this step to evaluate which activities need improvement across time and resource consumption. This analysis should be framed within the context of serving organisational objectives as well as any future obligations you may encounter.
2. ***Define Requirements:*** using your gap analysis, you can now develop a statement of requirements. This should be comprised of a complete list of what is needed to fill gaps and increase efficiency and effectiveness for your compliance function.
3. ***Identify Solutions:*** you should now be able to investigate options available to you based on your requirements. These solutions can comprise of anything that will enable the business through optimising activities including document management systems, outsourced legal services, automated legal and regulatory content and updates, advisory and

change management services, compliance management software, etc.

Before deciding on any single solution, technology, or partner, significant research should be done to evaluate each option against requirements identified, resources available and benefits that are expected. Many solutions or process changes will require buy-in from key decision-makers who may have pre-requisite expectations including:

- Business objective alignment
- Streamlined processes
- Return on investment
- Integration capabilities
- Improved compliance status

While there are many compliance processes and activities that rely on manual input there are also a multitude of ways to enhance this and lift the administrative burdens off compliance professionals. We can leverage an entire value chain of people, processes, and technology to get the most out of our compliance function and all it takes is a few steps to get started. How are you preparing now, for the multiple futures ahead?

Jessica Knight
Head of Strategy
CURA Software Solutions

THE BRILLIANCE OF PRE-DEFINED CONTROLS COULD MAKE COMPLIANCE MANAGEMENT VERY EFFECTIVE

During the annual conference we have asked participants if they think that pre-defined controls would enhance the compliance function. Our poll indicated that 97% of the participants agree with this statement.

Over 20 years of experience in audit, risk and legal compliance have shown me that the identification and the defining of a control has been the area that organisations struggle with most in implementing a compliance management programme in an organisation.

I have seen controls such as “Management takes care of that”; “We have a Health and Safety Officer” and I think the most common one “We have a Policy and Procedure “. So, what would be wrong with “We have a Policy and Procedure “? The simple answer to this is that the mere existence of a document that we call a policy cannot function as a control unless the following requirements have been met:

- The contents of the policy should have been thoroughly communicated to everyone that need to comply with it.
- Adequate training pertaining to the behaviour that the policy requires should have been provided.
- The trainees should have accepted the contents and agreed to the requirements; and
- Lastly compliance to this policy should be verified before we can determine if this is an effective control.

The topic of controls gets even more confusing when we discuss the Control Types. Do we make it easy and just use preventative and detective controls or do we bring directive, contingent, corrective and the rest of the team in to play?

What complicates matters even further is the fact that the effectiveness and adequacy of the controls have to be assessed by the audit and monitoring team. The problem here is if I do not have a specific taxonomy and way of defining controls, the audit team might be duplicating their efforts on assessing Safety team at one manufacturing site regularly checks the safety equipment. They have defined their control as follows: Regular monitoring is performed on all safety equipment by the plant engineer. The Health and Safety team at another site of the organisation has defined the same control as follows: Safety checks are performed on the fire extinguishers by the plant engineer. As these controls have been defined so differently, the audit team has allocated both these controls for effectiveness assessment.

Given all the difficulties of defining controls, I believe there is room for pre-defined controls. There are numerous benefits to pre-defined controls. These include:

- Properly defined controls. “No rubbish in, rubbish out scenarios.”
- Industry best practice methodologies are used.
- Decreasing audit and monitoring work.
- Obtaining more buy-in for compliance software as it is easy to use.
- Areas where the same weak control are used can easily be identified.
- Effective control reporting.

Like most things there are also disadvantages in utilising pre-defined controls. The most significant one is that general controls might be selected that are not appropriate for a specific site or situation. Pre-defined controls can also be likened to pre-cooked meals. Eventually we could get lazy to consider the compliance requirements adequately before we assign a control.

I do however believe that predefined controls used with the necessary caution and prudence could add significantly to the effectiveness of the compliance management programme and software used.

Ansa Jordaan
Executive Director
Exclaim

RISK RESILIENCE: MARSH ON THE RISE OF CYBER THREATS

As new challenges emerge and the risk landscape grows increasingly complex, it is important that businesses stay informed. Cyber threats are pervasive and accelerating, costing global businesses billions every year and creating exposures across almost every aspect of an organization's value chain.

Did you know that?

- The average business interruption outage from a ransomware attack now exceeds 20 days
- The average ransomware demand exceeds $1 million.
- Anticipated global ransomware recovery costs by the end of 2021: $20 billion
- Increase in ransomware attacks fueled by the pandemic: 148%
- Only 18% of surveyed organizations say they are highly prepared to deal with cyber risks.
- Less than one-third of surveyed organizations forecast and model cyber risks.
- 92% of surveyed organizations rate cyber/technology risks as important or highly important.
- By 2027, there could be more than 41 billion IoT (Internet of Things) devices in use, affecting nearly every aspect of business life with each device as a potential target for a cyber-attack.

Today, organizations can no longer view risks as a single threat vector. Organizations must identify, understand, and prepare for the impacts of systemic and emerging risks across their complete value chain.

While gaps in preparedness vs. perception of preparedness leave organizations vulnerable to immediate and long-term disruptions of their business operations, assets, and revenue streams, the path towards resilience involves four common steps and behaviors.

To learn the four key steps towards building a more resilient business, download the Marsh Risk Resilience Report.

Tips for Compliance Officers facing a ransomware attack: What to do during the Incident

Minimise Exposure and Maximise Backup

- Isolate the ransomware infection by turning off servers and computers throughout the enterprise and disabling their LAN and WiFi connections or blocking network traffic to them. Ransomware moves quickly and can substantially disable an entire enterprise in minutes.
- Eradicate the malware executable code from networks and systems. Be aware that there are likely to be many copies of the malware throughout your IT environment. Additionally, be mindful that hackers sometimes hide malware in unexpected places (such as connected network devices like printers) that can reactivate and execute the original attack.
- Do not delete related files such as key files, text files, or ransomware notes as they may be helpful for understanding the threat actor's tactics or needed for recovery. Secure the most recent good backup in offline storage.
- Recognise that regardless of the data restoration approach, full restoration of the affected data will require considerable hands-on work and can take many days.

Tap into Insurance Expertise

- If you have cyber insurance, engage your organisation's risk manager and your cyber insurance broker to review relevant requirements of the insurance program, the expectations of the insurer, and any ransomware-specific services that the carrier may offer (such as cryptocurrency payments support).
- If you decide to pay the ransom, confirm with your carrier before making the payment. Many carriers require that they pre-approve in advance of a client making a ransom payment.

Follow Your Internal and External Guidance

- Follow the organisation's cyber incident breach response plan, including pre-established procedures related to ransomware, such as those outlined above.
- If your company has a pre-existing contract with a cyber forensics provider, consider separate contract arrangements if that provider is to support the ransomware incident. Consult with your counsel. Payment to the providers through a distinct budget and management structure may preserve attorney-client privilege.

Execute on the Ransom Payment – Or Don't!

- The final decision on whether to pay should be made through careful internal deliberation after sufficient legal advice and cyber forensic technical analysis.

- If the decision is made to pay the ransom, follow the instructions provided, consistent with the guidance of the cyber forensic team.
- If the decision is to not pay the ransom, then:
- Identify impacted systems. Wipe and rebuild them in accordance with pre-defined IT procedures and priorities to ensure they have no remaining ransomware/malware. Do a complete wipe and reformat of all storage devices, and restore the data from known sound sources.
- Once all systems are cleaned—and operating systems, applications, and data are restored—then the network can be re-established and declared operational.

Remember: Ransomware is a critical risk faced by most organisations in the evolution of cyber risk, and cyber incidents. Compliance officers have a critical role to play in acting proactively, to prepare, respond, recover, and recoup losses from ransomware attacks.

Peter Links
Practice Leader: Strategic Risk Consulting
Marsh Africa

WHERE TO NEXT? THE CASE FOR CRYPTO-ASSET REGULATION JUST GOT BIGGER

The alleged loss of some $3.6bn bitcoin through Africrypt investment company brings home just how risky this asset class truly is. Such incredible loss, though unfortunately not yet falling under the FSCA's direct responsibility is likely to impact the velocity of crypto-asset regulatory development.

The recent announcement by the Intergovernmental Fintech Working Group (IFWG) sheds light on its position on regulating crypto-assets – and change in this arena couldn't come sooner. Through its new position paper, which may now be updated in light of this latest scandal, several principles are put forward and are at the core of the objectives of the IFWG. The main objective being protection against the risks of crypto-asset investing.

The inherent risks of investing in crypto-assets are being addressed differently

Through the current paper, the regulator will bring crypto-assets into the South African regulatory fold in 'a phased and structured manner'. The risks associated with this volatile asset class stand. Regardless of the status of regulation, investing in crypto-assets is risky and there is a high chance of financial loss, as clearly evidenced by the most recent market abuse scandal, even though there is also a high chance of reward through great returns. Keep in mind that liquidity in the market very much matters when it comes to selling out, provided you have chosen a profitable option, so timing becomes another crucial element of getting crypto-asset investing right, and earning a profit safely. Choosing the right cryptocurrency investment to align with is also an essential component. Due diligence has never been more important.

The principles that count!
The IFWG outlines six key principles as below:

1. Crypto-assets must be regulated appropriately.
2. An activities-based perspective must be maintained.
3. A risk-based approach to regulation crypto-assets must be applied.
4. The IFWG encourages a truly collaborative approach to crypto-asset regulation.
5. Digital and financial literacy must increase so consumers are aware of the inherent risks of crypto-assets.
6. A continuously proactive and dynamic approach must be taken to monitoring and maintaining the crypto marketplace, particularly in line with international best practice in real time. This could include setting up industry bodies, as an example.

Recommendations on the way to regulation

The FSCA's responsibility for market conduct supervision is to extend into the crypto-asset space, but while the IFWG has made 25 suggestions within this roadmap so far to get closer to regulation, the paper reiterates that the IFWG does not endorse this asset class. Their goal is to reduce risk through regulation and through the paper, their recommendations can be broken down into three key focus areas. These are anti-money laundering and dealing with the financing of terrorism, cross-border financial flows and the application of financial sector laws.

Current exchange control regulations do not explicitly include crypto-assets but the SARB's Financial Surveillance Department (FinSurv) is certainly taking notice, particularly with daily crypto asset trading values in South Africa exceeding the R2 billion mark at the beginning of this year. With the recent alleged losses far surpassing this figure, this really is a dynamic, if dangerous asset class that should be treated with extreme caution by potential investors. The position paper states that 'by gradually bringing crypto-assets into the South African regulatory purview, the most pertinent and immediate risks that have been identified around AML, cross-border financial flows and consumer protection will be addressed. 'Relevant developments through bodies like the Basel Committee on Banking Supervision have further supported the drive to regulate crypto-assets.

Crypto assets remain highly speculative at this time, and it is unlikely that this will change anytime soon, however, the regulatory wheels are turning and trying to bring this new asset class into the mainstream of the river. For consumers who cannot wait for regulatory protection, the rules of old apply. Understanding and noting the risks and not simply focusing on the potential reward can be the first step to avoiding a crypto scam. Undertaking an appropriate due diligence remains the best start to a good crypto-asset investment decision.

Crypto-assets should be monitored closely if it piques your interest as an investment asset class. It's a positive step that regulation has taken note of the trend towards this exciting asset class, with more protection for investors not too distant on the horizon. Compliance officers should also look to upskilling in preparation for new compliance requirements that are sure to arise.

Remember the old adage… if it is TGTBT then it probably is!

Richard Rattue
Managing Director
Compli-Serve SA

ARE THE STAKES HIGH ENOUGH? CHANGING THE NARRATIVE BY ADAPTING OUR ATTITUDES

Compliance, along with legal, is perhaps one of the most under-valued departments in any business. It is so often seen by the rest of a business as a stumbling block to "real" business activities – a view that can often make the job of a compliance officer more difficult and unrewarding.

How many times have you, as compliance officers, felt like other employees in the business behave like teenagers being told by their parents to do something as they rebel against having to take steps to comply with a particular requirement? How many times have you wanted to retort "Because I said so!" and perhaps ended up saying "Because FICA" or "Because POPI"? I was watching a medical tv drama the other night and the neurosurgeon was telling the parents of a child that even if he tried to explain why they needed to do a particular procedure on the child and what it all entailed, that they wouldn't understand, and that the situation was too urgent to "waste" time. Seeing the shock on the parent's faces you could see that they were aghast at the Dr implying that they were not intelligent enough to understand, but they begrudgingly had to blindly agree to the procedure without first having the required understanding. I've seen so many occasions in business where the rest of the business has felt like the Dr was the compliance department. People like to understand why they're compelled to do certain things, understand the risks for themselves and to make decisions accordingly.

Like most things in life, to obtain greater compliance a high degree of buy in is required from the relevant stakeholders. In a business setting, that may mean involving various departments in a workshop to thrash out what the compliance strategy of the business needs to be and how it should be implemented. Compliance should be there to guide the workshop in relation to the key compliance risks for the business, what the consequences of non-compliance are and together with the rest of the workshop, strategise on the ways in which the business chooses to mitigate against such risks.

You may have heard of the T-Shaped lawyer - in a similar way compliance is one of those areas that requires the compliance officers to either be multi-skilled, or to have access to multi-skills and involving other key stakeholders is one of the ways in which the compliance officer has access to multi-skills. We need to be thinking about how we, as compliance officers can be better communicators than my example of the neurosurgeon, to empower people through

relevant knowledge that enables them to choose to comply, rather than be compelled to comply.

So, how do we break it down? How do we make compliance the easy choice? You'll need to have a look at what is going to be best in your business environment, some of you are only going to be dealing with executives and that requires one level of communication, some of you perhaps deal with factory workers whose literacy skills are somewhat disparate. Get creative and break it down. There are many infographics, for example, that explain various pieces of legislation and what they mean to us. Think about what the main points are that you need employees to know and help them to understand how the actions you are asking them to take assists the business in attaining its risk strategy goals. Think about what the consequences would be if the business failed to comply…would it mean a fine under POPIA of up to R10million? What would that mean in practical terms for the employees of the company…how would it affect them…no bonuses perhaps…pay cuts?

As compliance officers, we have a choice in terms of how we carry out our duties. Do you have a look at a particular transaction and immediately send through to the relevant business unit a standard list of compliance requirements without applying your mind to it? (when last did you actually review such a list?) This often wastes the time of the business unit and can present a time hurdle for the go-ahead of a project. Or, do you as the compliance officer look at the transaction business has sent through and confirm in your mind that any compliance tasks are all relevant? Are there any milestones that you can perhaps suggest in terms of timing for the project and how you can assist business in achieving them? Ultimately, our job as compliance officers is to enable business whilst ensuring that business complies with its legislative and regulatory requirements.

If, as a compliance officer you are battling to enforce compliance in your business first check your approach. Is business seeing you as a hurdle, and if they are my suggestion would be to get back to basics. Go back to the beginning. Make a list of the most important pieces of legislation and regulations, which the business must comply with and next to it make a list of the consequences of non-compliance. If you do not already have a documented compliance strategy in place for the business, I would suggest that you attend to that first through the inclusion of relevant stakeholders. If you do have such a strategy in place, revisit it by including those stakeholders and asking them what works, what doesn't work and what suggestions they may have to achieve compliance whilst enabling the business. The key to the success of compliance, like with any relationship, is communication.

Cherryn-Paige Bissett
Director
Paige Law and accredited supplier of BarnOwl compliance content

LawExplorer

LOGGING INTO THE CYBERCRIMES ACT

Globally, the only international treaty that addresses cybercrime is the Budapest Convention. South Africa became a signatory in 2001, and this treaty is aimed at harmonising national laws and establishing international cooperation against cybercrime. On 2 June 2021, South Africa's own Cybercrimes Act was signed into law, which brings South Africa up to international standards for fighting cybercrime. It's a feather in our cap, but will this feather round off a good look, or cramp our style?

South Africa's Cybercrimes Act consolidates cybercrime laws into one place and aims to improve the security of our country. Our well-developed financial infrastructure makes us an attractive target for Cyber Criminals. Our digital economy also represents significant opportunities - from e-commerce to streaming and subscription models - which invites a welcome financial injection into our struggling economy. But, cybercrime threatens organisational operations, and can stifle innovation and growth. As countries and companies become increasingly dependent on complex, internet-enabled business models, their vulnerability to cyber-attacks increase. What does that mean for their stakeholders?

At the core of the Cybercrimes Act lies the offences that constitute cybercrimes. To date, the absence of any clear definition has hampered investigations and prosecutions of internet-based crimes in South Africa. The Act however does not define "cybercrime" as such, instead, it has created a number of offences that constitute cybercrime. These include:

- Unlawful access to a computer/device (even a USB)
- The illegal interception and processing of data
- Unlawful use or possession of a software or hardware tool
- Unlawful acquisition, possession, receipt or use of a password
- Cyber forgery
- Fraud, extortion and the theft of incorporeal property.
- Malicious communications if they incite violence or damage to property, threaten persons with violence or damage to property
- The disclosure of data messages that contain intimate images

This seems positive for South Africa and its people by showing tangible commitment to combatting cybercrime, but there are a few practical concerns around this new legislation. A disgruntled ex who shares your nudes, or scammers who steal your passwords through phishing will get their comeuppance. In the same breath, if you share your online banking details and log-ins so someone can access your money, you've just crossed a line and could be fined or imprisoned for 10 years. Not so rosy now, is it?

This Act affects everybody with an electronic device. The net is cast far and wide - from individuals, to organisations, to governments, to law enforcement. Cape Town-based corporate law firm Michalsons describes the Act as a "bad law", potentially rendering it highly lucrative for lawyers and consultants. Michalsons points out that POPI (the Protection of Personal Information Act) has few but specific crimes, and failure to comply doesn't mean one is committing a crime. However, once the Cybercrimes Act is effective, it essentially criminalises non-compliance with the POPI Act. Instead of these acts complementing each other, they have the potential to be in conflict. Deloitte advises that it's important to consider the Cybercrimes Act as part of "a larger privacy programme" as soon as possible, as post-compliance considerations will have a significant impact on cost, resourcing, technical solutions and information security architectures.

The Act imposes an obligation on all Electronic Communications Service Providers (ECSPs) and financial institutions to report cyber offences in the prescribed form and manner to the South African Police Service. Any information which may be of assistance in an investigation should be preserved and at their own expense. They are required to work with law enforcement (where applicable) in the investigation of cybercrimes which may involve the handing over of data and hardware. However, the Institute of Security Studies (ISS Africa) states a lack of trust between role-players could potentially hamper the spirt of willingness to do so. Balancing security, privacy and personal freedom when swift investigations are needed for cybercrimes has the real potential to lead to legal challenges.

This Act must be implemented effectively and speedily within a year of coming into force. However, with current levels of relevant knowledge, experience and staffing of key roleplayers in enforcement being in short supply, prospects seem rather gloomy.

The provision of training, and creating sufficient awareness is going to be absolutely crucial. Seasoned compliance officers are well acquainted with the fact that if not properly enforced, regulations cannot effectively achieve intended goals.

For now, it's best we play it safe!

The Cyber Crimes Act 19 of 2020's commencement date is yet to be proclaimed by the President and will appear in the Government Gazette sometime in the future.

Renate van Onselen
Marketing Manager and Compliance Consultant (CProf)
LawExplorer

THE COMPLIANCE INSTITUTE SOUTHERN AFRICA WOULD LIKE TO THANK ALL OF OUR CONFERENCE SPONSORS AND EXHIBITORS FOR A SUCCESSFUL 2021 CONFERENCE

WE LOOK FORWARD TO SEEING YOU
AT OUR CONFERENCE NEXT YEAR

24 – 25 AUGUST 2022

SAVE THE DATE