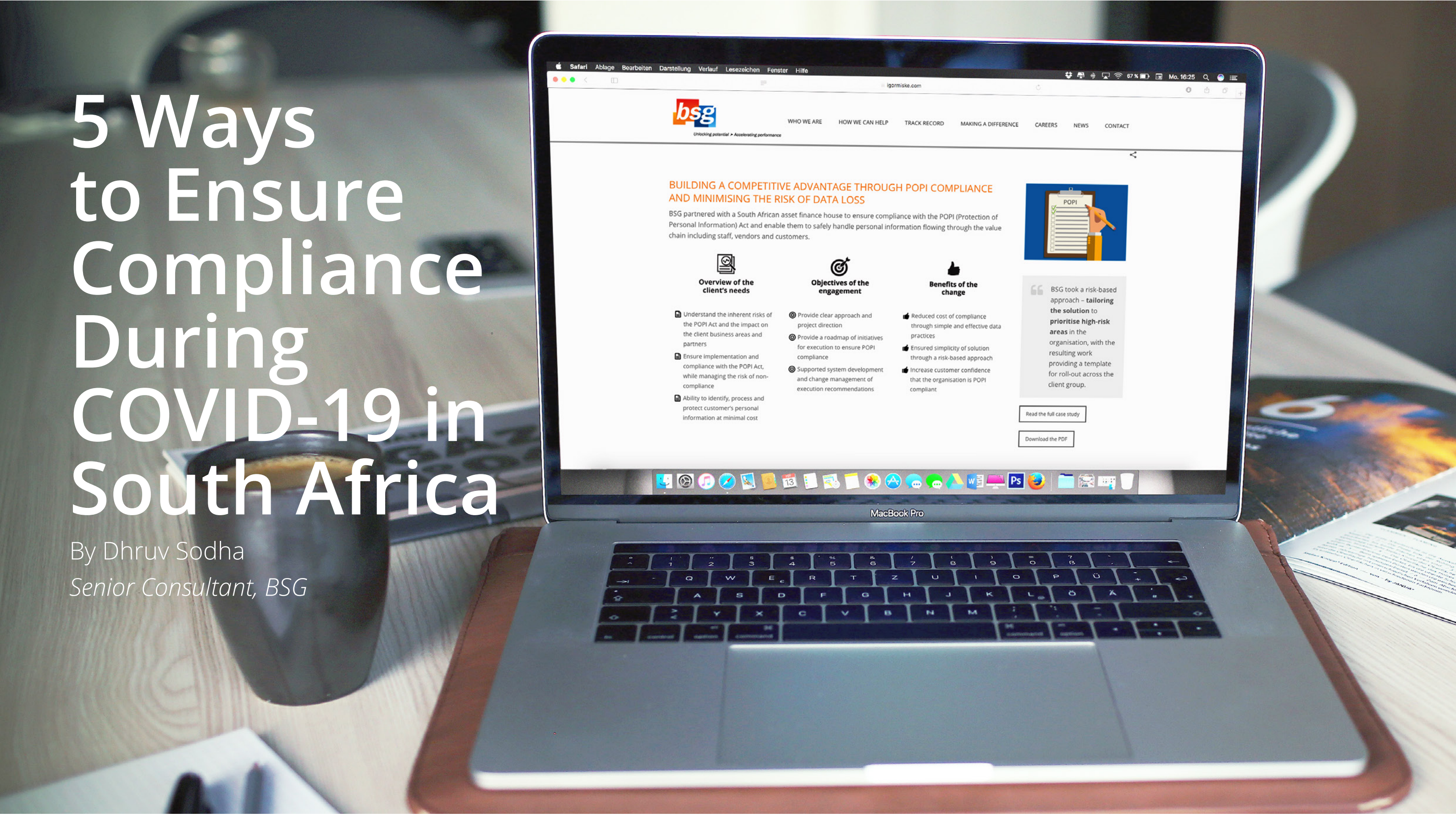
5 Ways to Ensure Compliance During COVID-19 in South Africa

By Dhruv Sodha
Senior Consultant, BSG



BUILDING A COMPETITIVE ADVANTAGE THROUGH POPI COMPLIANCE AND MINIMISING THE RISK OF DATA LOSS

BSG partnered with a South African asset finance house to ensure compliance with the POPI (Protection of Personal Information) Act and enable them to safely handle personal information flowing through the value chain including staff, vendors and customers.

Overview of the client's needs

- Understand the inherent risks of the POPI Act and the impact on the client business areas and partners
- Ensure implementation and compliance with the POPI Act, while managing the risk of non-compliance
- Ability to identify, process and protect customer's personal information at minimal cost

Objectives of the engagement

- Provide clear approach and project direction
- Provide a roadmap of initiatives for execution to ensure POPI compliance
- Supported system development and change management of execution recommendations

Benefits of the change

- Reduced cost of compliance through simple and effective data practices
- Ensured simplicity of solution through a risk-based approach
- Increase customer confidence that the organisation is POPI compliant

BSG took a risk-based approach – **tailoring the solution** to **prioritise high-risk areas** in the organisation, with the resulting work providing a template for roll-out across the client group.

The manner in which an organisation's employees collaborate with each other has been transformed since COVID-19 was declared a global pandemic. With a large portion of the global workforce working from home, this has turned out to be the largest, forced experiment in testing the effectiveness of a distributed workforce. While there are many proven benefits an organisation can reap, one must first understand the compliance challenges to determine the extent to which these benefits can be realised.

Ensuring adherence to various regulatory legislation and company policies relating to data security, for example, can become a challenge with a distributed workforce. Many organisations have been caught off guard and are now scrambling to implement measures to enable continued delivery, while mitigating risks of remote work. Despite a few organisations having tested such measures for some time, many are still experiencing some challenges. Some of these challenges and suggested mitigations associated are outlined below.

1. Ensure increased awareness of compliance requirements

Not only do existing policies that allow work to continue remotely need to be strengthened (e.g. policies on data security, client information confidentiality and management of company infrastructure), but there needs to be increased awareness and adherence to these policies. Driving awareness and change when employers have face-to-face interaction with employees is challenging enough, but doing so virtually is an even bigger challenge.

There is a need to be creative with how compliance requirements are communicated. Facilitating knowledge sharing sessions via video conferences to educate the workforce, or even implementing gamification methods to ensure adherence to risk mitigation measures are just some of the steps that must be taken.

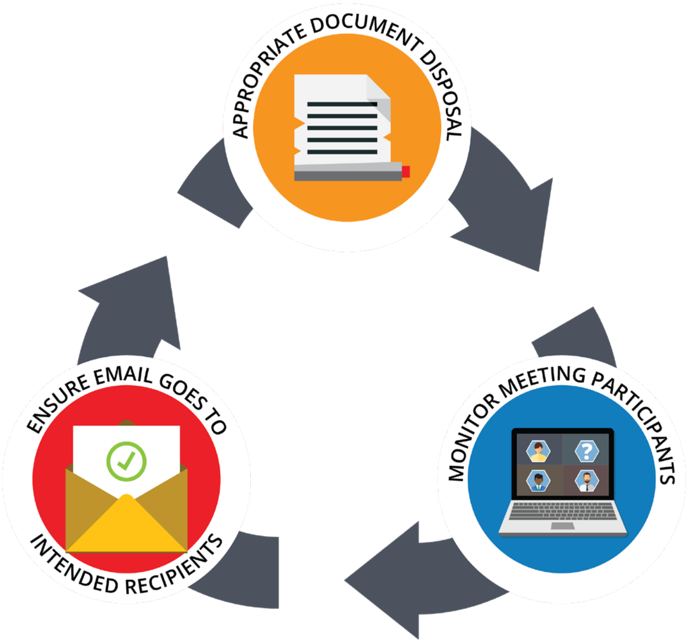
> ***Increase visibility of data security policies across your organisation***

2. Treat sensitive information even more securely than before

With employees utilising home network connections – and in some cases, even public networks – to access company resources, weakened security safeguards increases the risk of malicious attacks, such as hackers using unsecured network connections to distribute malware. Having infected software on corporate devices can financially cripple organisations. For smaller firms, this becomes a bigger challenge, as enterprise-grade security safeguards come at a significant, often unmanageable, cost.

Additionally, when dealing with personal information of stakeholders, most incidents typically take place due to human error. When employees are not located in an office, the tendency not to adhere to data security best practices increases, e.g. using personal email for work-related items. The Protection of Personal Information Act (2013) requires organisations to put in place additional security safeguards to protect the personal information of anyone it deals with. Ensuring measures such, as the following are in place will reduce the risks of leakage or misuse:

- Not disposing of sensitive documents irresponsibly, in home refuse bins, but instead waiting to get back to the office to dispose of them appropriately
- Ensuring only invited participants join on conference calls, to avoid sharing of sensitive information to the unintended recipients
- With a sharp spike in the use of electronic communications, like emails, it is imperative to ensure emails are sent to the right people. Tools can be developed in-house to warn the sender when a potentially unintended recipient has been included into a mail


APPROPRIATE DOCUMENT DISPOSAL
MONITOR MEETING PARTICIPANTS
ENSURE EMAIL GOES TO INTENDED RECIPIENTS

3. Put in place stricter measures on the use of collaboration tools, without restricting the usage where not necessary

In large organisations, collaboration tools are typically taken through stringent assessments to ensure they do not put the organisation at risk. However, organisations will struggle to stop the use of similar free-to-use tools. For example, the videoconferencing tool, *Zoom*, which lacks stringent security safeguards, such as end-to-end encryption, has recently dealt with several security issues as its usage has skyrocketed globally.

Wherever possible use videoconferencing tools with end-to-end encryption

Instead of trying to stop the use of such tools, organisations should focus on creating awareness of risk mitigating steps that can be taken. For example, advising employees to avoid recording calls, to not share sensitive data and to avoid clicking on or sharing links within these tools. Furthermore, password protecting all conference calls on these tools can be an added measure to stop rogue attendees from joining, which has become a reality recently.

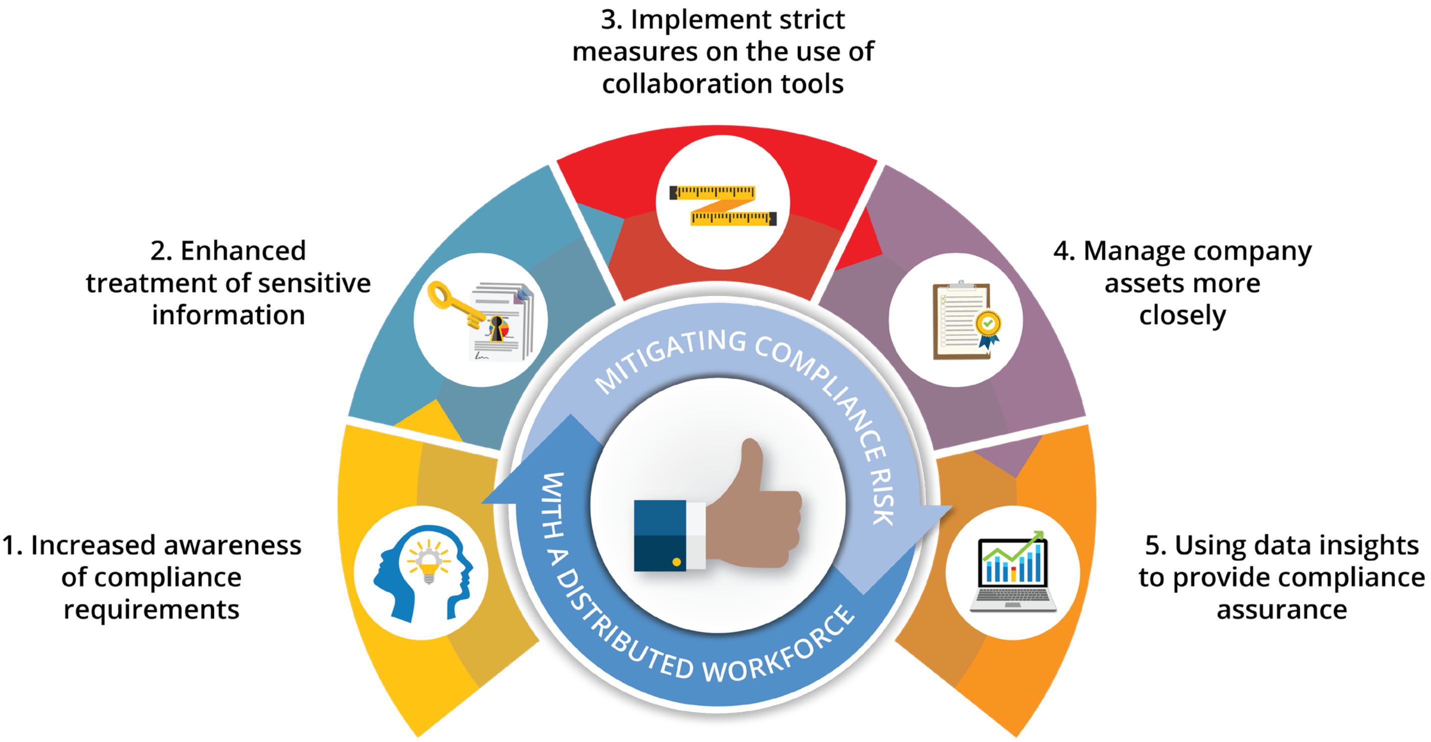
4. Managing company assets more closely

As part of an IT Asset Management Strategy, using company assets off-site isn't a new concept, the risk of mismanagement and loss of assets has increased exponentially. Implementing a comprehensive asset register will provide a view of the assets outside the organisation's premises. With a better view of the size of the risk, an organisation can make a fact-based decision about additional measures required, such as increasing insurance cover. Technological solutions, like geofencing, give organisations more control over additional security measures implemented on a device when it is not within a predefined location boundary.

Consider geofencing technology to implement additional security measures for off-site delivery

5. Use data to provide compliance assurance

Monitoring compliance and providing assurance depends on having the correct data to support it. With a distributed workforce, organisations have access to an increasing wealth of data with employees online, now more than ever. The increase in access to data must be seen as an opportunity to support compliance monitoring and testing, with an ultimate view to mature such a capability and realise predictive monitoring in the future.


3. Implement strict measures on the use of collaboration tools
2. Enhanced treatment of sensitive information
4. Manage company assets more closely
1. Increased awareness of compliance requirements
5. Using data insights to provide compliance assurance
MITIGATING COMPLIANCE RISK
WITH A DISTRIBUTED WORKFORCE

Data-driven insights can be used to understand which tools are being used, what data and how much is flowing between users and systems whether these controls are effective. This data can also be utilised to proactively identify data breaches taking place.

As much as these strengthened measures are necessary during this time, it is likely that a distributed workforce will become more widely accepted after this pandemic. It would be best for organisations to use this challenge as an opportunity to relook at the way it deals with the non-compliance risk of a distributed workforce and implement future-proofed measures to mitigate the risk now.

Use data to understand the effectiveness of controls in place across your business

Let us help you. If you have concerns, we can work with you to determine risks and put plans in place to mitigate them to help you reap the benefits of assured compliance. BSG is fully operational with local insight and experience, and we can work with you to design the best solutions for your needs.

About BSG

As a homegrown South African Consulting and Technology company, BSG is uniquely positioned to deliver solutions tailored to the South African context.

We have more than 20 years' experience across the banking, specialised financial services, insurance, healthcare, telecommunications, and oil and gas sectors. By employing a multi-skilled approach, BSG effectively leverages our clients' data to create solutions that improve the experiences of their customers and solve enterprise-scale challenges.

We understand the dynamics of Business and Technology, which allows us to create flow between supply and demand, bridging the gap between business and IT. We work with our clients to drive out success, transforming their operational platforms and creating the customer experiences they need.

Visit us at **www.bsg.co.za**

Get in touch

Jurie Schoeman
BSG Chief Executive Officer
jurie.schoeman@bsg.co.za
+27 (0)83 30 27169
+27 (0)11 215 6666

Unlocking potential ➤ Accelerating performance

BSG

The Towers - South Tower, 18th Floor
2 Heerengracht Corner
Hertzog Boulevard, Foreshore
Cape Town, 8000

Tel 021 418 0888
Email info@bsg.co.za

Oxford Terrace
No. 3 Ninth Street
Houghton Estate
2198

Tel 011 215 6666
Web ***www.bsg.co.za***