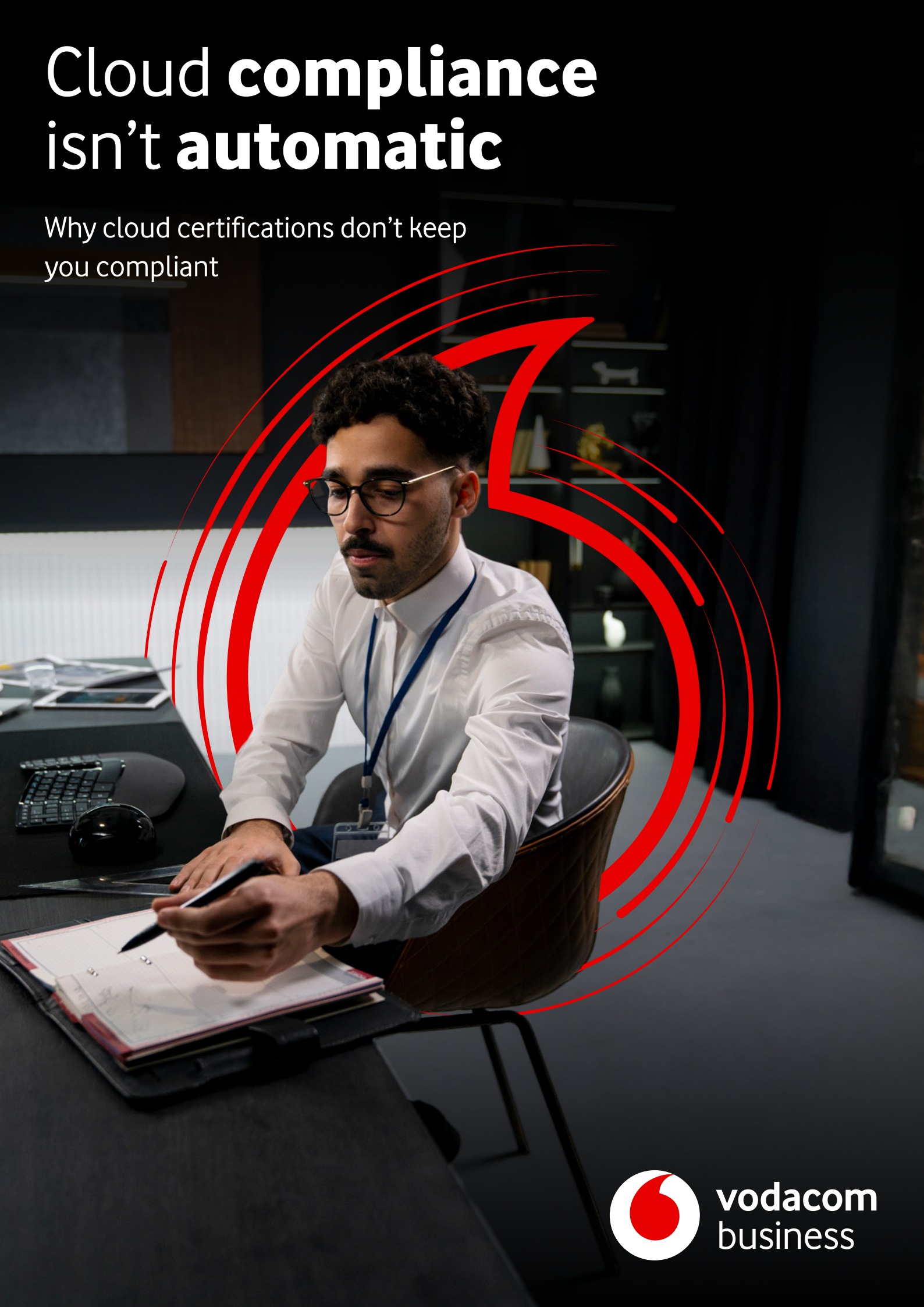
Cloud **compliance** isn’t **automatic**

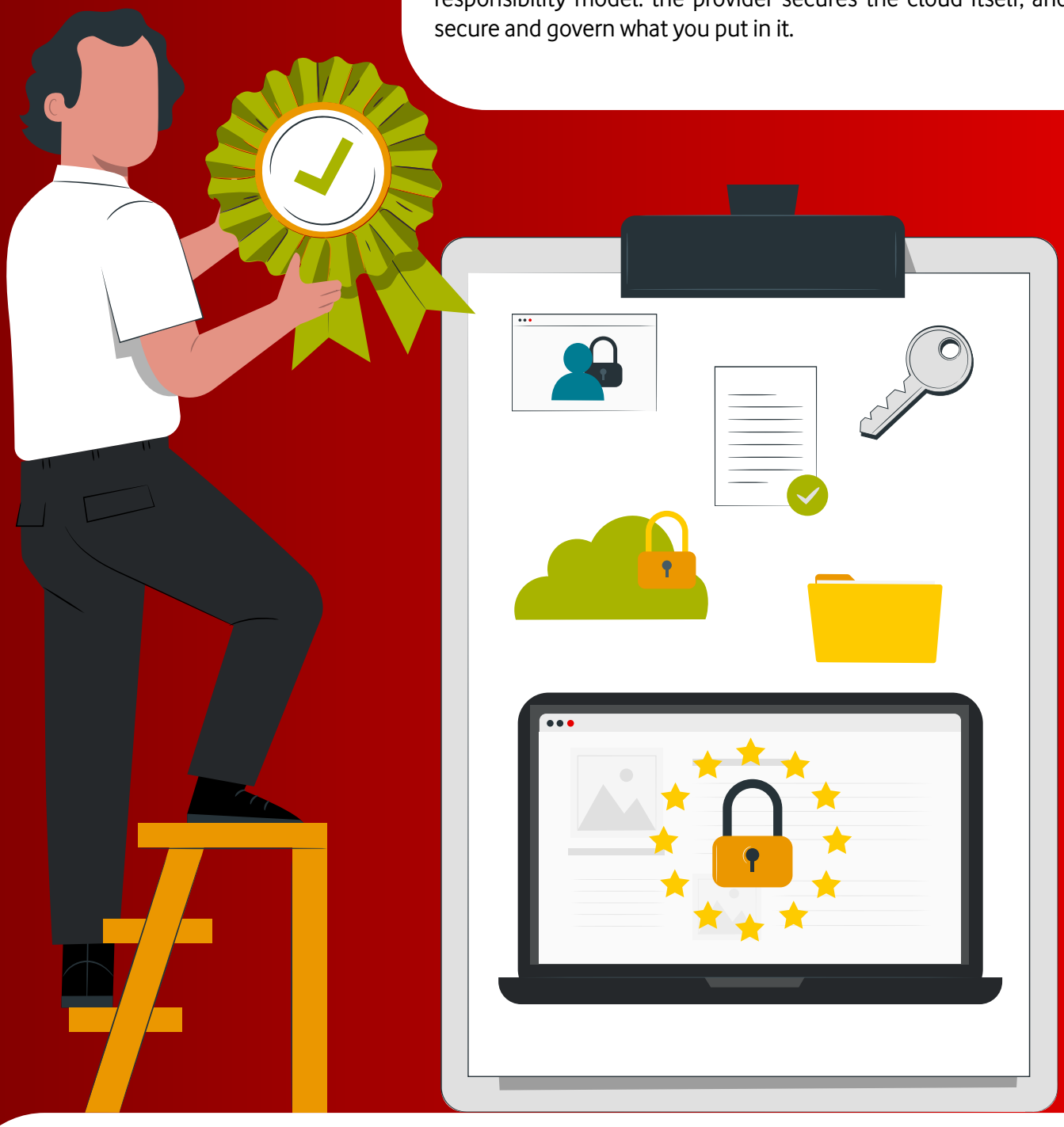
Why cloud certifications don’t keep you compliant



vodacom business

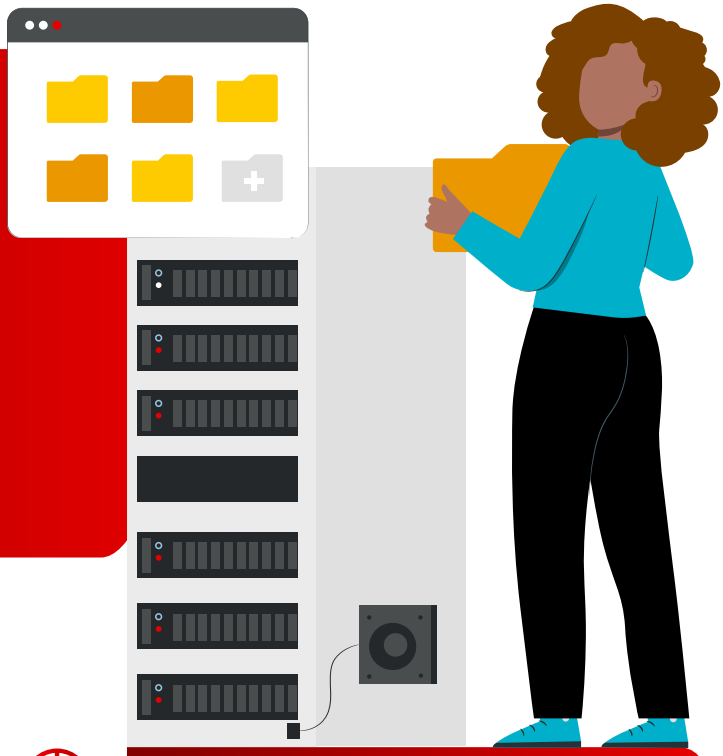
If you're already using cloud, you've probably seen the promise: **"Our platform keeps you compliant."** It's a comforting message, but it's not the full truth. Providers like **AWS**, **Azure**, and **Google Cloud** hold certifications such as ISO 27001 and SOC 2, and they offer GDPR-compliant data processing terms. That proves the platform is secure.

But regulators don't judge compliance on the platform alone. They judge how you configure it and how you handle your data. This is the shared responsibility model: the provider secures the cloud itself, and you must secure and govern what you put in it.



What the provider covers

Cloud providers take care of the foundation: physical datacentre security, infrastructure patching, managed services, and global certifications. Their job is to keep the environment itself safe and reliable, and to give you strong security tools to work with.



What you must cover

Data storage and movement

You choose the region where data is stored and whether it moves across borders. In South Africa, POPIA restricts cross-border transfers unless certain safeguards are in place. Selecting the wrong region in your console could mean a compliance violation before you even process a single record.

Retention and deletion

You decide how long data stays in your systems and when it gets erased. Both POPIA and GDPR require data to be deleted once it's no longer needed. That means setting up lifecycle rules or retention schedules in your cloud tools, not relying on the provider to do it automatically.

Access control

You configure who gets in and what they can do. Multi-factor authentication, role-based access, and least-privilege permissions don't switch on by themselves. They need to be enabled and reviewed in your identity and access management settings.

Encryption and key management

Encryption options are built into most cloud services, but they don't count unless you turn them on. You also need to decide how encryption keys are generated, rotated, and controlled.

Monitoring and incident response

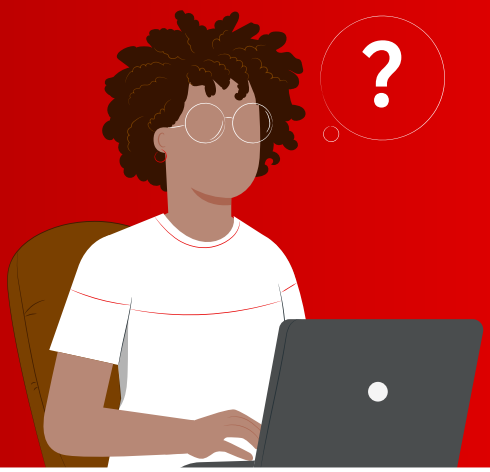
Cloud systems can keep a record of every action, but this isn't always switched on by default. You need to turn on logging, decide which activities should trigger alerts, and have a clear plan for how to respond when something suspicious happens. If you don't, you will have a hard time proving compliance or spotting security problems.

Policies and governance

Your provider does not write your policies. You need governance rules that cover how data is classified, who approves access, how incidents are handled, and how your cloud usage ties back to POPIA, GDPR, and ISO 27001.

Why this matters

Most compliance failures come from customer-side settings and data decisions, not from provider breakdowns. A storage folder left open on the internet, the wrong data region, or disabled logging is all it takes to put your organisation at risk of fines. Saying “but we were on Azure” won’t carry any weight with regulators. They’ll look at how you configured and managed the environment.

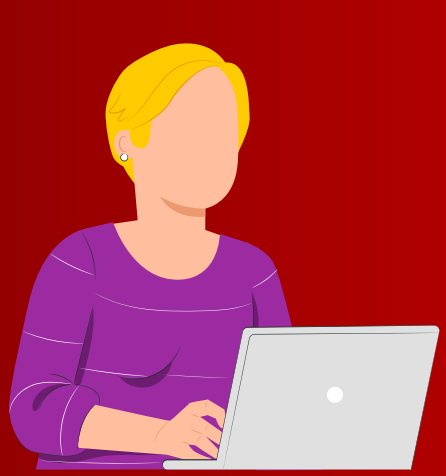


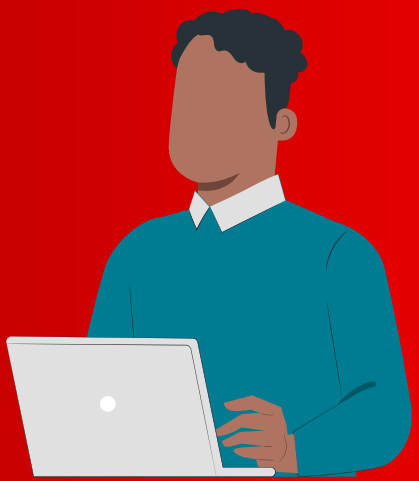
What’s an easy way to stay covered?

If you’re thinking, “This sounds like a lot to stay on top of,” then one way to make it easier is to work with a vendor-neutral partner. A provider like Vodacom Business can help you choose the right cloud setup for your compliance needs, guide you on how to configure built-in security features properly, and provide monitoring and connectivity services. It doesn’t replace your responsibility, but it removes much of the complexity and gives you practical support to keep your settings and data under control.

Wrap up

Your cloud provider gives you a secure, certified platform. Whether your business stays compliant depends on how you configure it and manage your data. By understanding your role, making the right settings decisions, and using the tools available, you can meet regulatory expectations and strengthen your overall security posture.





vodacom
business