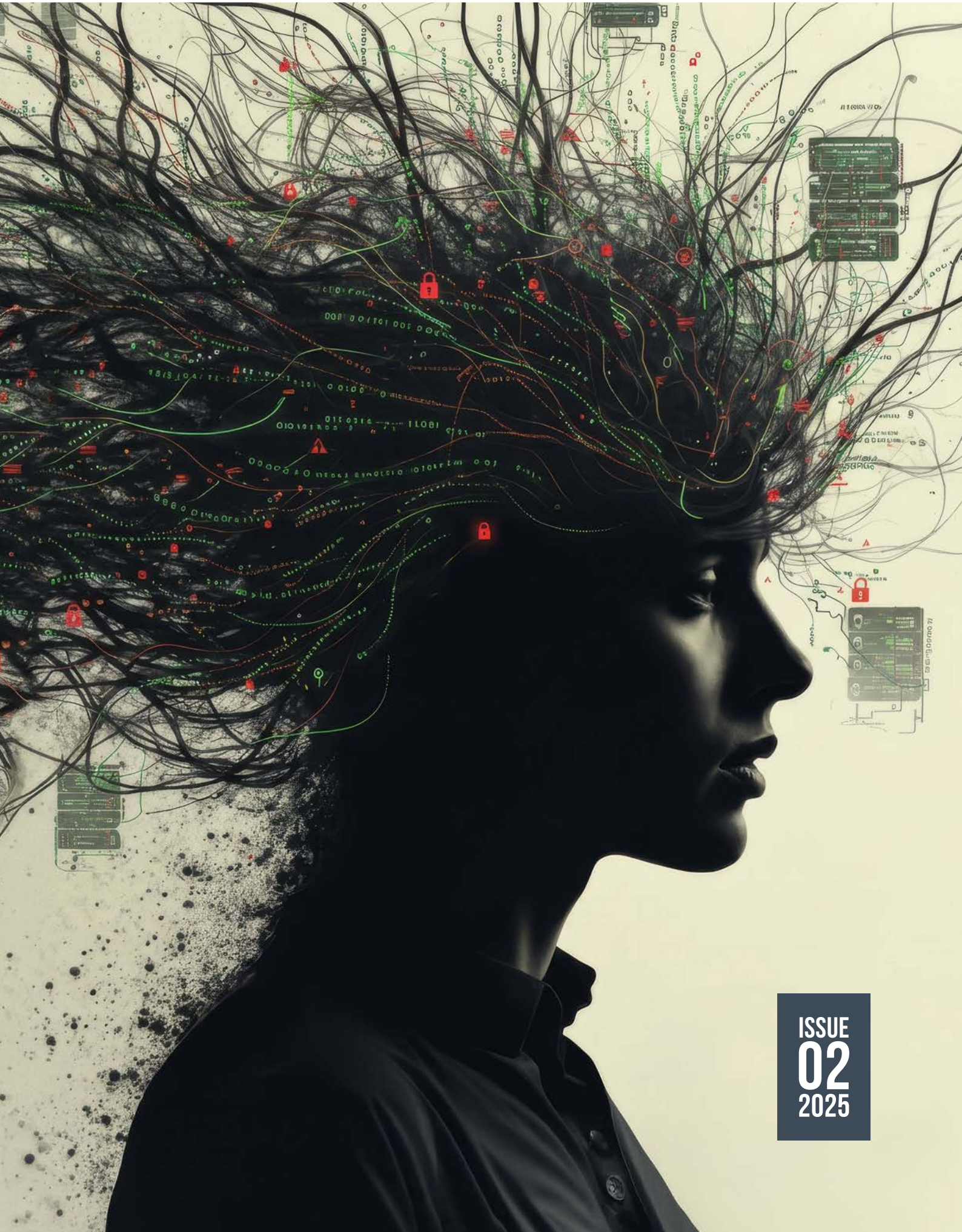


# TECHNOLOGY PRACTICE



ISSUE  
**02**  
2025



# CONSIDERATIONS FOR STORING CLIENT DATA IN THE CLOUD

## WHAT ACCOUNTANTS MUST WEIGH AS CLOUD ADOPTION RESHAPES COMPLIANCE, SECURITY, AND CLIENT TRUST

The shift to cloud storage promises accountants greater efficiency, agility, and scalability. But with these advantages come concerns about security, ethics, and compliance. As firms increasingly handle sensitive financial data in cloud environments, they must weigh issues such as data sovereignty, vendor lock-in, and shared responsibility.



Everyone in the profession knows the appeal of cloud: lower infrastructure costs, anywhere-access, and agility in scaling. For accounting practices, it means no more costly server rooms and no more frantic backups to external drives.

Instead, client data is stored, managed, and accessed seamlessly. But cloud is not a silver bullet, and according to Steve Porter, Managing Director at Metrofile Cloud, preparation and a firm strategy for usage should dominate any conversation about moving to the cloud, ahead of its technological benefits.

"I am not a proponent of public cloud. Every provider wants to lock you in," says Porter. "So the first step is having an exit strategy. The second is understanding that your data remains your responsibility. If it's gone, it's not the provider's problem."

For Porter, data sovereignty is equally critical. South African firms often default to American or European applications without considering whether those services hold data locally. The Protection of Personal Information Act (POPIA) places the burden of compliance squarely on the business, not the vendor.

He adds that understanding where and how your data is stored, encrypted, and backed up should form part of any cloud migration plan. Local hosting or hybrid solutions can reduce risk, ensure faster recovery, and simplify regulatory compliance. In the end, the goal isn't just cloud adoption. It's cloud accountability.

## SHARED RESPONSIBILITY IN PRACTICE

The "shared responsibility model" is often marketed by global providers. In theory, vendors handle infrastructure security while firms protect data and access. But in practice, Porter argues, many organisations misunderstand the split.

"How many of us actually read the terms and conditions when signing up? Very few. Most firms don't realise that if data is breached or lost, the responsibility lies with them."

Lee Syse, Director of Product & GTM at cloud provider Routed, agrees that firms cannot abdicate responsibility to providers. "There is always a demarcation between what the cloud provider secures and what the client must secure," he says. "Identity and access management, backups, redundancy; these all remain your responsibility. Too many firms assume being 'in the cloud' means everything is taken care of automatically."

This misunderstanding can have serious consequences. Firms that don't invest in proper governance, access control, and backup strategies often discover too late that cloud compliance doesn't equal cloud safety.

Syse advises developing a shared responsibility matrix that clearly defines who manages which controls, especially around encryption, patching, and recovery.

Regular testing, staff training, and documented protocols ensure that responsibility isn't left to assumption but embedded into daily operations.

## THE ETHICS OF CLOUD ADOPTION

For accountants, the ethical obligation goes beyond compliance checklists. Cloud makes firms custodians of client data in an environment where breaches have real consequences.

"From an ethical perspective, firms must ensure services are highly available and secure," says Syse. "If something goes down, the impact on clients can be massive. It's not about IT. It's about safeguarding client trust."

This requires more than technology investment. Staff training, access

controls, and clear policies are crucial. Human error remains the biggest vulnerability, whether through phishing emails or poor password practices.

A single careless click can compromise hundreds of client records. That's why building a culture of awareness is as vital as deploying sophisticated security tools. Regular simulations, clear incident response plans, and ongoing education can transform employees from weak points into the first line of defence.

Ethics in the digital age isn't just about keeping data safe. It's about preserving the integrity of the profession. Every accounting firm that handles sensitive information carries both a regulatory and moral duty to protect it.

## VENDOR LOCK-IN AND EXIT STRATEGIES

Both Porter and Syse highlight vendor lock-in as a recurring concern. While global providers deliver scale and convenience, they make it difficult, and sometimes costly, for firms to leave.

"Public providers build moats around their products," says Porter. "You only realise the scale of the lock-in when you try to migrate data. By then, you're trapped with costs or compatibility issues."

Syse adds that the deeper firms integrate with a vendor's platform services, the harder it becomes to move. Infrastructure as a Service is portable, but Platform and Software as a Service create dependencies that may require a full rebuild to exit. Even data formats and proprietary APIs can restrict freedom of movement. Without early planning, firms risk losing control over their own information and processes.

Both agree that the lesson for accountants is clear: read and understand the terms and



conditions before signing up, and build a plan for portability before it's really needed.

Keeping backups in neutral formats, maintaining clear data ownership clauses, and using open standards can prevent future headaches. Cloud agility is only real when you can leave as easily as you joined.

## DATA SOVEREIGNTY AND REGULATION

Cloud also raises pressing questions about where data is stored and who has access to it. POPIA sets requirements locally, while international frameworks such as GDPR add further complexity.

"Even if data is hosted in South Africa by a US-based provider, the US Cloud Act allows their government to subpoena it," says Syse. "If your client is concerned about sovereignty, you must consider a locally owned provider."

This issue is not merely legal. It is also about client perception. Firms must be able to reassure clients that their data is not only secure but protected from external interference. Data residency decisions influence how much trust clients place in their advisors. Even the appearance of exposure to foreign jurisdiction

can raise red flags for regulated industries such as finance or law.

For Syse, transparency is key: firms should know exactly where their data resides, how it's encrypted, and under which legal frameworks it falls. Clear communication about these factors strengthens relationships and builds lasting confidence in the digital services firms provide.

## SECURITY BEYOND THE BASICS

Relying on a provider's built-in tools is not enough. Firms need layered defences and these include:

- **Identity and access management:** Strong authentication, role-based access, and single sign-on.
- **Backups and redundancy:** Independent copies of data, not just provider-side replication.
- **Endpoint security:** Protecting staff devices, which often remain the weakest link.
- **Training and culture:** Regular awareness programmes to reduce phishing and social engineering risks.

"At home, you have an electric fence, dogs, infrared beams. Businesses need the same layers for their data," says Porter.

## LOCAL VS GLOBAL: FINDING THE BALANCE

This isn't to say that the value of global platforms should be dismissed outright. In fact, most firms already rely on multiple providers, such as Microsoft for email, Sage or Xero for accounting, and a local vendor for backups.

The challenge is balancing convenience with sovereignty, compliance, and exit flexibility.

Porter says he advocates for local solutions where possible.

"If a customer is unhappy, we hand them their data and say, 'Go find another vendor.' There are no egress fees. That's how trust should work," he says.

The sweet spot may involve smaller firms accepting that multi-cloud adoption is inevitable.

"Even a two-person consultancy will use different clouds for different needs," says Syse. "The key is to apply the same governance principles across all of them."

For most practices, this means standardising policies around access control, encryption, and backups, no matter the platform. Multi-cloud environments can provide resilience,





flexibility, and competitive pricing, but only if managed strategically. Consistency, visibility, and clear ownership are what keep complexity from turning into chaos.

## SKILLS AND STANDARDS

As cloud adoption matures, accountants will need fluency in both compliance frameworks and technology standards. Certifications such as ISO 27001 provide structured guidance for managing data, onboarding and offboarding staff, and developing recovery plans.

“You don’t know what you don’t know until someone shows you,” says Syse. “Frameworks like ISO 27001 help firms put the right policies in place to manage both people and technology.”

Beyond compliance, these frameworks instill discipline and accountability, which are key traits in an environment where client trust is everything. They ensure that firms show, not just security in theory, but traceability and control in practice.

For Syse, adopting a framework isn’t about ticking boxes; it’s about creating a repeatable standard for

how a firm operates digitally. In a landscape of evolving cyber threats, ransomware, and regulatory scrutiny, certification signals professionalism and readiness.

Firms that embed such standards into their daily culture don’t just meet compliance - they set themselves apart as trusted, future-ready custodians of client data.

## THE FUTURE IS IN THE CLOUD

Storing client data in the cloud is not optional anymore. It is a reality of modern practice. For accountants, the task is to ensure that efficiency does not come at the cost of security or trust.

The way forward lies in balance: leveraging the scale of global providers while building local resilience, investing in staff training alongside technical controls, and ensuring every contract is reviewed with an exit strategy in mind.

Cloud adoption is ultimately a question of responsibility. The provider may deliver the platform, but the ethical and regulatory duty remains with the accountant. In a profession built on trust, that responsibility cannot be - and must never be - outsourced.

**FROM AN ETHICAL PERSPECTIVE, FIRMS MUST ENSURE SERVICES ARE HIGHLY AVAILABLE AND SECURE.**

~ LEE SYSE, DIRECTOR, ROUTED