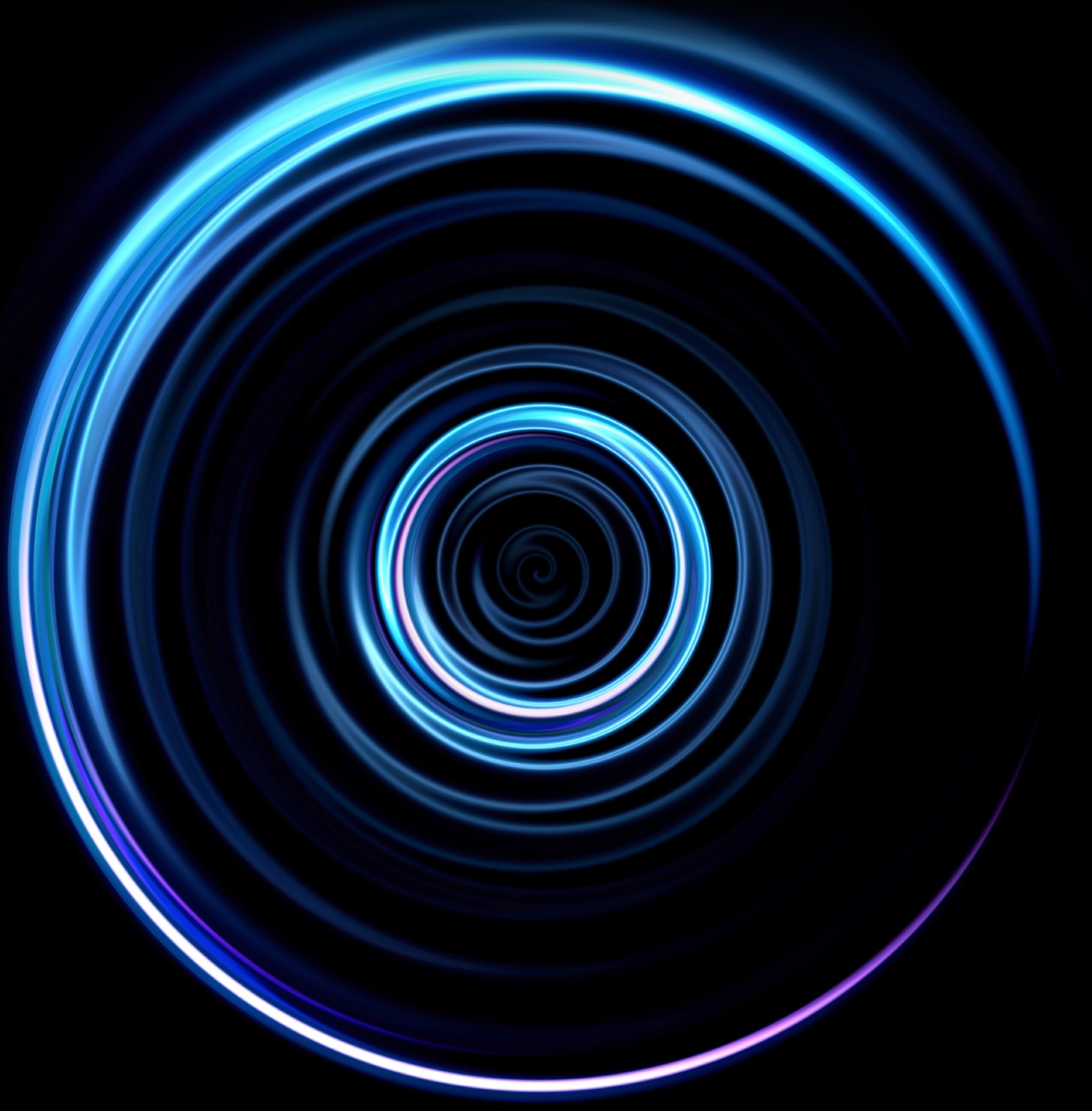
Feel Secure

Feel secure in the cloud
Imagining the changes, challenges
and opportunities



Deloitte.

CYBER
INTELLIGENCE
CENTRE™

When it comes to cloud computing, security and privacy can be ambiguous and difficult for organisations to quantify. As organisations expand their service portfolio, there is a move to leverage the scale and in some instances, business benefits to the cloud. Organisations that can manage enterprise risk in the cloud, stand to benefit by accelerating their business and competing in a connected world.

Security in the cloud relies on understanding the risks and developing a strategy – all while keeping in mind the end game: to transform your organisation into a secure, vigilant and resilient user of cloud technology. Risk awareness involves remembering that things are different in the cloud. For example, the enterprise security techniques you use to address your traditional problems might not have the same effectiveness when it comes to cloud technology.

As organisations flock to cloud computing, they will need new insights, new tools, and new procedures to effectively manage risk. Each new application of cloud technology and each form or configuration of cloud presents its own unique security and privacy challenges – its own set of policies, procedures, connections and checkpoints – that have specific considerations to address.

Plugging in

The future of cloud computing is analogous to modern electricity. In the 1800s, users needed to live near the generation point to get electric service. And safety was always an issue. Today, you don't ask about electricity availability. Outlets are everywhere. You just plug in and you rarely, if ever, think about safety or security. Cloud is headed in the same direction. Organisations are eager and willing to plug into the cloud, but safety is still on their minds. There are risks but organisations can mitigate the risks through new security tools and techniques, a vigilant approach to data-access issues, and practices that will allow them to operate resiliently in the face of threats.

Individuals and organisations are readily taking risks to get things done to move to the cloud. But often, amid the race to embrace the power of the cloud, they don't exactly know what the risks are. It's easy to say "it's worth the risk" when you don't fully grasp the nature of the risk and potential adverse consequences.

The highest-profile risks tend to centre on data residency (where data lives), data privacy (who can access data), and data leakage (loss or release of data through errors or malicious acts). In addressing data risks, organisations must focus on understanding the layers of risks and issues that are involved – from regulatory issues to reliance on service providers that have their own security concerns.

Mitigating risks

Mitigating and reducing risks can enable an organisation to operate efficiently as a secure, vigilant and resilient organisation – one that's on guard for new forms of threats to security and privacy. Successful organisations are policing themselves, their service providers, and their data partners to make sure that what they do meets internal security standards and the organisation's own risk appetite.

The relationship with suppliers stands out as especially critical. Organisations must seek a good understanding of suppliers' intentions and needs when it comes to using cloud technology, and then work to put in place the right controls for data to ensure privacy, guarantee residency and prevent loss.

Key questions

As organisations look to inject greater security into their cloud operations, essential questions emerge. Addressing these questions early can make the difference between a secure and insecure cloud.

Where does information reside, and where do you want it to end up?	In what small buckets, large pools, and massive lakes does your information now live? And where should it live? Sensitive information hidden in a seemingly benign pool of data could leak unexpectedly as you move more operations to the cloud. And leakage could have an impact on your reputation, resulting in real business losses.
How will you maintain control of your information as you turn to the cloud?	With traditional enterprise systems, encrypting and decrypting data as you move and share it offers a relatively easy way to assert control. But in the cloud, the system does not belong to you. It belongs to the cloud provider. Moreover, that provider might be based in another country, which could present some specific regulatory or privacy issues for you to address. You should realise that, from a regulatory angle, national and provincial privacy issues might not be as complex as you perceive them to be. For example, South Africa has privacy legislation like POPI that regulates the export of personal information (Data Sovereignty, Section 72) and it pertains both to the private and public sector. The dread of addressing privacy issues should not keep you from moving more operations decisively to the cloud. But you must address the control issue and know that, in some cases and for some applications, simply throwing an enterprise-centric technology at the problem might not work. The technology might not be mature enough to do what you want it to do. A more thoughtful approach can help you find the right encryption tools and allow you to collaborate with providers to ensure that the cloud approach will work and that it will work securely.
What is your organisation's role as your partners turn to the cloud?	Cloud providers are just one part of the picture. It's important to look at where established partners, such as suppliers or vendors, are going to. For example, the company that manages the building where your offices are housed might turn to the cloud to run building services and to manage building access. What's your organisation's role in that cloud approach? How do you control your data as part of that process? The broader issue at play is data segregation; making sure the various participants doing business with your organisation – and the organisations with which they, in turn, do business – have access to only the data to which they are entitled. For example, if you're using the same cloud provider that one of your competitors is using, you'll want to know what walls the provider has in place to prevent data leaking to your competitor and ensure that your information remains segregated.

Toward better security

Even as the industry of cloud service providers and related organisations work to develop protocols for advanced cloud security – through organisations such as the Cloud Security Alliance, which works to establish standards and practices for providers – customers of cloud technology must remain mindful of regulations, risks and their risk appetites, and they must augment their approach to cloud with custom rules and tools.

But the process starts with basic understanding. Here are three key starting points for improved security in the cloud:

Understand your current cloud usage.
Know what your organisation is already doing in the cloud. Some components within your organisation might be using cloud technology without your knowledge. Or you might be unsure of which operations have fully transitioned to the cloud. A cloud discovery phase is a good place to start.

Consider your information "crown jewels" and then map risks to understand how those crown jewels can be threatened and protected.
What information, specifically, is at risk in each cloud scenario for your organisation? What are the vulnerabilities and the potential threats? How important is the information at risk? Identifying the risks and knowing your risk appetite will help you approach your cloud usage in a more informed manner.

Review your current enterprise security and control environment – your tools and processes.
Understanding what you have in place now for your on-premise systems can help you determine what you can repurpose or augment for cloud-based operations.

Digging in

Organisations determined to make their cloud-based operations as secure as possible will encounter deeper questions and the need to take more specific action as they move forward.

They will need to:

- Clarify responsibilities inside and outside the organisation
- Establish meaningful mechanisms to share information and to ensure privacy and security
- Develop plans for identification management, rights access and user permissioning
- Manage access privileges rigorously to make sure administrators aren't abusing power when it comes to sensitive data
- Know the points at which use and access policies must be enforced – the trigger events, the trigger uses and the trigger users
- Put in place tools for policy enforcement for web services
- Anticipate additional challenges that might arise when outsourcing the most sensitive data. When forging agreements with providers, consider end-of-contract issues and the "fate" of data
- Clarify the ownership of data and any permissible secondary use of personal information, such as usage for statistical or analytical purposes
- Monitor and understand changes in the regulatory environment, at home and abroad
- From a privacy perspective, know your notification and consent requirements for managing customer information (whether on premises or in the cloud), and understand the cloud provider's notification process for privacy breaches
- Quantify and understand the benefits beyond basic reduction in IT costs and staff – such as broader business efficiency and the transfer of backup-and-recovery risk to the cloud provider
- Know specifically what the cloud provider provides and confirm that the appropriate audit, assurance, and review mechanisms are in place to ensure that the provider delivers as promised
- Plan for business continuity in the event of technical difficulties with the provider, ensuring that you have an understanding of the provider's security posture and how it will respond during/after an attack

Evolving mindset

Getting into the mindset of operating securely in the evolving realm of cloud technology requires not only action; it requires ongoing acts of imagination and vision. And it requires you to keep up with technology and with your needs – and to alter your plans as business needs and technologies change.

THINK about your internal architecture.
Get a detailed picture of what your IT architecture looks like now, and develop a picture of how you would like it to look for cloud deployment. Consider questions such as where you will need to tokenise or encrypt.

KNOW the technologies involved.
Embrace cloud tools that make the most sense for your business. In other words, prioritise your cloud plans based on the business case. To do that, you need to know what cloud technologies are available and what technologies are on the way. Keep yourself educated.

IMAGINE how events will unfold when "bad things" happen.
Think about your need to investigate to ensure security and understand potential data breaches – internally and with the cloud provider. Think about your worst-case scenarios with cloud and security. Imagine how you will react and what it will take to get back to normal. Review contract terms and do your due diligence with providers to uncover unexpected risks and to develop ways to mitigate them.

Cloud without cloudiness

As an “anytime, anywhere” solution, cloud is establishing itself as the preferred method for nearly all of the applications that organisations use to conduct business today. Cloud is and will continue to be interwoven with how you sell product, how you interact with your customers, and how you manage communications and relationships with employees and partners. The future of cloud is bright but for organisations that fail to ask the right questions and take the right steps when it comes to security, their cloud experience will be a stormy one.

Deloitte has extensive, hands-on experience with cloud security issues ranging from strategy to implementation, and we stand ready to help you.

Contacts

Navin Sing
Managing Director: Risk Advisory Africa
Mobile: +27 83 304 4225
Email: navising@deloitte.co.za

Derek Schraader
Risk Advisory Africa Leader: Cyber Risk Services
Mobile: +27 82 330 7711
Email: dschraader@deloitte.co.za

Werner Swanepoel
Risk Advisory Africa Leader: Data Analytics
Mobile: +27 82 442 5948
Email: wswanepoel@deloitte.co.za

Cathy Gibson
Director: Risk Advisory Southern Africa
Mobile: +27 79 499 9046
Email: cgibson@deloitte.co.za

Henry Peens
Associate Director: Risk Advisory Southern Africa
Mobile: +27 82 496 8694
Email: hpeens@deloitte.co.za

Tricha Simon
Risk Advisory Regional Leader: Central Africa
Mobile: +263 772 234 932
Email: tricsimon@deloitte.com

Julie Nyangaya
Risk Advisory Regional Leader: East Africa
Mobile: +254 720 111 888
Email: jnyangaya@deloitte.co.ke

Temitope Aladenusi
Director Risk Advisory: West Africa
Mobile: +234 190 41730
Email: taladenusi@deloitte.com

Deloitte.

Designed and produced by Creative Services at Deloitte, Johannesburg. (CIC/Vee)