Deloitte.

Dissolve your cloud concerns

How to de-risk your cloud transformation

Contents

01 Introduction

02 Handling the shift: Two main challenges

03 Governance and responsibility

04 Develop a cloud security strategy

05 Focus on identity and access management

Introduction

Organizations in every industry are continually striving to evolve into more agile, faster-moving businesses. They're searching for ways to reduce friction, unlock innovation, deliver better customer experiences, and stay competitive in an increasingly challenging world.

Cloud technology is often at the centre of such efforts, since it provides an agile environment that allows an organization to address its transformational needs. Cloud services are typically easy to access and convenient to use—but they can also create significant risks for organizations that don't have the necessary capability and capacity to adapt to the new model.

Organizations often fail to appreciate that setting up and managing technology infrastructure in the cloud is substantially different than managing on-premises infrastructure. This lack of understanding is at the root of major cloud-related risks and security incidents.

Handling the shift: Two main challenges

Legacy thinking, which can lead to vulnerabilities

Technology teams sometimes bring a legacy mindset to their cloud implementations. Rather than taking time to understand the features that are native to a given cloud service and to figure out how to incorporate them into new business practices, IT teams may try to replicate existing processes in the cloud or "lift and shift" existing assets to cloud assets, in an effort to move the system from one environment to another without a proper redesign. For example, rather than using the logging system built into the cloud service, they may attempt to virtualize the logging system they've been using with on-premises technology for years—even though using the cloud service's default offering would be simpler, faster, and potentially superior.

These replicated legacy processes, practices, or systems may not be properly configured for cloud, unlike the optimized cloud-native offerings. These misconfigurations can lead to new risks that leave a company and its data vulnerable.

Security incidents in 2019 showed how such vulnerabilities are ripe for exploitation. New projections show that almost all cloud cyber attacks are expected to be related to misconfiguration. Nearly all means over 99%.[1] While more organizations are undertaking cloud transformations, they're more inclined to simply extend their on-premise security capabilities, which have not been tailored for native cloud services, to the cloud.

Gaps in security configurations, which expose traditional vulnerabilities

Organizations have tended to focus on securing their assets against emerging threats and attacks. While they're now making better use of new technologies to secure their environment, cyberattacks continue to exploit old vulnerabilities. Using cloud-platform-specific threat modelling, penetration testing, and vulnerability assessments can help your organization evolve in its understanding of how its threat landscape has changed.

In many instances, resources are misconfigured because the implementation/infrastructure team either does not have the appropriate knowledge or it follows traditional processes that are not suitable for a cloud environment. For example, configuring network routes through the existing cloud-service provider route requires the correct configuration to manage traffic flow. One of the best ways to mitigate this is through the use of cloud security posture management systems and cloud-native compliance monitoring tools that use leading security practices.

Failure to recognize gaps in security configurations can lead to exploitation through existing vulnerabilities. It's therefore critical to gain visibility of the workloads in the environment and to implement appropriate controls by using benchmarks, through automated configuration management and remediation of identified misconfigurations. Staff will need to be equipped to manage and configure cloud-native tools according to these defined benchmarks.

1. Innovation Insight for Cloud Security Posture Management Gartner - Published 25 January 2019 - ID G00377795

Dissolve your cloud concerns | How to de-risk your cloud transformation

Reducing risk: where to start

- **Understand what you're already doing on the cloud.** Review how your organization is already using cloud services. Identify the related risks and the steps that have been taken to manage or mitigate them. Determine which, if any, guard rails currently exist for the use of cloud.
- **Benchmark your efforts.** To understand cloud-related gaps and risks, benchmark your efforts against well-established, best-practice frameworks for cloud architecture, such as those described by the US National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS). This assessment will show what the organization is doing well and what it needs to improve to mitigate cloud-related risk.
- **Make sure there's a strategy.** Ensure your organization has a clear, shared cloud strategy that describes what it's trying to achieve with cloud and how it intends to achieve those goals. Developing this strategy—which can evolve along with the cloud transformation—will ensure all parties are on the same page and help minimize rogue cloud experiments.
- **Upgrade your governance to include cloud.** To reflect the realities of doing business in the cloud, the organization's IT governance model needs to be upgraded. Set out clear accountabilities for cloud-based initiatives and establish the rules of engagement to govern cloud use and the management of data on the cloud. Put in place mechanisms to detect when cloud-based operations run into problems and resolve them quickly and effectively.
- **Invest in education.** Cloud is still a new frontier for most organizations, and the level of understanding about what it is and what it can do for the business can vary widely. Make sure leaders and their teams are provided with adequate, ongoing training and education to ensure they know what they need to know about cloud.

Governance and responsibility

One of the reasons companies find it challenging to understand and manage their cloud-related risk is that few have a thorough understanding of their cloud strategy and risks.

In our experience, CEOs, chief information officers, chief data officers, and other leaders often have differing views of what that strategy should be and what the results should be. In fact, most companies lack an all-encompassing cloud strategy. They have instead a series of tactical initiatives, launched for any number of reasons as they seek to innovate and reach a competitive breakthrough. This makes it hard for them to manage cloud effectively and mitigate the risks of an organizational transformation to cloud. Difficult, but by no means impossible. The first two steps are to prepare to govern the cloud program appropriately and to determine who is responsible for cloud security: the company or the cloud provider.

1. Make IT governance cloud-ready

Governing cloud services effectively is a key aspect of de-risking cloud-related programs. This is especially true given that it can be very easy, fast, and inexpensive to start using cloud services; in many cases, all it takes is one person with a credit card to complete a swift upload of company data, such as sales contacts. In just a few minutes, a company can find itself and its data unwittingly in the cloud. This demonstrates the importance of bringing visibility about cloud services to those responsible for IT and data security within an organization.

Ensure your teams are aware of the services your company is using so they can be better prepared to protect the company and its data in the cloud.

To avoid regulatory headaches, make sure your organization has ways to monitor and manage what data is put into the cloud, where it's stored, how it's secured, and when it's removed. Extending your information classification policy to the cloud and using tagging for your cloud resources is a good way to gain such visibility. For example, uploading European Union citizens' data into the cloud can result in a company suddenly being required to abide by the EU General Data Protection Regulation.

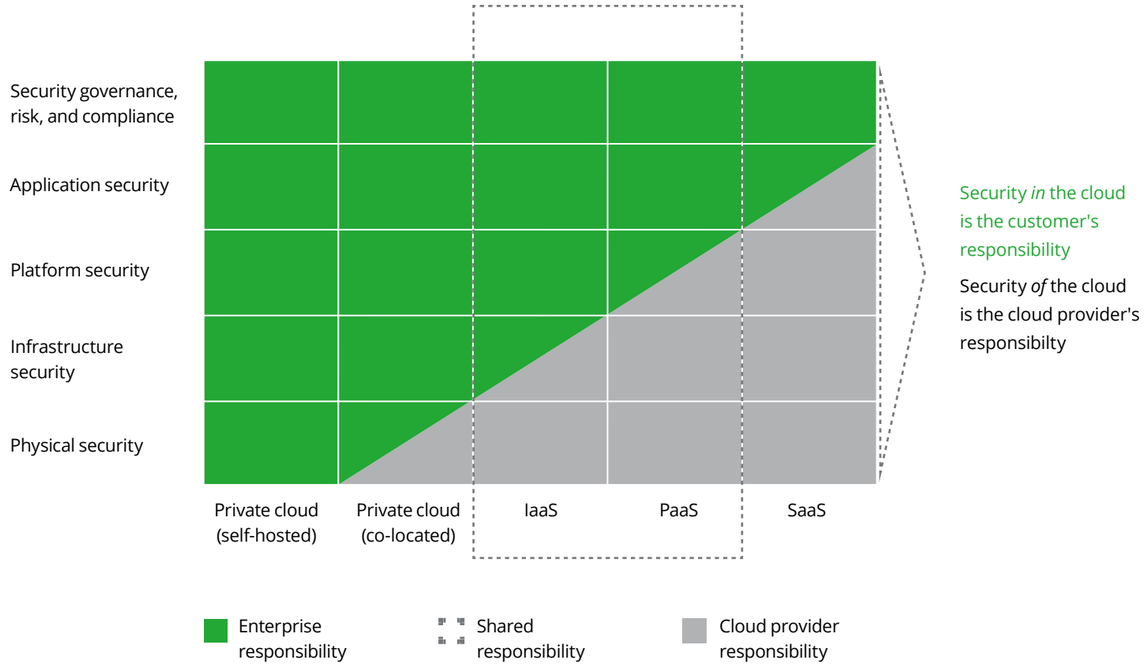
Finally, ensure your organization does not leave a host of data "artifacts" to linger in the cloud, lost and forgotten—until a hacker or cybercriminal discovers it. As we've seen time and again in recent years, data breaches can lead to significant financial, reputational, regulatory, and legal repercussions from which it can take a long time to recover.

2. Promote a shared-responsibility model

A fuzzy concept some organizations have is that cloud transformation reduces the effort needed to manage and secure resources, whether they migrate completely to cloud or share assets between on-premise and cloud environments. On the other end of the spectrum, some organizations think that protecting data in the cloud is always their responsibility, regardless of the service model utilized.

The reality is that cloud security is a shared responsibility between the customer and the cloud service provider, with the share of responsibility depending on the selected service model.

In general, infrastructure as a service (IaaS) models place more security responsibility on the customer, while platform as a service (PaaS) and software as a service (SaaS) puts more responsibility on the cloud service provider (CSP). Regardless of the model, it's critical to understand the details and to clear up any confusion with the CSP at the outset. Once defined, don't hesitate to promote your shared-responsibility model with your IT and security teams. The more people are aware of the responsibilities, the better prepared your organization will be.



Develop a cloud security strategy

To create a strategy for protecting your information in the cloud, start by **understanding the new risks** to your organization. It's important to prioritize those that are relevant to your public cloud environment based on the various regulations that may apply and the level of sensitivity of the company data you're considering moving to the cloud.

Identify your information crown jewels and then **map risks** to understand how those jewels can be threatened and protected. What specific information is at risk in each cloud scenario? What are the vulnerabilities and the potential threats? How important is the information at risk?

With the correct precautions, cloud environments can be as secure as on-premise ones. But, as with physical security, the more cloud security you enable, the more complex and costly it will be. Consider a **cloud threat risk assessment and cloud threat-modelling exercises** tailored to your proposed or existing cloud applications or environment. Identifying the risks and knowing your risk appetite will help you approach your cloud usage in a more informed manner. This will allow you to scale your security measures and budget by environment to make the most efficient use of your resources.

Next, **get your house in order.** What changes will need to be made to your operational and organizational models to ensure cloud doesn't run in a silo or as unmanaged shadow IT? This means prioritizing a new cloud responsible, accountable, consulted, and informed (RACI), ensuring you have **cloud cybersecurity standards and controls** that tie back to and align with your chosen cybersecurity framework (e.g., NIST, ISO, CSA) and fully integrating your cloud environments with your existing cybersecurity departments.

This won't happen overnight. **Staff is needed.** Cloud cybersecurity specialists are expensive and rare. Your existing cybersecurity team won't know how to address cloud security events or remediation strategies, and your cloud team is likely not going to understand the full depth of corporate cybersecurity. Start building nimble, integrated teams drawn from the best players of both worlds and cross-train from within.

These teams are going to need help, so automation and monitoring will be required. Now is the time to start thinking of **security as code (SaC).** Security development operations practices and automated monitoring will be differentiators for organizations that wish to capitalize on the velocity the cloud promised but that security concerns had slowed to a crawl. Investing in tools like cloud-native or cloud-enabled security information and event management **(SIEM)** and **cloud security posture management** will help you get a handle on security. Security configuration files like Azure Policy, AWS Organizations, and CloudFormation Templates can be adapted for your enterprise needs and deployed at scale using modern identity and access management (CI/CD) pipelines. Best of all, these tools can all be configured to match your chosen cybersecurity policy, giving those teams you've built a fighting chance to get the job done.

Dissolve your cloud concerns | How to de-risk your cloud transformation

Focus on identity and access management

One of the most important domains for cloud security is identity and access management (IAM). Disappearing or blurring network perimeters in the cloud introduce new difficulties in responding to risk, including how to best administer granular access controls to cloud services. All entities and cloud resources have an identity that must be secured.

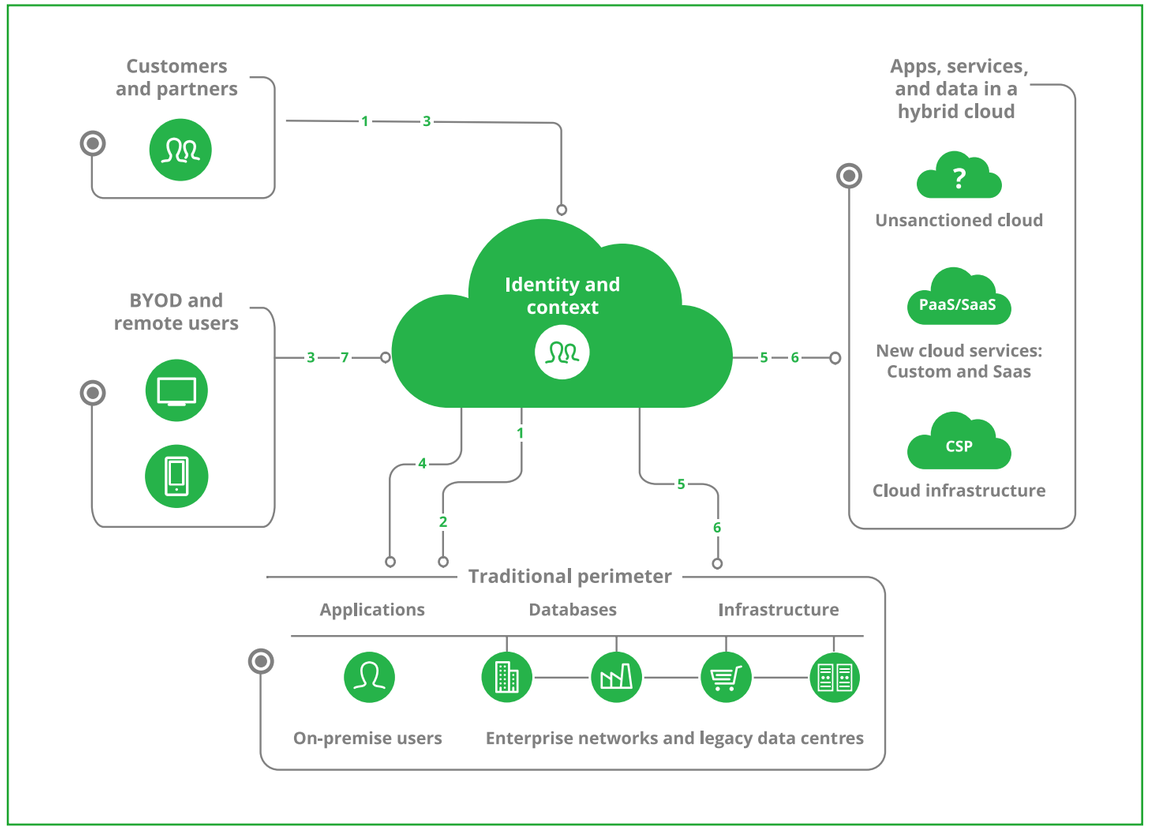
The following are critical cloud-identity capabilities and considerations:

- People are the new perimeter—spend as much time protecting the people in your cloud environments as you do setting up your cloud network security.
- Enterprise cloud needs federated identity and integration, with enterprise directories.
- Enterprise single sign-on (SSO) and multi-factor authentication with conditional access should be enabled for all users.
- Cloud user-provisioning, IAM roles, and role-based access control require careful planning and design, but add in-depth security.
- Privileged account management and privileged identity management can use solutions that are either native to cloud or enabled for it.
- Mobile device app and data management are important when the cloud extends to your mobile user base.

Some of the more notable IAM patterns include the following:

- Integrating cloud-based identity management solutions with enterprise security from the outset. While many companies are comfortable with creating security silos that use different approaches and technologies, such a strategy tends to be counterproductive over time. You'll eventually need to consolidate around a single security model.
- IAM solutions currently on the market seem to focus either on cloud computing or on the enterprise. Focus on the design and architecture of your identity-based security solution, and then select the technology. While the solution is more complex, the architecture should endure through many technological changes. Never let technology lead your requirements or design.
- Splurge on testing, including ethical security tests. These can lead to an understanding of where the vulnerabilities in your system exist and thus to a better choice of approaches and use of security technology. IAM systems that focus on cloud computing are becoming more critical with the expansion of what a cloud "identity" really is. Identity now is not just people, but can be secrets, containers and IOT devices among a myriad of other possibilities.[2] However, this could be because many on-premise enterprise systems are much less secure and therefore provide better pickings.
- In your design, make sure to consider things such as performance. While most IAM systems don't slow things down, they can, and they're hard to fix after deployment. They cause issues with security systems because users quickly figure out ways around the security.
- Make sure to consider your industry and all the regulations that require compliance. These are typically managed by the identity governance system within the IAM, and need to be understood from the outset. It's tough to retrofit these policies after implementation.

2. 2021 Planning Guide for Identity and Access Management, Gartner - Published 9 October 2020 - ID G00729005



Privileged account management and privileged identity management can use solutions that are either native to cloud or enabled for it.

Handle cloud risks—and realize its potential

Cloud will play a vital role in enabling companies to be quicker, more agile, and more competitive in the years to come, no matter their industry. But managing, reducing, and mitigating cloud-related risks are essential to ensuring their long-term health and vitality. It's time to act to position your organization to capitalize on all cloud has to offer while keeping the risks in check.

Key contact

Rob Masse
Partner, Risk Advisory
rmasse@deloitte.ca

Acknowledgements

Aaron Fleming
Director, Risk Advisory

Ian Guthrie
Senior Manager, Risk Advisory

Rene Heroux
Senior Advisor, Consulting

Naresh Kurada
Director, Risk Advisory

Gregory Lemaire
Senior Manager, Risk Advisory

Kevin Young
Partner, Consulting

Deloitte.

www.deloitte.ca

About Deloitte

Designed and produced by the Agency | Deloitte Canada. 20-3190014