Jump-start your cloud adoption with modern cloud security

Why your enterprise cloud transformation strategy may be stuck, and what to do about it

Why should the business executive care?

- Many enterprises are lagging behind in their cloud transformations and risk missing out on benefits including business growth and innovation.
- Elegant technologies such as the cloud almost always seem simpler than they are. But DIY cloud adoption is almost always a mistake: difficult, costly and time-consuming.
- Shortcuts often bring security risks, which stymies progress even more.
- A well-thought-out cloud security program can hasten the move so you finish your migration even faster than originally planned.

Why should the security pro care?

- Speed and scale — the promise of cloud — make it tempting to simply "lift and shift" data, applications and networks from on-prem to cloud.
- But security and privacy aren't "one size fits all." The cloud requires its own security considerations and architectures.
- You can help manage the migration and/or modernization process, demystify it and get buy-in from the right executives.
- To hasten the move, address these five common security challenges to enterprise cloud adoption.

On-premises-only work environments are so yesterday — rigid and boxed-in, limiting in scale and scope. Business happens largely in the cloud, a world that's amorphous, shifting and accessible anytime and from anywhere.

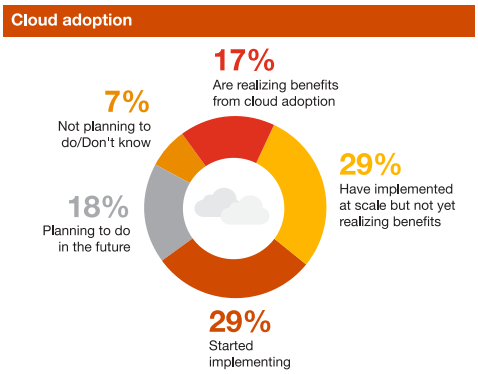
Freed from the old constraints, cloud-based enterprises can enjoy more flexibility, scalability and productivity than ever — at less cost. So why isn't everyone already there?

Just 17 percent of business and tech/security executives see their organizations benefiting from cloud adoption, according to PwC's **2021 Global Digital Trust Insights survey**.

They're the fortunate ones. A quarter told us they're using the cloud but haven't yet benefited, and 29 percent are just starting to move functions and operations to cloud environments. Another 29 percent haven't even begun the process.

We see it all the time: Clients convinced of the cloud's potential but overwhelmed by the complexities of properly securing it. Instead of moving forward with their cloud programs, they get stuck in a quagmire of questions and concerns.

The good news is that a well-thought-out, step-by-step approach to security can jump-start your stalled



Source: PwC, Global Digital Trust Insights, October 2020.

migration and/or modernization. It can even hasten the move so you finish faster than originally planned.

Get your cloud strategy back on track: Questions and solutions

What are the challenges to cloud adoption? Here are the questions we hear most often, along with security solutions to help restart your cloud engine and put you in the fast lane.

1. **What is the number-one reason why cloud transformations stall?** Lack of governance.

2. **What's key to getting privacy right on the cloud?** Understand what's required throughout your enterprise.

3. **Who's responsible for securing what?** The provider and you, but you'll have to be clear on areas of responsibility and control.

4. **Who's got a stake in accelerating and securing our cloud migration/modernization?** The entire C-suite — not just the CISO and the CIO.

5. **How do talent issues affect you beyond the risk implications?** Not being able to make the most of all the features and benefits of the cloud.

1. What is the number-one reason why cloud transformations stall?

Lack of governance.

Nearly half (48%) of organizations have a multi-cloud strategy. On average, organizations use three different cloud service providers (CSP), and **28 percent are using four or more**. While using more than one cloud service provider may be necessary and even beneficial, doing so can make security seem more challenging.

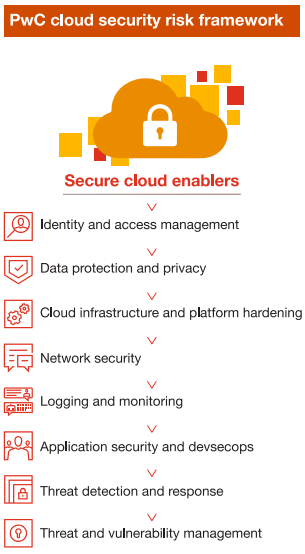
Cohesive governance is key: Each CSP may have different security abilities and requirements. And frequent releases of new features and updates means that, like the clouds in the sky, your enterprise cloud environment is continually changing.

Solution: Bring together all your enterprise security controls so you can secure them from one location, and with as much automation as possible. Here are steps:

- Create a cloud-platform-agnostic security controls framework, or use PwC's (pictured above). Tailor it to your business and incorporate industry-standard security baselines and regulatory requirements.
- Digitize the framework using collaborative tooling. By doing so, you create a living resource that's available to the right people and is auditable, editable and traceable — so it's as fluid as security and compliance requirements tend to be.
- Design an overarching security architecture that includes all the cloud platforms your enterprise is using. Build infrastructure-as-code (IaC) and DevSecOps tooling to set the right security checks on all your cloud platforms using automation.

  Using IaC offers immutability, meaning that each change to security settings and configurations occurs throughout your infrastructure, including your entire cloud environment. IaC also makes it easier for cloud administrators to test and deploy changes so that they take place cloud-wide, for faster, easier and more secure enterprise digitization.

  DevSecOps ties in security so that application code is free of vulnerabilities and



new code doesn't go into production until its security gaps are resolved. DevSecOps also provides real-time feedback on security bugs while developers are writing code. With the right processes and tooling, there's less need for lengthy reviews by information security teams — reviews that can slow and even stall changes that may be critical to innovation and new lines of revenue.

- Automate your compliance program. Verifying security controls manually can be difficult, costly and error-prone, and it can involve seemingly endless assessments and verifications. Using IaC and a holistic cloud-security framework lets you use code to run and monitor your compliance program. You won't get stuck in an endless cycle of compliance assessments, but instead get alerts in real-time when you slip out of compliance. And cloud-native tooling can revert any noncompliant changes to return your environment to its previous, compliant state.

A CISO-led, well-defined, automated cloud security program can benefit others in your organization, too. Your chief technology officer, for instance, may be able to measure, optimize and push changes to the enterprise cloud environment faster than ever before. In this way, the office of the CISO can not only remove governance roadblocks but also help accelerate your cloud transformation.

2. What's key to getting privacy right on the cloud?

Understand what's required throughout your enterprise.

Seventy-five percent of organizations find it more complex to manage privacy and data protection regulations in the cloud. Previously, organizations stored and maintained information in local data centers, and so only needed to concern themselves with local requirements. The cloud allows authorized users to access your enterprise information anytime and from anywhere — a more efficient way of working.

The caveat: You must correctly configure your global security restrictions on data accessibility and storage. Without thoughtful security configuration, the cloud has no borders, and that could put your enterprise at risk of violating privacy laws in other countries.

Solution: Your chief privacy officer as well as privacy officers in all your locations should make sure that their geographical requirements are included in your overarching cloud-platform-agnostic framework. You also must make sure that your architecture includes identity and access management considerations. Some regulatory requirements may restrict who can access your organizational data.

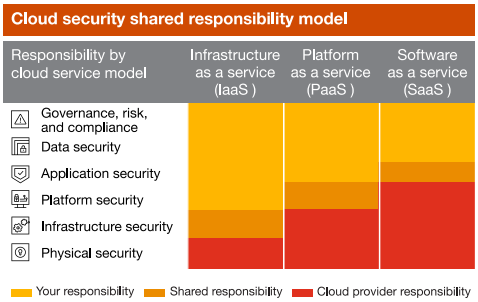
Being familiar with privacy requirements at the county, state and national levels can help your enterprise to reduce risk and design transparent solutions that people can trust.

3. Who's responsible for securing what?

The provider and you, but you'll have to be clear on areas of responsibility and control.

Of more than 3,000 IT and IT security practitioners **surveyed** in 2019, only one in three respondents said protecting data in the cloud is their responsibility. CSPs bear the most responsibility for sensitive data in the cloud, 35 percent said, and 33 percent said the responsibility is shared.

Solution: Responsibility for cloud security is almost always shared. CSPs are responsible for securing the platform itself — but the task of keeping your organization's data and intellectual property safe is up to you. Get familiar with each set of requirements and make sure your security teams and CIO are up to speed as well.



4. Who's got a stake in accelerating and securing our cloud migration/modernization?

The entire C-suite — not just the CISO and the CIO.

A lack of buy-in from C-suite executives is one of the most common reasons why cloud adoptions slow down or stall. You've probably approached your CISO, but what about the CFO, COO, chief risk officer, and chief legal officer? Cloud solutions exist for each of these roles and their organizations. Seeing cloud migration as only a security or IT problem misses the opportunity to engage key portions of the enterprise.

Solution: For each element in your cloud-agnostic security framework, define who's responsible and accountable and who's to be consulted and informed. Use a single framework and regularly report back to these individuals on your progress. Doing so can help you avoid duplicating tasks and help your cloud migration proceed smoothly and on schedule.

5. How can talent issues affect you beyond the risk implications?

Not being able to make the most of all the features and benefits of the cloud.

The cyber skills shortage is real, and it's expected to worsen — especially for cloud engineers. These professionals need the "full stack" of skills and knowledge. They need to know how all the technology components work and how they interact: databases, applications, operating systems, networks.

But people with this level of expertise are in short supply. Without cloud engineers on staff, businesses may take a lift-and-shift or rehosting approach to cloud adoption — simply moving applications to the cloud without redesigning them.

For example, they may use "compute services" to spin up virtual machines in which to place their code — just as they did when everything was in the data center. A lift-and-shift approach not only misses the point of cloud migration, it robs you of the opportunity to use all of the features and enjoy all of the benefits your CSP can provide.

Solution: Absent full-stack cloud engineers on staff, consider training one or more of your existing engineers in cloud technologies — but don't do this yourself. Elegant technologies such as the cloud almost always seem simpler than they are. Trial and

error can be an expensive way to learn, and will take much more time than working with someone who already knows the ins and outs of the cloud.

Partnering with an organization or individual with cloud migration/modernization and management experience is the best and most efficient way to move your project forward. A CISO-led strategic partnership could benefit other members of the C-suite, too. For instance, your CTO might save money on personnel if you can upskill the engineers you already have on staff and automate infrastructure and application changes to the cloud environments you use — a win-win.

Also, make sure you know what your CSP offers. Take advantage of every possible resource, such as platform as a service (PaaS), which allows you to scale up or down as needed.

Automating cloud security

The cloud is always on and always changing — so your cloud security program must be as well. Automation is key. Here are steps to take for powerful and effective automated cloud security.

- **Design secure cloud blueprints.**
  Draw common cloud-architecture blueprints that include security controls. Standardize your approved security architecture solutions.
- **Build hardened infrastructure-as-code templates (IaC).**
  Define secure resource configuration patterns using IaC tooling. Establish "golden templates" for infrastructure to establish security and architecture boundaries.
- **Test/scan your application and infrastructure security (DevSecOps).**
  Test against defined security baselines and detect misconfigurations before deploying to the cloud. Identify and address vulnerabilities and weaknesses in the codebase before release.
- **Post-deployment, use drift and runtime detection to manage your cloud security.**
  To enable compliance with cloud frameworks, use continuous configuration monitoring. Monitor for any changes that diminish your compliance with security standards as well as for nascent threats so you don't have to continually assess your cloud environment's security.
- **Use governance for continued cloud security hygiene.**
  Monitor adherence to life-cycle management standards to detect out-of-policy cloud resources. Collect cloud security hygiene metrics in a centralized dashboard to encourage self-monitoring.

Bottom line

Cloud security can seem overwhelming — but it is manageable. With the recommendations outlined here, you'll be well positioned to reap the rewards that motivated your migration to the cloud in the first place. You'll also position your organization for the coming evolution of cloud security, one that's poised to include prevalent machine learning, cloud security posture management and **confidential computing** — topics we shall turn to in future thought leadership.

Related content

Cloud Control: 4 Critical Steps to Better Cloud Security

Cybercriminals are drawn to the cloud to exploit increasing amounts of valuable data. The challenge for your business: how to protect it all.

☆

Contact us

Sean Joyce
Global and US Cybersecurity, Privacy & Forensics Leader, PwC US
Email

Joseph Nocera
Cyber & Privacy Innovation Institute Leader, PwC US
Email

Nitesh Dhanjani
Principal, PwC US
Email

Richard Kneeley
Managing Director, Cybersecurity and Privacy, PwC US
Email

Follow us

Get in touch

× Hide

Required fields are marked with an asterisk(*)

First Name*

Last Name*

Company Name*

Job Title*

Job Function*

- Please select

Email address*

Location*

- Please select

I agree PwC can email me about its insights, newsletters, events, services, products, and offerings.*

- Yes
- No

By submitting your email address, you acknowledge that you have read the Privacy Statement and that you consent to our processing data in accordance with the Privacy Statement (including international transfers). If you change your mind at any time about wishing to receive the information from us, you can send us an email message using the Contact Us page.

Submit