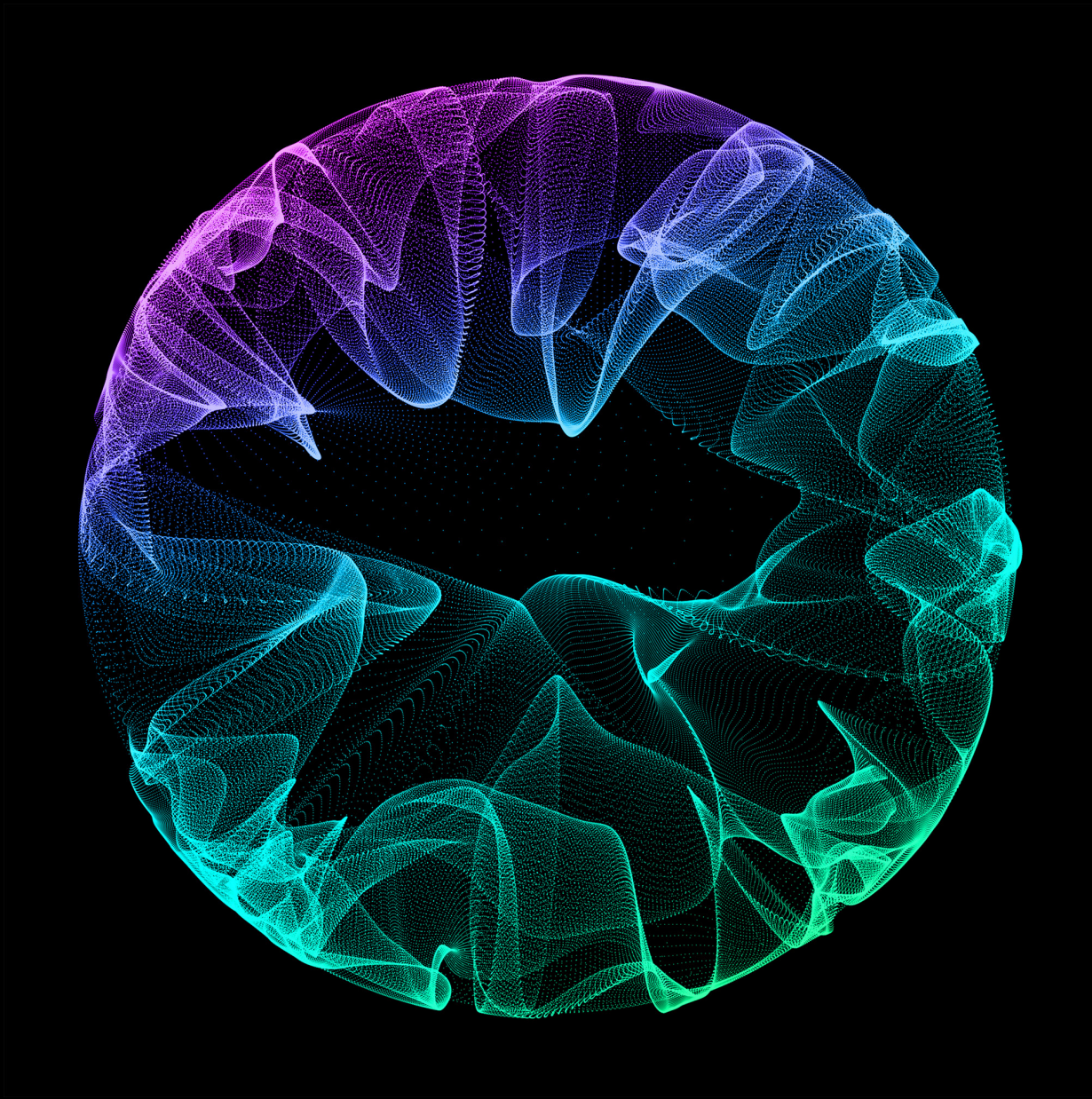
Deloitte.



Assurance in the cloud

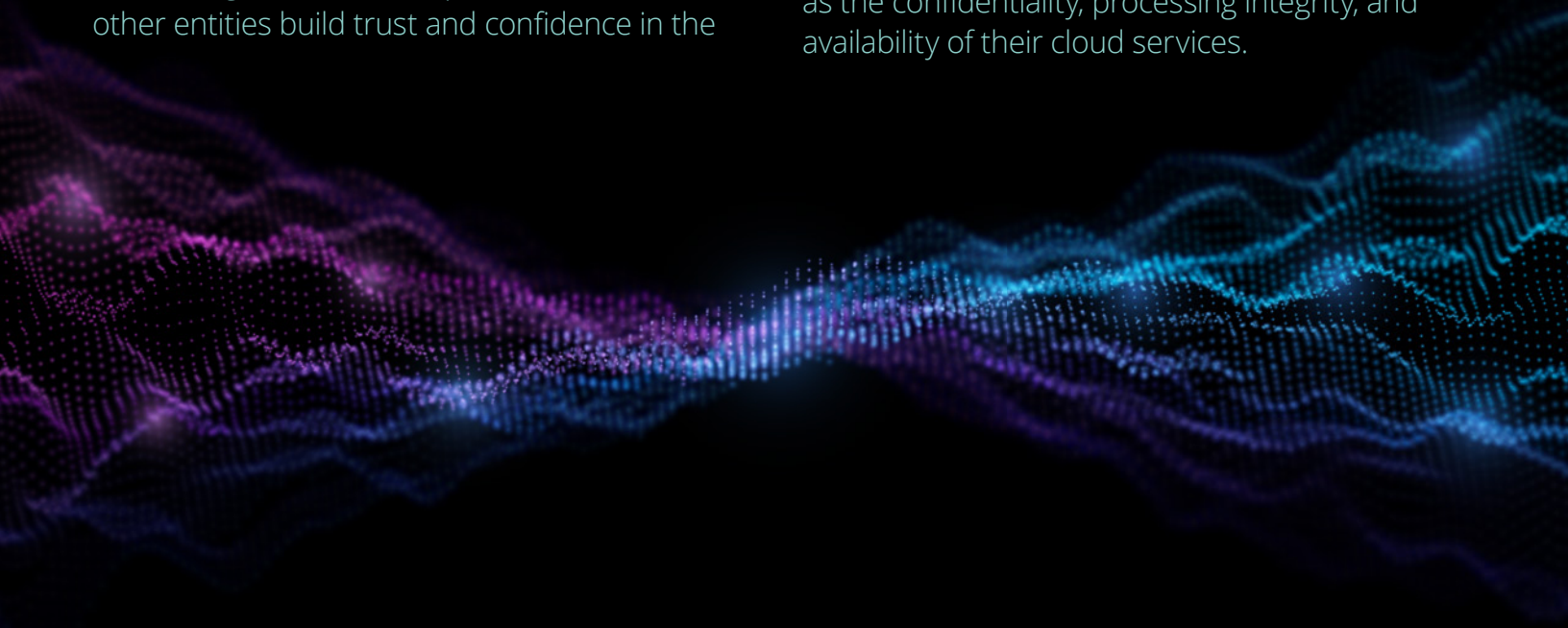
Don’t settle for a
check-the-box approach

Across industries, cloud computing continues to be a fast-growing segment of overall information technology (IT) spending.[1] For many businesses, it represents the new normal for enterprise IT.

As companies expand their presence in the cloud with hybrid or multicloud environments, new risks continue to emerge. Risk management leaders who fail to understand, assess, and address these cloud risks could expose their organization to increased reputational, financial, operational, and regulatory compliance consequences.

One way to gain assurance about cloud risks is through system and organization controls (SOC) reports that cloud service providers (i.e., service organizations) can make available to their customers (i.e., user organizations) and their auditors. SOC reports "are designed to help service organizations that provide services to other entities build trust and confidence in the service performed and controls related to the services."[2] For many larger organizations, they are a cornerstone of conducting business, and for many startup companies, they can provide a competitive advantage.

With the growing complexities of cloud environments, a traditional SOC report might not address all the risk domains a user organization might look for when subscribing to a service organization's offerings. This has resulted in the development of SOC 2+ reports, which expand in new directions and enable user organizations to gain more assurance based on industry frameworks. In the discussion that follows, we'll look at the high-level steps user organizations can take to move beyond a "check-the-box" approach to a more risk-informed way of assessing and managing security and privacy concerns, as well as the confidentiality, processing integrity, and availability of their cloud services.



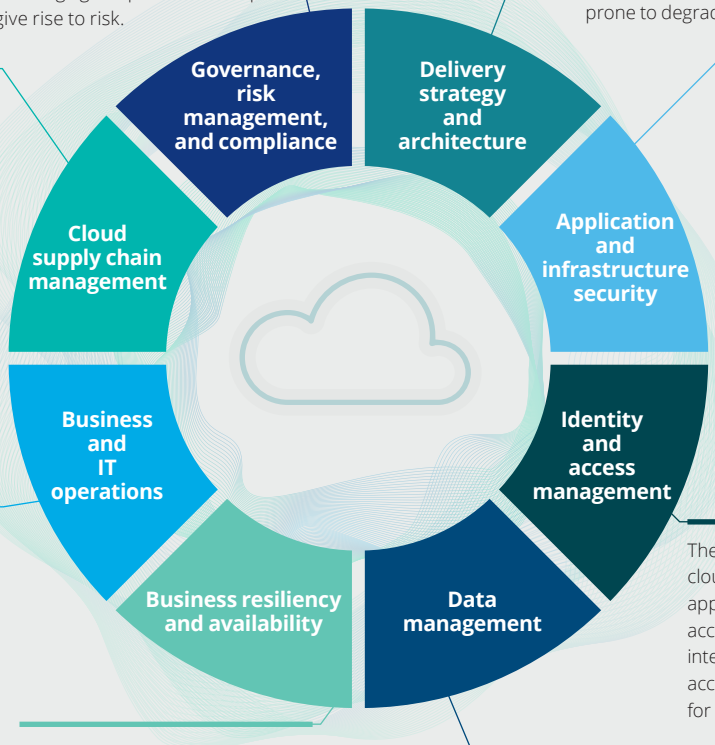
1 Grand View Research, "Cloud Computing Market Size, Share & Trends Report," April 2020, https://www.grandviewresearch.com/industry-analysis/cloud-computing-industry.

2 American Institute of Certified Public Accountants (AICPA), "SOC for Service Organizations: Information for Service Organizations," accessed February 2021, https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html.

Risk considerations

When it comes to cloud computing, risk has multiple dimensions (Figure 1) that can appear during the different phases of the cloud journey, from design to execute to operate.

Figure 1. Dimensions of cloud computing risk



Related risks include inadequate oversight, an inability to show compliance with regulatory requirements, and the lack of an independent assessment for the cloud solution. Governance responsibilities between cloud providers and their user organizations may also be unclear. On top of all this, a changing compliance landscape for regulations and standards can give rise to risk.

A coherent cloud strategy and road map for the user organization may be absent. If they exist, they may be out of sync with business needs or the user organization's technology maturity level. Beyond that, the cloud architecture may have limited customization and configuration features or be prone to degraded performance.

Lack of vendor monitoring (especially when multiple levels of service providers are involved in a cloud arrangement beyond the "third party" that an organization contracts with directly) and failure to plan for cloud portability and interoperability both fall in this risk category. So do contract issues, such as a lack of clarity around security requirements and subscriber responsibilities. Other risks include unclear legal liability, insurance coverage, and roles during incidents and investigations.

Cloud content and ecosystem partners may introduce security vulnerabilities. At the same time, organizations may have poor security practices that compromise the cloud environment, while "bad actors" can compromise cloud management interfaces. Internally, the user organization may lack security testing capabilities, defenses against attacks originating from within the cloud environment, or facilities to capture and store application logs. Uncertified environments (think FedRAMP[3] for government contracts) are another consideration.

Risks in this area include inadequate IT skills to manage cloud-based technologies, as well as poorly defined roles and responsibilities of cloud participants. The user organization may not be tracking its virtual assets or reporting data breach notifications in a timely manner. Records management, retention, and disposal policies may be inadequate, as well. Finally, the user organization may underestimate its operational or financial commitment to existing equipment or fail to understand overall technical requirements until the project is well underway.

The user organization may assign broad cloud management privileges without appropriate due diligence, fail to implement access controls for cloud management interfaces, or lack the ability to restrict access or implement segregation of duties for cloud provider staff.

Common challenges include an inability to verify cloud infrastructure resilience, interruption of cloud services due to subcontractor failure, and operational disruption. Risk can also increase as data replication or backups—whether to other clouds or back in-house—get more complicated.

Risks related to data management include unauthorized access to data storage, an inability to monitor data integrity inside cloud storage, and a lack of clear ownership of cloud-generated data. In addition, user organizations that have multiple data stores in the cloud may fail to remove or retain data as appropriate. There's also the risk of noncompliance with data privacy laws when data crosses jurisdictional lines.

Addressing these risk dimensions requires knowing which users are sharing data, where they're getting it, and who they're sending it to. That visibility extends to data flows between cloud services integrated at the back end through application programming interfaces (APIs). User organizations need to know they can protect their information by enabling cryptographic measures such as encryption, tokenization, masking, or redaction based on the sensitivity of information.

Cyber risk is a particularly challenging issue. Cloud service providers are a key target for cyberattacks because they're a concentrated data source. User organizations can find themselves worrying about their cloud provider's controls when they may be struggling to keep up with threats to their own systems—including from their own business users, who may be using the cloud services without the knowledge and threat management skills of the organization's information security group.

3 The Federal Risk and Authorization Management Process (FedRAMP) was created with the goal of providing a consistent means of applying security and measuring risk in commercial clouds for federal government usage.

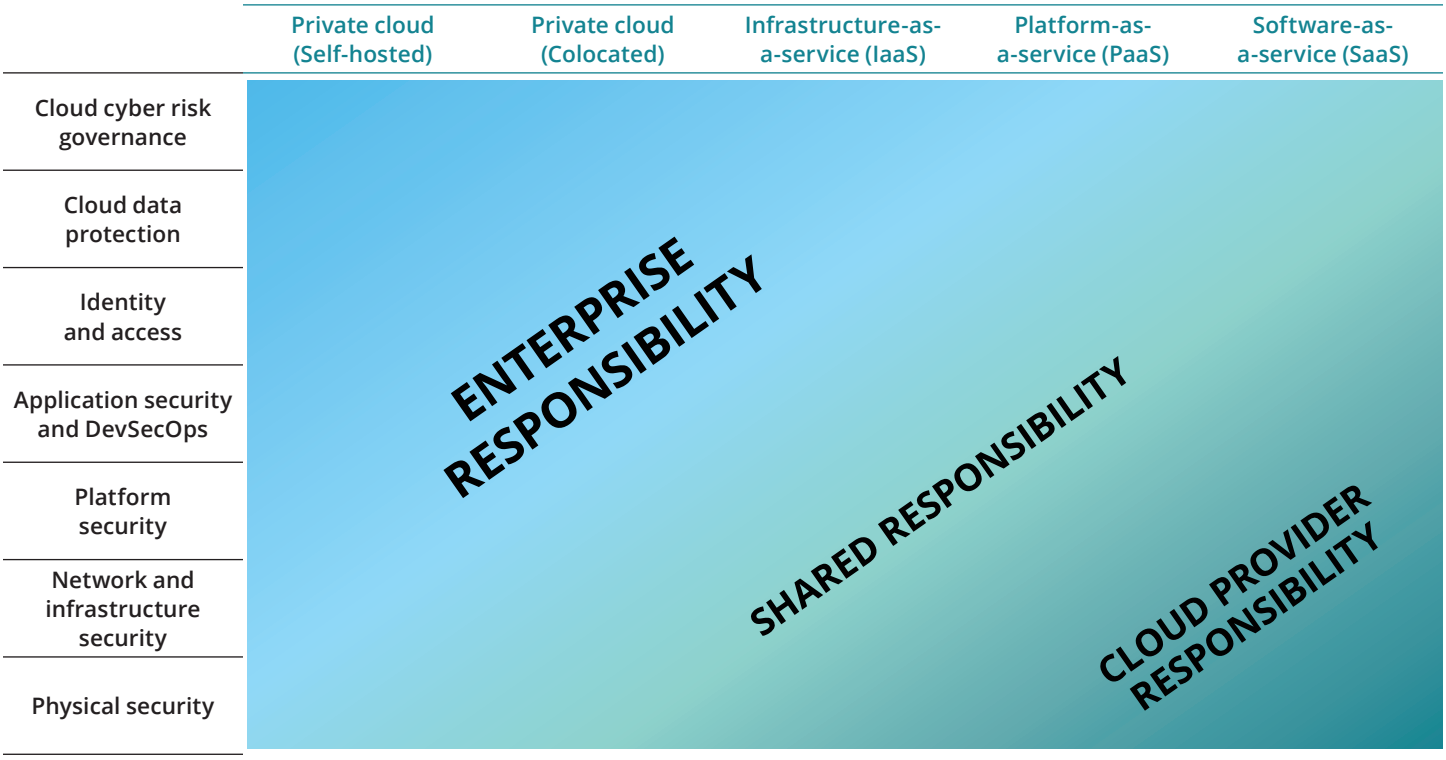
Shared responsibility

Managing risks in the cloud is a shared responsibility. However, the point where responsibility transitions from service organization to user organization can be a gray area, especially when multiple vendors and managed service providers are involved. Left undefined, a lack of clarity in this area can give a false sense of security to all parties concerned.

In general, service providers are responsible for their global infrastructure, including compute, storage, and network components. Meanwhile, user organizations are responsible for their data, the security considerations for protecting that data, and assuring that controls are in place and aligned to their requirements.

As user organizations grow more reliant on cloud services, service organizations tend to take on increasing responsibility for security domains and elements of the technology, depending upon the delivery model. For example, in a software-as-a-service (SaaS) environment, the service organization may handle not just physical, network, and infrastructure security (including platform security), but also components of application security and identity and access management, which are typically shared responsibilities between service and user organizations. Figure 2 measures the shared responsibility against the application technology stack and how the relationship between a service organization and an enterprise (i.e., a user organization) can vary depending on the cloud models that can be adopted and various security considerations.

Figure 2. Intersection of customer and provider responsibilities (security domains)



For organizations wanting to effectively manage their risks related to the use of a service organization, it is important to nail down this gray area so that there are no misunderstandings about which party is responsible for each aspect of security. This may not be a "one-and-done" exercise because the gray area can shift as the provider's services and user organization relationship evolve. One way to achieve clarity is to map the data flow between the user organization and service organization. Once the data flow is understood, the relative parties can determine who should be responsible for the controls at each point and communicate that information to user organizations.

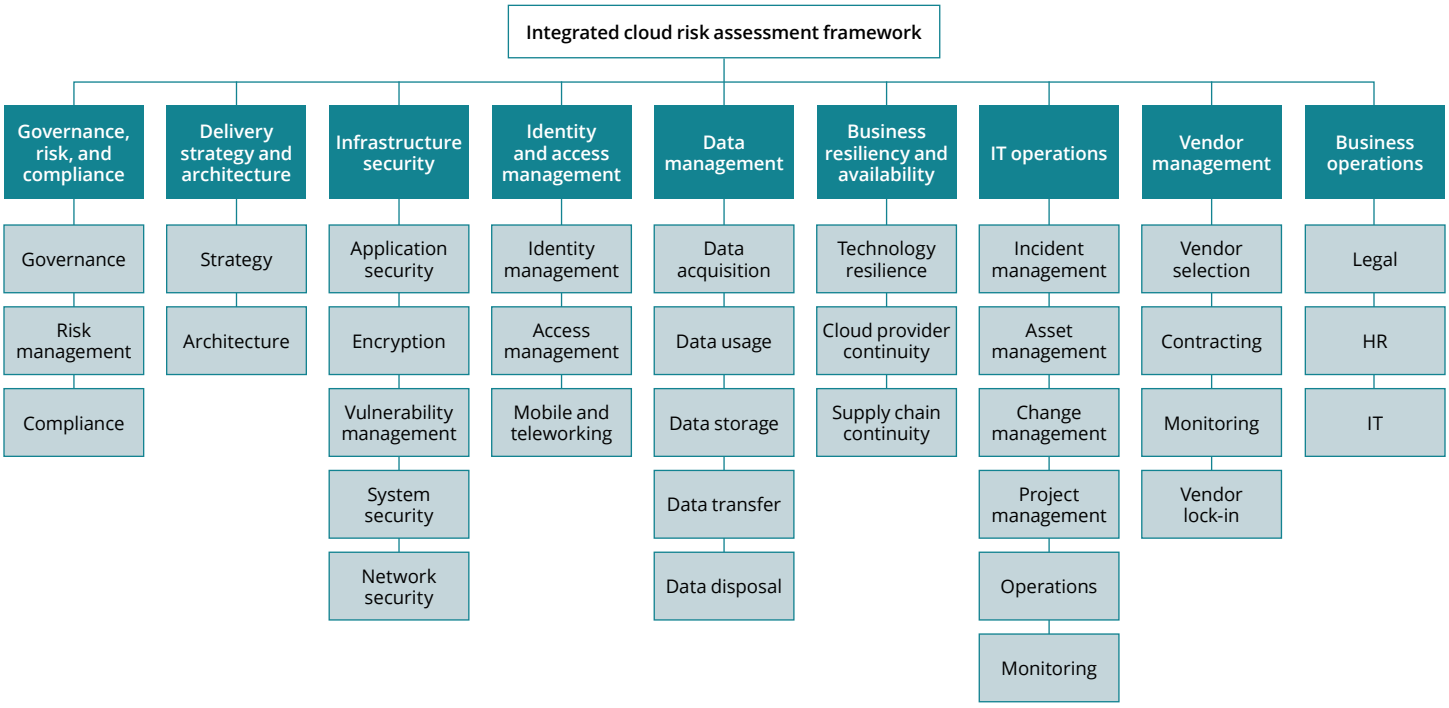
Frameworks for assurance in the cloud

Once user organizations understand the potential risks they face in the cloud and know who has what responsibility for those risks, they can focus on building a risk-based controls environment. They should map the risks they've identified in their specific environment to the controls report provided by each service provider to address any gaps that might exist. Service organizations typically offer some form of report, such as an SOC report, to their customers. Recent trends we are seeing indicate that some user organizations are going even further by asking service auditors to provide additional assurance around various frameworks in the form of SOC 2+ reports. These are highly flexible tools that can incorporate multiple frameworks and industry standards into third-party assurance reporting.

An important aspect of third-party assurance is understanding reporting requirements. Those requirements can be legal, regulatory, or contractual in nature. They can also be a matter of internal policy. All can drive the need for reasonable assurance that organizations are in compliance across multiple operational areas.

Whatever the requirement, there's a reasonable chance that a risk-based controls framework for it already exists. Well-known frameworks include the Cloud Security Alliance (CSA) Cloud Controls Matrix, International Standards Organization (ISO) 27002, Control Objectives for Information Technology (COBIT) 5, National Institute for Standards and Technology (NIST) 800-53, and many others. Organizations can tailor these to their own facts and circumstances, incorporate leading practices, and line them up against their own existing risk framework to create a customized, integrated risk framework (figure 3).

Figure 3. Example of a customized, integrated risk framework



By adopting a customized, integrated framework for cloud risk assessment, user organizations gain an instrument for assessing their controls environment against others. Service providers also gain a more concrete way to address the applicable criteria in an SOC 2+ report.

Cloud assurance in action

With all of that that in mind, let's look at an example of cloud assurance in action. Suppose an SaaS company created an application that medical offices use to book appointments. This software sits on top of a commercial cloud-based infrastructure provider and uses a third-party service to remind its user organization's employees of their appointments via text messages or email. The SaaS company might need an SOC 2+ report to provide controls assurance over its solution.

Now let's look at one of the SOC 2 "common criteria," CC 6.7, which addresses data protection features, and assume the following circumstances apply to this scenario:

- Each party (both SaaS company and user organization) bears some responsibility for data protection under this point of focus.
- The software application owner is responsible for encrypting the data.
- The cloud infrastructure provider is responsible for providing the infrastructure controls that enable encryption of data in transit and at rest.
- The messaging service is responsible for supporting the necessary transport layer security to encrypt network traffic.
- Finally, the medical office is responsible for protecting patient health information.

With this baseline understanding of how control responsibility is shared, the SaaS company can proceed to:

- Build that shared responsibility into a customized integrated framework;
- Validate who owns each set of controls;
- Get third-party validation of the effectiveness of the controls;
- Close any gaps in the control environment; and
- Educate customers about their responsibilities.

In the end, the aim of third-party cloud assurance is to address control responsibilities in alignment with technology security and regulatory requirements. But it's also a chance to go beyond compliance and create a robust, pervasive culture of risk awareness throughout the organization.

Collaboration can smooth the journey

Cloud assurance isn't just about frameworks and reports. It's an essential part of a collaborative relationship between the service provider, the user organization, and, importantly, stakeholders within the user organization. Service providers usually offer a considerable amount of information to help user organizations understand the service provider's side of the risk and control equation, the tools available to manage that risk, and the support needed to make the transition to the cloud. It's incumbent upon the user organizations, then, to get their risk-related processes, controls, and governance in order. This process should include all relevant stakeholders, usually including at least IT, security, cyber, risk and compliance management, legal, and operations.

With these stakeholders at the table, user organizations can sharpen their understanding of:

- Their specific risk environment;
- The shared responsibility model;
- The cloud provider's complementary user entity controls; and
- The cloud provider's compliance with privacy or other relevant laws in jurisdictions where the organization's data is stored.

For their part, service organizations can establish up front with each user organization:

- Where data will be stored (and whether location hinders availability or raises other concerns);
- How they move data between storage devices or locations;
- The data loss prevention steps they take;
- The responsibilities they share with their subservice organizations; and
- Who is responsible for a security breach, data leak, or other event that could prove a liability for the user organization.

The upshot? The more user organizations know about their cloud provider's security posture and gain consensus among internal stakeholders about what risks the user organization needs to address (in addition to those covered by the service provider), the less opportunity there's likely to be for misunderstandings and friction in the business relationship.

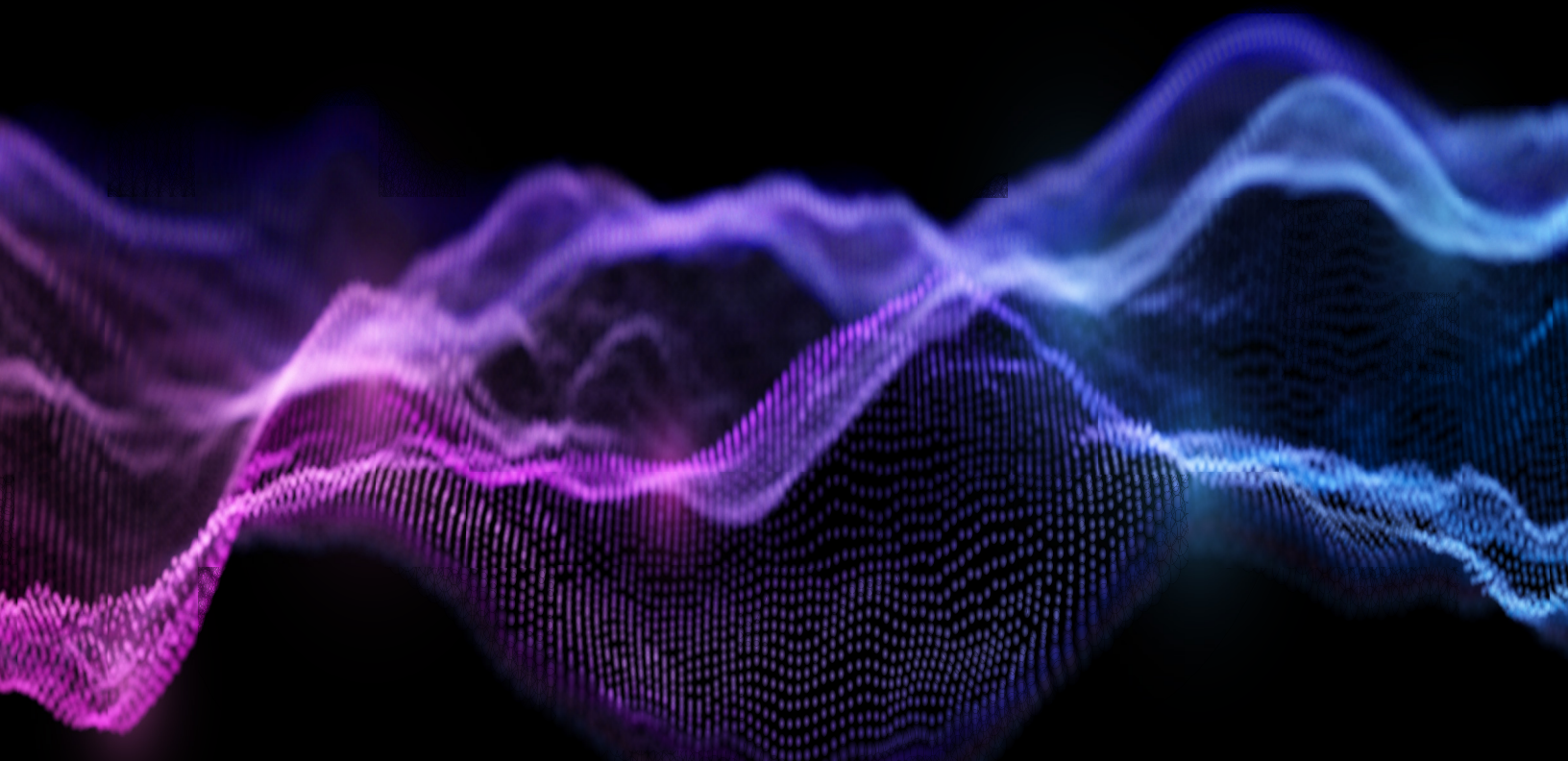
Optimize assurance in the cloud

In a boundaryless environment like the cloud, it can be all too easy to assume that certain risks are someone else's obligation. A clear understanding of what level of assurance is expected and who is responsible can help user organizations avoid the pitfalls that go with a false sense of security.

A risk-based approach begins with a clear understanding of the risks associated with cloud computing, as well as the responsibilities between cloud providers and user organizations—some shared, some not. From there, user organizations can make decisions about how to manage those risks in a way that complies with policies, leading practices, and applicable mandates. Many companies will start with an SOC 2 report to demonstrate their control environment and to achieve the related criteria. With the context that a customized, integrated framework provides, user organizations can use an SOC 2+ report to increase assurance that the cloud-based services they subscribe to are provided under the protection of a highly effective control environment.

If you want to learn more about our third-party assurance services, visit our website:

www.deloitte.com/us/thirdpartyassurance



Contacts

Charlie Willis
Managing Director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
chwillis@deloitte.co

Shar Qureshi
Senior Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
shqureshi@deloitte.com

Tom Polcar
Managing Director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
tpolcar@deloitte.com

Linghao Cui
Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
licui@deloitte.com

Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2022 Deloitte Development LLC. All rights reserved.