Shared responsibility and cloud migration

So far, you've learned about shared responsibility, and how security considerations are shared between cloud service providers (CSPs) and customers. You've also learned how this shared model differs from organizations operating in an on-premises environment. There are several considerations organizations should make before moving resources from an on-premises environment to a cloud environment.

In this reading, you'll explore the questions organizations should consider before deciding to migrate resources to the cloud.

Questions to consider

The following questions are relevant when an organization considers migrating resources to the cloud.

Which security controls are your responsibility?

First, it's important to determine which security controls are necessary for your organization. To start, put together a list of your assets, and determine the types of controls needed to secure them.

Which security controls are available as part of the cloud offering?

Once you know which controls your organization needs, your next step is to review the controls that the CSP offers to determine which ones align with your security requirements. CSPs should be able to provide you with detailed documentation of their security services along with the controls they own or share with their customers.

Which default security controls are inherited?

When migrating to the cloud, it's also important to consider inherited security controls. For example, the CSP might offer encryption and infrastructure-level controls by default. This arrangement means your organization would automatically receive these controls, which would help strengthen your security posture from the start.

What are your organization's compliance obligations?

An important factor for sharing responsibility with a CSP involves compliance obligations. If your organization must comply with any industry or government regulations, those requirements will play a significant role in moving your workloads to the cloud. Your organization will need to closely examine where the CSP will run your resources to verify compliance.

What are the security requirements for your customers and contractors?

Security requirements are not just relevant for organizational personnel; entering an agreement with CSPs involves considering all parties who engage with your cloud resources. For example, the users interacting with your services and the contractors your organization uses are all affected by a migration. You'll have to consider how access privileges will change for contractors, and how privacy disclosures may change for users.

Key takeaways

These are just a few questions that organizations should ask before migrating to the cloud. Security is a major theme and driving factor when preparing to move on-premises resources. Not only do organizations need to consider their security responsibilities and the ones they'll share with CSPs, but they also need to take their users and extended workforce into account. As a cloud security professional, your knowledge of shared security responsibilities and how they're applied is invaluable.