Understanding the Shared Responsibilities Model in Cloud Services

Também disponível em português
www.isaca.org/currentissue

The world of on-premises technology was practical when cloud services were not available. Originally, the management of end-to-end technology services, whether infrastructure or software, was the responsibility of the enterprise running them within their own brick and mortar establishments or leased from third-party vendors. Some services were outsourced or provided through managed contracts and included functions such as collecting backup tapes and storing them offsite. Otherwise, most services and risk areas were managed in-house.

Only recently has the as-a-service model become more prevalent. The advent of off-premises services has accelerated significantly, and this speedy increase has created a false assumption that accountability, responsibility and risk are not still a shared responsibilities model. This is the crux of the problem: Organizations are left in difficult situations without properly understanding their agreements and responsibilities when services are selected and handed off to cloud service providers (CSPs).

Significant Benefits of Cloud Processes

All organizations, whether small, medium or large, are rapidly transforming themselves by adapting to cloud processes. The term "cloud" is broad, but it can be defined as the portfolio of IT services that are delivered on-demand or as a service. The transformation to cloud processes that was originally anticipated over the next five years has been accelerated to just three years. Transitioning to cloud processes benefits an organization in several ways including easier scalability, increased resilience and continuity and cost savings. Numerous organizations have rapidly evolved their digital infrastructure using cloud-based solutions and adopting cloud-first strategies. This has resulted in the rise of smooth

JAI SISODIA | CISA, CCP, ITIL V3

Is the global manager of digital health, IT, cyber and privacy audit at a global medical device and healthcare organization. He is responsible for leading and executing global audit and advisory engagements across several areas including cloud platforms, manufacturing plants and industrial control systems, enterprise resource planning systems, privacy assessments, third-party risk, medical device cybersecurity and financial audit integration. Sisodia has previously worked as an assurance and advisory consultant for a leading Big Four consulting firm.

MOHAMMED KHAN | CISA, CRISC, CDPSE, CIPM, SIX SIGMA CERTIFIED GREEN BELT

Is the global head of digital health, IT, cyber and privacy audit at a global medical device and healthcare organization. He manages a global team responsible for enterprise risk management across the organization and conducting audits, assessments and advisory engagements. He has spearheaded multinational global audits and assessments in several areas including enterprise resource planning systems, global data centers, cloud platforms, third-party manufacturing and outsourcing reviews, process re-engineering and improvement, global privacy assessments and US Food and Drug Administration (FDA) guidance specific to medical device cybersecurity. He previously worked as an advisory consultant for leading consulting firms and multinational organizations. Khan frequently speaks at US and international conferences on topics related to data privacy, cybersecurity and risk advisory. He is an *ISACA® Journal* article reviewer and actively contributes to the *ISACA Journal* and blogs. He also serves on ISACA's Digital Healthcare Committee, recommending industry-leading thought leadership and guidance. He is a recipient of the ISACA® John W. Lainhart IV Global Award for recognition of his major contributions to the development and enhancement of the common body of knowledge used by ISACA and its members.

and secure connectivity from anywhere via hybrid multicloud architectures and increased agility to meet rapidly evolving business needs. Cloud operations have reached an unexpected level of maturity and usefulness as a result.

Scalability

Cloud solutions are advantageous in dealing with dynamic changes in demand and scale for digital services that can lead to huge shifts in data usage patterns. One example is a content delivery network (CDN), which is a group of geographically distributed servers that speed up the delivery of web content by bringing it closer to where users are located.[1] CDNs are critical components of any cloud infrastructure and provide a significant boost to reliability, response times and higher conversion rates. They were also highly beneficial during the COVID-19 pandemic when many enterprises suddenly had to run remotely.

Resilience and Continuity

Resilience is required to handle any potentially disastrous event, such as natural disasters (e.g., floods, hurricanes, earthquakes) and terrorist attacks, and the pandemic has provided ample evidence that it is critical to have resilience in an organization's processes to react to and recover from market disruptions quickly.

Cloud services offer controls across multiple layers of the network infrastructure to ensure security and continuity. These security solutions contain protocols that protect sensitive transactions and information. In addition, CSPs employ dedicated security teams whose full-time jobs are to ensure that bad actors are exposed. These security personnel have the experience of securing the assets of multiple clients, which makes the cloud even more trustworthy.

Cost Benefit

Benefits of cloud services include creating smaller carbon footprints, transferring resource management risk to service providers, reducing capital expenditures and streamlining computing processes:

> *The up-front cost of the cloud is also lower than in-house solutions. For companies that need top-tier products but don't have extensive funds immediately available, cloud solutions provide fantastic flexibility.*[2]

Cloud Deployment Models

CSPs offer various types of cloud environments based on their clients' requirements, which can be broadly categorized into ownership, access level and scale. These cloud deployment models are public cloud, private cloud, hybrid cloud and community cloud.

Public Cloud

The public cloud deployment model is a computing service that is offered by a third party to its customers via the Internet on a pay-per-use basis. This allows customers to take advantage of the scalability and flexibility that the cloud offers without bearing the costs associated with purchasing, managing and maintaining the underlying infrastructure.

The public cloud, due to its multitenant architecture, does have limitations. For example, it does not provide control of the underlying infrastructure such as hypervisors, network equipment or other services. This can be a high-risk factor for some organizations working in sensitive industries such as defense, banking or technology. Other major limitations of the public cloud include:

"The pandemic has provided ample evidence that it is critical to have resilience in an organization's processes to react to and recover from market disruptions quickly."

LOOKING FOR MORE?

- Read *Managing Security Impacts in a Multicloud Environment. www.isaca.org/multicloud-security-impacts*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

- Public CSPs offer a one-size-fits-all approach, which may not work for some organizations.
- Services provided in the public cloud model may not comply with certain government regulations. This is especially relevant for the financial industry.
- One security flaw in the cloud's infrastructure could make the whole environment and all of its customers vulnerable to an attack.

Private Cloud

The private cloud is a cloud computing environment that is dedicated to one business or organization. It provides all the benefits of a public cloud with additional control and a higher level of security and privacy. The services and infrastructure in a private cloud are always maintained on a private network. The cloud itself can be located in the organization's data center or hosted by a third-party service provider. However, there are other considerations when choosing the cloud deployment model:

- The private cloud offers dedicated computing resources, which cost more than the public cloud, where the cost is distributed between multiple tenants.
- The private cloud requires continuous support and maintenance of the cloud infrastructure.

This type of cloud is suitable for organizations that need higher control of their data or operations such as government agencies, financial institutions or healthcare organizations.

"The shared responsibility model is a framework that defines the security responsibilities between the CSP and its customers."

Hybrid Cloud

A hybrid cloud combines both the private and public cloud. This approach is selected by larger organizations with critical business needs, such as regulatory requirements, legacy applications that cannot be moved into the public cloud, security requirements or low latency. The hybrid cloud model allows the organization to benefit from the flexibility of the public cloud and the security of the private cloud.

Community Cloud

In the community cloud computing model, the cloud infrastructure is shared between different organizations from a specific community such as banks, trading firms or medical device manufacturers. This model lies somewhere between the public and private clouds and is well suited for organizations that are subject to similar regulatory requirements, working on joint projects or sharing trade resources.

Service Models

CSPs provide their services primarily based on three standard service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). These models offer a varied degree of abstraction and, as such, are portrayed as different layers in a stack: infrastructure, platform and application services.

Infrastructure as a Service

IaaS, also known as Hardware as a Service (HaaS), provides computing resources owned by the service provider to customers on demand over the Internet. The service provider manages and maintains the infrastructure, which offers several benefits including allowing an organization to avoid the costs associated with buying and managing physical infrastructure and the scaling of resources up and down based on demand.

Platform as a Service

PaaS providers offer both software and hardware computing resources, which allows developers to create, test and run applications without having to maintain a physical infrastructure or software. It provides a runtime environment that offers several benefits:

- Coding time is drastically reduced because the CSP offers application components such as security features and directories.
- The pay-per-use model makes it a cost-effective option for organizations that do not have the resources to purchase the software.
- Customers can focus on their core competencies without the need to maintain and manage the underlying resources.

Software as a Service

SaaS is a service delivery model through which the complete application is delivered to customers via the Internet. SaaS customers do not have to buy, manage or maintain complex hardware or software. The primary benefits of SaaS include:

- Significant cost benefits as SaaS applications are usually hosted in a multitenant environment where the costs associated with hardware and software licenses are distributed
- Ability to scale resources up and down, based on demand, without concern for hardware or software management or costs

Shared Responsibility Model

The shared responsibility model is a framework that defines the security responsibilities between the CSP and its customers (**figure 1**). It has evolved as a new and interesting concept for organizations that are planning to move to the cloud or have already moved. Responsibility of the customer depends on the types of services that they opt to use.[3] In general, a CSP is responsible for managing security, and the customer is responsible for securing their assets in the cloud.

Added complexity arises due to differences between the types of cloud services and between service providers of the same type. Control areas, such as regulatory compliance, are the responsibility of both parties.

In IaaS, the service provider's responsibility includes physical areas such as the facility, data centers and network components. CSP responsibility also extends to the host operating systems that run the applications and code.

The customer may be responsible for:

- Securely configuring cloud server workloads
- Identifying and remediating known vulnerabilities
- Implementing segmentation rules
- Applying runtime preventive, detective and corrective controls

In the PaaS model, service providers also manage the guest operating system so that customers can focus on application development, ensuring that application and data security controls are in place.

SaaS models put maximum responsibility on the service provider, such as managing physical, infrastructure and application-level control. However, the customer still owns the data and access-related processes.

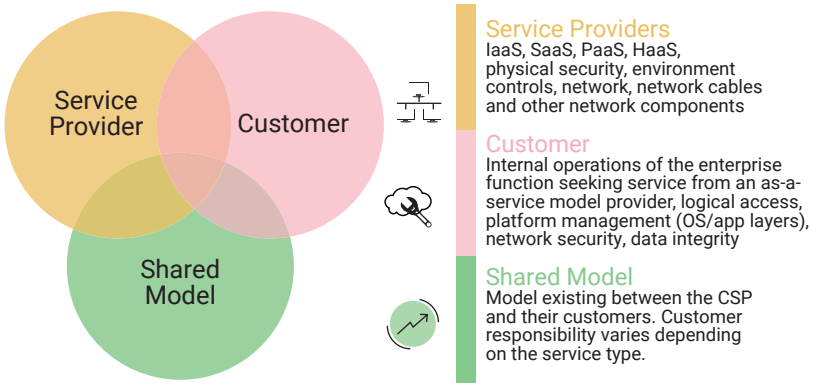
Figure 2 provides a summary of the controls that are owned by a typical CSP vs. its customers in each model.

Key Challenges in Cloud Adoption

Complementary user entity controls (CUECs), also known as user control considerations (UCCs),

FIGURE 1

Shared Responsibility Between Customer and Service Providers



are included within a vendor's system, which the customer must implement to ensure that the vendor's control objectives are accomplished.[4] Organizations that move their resources to the cloud often assume that all responsibility pertaining to management and security of these resources has been transferred to the CSP. However, this is not the case. In the *Demystifying the Cloud: Shared Responsibility Security Model* report, only 18 percent of respondents mentioned that they completely understand their responsibility regarding use of the cloud for all service types.[5] This is cause for concern.

Examples of CUECs in a service organization control report that customers should be aware of include:

- **Logical access**—Access rights to applications should be periodically monitored for appropriateness and to verify that duties are adequately segregated.
- **Change management**—The customer should identify how changes are set up and managed and review change orders for completeness against the established change management process.
- **Interface management**—Interfaces should be monitored to confirm that all data are accepted and processed and expected results are received.

"Organizations that move their resources to the cloud often assume that all responsibility pertaining to management and security of these resources has been transferred to the CSP."

FIGURE 2

Summary of Controls Owned by the CSP and Its Customers

Control Area	IaaS	PaaS	SaaS
Physical controls—Physical access to data centers is restricted to authorized personnel and mechanisms are in place to minimize the effect of a malfunction or physical disaster to data center facilities	CSP	CSP	CSP
Environmental controls—Controls tied to monitors for fire, air conditioning or other data center activity to support disaster risk reduction	CSP	CSP	CSP
Data integrity and confidentiality—Controls to provide reasonable assurance that data handling between the customer and the host service provider is secure	Customer	Customer	Customer
Identity and Access Management	**Customer**	**Shared**	**Shared**
Access policies—Logical access restriction to ascertain unauthorized access	Customer	Customer	Customer
Identity management—Secure control access to services and resources for users	Customer	CSP	CSP
Access and authentication—Multifactor authentication (MFA) controls across layers of access to the environment	Customer	CSP	CSP
Application Layer Processes	**Customer**	**Shared**	**CSP**
Application security—Controls such as hardening or patch management used to ascertain adequate security	Customer	CSP	CSP
Application specific logic and code—Controls around the entire application development life cycle	Customer	Customer	CSP
Network Management	**Shared**	**CSP**	**CSP**
Network security and configuration—Controls over protection against network security issues, including distributed denial of service (DDoS), man-in-the-middle-attacks (MitM), Internet Protocol (IP) spoofing, port scanning or packet sniffing	Customer	CSP	CSP
Network—Network cables and other network components	CSP	CSP	CSP
Network monitoring—Controls around network usage, port scanning, application usage or unauthorized intrusion attempts	CSP	CSP	CSP

- **Business continuity plan implementation**—The customer should review that the business continuity plan is in place and ensure that it adheres to the business recovery strategy.

Conclusion

Once the customer understands their security-related responsibilities according to the shared responsibility model of their CSP, they must then determine the controls that are applicable in their use case. Customer responsibility varies based on many factors, including cloud services and the model they choose, the integration of those services into their IT environment and the laws and regulations applicable to their organization and workload.[6]

Endnotes

1 Akamai, "Content Delivery Networks—What Is a CDN?" *https://www.akamai.com/our-thinking/cdn/what-is-a-cdn*

2 Turco, K.; "Four Ways Cloud Computing Can Save Your Company Money" Technology Advice, 24 June 2021, *https://technologyadvice.com/blog/information-technology/4-ways-cloud-computing-can-save-money/*

3 Simorjay, F.; E. Tierling; *Shared Responsibility for Cloud Computing*, Microsoft, USA, October 2019, *https://azure.microsoft.com/mediahandler/files/resourcefiles/shared-responsibility-for-cloud-computing/Shared%20Responsibility%20for%20Cloud%20Computing-2019-10-25.pdf*

4 Hill, L.-M.; "Importance of Complementary User Entity Controls for Vendor Relationships," Venminder, 12 October 2021, *https://www.venminder.com/blog/importance-complementary-user-entity-controls-vendor-relationships*

5 Oracle and KPMG, *Demystifying the Cloud Shared Responsibility Security Model,* 2020, *https://www.oracle.com/a/ocom/docs/cloud/oracle-ctr-2020-shared-responsibility.pdf*

6 Amazon, "Shared Responsibility Model," *https://aws.amazon.com/compliance/shared-responsibility-model/*