Computer Fraud & Security
ISSN (online): 1873-7056

Cloud security: sharing is caring

MARTIN WALSHAM
AMR Cyber Security

Abstract: When it comes to the security of data in the cloud, everyone has a part to play. Cloud service providers can only do so much, and it is the responsibility of the data owners to secure the parts that the service providers can't reach. This has led to the development of the shared responsibility model (SRM).

The shared responsibility model (SRM) is a cloud security strategy. It outlines that while cloud providers are responsible for safeguarding their security infrastructure, customers are also responsible for securing their applications and data within the bounds of their cloud environment. This article looks at the shared responsibility model, how it works and why it is needed.

Cloud SRM is a clearly defined way of outlining the security and compliance roles of both cloud service providers and their customers.

SRM is essential for effective cloud security management, providing clarity, accountability, risk management capabilities, compliance assurance and flexibility to organisations operating in cloud environments.

It also allows organisations to adapt their security strategies and controls to meet changing business needs and technological advancements. As organisations scale cloud deployments or adopt new cloud services, SRM provides the flexibility to adjust security measures, accordingly, ensuring ongoing protection of assets.

Background

The advent of cloud-hosted IT systems gives numerous advantages to organisations, enabling them to scale locally and internationally quickly, without the upfront costs of datacentres and hardware infrastructure. Such systems also deliver access to a wide variety of turnkey services and applications.

Historically, organisations were responsible for all aspects of security for their datacentres, covering the physical security of the datacentre and the room, management and security of physical servers and networking devices, along with the operating systems and applications that reside on them and user administration.

In a cloud environment, a shared responsibility model now exists where the cloud provider is responsible for certain aspects, the customer is responsible for other aspects and both parties share responsibility for yet other aspects. The development and adoption of SRM have paralleled the growth of cloud computing, today becoming a foundational concept in cloud security management practices.

SRM grew in importance as organisations increasingly migrated their workloads, data and applications to the cloud, recognising the need for a clearer understanding of who is responsible for securing the various components of a cloud environment. This understanding became crucial for organisations to effectively manage risk, comply with regulatory requirements and maintain trust in cloud services.

The exact demarcation of responsibility depends on the cloud services consumed by the organisation and the cloud hosting service provider. Depending on the type of cloud service (such as SaaS, PaaS or IaaS), the provider and the customer may have different levels of responsibility for different aspects of the cloud environment, such as hardware, infrastructure, data, applications and settings.

The general principle is that the customer should delegate as much security responsibility as possible to the trusted cloud provider, which has the expertise and resources to effectively manage security. However, customers always retain some responsibility for their data, endpoints, accounts and access management.

Risk assessment

When provisioning any service, it is important that organisations carry out a risk assessment to understand the impact of any

compromise of confidentially, integrity and availability of their data, and identify appropriate controls to mitigate those risks. They must also be clear on what risks they are willing to tolerate or transfer.

When looking to take on cloud services it is important to:

> Understand what the cloud provider is responsible for and complete due diligence regarding the strength and depth of those controls, to ensure the provider effectively implements the controls they are responsible for.
>
> Understand what controls the organisation is responsible for, and ensure they are effectively implemented.

Without both parts of the jigsaw being effectively addressed, there's a risk that control will drop through the cracks, potentially resulting in system compromise and data breaches.

Responsibilities under the shared model

Table 1 provides an overview of the key cloud service types and the responsibilities under the shared responsibility model.

Cloud service	Description of service	Cloud provider responsibilities
Infrastructure as a Service (IaaS)	Provides virtualised computing resources such as servers, storage and networking.	Provisioning and management of virtualised infrastructure components (eg, virtual machines, storage, networking). Physical security of datacentres and hardware infrastructure. Network security, including firewall configuration and traffic segregation. Host infrastructure patching and maintenance. Availability and uptime of infrastructure services.
Platform as a Service (PaaS)	Offers tools and services for application development, deployment and management in the cloud.	Provisioning and management of platform-level services (eg, databases, middleware, development tools). Configuration and maintenance of platform components and services. Ensuring scalability and performance of platform services. Database management and back-up solutions. Platform-level security controls and access management.
Software as a Service (SaaS)	Delivers software applications, accessible on-demand via a subscription model.	Deployment and management of software applications. Maintenance of application code and configurations. Ensuring high availability and reliability of the SaaS applications. Data back-up and recovery solutions. Application-level security controls and authentication mechanisms.

Table 1: Outline of responsibilities for various cloud services.

Compliance frameworks

Many larger cloud providers hold several industry-recognised certifications, such as ISO/IEC 27001 and PCI DSS QSA Attestation of Compliance. These certifications are useful as they provide a level of external verification that relevant controls have been effectively implemented, and also reduce the scope of any certification your organisation may be maintaining or undertaking.

When relying on the certification of a cloud provider, an organisation should pay careful attention to the scope of the service

provided, the scope of certification and the supporting documentation available – such as the statement of applicability – which will identify which controls the cloud provider has implemented.

The cloud service provider's certification will only provide assurance in the services it provides and within the scope of its certification. For the services you the organisation provide, you will need application provisioning and application user administration and must ensure these controls are effectively implemented. You may need to seek separate certification for the scope of these services, should you be required to do so by clients, regulators or for internal business reasons.

Penetration testing

Under a shared responsibility model, it is good practice for an organisation to carry out regular penetration testing of the services for which it is responsible, to ensure they are securely implemented and free from known vulnerabilities.

When arranging a penetration test of cloud-hosted services, the organisation should carefully review its scope of service responsibilities and check with its cloud service provider for authorisation processes relating to penetration testing.

Some cloud providers will require an organisation to gain specific authorisation for penetration testing or may require authorisation for specific types of testing such as malware testing, DDOS testing and simulated attack-based testing (eg, red team testing).

Most cloud service providers will specifically prohibit penetration testing of their back-end shared services. Typically, a cloud service provider will confirm that it carries out its own penetration testing of these but it will not generally share specific details of its testing reports and any vulnerabilities identified, for internal security reasons.

Risk assessment and due diligence

Risk assessment and due diligence are important steps before choosing a cloud service provider. They help you evaluate the security, compliance, performance and reliability of the cloud service, and compare different options based on your objectives and requirements.

To perform risk assessment and due diligence of cloud service providers, you should consider the following aspects.

Data protection and privacy: You should check how the cloud service provider handles your data, such as where it is stored, how it is encrypted, who can access it and how it is backed up. You should also verify that the cloud service provider complies with the relevant data protection and privacy laws and regulations, such as the General Data Protection Regulation (GDPR).

Service level agreements: Always review the service level agreements (SLAs) of the cloud service provider, which define the terms and conditions of the cloud service, such as availability, performance, reliability, support and compensation. You should also check if the SLAs align with the international standards for cloud service agreements, such as ISO/IEC 19086.

Security controls and certifications: You must also assess the security controls and measures that the cloud service provider implements to protect the cloud infrastructure, such as firewalls, anti-virus, intrusion detection and vulnerability scanning. Check if the cloud service provider has obtained any security certifications or accreditations, such as ISO/IEC 27001, SOC 2, or FedRAMP.

Business continuity and disaster recovery

Business continuity (BC) and disaster recovery (DR) are also vital points to consider when assessing the scope of an SRM. Just like security and compliance, business continuity and disaster recovery are shared responsibilities.

Evaluating the BC/DR plans of the cloud service provider means making a careful examination of how the cloud service provider ensures the continuity of its services and what plans it has in place to rapidly recover from any disruptions or disasters, such as power outages, network failures, cyber attacks or natural disasters. Of course, you should also test the effectiveness and efficiency of these plans.

Remember that while there are BC/DR aspects the cloud provider has to manage, the cloud customer is also ultimately responsible for how they use and manage the cloud service.

BC/DR solutions must take a risk-based approach. Many BC options may be cost-prohibitive in the cloud but may also not be necessary. For example, the odds of a major IaaS provider going out of business or changing its entire business model are low, but

this isn't all that uncommon for a smaller venture-backed SaaS provider.

Data governance

Cloud governance is the process of establishing and enforcing policies, standards and best practices for managing cloud resources and services. Cloud governance helps ensure your cloud environment is secure, compliant, efficient and aligned with your business objectives.

Cloud governance and the shared responsibility model are closely related, both helping you achieve security and compliance in the cloud. Cloud governance helps define and implement policies and standards appropriate for your cloud environment, based on your security and compliance requirements.

The SRM helps you understand and fulfill security and compliance obligations, based on the type of cloud service and cloud service provider used. Together, cloud governance and the shared responsibility model enable you to leverage the security advantages of the cloud, such as scalability, automation and intelligence.

In terms of data governance, the cloud customer plays a crucial role in defining and enforcing policies and controls to protect its data in the cloud environment. This includes establishing data governance frameworks, conducting risk assessments, implementing security controls, and regularly auditing and monitoring data activities to ensure compliance and mitigate risks.

By adhering to data governance best practices, organisations can effectively manage and secure their data in the cloud while leveraging the benefits of cloud computing.

Incident response

The cloud SRM has a direct impact on how cloud service providers and their customers collaborate in incident response and handling activities, such as incident notification and triage, evidence collection, investigation, eradication and recovery.

Both parties need to clearly understand their respective roles and responsibilities, and establish effective communication and coordination mechanisms. Each has distinct incident response responsibilities based on their respective roles and areas of control within the cloud environment. Effective incident response requires close collaboration between the parties to ensure incidents are addressed promptly with minimal impact, and cloud-based data and services safeguarded.

The service provider and customer should have a written agreement specifying the terms and conditions of the cloud service, including the service level agreements and incident response procedures.

Conclusion

By clearly defining the respective roles and responsibilities of each party, a shared responsibility model fosters a collaborative approach to security, enabling organisations to leverage the expertise and resources of their cloud service provider, while retaining control over their data and applications.

A shared responsibility model also allows organisations to focus their resources and efforts on securing their data and applications within the cloud environment, rather than solely on managing the underlying infrastructure.

This shift in focus enables organisations to adopt a more proactive approach to security, implementing robust security controls, encryption mechanisms, access management policies and monitoring tools to protect their assets effectively.

SRMs also facilitate compliance with regulatory requirements and industry standards by providing organisations with the necessary guidance and frameworks for security best practices. By aligning with established security frameworks and standards, organisations can demonstrate their commitment to security and build trust with customers, partners and regulatory bodies.

Ultimately, adopting a shared responsibility model empowers organisations to enhance their security posture, reduce risks and achieve greater confidence in their cloud-based operations, supporting their business objectives and enabling innovation and growth.

There are several security benefits to hosting IT systems within the cloud versus managing the system internally, as the cloud provider may have better scale, access to better security resources, tried-and-tested templates and automation.

But be mindful that cloud service providers do not have a magic wand. And cloud services are ultimately hosted in datacentres,

managed by (disconnected) staff, using commercial off-the-shelf technology components – so are subject to the same security vulnerabilities as any other IT systems.

Also, organisations must understand and effectively implement the security controls they are responsible for under the shared responsibility model in order for the end-to-end service to be secure.

Figure: Martin Walsham, AMR Cyber Security

About the author

Martin Walsham is director of cyber security at AMR CyberSecurity and is recognised throughout the industry as cyber security expert who has the business background and presence to successfully lead and deliver even the largest programmes.