Cloud Security

IT-321 | Cloud Computing

Abdullah Aldosariy

Dr. Beyzavi

Marymount University

12/10/2025

Abstract

This research study looks at modern cloud security, focusing on the 14 Cloud Security Principles that the UK National Cyber Security Centre (NCSC) issued. These principles spell out what you need to do to keep your data, identities, networks, and services safe in the cloud. IBM and Zscaler provide further information that is utilized to look at the shared responsibility model, types of deployment, types of service, and the overall pros and cons of cloud computing.

Introduction

Cloud computing has changed the way businesses work by giving them technology that is scalable, adaptable, and cheap. But as more people use the cloud, new security problems can up. IBM says that "cloud security is a set of procedures and technologies that protect businesses from threats both inside and outside." Zscaler also stresses that cloud security is a shared responsibility: the providers protect the infrastructure, and the consumers protect their access, identities, and data.

Cloud use has sped up in many fields, such as healthcare, government, the military, banking, and worldwide entertainment platforms. Remote workforces and distributed devices are increasingly the main parts of how businesses work, which makes the attack surface more than just the security borders of the firm. Zscaler says that the most common cause of cloud breaches is misconfigurations. This shows how important it is to know the basics of cloud security.

The NCSC 14 Cloud Security Principles give an organized way to check that cloud services fulfill high security standards. These principles help businesses understand what providers are responsible for, what technical safeguards they should have in place, what operational controls they should have, and what customers should do.

The 14 NCSC Cloud Security Principles

Principle 1: Data in Transit Protection

Your data needs to be safe from being changed or listened to when it moves between devices and the cloud. This needs strong network-level safeguards, encryption, and authentication. To protect privacy and data integrity, providers must use TLS, secure APIs, and encrypted tunnels.

Principle 2: Asset Protection and Resilience

A cloud provider must protect physical assets and infrastructure from damage, theft, loss, or seizure. This includes protecting the physical data center, building infrastructure that can withstand damage, making backups, and storing data in an encrypted format.

Principle 3: Separation Between Customers

One customer's data should not be accessible to another in cloud environments. To keep workloads safe, this is done by using virtualization borders, access controls, and network segmentation.

Principle 4: Governance Framework

Providers must follow a solid security governance architecture that makes sure policies, audits, compliance, and accountability are in place for the whole service lifecycle.

Principle 5: Operational Security

Providers must use incident response, vulnerability management, monitoring, and configuration control. Proper operational security makes sure that threats are found and dealt with quickly.

Principle 6: Personnel Security

Staff members of providers who have access to systems or consumer data must be trustworthy, checked out, and watched. Technical controls must limit acts that are privileged.

Principle 7: Secure Development

Cloud services must use secure development lifecycle methods like code review, automated testing, version control, and vulnerability scanning.

Principle 8: Supply Chain Security

Providers must make sure that third-party vendors follow the same security rules. Hardware, software, and any subcontractors must all follow rules for compliance and safety.

Principle 9: Secure User Management

Customers should have safe ways to manage their accounts, permissions, and access. This includes setting up RBAC, MFA, logging, and secure APIs.

Principle 10: Identity and Authentication

Strong authentication is required for every identity that uses cloud interfaces. This comprises people, service accounts, automated systems, and apps.

Principle 11: External Interface Protection

Authentication and throttling must be used to protect, monitor, and secure public-facing APIs, consoles, and command-line interfaces.

Principle 12: Secure Service Administration

To keep attackers from taking over, administrative consoles and controls must be kept separate from public networks and meet enterprise-grade security requirements.

Principle 13: Audit Information and Alerting

Customers need logs, alarms, and audit trails to find out whether someone is trying to get into their system or use it inappropriately. Providers should provide dashboards and alert systems that let you see what's going on in real time.

Principle 14: Secure Use of the Service

Providers must offer secure defaults and give clients documentation that helps them follow the rules and set up their security correctly.

Cloud Deployment and Service Models (Zscaler)

They divide cloud deployment models into four groups in Zscaler. They put the models into four groups: private, public, hybrid, and multicloud. Many customers share public clouds, and they can grow as needed. Private clouds are reserved for one business, which allows them the most control. Hybrid solutions combine the two for more options. Multicloud models bring together many providers to ensure reliability and compliance.

There are different types of cloud services, such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), and Functions-as-a-Service (FaaS). These differ in the level of control the customer possesses over the surroundings.

Pros and Cons of Cloud Security

Zscaler says that cloud security has many benefits, including the capacity to grow, centralized management, lower costs, redundancy, and automatic upgrades. But there are risks, such as misconfigurations, problems with compliance, latency, and worries about data sovereignty.

Conclusion

There is no one thing that makes cloud security safe; it is a tiered structure of rules, technology, and shared responsibilities. The 14 NCSC Cloud Security Principles give you a complete way to check out providers and make sure the cloud environment fulfills today's security needs. Organizations can establish strong strategies that safeguard data, applications, and identities while taking advantage of cloud innovation by using IBM's operational best practices and Zscaler's knowledge of deployment models and risks..

References

NCSC. 'The Cloud Security Principles.' https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

Zscaler. 'What is Cloud Security?' https://www.zscaler.com/resources/security-terms-glossary/what-is-cloud-security

IBM. 'Cloud Security Services.' https://www.ibm.com/services/cloud-security