14.1.8 Cloud Security Facts

Cloud security responsibilities involve both the client and the provider. Each party has different levels of control over resources. Both must take responsibility for their individual areas and commit to protect these assets. Cloud service providers and clients should work together to design, create, publish, and operate cloud-based systems.

This lesson covers the following topics:

- Guidelines
- Security control categories
- National Institute of Standards and Technology (NIST) guidelines
- Cloud security control layers
- Security tools

Guidelines

Cloud services should be tailor-made by the provider and fulfill all security requirements requested by the client. Security guidelines for a cloud service include:

- Provide rigorous security for data stored in the cloud.
- Engineer, operate, and integrate the security management process into the operational process.
- Use symmetric and asymmetric cryptographic algorithms to optimize data security.
- Implement and regularly monitor a Quality of Service (QoS) process in order to maintain the service level agreements between the cloud provider and the client.
- Include a disaster recovery plan for the stored data. This will help minimize information loss if an unexpected event occurs.

Additionally, the cloud service provider should:

- Provide a fast, reliable service.
- Respond to new requests quickly.
- Add load balancing to the cloud services to ensure maximum throughput.
- Invest in higher multi-tenancy architectures to maximize utilization of cloud resources and to better ensure data and application security.

Security Control Categories

To maintain an efficient security architecture throughout the entire cloud infrastructure, the cloud service provider must be familiar with and implement the necessary security controls. The table below describes types of security controls.

Type	Description
Deterrent	Deterrent controls make the system more difficult to attack and, therefore, decrease attacks.
Preventive	Preventive controls harden the system against attacks, as well as recognize and stop attacks.
Detective	Detective controls identify and take action as needed when incidents happen.
Corrective	Corrective controls lessen the aftermath of an incident by limiting the damage.

National Institute of Standards and Technology Guidelines

The NIST provides technical requirements and best practices for federal agencies implementing digital identity services. These NIST guidelines provide a strong framework for protecting data. These guidelines include:

- Evaluate risks involving the client’s data, software, and infrastructure.
- Choose the appropriate deployment model according to the client’s needs.
- Implement audit procedures for data protection and software isolation.
- Renew Service Level Agreements (SLAs) to cover security gaps between client’s security requirements and the provider security implementations.
- Implement incident detection and reporting mechanisms.
- Know and understand the security objectives of the organization.
- Establish responsibility for data privacy and security issues in the cloud.

Cloud Security Control Layers

Security control layers help establish barriers between cloud services and hackers to better protect data.

Layer	Description

Application layer	Security at the application layer involves putting in place policies that comply with industry standards such as OWASP. Examples of application layer controls are Software Development Life Cycle (SDLC), binary analysis, scanners, firewalls, and so on.
Information layer	To protect information from being deleted, modified, or stolen, implement an information security management program (ISMP) that identifies and details physical safeguards, as well as technical and administrative defenses. Some of the information controls include Data Loss Prevention (DLP), Capability Maturity Framework (CMF), cryptography, and database activity monitoring.
Management layer	The management layer involves all administrative tasks to promote continued, uninterrupted, and effective services. Good management controls include Governance, Risk, and Compliance (GRC); Identity and Access Management (IAM); variability-aware virtual memory management (VaVM); and patch management.
Network layer	The network layer implements policies and measures to prevent attackers from activities such as stealing, modifying, viewing, and redirecting data. Some of the network controls are Network Intrusion Detection Systems/Network Intrusion Protection Systems (NIDS/NIPS), deep packet inspection (DPI), firewalls, QoS, anti-Distributed Denial of Service (anti-DDoS), OAuth, and Domain Name System Security Extensions (DNSSEC).
Trusted computing	Trusted computing involves a computational environment that provides internal control, auditability, and maintenance so that the cloud is always available. Good security controls for trusted computing include hardware and software Roots of Trust (RoT) and Application Programing Interface (API).
Computation and storage	The cloud provider must have policies and procedures in place to protect data in storage. These policies and procedures could include backups, space availability, continuity of services, and so on. Some of the computation and storage controls include host-based firewalls, Host Intrusion Detection System/Host Intrusion Prevention System (HIDS/HIPS), encryption, and file/log management.
Physical layer	Physical layer security measures focus on data centers, physical resources, and cloud infrastructure. These security measures include physical plant security, fences, walls, barriers, security guards, gates, camera surveillance, and physical authentication mechanisms.

Security Tools

There are many tools specifically designed to test cloud security. The table below describes the most popular ones.

Tool	Description
LoadStorm	LoadStorm is a load-testing tool for web and mobile applications. It's not very expensive, and it is very easy to use. It checks performance while the application is experiencing traffic. It's able to find the breaking point of an application. It's very customizable.
BlazeMeter	BlazeMeter is meant for end-to-end performance and load testing. You can use it with mobile apps, websites, and APIs. BlazeMeter is JMeter compatible. It can simulate up to 1 million users, which makes realistic load tests easier. It also has performance monitoring as well as real-time reporting.
Nexpose	Nexpose is used as a vulnerability scanner. It detects weaknesses, misconfigurations, and missing patches. It may be used with firewalls, virtualized systems, and cloud infrastructure. It can be used to detect virus, malware, backdoors, and web services linked to malicious content.
Qualys Cloud Perform	Qualys Cloud Perform is an end-to-end security solution that gives continuous assessment. It's able to see all system assets, no matter where they reside.