Accedere

Cloud Security Assessment

This publication contains general information only and Accedere is not, by means of this publication, rendering any professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Accedere shall not be responsible for any loss sustained by any person who relies on this publication. As used in this document, “Accedere" means Accedere Inc. Please see https://accedere.io and email us at info@accedere.io for any specific services that you may be looking for.

Accedere Inc is a licensed CPA Firm listed with PCAOB. Restrictions on specific services may apply.

Table of Contents

1. Growing Cloud Adoption
2. Shared Cloud Security Responsibilities
3. Cloud Threats and Vulnerabilities
4. Attack Scenario and OSI Layers
5. VAPT Phases
6. Cloud Compliance Challenges
7. Our Comprehensive Assessment Methodology
8. OWASP Top 10 Cloud Challenges and Resolution
9. How Can we Help

Growing Cloud Adoption

The worldwide public cloud services market is forecast to grow 17% in 2020 to total $266.4 billion, up from $227.8 billion in 2019. According to some estimates there are about 20,000 SaaS providers globally. SaaS Software as a service (SaaS) will remain the largest market segment, which is forecast to grow to $116 billion next year due to the scalability of subscription-based software. The second-largest market segment is cloud system infrastructure services, or infrastructure as a service (IaaS), which will reach $50 billion in 2020. IaaS is forecast to grow 24% year over year, which is the highest growth rate across all market segments. This growth is attributed to the demands of modern applications and workloads, which require infrastructure that traditional data centers cannot meet. (according to Gartner, Inc.)

Shared Cloud Security Responsibilities

At a high level, security responsibility maps to the degree of control any given actor has over the The cloud architecture stack consists of:

- Software as a Service (SaaS)—The CSP is responsible for nearly all security, because the cloud user can only access and manage their use of the application and cannot alter how the application works. For example, a SaaS provider is responsible for perimeter security, logging/monitoring/auditing, and application security, while the consumer may only be able to manage authorization and entitlements.

- Platform as a Service (PaaS)—The CSP is responsible for the security of the platform, while the consumer is responsible for everything they implement on the platform, including how they configure any offered security features. The responsibilities are, thus, more evenly split. For example, when using a Database as a Service, the provider manages fundamental security, patching, and core configuration, while the cloud user is responsible for everything else, including which security features of the database to use to manage accounts or even authentication methods.

- Infrastructure as a Service (IaaS): Just like PaaS, the provider is responsible for foundational security, while the cloud user is responsible for everything they build on the infrastructure. Unlike PaaS, this places far more responsibility on the client. For example, the IaaS provider will likely monitor their perimeter for attacks, but the consumer is fully responsible for how they define and implement their virtual network security, based on the tools available on the service.

Business are failing to protect Cloud Data

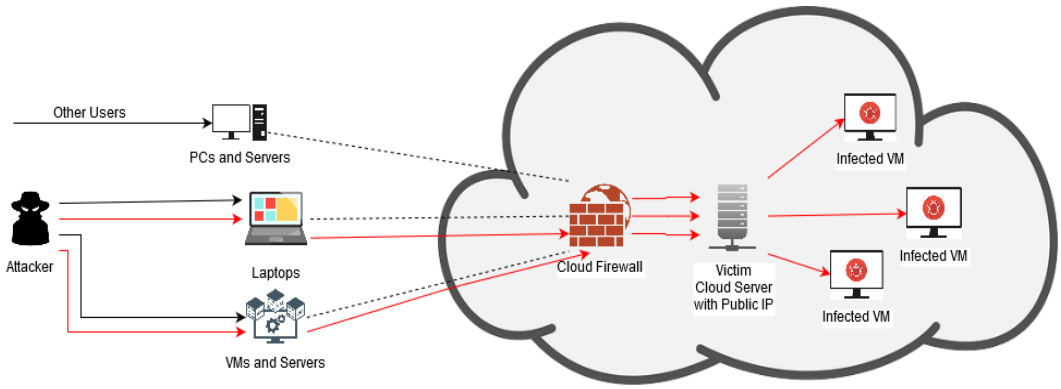
For most businesses, the cloud simply works better than so-called on-premises. And it isn't just about money. While any organization is interested in cutting costs, the main drivers of cloud migration are disaster recovery, ease of management, and archival. According to the 2019 Thales Cloud Security Study, organizations are failing to protect sensitive data in the cloud. Businesses are taking advantage of the cloud, but not applying adequate security.

Cloud Threats and Vulnerabilities

Threats	Vulnerabilities
Data Breaches	Targeted Attack Simple Human Errors Application Vulnerabilities Poor Security Policies Natural Disasters
Data Loss	Natural Disasters Simple Human Errors Hard Drive Failure Power Failures Malware Infection
Malicious Insider	Former Employee System Administrator Third Party Contractor Business Partner
Denial of Service	Weak Network Architecture Insecure Network Protocol Vulnerable Application
Vulnerable System and API	Weak API Credentials Key Management Operating Systems Bugs Hypervisor Bugs Unpatched Software

Attack Scenario and OSI Layers for Attack

During an attack, an outside party attempts to flood an organization's systems using a numerous amount of connections to overwhelm the system. Since the hackers can use programs or bots to generate numerous attacks, organizations cannot block just one IP address from shutting down a specific process.



OSI Layer	Protocol Data Unit (PDU)	Protocols	Examples of at each Level considering OWASP Risks	Potential Impact of an Attack
Application Layer	Data	Uses the protocols FTP, HTTP, POP3, & SMTP and uses Gateway as its device.	PDF GET Requests, HTTP GET, HTTP POST, website forms(login, uploading photo/video, submitting feedback).	Reach resource limits of services; Resource starvation.
Presentation Layer	Data	Uses the protocols Compression & Encryption.	Malformed SSL Requests -- Inspecting SSL encryption packets is resource-intensive. Attackers use SSL to tunnel HTTP attacks to target the server.	The affected systems could stop accepting SSL connections or automatically restart.
Session Layer	Data	Uses the protocols Logon/Logoff.	Telnet DDoS-attacker exploits a flaw in a Telnet server software running on the switch, rendering Telnet services unavailable.	Prevents administrators from performing switch management functions.
Transport Layer	Segment	Uses the protocols TCP & UDP.	SYN Flood, Smurf attack.	Reach bandwidth or connection limits of hosts or networking equipment.
Network Layer	Packet	Uses the protocols IP, ICMP, ARP, RARP, & RIP and uses Routers as its device.	ICMP Flooding - A Layer 3 infrastructure DDoS Attack method that uses ICMP messages to overload the targeted network's bandwidth.	It can affect available network bandwidth and impose extra load on the firewall.
Datalink Layer	Frame	Uses the Protocols 802.3 & 802.5 and its devices are NICs, switches bridges & WAPs.	MAC flooding - inundates the network switch with data packets.	Disrupts the usual sender to recipient flow of data - blasting across all ports.
Physical Layer	Bits	Uses the Protocols 100Base-T & 1000 Base-X and uses Hubs, patch panels, & RJ45 Jacks as devices.	Physical destruction, obstruction, manipulation, or malfunction of physical assets.	Physical assets will become unresponsive and may need to be repaired to increase availability.

Vulnerability Assessment and Penetration Testing Phases

Reconnaissance:

Also known as foot printing. It's a process of gathering data or preliminary inspection of an area of interest over a short period of time.

Scanning:

Collect more detailed information based on the previous phase. Also known as enumeration.

Gaining access:

This is the actual attack phase; so, the risk level is considered highest.

Maintaining access:

If the intentions of the hacker will not be satisfied by acquiring access, then maintaining that access is also important.

Covering tracks:

It is in the best interest of the hacker to erase his fingerprints from the scene. Rootkits to an extent does the job, but a hacker can modify log files to hide all those programs or applications that he has installed, from the view of the computer system.

Gathering logs:

Keeping a record of the scans or reports gathered from the attack/scan performed. Testing outcomes:
Detailed technical report
Executive summary
High-level fixation solutions

Vulnerability Assessment and Penetration Testing are two types of assessments:

Vulnerability scanners alert with flaws in code.

Penetration test attempt to exploit if any malicious activity is possible and identify which flaws pose a threat to the application, or if there is a threat by unauthorized access.

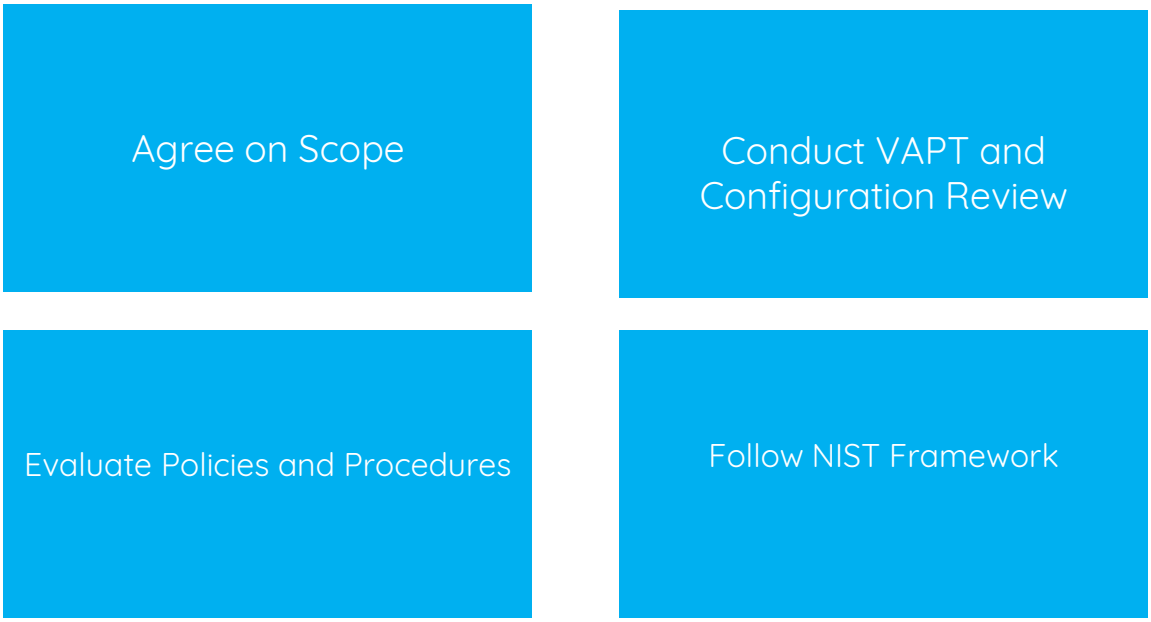
Cloud Compliance Challenges

Unlike information technology systems in a traditional data center, in cloud computing, responsibility for mitigating the risks that result from these software vulnerabilities is shared between the CSP and the cloud consumer. The risks include unauthorized access to customer data, security risk at vendor, Compliance and legal risks, risk related to lack of control, and availability risk.

Cloud application audit addresses these risks and safeguards the organization for Cloud functionalities.

Top Cloud Challenges by Cloud Security Alliance

Our Comprehensive Assessment Methodology



Scope for VAPT and Configuration Review

As part of a Cloud VAPT and Configuration Review, we conduct interviews with application stakeholders (business analysts, developers, testers, program and product managers, etc.) to understand your application's business context and security criteria. Following this, we assess the tool analysis of your cloud environment. The following are some of the security concerns we review during a Cloud Configuration Review:

#1. Authentication, authorization, and identity management

We assess your approach to access controls, including federation and realization as identity access management (IAM) policy. We evaluate the proper use of security groups to ensure that the principles of least privilege and separation of duties are followed. Other concerns include the protection of privileged accounts using appropriate technologies (e.g., multi-factor authentication) as well as key management methodologies implemented (i.e. Encryption standards).

#2. Cloud networking

We check your cloud networking configuration for proper isolation of sensitive cloud workloads from one another, correct use of network security groups and network ACLs, validation of authorization to make network changes, proper encryption of network traffic within and outside the cloud environment, and other controls required to guarantee secure networking in the cloud infrastructure.

#3. Cloud compute

We review the implementation of cloud virtual machines to ensure that they have been appropriately granted and secured to access company workloads.

#4. Cloud storage

We evaluate the implementation of controls used to protect cloud storage, including object storage, block storage, file storage, message queues, and other storage services used by the application. We determine whether data directed to application storage is properly protected in motion and at rest and not exposed to unauthorized parties, including anonymous users – a situation that is prevalent with many cloud service implementations.

#5. Other services

We assess other services you may have implemented to support your cloud workload, including database services (SQL or NoSQL based), server-less functions (e.g., AWS Lambda and Azure Functions), logging and monitoring services, and backup and disaster recovery infrastructure. In each case, we review the service's configuration, identify security misconfiguration scenarios, and determine whether these exist on your infrastructure.

At the end of a configuration review, we deliver a summary of your implemented security controls, our opinion on the effectiveness of these controls, and remediation guidance detailing how to improve poorly implemented controls. We can provide a sample of a configuration review deliverable on request.

OWASP Top 10 Cloud Challenges and Resolution

#1. Accountability and Data Ownership

Challenge

Using a third party to store and transmit data adds a new layer of risk. Cloud service providers often also operate across geographical jurisdictions. Data protection regulations such as the General Data Protection Regulation (GDPR) require that the data processors as well as the data controllers, meet the requirements of the regulation. It is important to ensure accountability of data protection, including recovery and backup, with any third-party cloud providers we use.

Resolution

Vendor risk management and accountability are the way to manage this issue. The Cloud vendor should have a set of security policies which you can map to your own, to ensure compatibility with your industry standards in data protection. This should include the Cloud vendor's use of technologies like robust authentication, encryption, and disaster recovery policies.

#2. User Identity Federation

Challenge

Digital identity is a key part of cybersecurity. It controls vital areas such as privileged access to sensitive resources. As enterprises increase their use of cloud and have data stored across cloud services, control of access through identity management is crucial.

Resolution

Implement a modern identity service or platform to provide robust, persistent, verified identity controls. Use this as a basis for controlling access to resources using a privileged access model.

#3. Regulatory Compliance

Challenge

OWASP points out the issues of meeting compliance across geographical jurisdictions. For example, if the organization is based in Europe but we use a U.S. Cloud provider, then it might be difficult to map the compliance requirements of EU-centric data protection, and vice versa.

Resolution

Use a cloud vendor who understands and applies solutions for the various data protection laws. They should also know how to handle cross-jurisdiction data protection requirements.

#4. Business Continuity and Resiliency

Challenge

Outsourcing IT infrastructure to a third-party cloud provider increases the risk of attaining business continuity for the simple reason that it is outside your control. An outage of cloud services can have serious repercussions for a business. When Amazon went down for 13 minutes, they lost an estimated $2,646,501.

Resolution

You need to make sure that your Service Level Agreements (SLAs) cover data resilience, protection, privacy, and that the vendor has a robust disaster recovery process in place. Evaluate their SOC reports.

#5. User Privacy and Secondary Usage of Data

Challenge

Once data enters the cloud realm, it is much more difficult to control across its life cycle. For example, social media sites can be difficult to manage, often defaulting to 'share all'. Data mining of data for secondary use in targeted advertisements is a privacy risks.

Resolution

Compliance frameworks like GDPR would expect an organization to perform a Data Protection Impact Assessment (DPIA) which extends to their Cloud vendors. Data encryption technologies, and multi-factor authentication can help augment data security and privacy risks.

#6. Service and Data Integration

Challenge

The safe transmission of data is a particular risk in cloud computing models where it is transmitted over the internet

Resolution

Transport Layer Security (TLS) should be fundamental protocols used by the cloud vendor. Additionally data must be encrypted in use and at rest.

#7. Multi-Tenancy and Physical Security

Challenge

Cost savings often dictate that cloud servers are used in a multi-tenancy setup. This means that we will share server resources and other services, with one or more additional companies. The security in multi-tenancy environments is focused on the logical rather than the physical segregation of resources. The aim is to prevent other tenants from impacting the confidentiality, integrity, and availability of data.

Resolution

If we are in a multi-tenancy agreement there are some ways you can mitigate the risk of sharing your cloud space with others. Starting with good design, your cloud vendor can configure the server for logical separation. The system can also have an architecture built for isolation so that a quarantined virtual infrastructure is created for each tenant. Technologies like encryption also help to prevent data exposure.

#8. Incident Analysis and Forensic Support

Challenge

If a data breach occurs, we must understand how to identify and manage critical vulnerabilities so as to respond to the incident as quickly and effectively as possible. Cloud computing can make the forensic analysis of security incidents more difficult. This is because audits and events may be logged to data centers across multiple jurisdictions.

.

Resolution

Check out our cloud vendor policy on handling, evaluating and correlating event logs across jurisdictions. Check if they have technologies in place, such as virtual machine imaging, to help in the forensic analysis of security incidents.

.

#9. Infrastructure Security

Challenge

This covers the entire gamut of how to harden the attack surface of a cloud infrastructure. It includes configuring tiers and security zones as well as ensuring the use of pre-established network and application protocols. It also includes regular risk assessments with updates to cover new issues.

Resolution

Implement Defence in Depth measures covering privileged access management, multifactor authentication, secure configuration of servers and services, and tiered architecture. Periodic VAPT and configuration reviews can surely help.

#10. Non-Production Environment Exposure

Challenge

Risks need to be accounted for across the entire life cycle of application development and implementation. This includes pre-production environments where design and test activities occur. Because these environments may have less stringent security applied, they may well open up security and privacy risks.

Resolution

In test environments, avoid using real or sensitive data. Have role based access control measures in place. Leverage the concepts of 'security and 'privacy by design' by implementing appropriate technical and organizational data protection principles through the entire project lifecycle.

Review Policies and Procedures

Information security policies**:** An overall direction and support help establish appropriate security policies. The security policy is unique to your company, devised in the context of your changing business and security needs.

Asset management: This component covers organizational assets within and beyond the corporate IT network., which may involve the exchange of sensitive business information.

Human resource policy: Policies and controls pertaining to your personnel, activities, and human errors, including measures to reduce risk from insider threats and workforce training to reduce unintentional security lapses.

Physical and environmental security: These guidelines cover security measures to protect physical IT hardware from damage, loss, or unauthorized access. While many organizations are taking advantage of digital transformation and maintaining sensitive information in secure cloud networks off-premise, the security of physical devices used to access that information must be considered.

Communications and operations management: Systems must be operated with respect and maintenance to security policies and controls. Daily IT operations, such as service provisioning and problem management, should follow IT security policies and ISMS controls.

Access control: This policy domain deals with limiting access to authorized personnel and monitoring network traffic for anomalous behavior. Access permissions relate to both digital and physical mediums of technology. The roles and responsibilities of individuals should be well defined, with access to business information available only when necessary.

Information system acquisition, development, and maintenance: Security best practices should be maintained across the entire lifecycle of the IT system, including the phases of acquisition, development, and maintenance.

Information security and incident management: Identify and resolve IT issues in ways that minimize the impact on end-users. In complex network infrastructure environments, advanced technology solutions may be required to identify insightful incident metrics and proactively to mitigate potential issues.

Business continuity management: Avoid interruptions to business processes whenever possible. Ideally, any disaster situation is followed immediately by recovery and procedures to minimize damage.

Risk management: Identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.

Change management: Guidelines to prepare, equip and support individuals to successfully adopt change in order to drive organizational success and outcomes.

Using Tools-NIST Framework

The NIST cloud computing definition is widely accepted and valuable in providing a clear understanding of cloud computing technologies and cloud services. A security framework like NIST, with its recommended set of security processes and controls, along with a risk assessment and management approach to match the appropriate set of controls to the business and threat environment, is an efficient way to meet these needs. Using an established framework can take the guesswork out of the process for smaller organizations while allowing larger and more mature security operations to justify their decisions and resource requests to management and auditors.

	NIST CSF Functions		
		Area of focus	Best Practice
Proactive	Identify	Configuration management	AppSec testing
		System management	Governance, risk, and compliance
		Vulnerability assessment	Penetration testing
		Awareness training	
	Protect	Access management	Encryption
		Data masking	Intrusion prevention systems
		DDOS filtering	Secure image/container
		Endpoint protection	Strong authentication
		Firewall	Firewall policy management
		Ops skills training	
Reactive	Detect	Intrusion detection system	Data analytics
		Network monitoring	Data loss prevention
		SIEM	
	Respond	Incident response services	Endpoint detect/respond
		Trouble ticket systems	Forensic analysis
	Recover	System/endpoint backup	High-avail/mirroring services

Areas covered by our Comprehensive Cloud Assessments

The following are some of the security concerns addressed during our Cloud Assessment:

- Cloud Vulnerability Assessment and Penetration Testing (Cloud VAPT)
- Authentication, authorization, and identity management
- Cloud network architecture review
- Cloud compute architecture review
- Cloud storage architecture review
- Configurations architecture review
- IaaS, PaaS, SaaS Assessment
- Data Backup and encryption configuration
- Configurations review

Our methodology used to develop and execute these reviews is an amalgam of techniques that features in best practices from cloud service providers and security standards from reputable sources (including hardening guides such as the NIST Benchmarks). We periodically align our methodology to the compliance and regulatory standards that many organizations have to adhere to when implementing computing services.

Sample Reports

OpenVas Vulnerability Report — HackerTarget.com

Summary

Scan started: Wed Feb 13 04:26:48 2019 UTC
Scan ended: Wed Feb 13 04:41:16 2019 UTC

3	4	0
HIGH	MEDIUM	LOW

Any HIGH and MEDIUM severity vulnerabilities should be investigated and confirmed so that remediation can take place. LOW risk items should not be ignored as they can be chained with other vulnerabilities to enable further attacks.

Illustrative

Host Summary

Host	Start	End	High	Medium	Low	Log
192.168.1.211	Feb 13, 04:27	Feb 13, 04:41	3	4	0	0
Total: 1			3	4	0	0

Vulnerability Summary

Severity	Description	CVSS	Count
High	Webmin <= 1.900 RCE Vulnerability	9.0	1
High	HTTP Brute Force Logins With Default Credentials Reporting	9.0	2
Medium	Webmin 1.880 Information Disclosure Vulnerability	5.0	1
Medium	Cleartext Transmission of Sensitive Information via HTTP	4.8	1
Medium	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili...	4.0	2

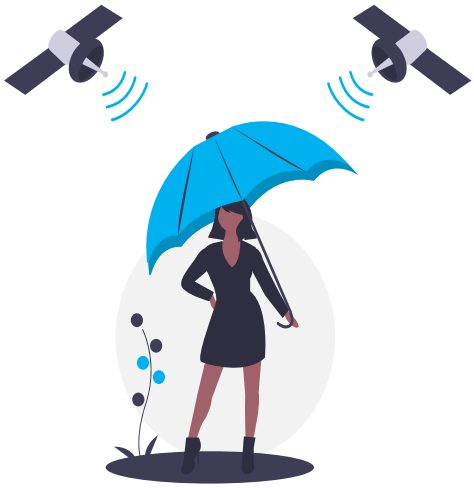
Accedere

Independent Service Auditor's Report

Illustrative

We Can Help With Your Cloud Compliance

We provide end to end cloud security assessments .We can cover all key requirements to provide an assurance of your compliance with cloud security. Our unique delivery method improves timelines and thus reduces costs of your compliance. Our proven methodology saves times as well as costs thus giving you the benefit of timely assurance towards privacy compliance with reasonable costs.



Other cloud security services

- SOC reports for Cloud Security
- SOC reports with C5 Cloud Controls
- CSA STAR Attestation/Certification
- ISO/IEC27001/27017/27018/27701 Certifications

Our Value Delivery

1. Experienced team in the area of Cyber Security.
2. Licensed CPA, Firm registered with PCAOB and Cloud Security Alliance.
3. Project management methodology applied to each engagement. These engagements are executed by senior professionals.
4. Prompt services with engagements completed in record time.
5. Ongoing support. We are with you whenever you need us.
6. Our services are competitively priced to provide you a higher ROI.