OWASP TOP 10 CLOUD SECURITY RISK

1. Acountability and data ownershipc:

Accountability: Responsible stewardship of data.

Data Ownership: Control and rights over one's information.

2.User identify federation:

User identity federation involves integrating and centralizing user authentication across multiple systems or services.

3.Regulatory compliance business:

Regulatory compliance businesses ensure companies adhere to laws and standards, mitigating legal risks. They offer expertise in navigating complex regulations, fostering a secure and compliant operating environment.

4. Business continuity and resiliency:

Business continuity ensures seamless operations during disruptions, while resiliency focuses on adapting and recovering swiftly from unexpected challenges, collectively safeguarding organizational stability and success.

5.User Privacy and Secondary Usage of Data:

User privacy is paramount; transparent communication on data usage builds trust. Secondary data usage should align with user expectations, ensuring ethical and responsible practices.

6.Service and Data Integration:

Service integration involves combining different software services to work together seamlessly, enhancing overall functionality. Data integration focuses on unifying information from diverse sources, ensuring coherence and accessibility across an organization.

7.Multi tenancy and physical security:

Multi-tenancy involves multiple users or entities sharing a single software instance, optimizing resource utilization. Physical security ensures protection of hardware and data through measures like access controls, surveillance, and environmental safeguards.

8.Incidence analysis and forensic support:

Incidence analysis involves examining events or situations to determine their causes and impacts. Forensic support in this context entails providing expert assistance in investigating and analyzing evidence related to incidents, aiding in legal or security proceedings.

9.Infrastructure security:

Infrastructure security involves safeguarding essential systems, networks, and assets to prevent unauthorized access, disruptions, or damage. It encompasses measures like firewalls, encryption, and monitoring to ensure the resilience and integrity of critical infrastructure.

10.Non-production environment exposure:

Exposing non-production environments can pose security risks, as they may lack the same safeguards as production setups. Limiting access and applying security measures is crucial to safeguard sensitive data and prevent unauthorized access.