OWASP TOP 10 CLOUD SECURITY RISKS

Accountability and ownership :

1. Accountability:
   Definition: Accountability refers to the obligation and responsibility of individuals, organizations, or entities to take ownership of their actions, decisions, and the consequences that arise from them.

2. Data Ownership:
   Definition: Data ownership refers to the right and control over data, determining who has the authority to make decisions regarding the collection, usage, and sharing of specific datasets.

User Identity Federation

User Identity Federation is a concept in identity and access management (IAM) that involves linking and coordinating user identity information across multiple systems, applications, or domains. The goal of identity federation is to enable a seamless and secure user experience across various platforms without the need for users to maintain separate credentials for each service.

Regulatory compliance business

Regulatory compliance in business refers to the process by which companies adhere to laws, rules, and regulations relevant to their industry and operations. Compliance ensures that businesses operate within the legal framework, uphold ethical standards, and meet the requirements set by regulatory authorities. Non-compliance can result in legal consequences, financial penalties, and damage to a company's reputation.

Business continuity and resiliency

Business continuity and resiliency are essential aspects of organizational management aimed at ensuring that a business can continue its critical operations, services, and functions even in the face of disruptions or disasters. These concepts involve proactive planning, risk management, and the development of strategies to maintain essential business functions during and after adverse events.

User Privacy and Secondary Usage of Data

User privacy and the secondary usage of data are critical considerations in the handling of personal information by organizations. User privacy involves protecting individuals' personal data and ensuring that it is handled in a manner that respects their rights and expectations. Secondary usage of data refers to the practice of using collected data for purposes other than the original intent for which it was collected.

Service and Data Integration

Service and data integration are two crucial components in the realm of information technology that focus on streamlining processes, enhancing functionality, and improving overall efficiency within an organization.

Multi tenancy and physical security

Multi-tenancy and physical security are two concepts that play important roles in different aspects of information technology and organizational management.

Incidence analysis and forensic support

Incident analysis and forensic support are critical components of cybersecurity and digital forensics. They involve the investigation, analysis, and response to security incidents or cyberattacks.

Infrastructure security

Infrastructure security involves safeguarding an organization's information technology (IT) infrastructure, including hardware, software, networks, and data, from unauthorized access, attacks, and disruptions. It encompasses a range of practices, policies, and technologies aimed at protecting the confidentiality, integrity, and availability of critical systems and data.