Certificate in Cloud Transformation Management

Cloud Governance and Vendor Management

Accountability refers to the responsibility of individuals or organizations to ensure that their actions and decisions are transparent, and they are answerable for the consequences of those actions. In Cloud Governance and Vendor Management, accountability is crucial to ensure that all stakeholders are held responsible for their actions and decisions related to cloud services. This includes ensuring that cloud vendors are held accountable for the security, integrity, and availability of cloud services.

Application Programming Interface (API) is a set of defined rules that enables different applications to communicate with each other. In Cloud Governance and Vendor Management, APIs play a critical role in integrating cloud services with existing systems and applications. APIs can be used to automate tasks, integrate cloud services with other systems, and monitor cloud usage.

Audit refers to the process of evaluating and examining an organization's cloud services to ensure compliance with regulatory requirements, industry standards, and organizational policies. In Cloud Governance and Vendor Management, audits are essential to identify risks, vulnerabilities, and areas for improvement. Audits can be conducted internally or by external auditors.

Business Continuity Planning (BCP) refers to the process of developing and implementing plans to ensure that an organization's operations continue to function during and after a disaster or outage. In Cloud Governance and Vendor Management, BCP is critical to ensure that cloud services are resilient and can recover quickly from disruptions. BCP involves identifying critical business processes, assessing risks, and developing plans to mitigate those risks.

Cloud Access Security Broker (CASB) refers to a security solution that acts as an intermediary between users and cloud services. In Cloud Governance and Vendor Management, CASB is used to monitor and control user access to cloud services, enforce security policies, and protect sensitive data.

Cloud Computing refers to the delivery of computing resources over the internet. In Cloud Governance and Vendor Management, cloud computing is a key concept that involves provisioning and managing cloud services, such as infrastructure, platforms, and applications.

Cloud Governance refers to the process of managing and regulating cloud services to ensure that they are aligned with organizational objectives and comply with regulatory requirements. In Cloud Governance and Vendor Management, cloud governance involves establishing policies, procedures, and standards for cloud services, as well as monitoring and reporting on cloud usage.

Cloud Service Provider (CSP) refers to a third-party organization that provides cloud services to customers. In Cloud Governance and Vendor Management, CSPs are responsible for provisioning and managing cloud

services, including infrastructure, platforms, and applications.

Compliance refers to the process of ensuring that an organization's cloud services adhere to regulatory requirements, industry standards, and organizational policies. In Cloud Governance and Vendor Management, compliance is critical to avoid penalties, fines, and reputational damage.

Contract Management refers to the process of negotiating, executing, and managing contracts with cloud vendors. In Cloud Governance and Vendor Management, contract management involves reviewing and approving contracts, monitoring contract performance, and renegotiating contracts as needed.

Data Encryption refers to the process of converting plaintext data into ciphertext to protect it from unauthorized access. In Cloud Governance and Vendor Management, data encryption is critical to protect sensitive data stored in or transmitted through cloud services.

Data Loss Prevention (DLP) refers to a set of technologies and processes designed to detect and prevent sensitive data from being leaked or stolen. In Cloud Governance and Vendor Management, DLP is used to identify and classify sensitive data, monitor data transfers, and block unauthorized data exfiltration.

Disaster Recovery (DR) refers to the process of restoring an organization's operations after a disaster or outage. In Cloud Governance and Vendor Management, DR involves developing and implementing plans to restore cloud services, recover data, and resume business operations.

FedRAMP refers to the Federal Risk and Authorization Management Program, which is a US government-wide program that standardizes the approach to security assessment and authorization of cloud services. In Cloud Governance and Vendor Management, FedRAMP is used to ensure that cloud services meet federal security standards.

HIPAA refers to the Health Insurance Portability and Accountability Act, which is a US law that regulates the use and disclosure of protected health information. In Cloud Governance and Vendor Management, HIPAA is used to ensure that cloud services comply with healthcare regulations.

Identity and Access Management (IAM) refers to the process of managing and controlling user access to cloud services. In Cloud Governance and Vendor Management, IAM involves authenticating and authorizing users, managing user roles and permissions, and monitoring user activity.

Incident Management refers to the process of identifying, containing, and resolving security incidents related to cloud services. In Cloud Governance and Vendor Management, incident management involves developing and implementing incident response plans, training incident response teams, and reviewing incident response procedures.

Information Security refers to the practice of protecting information from unauthorized access, use, disclosure, disruption, modification, or destruction. In Cloud Governance and Vendor Management, information security involves implementing security controls, monitoring security threats, and responding to

security incidents.

IT Service Management (ITSM) refers to the process of managing and delivering IT services to customers. In Cloud Governance and Vendor Management, ITSM involves defining and implementing IT service management processes, monitoring IT service performance, and continuously improving IT services.

Key Management refers to the process of managing and controlling encryption keys used to protect sensitive data. In Cloud Governance and Vendor Management, key management involves generating and distributing encryption keys, managing key lifecycle, and revoking keys as needed.

Managed Security Service Provider (MSSP) refers to a third-party organization that provides managed security services to customers. In Cloud Governance and Vendor Management, MSSPs are used to monitor and respond to security threats, manage security incidents, and provide security consulting services.

Network Security refers to the practice of protecting networks from unauthorized access, use, disclosure, disruption, modification, or destruction. In Cloud Governance and Vendor Management, network security involves implementing security controls, monitoring network traffic, and responding to network security incidents.

PCI-DSS refers to the Payment Card Industry Data Security Standard, which is a set of security standards for organizations that handle credit card information. In Cloud Governance and Vendor Management, PCI-DSS is used to ensure that cloud services comply with payment card industry regulations.

Platform as a Service (PaaS) refers to a cloud computing model in which a third-party provider delivers a platform for developing, running, and managing applications. In Cloud Governance and Vendor Management, PaaS involves provisioning and managing cloud-based platforms, such as application servers, databases, and middleware.

Risk Management refers to the process of identifying, assessing, and mitigating risks related to cloud services. In Cloud Governance and Vendor Management, risk management involves identifying and assessing risks, developing and implementing risk mitigation plans, and monitoring risk exposure.

Security Information and Event Management (SIEM) refers to a security solution that monitors and analyzes security-related data from various sources. In Cloud Governance and Vendor Management, SIEM is used to detect and respond to security threats, identify and contain security incidents, and improve security posture.

Service Level Agreement (SLA) refers to a contractual agreement between a cloud vendor and a customer that defines the terms and conditions of cloud services, including service availability, performance, and support. In Cloud Governance and Vendor Management, SLAs are used to establish and manage customer expectations, monitor cloud service performance, and resolve service-related issues.

Software as a Service (SaaS) refers to a cloud computing model in which a third-party provider delivers software applications over the internet. In Cloud Governance and Vendor Management, SaaS involves

provisioning and managing cloud-based applications, such as customer relationship management and enterprise resource planning.

Vendor Management refers to the process of managing and overseeing cloud vendors to ensure that they meet organizational requirements and comply with regulatory requirements. In Cloud Governance and Vendor Management, vendor management involves selecting and contracting with cloud vendors, monitoring vendor performance, and managing vendor relationships.

Virtual Private Network (VPN) refers to a network that uses encryption and tunneling to protect data transmitted over the internet. In Cloud Governance and Vendor Management, VPNs are used to secure remote access to cloud services, protect sensitive data, and comply with regulatory requirements.

Wide Area Network (WAN) refers to a network that connects multiple locations over a large geographic area. In Cloud Governance and Vendor Management, WANs are used to connect cloud services to on-premises infrastructure, enable remote access to cloud services, and improve network performance.