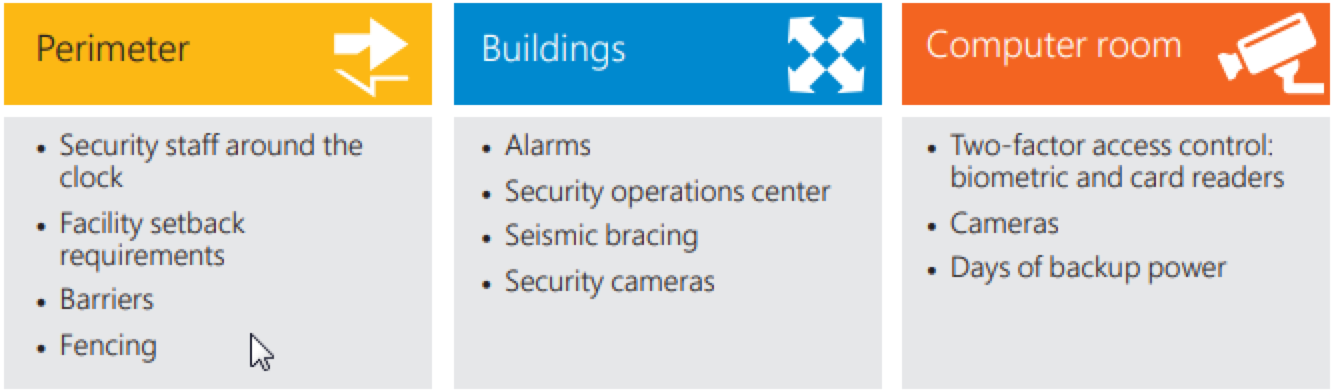
AWS, Google Cloud, Azure for security and compliance features.

As the cloud adoption within the enterprise is getting bigger and bigger and the importance of Cloud security is the highest priority, following are the key security and compliance features offered by the AWS, Microsoft and Google.

On any of the following offering, Permission is required for all penetration tests, Security is the shared responsibilities between Cloud service provider and the customer.

Cloud service provide manages security on following assets.

- Facilities
- Physical security of hardware
- Network infrastructure
- Virtualization infrastructure



Perimeter

- Security staff around the clock
- Facility setback requirements
- Barriers
- Fencing

Buildings

- Alarms
- Security operations center
- Seismic bracing
- Security cameras

Computer room

- Two-factor access control: biometric and card readers
- Cameras
- Days of backup power

And the customer is responsible for the security

- Amazon Machine Images (AMIs)/Virtual machines
- Operating systems
- Applications
- Data in transit
- Data at rest
- Data stores
- Credentials
- Policies and configuration

AWS Microsoft and Google cloud service providers adhere to the below compliance processes. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider.

- ISO 27001, FedRAMP, and
- HIPAA
- ISO 27001:5
- NIST 800-53
- SOC 1 Type 2
- SOC 2 Type 2
- FedRAMP/FISMA
- PCI DSS Level 1
- UK G-Cloud
- US-EU Safe
- Harbo.

AWS Security	**Microsoft Azure Security**	**Google Cloud Security.**

AWS IAM services centrally manage users, security credentials such as passwords, access keys, and permissions policies. Trusted Advisor tool is used to check the compliance with the security recommendations Consolidated billing across multiple accounts to ease the complexity and licensing model. AWS Multi-factor authentication (MFA) provides an extra level of security to login in to AWS resources. The same is applied for API calls Resource policies, Capability policies, IAM policies are to secure resources, capabilities and IAM users.	Azure offers Microsoft Antimalware for cloud services and virtual machines. Azure provided encryption capabilities up to AES-256. Azure Key Vault helps safeguard cryptographic keys and secrets. Certifications and attestations are provided to generate reports. Built-in cryptographic technology enables customers to encrypt communications within and between deployments. Network isolation feature is used to separate the deployments across Azure logically. Tools such as Guest operating system (OS) firewalls, Virtual Network Gateway	Google Cloud Security Scanner. This tool scans App Engine applications for cross-site scripting and mixed- content issues. Google Cloud Logging provides a generalized, centralized location for logs. Google Cloud Identity and Access Management (Cloud IAM) to create and manage permissions for GCP assets and resources. Google's Titan chip establishes trust at the hardware root for all machines and assets in GCP. Google's infrastructure provides a variety of storage services, such as Bitable and Spanner, and a central key management service to encrypt the data at rest. The GFE ensures that all TLS connections are terminated using correct certificates, Denial of Service (DoS) protection, and TLS termination

Data at rest is secured using HSMs or CloudHSM modules. Database encryption, Digital Rights Management (DRM), and Public Key Infrastructure (PKI) including authentication and Authorization, SQL cryptographic function Amazon RDS are some of the features offered to encrypt the data at rest. Decommission Data and Media Securely • AWS follows the techniques detailed in Department of Defense (DoD) 5220.22-M (“National Industrial Security Program Operating Manual”) or NIST SP 800-88 (“Guidelines for	configuration, and Virtual Private Networks and created and configured to control the security across the platform. Azure has a defense system against Distributed Denial-of-Service (DDoS) attacks on Azure platform services. It uses standard detection and mitigation techniques	GCE persistent disks are encrypted at-rest using keys protected by the central infrastructure key management system

Media Sanitization”) to destroy data as part of the decommissioning process Protect Data in Transit Encrypt data in transit using IPSec ESP and/or SSL/TLS. Bastion hosts (JUMP Server) are used to enforce control and visibility. Security groups and Network Access Control Lists (NACLs) that enable firewall rules across the AWS VPN. Flow Logs provides further visibility as it enables you to capture information about the IP traffic AWS uses proprietary techniques to mitigate and contain DoS/DDoS attack		