review section

Questions	Notes

shared responsability Model	• **AWS:Security of the cloud**
	  ◦ AWS is responsible for : regions , AZs , edgeLocation..
	  ◦ AWS controls access to its data centers
	  ◦ Networking componenets: generators,power supply
	  ◦ Software: is responsable for any managed service like RDS , S3 , ECS , or Lambda patching of host operating system , and data access enpoints
	• **You: Security in The Cloud**
	  ◦ Application data : including encryption
	  ◦ security Configuration : securing your account and API calls , rotating credentials , restricting internet, access from your VPCs
	  ◦ Patching: you are responsible for the guest operating system (os) includes updates and security patches
	  ◦ Identity and access management
	  ◦ Network traffic : you are responsible for network traffic protection which includes security group firewall configuration
	  ◦ Installed software

Well-Architected Framework	• **Operational Excellence:** plan for and anticipate failure,Deploy smaller , reversible changes,script operations as code,Learn from failure and refine: CodeCommit for version Control • **Security:** automate security tasks,encrypt data in transit and at rest,assign only the least privileges required,track who did what and when,ensure security at all applcation layers : Configure Central logging actions in your account using CloudTrail • **Reliability:** recover from failure automatically,scale horizontally for resilience,stop guessing capacity,manage change through automation,Test recovery procedures: Multi-AZ deployments using RDS • **Performance efficiency:** use severless arechitecture first ,Use multi-region deployments,delegate tasks to a cloud vendor,Expriments with virtual resources : You can use Lambda to run code with zero administration • **Cost Optimization:** utilize consumption-based pricing,Implement Cloud financial Managment,Measure overall efficiency,pay only for resources your application requires : S3 intelligent-tiering to automatically move your data between access tiers based on your usage patterns • **Sustainability:** understand your impact,establish sustainability goals,use managed services,reduce downstream impact: EC2 autoscaling you are maximizing utilization
security	• **Identity and Access Management (IAM):** IAM allows you to control access to your AWS services and resources. • **Web Application Firewall (WAF):** WAF helps protect your web applications against common web attacks. • **Shield:** Shield is a managed Distributed Denial of Service (DDoS) protection service. • **Macie:** Macie helps you discover and protect sensitive data. • **Config:** Config allows you to assess, audit, and evaluate the configurations of your resources. • **GuardDuty:** GuardDuty is an intelligent threat detection system that uncovers unauthorized behavior. • **Inspector:** Inspector works with EC2 instances to uncover and report vulnerabilities. • **Artifact:**Artifact offers on-demand access to AWS security and compliance reports. • **Cognito:** Cognito helps you control access to mobile and web applications.
Encryption	• **Key Management Service (KMS):** KMS allows you to generate and store encryption keys. • **CloudHSM:** CloudHSM is a hardware security module (HSM) used to generate encryption keys.
Secrets Manager	• Secrets Manager allows you to manage and retrieve secrets (passwords or keys).