TASK 2: Evaluation Using the AWS Well-Architected Framework (WAF)

The AWS Well-Architected Framework provides a set of best practices to help organizations design, build, and maintain secure, reliable, efficient and cost-effective cloud workloads. It is organized around five core pillars, each focusing on a different aspect of architecture: Operational Excellence, Security, Reliability, Performance Efficiency and Cost Optimization. By evaluating a workload against these pillars, architects can identify strengths and potential risks in the design before deployment. This proactive approach ensures that workloads are well-architected from day one, reducing the likelihood of failures, security issues, or unnecessary costs, while also enabling smooth scalability and operation efficiency. Each pillar provides guiding principles and recommended AWS services to address common design challenges, helping teams make informed decisions and align their architecture with AWS best practices.

Pillar	**Observation (strength)**	**Improvement Area**	**Recommendation**	**Supporting AWS service**
Operational Excellence	The architecture uses a simple understandable two-tier design, which makes deployment and management easier.	Lack of defined monitoring, alerting and automated deployment strategy.	Implement infrastructure as Code for reproducible deployments and define CloudWatch alarms and logging before launch	AWS CloudFormation, Amazon CloudWatch, AWS Systems Manager
Security	Use of private subnets for the database helps protect sensitive data from public access	Security groups may be overly permissive. For instance, Open SSH or database ports	Restrict security group rules to only the necessary IP ranges and ports; enforce least-privilege IAM roles for all resources	AWS IAM, AWS Security Hub, Amazon VPC security Groups

Reliability	Amazon RDS (managed database) is used, which provides built-in fault tolerance features.	Both the web and database tiers are in a single Availability Zone creating a single point of failure	Deploy resources across multiple Availability Zones and enable automated backups for the database.	Amazon RDS Multi-AZ, Amazon Route 53 and AWS Backup for automated snapshots.
Performance Efficiency	Using EC2 instances for the web tier allows fine-grained control over instance types and sizing.	No auto Scaling is defined, which could lead to performance bottlenecks under traffic spikes	Implement Auto Scaling for the web tier and consider using VPC endpoints to optimize traffic to AWS services.	Amazon EC2 Auto Scaling, Elastic Load Balancing, VPC Endpoints
Cost Optimization	The simple two-tier setup avoids unnecessary complexity, keeping initial costs lower.	Overprovisioning EC2 instances without scaling would increase costs.	Right-size EC2 instances and configure Auto Scaling to dynamically adjust resources based on traffic.	AWS Compute Optimizer, Amazon EC2 Auto Scaling

TASK 3

Below is an in-depth CAF readiness analysis, structured exactly around the six AWS cloud Adoption Framework (CAF) perspectives.

i. **Business Perspective**: From a business perspective, the organization appears moderately ready for cloud adoption, with a clear motivation to migrate the existing two-tier web application to AWS. Management's desire to align the migration with AWS best practices from day one suggests an understanding of the long-term value of cloud computing, such as improved scalability, availability and cost efficiency. However, the readiness could be strengthened by clearly defining business outcomes beyond the technical migration itself. For example, success metrics such as reduced infrastructure costs, improved application uptime, or faster feature delivery are not yet explicitly stated. To enable successful migration, the organization should align cloud goals with broader business objectives. This includes developing a clear business case that outlines expected benefits, costs and timeliness. Stakeholders should also prioritize workloads and confirm whether this application is part of a larger modernization strategy. Establishing executive sponsorship and ensuring ongoing business involvement will help maintain momentum and ensure the migration delivers measurable value rather than being treated as a purely technical exercise.

ii. **People Perspective:** The people perspective focuses on skills, roles and organizational culture. In this scenario, the organization shows early-stage readiness, as there is an initiative to migrate AWS, but no explicit mention of cloud skills, training or role changes. Teams that previously managed on-premises infrastructure may lack hands on experience with AWS services, automation tools and shared responsibility models. Without addressing this gap, the migration could lead to operational inefficiencies or misconfigurations. Key enablers for success include upskilling existing staff through AWS training, certifications, and hands-on labs. Roles and responsibilities may need to evolve, particularly for system administrators and operations teams, who will transition toward cloud engineers and DevOps-focused roles. Encouraging collaboration between development, operations, and security teams is also important to support cloud-native practices.

Leadership should promote a learning culture where experimentation and continuous improvement are encouraged. By investing in people early, the organization reduces risk and ensures teams are confident and capable of managing cloud workloads post-migration.

iii. **Governance Perspective:** From a governance standpoint, the organization appears to be in the early planning phase. While there is an emphasis on following AWS best practices, there is no clear indication that governance structures such as policies for cost control, resource ownership, or compliance are in place. This is common in organizations transitioning from on-premises environments, where governance is often implicit rather than policy-driven. To improve readiness, the organization should establish cloud governance frameworks before deploying production workloads. This includes defining account structures, naming conventions, tagging strategies, and cost allocation models. Guardrails should be implemented to ensure resources are deployed securely and consistently, such as using AWS Organizations and service control policies. Additionally, decision-making processes around architecture standards and risk management should be documented. Strong governance enables teams to innovate safely while maintaining control, reducing the likelihood of cost overruns, security gaps, or unmanaged resources as cloud adoption scales.

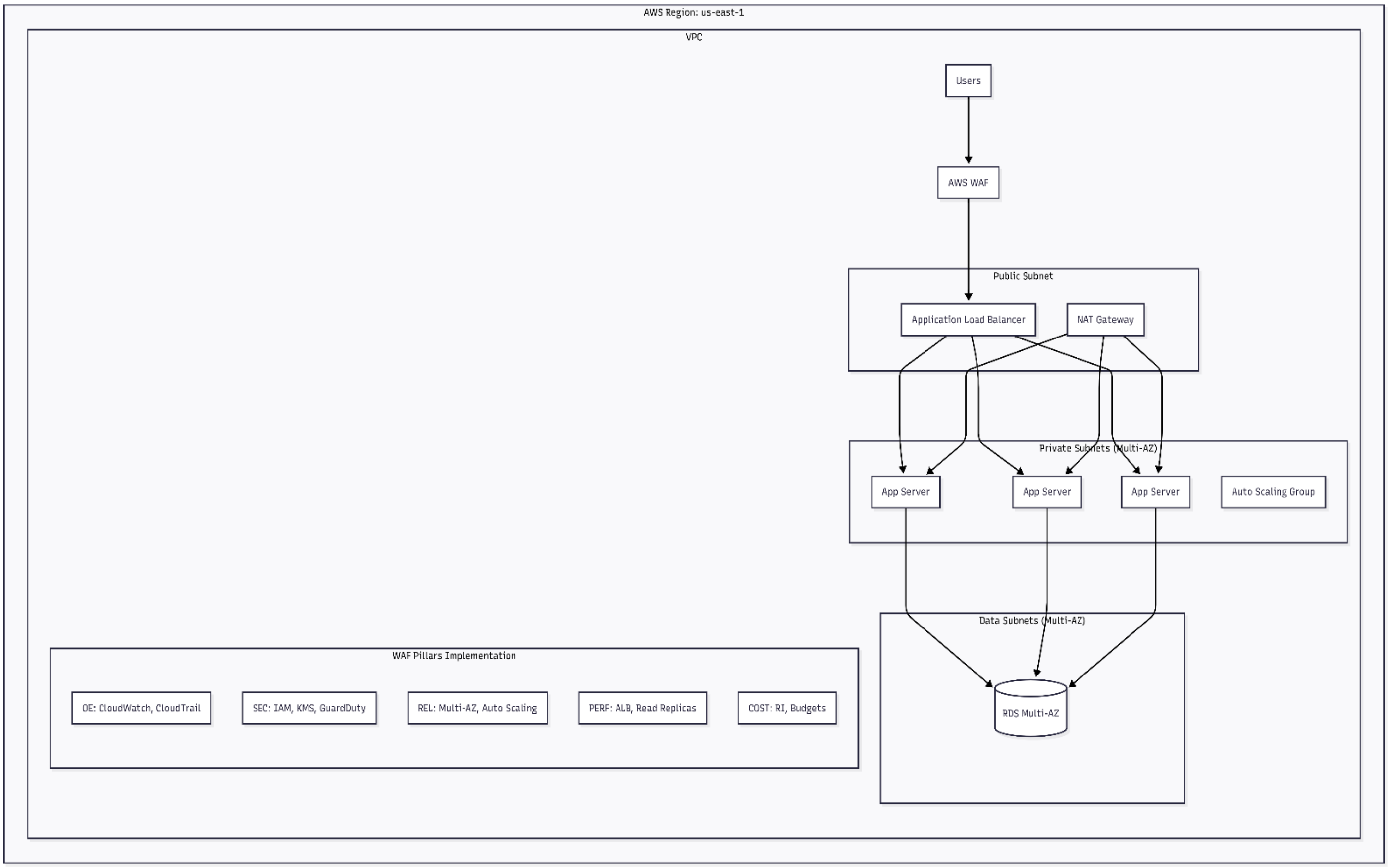
iv. **Platform Perspective:** The Platform perspective evaluates the technical foundation required to support cloud workloads. In this case, the organization demonstrates a reasonable level of readiness, as the target architecture leverages core AWS services such as VPCs, EC2, RDS, and load balancers. This shows an understanding of how traditional on-premises applications can be mapped to cloud infrastructure. However, to fully enable a successful migration, the platform should be designed with scalability, automation, and resilience in mind. Infrastructure as Code tools, such as AWS CloudFormation or Terraform, should be adopted to ensure consistent and repeatable deployments. Network architecture should support future growth, including multi-AZ designs and clear separation between public and private resources. Standardized templates and reusable components can accelerate future migrations. By strengthening the platform foundation early, the organization ensures the environment is not only functional but also flexible and ready to support additional workloads over time.

v. **Security Perspective**: From a security perspective, the organization shows baseline awareness, particularly using private subnets for the database and controlled access between tiers. This aligns well with AWS security best practices. However, overall readiness can be improved by adopting a more proactive and systematic approach to cloud security. Key actions include implementing identity and access management policies that enforce least privilege using IAM roles rather than static credentials. Logging and monitoring should be enabled from the start using services like CloudWatch and CloudTrail to provide visibility into system activity. Security responsibilities should be clearly defined under AWS's shared responsibility model so teams understand what AWS manages versus what the organization must secure. Automating security checks and incorporating them into deployment pipelines will further reduce risk. A strong security foundation ensures the migration does not introduce new vulnerabilities and builds trust in the cloud environment.

vi. **Operations Perspective**: Operational readiness is critical for long-term success after migration. In this scenario, the organization appears to be at an early maturity level, with limited mention of monitoring, incident response, or operational processes in the cloud. While the application may function after migration, operating it effectively at scale requires additional planning. To improve readiness, the organization should define operational processes for monitoring, alerting, backup, and recovery. Amazon CloudWatch can be used to collect metrics and logs, while automated backups and recovery strategies should be implemented for critical data. Operational playbooks and runbooks should be created to guide teams during incidents. Adopting DevOps practices, such as automation and continuous improvement, will help teams respond quickly to issues and optimize performance over time. A well-prepared operations model ensures the application remains reliable, maintainable, and cost-effective throughout its lifecycle in AWS.

TASK 4

Table 1: Revised AWS architecture that aligns with WAF and CAF best practices



The diagram depicts a secure, highly available, and scalable AWS architecture deployed in the us-east-1 region, organized within a Virtual Private Cloud (VPC). Internet users access the application through AWS WAF, which provides web-layer security, followed by an Application Load Balancer (ALB) located in a public subnet to distribute traffic. The ALB forwards requests to multiple application servers (EC2 instances) managed by an Auto Scaling Group spread across private subnets in multiple Availability Zones for fault tolerance and scalability. Outbound internet access for these servers is provided by a NAT Gateway, also in the public subnet. Application data is stored in an Amazon RDS database configured for multi-AZ deployment to ensure high availability and failover support. The "WAF Pillars Implementation" section highlights how the architecture addresses the AWS Well-Architected Framework’s five pillars: operational excellence, security, reliability, performance efficiency, and cost optimization, utilizing AWS services such as CloudWatch, CloudTrail, IAM, KMS, and budget controls to ensure best practices are followed throughout the environment.