LAB: DESIGN AND EVALUATE AN AWS SOLUTION USING THE WELL-ARCHITECTED AND CLOUD ADOPTION FRAMEWORKS

Task 1 – Review the Existing Architecture

1. Components of the Workload

The organization is migrating a **two-tier web application** consisting of:

- **Frontend Web Application**
  - Hosts the user interface.
  - Handles HTTP/HTTPS requests from users.
  - Typically deployed on web servers or application servers
- **Backend Database**
  - Stores application data (users, transactions, records)
  - Communicates only with the application layer.
- **Networking Layer**
  - Virtual network connecting frontend and backend.
  - Internet access for users
- **Compute Infrastructure**
  - Servers currently hosted on-premises
  - Responsible for application processing

2. Potential Risks or Weaknesses

Risk / Weakness	**Explanation**
Single Availability Zone deployment	Failure of one AZ could cause total service outage.
No automated backup strategy	Data loss risk if database fails or is corrupted.
Open security groups	May allow unauthorized access to servers or database.
Manual scaling	System cannot automatically handle traffic spikes.
Lack of monitoring/logging	Failures may not be detected quickly.
Tight coupling between tiers	Makes scaling and maintenance difficult.

Task 2 – Evaluation Using AWS Well-Architected Framework

Below is the evaluation using the **five AWS Well-Architected pillars**.

Well-Architected Evaluation Table

Pillar	Observation	Improvement Recommendation	Supporting AWS Service
Operational Excellence	Deployment and maintenance processes are manual, increasing risk of configuration errors and slow recovery during incidents.	Implement Infrastructure as Code (IaC) and automated monitoring to enable repeatable deployments and faster incident response.	AWS CloudFormation, AWS CloudWatch, AWS CodePipeline
Security	Application and database tiers may be exposed through permissive network access and lack centralized identity control.	Enforce least-privilege access, isolate backend resources in private subnets, enable encryption at rest and in transit, and apply edge protection.	AWS IAM, AWS KMS, AWS WAF, VPC Security Groups
Reliability	Current architecture introduces single points of failure due to single-instance and single-AZ deployment.	Design for fault tolerance using Multi-AZ deployment, load balancing, health checks, and automated backups to ensure high availability.	Elastic Load Balancer, EC2 Auto Scaling, Amazon RDS Multi-AZ
Performance Efficiency	Fixed compute capacity cannot dynamically adapt to workload demand, leading to latency during peak usage.	Use elastic scaling and distributed content delivery with caching to optimize response time and resource utilization.	EC2 Auto Scaling, Amazon CloudFront, Amazon ElastiCache
Cost Optimization	Always-on infrastructure may result in over-	Adopt consumption-based pricing through auto scaling,	AWS Cost Explorer, AWS Auto Scaling,

	provisioning and unnecessary operational expenses.	right-sizing resources, and continuous cost monitoring.	AWS Trusted Advisor

Structured Reasoning

The evaluation shows that while the current architecture supports application functionality, it lacks cloud-native resilience, automation, and scalability. By adopting AWS managed services and aligning with Well-Architected principles, the organization can achieve:

- Improved system availability
- Stronger security posture
- Automatic scaling during demand changes
- Reduced operational overhead.
- Better cost control

The recommended improvements transition the application from a traditional infrastructure model to a highly available, secure, and elastic cloud architecture aligned with AWS best practices.

Task 3 – Applying the AWS Cloud Adoption Framework (CAF)

1. Business Perspective

The organization demonstrates moderate readiness for cloud adoption, as management has already decided to migrate the application to AWS to improve scalability and reliability. This indicates alignment between IT initiatives and business objectives such as improved service availability and enhanced customer experience. However, business readiness may still be limited by unclear cost expectations and lack of defined cloud value metrics. Traditional on-premises budgeting models often focus on capital expenditure, whereas cloud environments require operational expenditure planning and continuous cost monitoring.

Key actions include defining measurable business outcomes such as uptime targets, performance improvements, and cost efficiency goals. Leadership should establish a cloud business case outlining expected return on investment (ROI), migration benefits, and long-term innovation opportunities. Financial governance practices, including cost forecasting and chargeback models, should also be introduced to ensure spending transparency. Additionally, stakeholders must align migration priorities with organizational strategy to avoid technology-driven decisions without business value. Strengthening business alignment ensures the cloud migration supports organizational growth, agility, and competitive advantage rather than simply replacing existing infrastructure.

2. People Perspective

From a people readiness standpoint, the organization may face skill gaps because teams previously managed on-premises infrastructure rather than cloud-native environments. Staff may lack experience with AWS services, automation practices, and DevOps methodologies. Without proper preparation, resistance to change and uncertainty about new roles could slow adoption and reduce productivity during migration.

To enable successful transformation, the organization should invest in structured cloud training and certification programs for developers, system administrators, and operations teams. Establishing clear role definitions, such as cloud architects and DevOps engineers, will help employees understand responsibilities within the new environment. Creating a cloud center of excellence (CCoE) can promote knowledge sharing, governance standards, and best practices across departments. Change management initiatives, including workshops and internal communication strategies, should also be implemented to encourage adoption and reduce organizational resistance. By empowering employees with the right skills and mindset, the organization can build a culture that supports continuous learning, collaboration, and innovation within the cloud ecosystem.

3. Governance Perspective

Governance readiness is likely limited during early migration stages because policies designed for on-premises environments may not adequately address cloud resource management. Risks may include inconsistent resource provisioning, lack of standardized configurations, and uncontrolled spending. Without governance controls, teams could deploy resources in ways that introduce security, compliance, or financial risks.

Key enablers include establishing cloud governance policies that define account structures, naming conventions, tagging strategies, and resource ownership. Implementing guardrails through policy enforcement ensures compliance with organizational and regulatory requirements. Financial governance practices should monitor usage and prevent cost overruns through budgeting and alerts. Decision-making frameworks must also clarify approval processes for deploying new services or accessing sensitive data. Introducing automated governance mechanisms helps maintain consistency while allowing teams to innovate safely. Strong governance ensures cloud adoption remains controlled, compliant, and aligned with organizational standards while reducing operational risks associated with decentralized resource creation.

4. Platform Perspective

The platform perspective evaluates the organization's technical readiness to build and manage cloud infrastructure. The current two-tier application suggests basic architectural maturity but limited cloud-native design capabilities. Existing systems may not yet be optimized for scalability, automation, or resilience required in AWS environments.

To improve readiness, the organization should design a standardized cloud platform using reusable infrastructure patterns. Establishing a secure Virtual Private Cloud (VPC) architecture with public and private subnets enables proper network segmentation. Infrastructure as Code should be adopted to automate provisioning and ensure consistency across environments. The organization should also implement scalable compute services, managed databases, and load balancing to support high availability. Standardized deployment pipelines and environment templates will reduce configuration errors and accelerate development cycles. By creating a well-defined cloud platform foundation, teams can deploy applications efficiently while maintaining reliability, scalability, and operational consistency across workloads.

5. Security Perspective

Security readiness is a critical concern during cloud migration because traditional perimeter-based security models do not directly translate to cloud environments. The organization may lack centralized identity management, encryption standards, and continuous monitoring capabilities suitable for AWS. Misconfigured access permissions or exposed resources could introduce significant risks.

Key actions include adopting a shared responsibility security model and implementing identity-first security controls. Strong identity and access management policies should enforce least-privilege access across all services. Data protection measures such as encryption at rest and in transit must be standardized. Continuous monitoring and logging should be enabled to detect threats and maintain audit visibility. Security awareness training for employees is also necessary to reduce human-related risks. Establishing automated security checks and compliance monitoring ensures consistent protection across environments. Strengthening the security perspective enables the organization to protect sensitive data while maintaining trust and regulatory compliance throughout the migration process.

6. Operations Perspective

Operational readiness focuses on the organization's ability to manage and maintain workloads after migration. Currently, operations may rely on manual monitoring and reactive troubleshooting practices inherited from on-premises infrastructure. Such approaches are inefficient in dynamic cloud environments where resources scale automatically.

To improve readiness, the organization should adopt cloud-based monitoring, logging, and incident response processes. Automated alerts and health checks allow teams to detect and resolve issues proactively. Operational runbooks and standard operating procedures should be updated to reflect cloud workflows. Backup, disaster recovery, and patch management strategies must also be automated to reduce downtime and manual effort. Implementing DevOps practices encourages collaboration between development and operations teams, improving deployment speed and reliability. Continuous improvement through performance metrics and operational reviews ensures systems remain efficient over time. A mature operations model allows the organization to maintain high availability while minimizing operational overhead in AWS.

Task 4 – Design an Improved AWS Architecture

1. Revised AWS Architecture Description

Based on the evaluation using the AWS Well-Architected Framework and Cloud Adoption Framework, the improved solution redesigns the two-tier application into a **highly available, secure, scalable, and cost-efficient cloud-native architecture**.

Proposed Architecture Components

Networking Layer

- A **Virtual Private Cloud (VPC)** spanning **multiple Availability Zones (Multi-AZ)**.
- Public and private subnet separation:
    - **Public Subnets:** Load balancer and internet-facing components.
    - **Private Subnets:** Application servers and database resources.
- Internet Gateway for external access.
- NAT Gateway allowing private resources to securely access updates without public exposure.

Frontend Layer (Presentation Tier)

- **Application Load Balancer (ALB)** distributes incoming traffic across multiple instances.
- Web/application servers hosted on **Amazon EC2 Auto Scaling Groups**.
- Optional **Amazon CloudFront** CDN to cache static content and reduce latency.

Backend Layer (Database Tier)

- **Amazon RDS (Multi-AZ deployment)** for managed relational database services.
- Automated backups and failover enabled.
- Database deployed in private subnets with no direct internet access.

Security Controls

- **IAM roles** enforcing least-privilege access.

- Security Groups and Network ACLs controlling traffic flow.
- **AWS WAF** protecting against common web attacks.
- Encryption enabled using **AWS KMS** for data at rest and TLS for data in transit.

Operations and Monitoring

- **Amazon CloudWatch** for monitoring metrics, logs, and alarms.
- **AWS CloudTrail** for auditing API activity.
- Automated deployment using **AWS CodePipeline** and Infrastructure as Code (CloudFormation).

Backup and Disaster Recovery

- Automated RDS snapshots.
- EC2 backups using AWS Backup.
- Multi-AZ deployment ensures automatic failover during outages.

2. Alignment with the Five Well-Architected Framework (WAF) Pillars

WAF Pillar	How the New Architecture Addresses It
Operational Excellence	Infrastructure as Code and CI/CD pipelines automate deployments, while CloudWatch monitoring enables proactive incident response and continuous improvement.
Security	Private subnets, IAM least privilege, encryption, WAF protection, and centralized logging strengthen the security posture and reduce attack surface.
Reliability	Multi-AZ deployment, load balancing, Auto Scaling, and automated backups eliminate single points of failure and ensure high availability.
Performance Efficiency	Auto Scaling dynamically adjusts compute resources, while CloudFront caching and managed database services optimize performance under varying workloads.

Cost Optimization	Auto Scaling prevents over-provisioning, managed services reduce operational overhead, and monitoring tools help track and optimize resource usage.

The redesigned architecture transforms the application from a traditional single-environment deployment into a resilient, scalable, and secure cloud-native solution. By integrating automation, multi-availability zone resilience, managed services, and strong governance practices, the architecture aligns with both AWS Well-Architected Framework principles and Cloud Adoption Framework readiness goals, ensuring long-term operational sustainability and business value.