Cloud Strategy & Azure Adoption for Enterprise Applications-DAY30ASSESMENT

Task 1 — Cloud Adoption Reasoning

1. Why should this organization move to the cloud instead of staying on-premises?

- Reduces infrastructure cost.

- It allows easy scaling when users increase.

- Applications can be deployed faster.

- Monitoring becomes automatic.

- Centralized authentication.

2.Which business problems will the cloud solve?

Problems cloud will solve:

- High infrastructure cost.

- Limited scalability.

- Delayed deployments.

- Manual monitoring.

- Fragmented authentication.

3. Problems cloud will NOT automatically solve:

- Poor internal processes.

- Lack of skilled staff.

- Poor application design.

- Security misconfiguration.

Task 2 — Why Azure Selection Analysis

- Works well with Microsoft products.

- Strong security features.

- Easy to scale globally.

- Strong developer ecosystem.

- Hybrid cloud support.

Task 3 — Role-Based Cloud Usage Mapping

Role	How They Use Azure	Business Benefit
Developers	Build and deploy applications	Faster releases
IT Admins	Manage servers and monitor systems	Less downtime
Security Team	Manage access and security policies	Better data protection
Executives	View dashboards and reports	Better decision making
Data Team	Analyze business data	Business insights

Task 4 — Architecture Decision Scenario

High-Level Components:

- Web Application (Frontend)

- Authentication System

- Application Layer

- Database

- Monitoring System

- Analytics Dashboard

Azure Service Categories:

- Compute Services

- Identity Services

- Database Services

- Monitoring Services

- Analytics Services

- Networking Services

Data Flow:

User → Login → Application Layer → Database → Monitoring → Analytics Dashboard

Task 5 — Decision Justification

Business: Reduces cost and improves efficiency.

Technical: Secure, automated, and integrated services.

Scalability: Auto-scaling during high traffic.

Cost: Pay-as-you-use model reduces capital expenses.

Task 6 — Risk Awareness

1. Data Security Risk – Use encryption and strong access control.

2. Vendor Lock-in – Use hybrid and open technologies.

3. Downtime Risk – Use backup and multiple regions.