Title: Cloud Strategy & Azure Adoption for Enterprise Applications

1. **Task 1 — Cloud Adoption Reasoning**
    1. Why should this organization move to the cloud instead of staying on-premises?
        - It reduces capital expenditure by eliminating hardware purchases.
        - It enables faster deployments through automation and DevOps practices.
        - It supports global availability through distributed data centers.
    2. Which business problems will the cloud solve?

High infrastructure cost	Pay-as-you-go pricing and resource optimization
Limited scalability	Auto-scaling and load balancing
Delayed deployments	CI/CD pipelines and automation

    3. Which problem will the cloud NOT automatically solve?
        - Poor application architecture
        - Inefficient coding practices
        - Weak governance policies

2. **Task 2 — Why Azure Selection Analysis**
    1. Integration
       Capability Azure provides strong integration with existing Microsoft technologies such as Windows Server, Active Directory, SQL Server, and Microsoft 365. This reduces retraining effort and ensures continuity of operationsDeveloper Ecosystem & DevOps Support
       Azure supports multiple programming languages and frameworks including:
        - .NET
        - Java
        - Python
        - Containers & Kubernetes.
    2. Security & Identity Management
       Azure offers enterprise-grade security features including:
        - Role-Based Access Control (RBAC)
        - Multi-Factor Authentication (MFA)
        - Threat detection and monitoring tools
    3. Scalability & Global Reach
       Azure operates multiple global data centers across regions worldwide.
       It enables:
        - Auto-scaling of applications
        - Load balancing

3. **Task 3 — Role-Based Cloud Usage Mapping**

Role	How They Use	Azure Business Benefit
Developers	Deploy applications, use DevOps pipelines, test environments	Faster development cycles
IT Admins	Manage infrastructure, monitoring, scaling	Reduced operational burden
Security Team	Identity policies, threat monitoring, compliance controls	Stronger security posture
Executives	Dashboards, cost reports, performance insights	Data-driven decisions
Data Team	Data storage, analytics platforms, BI tools	Business intelligence & forecasting

4. Task 4 — Architecture Decision Scenario

High-Level Architecture Components

1. Web Frontend (Customer Portal)
2. Application Layer / API Services
3. Identity & Authentication Service
4. Transactional Database
5. Monitoring & Alerting System
6. Analytics & Reporting Dashboard

Azure service categories

Layer	Azure Service Category
Web Frontend	App Hosting / PaaS Web Services
Application Layer	API / Microservices Platform
Authentication	Identity & Access Management (IAM)
Database	Managed Relational Database
Monitoring	Logging & Monitoring Services

Data flow sequence

1. User Access:
   User visits the portal; requests are routed via global load balancer/CDN.
2. Authentication:
   User credentials verified through centralized identity service (SSO/MFA).
3. Application Processing:
   Authenticated requests are handled by application layer; business logic executed.
4. Database Interaction:
   Transactions and user data are stored in the managed database; read/write operations processed.
5. Monitoring & Alerts:
   System logs and metrics are collected; automated alerts triggered for anomalies.

5. **Task 5 — Decision Justification**

Business Justification

1. Azure enables faster go-to-market for new applications, reducing time-to-value.
2. Supports global expansion with multi-region availability.

Technical Justification

1. Offers managed services for compute, storage, databases, and networking.
2. Centralized identity and access management improve security and compliance.

Scalability Reasoning

1. Auto-scaling ensures applications can handle peak loads efficiently.
2. High-availability zones and global data centers provide resilience.

Cost Reasoning

1. Pay-as-you-go pricing eliminates large upfront capital expenditure.

6. **Task 6 — Risk Awareness**

Risk	**Description**	**Mitigation Strategy**	**Risk**
Cost Overrun	Without monitoring, cloud resources can exceed budget	Implement cost management tools, budgets, and alerts	Cost Overrun
Security Misconfiguration	Misconfigured access or policies may lead to breaches	Apply security best practices, zero-trust policies, and regular audits	Security Misconfiguration
Vendor Lock-In	Relying heavily on Azure-specific services can limit flexibility	Use containers, microservices, and multi-cloud compatible architecture	Vendor Lock-In