PDF 3: Data Security & Compliance

Subjective Case Study Questions and Answers

Q1. Row-Level Security (RLS) Implementation
Scenario: Sales team should access only their region's data in Power BI/Synapse.
Answer: Implement RLS in Synapse using roles and predicates based on region column. Map users to roles via Active Directory groups. Validate using test accounts to ensure data isolation.

Q2. Data Encryption Strategy
Scenario: Sensitive customer data in Azure SQL Database.
Answer: Use Transparent Data Encryption (TDE) for data-at-rest and Always Encrypted for sensitive columns. Enable TLS/SSL for data-in-transit. Combine with key vault for key management.

Q3. Compliance with GDPR
Scenario: Company collects EU customer data.
Answer: Implement data retention policies, purge old records, encrypt personal data, and provide access auditing. Use Azure Purview for cataloging and data classification to ensure regulatory compliance.

Q4. Auditing and Monitoring Access
Scenario: Financial data access must be monitored.
Answer: Enable auditing in Azure SQL Database. Log events to Azure Monitor or Log Analytics. Configure alerts for suspicious access. Regularly review audit logs for compliance.

MCQs

1. Which feature restricts users to specific rows in SQL Database?
   Answer: B. Row-Level Security — filter data per user.
2. Encryption for sensitive columns?
   Answer: C. Always Encrypted — protects columns without changing apps.
3. Data-at-rest encryption in SQL Database?
   Answer: A. Transparent Data Encryption — encrypts storage files.
4. Compliance solution for data cataloging?
   Answer: B. Azure Purview — classification and lineage.
5. Recommended for monitoring access to sensitive data?
   Answer: A. SQL Auditing + Log Analytics.
6. Access control via Active Directory groups?
   Answer: B. Role-based access control (RBAC) — manage Synapse or SQL roles.
7. TLS/SSL ensures:
   Answer: B. Data-in-transit encryption — secure communication.
8. GDPR compliance requires:
   Answer: D. Data retention + auditing + encryption — personal data protection.