Experian Cloud Architecture Principles These principles define the required controls and guidelines for cloud workloads deployed across AWS, Azure, and GCP environments. 1. Identity-Driven Access All access must flow through centralized IAM systems with least privilege, MFA, role-based access controls, and automated provisioning. 2. Network Security Cloud workloads must use private subnets, security groups, firewall policies, service endpoints, and zero-trust networking principles. 3. Resource Standardization Cloud resources must align with approved blueprints, naming conventions, tagging requirements, and cost enforcement policies. 4. DR & Backup Requirements Workloads must include backup schedules, cross-region replication where required, and tested DR failover plans. 5. Monitoring & Alerting Cloud workloads must implement cloud-native observability tools with mandatory metrics, traceability, anomaly detection, and alert routing. 6. Approved Cloud Patterns Event-driven microservices Containerized workloads (AKS/EKS/GKE) Serverless functions Managed data services 7. Cost Accountability Teams must track cloud spend using mandatory cost dashboards, budgets, and forecast-based alerts.