**Cloud Architecture Blueprint: Telco Hybrid Cloud Migration**

**1. Overview**

The target architecture adopts a **Hybrid Cloud Model** to balance control, compliance, and scalability. Mission-critical and compliance-sensitive systems (e.g., OSS/BSS core, subscriber data) are hosted in a **Private Cloud**, while customer-facing apps (e.g., CRM portals, M-PESA integration APIs) leverage **Public Cloud** for agility, elasticity, and faster deployment.

**2. Architecture Layers**

| **Layer** | **Description** |
| --- | --- |
| **User Interface (UI)** | Access via CRM web portals, mobile apps (for customers, support agents, and vendors) |
| **Application Layer** | OSS/BSS, CRM, Network Managers, Monitoring tools |
| **Integration/API Layer** | REST APIs, M-PESA API, middleware for legacy interconnect, service bus (e.g., Apache Kafka, MuleSoft) |
| **Data Layer** | Central Data Lake on private cloud, operational databases (RDS on AWS, Azure SQL, or Oracle) |
| **Infrastructure Layer** | Compute, network, storage distributed across private cloud DC and public cloud provider |

**3. Hybrid Deployment Design**

* **Private Cloud (On-Premises or VPC):**
  + OSS Core (Provisioning, Fault Mgmt, Mediation)
  + BSS Core (Billing, Charging, Product Catalog)
  + Subscriber Databases (HLR/HSS equivalent)
  + Data Governance Tools (DLP, Backup, Metadata Catalog)
* **Public Cloud (e.g., AWS, Azure):**
  + CRM System (SaaS or Containerized)
  + Customer Portals & Self-Service Apps
  + API Gateways for M-PESA Integration
  + Analytics, reporting dashboards (Power BI, AWS QuickSight)
* **Connectivity:**
  + VPN or Dedicated MPLS between private cloud and public cloud VPC
  + API Gateway secured with OAuth 2.0, mutual TLS

**4. Technology Stack**

| **Component** | **Tool/Technology** |
| --- | --- |
| Compute | Kubernetes (EKS/AKS), EC2, VMs |
| Storage | Amazon S3, Azure Blob, SAN (on-prem) |
| Databases | PostgreSQL, Oracle, MongoDB |
| IAM & Security | Azure AD, AWS IAM, Vault, SSO, Firewall |
| Monitoring | Prometheus, Grafana, AWS CloudWatch |
| DevOps | Jenkins, GitHub Actions, Docker, Terraform |
| Data Integration | Apache NiFi, AWS Glue |
| CI/CD | GitLab, ArgoCD, CodePipeline |

**5. Security Architecture**

* **Identity & Access Control:** Role-Based Access Control (RBAC) enforced via Azure AD or AWS IAM
* **Data Protection:** Encryption in-transit (TLS 1.2), at-rest (AES-256), tokenization for PII
* **Firewalls:** Network firewalls, WAFs at ingress points
* **Audit Logs:** Centralized in CloudTrail, Azure Monitor, and SIEM

**6. Disaster Recovery & High Availability**

| **Component** | **DR Strategy** |
| --- | --- |
| CRM & Web Apps | Multi-region deployments on public cloud |
| OSS/BSS | Active-Passive cluster in private cloud with weekly snapshot replication |
| Data Backup | Daily cloud backup to cross-region S3 or Azure Storage |

**7. Compliance Integration**

* **GDPR**: Customer data anonymization, consent logging, data export tools
* **ISO 27001**: Controls mapped to access, encryption, operations
* **CAK (Communications Authority of Kenya)**: Data localization enforced for subscriber data

**8. Deployment Diagram (Textual)**

+----------------------------+

| User Devices |

+-------------+--------------+

|

[Secure API Gateway]

|

+-------------------------+-------------------------+

| |

+--------v--------+ +--------v--------+

| Public Cloud | | Private Cloud |

| (AWS/Azure) | | (On-Premise VPC)|

+-----------------+ +------------------+

| CRM SaaS | | OSS, BSS Core |

| Web Portals | | Mediation Layer |

| Customer APIs | | Subscriber DBs |

| Reporting/BI | | DLP, Backup |

+-----------------+ +------------------+

<--- VPN / MPLS Link --->