Cloud Onboarding Workflow

Phase 1: Discovery & Assessment (Week 1-2)

1.1 Initial Stakeholder Engagement

- Conduct stakeholder kickoff meeting with application owners, cloud architects, and security teams
- Define project scope, timeline, and success criteria
- Establish communication protocols and escalation paths

1.2 Application Assessment

- Perform cloud readiness assessment for target applications
- Document current architecture, dependencies, and integrations
- Identify technical debt and modernization opportunities
- Assess security, compliance, and data residency requirements

1.3 Resource Planning

- Determine required cloud resources (compute, storage, networking)
- Estimate costs and create budget allocation
- Identify team members and skill requirements

Phase 2: Planning & Design (Week 3-4)

2.1 Architecture Design

- Collaborate with cloud architects to design target cloud architecture
- Define migration strategy (lift-and-shift, refactor, or rebuild)
- Create network topology and security design
- Plan for disaster recovery and backup strategies

2.2 Project Planning

- Develop detailed project timeline with milestones
- Create risk register and mitigation strategies

- Establish testing and validation criteria
- Define rollback procedures

2.3 Governance Setup

- Implement cloud governance policies and guardrails
- Set up monitoring and alerting frameworks
- Define cost management and optimization strategies

Phase 3: Environment Preparation (Week 5-6)

3.1 Cloud Account Setup

- Provision cloud accounts with proper organizational structure
- Configure identity and access management (IAM)
- Set up billing and cost allocation
- Implement security baseline configurations

3.2 Infrastructure Provisioning

- Deploy core infrastructure components (VPC, subnets, security groups)
- Set up networking and connectivity (VPN, ExpressRoute, etc.)
- Configure monitoring, logging, and observability tools
- Establish CI/CD pipelines for automated deployments

3.3 Security Implementation

- Apply security policies and compliance controls
- Configure encryption at rest and in transit
- Set up vulnerability scanning and security monitoring
- Conduct security validation testing

Phase 4: Migration & Testing (Week 7-10)

4.1 Application Migration

- Execute migration plan with staged approach
- Migrate data with minimal downtime strategies

- Deploy applications to cloud environment
- Configure load balancing and auto-scaling

4.2 Testing & Validation

- Conduct functional testing of migrated applications
- Perform performance and load testing
- Validate security and compliance requirements
- Test disaster recovery and backup procedures

4.3 Integration Testing

- Test API integrations and data flows
- Validate authentication and authorization
- Conduct end-to-end system testing
- Perform user acceptance testing

Phase 5: Go-Live & Optimization (Week 11-12)

5.1 Production Cutover

- Execute go-live plan with coordinated cutover
- Monitor application performance and user experience
- Implement gradual traffic migration (blue-green or canary)
- Provide immediate support and issue resolution

5.2 Post-Migration Activities

- Conduct post-migration review and lessons learned
- Optimize cloud resources and costs
- Update documentation and runbooks
- Train operations team on new environment

5.3 Handover & Closure

- Transfer ownership to operations team
- Provide knowledge transfer sessions

- Complete project documentation
- Conduct project retrospective and close

Key Success Metrics

- **Migration Success Rate**: Percentage of applications successfully migrated
- **Downtime**: Actual vs. planned downtime during migration
- **Performance**: Application response time and throughput post-migration
- **Cost Optimization**: Actual vs. estimated cloud costs
- **Time to Market**: Overall project timeline adherence
- **Security Compliance**: Successful security and compliance validation

Risk Management

High Priority Risks

- Data loss during migration
- Extended downtime beyond planned windows
- Security vulnerabilities in new environment
- Cost overruns due to resource miscalculation

Mitigation Strategies

- Comprehensive backup and rollback procedures
- Staged migration with validation checkpoints
- Security reviews at each phase
- Continuous cost monitoring and optimization

Communication Plan

- **Daily**: Stand-up meetings with core team
- **Weekly**: Stakeholder status updates
- **Bi-weekly**: Steering committee reviews
- **Monthly**: Executive dashboard updates
- **Ad-hoc**: Issue escalation and resolution communications

Tools & Technologies

- **Project Management: JIRA, Azure DevOps, Monday.com**
- **Cloud Platforms: AWS, Azure, GCP**
- **Monitoring: CloudWatch, Azure Monitor, Stackdriver**
- **Security: AWS Security Hub, Azure Security Center**
- **Cost Management: AWS Cost Explorer, Azure Cost Management**
- **Documentation: Confluence, SharePoint**