**Change Control Strategy**

**Project:** Telco Cloud Migration  
**Project Manager:** Barbara Nzisa  
**Version:** 1.0  
**Date:** may 2025

**1. Purpose**

To establish a structured process for evaluating, approving, and managing changes to the cloud migration project scope, timeline, cost, technology stack, or compliance posture—especially critical in regulated telco environments.

**2. Scope of Change Control**

This strategy applies to any change that may affect:

* Project **schedule**, **cost**, or **resources**
* **Infrastructure design** (e.g., moving from Lift-and-Shift to Replatforming)
* **Data migration rules** (e.g., subscriber data)
* **Security policies** (IAM, encryption)
* **Third-party system integration** (CRM, OSS/BSS, M-PESA)
* **Regulatory requirements** (e.g., GDPR, Kenya Data Protection Act)

**3. Change Request Types**

| **Type** | **Example** | **Approval Required From** |
| --- | --- | --- |
| Scope Change | Adding new NEM interface | Project Sponsor, PM |
| Technical Change | Moving from AWS to GCP | Cloud Architect, CTO |
| Cost/Budget | Extending vendor license | Finance, PMO |
| Schedule | Delaying CRM migration | PM, Program Manager |
| Compliance | Adjusting encryption standard | DPO, Compliance Officer |

**4. Change Control Process**

**Step 1: Initiation**

* Requestor submits a **Change Request Form (CRF)** via Jira/ServiceNow
* CR must include: description, justification, impact analysis (time/cost/risk), affected systems

**Step 2: Impact Assessment**

* Performed by technical leads, finance, risk, compliance as needed
* Assessment covers:
  + Budget/time/resource impact
  + Risk to system uptime or subscriber data
  + Compliance implications

**Step 3: Review and Approval**

* **Low Impact** → PM or Tech Lead approval
* **Medium Impact** → PM + Change Advisory Board (CAB)
* **High Impact/Regulatory** → CAB + Executive Sponsor + Compliance

**Step 4: Implementation**

* Assigned to appropriate technical team
* Update project plan, configuration documents, and testing plans
* Inform stakeholders via updated communication channels

**Step 5: Post-Implementation Review**

* Confirm success or rollback if needed
* Document lessons learned
* Close the CR ticket

**5. Change Advisory Board (CAB)**

| **Role** | **Responsibility** |
| --- | --- |
| Project Manager | Facilitate review |
| Technical Lead | Evaluate system impact |
| Compliance Officer | Review data/privacy implications |
| Security Lead | Assess IAM/encryption effects |
| Vendor PM (if external) | Provide input on scope/cost impact |

Meetings: Weekly, with ad hoc sessions for urgent changes.

**6. Change Priority and Risk Rating**

| **Priority** | **Risk Level** | **Response Time** |
| --- | --- | --- |
| Critical (Affects Live Services) | High | Immediate |
| Major (Affects Schedule/Budget) | Medium | 1–2 business days |
| Minor (Internal or Non-critical) | Low | Within 3 business days |

**7. Documentation & Tracking Tools**

| **Item** | **Tool** |
| --- | --- |
| Change Request Form | Jira, ServiceNow |
| Change Log | Confluence, Excel |
| Approval Records | Shared Drive, Signed PDF |
| Version Control | Git/GitHub for scripts & IaC |

**8. Success Metrics for Change Control**

| **Metric** | **Target** |
| --- | --- |
| Approved changes implemented on time | ≥ 95% |
| Unauthorized changes detected | 0 |
| Mean time to assess/approve changes | ≤ 48 hours |
| Post-change incidents or rollbacks | < 5% of changes |

**9. Version Control**

| **Version** | **Date** | **Description** | **Author** |
| --- | --- | --- | --- |
| 1.0 | [Insert Date] | Initial Version | [Your Name] |