# CONFIGURATION MANAGEMENT PLAN

National Currency Printing and Secure Banknote Production Facility Project (NCPBF)

**Project Title:**

National Currency Printing and Secure Banknote Production Facility Project (NCPBF)

**Project Sponsor:**

Central Bank

*Prepared by: PMIC of Lazuli Pamir Consulting – for learning purpose only*

# Table of Contents

## 1. Purpose:

The purpose of this Configuration Management Plan (CMP) is to establish a formal, structured, and rigorously controlled framework for identifying, defining, baselining, controlling, tracking, auditing, and reporting all Configuration Items (CIs) throughout the entire lifecycle of the National Currency Printing and Secure Banknote Production Facility (NCPBF) Project.

The NCPBF project represents a strategic national infrastructure initiative involving highly sensitive security systems, complex technical integrations, regulatory oversight, and multi-phase delivery across design, construction, installation, commissioning, and operational transition. As such, uncontrolled modifications, undocumented changes, inconsistent versions, or misaligned design artifacts could result in significant risks — including schedule delays, cost overruns, quality defects, regulatory non-compliance, or security vulnerabilities.

This Configuration Management Plan ensures that every approved project element—whether documentation, technical design, security architecture, system configuration, physical infrastructure specification, or operational procedure—is:

- Clearly identified and uniquely coded
- Formally approved and baselined
- Protected against unauthorized modification
- Version-controlled and traceable
- Linked to approved requirements and design decisions
- Auditable and compliant with governance standards

Given the project's:

- High security sensitivity involving vault systems, access control architecture, cybersecurity infrastructure, and restricted facility layouts
- Multi-phase execution spanning authorization, planning, secure design, construction, systems integration, testing, commissioning, and operational readiness
- Complex technical integration between mechanical, electrical, IT, cybersecurity, and printing systems
- Long project lifecycle with evolving regulatory, technical, and operational requirements

- Strict regulatory and audit exposure under Central Bank governance

Configuration management functions as the structural integrity mechanism that protects project coherence and institutional accountability.

Through disciplined configuration control, the project ensures:

- Preservation of approved scope, schedule, cost, and design baselines
- Prevention of unauthorized, informal, or undocumented changes
- Full traceability from business requirements to technical design to constructed facility to operational systems
- Alignment between architectural design, engineering drawings, security zoning, machinery specifications, and installed systems
- Accurate synchronization between documentation and physical implementation
- Compliance with regulatory, security, and audit requirements
- Controlled transition from project delivery into stable operations

In a project of this magnitude and sensitivity, configuration management is not merely document version control—it is a governance safeguard that ensures that what is designed is what is built, what is built is what is tested, and what is tested is what becomes operational.

Without disciplined configuration management, the project would be exposed to:

- Scope creep disguised as minor adjustments
- Version confusion across technical drawings
- Inconsistent system configurations
- Security control gaps
- Rework due to misalignment between documentation and execution
- Audit findings and regulatory non-compliance

Therefore, this Configuration Management Plan establishes configuration control as a mandatory governance function integrated with:

- Scope Management
- Change Management
- Requirements Management
- Risk Management
- Quality Assurance

- Security Governance
- Stage-Gate Oversight

Ultimately, the CMP ensures that the NCPBF project maintains structural integrity, security assurance, institutional transparency, and traceable decision-making from initiation through operational handover and beyond.

## 2. Configuration Management Objectives:

The Configuration Management Plan (CMP) establishes clear and disciplined objectives to ensure structural integrity, security protection, and governance alignment throughout the NCPBF project lifecycle. The CMP aims to:

**A. Clearly Define and Classify Configuration Items (CIs)**

To formally identify, categorize, and uniquely code all configuration items—including documents, design packages, system specifications, baselines, technical drawings, security configurations, and operational artifacts—so that each item is traceable, controlled, and unambiguously referenced throughout the project.

This prevents confusion, duplication, and uncontrolled artifacts across multiple phases and workstreams.

**B. Establish and Protect Configuration Baselines**

To formally approve and freeze key baselines—including scope, schedule, cost, design, security architecture, and operational documentation—at defined stage gates.

Baselines serve as authoritative reference points against which all future performance, changes, and deviations are measured. Protecting baselines ensures stability in a long-duration, multi-phase project.

**C. Ensure All Changes Follow Formal Governance and Change Control**

To guarantee that no configuration item is modified without a documented, impact-analyzed, and formally approved Change Request processed through the Change Control Board (CCB) and, where required, escalated to the Steering Committee.

This objective safeguards the project from unauthorized adjustments, informal decisions, and undocumented deviations that could compromise security, compliance, or budget integrity.

**D. Maintain Robust Version Control and End-to-End Traceability**

To implement disciplined version numbering, status tracking, and historical archiving for every configuration item.

Traceability will be maintained:

- From business case objectives to requirements
- From requirements to design
- From design to construction
- From construction to testing
- From testing to operational acceptance

This ensures complete visibility and accountability across the project lifecycle.

**E. Support Independent Audits and Regulatory Compliance Verification**

To enable structured configuration audits (Functional and Physical Configuration Audits) that verify:

- Deliverables meet approved requirements
- Physical systems match approved design documents
- Security controls are implemented as approved
- Documentation reflects actual system configuration

This objective ensures readiness for internal PMO reviews, Central Bank audits, and external regulatory scrutiny.

**F. Protect Security-Sensitive Design and System Artifacts**

To enforce strict control over highly sensitive configuration items, including:

- Vault design layouts
- Security zoning maps
- Access control configurations
- Cybersecurity architecture
- Encryption parameters
- Restricted facility blueprints

Security-classified CIs will be protected through role-based access control, encryption, controlled repositories, and segregation-of-duties enforcement.

**G. Ensure Alignment Between Design, Construction, Systems Integration, and Documentation**

To maintain continuous synchronization between approved design packages and actual field implementation.

This objective prevents:

- Design-to-build misalignment
- Documentation lag behind implementation
- Inconsistent system configurations
- Rework caused by outdated drawings

**H. Enable Accurate Status Accounting and Executive Oversight**

To provide accurate reporting on:

- Number of baselined configuration items
- Items under change
- Open change requests
- Audit findings
- Configuration-related risks

This allows executive leadership and the PMO to monitor configuration health as a governance performance indicator.

**I. Reduce Rework, Cost Escalation, and Schedule Disruption**

By controlling configuration integrity, the CMP aims to minimize:

- Late discovery of inconsistencies
- Unauthorized field modifications
- Design rework
- Installation errors
- Commissioning delays

This directly contributes to schedule performance and cost discipline.

**J. Ensure Smooth Transition to Operations and Long-Term Sustainability**

To guarantee that all approved and validated configuration items—design documents, system settings, operational procedures, and security controls—are fully documented, verified, and transferred to operations at project handover.

This ensures that the operational facility reflects the approved configuration and can be maintained sustainably beyond project closure.

## 3. Configuration Management Principles:

The Configuration Management Principles governing the National Currency Printing and Secure Banknote Production Facility (NCPBF) Project are established to ensure governance discipline, structural integrity, security protection, and institutional accountability throughout the entire project lifecycle.

All approved configuration items (CIs) shall be maintained within a centralized and controlled repository serving as the single source of truth, and no document, design package, technical specification, system configuration, or operational artifact shall be considered valid unless formally approved and stored within this authorized environment.

Baselines—including scope, schedule, cost, design, security architecture, and operational documentation—shall be formally approved at defined stage gates and treated as protected governance commitments, with any modification requiring a documented, impact-assessed, and formally approved Change Request processed through the established Change Control Board (CCB) and escalated when necessary according to governance thresholds.

Version control is mandatory for all configuration items, with disciplined numbering, documented change histories, and full traceability maintained from strategic objectives through requirements, design, construction, systems integration, testing, and operational handover.

Configuration status must remain transparent, measurable, and auditable at all times, enabling executive oversight, PMO assurance, and regulatory verification through structured status accounting and configuration audits.

Security classification shall be applied to all sensitive configuration items—including vault layouts, access control systems, cybersecurity architecture, restricted facility designs, and encryption parameters—with role-based access control, encryption, audit trails, and backup mechanisms enforced to protect against unauthorized access or modification.

Segregation of duties shall be strictly maintained so that the initiation, approval, and implementation of configuration changes are performed by independent authorized roles, thereby preserving governance integrity and preventing conflicts of interest.

Through these principles, configuration management ensures that what is approved is what is built, what is built is what is tested, and what is tested is what becomes operational, safeguarding the project against uncontrolled scope drift, version confusion, technical misalignment, documentation inconsistency, regulatory non-compliance, and security exposure, and ultimately preserving the structural, technical, and institutional integrity of this high-security national infrastructure initiative.

## 4. Configuration Items (CIs):

Configuration Items (CIs) are any project elements—physical, technical, documentary, digital, or operational—that require formal identification, version control, baseline protection, and change governance to ensure the integrity, traceability, and security of the NCPBF project throughout its lifecycle.

In the context of the National Currency Printing and Secure Banknote Production Facility (NCPBF) Project, configuration items span strategic documentation, engineering artifacts, technical systems, security architecture, regulatory requirements, and operational deliverables. Each CI must be uniquely identified, formally approved, traceable to requirements, and protected from unauthorized modification.

The following categories define the structured classification of Configuration Items within the project:

### 4.1 Strategic and Governance-Level Configuration Items

These configuration items establish the formal authority, direction, and control structure of the project and represent high-level governance commitments.

- Project Charter
- Business Case
- Approved Project Management Plan (Integrated Plan)
- Approved Scope, Schedule, and Cost Baselines
- Governance Framework documentation
- Stage-Gate approval records

These items define the strategic intent, approved commitments, and control boundaries of the project and therefore require strict baseline protection.

### 4.2 Scope and Technical Configuration Items

These configuration items define the physical, architectural, engineering, and systems design of the facility and are critical to ensuring that what is constructed and implemented matches approved specifications.

- Scope Statement
- Work Breakdown Structure (WBS)
- WBS Dictionary

- Architectural and Engineering Design Packages
- Secure Facility Layout Drawings
- Security Zoning and Restricted Area Design
- Vault Engineering Specifications
- Printing Machinery Technical Specifications
- Systems Integration Design Documentation
- IT Infrastructure Architecture
- Cybersecurity Architecture
- Access Control System Design
- Surveillance and Monitoring System Designs

These items form the Design Baseline and are subject to strict version control and audit verification prior to construction and installation.

### 4.3 Requirements and Compliance Configuration Items

These configuration items ensure traceability between strategic objectives, stakeholder expectations, regulatory mandates, and technical implementation.

- Requirements Register
- Requirements Traceability Matrix (RTM)
- Regulatory and Compliance Requirement Documentation
- Security Standard Compliance Specifications
- Quality and Performance Acceptance Criteria

These CIs ensure that every approved requirement is traceable to design, construction, testing, and final operational validation.

### 4.4 Security-Sensitive Configuration Items

Due to the national-security sensitivity of the project, certain configuration items are classified as restricted and subject to enhanced control measures.

- Restricted Facility Layouts
- Vault Configuration Drawings
- Security Zoning Schematics
- Cybersecurity System Configurations
- Firewall and Network Segmentation Configurations
- Encryption Algorithms and Parameters
- Access Control Credentials Architecture

- Physical Security Redundancy Design

These CIs require enhanced access control, encryption, audit logging, and segregation-of-duties enforcement to prevent unauthorized disclosure or modification.

### 4.5 Operational and Commissioning Configuration Items

These configuration items govern the transition from project delivery to stable operations and ensure long-term sustainability.

- Standard Operating Procedures (SOPs)
- Commissioning Plans and Records
- Testing and Validation Protocols
- Factory Acceptance Test (FAT) Reports
- Site Acceptance Test (SAT) Reports
- Operational Readiness Documentation
- Training Manuals
- Acceptance Certificates
- As-Built Documentation

These items collectively form the Operational Baseline and must reflect the final approved configuration of the constructed and integrated facility.

## 5. Configuration Identification:

Configuration Identification establishes the formal method by which all Configuration Items (CIs) within the NCPBF project are uniquely defined, categorized, coded, classified, and tracked throughout their lifecycle. The purpose of configuration identification is to eliminate ambiguity, ensure traceability, prevent duplication, and enable disciplined configuration control across governance, technical, security, and operational domains.

Every Configuration Item must be formally registered in the Configuration Register before it can be reviewed, approved, or baselined. No document, drawing, system configuration, or operational artifact shall be considered a controlled CI unless it has been assigned a unique CI identification code and recorded in the authorized repository.

### 5.1 Mandatory Configuration Identification Attributes

Each Configuration Item shall include, at a minimum, the following attributes:

- **CI ID** – A unique identifier following the approved CI coding structure.
- **CI Name** – Clear and descriptive title of the configuration item.
- **Category** – Classification (e.g., Strategic, Scope, Design, Security, Operational, Requirements).
- **Owner** – Accountable individual or function responsible for the CI's integrity.
- **Version Number** – Current version in accordance with version control standards.
- **Status** – Lifecycle state (Draft / Under Review / Approved / Baselined / Archived).
- **Security Classification** – Public / Internal / Confidential / Restricted / Highly Restricted.
- **Repository Location** – Controlled storage path within the authorized configuration system.
- **Related Requirement ID(s)** – Traceability link to approved requirements.
- **Related Risk ID(s)** – Link to associated risks in the Risk Register (if applicable).

- **Baseline Reference (if applicable)** – Identification of the baseline to which the CI belongs.
- **Change Request Reference (if applicable)** – Link to approved CR authorizing the version.

This structured identification ensures complete traceability from strategic intent to technical execution and operational delivery.

### 5.2 CI Coding Structure

Configuration Item identification codes shall follow a standardized alphanumeric structure to reflect category and sequencing.

**Format:**
CI-[Category Code]-[Sequential Number]

Where:

- **CI** = Configuration Item
- **Category Code** = Functional classification
- **Sequential Number** = Unique numeric sequence

**Approved Category Codes**

- **SC** – Scope
- **DG** – Design
- **REQ** – Requirements
- **SEC** – Security
- **IT** – IT & Cybersecurity
- **OPS** – Operational
- **GOV** – Governance
- **SCH** – Schedule
- **CST** – Cost
- **QAL** – Quality

**Example CI Identification Codes**

- CI-SC-001 → Scope Statement
- CI-DG-015 → Secure Facility Architectural Design Package
- CI-REQ-004 → Regulatory Compliance Requirement Document
- CI-SEC-007 → Vault Security Configuration

- CI-IT-010 → Network Segmentation Architecture
- CI-OPS-003 → Commissioning Protocol
- CI-GOV-002 → Approved Project Charter

This structured approach allows quick identification of CI type, domain, and sequencing.

### 5.3 CI Lifecycle Status Definitions

Each Configuration Item shall move through controlled lifecycle states:

- **Draft** – Under development, not approved.
- **Under Review** – Submitted for formal approval.
- **Approved** – Formally accepted but not yet baselined.
- **Baselined** – Official reference configuration.
- **Superseded** – Replaced by a new approved version.
- **Archived** – Retained for audit history, no longer active.

Status transitions must be documented and traceable.

### 5.4 Traceability and Cross-Referencing

Configuration identification shall ensure integration with:

- Requirements Traceability Matrix (RTM)
- Risk Register
- Change Register
- Scope Baseline
- Design Baseline
- Operational Baseline

No CI shall exist in isolation. Each must be traceable to at least one strategic, requirement, or technical driver.

### 5.5 Governance Control

The Configuration Manager or PMO Governance Lead shall maintain the Configuration Register and ensure:

- No duplicate CI IDs exist.
- All required fields are completed.
- Security classification is applied.

- Version control discipline is maintained.
- Audit trails are preserved.

Any CI found without formal identification shall be considered uncontrolled and must be regularized before further use.

---

## 6. Configuration Baselines:

Configuration baselines represent formally approved and protected reference points that define the authorized state of the project at specific stages of its lifecycle. Once established, baselines serve as the official benchmark against which performance, compliance, changes, and deviations are measured.

In the National Currency Printing and Secure Banknote Production Facility (NCPBF) Project, baselines are not merely documentation milestones—they represent governance commitments endorsed by authorized decision-making bodies, including the Project Sponsor, Change Control Board (CCB), PMO, and Steering Committee where applicable.

Baselines provide structural stability across a long-duration, multi-phase project involving secure design, construction, systems integration, testing, commissioning, and transition to operations.

### 6.1 Scope Baseline

The Scope Baseline defines the total authorized project work and forms the foundation for schedule development, cost estimation, resource planning, and performance measurement.

The Scope Baseline consists of:

- Approved Scope Statement
- Approved Work Breakdown Structure (WBS)
- Approved WBS Dictionary

Together, these documents establish:

- In-scope and out-of-scope boundaries
- Deliverable definitions
- Work package descriptions
- Acceptance criteria
- Control account structure

Once approved, the Scope Baseline serves as the definitive reference for scope validation and scope control. Any modification to scope elements requires formal change control and baseline revision approval.

### 6.2 Schedule Baseline

The Schedule Baseline defines the approved project timeline and sequencing of authorized work.

The Schedule Baseline consists of:

- Approved Master Integrated Schedule
- Approved Milestone Plan
- Approved Stage-Gate Dates

The Schedule Baseline:

- Establishes authorized start and finish dates
- Defines critical path activities
- Supports performance measurement (SPI, SV)
- Enables stage-gate readiness reviews

Schedule deviations are measured against this baseline, and modifications may only occur through formally approved change requests.

### 6.3 Cost Baseline

The Cost Baseline represents the approved time-phased budget against which cost performance is measured.

The Cost Baseline consists of:

- Approved Budget Breakdown Structure
- Time-phased funding allocation
- Management reserve and contingency structure

The Cost Baseline enables:

- Cost performance tracking (CPI, CV)
- Earned Value Management (EVM) integration
- Financial governance and funding control

Unauthorized financial reallocation outside approved thresholds is strictly prohibited.

### 6.4 Design Baseline

The Design Baseline establishes the formally approved technical and engineering configuration of the facility and its integrated systems.

The Design Baseline includes:

- Approved architectural and engineering design packages
- Approved security zoning design
- Vault and restricted-area specifications
- Machinery technical specifications
- IT and cybersecurity architecture documentation
- Security compliance approvals

The Design Baseline ensures that what is constructed, installed, and configured matches the authorized design. Physical Configuration Audits (PCA) verify conformance to this baseline prior to commissioning.

**6.5 Operational Baseline**

The Operational Baseline represents the validated and accepted state of the facility prior to transition into steady-state operations.

The Operational Baseline includes:

- Commissioned and fully validated facility
- Completed testing and acceptance documentation
- Approved Standard Operating Procedures (SOPs)
- Operational readiness certification
- As-built documentation
- Final security validation approvals

The Operational Baseline ensures that the delivered system reflects approved design, tested performance, and verified security integrity before formal handover to operational authority.

**Baseline Protection and Change Control**

All baselines established under this Configuration Management Plan are considered protected governance artifacts.

Baselines may only be:

- Modified through a formally submitted Change Request

- Subjected to documented impact analysis (scope, schedule, cost, risk, security)
- Reviewed by the Change Control Board
- Escalated to the Steering Committee when required
- Re-baselined through formal approval

No baseline shall be informally adjusted, partially modified, or retroactively corrected without proper authorization.

**Baseline Integrity Assurance**

Baseline integrity will be safeguarded through:

- Version-controlled documentation
- Centralized repository control
- Configuration audits
- Stage-gate verification
- Executive reporting

Any deviation discovered between approved baselines and actual implementation shall trigger corrective action and governance escalation.

---

## 7. Configuration Change Control Process:

All modifications to approved Configuration Items (CIs) within the NCPBF project must follow a formally structured, traceable, and governance-controlled change process. No configuration item—whether strategic document, design package, system configuration, or operational artifact—may be altered without completing the approved Configuration Change Control procedure.

This process ensures that changes are evaluated holistically across scope, schedule, cost, risk, security, and regulatory dimensions before authorization.

### 7.1 Change Request Submission

Any proposed modification to a Configuration Item must begin with a formally documented Change Request (CR). The request must clearly define:

- The Configuration Item(s) affected
- Description of the proposed change
- Justification and business rationale
- Urgency level
- Initiating stakeholder
- Reference to related requirement or issue

Verbal requests, informal approvals, or undocumented field changes are strictly prohibited.

### 7.2 Impact Analysis

Upon submission, a structured impact analysis must be conducted covering:

- Scope impact
- Schedule impact
- Cost impact
- Resource impact
- Risk impact
- Quality impact
- Regulatory impact
- Security impact

The analysis must identify whether the change affects any established baseline and whether re-baselining is required.

### 7.3 Risk Review

The Risk Manager shall assess:

- Introduction of new risks
- Change to probability or impact of existing risks
- Impact on contingency reserves
- Interaction with security or compliance risks

All risk implications must be documented and linked to the Risk Register.

### 7.4 Security Impact Review (If Applicable)

For changes affecting:

- Vault specifications
- Restricted facility layouts
- Cybersecurity architecture
- Encryption configurations
- Access control systems

A formal Security Impact Review must be conducted by the Security Board or designated authority.

No security-sensitive configuration change may proceed without explicit security clearance.

### 7.5 Change Control Board (CCB) Decision

The Change Control Board (CCB) shall review:

- Impact analysis results
- Risk assessment
- Security review findings
- Alignment with strategic objectives

The CCB may:

- Approve the change
- Reject the change
- Request additional analysis
- Defer the decision

All decisions must be formally documented.

### 7.6 Steering Committee Escalation (If Threshold Exceeded)

Changes exceeding predefined governance thresholds (e.g., budget deviation, milestone shift, scope expansion, regulatory implications) must be escalated to the Steering Committee for executive approval.

Threshold criteria are defined in the Governance Framework.

### 7.7 Update Configuration Item Version

Upon approval:

- A new CI version shall be created following version control standards
- The new version shall reference the approved Change Request ID
- Baseline designation shall be updated if required

Direct editing of baselined documents is strictly prohibited.

### 7.8 Update Configuration Register

The Configuration Register must be updated to reflect:

- New version number
- Change description
- Approval authority
- Effective date
- Related CR reference

Status accounting must reflect the updated configuration state.

### 7.9 Communicate Approved Change

Approved changes must be formally communicated to:

- Affected workstreams
- PMO
- Security teams (if applicable)
- Quality and audit teams
- Operational readiness stakeholders

Communication must include updated documentation references and implementation instructions.

### 7.10 Archive Previous Version

Superseded configuration items must be:

- Archived in the controlled repository
- Retained for audit purposes
- Protected against deletion
- Clearly marked as superseded

Historical traceability must be preserved at all times.

### Prohibition of Unauthorized Editing

Under no circumstances shall baselined documents, drawings, system configurations, or security artifacts be directly edited, overwritten, or replaced without completing the formal change control process.

Unauthorized modification constitutes a governance breach and shall be escalated according to project compliance protocols.

## 8. Version Control Rules:

Version control establishes the formal mechanism for tracking the evolution of all Configuration Items (CIs) throughout the lifecycle of the NCPBF project. It ensures that every approved document, design package, technical specification, system configuration, and operational artifact is uniquely identifiable, traceable to its authorization, and protected from unauthorized or undocumented modification.

Version control within the NCPBF project is mandatory for all configuration items, without exception.

### 8.1 Version Numbering Structure

All Configuration Items shall follow a standardized version numbering convention to clearly distinguish draft states, baseline approvals, minor revisions, and major changes.

**Draft Versions**

- v0.1, v0.2, v0.3, etc.
  Used for working drafts prior to formal approval.
  Draft versions are not considered authoritative and may not be used for execution, procurement, construction, or operational activities.

**Initial Approved Baseline**

- v1.0
  Represents the first formally approved and baselined version of the Configuration Item.
  Once approved as v1.0, the document becomes a controlled baseline artifact.

**Minor Approved Updates**

- v1.1, v1.2, v1.3, etc.
  Used when approved changes do not materially alter scope, architecture, compliance status, or governance commitments.

Minor changes may include:

- Clarifications
- Non-structural refinements

- Minor technical adjustments
- Corrective documentation updates

All minor updates must still pass formal change control and reference an approved Change Request.

**Major Approved Changes**

- v2.0, v3.0, etc.
  Used when changes materially impact:
- Scope
- Design architecture
- Security configuration
- Regulatory compliance
- Cost baseline
- Schedule baseline
- Operational procedures

Major version changes require formal re-baselining approval and may trigger stage-gate review.

**8.2 Mandatory Version Metadata**

Every Configuration Item version must include complete version control metadata to ensure traceability and audit readiness.

Each version shall clearly document:

- Date of version release
- Change description (summary of modifications)
- Author or originating role
- Approval authority (CCB / Sponsor / Steering Committee)
- Change Request (CR) ID reference
- Baseline designation (if applicable)
- Security classification

This information must appear either:

- In a formal document control table
- In a version history section
- Or within the configuration repository metadata fields

No version may exist without complete traceability documentation.

### 8.3 Baseline Protection Rules

Once a Configuration Item has reached baseline status (v1.0 or higher):

- Direct editing is strictly prohibited.
- A new version must be created for any approved change.
- The previous version must be archived but retained.
- The baseline register must be updated accordingly.

Overwriting baselined documents is not permitted under any circumstance.

### 8.4 Repository and Audit Integrity

The configuration repository must:

- Maintain full version history
- Preserve superseded versions
- Record user access and modification logs
- Prevent deletion of baselined items
- Protect restricted versions through access control

Version history must remain auditable for the full project lifecycle and any post-project regulatory review period.

### 8.5 Security-Sensitive Version Control

For security-classified Configuration Items (e.g., vault drawings, encryption parameters, cybersecurity architecture):

- Version increments must trigger security review validation
- Access to draft and approved versions must be role-restricted
- Archived versions must remain encrypted
- Security-related version changes must reference formal security clearance documentation

### 8.6 Version Control Objectives

Version control within the NCPBF project ensures:

- Elimination of version confusion
- Prevention of unauthorized edits

- Traceability of all changes
- Protection of governance commitments
- Alignment between documentation and physical implementation
- Audit readiness at all lifecycle stages

## 9. Configuration Status Accounting:

Configuration Status Accounting (CSA) establishes the formal mechanism for recording, tracking, analyzing, and reporting the current state of all Configuration Items (CIs) throughout the lifecycle of the NCPBF project. It provides continuous visibility into the health, integrity, and governance compliance of the project's configuration baseline.

In a high-security, multi-phase national infrastructure project such as the NCPBF, configuration status accounting serves as a critical oversight tool enabling executive leadership, the PMO, and governance bodies to monitor configuration stability and detect emerging risks early.

### 9.1 Purpose of Configuration Status Accounting

The purpose of CSA is to:

- Maintain real-time visibility of configuration integrity
- Track baseline stability and change volume
- Detect unauthorized modifications
- Support stage-gate readiness reviews
- Enable audit and regulatory compliance verification
- Provide early warning signals of configuration instability

Configuration status accounting ensures that configuration management remains measurable and not merely procedural.

### 9.2 Configuration Status Reporting Metrics

Configuration status reporting shall include, at a minimum, the following indicators:

- **Total number of registered Configuration Items (CIs)**
- **Number of Baselined CIs**
- **Number of Draft or Under-Review CIs**
- **Number of CIs currently under approved change**
- **Number of Open Change Requests affecting CIs**
- **Number of Rejected Change Requests**
- **Number of Major vs Minor version updates**
- **Number of Security-sensitive CIs under change**

- **Unauthorized modification incidents (if any)**
- **Configuration audit findings (open and closed)**

These metrics allow governance bodies to assess configuration stability trends over time.

### 9.3 Status Categories

Each Configuration Item shall be categorized within one of the following states for reporting purposes:

- Draft
- Under Review
- Approved
- Baselined
- Under Change
- Superseded
- Archived

This structured categorization supports lifecycle transparency and prevents ambiguity regarding CI status.

### 9.4 Reporting Frequency and Governance Escalation

Configuration status reports shall be formally submitted according to the following governance cadence:

**Monthly Reporting – PMO**

A detailed Configuration Status Report shall be submitted monthly to the PMO, including:

- CI status summary
- Change activity summary
- Trend analysis
- Audit findings
- Configuration-related risks

This supports operational oversight and control monitoring.

**Quarterly Reporting – Steering Committee**

A summarized executive Configuration Health Report shall be presented quarterly to the Steering Committee, highlighting:

- Baseline stability
- Major configuration changes
- Security-sensitive configuration changes
- Significant deviations
- Configuration-related risks or incidents

This ensures executive-level awareness and governance accountability.

**Immediate Reporting – Security or Governance Breach**

In the event of:

- Unauthorized modification
- Repository breach
- Security-sensitive CI exposure
- Direct editing of baselined artifacts
- Configuration mismatch discovered during audit

Immediate escalation must occur to:

- Project Sponsor
- PMO Governance Lead
- Security Board
- Steering Committee (if severity warrants)

Incident reporting shall include corrective action plans and containment measures.

### 9.5 Configuration Trend Monitoring

In addition to periodic reporting, the project shall monitor:

- Rate of change volume
- Rework due to configuration mismatch
- Frequency of baseline revisions
- Security-impacting configuration changes

Unusual increases in change activity may indicate:

- Scope instability
- Poor requirements definition
- Design maturity issues
- Governance breakdown

Such trends must be escalated and investigated.

### 9.6 Integration with Other Governance Controls

Configuration Status Accounting integrates with:

- Change Management reporting
- Risk Register updates
- Quality Assurance findings
- Security monitoring controls
- Stage-gate readiness reviews

Configuration metrics may serve as indicators of overall project governance maturity.

---

## 10. Configuration Audits:

Configuration Audits are formal, structured verification activities conducted to ensure that Configuration Items (CIs) comply with approved requirements, baselines, and technical specifications. In the NCPBF project, configuration audits serve as a governance assurance mechanism that validates alignment between approved documentation and actual implementation.

Given the project's complexity, security sensitivity, and regulatory exposure, configuration audits are mandatory and cannot be waived.

### 10.1 Functional Configuration Audit (FCA)

The Functional Configuration Audit verifies that project deliverables meet all approved functional and performance requirements as defined in:

- The Requirements Register
- Requirements Traceability Matrix (RTM)
- Approved Design Specifications
- Regulatory Compliance Requirements
- Security Standards

The FCA confirms that:

- All requirements have been implemented
- Acceptance criteria have been satisfied
- Functional testing results meet defined thresholds
- Security requirements are validated
- No requirement has been omitted or improperly implemented

The FCA is conducted prior to commissioning approval and operational transition. Any discrepancy must be documented, corrected, and re-validated before proceeding.

### 10.2 Physical Configuration Audit (PCA)

The Physical Configuration Audit verifies that the physical systems, installations, and configurations match the approved Design Baseline and technical documentation.

The PCA confirms that:

- Constructed facility elements match approved architectural and engineering drawings
- Vault construction matches approved specifications
- Security zoning aligns with authorized layouts
- Installed machinery matches approved technical specifications
- IT and cybersecurity systems reflect approved architecture
- Access control and surveillance systems are configured as documented

The PCA ensures that what has been physically built and installed is fully aligned with the authorized configuration.

**10.3 Mandatory Audit Milestones**

Configuration Audits shall be conducted at the following critical control points:

- Design Freeze
- Construction Completion
- Machinery Installation Completion
- Systems Integration Completion
- Commissioning Phase
- Pre-Operational Handover

No phase transition or stage-gate approval shall proceed without successful completion of required configuration audits.

**10.4 Audit Independence and Governance**

Configuration audits shall be conducted by:

- PMO Assurance Team
- Designated Configuration Manager
- Security Board (for security-sensitive CIs)
- Independent Quality or Compliance Review (where required)

Audit findings shall be formally documented, categorized by severity, and tracked to closure.

## 11. Tools and Repository:

The NCPBF project shall utilize a centralized, controlled Configuration Repository to manage all Configuration Items (CIs). This repository serves as the single source of truth for approved documentation, baselines, and configuration records.

Under no circumstances shall configuration items be stored, transmitted, or maintained outside authorized systems.

### 11.1 Repository Requirements

The configuration repository must include:

- Role-based access control (RBAC)
- Segregation of duties enforcement
- Full audit trail logging
- Version history preservation
- Automated backup and redundancy
- Encrypted storage for classified or restricted items
- Controlled archival functionality
- Change tracking capabilities

Access to security-sensitive CIs shall be limited to authorized personnel under the principle of least privilege.

### 11.2 Prohibited Practices

The following practices are strictly prohibited:

- Storing CIs in personal email accounts
- Maintaining CIs on personal drives or unauthorized cloud platforms
- Sharing restricted configuration items via unsecured communication channels
- Direct editing of baselined documents without version control
- Deleting superseded versions

Violation of repository controls shall be treated as a governance and security breach and escalated accordingly.

### 11.3 Security Controls for Sensitive CIs

For restricted or highly restricted configuration items (e.g., vault layouts, encryption parameters, cybersecurity configurations), additional controls shall apply:

- Encrypted storage
- Multi-factor authentication
- Access logging and monitoring
- Security clearance validation
- Dual authorization for sensitive changes

### 11.4 Repository Governance Oversight

The PMO Governance Lead or designated Configuration Manager shall:

- Monitor repository integrity
- Review access logs
- Validate backup systems
- Ensure version control compliance
- Report anomalies immediately

Repository integrity is considered a critical security and governance control point within the project.

---

## 12. Roles and Responsibilities:

Effective configuration management within the NCPBF project requires clearly defined roles, segregation of duties, and governance accountability. The following roles are responsible for ensuring configuration integrity, baseline protection, and compliance with the Configuration Management Plan (CMP).

**Project Manager**

The Project Manager holds overall accountability for ensuring compliance with the CMP throughout the project lifecycle.

Responsibilities include:

- Ensuring all configuration processes are implemented and followed
- Preventing unauthorized changes to baselines
- Ensuring that no work proceeds based on uncontrolled documentation
- Overseeing the Change Control Board (CCB) process
- Escalating major configuration risks to the Steering Committee
- Ensuring integration between configuration management and scope, schedule, cost, risk, and quality controls

The Project Manager acts as the primary guardian of baseline integrity at the execution level.

**PMO Governance Lead**

The PMO Governance Lead provides independent oversight and assurance of configuration management activities.

Responsibilities include:

- Maintaining the official Configuration Register
- Ensuring all Configuration Items (CIs) are uniquely identified and properly classified
- Verifying version control compliance
- Conducting Functional and Physical Configuration Audits
- Monitoring configuration status reporting metrics
- Ensuring traceability between requirements, design, implementation, and testing
- Reporting configuration health to executive governance bodies

The PMO Governance Lead ensures configuration discipline remains measurable and auditable.

**Configuration Manager (If Appointed)**

Where formally designated, the Configuration Manager administers the day-to-day configuration control processes.

Responsibilities include:

- Managing CI identification and coding
- Administering version control procedures
- Updating configuration records following approved changes
- Ensuring repository integrity and compliance
- Coordinating configuration status accounting reports
- Supporting audit preparation and documentation

The Configuration Manager ensures operational execution of configuration governance processes.

**Security Board**

The Security Board holds authority over all security-sensitive Configuration Items.

Responsibilities include:

- Reviewing changes impacting vault design, restricted layouts, cybersecurity architecture, encryption parameters, and access control systems
- Conducting Security Impact Reviews
- Ensuring compliance with security standards and regulatory mandates
- Approving or rejecting security-related configuration modifications
- Escalating high-risk security configuration issues

The Security Board protects national security integrity within configuration control activities.

**Change Control Board (CCB)**

The Change Control Board is the formal decision-making authority for Configuration Item modifications.

Responsibilities include:

- Reviewing impact analysis results
- Assessing scope, cost, schedule, risk, and security implications
- Approving, rejecting, or deferring Change Requests
- Determining whether re-baselining is required
- Ensuring alignment with project objectives and governance thresholds

The CCB ensures disciplined and documented decision-making for all configuration changes.

**Segregation of Duties Principle**

To preserve governance integrity:

- The individual requesting a change shall not approve it.
- The approving authority shall not implement the change.
- Security-sensitive changes require independent review.

This segregation ensures independence, transparency, and accountability.

## 13. Configuration Risks:

Configuration management is implemented to mitigate systemic risks inherent in a complex, multi-phase, high-security infrastructure project. The CMP directly addresses the following key configuration risks:

### 13.1 Unauthorized Change

Risk: Informal or undocumented changes to baselined documentation, design artifacts, or system configurations.

Impact:

- Scope creep
- Cost overruns
- Security vulnerabilities
- Regulatory non-compliance

Mitigation:

- Formal change control
- Role-based repository access
- Audit trails
- Governance escalation

### 13.2 Version Confusion

Risk: Multiple versions of documents circulating without clear identification of the authoritative baseline.

Impact:

- Construction errors
- Installation of outdated configurations
- Rework and delays
- Audit findings

Mitigation:

- Strict version control rules
- Single source of truth repository
- Controlled archiving of superseded versions

### 13.3 Design-to-Build Misalignment

Risk: Physical implementation deviates from approved design baseline.

Impact:

- Structural inconsistencies
- Security compliance failure
- Increased remediation costs

Mitigation:

- Physical Configuration Audits
- Stage-gate verification
- Strict baseline protection

### 13.4 Security Exposure

Risk: Unauthorized access to sensitive configuration items (vault layouts, cybersecurity architecture, encryption parameters).

Impact:

- National security risk
- Institutional reputation damage
- Legal and regulatory consequences

Mitigation:

- Security classification enforcement
- Encryption and access control
- Security Board oversight
- Multi-factor authentication

### 13.5 Documentation Inconsistency

Risk: Operational documentation does not reflect actual installed systems.

Impact:

- Operational failure
- Maintenance errors
- Safety risks
- Commissioning delays

Mitigation:

- Configuration audits
- Operational baseline validation
- As-built documentation verification

### 13.6 Operational Readiness Gaps

Risk: Transition to operations occurs without validated and synchronized configuration documentation.

Impact:

- System instability
- Training deficiencies
- Security control failures
- Reduced sustainability

Mitigation:

- Mandatory pre-operational configuration audit
- Validation of operational baseline
- Formal handover documentation approval

### Systemic Governance Risk Reduction

The Configuration Management Plan reduces systemic governance risk by:

- Protecting baseline integrity
- Enforcing traceability
- Preventing unauthorized modification
- Enabling audit readiness
- Strengthening executive oversight
- Ensuring alignment between documentation and implementation

In a national strategic infrastructure initiative such as the NCPBF project, disciplined configuration management is not merely a control mechanism—it is a structural safeguard protecting institutional credibility, security assurance, and long-term operational sustainability.

## 14. Integration With Other Plans:

Configuration Management within the NCPBF project does not operate as an isolated administrative function. It is fully integrated with the broader project governance and control ecosystem and serves as the structural control backbone supporting all knowledge areas.

The Configuration Management Plan (CMP) directly interfaces with and reinforces the following management plans and governance frameworks:

**Scope Management Plan**

Configuration management protects the Scope Baseline by ensuring that all scope-related artifacts—Scope Statement, WBS, and WBS Dictionary—are formally identified, version-controlled, and modified only through approved change control. Any scope modification automatically triggers configuration update procedures, ensuring alignment between documentation and execution.

**Change Management Plan**

Configuration management and change management are tightly linked. Every approved Change Request that impacts a Configuration Item must result in:

- Updated CI version
- Configuration Register update
- Baseline adjustment (if applicable)

The CMP ensures that change approval decisions are reflected accurately in controlled documentation and that no change is implemented without corresponding configuration updates.

**Requirements Management Plan**

Configuration identification ensures traceability from business requirements to design, construction, testing, and operational deliverables. The Requirements Traceability Matrix (RTM) must remain aligned with configuration records at all times. Any requirement change requires synchronized configuration updates to prevent functional misalignment.

**Risk Management Plan**

Configuration status accounting and change control processes contribute directly to risk mitigation. Configuration instability, version confusion, or unauthorized changes are treated as project risks and recorded in the Risk Register. Configuration audits serve as proactive risk detection mechanisms.

**Quality Management Plan**

Configuration audits (Functional and Physical Configuration Audits) are integrated with quality assurance and quality control processes. Ensuring that implemented systems match approved configuration baselines supports defect prevention, compliance verification, and acceptance validation.

**Communication Management Plan**

All approved configuration changes must be formally communicated to affected stakeholders. The CMP ensures that only the latest approved versions are distributed and referenced in official communications, preventing confusion and misinterpretation.

**Governance Framework**

Configuration Management supports the Governance Framework by:

- Protecting baseline commitments
- Enforcing escalation thresholds
- Supporting stage-gate reviews
- Providing executive-level reporting
- Preserving audit transparency

Configuration management therefore functions as a foundational governance safeguard that ensures consistency across strategic intent, technical implementation, and operational transition.

**Structural Backbone Statement**

Configuration Management acts as the structural integrity mechanism that binds scope, schedule, cost, quality, risk, security, and operational controls into one coherent and traceable governance system. Without disciplined configuration control, alignment across knowledge areas cannot be sustained in a complex and high-security project environment.

## 15. Monitoring & Continuous Improvement:

Configuration Management effectiveness within the NCPBF project will be continuously measured, evaluated, and improved to ensure long-term governance maturity and operational sustainability.

### 15.1 Configuration Performance Metrics

The effectiveness of configuration control shall be measured using quantitative and qualitative indicators, including:

- Percentage of changes processed through formal change control
- Number of unauthorized modification incidents
- Number and severity of configuration audit findings
- Percentage of configuration items fully traceable to requirements (RTM completeness)
- Instances of rework due to configuration mismatch
- Frequency of baseline revisions
- Time required to process configuration changes

These metrics provide early indicators of governance discipline and configuration stability.

### 15.2 Trend Analysis

Configuration status data will be analyzed periodically to detect patterns such as:

- Excessive change volume
- Recurring documentation inconsistencies
- High rate of minor corrections indicating design maturity issues
- Security-sensitive configuration volatility

Such trends may indicate deeper issues in requirements clarity, design maturity, or governance effectiveness and must be addressed proactively.

### 15.3 Lessons Learned and Continuous Refinement

Configuration-related lessons learned shall be formally captured at:

- Major stage-gate reviews
- Commissioning completion
- Post-operational handover

- Significant audit findings

Lessons learned will inform:

- Process refinements
- Template improvements
- Role clarification
- Security control strengthening
- Repository enhancement

The CMP shall be periodically reviewed and updated to reflect evolving best practices, regulatory updates, and institutional learning.

### 15.4 Governance Maturity Objective

The long-term objective of monitoring and continuous improvement is to strengthen configuration governance maturity so that:

- Configuration discipline becomes institutionalized
- Baseline integrity is consistently protected
- Audit findings decrease over time
- Operational sustainability improves
- Security assurance remains uncompromised

Continuous improvement ensures that configuration management evolves alongside project complexity and organizational capability.

### Closing Statement

Through integration, monitoring, and structured improvement, the Configuration Management Plan becomes a dynamic governance instrument rather than a static procedural document. In a national strategic initiative such as the NCPBF project, configuration management discipline directly contributes to institutional trust, regulatory compliance, security integrity, and sustainable operational excellence.