REQUIREMENT 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: 4

2. Requirements Governance Framework: 7

2.1 Governance Structure: 7

2.2 Requirements Classification: 9

3. Requirements Lifecycle Overview: 12

4. Collect Requirements Process: 13

4.1 Objectives: 13

4.2 Recommended Collection Techniques: 14

4.2.1 Stakeholder Interviews: 14

4.2.2 Facilitated Workshops (High Priority Technique): 15

4.2.3 Document Analysis: 15

4.2.4 Observation & Site Assessment: 16

4.2.5 Prototyping (Controlled Iterative Validation): 16

4.2.6 Surveys (Limited and Targeted Use): 17

4.2.7 Benchmarking: 17

5. Requirements Prioritization: 19

5.1 Prioritization Governance Rules: 19

5.2 Recommended Prioritization Techniques: 20

5.2.1 MoSCoW Method (Recommended for Functional Systems): 20

5.2.2 Weighted Scoring Model (Recommended for Strategic Decisions): 21

5.2.3 Kano Analysis (Selective Use): 22

5.2.4 Risk-Based Prioritization: 22

7. Product Analysis Methods: 24

7.1 Decomposition (Primary Method): 24

7.2 Systems Engineering Analysis: 25
7.3 Value Engineering: 26
7.4 Process Modeling: 27
7.5 Simulation & Scenario Modeling: 28
8. Requirements Documentation: 30
8.1 Requirements Register Template: 30
8.2 Requirements Traceability Matrix (RTM) Template: 32
8.3 Technical Specification Document Template: 33
8.4 Security Specification Addendum Template: 35
8.5 Interface Control Document (ICD) Template: 36
9. Requirements Traceability: 40
10. Requirements Change Control: 43
11. Integration with Other Domains: 46
12. Tools & Systems: 48
13. Requirements Validation & Verification: 50
14. Requirements Success Criteria: 53
REQUIREMENTS TRACEABILITY MATRIX (RTM) TEMPLATE: 55

1. Purpose:

The purpose of this Requirements Management Plan is to establish a structured, controlled, and value-driven framework for managing all project requirements throughout the entire lifecycle of the National Currency Printing and Secure Banknote Production Facility (NCPBF) Project. This plan defines how requirements will be systematically identified, analyzed, documented, validated, prioritized, traced, approved, monitored, and controlled in alignment with strategic objectives and governance expectations.

This document provides a disciplined approach to ensure that every requirement introduced into the project environment is formally evaluated, justified, and aligned with approved business needs. It establishes clear processes and responsibilities to maintain requirement integrity, prevent ambiguity, reduce risk exposure, and avoid uncontrolled scope expansion.

The plan defines the mechanisms through which requirements are captured from authorized stakeholders, including executive leadership, regulatory bodies, security authorities, operational teams, technical experts, and external partners. It ensures that requirement collection activities are structured, documented, and traceable to their originating source.

This plan further defines the analytical methods used to assess requirement feasibility, clarity, completeness, consistency, and impact. Each requirement must be evaluated not only for technical soundness but also for its operational, financial, security, regulatory, and lifecycle implications. No requirement shall be accepted into the baseline without structured analysis and validation.

The Requirements Management Plan establishes prioritization frameworks that ensure critical regulatory and security requirements receive immediate and non-negotiable attention, while other requirements are evaluated based on strategic alignment, value contribution, risk mitigation, operational efficiency, and financial impact. Prioritization decisions will follow transparent and documented governance procedures.

This plan outlines documentation standards to ensure that all requirements are recorded using uniform identification structures, clear descriptions, defined acceptance criteria, assigned ownership, and traceability links to deliverables, work

packages, benefits, and verification methods. This structured documentation approach supports transparency, accountability, and audit readiness.

The plan also defines the traceability model to ensure that each requirement is directly connected to approved business benefits, system designs, procurement packages, construction components, security frameworks, testing protocols, and commissioning criteria. This traceability ensures that no deliverable exists without a validated requirement and no requirement remains unimplemented without documented justification.

A key purpose of this plan is to integrate requirements management with other core management domains, including scope management, risk management, financial management, schedule management, stakeholder engagement, and security governance. Requirements shall not be managed in isolation but as interconnected components of an integrated performance system.

This document establishes governance roles and responsibilities for requirement oversight. It clarifies the authority of the Change Control Board (CCB), Steering Committee, Executive Sponsor, Security Review Authority, and Technical Review Board in reviewing, approving, or rejecting requirement additions or modifications. It ensures that requirement decisions are made at appropriate governance levels based on impact and strategic significance.

The Requirements Management Plan also introduces structured controls to prevent unauthorized requirement expansion, informal design modifications, or undocumented feature additions. Any proposed requirement change must undergo formal impact analysis assessing scope, cost, schedule, risk, security, and operational readiness implications before approval.

The plan supports lifecycle discipline by defining requirement freeze points prior to major procurement, construction, and commissioning milestones. These freeze gates ensure design stability, cost certainty, risk reduction, and contractual clarity.

This plan ensures that requirement validation confirms that the correct needs have been defined, while verification confirms that each requirement has been correctly implemented. These dual controls reduce the likelihood of rework, compliance gaps, and post-implementation deficiencies.

Another critical purpose of this document is to ensure regulatory compliance and national security integrity. Given the strategic sensitivity of the NCPBF Project, security requirements must be preserved, protected, and controlled with enhanced scrutiny and restricted access protocols.

The plan promotes clarity in communication by defining how requirements are shared, reviewed, and updated across multidisciplinary teams. It supports collaboration while maintaining governance discipline.

This document also ensures that requirements contribute to long-term sustainability, maintainability, and operational resilience. Requirements shall not only address immediate project delivery but also lifecycle performance, scalability, and future adaptability.

Through structured monitoring and control mechanisms, this plan ensures that requirement performance is periodically reviewed against approved baselines. Deviations are identified early, analyzed formally, and addressed through governance channels.

The Requirements Management Plan ultimately safeguards the project from scope creep, unmanaged expectations, uncontrolled customization, and fragmented decision-making. It ensures that project outputs are directly aligned with strategic intent, measurable benefits, and operational readiness criteria.

By establishing formal processes, accountability structures, analytical rigor, and governance checkpoints, this plan ensures that all deliverables are purposeful, traceable, compliant, secure, and value-driven.

The successful implementation of this Requirements Management Plan will result in disciplined requirement control, minimized rework, enhanced stakeholder confidence, improved audit readiness, and successful commissioning without deficiencies caused by uncontrolled requirement changes.

This plan therefore serves as a foundational governance instrument that protects strategic intent, reinforces accountability, and ensures that the NCPBF Project delivers secure, compliant, high-quality, and value-aligned outcomes.

2. Requirements Governance Framework:

Given the strategic national importance, financial sensitivity, and security-critical nature of the National Currency Printing and Secure Banknote Production Facility (NCPBF) Project, requirements governance operates under a structured, multi-layered control framework. This framework ensures that all requirements are authorized, reviewed, validated, and approved at the appropriate decision-making level based on their impact, sensitivity, and strategic significance.

The governance framework is designed to maintain stability of the requirements baseline, protect security architecture integrity, ensure regulatory compliance, and preserve alignment with approved strategic objectives. No requirement shall enter or modify the project baseline without formal governance review and documentation.

This framework establishes clear accountability, defined authority boundaries, escalation mechanisms, and documentation controls to ensure disciplined requirement oversight throughout the project lifecycle.

2.1 Governance Structure:

The governance structure for requirements management is designed to ensure separation of strategic oversight, technical validation, security control, and operational coordination. Each governance body holds defined authority and review responsibilities.

Business Sponsor

The Business Sponsor holds ultimate authority for strategic requirement approval. All requirements that affect strategic direction, national policy alignment, financial commitments, or long-term operational objectives must receive sponsor endorsement. The Business Sponsor ensures that requirements contribute directly to approved benefits and national value objectives.

The Sponsor also resolves conflicts that cannot be settled at lower governance levels and authorizes major requirement changes impacting funding, scope boundaries, or performance commitments.

Steering Committee

The Steering Committee is responsible for validating high-impact requirements that significantly influence project outcomes, schedule commitments, cost baselines, regulatory exposure, or stakeholder expectations.

The Committee reviews cross-domain implications of major requirements and ensures alignment between technical feasibility, business value, financial sustainability, and risk exposure. Requirements with broad institutional or operational impact must be reviewed by this body before baseline integration.

Security Board

The Security Board oversees all security-related requirements, including physical security, cyber security, access controls, classified system protections, vault standards, surveillance architecture, encryption mechanisms, and information protection protocols.

All security requirements, whether new or modified, must undergo formal security impact assessment before approval. Classified requirements are handled through restricted documentation procedures and controlled distribution channels.

The Security Board ensures that no requirement compromises facility integrity, national currency protection standards, or information security controls.

Technical Review Board

The Technical Review Board evaluates engineering feasibility, systems integration complexity, performance thresholds, maintainability considerations, scalability, and compliance with design standards.

This board ensures that requirements are technically sound, measurable, verifiable, and compatible with the overall architecture. It validates integration points between hardware, software, infrastructure systems, and vendor solutions.

Technical validation is mandatory before requirement approval to prevent downstream rework or system conflicts.

Change Control Board (CCB)

The Change Control Board governs all baseline modifications. Any addition, removal, or modification of an approved requirement must pass through the CCB process.

The CCB conducts structured impact analysis across scope, cost, schedule, risk, security, procurement, and operational domains. Only upon documented review and approval may requirement changes be integrated into the baseline.

Unauthorized requirement additions are strictly prohibited and subject to formal corrective action procedures.

Project Manager

The Project Manager is responsible for operational coordination of requirement activities. This includes organizing requirement workshops, maintaining documentation, facilitating reviews, ensuring traceability, and monitoring compliance with governance procedures.

The Project Manager ensures that requirements flow through proper review channels and that documentation remains current, consistent, and controlled.

While the Project Manager coordinates the process, approval authority remains within the defined governance bodies.

2.2 Requirements Classification:

To ensure clarity, consistency, and appropriate review routing, all requirements are categorized according to their nature, impact, and governance sensitivity. Each category follows defined review protocols and approval pathways.

Business Requirements

Business requirements define the strategic outcomes, capability expectations, and value propositions that justify the project's existence. These requirements originate primarily from executive leadership and policy authorities.

Business requirements must align with approved benefits and long-term operational vision. They undergo sponsor-level review before validation.

Regulatory & Compliance Requirements

These requirements originate from national laws, financial regulations, currency production standards, environmental compliance mandates, and institutional oversight frameworks.

Regulatory requirements are mandatory and non-negotiable. They must be verified for completeness and traceability to legal sources. Approval requires confirmation from compliance authorities.

Security Requirements (Physical & Cyber)

Security requirements define standards for facility access control, vault protection, production area segregation, surveillance systems, cybersecurity architecture, data encryption, system resilience, and classified information handling.

Due to the national security implications, these requirements follow enhanced review and restricted documentation protocols. Security Board approval is mandatory.

Functional Requirements

Functional requirements describe what systems, processes, or components must perform. These include production system capabilities, monitoring functions, IT workflows, reporting dashboards, automation functions, and operational control mechanisms.

Functional requirements are validated by the Technical Review Board to ensure clarity and measurability.

Non-Functional Requirements

Non-functional requirements define performance characteristics such as reliability, availability, capacity, throughput, response time, scalability, maintainability, and durability.

These requirements ensure long-term sustainability and operational stability. They are analyzed for measurable acceptance criteria and lifecycle impact.

Technical Requirements

Technical requirements specify engineering standards, hardware specifications, software protocols, system architecture constraints, network configurations, and equipment performance thresholds.

These requirements must align with integration architecture and procurement strategies.

Interface Requirements

Interface requirements define interaction points between systems, vendors, infrastructure components, security systems, and operational platforms.

Given the multi-vendor nature of the project, interface requirements undergo detailed dependency and compatibility analysis.

Operational & Maintenance Requirements

These requirements ensure long-term operability, maintainability, training readiness, spare parts availability, documentation completeness, and lifecycle sustainability.

Operational teams must validate these requirements to ensure smooth transition to steady-state operations.

Contractual & Vendor Requirements

These requirements define procurement specifications, performance guarantees, service-level agreements, warranty provisions, penalty clauses, testing protocols, and delivery conditions.

They are reviewed jointly by technical, financial, and procurement authorities to ensure enforceability and clarity.

Each requirement category follows specific review protocols aligned with its risk level, financial exposure, technical complexity, and security sensitivity. Classification ensures that requirements are evaluated by the appropriate governance authority and prevents inappropriate routing or unauthorized approval.

Through this structured governance framework and disciplined classification system, the project ensures requirement clarity, accountability, security integrity, compliance assurance, and strategic alignment.

3. Requirements Lifecycle Overview:

The requirements lifecycle aligns with project focus areas:

Focus Area	Requirements Activity
Initiating	High-level business requirements
Planning	Detailed collection, analysis, prioritization
Executing	Validation & controlled refinement
Monitoring & controlling	Traceability & change management
Closing	Requirements verification & acceptance confirmation

4. Collect Requirements Process:

The Collect Requirements Process establishes a structured and controlled approach for identifying, capturing, clarifying, and documenting all project requirements necessary to deliver the National Currency Printing and Secure Banknote Production Facility (NCPBF). Given the project's national importance, financial sensitivity, and high-security environment, requirements collection must be comprehensive, disciplined, and governed by formal protocols.

The objective of this process is not merely to gather stakeholder expectations, but to transform strategic intent, regulatory obligations, operational needs, and technical constraints into clearly defined, verifiable, and traceable requirements that can be integrated into the project baseline.

This process is executed primarily during the planning phase but may continue in a controlled manner throughout the lifecycle, subject to governance controls and baseline management procedures.

4.1 Objectives:

The primary objective of the Collect Requirements Process is to capture complete, unambiguous, and verifiable requirements. Each requirement must be written in clear, measurable language that avoids subjective interpretation. Ambiguity in requirements increases the risk of misalignment, rework, disputes, and security vulnerabilities; therefore, clarity and precision are mandatory.

Another core objective is to ensure that all requirements align directly with defined project benefits and measurable Key Performance Indicators (KPIs). Requirements must not exist in isolation. Each requirement must demonstrate contribution to strategic objectives, operational performance, regulatory compliance, risk mitigation, or security reinforcement.

The process also seeks to identify constraints and assumptions that influence requirement feasibility and implementation. Constraints may include budget ceilings, regulatory mandates, security classifications, procurement limitations, or technological dependencies. Assumptions must be documented and periodically reviewed to prevent future misalignment.

An additional objective is to prevent late discovery of critical needs. Early and structured engagement reduces the likelihood of design modifications during

construction, procurement rework, contractual disputes, or commissioning delays. Front-loaded requirement clarification significantly enhances project stability and cost predictability.

Finally, the Collect Requirements Process ensures cross-functional alignment among executive leadership, technical teams, security authorities, operational managers, procurement specialists, and regulatory representatives. Requirements must reflect integrated understanding rather than isolated departmental perspectives.

4.2 Recommended Collection Techniques:

Given the complexity of integrating secure physical infrastructure, advanced currency production systems, cybersecurity architecture, multi-vendor IT integration, and operational readiness planning, a combination of complementary requirement collection techniques is required. No single method is sufficient for capturing the full spectrum of needs.

Each technique must be applied deliberately, documented formally, and routed through governance review channels before requirement baseline integration.

4.2.1 Stakeholder Interviews:

Stakeholder interviews are a foundational requirement collection method for capturing strategic, regulatory, and operational insights directly from authorized decision-makers.

Structured and semi-structured interviews are conducted with:

- Central bank leadership to clarify strategic objectives and long-term capability expectations.
- Security authorities to define physical and cyber protection requirements.
- Regulatory bodies to confirm compliance mandates and reporting obligations.
- Operations managers to capture workflow, maintenance, and sustainability requirements.

Structured interviews ensure consistency across sessions by using predefined question sets aligned with requirement categories. Semi-structured interviews allow for deeper exploration of emerging concerns or contextual nuances.

All interviews must be documented with formal minutes, requirement summaries, and traceable source references. Interview-derived requirements must undergo validation sessions before baseline inclusion.

4.2.2 Facilitated Workshops (High Priority Technique):

Facilitated workshops are considered a high-priority collection method for this project due to the need for cross-functional integration and rapid clarification of interdependent requirements.

Workshops are particularly effective for:

- Technical architecture definition
- IT system integration mapping
- Facility design alignment
- Security system coordination
- Cross-functional operational alignment

Workshops must be conducted in a controlled environment with clearly defined agendas, structured facilitation, documented outputs, and formal attendance records.

A neutral moderator should guide sessions to prevent dominance by specific stakeholders and to ensure balanced participation. Real-time documentation is required to reduce interpretation gaps.

Outputs from workshops typically include requirement lists, clarified acceptance criteria, interface definitions, identified dependencies, and documented constraints. These outputs must be reviewed and formally approved before being incorporated into requirement registers.

4.2.3 Document Analysis:

Document analysis provides a systematic review of authoritative sources to extract compliance-driven and benchmark-based requirements.

Sources include:

- Regulatory frameworks governing currency production and financial operations
- National security policies and compliance manuals
- International printing and anti-counterfeit standards

- Currency production benchmarks from comparable facilities
- Procurement policies and contractual guidelines

Document analysis ensures that regulatory and compliance requirements are not overlooked. It also helps identify industry best practices and mandatory technical standards.

Each extracted requirement must reference its source document and include citation identifiers to support audit readiness and verification.

4.2.4 Observation & Site Assessment:

Observation and site assessment are critical for understanding current operational conditions and identifying gaps between existing capabilities and target-state requirements.

This method is used for:

- Benchmarking existing facilities
- Analyzing production workflows
- Identifying physical security vulnerabilities
- Evaluating operational inefficiencies

Direct observation provides insights that may not emerge during interviews or workshops. It reveals real-world constraints, process bottlenecks, and environmental conditions that influence requirement feasibility.

Findings must be documented in structured assessment reports and translated into measurable requirements where appropriate.

4.2.5 Prototyping (Controlled Iterative Validation):

Prototyping is recommended for technology-driven components where visualization improves requirement clarity.

Applicable areas include:

- IT dashboards and reporting interfaces
- Security monitoring systems
- Access control management systems
- Operational control panels

Prototyping allows stakeholders to validate functional expectations before full-scale implementation. However, due to governance sensitivity, prototypes must not bypass formal requirement approval processes.

Prototype outputs must be evaluated through structured validation sessions and formally documented before requirement finalization.

4.2.6 Surveys (Limited and Targeted Use):

Surveys are used selectively to gather input from larger operational groups where individual interviews are impractical.

Surveys may assess:

- Operational staff readiness
- Training requirements
- Process improvement opportunities

Survey questions must be carefully designed to avoid ambiguity. Results must be statistically summarized and validated before translation into formal requirements.

Due to the strategic sensitivity of the project, surveys are not used for high-level strategic or security requirement collection.

4.2.7 Benchmarking:

Benchmarking compares proposed requirements against established international standards and similar high-security industrial facilities.

Comparison may include:

- International currency printing facilities
- Secure manufacturing plants
- High-security data centers
- Advanced industrial automation environments

Benchmarking supports technical validation and performance calibration. It ensures that requirements are neither under-specified nor excessively complex relative to global best practices.

Benchmark findings must be analyzed for contextual applicability and documented within technical validation reports.

Integration and Control

All requirement collection activities must be:

- Logged in the Requirements Register
- Assigned unique identifiers
- Classified under approved requirement categories
- Routed for governance review
- Linked to defined benefits and KPIs

Informal requests, undocumented expectations, or ad-hoc design ideas are not recognized as requirements unless processed through the formal collection and validation framework.

The Collect Requirements Process therefore functions not only as a discovery mechanism but as a governance filter that protects scope stability, ensures regulatory integrity, reinforces security controls, and supports long-term value realization.

5. Requirements Prioritization:

Due to defined budget ceilings, national security obligations, regulatory compliance mandates, procurement sequencing constraints, and schedule commitments, requirements prioritization within the NCPBF Project must follow a structured, formalized, and governance-controlled methodology. Prioritization cannot be informal, subjective, or politically influenced. It must be transparent, documented, analytically justified, and aligned with strategic value delivery.

Requirements prioritization ensures that limited financial, technical, and operational resources are allocated to the most critical capabilities first. It also ensures that the project remains focused on delivering mandatory regulatory compliance, safeguarding security integrity, and achieving measurable performance outcomes without uncontrolled expansion.

Prioritization does not determine whether a requirement is valid; rather, it determines the sequencing, urgency, and funding allocation associated with its implementation. Every requirement that enters the validated register must undergo structured prioritization before integration into the execution roadmap.

5.1 Prioritization Governance Rules:

Prioritization decisions must follow clearly defined governance rules to maintain accountability and strategic alignment.

All requirements must map to at least one defined project benefit or measurable KPI. A requirement that cannot demonstrate direct or indirect contribution to approved benefits must be reconsidered, refined, or rejected. This rule ensures that prioritization supports value realization rather than preference-based enhancements.

Regulatory and security requirements are classified as non-negotiable. These requirements automatically receive top-tier priority status because failure to implement them exposes the project to legal, financial, reputational, and national security risks. Their sequencing may be adjusted for logical dependencies, but their implementation cannot be deferred without formal sponsor-level justification.

Financial impact must be evaluated before finalizing prioritization. Each requirement must undergo cost implication assessment, including capital

expenditure, lifecycle cost, maintenance implications, and integration cost. Requirements with high cost and low value contribution must be challenged and justified through governance review.

Sponsor approval is required for priority shifts that materially affect baseline sequencing, contractual obligations, regulatory commitments, or strategic outcomes. No department or technical team may independently downgrade or elevate requirement priority without documented governance approval.

Priority decisions must be recorded within the Requirements Register, including rationale, scoring outcome, approving authority, and date of decision. This documentation ensures audit readiness and traceability.

5.2 Recommended Prioritization Techniques:

Given the complexity of the NCPBF Project, a combination of prioritization techniques is recommended. Different requirement categories may require different prioritization methods depending on their nature and impact.

5.2.1 MoSCoW Method (Recommended for Functional Systems):

The MoSCoW method is recommended for functional and operational system requirements, particularly within IT systems, dashboard interfaces, automation controls, and workflow management components.

Under this method, requirements are classified as:

Must Have – These are essential requirements without which the system or facility cannot operate safely, legally, or effectively. They include mandatory regulatory controls, core production capabilities, and critical security features.

Should Have – These are important requirements that significantly enhance performance, efficiency, or usability but do not prevent fundamental operation if temporarily deferred.

Could Have – These are desirable improvements that increase convenience, optimization, or advanced functionality but are not essential for core operation.

Won't Have – These are requirements intentionally excluded from the current phase due to budget, scope, or strategic considerations. They may be considered in future enhancement phases.

The MoSCoW method supports structured decision-making and prevents overloading the baseline with optional features. It is particularly useful in managing system configuration complexity and balancing operational expectations with technical feasibility.

All MoSCoW classifications must be validated through governance review before formal adoption.

5.2.2 Weighted Scoring Model (Recommended for Strategic Decisions):

The Weighted Scoring Model is recommended for evaluating high-impact strategic requirements, particularly those involving significant capital investment, architectural modification, procurement commitments, or long-term operational implications.

Under this model, each requirement is evaluated against defined criteria using pre-approved weighting factors. Recommended evaluation criteria include:

Strategic alignment – Degree to which the requirement supports national objectives and long-term operational strategy.

Risk reduction – Extent to which the requirement mitigates operational, security, compliance, or financial risk.

Compliance necessity – Whether the requirement fulfills legal, regulatory, or audit obligations.

Operational efficiency – Expected improvement in productivity, reliability, scalability, or maintainability.

Financial impact – Cost-benefit ratio, lifecycle cost implications, and return on investment.

Each criterion receives a weighted value reflecting its strategic importance. Requirements are scored against each criterion, and aggregate scores determine relative prioritization.

The Weighted Scoring Model enhances transparency and reduces subjective influence in strategic decision-making. It ensures alignment between financial stewardship and performance outcomes.

Scoring results must be documented and approved at the appropriate governance level.

5.2.3 Kano Analysis (Selective Use):

Kano Analysis may be applied selectively for user-facing systems and operational usability improvements, particularly within IT dashboards, monitoring interfaces, reporting systems, and workflow optimization tools.

This method classifies requirements into categories such as:

Basic Needs – Requirements that users expect by default; absence causes dissatisfaction.

Performance Needs – Requirements where better performance directly increases satisfaction.

Excitement Features – Enhancements that exceed expectations but are not mandatory.

Within the NCPBF context, Kano Analysis is useful for improving operational experience without compromising baseline stability. However, it must be applied cautiously to avoid prioritizing convenience over security or compliance.

All excitement-level features must undergo financial and security impact review before prioritization.

5.2.4 Risk-Based Prioritization:

Risk-Based Prioritization ensures that requirements associated with high-risk exposure receive elevated attention.

Security requirements and regulatory compliance requirements are automatically elevated under this method. Requirements that mitigate high-probability or high-impact risks are prioritized over low-risk enhancements.

Risk-based prioritization also considers:

- Operational continuity risks
- System integration failure risks
- Contractual exposure risks
- Financial overrun risks
- National security vulnerability risks

Requirements that significantly reduce systemic risk may receive accelerated implementation even if they carry moderate cost implications.

Risk prioritization decisions must align with the project's approved Risk Management Plan and be documented within both the Risk Register and Requirements Register.

Integrated Prioritization Framework

No single prioritization technique should operate in isolation. The project adopts an integrated approach where:

- Regulatory and security requirements are automatically classified as Must Have and high-risk priority.
- Strategic capital decisions undergo weighted scoring evaluation.
- Functional system requirements may use MoSCoW classification.
- Usability enhancements may undergo Kano analysis.
- Risk exposure overlays influence final prioritization decisions.

This integrated framework ensures that prioritization reflects strategic alignment, regulatory integrity, financial discipline, operational efficiency, and risk mitigation simultaneously.

Prioritization Control and Review

Requirement priorities are not static. They may be reviewed at defined governance checkpoints, particularly during stage-gate reviews, major procurement milestones, or baseline revisions.

However, priority adjustments must follow formal governance approval and documented impact analysis. Informal reprioritization is prohibited.

The Requirements Management Plan therefore ensures that prioritization remains disciplined, transparent, value-driven, risk-aware, and governance-controlled.

Through structured prioritization, the NCPBF Project safeguards national objectives, protects security architecture, maintains financial accountability, and ensures that the most critical capabilities are delivered in a stable and predictable manner.

7. Product Analysis Methods:

Given the nature of the National Currency Printing and Secure Banknote Production Facility (NCPBF) Project—which combines high-security physical infrastructure, precision production equipment, cybersecurity architecture, enterprise IT systems, vault protection mechanisms, and multi-vendor technology integration—product analysis must be rigorous, systematic, and multidisciplinary.

Product analysis in this project goes beyond defining deliverables. It requires deep examination of how individual components function independently and collectively as an integrated secure ecosystem. The analysis must ensure architectural integrity, regulatory compliance, operational continuity, performance reliability, security resilience, and lifecycle sustainability.

The following product analysis methods are formally adopted for this project.

7.1 Decomposition (Primary Method):

Decomposition is the primary product analysis method used to break down the overall NCPBF facility into manageable, logically structured components. This method transforms a complex, multi-dimensional system into structured subsystems that can be analyzed, designed, procured, constructed, and validated in a controlled manner.

The decomposition process begins by identifying the highest-level product components and progressively breaking them down into smaller subsystems, assemblies, modules, and functional units. This structured breakdown enables clarity of scope, assignment of responsibilities, traceability to requirements, and alignment with procurement packages.

The NCPBF product is decomposed into the following major categories:

Facility Components – This includes the physical structure, reinforced construction, secure vault chambers, access-controlled zones, perimeter security systems, environmental control systems, utilities infrastructure, and secure storage areas. Each facility element must be analyzed for durability, access segregation, compliance with safety standards, and integration with security controls.

Production Systems – These include printing presses, substrate handling systems, ink management systems, finishing equipment, serial numbering systems, inspection systems, packaging units, and waste destruction mechanisms. Decomposition ensures each production subsystem has clearly defined performance specifications, throughput capacity, quality tolerance levels, and maintenance protocols.

Security Architecture – This includes surveillance systems, biometric access controls, intrusion detection systems, armored vault doors, cyber defense mechanisms, encryption systems, and classified data handling frameworks. Decomposition ensures that security components are analyzed individually while maintaining systemic integrity.

IT Systems – These include enterprise resource planning systems, production monitoring platforms, asset tracking systems, reporting dashboards, data storage infrastructure, cybersecurity monitoring tools, and integration middleware. Decomposition ensures clarity in system interfaces, data flows, and user access layers.

Monitoring Systems – These include environmental monitoring, production performance monitoring, compliance tracking, real-time alert systems, and risk dashboards. Each monitoring function must be analyzed for accuracy, reliability, and response time thresholds.

Through decomposition, each subsystem becomes traceable to specific requirements, cost estimates, risk exposures, and performance criteria. This method prevents scope ambiguity and supports structured verification during commissioning.

7.2 Systems Engineering Analysis:

Systems Engineering Analysis is essential for evaluating how independent components interact within an integrated ecosystem. The NCPBF Project operates in a multi-vendor, multi-technology environment where hardware, software, security infrastructure, and operational processes must function seamlessly.

This method examines the product from a holistic, lifecycle-oriented perspective. Rather than focusing on isolated components, systems engineering evaluates

interdependencies, integration interfaces, performance alignment, and failure propagation risks.

This analysis is particularly critical for:

Integration of hardware and software – Printing machinery must interface with digital tracking systems. Security hardware must integrate with cybersecurity monitoring platforms. Production reporting systems must connect to executive dashboards. Systems engineering ensures data consistency and operational synchronization.

Multi-vendor environment coordination – Vendors supplying presses, vault systems, IT infrastructure, surveillance equipment, and access controls must operate under interoperable standards. Systems engineering ensures compatibility, interface control documentation, and unified configuration management.

Security system coordination – Physical and cyber security systems must operate in layered defense alignment. For example, access control data must integrate with surveillance logging, and cybersecurity alerts must trigger operational controls where appropriate.

Systems engineering also includes requirements traceability across system levels, failure mode analysis, redundancy planning, and lifecycle maintenance modeling. This approach reduces integration risk and enhances overall system reliability.

7.3 Value Engineering:

Value Engineering is applied to optimize cost, performance, and lifecycle sustainability without compromising security integrity or regulatory compliance.

In a high-capital project such as NCPBF, value engineering ensures that design decisions achieve the required functionality at optimal lifecycle cost. It does not focus solely on initial procurement price but evaluates long-term operational cost, energy efficiency, maintainability, spare parts availability, and upgrade potential.

Value engineering supports:

Cost optimization – Evaluating alternative materials, technologies, or configurations that achieve required performance at reduced lifecycle expense.

Lifecycle sustainability – Assessing durability, maintenance cycles, energy consumption, and upgrade flexibility to ensure long-term operational resilience.

Operational efficiency – Identifying design improvements that streamline workflows, reduce downtime, and improve throughput without compromising security.

All value engineering proposals must undergo security and compliance review before adoption. Cost savings cannot override mandatory regulatory or security requirements.

7.4 Process Modeling:

Process modeling analyzes the operational workflows that will occur within the NCPBF facility. This method ensures that physical infrastructure, production equipment, security systems, and IT platforms support efficient, compliant, and secure processes.

Process modeling is used extensively for:

Currency production workflow – Mapping end-to-end processes from raw material intake to finished banknote packaging and secure storage. This includes print sequencing, inspection checkpoints, rejection handling, destruction procedures, and inventory logging.

Quality control checkpoints – Modeling inspection stages, defect identification procedures, serial number verification processes, and compliance validation steps.

Logistics and vault operations – Mapping secure material movement, controlled access flows, inventory rotation protocols, and secure dispatch operations.

Process modeling identifies bottlenecks, duplication, handoff risks, and security vulnerabilities. It ensures that workflows align with regulatory mandates and security segregation principles.

Model outputs typically include flow diagrams, swimlane charts, decision trees, and process validation matrices. These models support requirement clarification and operational readiness planning.

7.5 Simulation & Scenario Modeling:

Simulation and scenario modeling provide predictive evaluation of system behavior under normal and abnormal conditions. Given the national security implications of currency production, stress testing and scenario planning are essential.

Simulation is recommended for:

Security breach scenarios – Modeling intrusion attempts, cyber-attack vectors, insider threat events, or vault access anomalies. Simulation evaluates response times, system resilience, alert escalation mechanisms, and containment effectiveness.

Production throughput modeling – Evaluating production capacity under peak demand, maintenance downtime, equipment malfunction, or supply chain delay conditions. Simulation ensures throughput targets are realistic and sustainable.

Emergency response planning – Modeling fire events, power outages, natural disasters, cyber incidents, or security lockdown situations. Scenario modeling ensures that emergency procedures are practical and coordinated across systems.

Simulation outputs support contingency planning, resource allocation, redundancy design, and risk mitigation strategies. They provide evidence-based validation before full-scale operational activation.

Integrated Product Analysis Approach

These product analysis methods are not applied independently. Decomposition provides structural clarity. Systems engineering ensures integration integrity. Value engineering optimizes performance and cost. Process modeling aligns operations. Simulation validates resilience.

Together, these methods create a comprehensive product analysis framework that ensures:

- Architectural coherence
- Security robustness
- Regulatory compliance
- Operational efficiency
- Financial sustainability
- Lifecycle reliability

Through rigorous application of these product analysis methods, the NCPBF Project ensures that the final facility is not only constructed according to specification but operates as a secure, resilient, integrated, and value-driven national asset.

8. Requirements Documentation:

8.1 Requirements Register Template:

Purpose:

Central master log of all approved and proposed requirements.

Primary control document for requirements governance.

A. Header Information

Field	Description
Project Name	NCPBF Project
Document Version	
Date Updated	
Prepared By	
Approved By	
Configuration Status	Draft / Approved / Baselined

B. Requirements Register Table:

Req ID	Category	Description	Source	Benefit ID	KPI Link	Priority	Owner	WBS ID	Risk ID	Security Classification	Status	Verification Method	Change Ref

Field Definitions

- **Req ID:** Unique structured code (e.g., SEC-IT-001, FAC-ARCH-012)
- **Category:** Business / Regulatory / Security / Functional / Non-Functional / Technical / Interface / Operational / Contractual
- **Description:** Clear, measurable statement
- **Source:** Stakeholder / Regulation / Workshop / Benchmark
- **Benefit ID:** Link to Benefits Management Plan
- **KPI Link:** Measurable success indicator
- **Priority:** Must / Should / Could / Strategic Tier
- **Owner:** Accountable authority
- **WBS ID:** Linked deliverable
- **Risk ID:** Related risk exposure
- **Security Classification:** Public / Restricted / Confidential / Classified
- **Status:** Proposed / Approved / Deferred / Rejected / Implemented

- **Verification Method:** Inspection / Test / Review / Audit
- **Change Ref:** Link to Change Register

8.2 Requirements Traceability Matrix (RTM) Template:

Purpose:

Ensures end-to-end traceability from strategic objective to implementation and verification.

A. RTM Structure:

Req ID	Strategic Objective	Benefit ID	Scope Ref	WBS ID	Design Doc Ref	Procurement Package	Risk ID	Test Case ID	Acceptance Record	Status

Traceability Logic

Requirement → Business Case → Benefit → Scope → WBS → Design → Procurement → Risk → Test → Acceptance

Governance Control Rule

- No WBS element without requirement
- No requirement without benefit link

- No acceptance without verification reference

8.3 Technical Specification Document Template:

Purpose:

Defines detailed technical and performance requirements for engineering, IT, and production systems.

A. Document Header

Field	Entry
System Name	
Spec Version	
Related Req IDs	
Prepared By	
Reviewed By	Technical Review Board
Approved By	Steering Committee / CCB
Classification	

B. System Overview

- System Purpose
- Functional Summary

- Regulatory References
- Security Impact Level
- Lifecycle Considerations

C. Detailed Technical Requirements:

Req ID	Requirement Statement	Performance Criteria	Interface Impact	Compliance Standard	Validation Method

D. Non-Functional Requirements Section

- Availability Targets
- Reliability Targets
- Capacity Targets
- Cybersecurity Controls
- Maintainability Standards

E. Integration Requirements

- External Interfaces

- Data Exchange Protocols
- Vendor Dependencies

F. Verification Plan

- Testing Approach
- Inspection Protocol
- Acceptance Threshold

8.4 Security Specification Addendum Template:

Purpose:

Captures all physical and cyber security requirements separately under controlled access.

A. Security Classification Header

Field	Entry
Classification Level	Restricted / Confidential / Classified
Controlled Distribution	Yes / No
Security Board Approval Date	

B. Security Requirements Table

Sec Req ID	Category (Physical/Cyber)	Description	Threat Addressed	Control Type	Linked System	Risk ID	Verification Method

C. Layered Defense Model Section

- Perimeter Controls
- Internal Access Controls
- Vault Protection
- Network Segmentation
- Monitoring & Incident Response

D. Security Testing & Certification Plan

- Penetration Testing
- Intrusion Simulation
- Compliance Audit
- Certification Authority

E. Governance Rule

No security requirement modification without Security Board approval.

8.5 Interface Control Document (ICD) Template:

Purpose:

Defines technical and operational interfaces between systems and vendors.

A. Document Header

Field	Entry
Interface Name	
Systems Involved	
Vendors Involved	
Version	
Approval Authority	Technical Review Board

B. Interface Description

- Purpose of Interface
- Data Type / Signal Type
- Communication Protocol
- Physical Connection Type

C. Interface Requirements Table:

Interface ID	Source System	Target System	Data Format	Frequency	Security Control	Validation Method

D. Dependency Mapping

- Upstream Dependencies
- Downstream Dependencies
- Failure Impact Assessment

E. Configuration Management

- Version Control Reference
- Change Request Reference
- Impacted Requirement IDs

Integrated Control Mechanism

All five documents integrate as follows:

- Requirements Register = Master source
- RTM = Traceability control
- Technical Spec = Engineering implementation
- Security Addendum = Protected controls
- ICD = System integration governance

Each document must be:

- Version controlled
- Stored in secure repository
- Updated only via formal change control

- Reviewed at stage-gate checkpoints

Master Integration Map

Requirement →
Requirements Register →
RTM →
WBS →
Technical Specification →
Security Addendum →
ICD →
Test Plan →
Acceptance Record →
Benefits Realization Tracking

9. Requirements Traceability:

Requirements traceability is a foundational control mechanism within the NCPBF Project. It ensures that every approved requirement is logically connected to design elements, scope components, cost allocations, schedule activities, risk exposure, testing procedures, acceptance confirmation, and measurable benefits. Traceability protects the project from misalignment, undocumented work, and value leakage.

Traceability must follow a structured end-to-end chain:

Requirement → Design → WBS → Cost → Schedule → Risk → Test → Acceptance → Benefit

This structured traceability chain ensures that requirements are not isolated statements but operational drivers that influence engineering decisions, financial planning, and performance measurement.

Every requirement entered into the Requirements Register must be uniquely identified and mapped to corresponding design documents. No design component may be developed unless it references at least one validated requirement. This ensures design integrity and prevents unnecessary or unauthorized features from entering the system architecture.

Each requirement must also be linked to a defined WBS element. The Work Breakdown Structure represents the authorized deliverable structure of the project. By linking requirements directly to WBS work packages, traceability ensures that scope execution reflects approved needs and that deliverables are not created without formal justification.

Cost traceability ensures that financial allocations correspond directly to validated requirements. Budget lines must be mapped to WBS components, which in turn link to requirement IDs. This enables cost control and prevents unbudgeted requirement expansion. If a requirement cannot be linked to an approved cost allocation, it cannot proceed to implementation.

Schedule traceability ensures that requirements are represented within the project timeline. Activities within the schedule must support requirement

implementation and verification. If a requirement lacks scheduled activities, it risks being overlooked during execution.

Risk traceability ensures that requirement-related risks are identified and managed. Each requirement must be evaluated for risk exposure, including technical feasibility, integration complexity, compliance risk, security vulnerability, and vendor dependency. The Risk Register must reference requirement IDs where applicable.

Testing traceability ensures that every requirement has a defined verification method. Test cases, inspection plans, validation workshops, simulation exercises, and audit procedures must reference requirement IDs. No requirement may be considered complete without documented verification evidence.

Acceptance traceability confirms that validated requirements are formally approved by authorized stakeholders. Acceptance records must reference requirement identifiers and confirm that defined acceptance criteria were satisfied.

Benefit traceability ensures that requirements contribute directly to defined benefits and measurable KPIs. Requirements that do not map to approved benefits must be reviewed and justified. This alignment protects strategic value realization.

The Requirements Traceability Matrix (RTM) serves as the central control artifact for managing these linkages. The RTM must be maintained under strict configuration control. Version history, approval records, and change logs must be documented to ensure audit readiness and transparency.

Traceability must be reviewed at stage-gate checkpoints, including design freeze, procurement freeze, construction completion, system integration, operational readiness review, and final commissioning. Any broken traceability chain must be treated as a governance exception and resolved before proceeding.

Unauthorized requirements—those introduced without formal documentation, governance review, or baseline integration—must be rejected immediately. Such instances must be logged in the Governance Exception Register and escalated as appropriate.

Through disciplined traceability, the NCPBF Project ensures structural coherence, financial discipline, regulatory compliance, risk awareness, and value alignment. Traceability transforms requirements from conceptual statements into controlled, measurable drivers of project success.

10. Requirements Change Control:

Requirements Change Control establishes the formal process through which approved requirements may be modified, added, deferred, or removed. Given the scale, security sensitivity, and financial magnitude of the NCPBF Project, uncontrolled requirement changes present significant risk to cost, schedule, compliance, and operational readiness. Therefore, all requirement modifications must follow a structured governance process.

All requirement changes must be formally submitted through a documented Change Request. Informal verbal instructions, email requests, or undocumented design modifications are strictly prohibited. Each change request must include a clear description of the proposed modification, justification, source, and anticipated impact.

Upon submission, the proposed change must undergo structured impact analysis. This analysis must evaluate implications across:

- Scope boundaries
- WBS structure
- Cost baseline
- Schedule baseline
- Risk exposure
- Security integrity
- Regulatory compliance
- Procurement commitments
- Operational readiness

Impact analysis must be documented in writing and reviewed by relevant subject matter experts before governance evaluation.

Following impact analysis, the change request must be reviewed by the Change Control Board (CCB). The CCB assesses whether the change aligns with strategic objectives, financial capacity, technical feasibility, and risk tolerance. The Board may approve, reject, defer, or request additional analysis.

If the proposed change has strategic implications—such as altering project objectives, affecting major funding allocations, or impacting national policy alignment—Executive Sponsor approval is required.

If the proposed change affects security architecture, classified systems, physical protection layers, cybersecurity mechanisms, or access control protocols, approval from the Security Board is mandatory before CCB decision finalization.

No change may be implemented until formal written approval is issued and documented. Upon approval, the following baseline components must be updated:

- Requirements Register
- Requirements Traceability Matrix
- Scope Statement (if applicable)
- WBS and WBS Dictionary (if impacted)
- Cost Baseline
- Schedule Baseline
- Risk Register
- Benefits Tracking Framework
- Technical Specifications
- Interface Control Documents

Baseline updates must follow configuration management procedures, including version control, approval signatures, and distribution control.

All rejected changes must be documented with rationale to maintain transparency and historical traceability. Deferred changes may be reconsidered at future stage-gate reviews.

Emergency changes, if required due to regulatory mandate or critical security vulnerability, must follow expedited governance review procedures while maintaining documentation integrity.

No informal additions are allowed under any circumstance. Unauthorized implementation of requirement changes constitutes a governance violation and may result in corrective action.

Periodic audits of requirement changes must be conducted to monitor change frequency trends. Excessive or poorly justified changes may trigger governance review to assess stability of initial requirement definition.

Through structured change control, the NCPBF Project protects baseline stability, preserves financial discipline, maintains security integrity, and safeguards long-term value realization.

Requirements stability is essential to predictable delivery.
Predictable delivery is essential to national trust.

11. Integration with Other Domains:

Requirements management does not operate as an isolated discipline within the NCPBF Project. It functions as a central integration mechanism connecting strategic intent, scope definition, cost planning, schedule development, risk management, security governance, procurement control, stakeholder engagement, and benefits realization. Effective integration ensures coherence across all management domains and prevents fragmentation of decision-making.

Integration with Scope Management is foundational. Every approved requirement must be reflected within the Scope Statement, decomposed into the Work Breakdown Structure (WBS), and further clarified in the WBS Dictionary. Scope elements without corresponding requirements are not authorized, and requirements without scope representation cannot be implemented. This bidirectional alignment ensures boundary control and protects against scope creep.

Integration with Schedule Management ensures that requirements are translated into executable activities within the project timeline. Milestones such as design approval, procurement freeze, system integration, testing cycles, and commissioning reviews must explicitly reference requirement verification checkpoints. Requirements that lack schedule representation risk delayed implementation and operational gaps.

Integration with Cost Management ensures financial discipline. Budget allocations must trace back to validated requirements. Cost estimates, procurement packages, and contingency reserves must reflect the financial implications of approved requirements. Any requirement change must trigger reassessment of cost baselines to maintain fiscal integrity.

Integration with Risk Management ensures proactive control of uncertainty. Each requirement must be assessed for associated risks, including technical feasibility risk, integration risk, vendor dependency risk, compliance exposure, and security vulnerability. The Risk Register must reference requirement identifiers where applicable. Conversely, high-risk areas may generate new requirements aimed at mitigation.

Integration with Security Governance is critical given the national sensitivity of the project. Security-related requirements must be aligned with the Security Specification Addendum, physical protection architecture, cybersecurity protocols, and incident response frameworks. Security controls must not be modified without synchronized requirement updates and formal approval.

Integration with Procurement and Contract Management ensures that contractual obligations reflect validated requirements. Technical specifications, performance guarantees, acceptance criteria, and service-level agreements must be derived from approved requirement documentation. This alignment reduces ambiguity, vendor disputes, and performance misinterpretation.

Integration with Stakeholder Engagement ensures transparent communication of requirement expectations, validation decisions, prioritization outcomes, and change approvals. Stakeholders must understand how their inputs are evaluated and governed.

Integration with Benefits Management ensures that requirements contribute directly to defined outcomes. Each major requirement must map to at least one measurable benefit and performance indicator. Requirements that do not contribute to benefit realization must undergo strategic justification review.

Integration with Governance Framework ensures that requirement decisions are reviewed at appropriate authority levels. Escalation pathways, approval thresholds, and decision accountability structures must be respected.

Through systematic integration across domains, requirements management becomes the structural backbone of the project's control system. It ensures alignment between intent and execution, policy and implementation, funding and performance, and security and operation.

This integrated approach enhances predictability, reduces rework, strengthens audit readiness, and ensures that the NCPBF Project delivers secure, compliant, and value-driven outcomes.

12. Tools & Systems:

Effective requirements management within a complex and security-sensitive project requires structured technological support. Tools and systems must enable control, traceability, access management, version integrity, collaboration, and audit transparency while maintaining strict security protocols.

The project will implement a Controlled Document Management Platform as the primary repository for all requirements-related documentation. This platform must support version control, approval workflows, digital signatures, access-level restrictions, and full audit trails. Each document revision must be recorded with timestamp, author identification, and approval authority.

A Version-Controlled Specification Repository will store all technical specifications, security addendums, interface control documents, and design artifacts. This repository ensures that engineering teams, security authorities, and procurement specialists reference the most current and approved versions. Obsolete versions must be archived but remain retrievable for audit and traceability purposes.

A Centralized Requirements Traceability Matrix (RTM) system will serve as the core integration engine. The RTM must allow dynamic linking between requirement IDs, WBS components, risk entries, cost allocations, schedule activities, test cases, and acceptance records. The system must support filtering, reporting, and impact analysis queries.

A Secure Collaboration Portal will facilitate controlled stakeholder communication, workshop documentation, requirement review cycles, and validation discussions. The portal must incorporate encryption, role-based access control, and secure data transmission protocols.

An Access-Controlled Requirements Database will function as the master record for requirement lifecycle management. It must include structured fields for requirement attributes, status tracking, prioritization classification, ownership assignment, governance approval history, and change references.

All tools must integrate with configuration management procedures to ensure baseline protection. Automated alerts should notify relevant authorities of pending approvals, expiring reviews, or unlinked requirements.

Data integrity must be maintained through regular system audits, backup protocols, disaster recovery planning, and restricted administrative access. Security-sensitive requirements must be stored in encrypted formats with limited distribution rights.

Tool selection must consider scalability, cybersecurity resilience, audit functionality, integration capability with cost and schedule systems, and compatibility with procurement platforms.

Periodic system health checks must confirm that tools are functioning correctly and that traceability links remain intact. Any tool failure or data inconsistency must be treated as a governance risk.

Through disciplined use of structured tools and systems, the NCPBF Project ensures requirement integrity, data accuracy, process transparency, and long-term documentation sustainability.

13. Requirements Validation & Verification:

Requirements Validation and Verification are distinct but complementary control mechanisms within the NCPBF Project. Together, they ensure that the project defines the correct requirements and implements them correctly. These controls protect the project from misalignment, rework, compliance gaps, security vulnerabilities, and operational instability.

Validation confirms that the right requirement is defined. It ensures that the documented requirement accurately reflects stakeholder intent, regulatory mandates, operational necessity, and strategic objectives. Validation occurs before or during requirement baseline integration and is focused on correctness of definition.

Verification confirms that the requirement is correctly implemented. It ensures that the delivered product, system, facility component, or process meets the defined requirement and acceptance criteria. Verification occurs during and after implementation and is focused on performance confirmation.

Validation is concerned with “Are we defining the right need?”
Verification is concerned with “Have we built it correctly?”

Validation activities must involve authorized stakeholders, subject matter experts, regulatory representatives, security authorities, and operational leaders, depending on requirement classification. Every requirement must be reviewed for clarity, feasibility, necessity, compliance alignment, and measurable acceptance criteria before being approved.

Verification activities must be documented, measurable, repeatable, and auditable. No requirement may be considered complete without formal evidence of verification and authorized acceptance.

The following structured methods are adopted for validation and verification.

Inspections

Inspections involve structured examination of deliverables, system components, documentation artifacts, or constructed elements to confirm compliance with defined requirements. Inspections may be physical (e.g., vault door thickness

measurement), technical (e.g., network encryption configuration review), or documentary (e.g., compliance certificate verification).

Inspection protocols must reference requirement IDs and acceptance criteria. Findings must be documented in formal inspection reports. Non-conformances must be logged in the Issue Log and resolved before acceptance.

Inspections are particularly critical for security architecture, regulatory compliance components, structural reinforcements, and production equipment installation.

Walkthroughs

Walkthroughs involve guided review sessions where subject matter experts examine design artifacts, process models, system configurations, or operational procedures against documented requirements.

Walkthroughs are especially useful during design phases and prior to procurement freeze. They provide early detection of requirement misinterpretation and reduce downstream rework.

Walkthrough records must include participant lists, reviewed requirement references, identified discrepancies, and resolution actions. Walkthrough outcomes may result in refinement prior to baseline freeze.

Testing

Testing confirms that implemented systems perform according to defined functional and non-functional requirements. Testing includes functional testing, performance testing, stress testing, security testing, integration testing, and system acceptance testing.

Each test case must reference the corresponding requirement ID and acceptance threshold. Testing protocols must define measurable pass/fail criteria. Test results must be documented in a controlled repository and linked within the Requirements Traceability Matrix.

Testing is mandatory for IT systems, monitoring platforms, security controls, and production equipment calibration.

User Acceptance Validation

User Acceptance Validation confirms that implemented systems meet operational needs and usability expectations. Operational managers and authorized users review the delivered capability in simulated or real operational environments.

User acceptance must reference defined acceptance criteria. Feedback must be documented formally. Conditional acceptance must specify required corrective actions before final sign-off.

This method ensures operational readiness and supports smooth transition to steady-state operation.

Commissioning Verification

Commissioning verification is the final structured confirmation that integrated systems, facility infrastructure, production lines, and security controls function collectively according to defined requirements.

Commissioning includes end-to-end system testing, integrated workflow simulation, emergency scenario exercises, throughput validation, compliance audits, and final security clearance confirmation.

Commissioning verification must demonstrate that all requirements—strategic, regulatory, security, technical, and operational—have been satisfied before final acceptance and handover.

No deliverable may be considered complete without documented validation and verification evidence. The Requirements Register and RTM must be updated to reflect verification status.

Through disciplined validation and verification, the NCPBF Project ensures requirement accuracy, implementation integrity, compliance adherence, and operational readiness.

14. Requirements Success Criteria:

The Requirements Management System is considered successful when it consistently demonstrates stability, traceability, governance discipline, and value alignment throughout the project lifecycle.

Success is first measured by the absence of untraceable requirements. Every requirement must be linked to design, scope, cost, schedule, risk, testing, and benefit realization. Broken traceability chains indicate governance weakness and must trigger corrective review.

Another success indicator is the absence of unauthorized requirement implementation. No deliverable, feature, system component, or facility modification may exist without documented approval and baseline integration. Informal additions represent control failure and undermine configuration integrity.

The system is also successful if commissioning occurs without rework attributable to missing or misunderstood requirements. Rework at commissioning stage indicates inadequate early validation, incomplete traceability, or poor change control discipline. Stability at commissioning reflects strong upstream governance.

All regulatory and security requirements must be fully satisfied prior to operational activation. Compliance certificates, security clearances, and audit confirmations must demonstrate complete requirement fulfillment. Any unresolved regulatory or security requirement represents unacceptable risk.

Requirements stability prior to construction and procurement freeze is another key performance indicator. Significant requirement volatility during or after freeze milestones indicates inadequate early definition and threatens cost and schedule predictability.

Additional success indicators include:

- Controlled change frequency within predefined governance thresholds
- High percentage of first-time acceptance at inspection and testing stages
- Zero critical security deficiencies identified during final audit
- Full alignment between requirements and approved benefits
- Clear audit trail demonstrating approval authority and impact analysis

Periodic performance reviews must assess requirement change trends, traceability integrity, and validation effectiveness. Excessive changes or traceability gaps may trigger governance escalation.

The ultimate measure of success is predictable delivery of a secure, compliant, operationally ready facility without scope instability or uncontrolled requirement expansion.

A disciplined Requirements Management System ensures:

- Strategic alignment
- Financial control
- Risk containment
- Security integrity
- Operational readiness
- Sustainable value realization

When requirements remain controlled, integrated, validated, and verified, the project delivers not only outputs but trusted outcomes.

REQUIREMENTS TRACEABILITY MATRIX (RTM) TEMPLATE:

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

Document Type: Requirements Traceability Matrix

Version:

Configuration Status: Draft / Approved / Baselined

Prepared By:

Approved By:

Last Updated:

MASTER TRACEABILITY TABLE:

Req ID	Requirement Description	Category	Strategic Objective Ref	Benefit ID	KPI Ref	Scope Ref	WBS ID	Cost Account	Schedule Activity ID	Risk ID	Design Doc Ref	Procurement Package	Test Case ID	Acceptance Ref	Security Class	Status