RISK 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 Risk Management Plan is to establish a structured, systematic, and governance-aligned framework through which risks affecting the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) are identified, analyzed, prioritized, addressed, monitored, escalated, and documented throughout the entire project lifecycle. This plan defines not only the processes for managing uncertainty, but also the accountability structures, authority boundaries, reporting mechanisms, and escalation paths required to ensure that risk exposure remains within approved tolerance levels and aligned with strategic objectives.

The NCPBF project represents a strategic national infrastructure initiative involving secure facility development, specialized machinery procurement, cybersecurity systems integration, operational readiness preparation, and long-term institutional capability transfer. Due to its high level of security sensitivity, extended duration, multi-phase execution roadmap, and multi-layered governance structure, the project operates within a risk environment that is materially more complex than conventional infrastructure or technology projects. As such, unmanaged or poorly governed risks could lead to severe consequences not only for project performance, but also for national security, financial stewardship, regulatory compliance, and institutional reputation.

In this context, unmanaged risk represents a direct and significant threat to:

- National security and confidentiality of secure production systems
- Schedule performance across critical design, construction, and integration milestones
- Cost containment and approved budget baselines
- Operational readiness and commissioning stability
- Long-term benefits realization and sovereign capability transfer
- Institutional credibility, audit transparency, and governance integrity

Accordingly, this Risk Management Plan ensures that risk management is treated as a core governance discipline rather than a reactive or administrative activity. Risk management is embedded into decision-making, change control, stage-gate approvals, procurement oversight, security governance, and executive reporting processes. Every major decision within the project must consider risk implications

before approval, and no phase transition may proceed without formal risk review and documentation.

This plan establishes a proactive risk management philosophy. Rather than responding to issues after they materialize, the project commits to early identification of potential threats and opportunities, structured assessment of their likelihood and impact, and disciplined implementation of mitigation and contingency measures. The intent is to reduce uncertainty, increase predictability, and protect both tangible and intangible project assets. Risk management activities are therefore continuous and integrated across all phases defined in the approved Project Roadmap, from Authorization and Mobilization through Operational Handover and Closure.

The purpose of this plan also extends to protecting governance integrity. In complex and high-visibility projects, risk often emerges not only from technical or operational factors, but from informal decision-making, unclear authority boundaries, or bypassed controls. This Risk Management Plan reinforces that all risk responses must operate within the approved governance hierarchy (Sponsor → Steering Committee → PMO → Project Manager) and must respect segregation-of-duties principles and security clearance requirements. No risk response may contradict formal approval processes, contractual obligations, or information classification policies.

Another central purpose of this plan is to ensure informed executive oversight. By providing standardized risk scoring methodologies, structured risk registers, escalation thresholds, and consolidated reporting dashboards, the plan enables senior leadership to make evidence-based decisions. Risks are categorized, quantified where necessary, and trended over time to support proactive intervention. High and critical risks are automatically elevated to appropriate governance bodies to ensure transparency and timely resolution.

Furthermore, the Risk Management Plan supports long-term sustainability and operational transition. Because the NCPBF project is designed not merely to deliver infrastructure but to transfer secure operational capability, risk management must address knowledge transfer gaps, vendor dependency exposure, institutional readiness, and continuity planning. Risk identification therefore extends beyond construction and installation phases into commissioning, trial production, and

operational stabilization. This ensures that residual risks are minimized prior to formal handover to Operations Management.

Security sensitivity is also central to the purpose of this plan. The project involves protected systems, secure facilities, sensitive technical designs, and restricted operational data. Therefore, security-related risks are treated with elevated priority, subject to enhanced oversight, and governed through formal information classification and access control mechanisms. Risk documentation itself must adhere to approved security protocols to prevent exposure of sensitive vulnerabilities.

Finally, this Risk Management Plan serves as a cultural foundation for disciplined project execution. It promotes transparency in reporting risk exposure, encourages early escalation without fear of penalty, and reinforces professional accountability. All project participants—whether internal staff, contractors, consultants, or vendors—are expected to actively participate in identifying and managing risks within their areas of responsibility. Risk ownership is clearly assigned, and closure of risks requires documented evidence and PMO approval.

In summary, the purpose of this Risk Management Plan is to:

- Establish a disciplined, repeatable, and auditable risk management framework
- Protect strategic, financial, security, and operational interests
- Embed risk thinking into governance and decision-making
- Enable proactive mitigation rather than reactive correction
- Maintain risk exposure within approved tolerance levels
- Safeguard institutional credibility and long-term benefits realization

Through this structured approach, the NCPBF project strengthens its resilience against uncertainty and ensures that risk management contributes directly to secure, controlled, and successful project delivery.

2. Risk Management Objectives:

The objectives of risk management for the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) are to establish a proactive, disciplined, and governance-aligned approach to managing uncertainty in a manner that safeguards strategic outcomes, protects sensitive assets, and supports successful project delivery across all phases of execution.

First, risk management aims to proactively identify threats and opportunities throughout the entire project lifecycle—from authorization and planning through construction, integration, commissioning, and operational handover. Risk identification is not treated as a one-time workshop activity, but as a continuous process embedded within planning sessions, design reviews, procurement evaluations, security assessments, stage-gate reviews, and executive reporting cycles. This ensures early visibility of emerging risks before they escalate into material issues.

Second, the plan seeks to systematically reduce uncertainty affecting scope, schedule, cost, security, quality, and operational readiness. By applying structured qualitative and, where appropriate, quantitative analysis methods, the project assesses the likelihood and impact of identified risks and prioritizes them based on exposure level. This structured prioritization enables resources to be focused on high-impact risks, thereby improving predictability and stability across key performance baselines.

A core objective of this plan is to prevent governance breaches and informal decision-making. In complex and high-security projects, risk often emerges not only from technical factors but from bypassed controls, unclear authority boundaries, or undocumented commitments. Risk management is therefore integrated into formal governance processes, reinforcing that no significant decision, scope adjustment, or contractual modification may occur without documented risk assessment and approval through the established hierarchy.

Protecting sensitive information and critical infrastructure is another fundamental objective. Given the security-sensitive nature of the NCPBF project, risk management explicitly addresses threats related to physical security, cybersecurity, insider risk, data confidentiality, and system integrity. All security-

related risks are treated with heightened scrutiny and aligned with access control, segregation-of-duties, and information classification policies.

The plan also supports informed executive decision-making. By consolidating risk data into structured registers, dashboards, and escalation reports, senior leadership receives clear, evidence-based visibility of risk exposure, trends, mitigation status, and residual impact. This transparency strengthens strategic oversight and enables timely intervention when risk thresholds are approached or exceeded.

Furthermore, risk management is fully integrated with change control and issue management processes. Proposed changes are evaluated for risk impact prior to approval, and realized risks that materialize into issues are transitioned into the Issue Log for active resolution. This integration prevents fragmentation of control systems and ensures traceability from risk identification through resolution.

Finally, the objectives of risk management extend beyond project completion to support smooth operational transition and sustainable benefits realization. By identifying risks related to knowledge transfer, vendor dependency, operational readiness, and institutional capacity, the project ensures that residual exposure is minimized before handover and that long-term value is protected.

Collectively, these objectives position risk management as a strategic enabler of secure, disciplined, and resilient project delivery rather than a reactive compliance exercise.

3. Risk Governance Structure:

3.1 Oversight Roles:

Role	Responsibility in Risk Management
Project Sponsor	Receives escalated critical risks; approves major response strategies
Steering Committee	Reviews high and strategic risks; approves risk tolerance levels
PMO	Defines standards, assures compliance, monitors risk trends
Project Manager	Accountable for risk management execution
Risk Manager	Facilitates identification, analysis, and monitoring
Workstream Leads	Own risk identification and mitigation within their areas
Security Board	Reviews all security-related risks
Finance Manager	Oversees financial risk exposure

3.2 Escalation Thresholds:

To ensure disciplined governance and timely executive oversight, clearly defined escalation thresholds are established for the National Currency Printing and Secure Banknote Production Facility Project (NCPBF). These thresholds determine when risks must be elevated beyond the project team to higher levels of authority for visibility, decision-making, or intervention.

Risks assessed as **High** (Risk Score ≥ 16 based on the approved probability–impact matrix) require formal visibility at the Steering Committee level. Such risks represent material exposure to schedule, cost, security, compliance, or strategic objectives and therefore demand executive awareness and, where necessary, direction on response strategies or tolerance levels.

All **security-related risks**, regardless of overall score, must be reviewed by the Security Board. Given the sensitive nature of the project—including secure facility design, protected systems, and restricted information—security risks receive

enhanced scrutiny and cannot be managed solely within the delivery team. This ensures alignment with information classification rules, access control policies, and national security safeguards.

Where a risk results in **financial exposure exceeding approved tolerance levels**—including potential cost overruns beyond contingency reserves or significant claims exposure—the Project Sponsor must be formally notified. Financial risks at this level may affect funding confidence, reserve allocation, or baseline approval and therefore require sponsor-level awareness and potential decision.

Risks that threaten **stage-gate readiness or phase transition approval** must be resolved, mitigated to an acceptable level, or formally accepted before proceeding to the next phase. No stage gate may advance if unresolved risks materially compromise scope integrity, security compliance, operational readiness, or governance requirements. Pre-gate risk review is therefore mandatory as part of the readiness validation process.

These escalation thresholds reinforce transparency, accountability, and disciplined decision-making, ensuring that material risks are addressed at the appropriate authority level in a timely and controlled manner.

---

4. Risk Management Approach:

Risk management will follow the structured process:

1. Plan Risk Management
2. Identify Risks
3. Perform Qualitative Risk Analysis
4. Perform Quantitative Risk Analysis (where applicable)
5. Plan Risk Responses
6. Implement Risk Responses
7. Monitor and Control Risks

This approach is applied continuously across all roadmap phases.

---

5. Risk Categories (Risk Breakdown Structure – RBS):

Risks are categorized as:

- Strategic & Governance Risks
- Schedule Risks
- Cost & Financial Risks
- Security & Cyber Risks
- Operational Readiness Risks
- Resource & Capability Risks
- Vendor & Commercial Risks
- Regulatory & Compliance Risks
- Environmental & HSE Risks
- Integration & Technical Risks

This structured categorization supports traceability and trend analysis.

---

6. Risk Identification:

Risk identification for the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) is conducted through a structured, continuous, and multi-layered approach designed to ensure comprehensive visibility of threats and opportunities throughout the entire project lifecycle. Given the project's strategic national importance, high security sensitivity, technical complexity, multi-phase roadmap, and governance intensity, risk identification is not treated as a periodic activity but as an embedded management discipline integrated into planning, execution, assurance, and oversight processes.

The objective of risk identification is to systematically recognize potential events, conditions, vulnerabilities, or uncertainties that could positively or negatively affect project objectives, including scope, schedule, cost, quality, security, compliance, operational readiness, and benefits realization. Risk identification also supports early detection of governance gaps, security weaknesses, integration conflicts, vendor dependency exposures, and institutional readiness challenges.

Risk identification activities are conducted at multiple levels and through structured forums, as described below.

6.1 Phase Planning Workshops:

At the beginning of each major roadmap phase—including planning, secure facility design, construction, machinery procurement, integration, testing, commissioning, and operational transition—structured risk identification workshops are conducted. These workshops are facilitated by the Risk Manager or PMO and involve relevant Workstream Leads, technical experts, commercial representatives, security personnel, and operational stakeholders.

The purpose of these workshops is to:

- Identify phase-specific technical, commercial, schedule, and security risks
- Assess interface dependencies between workstreams
- Evaluate resource constraints and capacity risks
- Detect potential regulatory or compliance exposure
- Identify risks introduced by external factors or environmental conditions

Risk identification during phase planning is forward-looking and scenario-based. Participants are encouraged to evaluate "what could go wrong," "what assumptions may fail," and "where dependencies create vulnerability." Structured techniques such as brainstorming, assumption analysis, interface mapping, and dependency analysis are applied to ensure completeness.

All identified risks are formally recorded in the Risk Register with a clear description, root cause, potential impact, and proposed ownership.

6.2 Stage-Gate Readiness Reviews:

Risk identification is a mandatory component of every stage-gate readiness review. Prior to requesting formal approval to transition to the next phase, the project team conducts a comprehensive risk assessment to determine whether any residual or emerging risks could materially compromise the integrity of the next phase.

Stage-gate risk identification focuses on:

- Residual design uncertainties
- Unresolved integration risks
- Incomplete compliance or regulatory conditions
- Security exposure prior to system activation
- Readiness of operational staff
- Vendor performance gaps
- Contractual ambiguities

No phase may proceed without formal documentation of risk status. If risks exceed approved tolerance thresholds, mitigation or formal acceptance must occur before transition approval. This ensures that phase progression does not conceal or transfer unmanaged exposure into subsequent phases.

6.3 Security Assessments:

Given the high-security nature of the NCPBF project, risk identification includes dedicated security assessment activities. These assessments are conducted in coordination with the Security Manager, CISO, and Security Board.

Security risk identification includes:

- Physical security vulnerability assessments

- Cybersecurity threat modeling
- Access control audits
- Insider threat evaluations
- System penetration testing
- Information classification reviews

Security risks are identified regardless of overall project risk score and are subject to enhanced documentation controls. Security assessments are conducted periodically and prior to commissioning, system activation, and operational handover.

Security-related risks are recorded in the Risk Register and may also be tracked within restricted security risk logs where classification requirements apply.

6.4 Vendor and Commercial Risk Reviews:

Vendor performance and contractual exposure represent significant risk sources in multi-year infrastructure and systems projects. Risk identification therefore includes structured vendor risk reviews at key points:

- During procurement planning
- During bid evaluation
- At contract award
- During periodic performance reviews
- When change orders are proposed

Vendor risk identification focuses on:

- Financial stability of suppliers
- Supply chain vulnerability
- Single-source dependency
- Contractual ambiguity
- Claims exposure
- Performance capacity
- Delivery schedule reliability
- Technology obsolescence

Commercial and procurement representatives collaborate with Workstream Leads and the PMO to ensure vendor-related risks are captured, assessed, and mitigated proactively.

6.5 Design and Integration Workshops:

Due to the technical complexity of secure facility construction, printing machinery installation, IT system integration, and cybersecurity controls, risk identification includes structured design and integration workshops.

These workshops examine:

- Interface compatibility between systems
- Infrastructure dependencies
- Data flow vulnerabilities
- Testing sequence risks
- Interoperability gaps
- Capacity assumptions
- Environmental and load constraints

Integration risk identification is particularly critical prior to Factory Acceptance Testing (FAT), Site Acceptance Testing (SAT), and system commissioning. Early detection of integration vulnerabilities significantly reduces rework risk and schedule delay.

6.6 Stakeholder Engagement Sessions:

Stakeholder engagement is another structured source of risk identification. Executive stakeholders, governance bodies, operations leadership, and oversight authorities may identify risks not visible at the technical level.

Through structured engagement sessions, the project identifies:

- Strategic alignment risks
- Funding confidence concerns
- Regulatory sensitivities
- Political or reputational exposure
- Institutional resistance
- Operational readiness gaps

Feedback from stakeholder sessions is formally documented and evaluated for risk implications. Informal concerns are not ignored; they are analyzed and, where appropriate, converted into documented risks.

6.7 Lessons Learned Reviews:

Risk identification incorporates continuous learning from:

- Internal project milestones
- Audit findings
- Security incidents
- Vendor performance observations
- Comparable industry projects

Lessons learned are analyzed for patterns of failure, recurring weaknesses, or systemic vulnerabilities. Where relevant, risks are created or updated in the Risk Register to prevent recurrence.

Lessons learned reviews occur:

- At phase closure
- After major testing events
- Following issue resolution
- At project closure

This feedback loop strengthens institutional resilience and reduces repeated exposure.

6.8 Audit and Assurance Observations:

Internal audit, external audit, and PMO assurance activities frequently identify areas of control weakness, documentation gaps, or governance vulnerabilities. These observations are evaluated for potential risk exposure.

Where audit findings indicate systemic vulnerability, new risks are recorded in the Risk Register, even if no immediate issue has occurred. This proactive approach prevents escalation of minor control weaknesses into major governance failures.

6.9 Documentation and Control Requirements:

All identified risks—regardless of source—must be formally recorded in the approved Risk Register. Each risk entry must include:

- Unique Risk ID
- Clear description
- Root cause

- Potential impact
- Risk owner
- Initial qualitative assessment
- Proposed response strategy

No informal risk tracking is permitted outside the controlled Risk Register. Personal spreadsheets, email-based tracking, or undocumented risk lists are strictly prohibited. This ensures:

- Traceability
- Audit readiness
- Governance transparency
- Consistent prioritization
- Integrated reporting

The Risk Register is maintained under configuration control and reviewed regularly by the PMO.

6.10 Continuous Identification:

Risk identification is not limited to scheduled workshops. All project participants—internal staff, contractors, consultants, and vendors—are expected to proactively report emerging risks within their areas of responsibility.

A culture of transparency is promoted, where early reporting of risk is encouraged and not penalized. Timely identification strengthens control and reduces reactive crisis management.

7. Risk Analysis:

7.1 Qualitative Risk Analysis:

Each risk is evaluated using:

- Probability (1–5)
- Impact (1–5)
- Risk Score = Probability × Impact

Risk Levels:

- High: ≥16
- Medium: 9–15
- Low: ≤8

Impact is evaluated across:

- Schedule
- Cost
- Security
- Compliance
- Reputation
- Operational readiness

Probability/Impact	1	2	3	4	5
5	5 (Low)	10 (Medium)	15 (Medium)	20 (High)	25 (High)
4	4 (Low)	8 (Low)	12 (Medium)	16 (High)	20 (High)
3	3 (Low)	6 (Low)	9 (Medium)	12 (Medium)	15 (Medium)
2	2 (Low)	4 (Low)	6 (Low)	8 (Low)	10 (Medium)
1	1 (Low)	2 (Low)	3 (Low)	4 (Low)	5 (Low)

7.2 Quantitative Risk Analysis:

Quantitative analysis is performed for:

- Major schedule risks
- Financial exposure risks

- Commissioning readiness risks
- Contingency reserve validation

Tools may include:

- Monte Carlo schedule simulations
- Sensitivity analysis
- Contingency estimation models

Quantitative analysis is coordinated by PMO Controls.

---

8. Risk Response Strategies:

Threat response strategies include:

- Avoid
- Mitigate
- Transfer
- Accept

Opportunity response strategies include:

- Exploit
- Enhance
- Share
- Accept

All response plans must:

- Have a named risk owner
- Include measurable mitigation actions
- Be integrated into the schedule
- Be budgeted if necessary
- Be traceable and auditable

9. Integration with Governance:

Risk management for the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) is fully embedded within the project's governance framework and is not treated as a standalone control activity. It operates as an integrated discipline that informs decision-making, protects strategic objectives, and ensures accountability across all levels of authority. The effectiveness of risk management depends on its structured alignment with established governance mechanisms, including change control, issue management, executive reporting, resource allocation, security oversight, and benefits realization.

Risk management is directly integrated with the **Change Control Process**. Every proposed change—whether related to scope, schedule, cost, technical design, procurement strategy, or security configuration—must undergo formal risk impact analysis prior to approval. The analysis must assess potential exposure across schedule, financial reserves, compliance obligations, operational readiness, and security sensitivity. No change request may be presented to the Change Control Board (CCB) or Steering Committee without documented risk assessment. This requirement prevents unintended consequences and ensures that governance bodies make informed decisions based on quantified exposure rather than assumptions.

Risk management is also tightly linked with **Issue Management**. Risks represent potential future events, while issues represent realized risks requiring immediate action. When a risk materializes, it is formally transferred from the Risk Register to the Issue Log, where it is managed through structured resolution procedures. Conversely, recurring issues may signal systemic vulnerabilities and trigger the creation of new risk entries. This bidirectional integration ensures continuity between preventive and corrective controls and avoids fragmented tracking systems.

The **Communication Plan** reinforces risk transparency by defining how risk information is reported, escalated, and reviewed. High and critical risks are included in executive dashboards and monthly PMO reporting. Risk trends, emerging threats, and mitigation status are presented in structured formats to ensure senior leadership maintains visibility of exposure levels. Security-related

risks are communicated through controlled channels consistent with information classification requirements.

Risk management is a mandatory component of **Stage-Gate Reviews**. Prior to any phase transition, the project team must present a comprehensive risk status summary, including unresolved high risks, mitigation effectiveness, contingency usage, and residual exposure. No stage gate may proceed without formal risk status review and documented acceptance of residual risks within approved tolerance thresholds. This requirement ensures that phase progression does not conceal or transfer unmanaged risk into subsequent stages.

Integration with **Resource Planning** ensures that mitigation strategies are supported by appropriate capacity, expertise, and authority. Identified risks may require additional staffing, specialized technical resources, or reallocation of effort. Risk exposure therefore directly influences workforce planning and competency management decisions.

Given the sensitive nature of the project, risk management operates in close coordination with **Security Oversight** mechanisms. All security-related risks are reviewed in alignment with the Security Board and must comply with access control, segregation-of-duties, and classification policies. Security risks are not subject to informal mitigation and must follow formal approval and documentation procedures.

Finally, risk management supports the **Benefits Management Plan** by identifying threats that could undermine long-term value realization, including knowledge transfer gaps, vendor dependency exposure, or operational readiness weaknesses. By proactively addressing such risks, the project protects both immediate delivery objectives and sustainable institutional capability.

In summary, risk management is embedded across governance processes to ensure disciplined decision-making, structured accountability, and continuous executive visibility. No change may be approved without documented risk impact analysis, and no stage gate may proceed without formal risk status review. This integration safeguards the project's strategic, financial, and security integrity throughout its lifecycle.

10. Security Risk Controls:

Given the strategic and security-sensitive nature of the National Currency Printing and Secure Banknote Production Facility Project (NCPBF), security risk management represents a critical control domain within the overall Risk Management Plan. The project involves secure facility design, controlled production systems, protected infrastructure, restricted technical specifications, and sensitive operational data. As such, security risks are treated with elevated priority, enhanced governance oversight, and structured control mechanisms beyond standard project risk practices.

All security-related risks are formally classified as **Restricted**, regardless of their qualitative risk score. This classification reflects the potential national, financial, reputational, and institutional consequences of security compromise. Restricted risks are documented within the approved Risk Register under controlled access protocols. Where necessary, detailed vulnerability information is maintained within secured annexes to prevent inadvertent exposure of sensitive system weaknesses.

Security risks are managed under the principle of **defense-in-depth**, ensuring that preventive, detective, and corrective controls operate simultaneously across physical, operational, and digital environments.

10.1 Role-Based Access Controls (RBAC):

Access to project information, systems, facilities, and risk documentation is strictly governed through **role-based access controls**. Access rights are assigned based on the principle of least privilege, meaning that individuals are granted only the minimum access necessary to perform their defined responsibilities.

Access control applies to:

- Design documentation and technical specifications
- Procurement and vendor data
- Secure system architecture
- Integration and cybersecurity configurations
- Risk registers containing security exposure details
- Testing and commissioning documentation

Access provisioning requires formal approval and security clearance verification where applicable. All access rights are time-bound and subject to periodic review.

Upon role change, completion of assignment, or termination, access privileges are immediately revoked in coordination with the Security Manager and Document Control Manager.

Unauthorized access attempts are logged, monitored, and investigated under approved incident management procedures.

10.2 Segregation of Duties:

To prevent fraud, error, unauthorized system manipulation, or concealment of security vulnerabilities, **segregation-of-duties (SoD)** is strictly enforced across all security-sensitive functions.

No individual may simultaneously:

- Design and approve the same security control
- Implement and verify the same system configuration
- Authorize and audit the same deliverable
- Approve access and perform independent security review

Segregation-of-duties principles apply to:

- Cybersecurity architecture and testing
- Physical access control configuration
- Procurement and vendor acceptance
- Security audit validation
- Change implementation and verification

These controls are embedded within governance procedures and reinforced through PMO oversight and internal audit monitoring.

10.3 Pre-Approved Incident Response Plans:

Given the potential severity of security incidents, **incident response plans are pre-approved** and validated before high-risk project phases begin. Incident response planning covers:

- Cybersecurity intrusion
- Data breach
- Unauthorized physical access
- Insider threat activity
- System compromise

- Facility security breach

Each incident response plan defines:

- Escalation hierarchy
- Communication protocols
- Containment procedures
- Evidence preservation requirements
- Recovery and restoration steps
- Post-incident review and corrective action processes

Incident response plans are tested through structured tabletop exercises and scenario simulations prior to commissioning and system activation. This proactive validation ensures that response teams can act swiftly and decisively under real-world conditions.

10.4 Penetration Testing and Vulnerability Assessments:

Penetration testing and vulnerability assessments are mandatory components of the project's security risk control framework. These assessments are conducted at key lifecycle milestones, including:

- Completion of system integration
- Prior to factory acceptance testing (FAT)
- Prior to site acceptance testing (SAT)
- Before system go-live
- Before operational handover

Testing is conducted by qualified and authorized cybersecurity professionals under controlled conditions. Identified vulnerabilities are documented, prioritized, and tracked through remediation plans before system approval. No critical vulnerability may remain unresolved prior to commissioning or activation.

In addition to cybersecurity testing, physical security vulnerability assessments are conducted to evaluate perimeter controls, surveillance systems, access mechanisms, and secure storage arrangements.

10.5 Monthly Security Risk Review:

Security risks are formally reviewed on a monthly basis, independent of standard project risk reviews. The Security Manager, CISO, PMO representative, and relevant technical leads participate in these structured reviews.

Monthly review activities include:

- Status update of identified security risks
- Validation of mitigation effectiveness
- Review of access control logs
- Assessment of new or emerging threat intelligence
- Monitoring of vendor security compliance
- Confirmation of segregation-of-duties adherence

High or critical security risks are escalated to the Security Board and, where necessary, to the Steering Committee. Security risks are never downgraded or closed without documented evidence of mitigation effectiveness and formal approval.

10.6 Continuous Monitoring and Cultural Reinforcement:

Security risk control extends beyond procedural enforcement; it is reinforced through cultural discipline. All team members, contractors, consultants, and vendors are required to:

- Acknowledge confidentiality commitments
- Complete security orientation training
- Report suspicious activity immediately
- Avoid informal sharing of sensitive information
- Comply strictly with approved communication channels

Security awareness is reinforced through onboarding sessions, periodic briefings, and controlled documentation practices.

11. Risk Monitoring and Reporting:

Risk monitoring and reporting for the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) is conducted through a structured, multi-layered governance framework designed to ensure continuous visibility, disciplined oversight, and informed executive decision-making. Given the project's strategic significance, extended duration, and security-sensitive nature, risk monitoring is treated as an ongoing control function rather than a periodic administrative exercise.

The objective of risk monitoring is to track identified risks, evaluate the effectiveness of mitigation measures, detect emerging threats, assess residual exposure, and ensure that risk levels remain within approved tolerance thresholds. Risk reporting supports transparency, accountability, and proactive intervention at the appropriate authority level.

11.1 Monitoring Mechanisms:

Risk monitoring occurs through the following structured mechanisms:

Monthly PMO Dashboards

The PMO consolidates risk information into a structured monthly dashboard that provides executive-level visibility of overall risk exposure. The dashboard includes:

- Distribution of risks by category (strategic, security, schedule, financial, operational, etc.)
- Breakdown by risk level (High, Medium, Low)
- Trend comparison against previous reporting periods
- Status of high and critical mitigation actions
- Contingency reserve utilization

The dashboard ensures that risk exposure is communicated in a concise, data-driven format suitable for Steering Committee and Sponsor review. Any deterioration in risk profile triggers additional analysis and potential escalation.

Bi-Weekly Risk Review Meetings:

The Project Manager and Risk Manager facilitate bi-weekly risk review sessions with Workstream Leads and key functional representatives. These meetings focus on operational-level risk management and include:

- Review of newly identified risks
- Status update on mitigation actions
- Validation of risk scoring
- Identification of interdependencies between risks
- Assessment of potential risk triggers

These sessions provide an early-warning mechanism, ensuring that risks are actively managed at the delivery level before escalation becomes necessary. Minutes of risk review meetings are documented and stored in the controlled repository.

Stage-Gate Risk Assessments:

Risk monitoring is a mandatory component of stage-gate readiness validation. Prior to each phase transition, a formal risk assessment is conducted to confirm:

- Status of all High and critical risks
- Residual exposure after mitigation
- Contingency reserve sufficiency
- Security readiness validation
- Operational readiness risk exposure

No stage gate may proceed without formal documentation of risk status and confirmation that remaining exposure is within acceptable tolerance levels. Where risks exceed thresholds, mitigation must be implemented or formally accepted by the appropriate authority.

Security Review Sessions:

Security-related risks are subject to additional monitoring through structured security review sessions conducted monthly or as required. These sessions involve the Security Manager, CISO, PMO representative, and relevant technical leads.

Security reviews assess:

- Effectiveness of access controls
- Status of vulnerability remediation
- Incident response readiness
- Emerging cyber or physical threat intelligence
- Vendor security compliance

Security risks are reported separately where classification requirements apply and are escalated to the Security Board when required.

Audit and Assurance Activities:

Internal audit, external audit, and PMO assurance reviews provide independent oversight of risk management effectiveness. Audit observations may:

- Validate risk control implementation
- Identify gaps in mitigation
- Highlight unrecorded exposure
- Trigger creation of new risk entries

Findings are incorporated into the Risk Register and tracked to closure. This independent validation strengthens governance credibility and ensures compliance with institutional standards.

11.2 Risk Reporting Content:

Structured risk reports are prepared monthly and at key governance milestones. Reports include, at a minimum:

Top 10 Risk Summary:

A ranked summary of the highest exposure risks based on score and impact severity. Each entry includes:

- Risk description
- Current score
- Mitigation status
- Risk owner
- Escalation level

This summary provides rapid executive visibility of material exposure.

Risk Trend Analysis:

Trend analysis compares current risk scores against previous reporting periods to identify:

- Increasing risk exposure
- Decreasing risk exposure
- Emerging clusters of risk

- Repeated or recurring risk themes

Trend analysis supports proactive management rather than reactive correction.

Newly Identified Risks:

A summary of all risks added during the reporting period, including:

- Description and category
- Initial scoring
- Assigned owner
- Planned response

This ensures transparency regarding emerging exposure.

Closed Risks:

Risks formally closed during the reporting period are listed with evidence of closure. Closure requires documented validation that:

- The risk is no longer relevant, or
- Mitigation has neutralized the exposure

Closed risks remain archived for audit traceability.

Escalated Risks:

Any risks escalated to:

- Steering Committee
- Sponsor
- Security Board

are clearly identified, including reason for escalation and required decision or action.

Contingency Usage Status:

Reporting includes:

- Current contingency reserve balance
- Approved drawdowns
- Pending contingency requests
- Forecast of remaining exposure

This ensures financial risk remains within approved tolerance levels.

11.3 Escalation and Accountability:

Risk monitoring reinforces accountability. Where mitigation actions are delayed or ineffective, the Risk Owner is required to provide corrective action plans. Persistent inaction or governance breaches may trigger escalation to the PMO or Steering Committee.

Risk reporting is not merely informational—it drives accountability, supports executive decision-making, and reinforces disciplined project execution.

11.4 Continuous Improvement:

Risk monitoring also supports continuous improvement. Lessons learned from realized risks, near-miss incidents, or mitigation failures are documented and integrated into future planning cycles. This feedback mechanism strengthens institutional resilience and reduces repeated exposure.

12. Contingency and Management Reserves:

To ensure disciplined financial and schedule control within the National Currency Printing and Secure Banknote Production Facility Project (NCPBF), structured reserve mechanisms are established to manage identified and unforeseen uncertainties. These reserves provide controlled flexibility while maintaining governance integrity, audit transparency, and executive oversight.

Contingency reserves are established to address identified risks that have been analyzed, quantified, and documented within the Risk Register. These reserves are embedded within approved cost and schedule baselines and are specifically allocated to manage known risk exposure. Contingency reserves may be applied to mitigate impacts arising from:

- Schedule risks, including construction delays, integration sequencing challenges, or extended testing cycles
- Cost variability resulting from material price fluctuations, approved change impacts, or scope clarification
- Vendor claims or contractual adjustments within defined tolerance thresholds
- Integration delays associated with system interoperability, commissioning complexity, or phased activation

Contingency reserves are not discretionary funds. They may only be utilized when a documented risk materializes and when mitigation actions require controlled financial or schedule adjustment. All drawdowns must be supported by:

- Reference to the specific Risk ID
- Quantified impact analysis
- Confirmation that mitigation strategies were applied
- Updated forecast reflecting residual exposure

Requests for contingency usage are reviewed by the Project Manager and PMO, and approval authority follows the delegated governance structure defined in the Project Governance Framework.

In contrast, **management reserves** are maintained at a higher governance level and are controlled directly by the Project Sponsor. Management reserves are intended to address unforeseen risks—events that could not reasonably have been

identified during planning or that exceed approved contingency thresholds. These reserves are not included within the cost performance baseline and therefore require formal sponsor-level authorization prior to use.

Drawdown of management reserves requires:

- Formal justification memorandum
- Risk impact explanation and exposure analysis
- Confirmation that contingency reserves are insufficient
- Steering Committee visibility (where applicable)

All reserve adjustments—whether contingency or management—must be documented, traceable, and reflected in updated project forecasts and dashboards. Unauthorized or informal reserve use is strictly prohibited.

Through this structured reserve framework, the NCPBF project ensures disciplined financial control, transparent governance oversight, and resilience against uncertainty while protecting strategic, security, and operational objectives.

13. Risk Documentation Standards:

To ensure consistency, traceability, audit readiness, and governance integrity, all risks within the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) must be documented in a structured and standardized format. Risk documentation is not optional or informal; it is a mandatory control requirement embedded within the project's governance framework.

Every risk recorded in the approved Risk Register must include the following minimum information fields:

- **Unique Risk ID** – A sequential, traceable identifier aligned with the approved numbering convention. This ensures no duplication, enables cross-referencing in reports, and supports audit traceability.
- **Clear Risk Description** – A concise but specific statement describing the uncertain event or condition, written in cause–event–impact format where applicable.
- **Root Cause** – Identification of the underlying source or driver of the risk (e.g., dependency, technical uncertainty, vendor capability gap, regulatory complexity, security vulnerability).
- **Impact Description** – Clear articulation of potential consequences across one or more impact dimensions, including schedule, cost, security, compliance, operational readiness, reputation, or benefits realization.
- **Probability and Impact Rating** – Documented qualitative scoring in accordance with the approved risk matrix.
- **Risk Owner** – Named individual with authority and accountability for monitoring, mitigation implementation, and reporting.
- **Mitigation Plan (Preventive Actions)** – Defined actions intended to reduce probability and/or impact prior to occurrence, including responsible parties and target completion dates.
- **Contingency Plan (Response Actions)** – Pre-defined corrective measures to be implemented if the risk materializes.
- **Current Status** – Active, Monitoring, Escalated, Mitigated, or Closed.
- **Escalation Level (if applicable)** – Indication of whether the risk requires Steering Committee, Sponsor, or Security Board visibility.

- **Closure Evidence** – Documented proof that the risk has been neutralized, transferred, accepted, or is no longer relevant. Closure requires formal validation and approval.

All risk records must be factual, clear, and written in professional language. Vague, speculative, or incomplete entries are not permitted. Risk documentation must reflect current reality and be updated following each risk review cycle.

The Risk Register is maintained under formal **configuration control** within the PMO-controlled repository. Version control, access rights, and change history tracking are enforced to ensure integrity and prevent unauthorized modification. No parallel or informal risk tracking tools are permitted outside the approved system.

Through disciplined documentation standards, the project ensures transparency, accountability, structured analysis, and defensible governance across the entire risk management lifecycle.

14. Risk Closure Criteria:

Risk closure within the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) is a controlled governance action and may not occur informally or without documented validation. Closure signifies that the risk no longer presents a credible exposure to the project's scope, schedule, cost, security, compliance, operational readiness, or benefits realization objectives.

A risk may be formally closed only when one or more of the following conditions are fully satisfied:

- **The triggering condition is no longer possible.** The underlying cause or dependency has been eliminated. For example, a design uncertainty may be resolved through final approval, a vendor risk may be neutralized through contract execution, or a regulatory exposure may be removed through formal authorization.
- **Mitigation actions have fully neutralized the exposure.** All approved preventive measures have been implemented, verified, and validated, and the residual risk falls within an acceptable tolerance level defined by the governance framework.
- **Risk transfer has been completed and contractually confirmed.** Where applicable, the risk has been formally transferred (e.g., through insurance, contractual allocation, or third-party guarantees), and documentation confirms the transfer.
- **The risk event has occurred and has been fully resolved as an issue.**
  If a risk materializes, it transitions to the Issue Log. Once corrective actions are implemented and verified, and no residual exposure remains, the original risk entry may be closed with reference to issue resolution evidence.

Closure requires documented evidence supporting the justification for removal. Evidence may include approved design documents, signed acceptance certificates, audit validation reports, contract amendments, security clearance confirmations, or performance verification results.

No risk may be marked as "Closed" solely due to time passage, reporting convenience, or absence of recent discussion.

Formal closure approval must be provided by the **PMO**, ensuring independent validation and governance oversight. The Risk Owner proposes closure; the PMO confirms adequacy of evidence before status change.

Closed risks remain archived within the controlled Risk Register to preserve full audit traceability, historical analysis capability, and lessons learned reference. Archived risks may be re-opened if circumstances change or exposure re-emerges.

This disciplined closure framework ensures accountability, prevents premature removal of exposure records, and maintains the integrity of the project's risk management system throughout its lifecycle.

15. Risk Culture and Accountability:

The National Currency Printing and Secure Banknote Production Facility Project (NCPBF) promotes a proactive, disciplined, and transparent risk culture as a foundational element of governance and project success. Risk management is not confined to the Risk Manager or PMO; it is a shared responsibility embedded across all roles, functions, and governance layers. Every team member, workstream lead, vendor representative, and oversight participant is accountable for identifying, communicating, and addressing risk exposure within their area of responsibility.

The project actively encourages **early reporting of risks**, including emerging uncertainties, near-miss events, and weak signals that may indicate future exposure. Individuals are expected to raise concerns promptly through approved reporting channels without delay. Early visibility allows mitigation to occur before escalation becomes necessary.

The project maintains a **no-penalty principle for raising risks in good faith**. Individuals who report legitimate concerns or potential vulnerabilities will not face adverse consequences for transparency. Concealment, however, is treated as a governance breach. This distinction reinforces psychological safety while maintaining accountability.

Transparency is mandatory. All identified risks must be documented in the approved Risk Register and managed through formal processes. Informal suppression, undocumented side agreements, or attempts to bypass governance review are strictly prohibited. Risk discussions must be fact-based, documented, and traceable.

Given the project's sensitivity, **security considerations override schedule or cost pressure.** No milestone, delivery target, or operational objective may justify compromising security controls or withholding risk information. Where conflict arises between timeline pressure and security exposure, security risk takes precedence and is escalated accordingly.

Leadership plays a critical role in reinforcing risk culture. The Project Manager and PMO demonstrate commitment through open discussion of risk exposure, data-driven reporting, and consistent enforcement of escalation protocols. Workstream Leads are responsible for cultivating the same discipline within their teams.

Risk accountability includes:

- Clear assignment of Risk Owners
- Active monitoring and mitigation execution
- Timely reporting of status changes
- Honest reassessment of probability and impact
- Escalation when exposure exceeds authority limits

A mature risk culture ensures that uncertainty is addressed proactively rather than reactively. By embedding shared accountability, encouraging transparency, and prioritizing security and governance integrity, the project safeguards its strategic objectives, operational readiness, and institutional credibility throughout the lifecycle.

16. Review and Maintenance:

The Risk Management Plan for the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) is a controlled governance document and is maintained as a living framework throughout the project lifecycle. Given the project's long duration, phased implementation structure, evolving security landscape, and multi-layered governance environment, periodic review and structured maintenance are mandatory to ensure continued relevance, effectiveness, and compliance.

This Risk Management Plan is formally reviewed on a **quarterly basis by the PMO**. The quarterly review evaluates:

- Alignment with the current Project Roadmap and phase status
- Adequacy of risk identification methods
- Effectiveness of escalation thresholds
- Consistency of risk scoring methodology
- Performance of mitigation and contingency mechanisms
- Integration with change control, issue management, and governance reporting

Findings from the quarterly review are documented and, where necessary, result in recommended updates to methodology, thresholds, reporting structures, or documentation standards.

In addition to periodic review, the plan is **reviewed prior to each major phase transition**. Stage-gate readiness assessments require confirmation that the risk management framework remains appropriate for the upcoming phase. For example, the transition from construction to integration or from commissioning to operations may introduce different categories of risk (e.g., cybersecurity exposure, operational dependency, vendor transition risk). The Risk Management Plan must be validated to ensure it adequately addresses these evolving exposures.

The plan is also subject to mandatory review and potential update following **significant governance, regulatory, organizational, or security changes**. This includes:

- Revisions to the Project Governance Framework

- Changes in Sponsor or Steering Committee authority structures
- Introduction of new regulatory or compliance requirements
- Major security incidents or threat landscape shifts
- Structural reorganization affecting reporting or authority lines

Any required modification to the Risk Management Plan must follow **formal change control procedures**. Updates are:

- Documented with version history
- Reviewed by the PMO
- Approved by the appropriate governance authority
- Communicated through approved channels
- Archived under configuration control

No informal amendments are permitted. All changes must be traceable and auditable to maintain governance integrity.

Through structured review and disciplined maintenance, the Risk Management Plan remains current, aligned with project realities, and fully integrated within the project's broader governance ecosystem, ensuring continuous protection of strategic, operational, financial, and security objectives.

Approval

This Risk Management Plan becomes effective upon approval by:

- Project Manager
- PMO Director
- Steering Committee