COMMUNICATION 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 of the Communication Management Plan:

The purpose of this Communication Management Plan is to establish a structured, disciplined, and secure framework for how project information will be planned, created, reviewed, approved, distributed, stored, retrieved, and controlled throughout the entire lifecycle of the National Currency Printing and Secure Banknote Production Facility Project (NCPBF). This plan defines what information will be communicated, to whom, by whom, in what format, through which channels, and at what frequency, ensuring consistency, accountability, and traceability in all project communications.

In full alignment with PMI and the PMBOK® Guide, this plan recognizes communication as a critical success factor for complex and high-risk projects. The NCPBF project involves multiple governance layers, specialized technical domains, external vendors, regulatory oversight, and strict security and confidentiality requirements. As such, unstructured or ad-hoc communication could lead to misalignment, unauthorized decisions, security exposure, rework, cost overruns, or delays. This plan ensures that communication supports—not undermines—project control and governance.

The Communication Management Plan ensures that the right information reaches the right stakeholders, at the right time, in the right level of detail, and through approved channels, enabling informed decision-making at all levels. Strategic stakeholders receive concise, decision-focused information, while operational teams receive detailed, execution-level data necessary for effective delivery. Sensitive and restricted information is managed through defined classification and access controls to protect confidentiality and national-level interests.

This plan also establishes clear escalation and decision-making pathways, ensuring that risks, issues, changes, and exceptions are communicated promptly and through the appropriate governance bodies. By defining formal communication routes and thresholds, the plan reduces ambiguity, prevents bypassing of controls, and supports timely resolution of challenges.

Furthermore, the plan promotes alignment between strategic intent and execution by ensuring that objectives defined in the Project Charter, Business Case, and Governance Framework are consistently reflected in progress reporting, performance dashboards, and stage-gate reviews. Consistent reporting across all

governance layers enables transparency, comparability, and accountability, allowing the PMO and executive leadership to maintain effective oversight.

Finally, this Communication Management Plan aims to reduce misunderstandings, rework, and delays by standardizing communication formats, clarifying responsibilities, and establishing a single source of truth for project information. By doing so, it strengthens collaboration, enhances trust among stakeholders, and contributes directly to successful project delivery.

The Communication Management Plan is a living document, governed by formal change control and reviewed periodically to ensure it remains fit-for-purpose as the project evolves.

2. Communication Objectives:

The key objectives of project communications for the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) are to establish a clear, reliable, and secure flow of information that enables effective governance, informed decision-making, and coordinated execution throughout the project lifecycle. In accordance with PMI and PMBOK® Guide principles, communication is treated as a strategic management function that directly supports value delivery and risk control.

First, project communications are designed to ensure continuous alignment with the approved Project Charter and Business Case. All formal communications, reports, and governance updates are structured to reflect the project's authorized objectives, scope, assumptions, constraints, and success criteria. This alignment ensures that execution activities remain focused on delivering the intended strategic and operational outcomes and prevents scope drift or misinterpretation of project intent.

Second, communications support effective governance, oversight, and assurance by providing accurate, timely, and decision-oriented information to governance bodies. Standardized reporting and dashboards enable the Project Sponsor, Steering Committee, and PMO to monitor performance, assess risks, and exercise control without becoming involved in day-to-day management. Independent assurance communications further strengthen accountability and transparency.

Third, a core objective is to enable timely escalation of risks, issues, and decisions. The communication framework defines clear escalation paths, thresholds, and response timelines so that emerging threats or opportunities are communicated early and resolved at the appropriate authority level. This proactive approach reduces delays, minimizes impacts, and supports disciplined decision-making.

Fourth, the communication objectives emphasize the need to maintain security, confidentiality, and information classification at all times. Given the sensitive nature of the project, communications are structured to protect restricted information through controlled access, approved channels, and formal authorization processes, ensuring that transparency does not compromise security.

Fifth, communications are intended to facilitate effective collaboration across internal teams, the PMO, vendors, and oversight bodies. Clear, consistent, and well-structured communication enables coordination across technical, commercial, security, and operational workstreams, reducing misunderstandings and improving integration.

Finally, project communications provide reliable inputs for stage-gate reviews and executive decisions and support stakeholder engagement and expectation management, ensuring that stakeholders remain informed, aligned, and confident throughout the project lifecycle.

3. Communication Principles:

All communications for the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) are governed by a set of mandatory principles designed to ensure effective control, security, transparency, and accountability throughout the project lifecycle. These principles apply to all forms of communication, including reports, dashboards, meetings, briefings, correspondence, and electronic records.

Accuracy:

All project communications must be fact-based, validated, and traceable to approved sources. Information provided for decision-making must reflect the most current and verified data available. Estimates, assumptions, and forecasts must be clearly identified as such, and any uncertainties must be explicitly stated. This principle ensures that decisions are made using reliable and credible information.

Timeliness:

Project information must be communicated in accordance with defined frequencies, reporting cycles, and escalation triggers. Delayed communication can undermine governance, increase risk exposure, and result in missed decision windows. Therefore, adherence to agreed communication schedules and response timelines is mandatory.

Clarity:

All communications must be clear, concise, and purpose-driven. Messages should be structured to support understanding and decision-making, avoiding unnecessary complexity or ambiguity. Communications must clearly state objectives, key messages, required actions, and decision requests, and be tailored to the needs of the intended audience.

Security-by-Design:

Security and confidentiality are integral to all project communications. Sensitive, confidential, and restricted information must be shared strictly on a need-to-know basis and only through approved and secure channels. Information classification rules must be applied consistently to protect the integrity of sensitive assets, systems, and decisions.

Single Source of Truth:

All official project information must be maintained within PMO-controlled repositories and approved reporting systems. These repositories serve as the authoritative source for project data, baselines, and records. Informal documents or parallel data sources are not recognized for governance or decision-making purposes.

Accountability:

Every communication artifact has a clearly assigned owner who is accountable for its accuracy, completeness, approval, and timely distribution. Ownership ensures traceability and prevents gaps in responsibility across governance and delivery layers.

Escalation Discipline:

Risks, issues, and decisions must follow defined escalation paths and authority thresholds. Bypassing established escalation routes is not permitted. This principle ensures that matters are addressed at the appropriate level of authority and that governance integrity is maintained.

4. Stakeholder Communication Requirements:

Effective communication for the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) is driven by a clear understanding of stakeholder needs, authority levels, responsibilities, and security access. Stakeholder communication requirements are derived directly from the approved Stakeholder Register and the established project governance structure, ensuring that communications are targeted, relevant, and appropriately controlled.

Given the complexity, sensitivity, and strategic importance of the project, a one-size-fits-all communication approach is not acceptable. Each stakeholder group requires different information, levels of detail, frequency, and security classification. Communication must therefore be deliberately tailored to support decision-making, oversight, execution, and assurance without overloading stakeholders or exposing sensitive information.

Project Sponsor:

The Project Sponsor requires high-level, strategic communications focused on overall project performance, alignment with authorized objectives, major risks and issues, and decisions requiring executive intervention. Communications to the Sponsor are concise, decision-oriented, and focused on exceptions rather than operational detail. Information is typically aggregated, emphasizing strategic impact, funding status, and benefits realization outlook. Security classification is high, and access is restricted to approved reports and briefings.

Steering Committee:

The Steering Committee requires comprehensive governance-level information to exercise oversight and approve key decisions. Communications include integrated status reports, stage-gate review packs, major change requests, risk escalations, and benefits realization updates. The information provided balances strategic context with sufficient detail to support informed approvals, trade-off decisions, and prioritization. Communications follow a structured cadence aligned with Steering Committee meetings and formal approval cycles.

Project Management Office (PMO):

The PMO requires detailed, timely, and structured project information to perform its governance, control, reporting, and assurance functions. This includes schedule

and cost data, change logs, risk and issue registers, quality and compliance evidence, and performance metrics. Communications with the PMO are frequent and data-driven, enabling independent validation, baseline control, and governance assurance. The PMO also serves as a central hub for consolidating and distributing approved project information.

Project Manager and Core Team:

The Project Manager and core delivery team require detailed, execution-level communications to plan, coordinate, and control daily work. This includes task assignments, technical specifications, schedules, dependencies, risks, issues, and change decisions. Communications are frequent, operational in nature, and focused on coordination and problem-solving. While transparency within the team is essential, access to sensitive information is still governed by role-based permissions.

Operations Management (Future Owner):

Operations Management requires communications that support readiness, transition, and long-term ownership. Information focuses on operational requirements, performance baselines, training status, SOPs, maintenance plans, and acceptance criteria. Communications increase in frequency and detail as the project approaches commissioning and handover, ensuring that Operations is fully prepared to assume responsibility for assets and benefits realization.

Security and Compliance Authorities:

Security and compliance stakeholders require highly controlled communications related to security architecture, access controls, testing results, audit findings, and incident management. Information shared with this group is often classified and subject to strict handling rules. Communications are formal, evidence-based, and aligned with approval and certification processes to ensure compliance with security and regulatory requirements.

Procurement and Commercial Boards:

Procurement and commercial stakeholders require communications related to procurement strategy, tender processes, contract awards, vendor performance, claims, and contractual changes. Information is structured to support transparency, fairness, and compliance while maintaining confidentiality and

segregation of duties. Communications follow formal procurement governance processes and approval thresholds.

Vendors and Contractors:

Vendors and contractors receive communications necessary to perform their contractual obligations, including technical requirements, schedules, performance expectations, and change instructions. Communications with vendors are formal, documented, and routed through approved contract management channels. Access to sensitive information is strictly limited to what is contractually required.

Internal Audit and Oversight Bodies:

Internal audit and oversight stakeholders require access to objective, verifiable information related to governance compliance, controls, decision-making, and benefits realization. Communications are typically retrospective, evidence-based, and structured to support independent assurance and audits. Transparency and traceability are critical for this group.

5. Communication Matrix (Core Communications):

5.1 Governance & Executive Communications – Comprehensive Communication Matrix:

Communication Item	Primary Audience	Secondary Audience	Purpose / Decision Supported	Key Content (Minimum)	Format	Security Classification	Frequency / Trigger	Preparation Responsibility	Approval Authority	Distribution Channel
Executive Project Status Report	Project Sponsor, Steering Committee	PMO (record)	Strategic oversight, executive awareness, early warning	Overall progress vs baselines, KPI dashboard, major risks & issues, financial summary, decisions required, benefits outlook	Executive dashboard + narrative report	Confidential	Monthly	Project Manager (content) / PMO (validation)	PMO Governance Lead	PMO-controlled repository + executive briefing
Stage-Gate Review Pack	Steering Committee	Project Sponsor, PMO	Go / No-Go decision, phase authorization	Gate objectives, completed deliverables, baseline performance, risk exposure, security & compliance status, readiness confirmation, recommendation	Formal decision pack	Restricted	Per approved stage gate	Project Manager	Steering Committee	Secure governance portal
Benefits Realization Update	Project Sponsor	PMO, Steering Committee	Confirmation of value delivery and benefits protection	Benefit status, KPIs, assumptions validation, emerging benefit risks, corrective actions	Formal report	Confidential	Quarterly	PMO	Project Sponsor	PMO repository
Risk & Issue Escalation Brief	Project Sponsor	Steering Committee, PMO	Executive decision on critical risks/issues	Issue description, impact analysis, options, recommendation, urgency	Briefing note / memo	Restricted	As needed (event-driven)	Project Manager	Project Sponsor	Secure executive channel

Communication Item	Primary Audience	Secondary Audience	Purpose / Decision Supported	Key Content (Minimum)	Format	Security Classification	Frequency / Trigger	Preparation Responsibility	Approval Authority	Distribution Channel
Change Impact Executive Summary	Steering Committee	Sponsor, PMO	Approval of major changes beyond delegation	Change rationale, scope/schedule/cost/security impact, options, recommendation	Summary paper	Confidential	As required	Project Manager + PMO	Steering Committee	Governance repository
Security Compliance Status Report	Steering Committee	Sponsor, PMO	Oversight of security posture and approvals	Security controls status, test results, incidents, approvals required	Formal report	Restricted	Monthly / milestone-based	Security Board	Steering Committee	Restricted-access system
Financial Performance & Forecast Report	Sponsor	Steering Committee, PMO	Funding control and forecast validation	Budget vs actuals, forecast to complete, reserves status	Financial report	Confidential	Monthly	PMO Finance / Controls	Sponsor	PMO financial system
Audit & Assurance Summary	Steering Committee	Sponsor	Governance assurance and compliance confirmation	Audit findings, control gaps, corrective actions	Assurance report	Confidential	Quarterly / audit-triggered	PMO / Internal Audit	Steering Committee	Secure audit channel

5.2 PMO & Control Communications:

Communication Item	Primary Audience	Secondary Audience	Purpose	Key Content	Format	Security Level	Frequency / Trigger	Owner (Preparation)	Approval / Validation	Distribution Channel
Integrated Project Dashboard	PMO, Project Sponsor	Steering Committee	Performance control and trend analysis	Schedule status, cost performance, risk exposure, change trends, milestone health	Dashboard	Confidential	Monthly	PMO Controls	PMO Governance Lead	PMO repository
Schedule & Cost Variance Report	PMO	Project Manager	Baseline integrity and variance control	SPI/CPI, forecast to complete, variance explanation, corrective actions	Analytical report	Confidential	Monthly	PMO Controls	PMO Director	PMO system
Change Control Summary	PMO, Steering Committee	Sponsor	Governance visibility of scope/cost/schedule changes	Approved/rejected changes, thresholds, cumulative impact	Register extract	Confidential	Monthly	Project Manager	PMO Governance Lead	Governance portal
Governance Assurance Report	Sponsor, Steering Committee	Internal Audit	Independent governance and compliance assurance	Findings, control gaps, recommendations, maturity assessment	Formal assurance report	Restricted	Quarterly	PMO	Steering Committee	Secure repository
Risk Exposure Trend Analysis	PMO	Project Manager	Early warning and risk escalation	Top risks, trends, mitigation effectiveness	Dashboard + brief	Confidential	Monthly	PMO Risk Analyst	PMO Governance Lead	PMO dashboard
Baseline Change Log	PMO	Steering Committee	Configuration control	Baseline versions, approvals, traceability	Controlled register	Confidential	Ongoing	PMO Document Control	PMO	Configuration system

5.3 Project Team Communications:

Communication Item	Audience	Purpose	Key Content	Format	Security Level	Frequency	Owner	Records Maintained By
Project Team Meeting	Core project team	Coordination and alignment	Progress, upcoming tasks, blockers, dependencies	Structured meeting	Internal	Weekly	Project Manager	PMO
Workstream Status Update	Project Manager	Progress tracking and control	Activities completed, next steps, risks, support needs	Standard template	Internal	Weekly	Workstream Leads	PMO
Risk & Issue Review Workshop	Project team	Proactive control and mitigation	New risks/issues, response actions, ownership	Facilitated workshop	Confidential	Bi-weekly	Risk Manager	PMO
Lessons Learned Capture	PMO, Project Team	Continuous improvement	Successes, challenges, recommendations	Lessons log	Internal	Ongoing	PMO	PMO
Technical Coordination Session	Technical teams	Integration and problem resolution	Interfaces, dependencies, technical decisions	Working session	Confidential	As required	Technical Leads	PMO
Action Tracking Log	Project team	Accountability and follow-up	Action items, owners, due dates	Register	Internal	Weekly update	Project Manager	PMO

5.4 External & Vendor Communications:

Communication Item	Audience	Purpose	Key Content	Format	Security Level	Frequency / Trigger	Owner	Approval Authority
Vendor Progress Review	Vendors, Project Manager	Performance management	Schedule adherence, quality, risks, corrective actions	Meeting + report	Confidential	Monthly	Contract Manager	Project Manager

Communication Item	Audience	Purpose	Key Content	Format	Security Level	Frequency / Trigger	Owner	Approval Authority
Technical Coordination Meeting	Vendors, Technical Teams	Systems and interface integration	Design alignment, installation sequencing, testing	Workshop	Restricted	As required	Technical Leads	Project Manager
Contract Change Notice	Vendors	Formal contractual instruction	Approved changes, scope adjustments, timelines	Formal letter	Confidential	As needed	Contract Manager	Authorized signatory
Security Compliance Briefing	Vendors	Enforcement of security obligations	Access rules, incident protocols, compliance requirements	Formal briefing	Restricted	As required	Security Board	Steering Committee
Vendor Performance Scorecard	Procurement Board	Contract governance	Delivery, quality, responsiveness, compliance	Scorecard	Confidential	Monthly	Commercial Manager	Procurement Board
Claims & Dispute Communication	Vendors	Contractual resolution	Claims, responses, supporting evidence	Formal correspondence	Confidential	Event-driven	Contract Manager	Legal / Steering Committee

6. Information Classification and Security:

Information classification and security are fundamental to the effective and safe execution of the National Currency Printing and Secure Banknote Production Facility Project (NCPBF). Given the project's strategic importance, technical complexity, and sensitivity of its deliverables, all communications must adhere strictly to the approved information classification model. This model ensures that information is protected appropriately while still enabling effective collaboration and decision-making.

All project information is classified into one of the following categories:

Public information includes non-sensitive material that has been formally approved for broad distribution. This may include high-level project announcements, approved non-technical summaries, or information explicitly authorized for external disclosure. Public information must still be reviewed and approved through formal channels before release.

Internal information covers general project data intended for use within the organization and project team. This includes routine status updates, internal meeting minutes, and working documents that do not expose sensitive commercial, security, or control-related details. Internal information is shared through approved internal systems and is not distributed externally.

Confidential information includes commercial, contractual, financial, governance, and control-related data. Examples include procurement evaluations, contract terms, financial forecasts, change requests, audit findings, and internal control documentation. Access to confidential information is restricted to authorized individuals based on role and responsibility, and distribution is limited to approved channels.

Restricted information represents the highest level of sensitivity and includes security designs, access controls, technical specifications, system architectures, and other information whose unauthorized disclosure could result in significant harm. Restricted information is shared strictly on a need-to-know basis and only through secure, controlled systems with enhanced access controls and monitoring.

To enforce this classification model, the following rules apply to all project communications:

- Restricted information must only be shared through approved secure channels with formally authorized recipients.
- Informal distribution of sensitive information, including verbal, email, or unsecured digital sharing, is strictly prohibited.
- The PMO is responsible for controlling document access rights, maintaining version control, and ensuring that information repositories reflect approved permissions.
- Any suspected or confirmed breach of information security or classification rules triggers immediate escalation through the defined governance and incident management processes, including notification of appropriate authorities and implementation of corrective actions.

This disciplined approach to information classification and security ensures that transparency, control, and protection are balanced appropriately, safeguarding the project's objectives, assets, and integrity throughout its lifecycle.

7. Communication Channels and Tools:

To ensure consistency, security, traceability, and effective governance, all communications for the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) must be conducted using formally approved communication channels and tools. These channels are selected to support controlled information flow, protect sensitive data, and provide auditable records of decisions, approvals, and actions throughout the project lifecycle.

The approved communication channels and tools are defined as follows:

PMO-controlled document repository:

The PMO-controlled document repository is the authoritative platform for storing, managing, and retrieving all official project documents and records. This includes plans, baselines, registers, reports, meeting minutes, approvals, and correspondence. The repository enforces document version control, approval workflows, access permissions, and audit trails. Only documents stored and approved within this repository are considered valid for governance review, assurance, and executive decision-making.

Formal reports and dashboards:

Formal reports and dashboards are used to communicate project status, performance, risks, issues, changes, and benefits. These reports follow standardized templates and reporting cycles to ensure clarity, consistency, and comparability across reporting periods. Dashboards provide summarized, visual insights for governance and executive audiences, while detailed reports support control, analysis, and assurance activities.

Structured meetings with agendas and minutes:

All official project meetings—including governance reviews, stage-gate sessions, risk and issue reviews, vendor performance meetings, and technical coordination sessions—must be conducted using pre-approved agendas. Meeting outcomes are documented through formal minutes capturing key discussions, decisions, action items, owners, and deadlines. Approved minutes are stored in the PMO repository to ensure traceability and accountability.

Secure email for official correspondence:

Secure email is the approved medium for formal project correspondence, including instructions, approvals, notifications, contractual communications, and escalations. Emails related to sensitive, confidential, or restricted matters must comply with information classification rules, be sent only to authorized recipients, and be archived in accordance with document control procedures.

Governance portals (where applicable):

Where available, approved governance or project management portals may be used to facilitate controlled information sharing, reporting, workflow approvals, and performance tracking. These portals provide role-based access control, secure authentication, and centralized visibility of governance information, supporting efficiency while maintaining compliance.

The use of unapproved tools, informal platforms, personal messaging applications, or unsecured file-sharing services for official or sensitive project communications is strictly prohibited. Such tools create risks related to data leakage, loss of version control, lack of auditability, and governance breakdown. Any violation of approved communication channel requirements is subject to escalation and corrective action under the project's governance and security procedures.

This disciplined use of approved communication channels and tools ensures that all project communications are secure, reliable, auditable, and aligned with governance expectations, thereby supporting effective project delivery and long-term institutional accountability.

8. Escalation Communication Path:

The escalation communication path for the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) defines a formal, time-bound mechanism for raising issues, risks, and exceptions to the appropriate level of authority. This structured escalation model ensures that matters are resolved at the lowest effective level, while providing clear pathways for timely executive intervention when impacts exceed delegated authority or threaten strategic objectives, security, or benefits realization.

Escalation is not a sign of failure; it is a control mechanism designed to protect the project, maintain governance integrity, and enable informed decision-making. All escalations must be documented, supported by evidence, and communicated through approved channels.

Escalation Level	Trigger / Condition	Typical Examples (Project-Specific)	Escalation Authority	Required Information	Decision Authority	Timeframe for Escalation	Resolution Documentation
Level 1 – Workstream Escalation	Issue confined to a single workstream with no baseline or security impact	Local technical issue, minor quality defect, short-term resource constraint, coordination issue within one workstream	Project Manager	Issue description, root cause, immediate impact, proposed corrective action	Project Manager	Within **48–72 hours** of identification	Issue Log, meeting minutes, action tracker
Level 2 – Control / Cross-Workstream Escalation	Issue affects multiple workstreams or indicates deviation from approved plans or controls	Interface conflicts (construction vs machinery), emerging schedule slippage, repeated quality non-conformance, control breach	PMO	Impact analysis (scope/schedule/cost/risk), options, recommended action	PMO (with PM)	Within **5 working days**	Issue Log, variance report, corrective action plan

Escalation Level	Trigger / Condition	Typical Examples (Project-Specific)	Escalation Authority	Required Information	Decision Authority	Timeframe for Escalation	Resolution Documentation
Level 3 – Governance / Strategic Escalation	Impact exceeds delegated authority or affects key milestones, security, or benefits	Major change request, significant vendor failure, compliance concern, high-severity risk	Steering Committee	Full impact assessment, alternatives, risk exposure, recommendation	Steering Committee	**Next scheduled meeting** or **urgent session**	Steering decision record, updated baselines/registers
Level 4 – Critical / Executive Escalation	Immediate or severe threat to project viability, security, or organizational integrity	Major security incident, critical safety event, funding disruption, project continuation risk	Project Sponsor	Situation briefing, immediate risks, emergency actions taken	Project Sponsor	**Immediate** (no delay)	Executive directive, incident report, recovery plan

9. Communication Roles and Responsibilities:

Clear definition of communication roles and responsibilities is essential to ensure accountability, accuracy, and disciplined information flow throughout the project lifecycle. Each role has a defined communication mandate aligned with governance authority, decision rights, and information sensitivity.

9.1 Communication Responsibility Matrix:

Role	Communication Responsibilities	Key Outputs	Authority / Accountability
Project Sponsor	Receives strategic-level communications, approves major decisions, provides executive direction	Executive status reports, escalation briefs, stage-gate decisions	Accountable for strategic decisions and approvals
Steering Committee	Receives governance-level information, reviews performance, approves major changes and stage gates	Stage-gate approvals, governance decisions, corrective actions	Accountable for governance oversight
Project Management Office (PMO)	Owns communication standards, templates, dashboards, reporting cadence, and assurance	Dashboards, assurance reports, governance metrics	Accountable for communication quality, consistency, and independence
Project Manager	Ensures accurate, timely, and complete project communications across all levels	Status reports, escalation briefs, coordination communications	Accountable for overall project communication execution
Workstream Leads	Provide validated, timely inputs related to progress, risks, issues, and deliverables	Workstream reports, risk/issue updates	Responsible for accuracy of workstream data
Security Board	Controls and approves sensitive and restricted communications	Security briefings, compliance reports	Accountable for confidentiality and security integrity
Contract / Commercial Manager	Manages formal communications with vendors and contractors	Contract notices, performance reports	Accountable for contractual communication
Operations Management	Receives readiness and transition communications, accepts ownership post-handover	Handover documentation, operational reports	Accountable for post-project benefit realization

Role Accountability Principle:

Each communication artifact has one clear owner responsible for its accuracy, approval, and timely distribution. Shared responsibility is not permitted for accountability.

10. Communication Monitoring and Effectiveness:

Communication effectiveness is continuously monitored to ensure that information supports decision-making, governance, and project performance rather than creating noise, delay, or confusion. Monitoring focuses on outcomes, not volume.

10.1 Communication Effectiveness Indicators

Assessment Area	Measurement Method	Target / Expectation	Owner
Timeliness of reports	Actual vs planned delivery dates	≥ 95% on-time delivery	PMO
Decision turnaround time	Time from escalation to decision	Within defined escalation timelines	Steering Committee
Stakeholder satisfaction	Structured feedback / reviews	No critical communication gaps	Project Manager
Rework due to miscommunication	Issue root-cause analysis	Continuous reduction trend	PMO
Audit and assurance findings	Audit observations related to communication	No repeat findings	PMO
Information accuracy	Variance between reported and verified data	Zero material discrepancies	PMO Controls

10.2 Corrective Actions

When communication gaps, delays, or quality issues are identified:

- Root cause analysis is performed
- Corrective actions are defined and tracked
- Reporting formats, frequencies, or responsibilities may be adjusted
- Recurrent issues are escalated through governance channels

Communication effectiveness is reviewed regularly and formally as part of governance assurance activities.

11. Updates and Maintenance:

This Communication Management Plan is a controlled governance document and is maintained to remain relevant and effective throughout the project lifecycle.

11.1 Review Cycle

- Reviewed **quarterly** by the PMO
- Reviewed additionally prior to major stage gates

11.2 Mandatory Update Triggers

Updates to this plan are required following:

- Major governance or organizational changes
- Significant security incidents or information breaches
- Material changes to stakeholder structure or authority
- Introduction of new communication tools or platforms

11.3 Change Control

- All updates follow formal change control procedures
- Changes are documented, approved, versioned, and communicated
- Superseded versions are archived for audit traceability