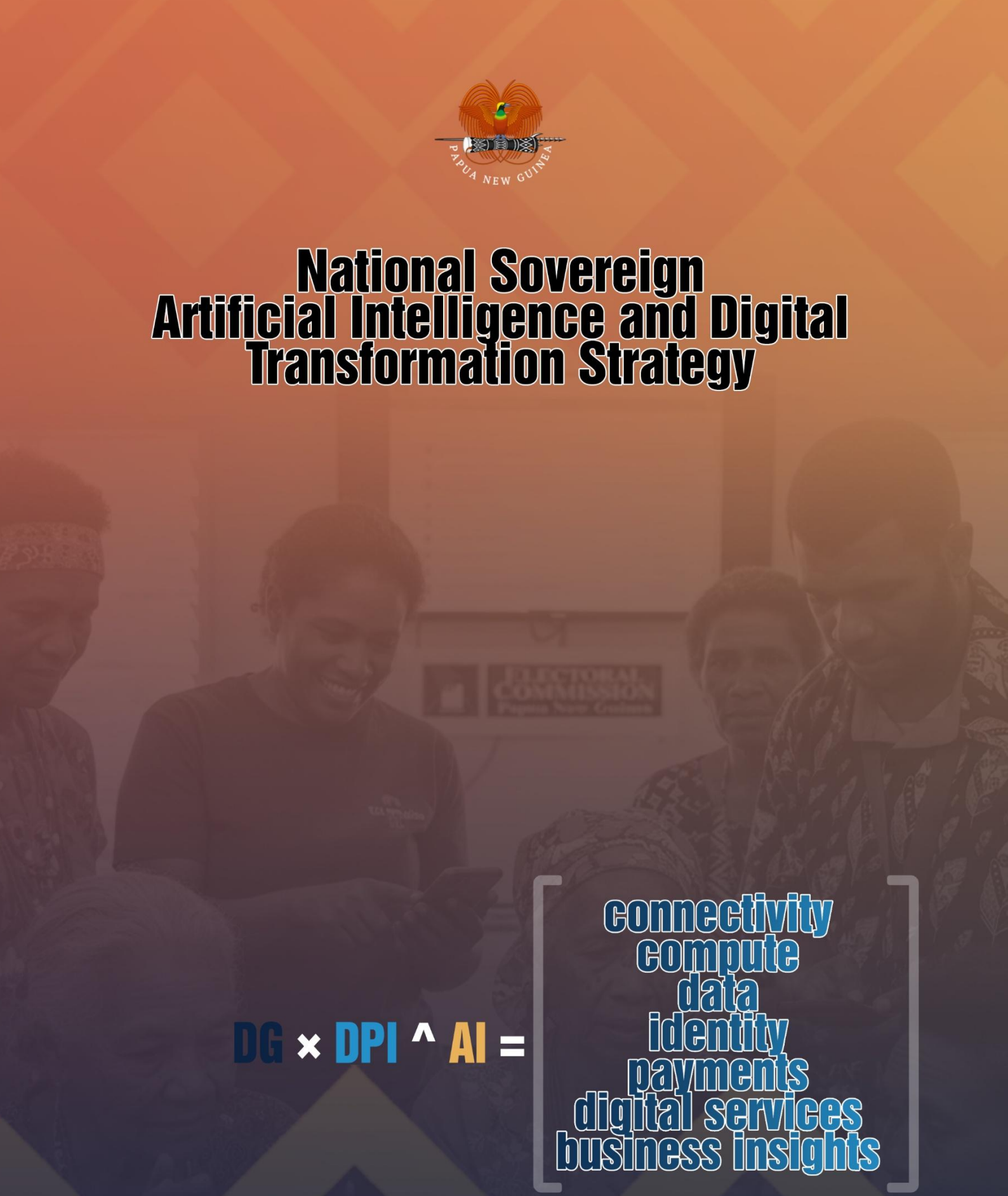
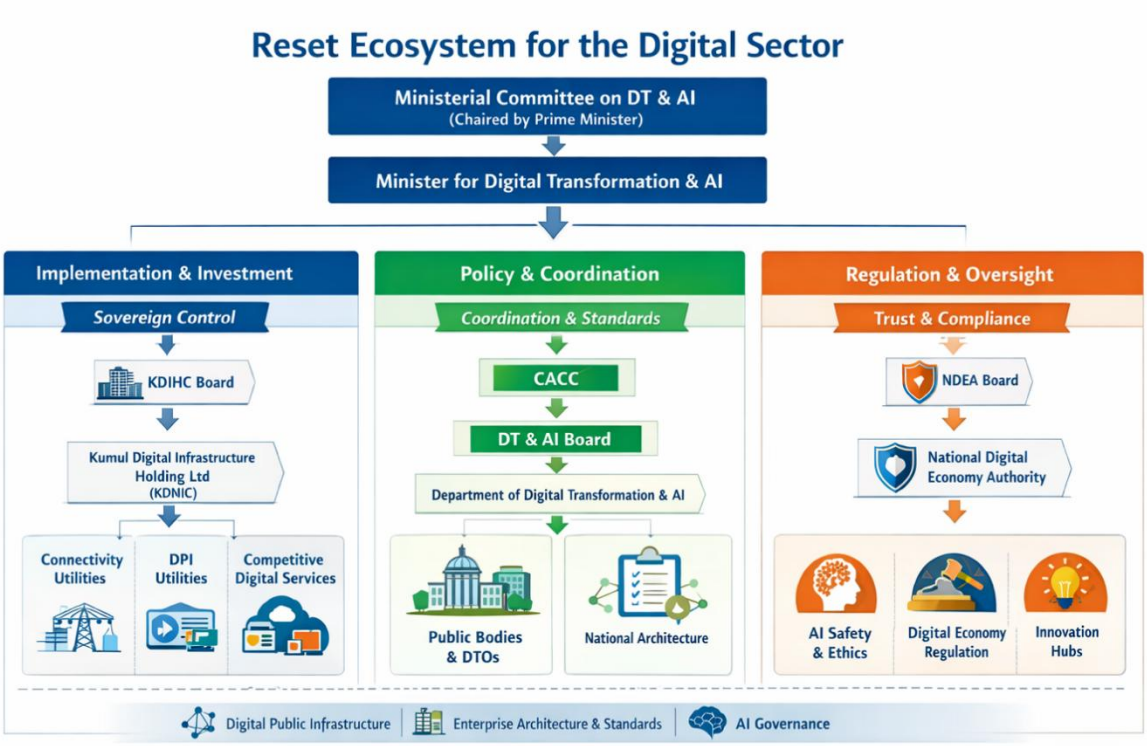
National Sovereign Artificial Intelligence and Digital Transformation Strategy



A Reset Blueprint for Digital Government, Digital Public Infrastructure, and the Digital Sector of Papua New Guinea


Reset Ecosystem for the Digital Sector
Ministerial Committee on DT & AI
(Chaired by Prime Minister)
Minister for Digital Transformation & AI
Implementation & Investment
Sovereign Control
KDIHC Board
Kumul Digital Infrastructure Holding Ltd (KDNIC)
Connectivity Utilities
DPI Utilities
Competitive Digital Services
Policy & Coordination
Coordination & Standards
CACC
DT & AI Board
Department of Digital Transformation & AI
Public Bodies & DTOs
National Architecture
Regulation & Oversight
Trust & Compliance
NDEA Board
National Digital Economy Authority
AI Safety & Ethics
Digital Economy Regulation
Innovation Hubs
Digital Public Infrastructure
Enterprise Architecture & Standards
AI Governance

1. Prime Minister's Statement

Papua New Guinea stands at a defining moment in its national journey.

Having marked our 50th year of Independence, we now move forward with a renewed sense of purpose under the Government's *Reset@50* agenda—focused on repositioning our nation for the next era of growth, inclusion, and resilience. Central to this reset is digital transformation as a key driver of economic expansion and national productivity.

Today, our economy is estimated at approximately K120–125 billion. We have set a national ambition to grow this into a K200 billion economy. This National Sovereign AI Strategy presents a pathway to go even further—to *reforecast Papua New Guinea toward a K500 billion digital economy over time*, driven by productivity gains, new digital industries, and expanded participation across our population of 10.1 million people.

This Strategy is not about Artificial Intelligence alone.

AI creates value only when it is applied on top of strong digital foundations. That is why we adopt a clear national model:

Digital Government × Digital Public Infrastructure ^ Artificial Intelligence

Through this model, we will establish trusted national platforms for digital identity, payments, and data exchange, modernize government systems into a single interoperable architecture, and deploy AI to improve decision-making, efficiency, and service delivery.

This is a structural reform agenda.

It will reduce inefficiencies, eliminate duplication, and lower the cost of doing business across government and the wider economy. It will expand financial inclusion, enable more citizens and businesses to participate in the formal economy, and unlock new opportunities for innovation and investment.

Indicative modelling suggests that this Strategy can generate between *K1.0 billion and K3.0 billion in additional economic output per year* at maturity, with further upside as adoption scales across sectors. Over time, these gains will compound—driving higher productivity, stronger revenue performance, and sustained economic growth.

Importantly, this Strategy is also about *sovereignty and trust.*

As we digitize, we must ensure that our data is protected, our systems are secure, and our digital infrastructure is developed in the national interest. At the same

time, we will pursue strategic partnerships that accelerate capability while safeguarding national interests.

This is our opportunity to leap forward—not incrementally, but structurally.

To move from fragmented systems to a unified digital nation.
To move from limited participation to an inclusive digital economy.
And to move from our current baseline toward a significantly larger and more dynamic economy.

I commend this Strategy as a central pillar of our *Reset@50* agenda and call on all stakeholders to support its implementation.

Together, we will build a modern, trusted, and digitally enabled Papua New Guinea.

HON JAMES MARAPE, MP
Prime Minister

Table of Contents

1. Prime Minister's Statement 3

2. Strategic Context 6

3. Vision 8

4. Strategic Framework: DG × DPI ^ AI 9

5. National Sovereign AI TechStack 10

6. National AI-Ready Infrastructure and Data Architecture 14

7. Governance Framework 22

8. Digital Sector Legislative Institutional Reset 31

9. Structural Reforms 38

10. Implementation Roadmap 45

11. Expected Outcomes 45

2. Strategic Context

Papua New Guinea's digital sector has evolved through multiple independent initiatives across government agencies, state-owned enterprises, and private operators. While these efforts have delivered important progress, the absence of a unified national digital architecture has resulted in fragmented infrastructure, duplication of platforms, limited interoperability, and uneven digital capability across the public sector. As artificial intelligence begins to reshape global public administration, economic systems, and service delivery models, Papua New Guinea must move beyond isolated ICT projects toward a more coherent sovereign digital architecture that integrates connectivity, compute, data, digital public infrastructure, and AI capability into one national framework.

This challenge is not only technological. It is institutional. Many of the country's current digital systems were established to solve specific operational problems at different points in time, often without a common architecture for interoperability, shared infrastructure, or coordinated governance. As a result, digital investments have often been implemented as separate projects rather than as components of a unified state platform. In an era of AI-enabled governance, this fragmented model is no longer sufficient. AI systems derive value from trusted data, interoperable workflows, reusable infrastructure, and clear governance. Without those foundations, AI adoption risks becoming fragmented, costly, and difficult to govern.

Papua New Guinea is not starting from zero. Important foundations have already been established through the Digital Transformation Policy 2020, the Digital Government Plan 2023–2027, the Digital Government Act 2022, and related policies on digital identity, cybersecurity, government cloud, and data governance. Together, these instruments already point toward a whole-of-government model based on shared digital infrastructure, interoperable platforms, digital identity, secure data exchange, and reusable government services. They also establish the legal and institutional basis for stronger coordination of digital transformation across the state.

At the same time, a structural gap remains between whole-of-government digital coordination and the wider ecosystem of strategic digital infrastructure entities that increasingly shape national connectivity, hosting, cloud services, and digital platforms. This gap matters because sovereign AI capability cannot be built through public-sector systems alone. It depends on the alignment of policy, law, data governance, hosting environments, connectivity backbones, and implementation capability across the broader digital sector. A more coherent national architecture is therefore required to align digital government, digital public infrastructure, and strategic digital utilities within one sovereign framework.

Global experience increasingly demonstrates that countries derive the greatest long-term value from digital transformation when they treat foundational systems such as identity, payments, and data exchange as reusable public infrastructure rather than as isolated applications. The core logic of Digital Public Infrastructure is to separate foundational rails from downstream services, adopt open standards, enable interoperability, and support innovation on top of trusted common platforms. More recent DPI–AI thinking extends this logic further by arguing that AI should be deployed on top of governed digital public infrastructure through modular workflows, shared standards, bounded public agents, and sovereign safeguards. In this model, the strategic question is not whether to adopt AI, but whether AI will be deployed on fragmented legacy systems or on trusted national digital rails.

This logic is already reflected in Papua New Guinea's own digital identity and trust architecture. The Digital ID Policy 2025 positions SevisPass as a foundational trust layer and links it to a wider ecosystem of interoperable platforms including SevisWallet, SevisDEx, SevisAdminPortal, and SevisPay. This demonstrates that the country's digital reform trajectory is already moving toward a platform-based model in which shared digital infrastructure supports both government services and wider economic participation.

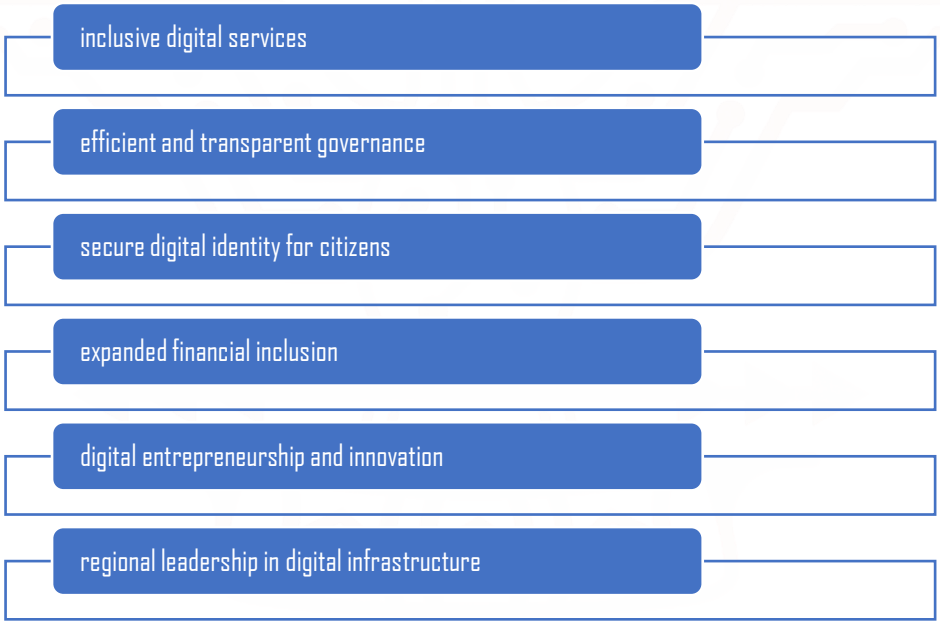
Current national reform efforts, including the broader Reset@50 agenda and recent leadership emphasis on digital modernization, have added political momentum to this transition. However, the strategic case for this document does not rest on political direction alone. It rests on a deeper national reality: Papua New Guinea now requires a more integrated digital sector architecture capable of supporting trusted digital government, sovereign digital public infrastructure, AI-ready infrastructure, and accountable institutional reform over the next phase of national development.

These conditions lead to a clear conclusion. Papua New Guinea's digital future can no longer be pursued as a loose collection of ICT projects, disconnected institutions, platform pilots, and externally procured systems. What is now required is a National Sovereign AI Strategy that brings together digital government, digital public infrastructure, national data architecture, AI-ready infrastructure, legal modernization, and institutional reform into one coherent state architecture. The purpose of this strategy is therefore to provide Papua New Guinea with a sovereign, interoperable, and implementation-oriented blueprint for the next generation of governance, service delivery, and digital economic development.

3. Vision

Papua New Guinea will become a sovereign digital nation, where trusted digital public infrastructure, AI-enabled governance, and open digital platforms power inclusive economic growth, transparent government, and innovation across the Pacific.

This vision will deliver:



This vision recognizes that digital infrastructure has become as strategically important to national development as transport, energy, and financial systems. The strategy therefore treats digital identity, data infrastructure, connectivity networks and artificial intelligence capabilities as critical national infrastructure for the next phase of Papua New Guinea's development.

4. Strategic Framework: DG × DPI ^ AI

The framework expressed as *Digital Government × Digital Public Infrastructure ^ Artificial Intelligence (DG × DPI ^ AI)* captures the central logic of this strategy. Digital government represents the transformation of public administration through technology. Digital public infrastructure provides the foundational platforms on which services operate. Artificial intelligence then amplifies the value of both by enabling intelligent automation, analytics and decision support.

The expression **DG × DPI ^ AI** signifies that artificial intelligence exponentially amplifies the impact of digital government when built on interoperable digital public infrastructure. The proposed national architecture is built on three mutually reinforcing pillars.

Digital government enables public institutions to deliver services electronically through interoperable platforms and shared digital infrastructure. Key outcomes include:

Digital Government (DG)

- digital citizen services
- paperless government
- automated administrative processes
- AI-supported decision making

Digital Public Infrastructure represents the **core digital rails of the economy**. These include:

Digital Public Infrastructure (DPI

- digital identity
- digital payments
- secure data exchange
- digital wallets
- citizen service platforms

Artificial intelligence will amongst other benefits, enhance both government services and economic productivity by enabling:

Artificial Intelligence (AI)

- intelligent data analysis
- automation of administrative processes
- predictive governance systems
- AI-driven public service delivery
- innovation across the private sector

5. National Sovereign AI TechStack

5.1. Strategic Approach

Artificial intelligence adoption across government must occur within a structured, interoperable, and fiscally disciplined national architecture. Without such coordination, institutions risk procuring fragmented technologies, duplicating infrastructure, increasing costs, and creating disconnected systems that cannot support whole-of-government transformation. Papua New Guinea therefore adopts a *National Sovereign AI TechStack* as the national reference model for organizing AI adoption across government and the wider digital economy.

The National Sovereign AI TechStack is a layered model showing how governance, infrastructure, digital public infrastructure, services, and intelligence must operate together as one coherent national system. It is both a planning tool and a sovereign architecture model. It helps government determine what must be governed centrally, what should be shared nationally, what can remain sector-specific, and how AI can be introduced in a way that protects sovereignty, interoperability, and public trust.

Under this strategy, Papua New Guinea's sovereign AI adoption model is organized into five interdependent layers:

Layer No	Layer	Blocks
6	Business Insights and Intelligence	AI Dashboarding
5	Digital Services (Workflows)	G2C, G2B, G2G, B2B, B2C, C2B Workflows
4	Shared Digital Government Services	eProcurement, eBudget, eRecruitment, eHR, eCabinet, Office Productivity, eFinance, etc
3	Foundational Digital Public Infrastructure	Digital ID (SevisPass), Payment (SevisPay), Interoperability (SevisDEx), Citizen's Portal (SevisWallet and SevisPortal), AI Public Agents
2	Infrastructure: Connectivity, Compute, Cloud and Data	AI GPU Compute Clusters, Sovereign AI Model Hosting, GovCloud, M365
		National Transmission Network, Pukpuk Digital Connectivity Initiative, Government Private Network
1	Governance – Policy, Legislation, Standards, Coordination	National Artificial Intelligence Legislation Updated National ICT Legislation Updated Digital Government Legislation Digital ID Legislation National Cyber Security Legislation Data Governance and Protection Legislation
		Digital Transformation Policy AI Adoption Framework (DG X DPI ^ AI)

5.2 Layers of the Stack

Layer 1. Governance, Policy, Legislation, Standards, and Coordination
This is the foundation of the stack. It provides the national rules, mandates, standards, safeguards, and coordination mechanisms that govern how digital infrastructure and AI systems are designed, procured, deployed, and overseen.

This layer includes national AI legislation, updated ICT and Digital Government laws, Digital ID legislation, cybersecurity and data governance laws, the Digital Transformation Policy, the AI Adoption Framework, and national standards and compliance mechanisms.Its purpose is to ensure that AI adoption remains aligned with public purpose, legal authority, institutional accountability, and sovereign control.

Layer 2. National Infrastructure: Connectivity, Compute, Cloud, and Data
This layer consists of the underlying physical and virtual infrastructure required to support digital government and AI-enabled systems at scale.

It includes national connectivity backbones, the Pukpuk Digital Connectivity Initiative and other strategic connectivity assets, the Government Private Network, Government Cloud and sovereign hosting environments, AI-ready compute capability, and governed data and analytical platforms.

Its purpose is to provide the shared national utility layer on which higher-order digital platforms and AI capabilities can operate efficiently, securely, and at scale.

Layer 3. Foundational Digital Public Infrastructure
This layer consists of the shared national digital rails that allow systems to verify identity, exchange data, move value, and provide citizens with access to services through trusted national channels.

This includes SevisPass as the Digital ID layer, SevisPay as the payment layer, SevisDEx as the interoperability and data exchange layer, and SevisWallet and SevisPortal as citizen access and service interface layers. It may also include bounded AI public agents operating on top of trusted workflows and DPI rails. Its purpose is to ensure that AI operates on trusted, reusable, and nationally governed foundations rather than fragmented standalone systems.

Layer 4. Shared Digital Government Services
This layer consists of comprising declared standardized, reusable, and centrally governed digital platforms that enable the delivery of government services and core administrative functions across agencies. Shared Digital Government Services are defined as shared, high-volume, and nationally significant digital

platforms that provide common capabilities across multiple sectors, eliminate duplication, and support scalable service delivery at national level.

This layer shall operate under a Single Enterprise Architecture, which shall define common system design standards, interoperability requirements, data models, APIs, and service workflows. All Shared Digital Government Services shall be developed, deployed, and integrated in accordance with this architecture to ensure consistency, scalability, and a unified user experience across government. No system shall be implemented outside this framework, and all existing systems shall be progressively aligned through structured transition arrangements.

The Shared Digital Government Services Layer shall function as the application and service delivery layer, built on top of foundational Digital Public Infrastructure layer. All services within this layer shall mandatorily integrate with Digital Identity (SevisPass) for authentication, national payment systems (including SevisPay and SevisWallet) for transactions, and the national data exchange (SevisDEx) as the exclusive mechanism for secure and standardized interoperability.

The scope of this layer shall include, but not be limited to, the following platforms: a unified government service delivery platform (SevisPortal); public finance and budget systems; human resource and e-recruitment systems; procurement and e-procurement systems; revenue and taxation systems; regulatory and licensing systems; and sectoral digital service platforms across priority sectors such as health, education, agriculture, and social services. All such platforms shall be designed and implemented as shared national systems, rather than agency-specific solutions.

This layer will serve as the primary environment for the deployment of Artificial Intelligence across government, with AI capabilities embedded into service workflows, operational systems, and decision-making processes. Standardization of platforms within this layer shall enable scalable, reusable, and cost-effective AI adoption.

The establishment of the Shared Digital Government Services Layer shall enable the government to transition to a unified, interoperable, and scalable digital government, reducing duplication and cost, improving service delivery, enabling seamless data exchange, and providing a strong foundation for Artificial Intelligence and digital economic growth.

Layer 5. Digital Services and Workflows

This layer consists of the service environments through which citizens, businesses, and institutions interact. It includes G2C, G2B, and G2G workflows, as well as wider digital economy workflows where relevant. It also includes government workflow engines, case handling systems, transaction processes, and service rules integrated with DPI and AI support functions.

At this layer, AI is applied in a bounded and practical way to improve service delivery, workflow efficiency, translation, summarization, document handling, risk flagging, and user support, while remaining subject to institutional rules and human oversight.

Respective public bodies are responsable for respective sector-specific systems and workflows (e.g. health, education, policing, utilities).

Layer 6. Business Insights, Intelligence, and Decision Support
This is the intelligence layer of the stack. It is where transactions, records, and interoperable data generated through lower layers are converted into actionable insight.

This includes dashboards, predictive analytics, risk detection, policy intelligence, service performance monitoring, procurement and finance intelligence, and sector-specific decision-support tools. Its purpose is to help government move beyond digitization toward evidence-based, anticipatory, and performance-driven governance.

5.3 The Approach of the Stack

The National Sovereign AI TechStack works from the bottom up. Governance establishes the rules. Infrastructure provides connectivity, cloud, compute, and data environments. Digital public infrastructure provides trusted national rails such as identity, payments, interoperability, and citizen access. Service workflows use those shared layers to deliver services. Those services then generate the data and intelligence needed for monitoring, planning, reform, and better decision making.

This layered approach ensures that AI is introduced as part of a national system rather than as isolated software procurements. It allows Papua New Guinea to prioritize shared infrastructure, reduce fragmentation, improve interoperability, and create a scalable pathway from basic digital services to intelligent government.

The purpose of the National Sovereign AI TechStack is to give Papua New Guinea a common national model for planning, sequencing, governing, and investing in sovereign AI adoption. It helps government to direct common investment toward shared national layers, align AI adoption with digital identity and interoperability, reduce duplication, preserve sovereign control over critical digital rails, and support modular innovation built on trusted national foundations.

The next chapter, National AI-Ready Infrastructure and Data Architecture**,** operationalizes the infrastructure layer of this stack by defining the governed data environments, compute platforms, sovereign hosting arrangements, resilience requirements, and reusable AI capabilities needed to support AI deployment at

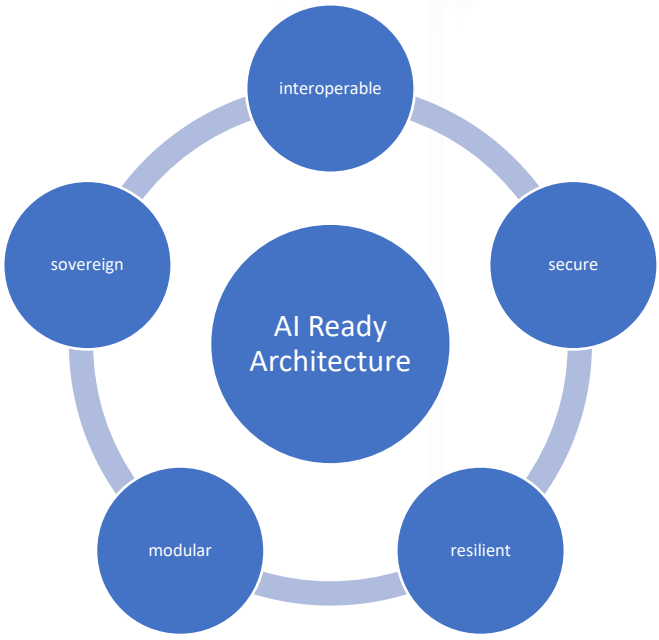
scale. In simple terms, this chapter defines the logical stack; the next chapter defines the technical architecture required to make that stack real.

6. National AI-Ready Infrastructure and Data Architecture

While the *National Sovereign AI TechStack* defines the logical layers of Papua New Guinea's sovereign AI adoption model, this chapter sets out the *technical, platform, and data architecture* required to operationalize those layers at national scale. It translates the conceptual stack into deployable national capability, including governed data environments, AI-ready compute platforms, sovereign hosting arrangements, resilient connectivity, and reusable AI services.

Artificial intelligence capability is ultimately shaped by the strength of the infrastructure, data systems, and interoperability frameworks on which it operates. For Papua New Guinea to deploy AI in a way that improves governance, supports inclusive economic growth, strengthens public administration, and protects national sovereignty, the country must establish a national architecture that is interoperable, modular, secure, resilient, and sovereign by design.

This strategy therefore provisions the framework for a National AI-Ready Infrastructure and Data Architecture, designed to operate in alignment with the National Sovereign AI TechStack and the broader Digital Public Infrastructure framework. The architecture will ensure that AI systems deployed across government and the wider economy operate on trusted national infrastructure, use governed data environments, and remain interoperable with digital identity, payments, secure data exchange, and citizen service platforms.



The objective is to build an AI-ready digital foundation that allows Papua New Guinea to deploy advanced analytics, intelligent automation, workflow support systems, and predictive decision-support capability while maintaining sovereign control over critical data, strategic digital infrastructure, and nationally significant AI systems. The architecture consists of five interrelated domains:

1. National architecture principles and control settings
2. National data architecture
3. AI compute and platform architecture
4. Sovereign hosting and resilience architecture
5. National AI capability architecture

Together, these domains form the operational foundation for the infrastructure layer of the National Sovereign AI TechStack and provide enabling support to the digital public infrastructure, service delivery, and business intelligence layers above it.

6.1 Architecture Principles

Papua New Guinea's National AI-Ready Infrastructure and Data Architecture will be guided by the following principles:

Interoperability and Open Standards

Infrastructure, data environments, AI services, and public-sector platforms should interoperate through open standards, APIs, and shared technical specifications to reduce fragmentation and enable cross-agency integration.

Modularity and Reuse

National digital and AI capabilities should be built as reusable components that can be deployed once and reused across multiple institutions, sectors, and service workflows.

Federated by Design

The architecture should enable multiple agencies, provinces, state-owned entities, and trusted ecosystem partners to participate through shared standards and trust frameworks rather than relying on a single monolithic system or unnecessary centralization.

Sovereignty by Design

Papua New Guinea must retain strategic control over critical data, nationally significant AI systems, core digital public infrastructure, and key policy rules governing their use, while still allowing structured partnerships with global technology providers where necessary.

Privacy, Security, and Trust by Design
Security controls, access restrictions, consent rules, audit logging, explainability, and lawful use requirements must be embedded into infrastructure and data environments from the outset.

Resilience and Continuity by Design
The architecture must support redundancy, disaster recovery, cyber resilience, and continuity of critical public services, especially for systems supporting identity, payments, service access, and national records.

Inclusion and Practical Deployment
Infrastructure and AI-enabled services should support low-connectivity environments, multilingual access, voice-enabled workflows where feasible, and incremental integration with legacy systems rather than assuming immediate full replacement.

6.2 National Data Architecture
Data is the foundational input for artificial intelligence systems. Effective AI deployment requires data environments that are structured, discoverable, secure, interoperable, and governed according to clear institutional and legal rules. Papua New Guinea will therefore establish a National Data Architecture that enables responsible data access and reuse while protecting citizen rights, national interests, and regulatory integrity.

The purpose of this architecture is not to centralize all government data into one uncontrolled repository. Rather, it is to create a federated and governed data ecosystem in which data can be exchanged, verified, catalogued, accessed, and used responsibly across institutions through common standards, trust arrangements, and lawful controls.

The National Data Architecture will include the following elements:

National Data Exchange Layer
The SevisDEx interoperability platform will serve as the national data exchange layer connecting government agencies and trusted institutions through standardized APIs, shared schemas, trust protocols, and governed access rules. This will enable institutions to exchange verified data without unnecessary duplication of databases or the creation of disconnected systems.

Government Data Platforms and Analytical Environments
Government agencies will progressively integrate structured administrative data into secure analytical and operational platforms that support reporting, advanced analytics, machine learning, and decision-support systems.

These environments should support priority national use cases across public finance, recruitment, procurement, agriculture, health, education, infrastructure planning, and regulatory administration.

National Data Catalogue and Metadata Standards
A national catalogue of government datasets will be established to improve discoverability, stewardship, and reuse. Standard metadata requirements will enable agencies to identify what datasets exist, who owns them, what quality conditions apply, what legal restrictions govern them, and how access may be requested or authorized.

Data Classification and Stewardship
Government data will be managed according to formal classification rules, including public, internal, restricted, confidential, and highly sensitive categories where appropriate. Each significant dataset should have a designated steward or accountable institution responsible for quality, lawful access, lifecycle management, and compliance.

Data Quality, Lineage, and Documentation
To support trustworthy AI and evidence-based decision making, the architecture must include measures for data quality assurance, version control, provenance, lineage, validation, and documentation. AI systems should not rely on undocumented, low-quality, or poorly governed datasets.

Access Control, Consent, and Lawful Reuse
The National Data Architecture will operate under clear rules for identity-based access control, consent where applicable, purpose limitation, retention, audit logging, and lawful reuse across the data lifecycle. This will ensure that AI systems operate on governed data environments rather than informal or uncontrolled data extraction practices.

Open Data and Innovation Access
Where lawful and appropriate, selected public datasets should be made available through open data frameworks to support research, civic technology, entrepreneurship, academic collaboration, and public-interest innovation.

6.3 AI Compute and Platform Architecture

Artificial intelligence systems require computing environments capable of supporting data processing, model training where justified, model fine-tuning, inferencing, orchestration, secure APIs, and integration into government workflows. Papua New Guinea will therefore establish an **AI Compute and Platform Architecture** that provides scalable and reusable computational capability for government and nationally significant platforms. This architecture will include:

National AI Compute Capability
GPU-enabled compute infrastructure will be progressively established within trusted hosting environments to support machine learning workloads, advanced analytics, model adaptation, and AI-enabled workflow services. These investments should be sized pragmatically around high-value use cases and shared public-sector needs rather than procured as oversized standalone assets.

AI-Ready Government Cloud
The Government Cloud will evolve into an AI-ready environment capable of supporting model deployment, retrieval and knowledge services, analytics pipelines, workflow automation, and application integration. This will allow agencies to deploy AI-enabled systems through shared infrastructure instead of each institution procuring isolated technology stacks.

Reusable AI Platform Services
Where feasible, common capabilities such as model hosting, prompt orchestration, API gateways, retrieval layers, model monitoring, logging, policy enforcement, and workflow integration should be provided as reusable shared services across government. This will reduce duplication, improve consistency, and support faster deployment of AI-enabled services.

Hybrid Cloud and Portability Model
Papua New Guinea may use a hybrid model combining sovereign infrastructure, national cloud capability, and carefully governed partnerships with trusted international providers. However, sensitive government workloads, strategic DPI systems, and nationally significant data assets must remain subject to sovereign policy control, contractual safeguards, portability requirements, and cybersecurity oversight.

MLOps, DataOps, and Platform Operations
AI-ready infrastructure requires more than hardware. It also requires operational capability. Government should therefore progressively establish platform operations capability covering data engineering, MLOps, model monitoring, security operations, lifecycle management, service support, and performance governance to ensure that AI systems remain reliable, auditable, and maintainable over time.

Workforce and Technical Capability
The architecture should be supported by targeted capacity-building in data engineering, cloud administration, cybersecurity, platform architecture, AI operations, and public-sector product delivery. Long-term sustainability depends on local technical capability, not infrastructure procurement alone.

6.4 Sovereign Hosting and Resilience Architecture

As AI systems become increasingly dependent on large volumes of data, sustained compute, and always-on digital operations, hosting infrastructure becomes a strategic national asset. Papua New Guinea must therefore develop a **Sovereign Hosting and Resilience Architecture** that protects critical systems while supporting long-term national capability. This architecture will prioritize:

National Data Centre Capacity
The development and modernization of high-availability data centre environments capable of supporting government cloud services, digital public infrastructure platforms, secure data environments, and AI compute capability.

Sovereign Hosting for Critical Systems
Critical government systems, sensitive citizen data, strategic registries, and nationally significant digital public infrastructure should be hosted within trusted sovereign environments or equivalent arrangements that preserve national control, regulatory visibility, cybersecurity assurance, and continuity of service.

Integrated National Connectivity Backbone
Hosting environments should be integrated with the wider national digital infrastructure, including domestic backbones, government private networks, international connectivity assets, and future high-capacity transmission systems. This is necessary to ensure service performance, secure interconnection, and resilient operation across the country.

Disaster Recovery and Business Continuity
Critical systems should be supported by backup environments, redundancy arrangements, disaster recovery planning, failover capability, and continuity procedures proportionate to their national importance.

Energy Adequacy and Infrastructure Reliability
Because AI compute, data centres, and digital public infrastructure require reliable power, hosting strategy should include consideration of energy reliability, cooling, backup power, and infrastructure continuity standards. AI-ready national infrastructure is only sustainable if physical hosting conditions are dependable.

Cybersecurity and Infrastructure Assurance
Sovereign hosting environments must operate with strong cybersecurity controls, vulnerability management, logging, monitoring, incident response, and assurance mechanisms consistent with national cyber policy and critical infrastructure protection objectives.

Regional Digital Infrastructure Positioning
As domestic and international connectivity expands, Papua New Guinea has the opportunity to strengthen its long-term role as a regional digital infrastructure and

hosting node for the Pacific. National hosting and cloud capability can therefore serve both sovereignty objectives and future digital economy opportunities.

6.5 National AI Capability Architecture

Beyond infrastructure and hosting, Papua New Guinea must also develop nationally relevant AI capability that can operate on top of this architecture in a reusable, governed, and publicly aligned manner. The objective is not to build one monolithic national AI system, but to create a portfolio of strategic capabilities that support government workflows, citizen service delivery, and local innovation. Key priorities include:

Government AI Workflow Systems

AI-enabled systems will be progressively introduced across government to support analytics, case handling, document processing, recruitment, public finance administration, procurement monitoring, compliance support, fraud detection, service assistance, and policy intelligence. These systems should operate within bounded workflows and institutional safeguards rather than as unconstrained autonomous tools.

Public AI Agents and Service Assistants

Citizen-facing AI assistants integrated into platforms such as SevisPortal and SevisWallet may help users navigate services, understand requirements, complete forms, and access public information. These agents must operate with defined service boundaries, identity-aware controls where relevant, auditability, and clear escalation pathways to human decision-makers.

Local Language and Inclusion Capability

AI systems should progressively support Tok Pisin and, where feasible, other local language and accessibility needs through translation, transcription, speech, and low-literacy service interfaces. This is essential to ensure that national AI capability strengthens inclusion rather than widening digital divides.

National Model Strategy

Papua New Guinea will adopt a pragmatic approach to national model capability. In the near to medium term, priority should be given to:

- adapting and fine-tuning trusted open models for government use cases
- developing smaller domain-specific and language-specific models where justified
- building national knowledge and retrieval layers linked to trusted government data
- only pursuing larger sovereign models where there is a clear public-interest, language, security, or strategic justification

This approach is more realistic, cost-effective, and sustainable than assuming that the country must build large-scale frontier models from scratch in the first instance.

Research, Innovation, and Ecosystem Collaboration
Partnerships with universities, research institutions, start-ups, and private-sector innovators should support the development of locally relevant AI applications across agriculture, fisheries, health, education, finance, logistics, and public administration. This will help ensure that national AI capability supports local problem-solving and not just imported solutions.

6.6 Implementation Logic
The National AI-Ready Infrastructure and Data Architecture should be implemented progressively using a modular, practical, and fiscally disciplined approach. Legacy systems should be enhanced through interoperability and incremental integration rather than immediate wholesale replacement. Shared infrastructure should be prioritized first, followed by reusable platform services, and then sector-specific AI deployments built on top of trusted national rails.

Implementation should therefore prioritize:

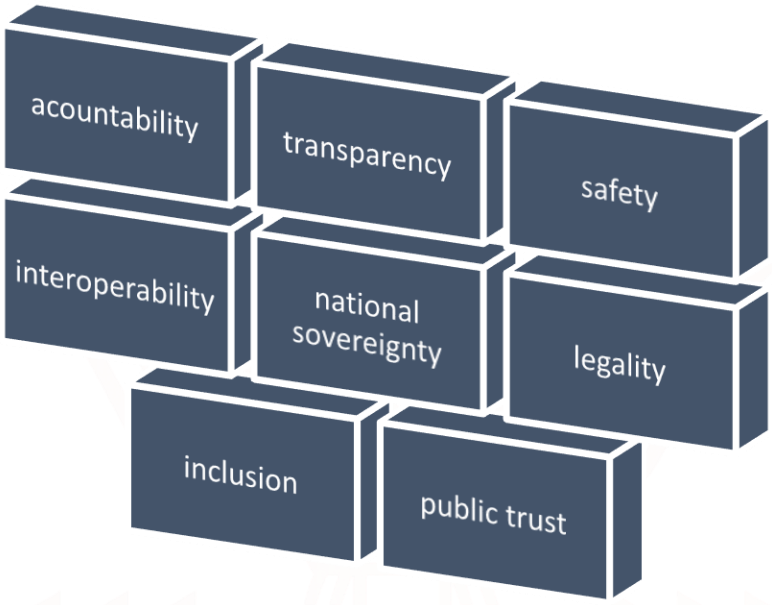
- strengthening shared interoperability and governed data exchange
- establishing reusable analytical and compute environments
- securing sovereign hosting arrangements for critical systems
- building core public-sector platform operations capability
- deploying high-value AI workflow systems on top of existing DPI rails
- progressively expanding local language support, research partnerships, and national innovation capability

6.7 Strategic Outcome
Papua New Guinea will establish an AI-ready digital foundation capable of supporting intelligent public services, evidence-based decision making, secure national platforms, and locally relevant innovation. This architecture will ensure that AI deployment strengthens the country's wider Digital Government and Digital Public Infrastructure agenda rather than fragmenting it. It will also ensure that Papua New Guinea's future AI capability is built on trusted infrastructure, governed data, sovereign control, resilient hosting, and reusable national digital rails.

7. Governance Framework

7.1 Governance Principles and Architecture

The governance of Artificial Intelligence in Papua New Guinea will be guided by the principles of sovereignty, accountability, transparency, safety, interoperability, legality, inclusion, and public trust.



Artificial Intelligence will increasingly influence public administration, service delivery, compliance, planning, and economic participation. For that reason, AI adoption within government must operate within a governance framework that clearly allocates responsibility for policy direction, system design, implementation, operational control, regulatory oversight, auditability, and public redress.

National governance of AI will operate through the following institutional structure:

- Ministerial Committee on Digital Transformation and Artificial Intelligence
- Digital Transformation and AI Board
- Department of Digital Transformation and Artificial Intelligence
- National Digital Economy Authority
- Public Bodies and their designated Digital Transformation Officers

These institutions will perform distinct but complementary functions. Policy leadership, strategic coordination, implementation, operational service ownership, regulatory assurance, and auditability must remain functionally separated in order to avoid confusion, duplication, or conflict of interest.

7.2 Ministerial Committee on Digital Transformation and Artificial Intelligence

The Ministerial Committee on Digital Transformation and Artificial Intelligence will provide the highest level of political oversight for the national AI agenda.

The Committee will be chaired by the Prime Minister, with the Minister responsible for Digital Transformation and Artificial Intelligence serving as Deputy Chair.

The Committee will:

- provide national political leadership for AI adoption and digital transformation
- approve national AI policy positions, reform directions, and strategic priorities
- ensure alignment between AI, economic transformation, public sector modernization, and national development planning
- oversee major national decisions relating to sovereign digital infrastructure, national digital platforms, and strategic public investment
- provide policy direction on the use of AI in high-priority national reforms and public administration
- review progress on implementation of the National Sovereign AI Strategy and direct corrective action where national coordination is failing

The Ministerial Committee will not manage technical implementation or routine operational matters. Its role is to provide strategic political leadership, national coordination at Cabinet level, and top-level accountability for reform delivery.

7.4 Digital Transformation and AI Board

The Digital Transformation and AI Board will serve as the principal whole-of-government strategic coordination body for digital transformation and AI adoption. It will operate as a subcommittee of the Central Agency Coordination Committee and will supersede the Public Service ICT Steering Committee as the permanent cross-government governance mechanism for digital transformation and AI.

The Board will be chaired by the Chief Secretary, with the Secretary of the Department of Digital Transformation and Artificial Intelligence serving as Deputy Chair. The Board will:

- approve whole-of-government AI architecture, technical standards, and governance protocols
- oversee implementation of the **DG × DPI ^ AI** adoption framework across government
- declare, prioritize, and oversee Shared Digital Government Services
- approve whole-of-government priorities for AI-enabled public service transformation

- ensure interoperability across government systems, platforms, and shared digital services
- resolve cross-agency implementation issues that affect national digital architecture
- oversee institutional readiness, workforce capability, and change management across government
- review major or high-risk public-sector AI initiatives before scaled deployment
- monitor whole-of-government implementation performance and direct remedial action where required

The Board will ensure that government AI deployments are aligned with each layer of the national AI TechStack, including:

- SevisPass
- SevisWallet
- SevisDEx
- national digital payments infrastructure
- Government Cloud
- Shared Digital Government Services
- other approved national digital platforms

The Board is responsible for **strategic coordination and architecture governance**. It is not the operational owner of agency services, nor the independent regulator.

7.5 Department of Digital Transformation and Artificial Intelligence

The *Department of Digital Transformation and Artificial Intelligence* will replace the Department of Information and Communications Technology (also referred to as the Department of Digital Communications) and will serve as the central executive authority responsible for coordinating implementation of digital transformation and AI adoption across government.

The Department will coordinate implementation of the National Sovereign AI Strategy and ensure operational alignment with the national digital architecture, the Government Adoption Framework for AI, and approved whole-of-government technical standards. The Department will:

- coordinate implementation of the National Sovereign AI Strategy
- prepare national AI implementation roadmaps, standards adoption plans, and capability programs
- operationalize whole-of-government AI architecture and implementation frameworks approved by the Board

- coordinate implementation of Shared Digital Government Services, Digital Public Infrastructure, Government Cloud, and other common digital enablers
- provide technical guidance, reference models, templates, and implementation support to public bodies
- support agencies in identifying, prioritizing, and structuring AI use cases
- maintain whole-of-government visibility of major AI deployments and strategic implementation risks
- promote responsible AI practices across the public sector
- coordinate cross-government capability development, knowledge sharing, and implementation support
- prepare consolidated progress reports for the Board and Ministerial Committee

The Department is the executive implementation and coordination authority. It is responsible for enabling implementation, but it is not the legal owner of each agency service and it is not the independent regulator.

7.6 National Digital Economy Authority

The National Digital Economy Authority will serve as the independent regulatory authority for the digital economy, including regulatory oversight for digital services, data governance and privacy, digital trust services, telecommunications and broadcasting where applicable, and artificial intelligence, including AI safety and assurance.

The Authority will provide independent oversight to ensure that AI systems deployed or offered in Papua New Guinea meet national requirements for safety, accountability, transparency, legality, and responsible use. The Authority will:

- develop and issue national AI safety, assurance, and compliance standards
- classify AI systems according to risk level
- establish regulatory requirements for high-risk and designated AI systems
- conduct compliance monitoring and regulatory inspections
- establish testing, conformity, and certification frameworks where required
- investigate incidents involving AI system failure, misuse, harm, or unlawful deployment
- issue guidance, notices, directions, or restrictions relating to unsafe or non-compliant AI deployments
- maintain regulatory coordination with institutions responsible for cybersecurity, data protection, digital identity, finance, telecommunications, consumer protection, and other relevant sectors
- publish periodic oversight reports on the state of AI compliance and safety in Papua New Guinea

The Authority is responsible for independent assurance and enforcement. It must remain institutionally distinct from implementation and service delivery functions.

7.7 Allocation of Responsibility and Accountability

Responsibility for AI governance will be allocated as follows:

- **Ministerial Committee**: politically accountable for national direction, reform leadership, and strategic alignment
- **Digital Transformation and AI Board**: strategically accountable for whole-of-government coordination, architecture approval, prioritization, and cross-government implementation discipline
- **Department of Digital Transformation and Artificial Intelligence**: operationally responsible for implementation coordination, standards operationalization, technical guidance, and capability uplift
- **National Digital Economy Authority**: independently accountable for regulatory oversight, assurance, certification where required, compliance monitoring, and enforcement
- **Head of Public Body**: ultimately accountable for the lawful, safe, fair, and effective use of AI within that institution's services, decisions, and operations
- **Digital Transformation Officer**: responsible for institutional coordination, controls, records, risk management, reporting, and compliance administration within the public body
- **System or Service Owner**: responsible for day-to-day operation, performance, safeguards implementation, and service outcomes of the specific AI-enabled system
- **Shared Platform Owner**: responsible for the operational integrity, security, availability, and standards compliance of shared digital platforms and common AI-related infrastructure under its control

Use of a shared platform, common model, or national digital rail does not remove accountability from the public body that deploys AI within its own mandate. Each public body remains accountable for the decisions, outcomes, and rights impacts arising from the services it provides.

7.8 Approval, Assurance, and Escalation Lifecycle

AI systems deployed within government will be subject to a structured approval and assurance lifecycle, proportionate to the level of risk. At a minimum, this lifecycle will include:

1. **Use case identification and institutional sponsorship** by the relevant public body
2. **Risk assessment and classification**, including assessment of legal, operational, ethical, privacy, security, and public-interest implications

3. **Architecture and standards review** to ensure alignment with national digital architecture, interoperability requirements, and Shared Digital Government Services
4. **Regulatory assurance or certification**, where required for high-risk or designated systems
5. **Deployment approval** by the accountable public body
6. **Operational monitoring**, including audit logging, performance review, incident monitoring, and model or workflow oversight
7. **Escalation, suspension, remediation, or withdrawal** where safeguards fail, material risks arise, or non-compliance is identified

Detailed procedures, thresholds, and documentation requirements will be prescribed through standards, regulations, directives, or operational manuals.
No high-risk AI system may be deployed in government without documented accountability, defined human oversight, and auditable control mechanisms.

7.9 Agency-Level Accountability

While national institutions provide political leadership, coordination, implementation support, and regulatory oversight, each public body remains accountable for the services it delivers, including services supported by AI systems.

Each public body will designate a *Digital Transformation Officer (DTO)* responsible for digital transformation and AI governance within that institution. The DTO shall:

- be designated by the Head of Public Body
- be appointed at Secretary or Deputy Secretary level, or at an equivalent executive level approved by the Board
- possess relevant qualifications or demonstrated competence in digital systems, data, technology governance, artificial intelligence, or related fields as approved by the Board

In addition to existing responsibilities, DTOs will be responsible for:

- leading institutional digital transformation and AI adoption
- ensuring compliance with national AI policy, standards, and regulatory obligations
- maintaining an up-to-date inventory of AI systems used, procured, piloted, or integrated by the institution
- ensuring risk assessments are completed prior to deployment
- ensuring appropriate documentation, model records, workflow definitions, and audit logs are maintained
- ensuring transparency obligations are met where AI materially influences service delivery or decisions

- ensuring incidents, failures, complaints, and material changes are reported through appropriate channels
- coordinating with the Department and the National Digital Economy Authority on implementation, oversight, and corrective action
- ensuring that high-impact use cases include effective human review pathways

DTOs will act as the principal coordination interface between each public body and the national digital governance architecture.

7.10 Responsible AI Safeguards

In compliance with the Government AI Adoption Framework, AI systems deployed across government must adhere to mandatory safeguards. Accordingly:

- no AI-only decision may be made in matters affecting legal rights, benefits, penalties, entitlements, or significant public services
- meaningful human oversight must be available for high-impact decisions supported by AI systems
- AI systems must operate within approved institutional mandates and defined operational boundaries
- transparency measures must ensure that citizens are aware when AI materially influences public service delivery
- high-risk systems must undergo appropriate bias, fairness, safety, privacy, and security assessment
- all government AI systems must maintain adequate records, audit logs, and traceability of material actions and outputs
- citizens must have a pathway to request human review, correction, or escalation where appropriate
- incident reporting and corrective action mechanisms must be established for failures, misuse, or harmful outcomes
- AI deployment must align with national digital identity, data exchange, cybersecurity, privacy, and interoperability requirements

These safeguards apply irrespective of whether the AI capability is developed internally, procured from a vendor, embedded within a platform, or accessed through cloud-based services.

7.11 Governance of AI Public Agents and Workflow Systems

As government begins to deploy AI Public Agents, digital assistants, and workflow-based AI systems, additional governance controls will apply. AI Public Agents and workflow systems must:

- operate only within approved government workflows and legally authorized service boundaries

- use trusted Digital Public Infrastructure where identity, payments, consent, or data exchange are required
- maintain complete and auditable system logs
- apply escalation rules where uncertainty, safeguard failure, exception conditions, or risk thresholds are triggered
- provide citizens with access to human assistance or human review where required
- avoid autonomous operation outside approved institutional processes
- remain subject to service-owner accountability and regulator oversight

Government AI agents are therefore not to be treated as independent autonomous actors, but as bounded digital instruments operating under public authority, documented workflows, and human accountability.

7.12 Audit, Assurance, and Reporting

A credible governance framework requires not only policy direction and regulatory oversight, but also structured audit and public reporting. Accordingly:

- high-risk and designated AI systems will be subject to periodic audit and assurance review
- audits may cover legality, model performance, workflow integrity, data governance, privacy, security, fairness, operational resilience, and compliance with national standards
- public bodies must retain records sufficient to support internal review, external inspection, and regulatory inquiry
- the Department will maintain whole-of-government implementation reporting
- the National Digital Economy Authority will publish periodic reports on regulatory oversight, compliance trends, incidents, and systemic risks
- Government will progressively establish public reporting mechanisms on approved AI use cases, safeguard implementation, and national readiness

Where appropriate, the existing public-sector ICT audit architecture may be expanded or updated to incorporate AI systems and related controls.

7.13 Public Trust, Redress, and Continuous Improvement

Public trust is fundamental to the successful adoption of AI in government. Government will therefore:

- establish channels through which citizens may raise concerns, complaints, or requests for review in relation to AI-enabled services
- ensure institutions maintain grievance and escalation mechanisms proportionate to the nature of the service
- use audit findings, incident reports, and grievance data to improve policy, systems, and safeguards over time

- periodically review the effectiveness of the governance framework and update standards, regulations, and operational guidance as AI capability matures

8. Digital Sector Legislative Institutional Reset

8.1 Purpose of the Legislative and Institutional Reset

Papua New Guinea will undertake a comprehensive legislative and institutional reset to enable the transition toward a digitally enabled State, anchored on the integration of Digital Government, Digital Public Infrastructure, and Artificial Intelligence.

This reset recognises that the current legal framework, while foundational, was developed in a pre-platform and pre-AI environment and does not fully support a modern, interoperable, and scalable digital ecosystem. The Government will therefore establish a legal architecture that is aligned to the national digital infrastructure model and capable of supporting long-term technological evolution. Legislation under this framework will be designed to follow the structure of the digital economy, ensuring that governance, ownership, and regulatory functions are clearly aligned to the roles they are intended to serve.

8.2 Guiding Policy Principles for Legislative Reform

All legislative reforms under this Strategy will be guided by a set of core principles that ensure both durability and effectiveness.

The State will ensure that legislation is architecturally aligned, reflecting the layered structure of digital infrastructure, shared platforms, and service delivery systems. Laws will be framed in a technology-neutral and function-based manner**,** ensuring they remain applicable to future technological developments.

The State will exercise sovereign stewardship over critical digital infrastructure and national digital trust systems, while maintaining competitive neutrality in downstream digital service markets. This ensures that the Government retains control where national interest is paramount, while enabling innovation and private sector participation.

The legislative framework will enforce a clear separation of policy, regulation, and ownership**,** ensuring that institutions operate within well-defined mandates. At the same time, all state-invested entities will be structured to operate under commercial discipline**,** enabling them to attract investment and partnerships while maintaining public accountability.

8.3 Critical Digital Infrastructure Investment Act

Papua New Guinea will introduce a new primary legislation, the *Critical Digital Infrastructure Investment Act,* as the anchor law for the digital sector.

This Act will establish the legal foundation for the ownership, governance, and coordinated public driven investment of critical digital infrastructure. It will define classes of infrastructure that are essential to national development, including

connectivity infrastructure, shared digital platforms, and other nationally significant digital systems.

The Act will provide a framework through which the State may retain strategic control over such infrastructure while enabling co-investment by private sector partners, institutional investors, and development partners. It will also provide for open access and non-discriminatory use of designated infrastructure where appropriate, ensuring that national digital assets function as shared enablers of economic activity.

The Act will be designed to remain flexible, allowing the classification of infrastructure and the scope of its application to evolve over time without requiring frequent legislative amendment.

8.4 Establishment of Kumul Digital Infrastructure Holding Company (KDIHC)

The Critical Digital Infrastructure Investment Act will provide for the establishment of the *Kumul Digital Infrastructure Holding Company (KDIHC)* as the State's digital infrastructure investment and asset management entity.

KDIHC will operate as a state-owned infrastructure holding entity responsible for critical digital infrastructure, with a dual mandate of sustainability ensuring to delivering government's objectives on increasing secure access, affordability, reliability while ensuring and strategic sovereignty.

KDIHC will hold the State's equity in designated critical digital infrastructure utilities and will act as the central vehicle for coordinating investment across the digital sector. It will operate under an independent, merit-based Board and will function at arm's length from Government, ensuring that operational decisions are guided by commercial principles rather than administrative direction.

The governance model of KDIHC will reflect the structure applied in *Kumul Petroleum Holdings Limited*, adapted to the digital sector. This includes clear separation between ownership and policy functions, transparent reporting obligations, and protection from undue political interference.

Through KDIHC, the State will consolidate fragmented digital infrastructure assets into a coherent ownership structure, enabling more efficient management, stronger strategic alignment, and improved ability to attract investment.

8.5 Recognition and Governance of Shared Digital Platforms

The State will recognise shared digital platforms as *critical digital infrastructure utilities* that provide foundational services across government and the broader economy.

These platforms will operate as trusted, interoperable systems that enable identity verification, secure data exchange, and financial transactions. The State will retain control over their governance, standards, and trust frameworks to ensure neutrality, security, and interoperability.

At the same time, access to these platforms will be made available to public institutions, private sector entities, and accredited partners on a fair and non-discriminatory basis. This approach ensures that shared platforms function as enablers of innovation and economic participation, rather than as closed or proprietary systems.

The legal framework will define these platforms in functional terms, allowing for evolution in their design and implementation without requiring legislative change.

8.6 Governance of Artificial Intelligence

Papua New Guinea will enact a *National Artificial Intelligence Act* to establish a comprehensive and future-proof governance framework for the adoption, management and use of AI.

This legislation will adopt a risk-based and technology-neutral approach, ensuring that it applies to both current and emerging forms of AI and automated systems. It will define obligations relating to transparency, accountability, human oversight, and auditability, particularly in cases where AI systems impact citizens or critical public functions.

The Act will ensure that AI systems operating within Papua New Guinea are aligned with national digital infrastructure, including identity, data, and interoperability frameworks, thereby preventing fragmentation and ensuring trust.

8.7 Digital Identity and Trust Framework

The State will enact a *Digital Identity and Trust Framework Act* to provide legal recognition for a national digital identity system and its associated trust framework and services.

This legislation will establish the legal validity of digital identity-based transactions and authentication mechanisms, enabling secure and seamless interaction across government and the economy. It will define the rights of individuals in relation to their identity and ensure that identity systems operate on principles of consent, privacy, and security.

The law will empower the State to designate systems that meet national standards as official digital identity systems, while maintaining flexibility to accommodate future developments in identity technologies.

8.8 Data Governance and Protection Framework

Papua New Guinea will introduce a *Data Governance and Protection Act* to regulate the management and use of data.

This legislation will establish clear rules governing data ownership, access, sharing, and protection, ensuring that data is used in a lawful, secure, and responsible manner. It will support the development of interoperable data systems and enable secure data exchange across government and between sectors.

The framework will be principle-based to ensure that it remains adaptable to evolving technologies and data use cases, including those related to artificial intelligence.

8.9 Realignment of Existing Legislation

Existing laws will be reviewed and amended to ensure alignment with the national digital architecture and the objectives of this Strategy.

The Digital Government Act 2022 will be strengthened to mandate alignment with national enterprise architecture and the use of shared digital platforms in service delivery.

The National Information and Communications Technology Act 2009 will be modernised to reflect the expanded scope of digital infrastructure and to support regulatory oversight of emerging domains.

Other relevant legislation—including those governing electronic transactions, civil registration, financial compliance, cybersecurity, public finance, procurement, and public administration—will be reviewed and updated as necessary to ensure coherence and consistency across the legal framework.

8.10 Strategic Shareholding and Investment Framework

The State will adopt a structured approach to strategic shareholding in the digital sector to balance sovereign control with investor confidence.

Mechanisms will be established to protect national interests in critical infrastructure while ensuring transparent governance, fair treatment of minority investors, and commercial discipline. This approach will enable the mobilisation of capital and expertise required to scale digital infrastructure while maintaining alignment with national priorities.

8.11 Institutional Coordination and Oversight

The implementation of the legislative and institutional reset will be supported by strengthened coordination mechanisms across Government.

The Department responsible for Digital Transformation and Artificial Intelligence will provide strategic policy leadership, while KDIHC will manage infrastructure

investments. Regulatory authorities will continue to exercise independent oversight within their mandates.

Whole-of-government coordination will be reinforced through existing governance structures, including the Public ICT Steering Committee and the Ministerial Committee on Digital Transformation and Artificial Intelligence.

8.12 Sustainable Financing of Critical Digital Infrastructure

The Government will establish a sustainable financing mechanism to support the development of critical digital infrastructure.

In alignment with the national development financing framework, the State will allocate **1.5 percent of the 5.6 percent funding envelope under the Connect PNG Program** to the development of critical digital infrastructure.

This allocation recognises that digital infrastructure is a foundational component of national connectivity and economic development, equivalent in importance to physical transport infrastructure.

Funds allocated under this mechanism will be channelled through KDIHC, which will act as the implementing agency responsible for planning, investing in, and delivering critical digital infrastructure projects.

This approach ensures:

- Predictable and sustained funding for digital infrastructure
- Integration of digital connectivity with national infrastructure planning
- Efficient deployment of capital through a commercially governed entity

8.13 Implementation of the Legislative Reset

The legislative and institutional reset will be implemented in a phased manner, beginning with the development and consultation of new legislation, followed by the establishment of institutional structures and the progressive alignment of existing laws.

This phased approach ensures continuity of existing systems while enabling the orderly transition to the new digital architecture.

8.14 Strategic Outcome

Through this legislative and institutional reset, Papua New Guinea will establish a coherent, future-ready legal and governance framework for its digital economy. The resulting system will be sovereign in its control of critical infrastructure, open in its support for innovation and competition, and adaptable to future technological change. It will provide the legal and institutional foundation necessary to deliver digital government services at scale, support the responsible adoption of artificial

intelligence, and position Papua New Guinea as a competitive and trusted digital economy.

Matrix of Legislative Reforms

Category	Legislation	Type	Purpose / Policy Intent	Key Provisions (Indicative)	Institutional / Implementation Implications
Foundational Infrastructure Governance	**Critical Digital Infrastructure Investment Act**	New	Establish legal framework for ownership, governance, and investment of critical digital infrastructure	Define classes of critical digital infrastructure; Establish KDIHC; Provide for strategic shareholding; Enable co-investment and PPP models; Open access provisions where applicable	Establishment of KDIHC; Consolidation of state digital assets; Centralised infrastructure investment governance
State Investment Vehicle	**Kumul Digital Infrastructure Holding Company (KDIHC) Establishment (via Act)**	New (within above Act)	Create a state-owned holding entity to manage digital infrastructure assets	Independent Board; Commercial mandate; Asset consolidation powers; Investment and divestment authority; Reporting and governance requirements	Mirrors Kumul Petroleum Holdings Limited model; separates ownership from policy and regulation
Artificial Intelligence Governance	**National Artificial Intelligence Act**	New	Establish governance framework for AI adoption and deployment	Risk-based classification of AI systems; Obligations for transparency, explainability, auditability; Human oversight requirements; Registration of high-risk systems	Establish AI oversight function; Integration with DPI and Digital Government systems
Digital Identity	**Digital Identity and Trust Framework Act**	New	Provide legal recognition of digital identity and trust services	Legal validity of digital identity; Authentication and credentialing framework; Consent management; Accreditation of identity providers	Enables SevisPass-type systems; Supports eKYC, authentication, and cross-sector identity use
Data Governance	**Data Governance and Protection Act**	New	Regulate data ownership, sharing, and protection across sectors	Data classification framework; Data sharing protocols; Privacy and protection obligations; Cross-border data considerations	Enables secure data exchange; Supports AI and DPI ecosystems
Digital Government Alignment	**Digital Government Act 2022**	Amendment	Strengthen enforcement of whole-of-government digital architecture	Mandatory compliance with enterprise architecture; Mandatory use of shared DPI platforms; Strengthened enforcement mechanisms	Positions DPI as default infrastructure for all G2C and G2G services
ICT Sector Regulation	**National Information and Communications**	Amendment	Modernise regulatory framework to	Expand definition of ICT infrastructure to include cloud, data	Aligns NICTA role with emerging infrastructure

Category	Legislation	Type	Purpose / Policy Intent	Key Provisions (Indicative)	Institutional / Implementation Implications
	Technology Act 2009		reflect expanded digital infrastructure scope	infrastructure, and digital platforms; Strengthen regulatory oversight of new infrastructure layers	domains. Updates NICTA to National Digital Economy Authority
Electronic Transactions	**Electronic Transactions Act (if existing, or introduce if absent)**	Amendment / New	Enable legal recognition of digital transactions and records	Recognition of digital signatures; Digital contracts; Electronic records admissibility	Supports digital government services and e-commerce
Cybersecurity	**Cybercrime Code Act 2016 / Cybersecurity Legislation**	Amendment	Strengthen legal framework for cybersecurity in a digital economy	Protection of critical digital infrastructure; Expanded cyber offence definitions; Incident reporting obligations	Aligns with CERT and national cybersecurity strategy
Civil Registration	**Civil and Identity Registration Laws**	Amendment	Align civil registration systems with digital identity framework	Integration with digital ID systems; Data sharing provisions; Identity verification standards	Enables foundational identity data integration
Financial Sector Compliance	**AML/CTF Act 2015**	Amendment	Align financial compliance with digital identity and digital payments	Recognition of digital ID for KYC; Digital onboarding provisions; Risk-based compliance frameworks	Enables financial inclusion via DPI
Payments & Financial Systems	**National Payments System Act / BPNG Regulations**	Amendment	Enable interoperability between DPI payment systems and financial sector	Recognition of digital wallets; Integration with national payment rails; Licensing clarity for government-linked payment systems	Supports SevisWallet / Service Pay Layer integration
Public Finance	**Public Finances (Management) Act**	Amendment	Enable structured investment into digital infrastructure	Allow allocation of infrastructure funds (e.g. Connect PNG allocation); Enable equity investment via KDIHC	Supports 1.5% allocation mechanism
Public Procurement	**Public Finance Management / Procurement Laws**	Amendment	Enable agile and technology-appropriate procurement models	Framework agreements; Digital platform procurement; Innovation partnerships; PPP enablement	Reduces delays in digital project delivery
State-Owned Enterprises Governance	**Kumul Consolidated Holdings Authorisation Act / SOE Framework**	Amendment	Align governance of digital SOEs with KDIHC structure	Clarify relationship between KCH and KDIHC; Define asset transfer and shareholding arrangements	Ensures clean institutional separation and avoids mandate overlap
Competition & Consumer Protection	**Independent Consumer & Competition Commission Act**	Amendment	Ensure competitive neutrality in digital services market	Prevent anti-competitive behaviour; Regulate access to shared infrastructure; Consumer protection in digital services	Supports open access and fair competition

Category	Legislation	Type	Purpose / Policy Intent	Key Provisions (Indicative)	Institutional / Implementation Implications
Data Sharing Across Government	**Inter-Agency Data Sharing Regulations (New or Subsidiary)**	New (Subsidiary)	Enable secure and standardised data exchange across agencies	Data sharing protocols; API standards; Security requirements; Governance framework	Enables interoperability across government systems
Cloud & Data Infrastructure	**Government Cloud Policy (to be backed by regulation if needed)**	Policy / Possible Regulation	Establish sovereign and hybrid cloud framework	Data residency requirements; Cloud accreditation; Multi-cloud interoperability	Supports national AI and data infrastructure
Sector-Specific Laws (Health, Education, etc.)	Various Sectoral Acts	Amendment	Align sector systems with digital identity and data frameworks	Enable digital service delivery; Data sharing compliance; Integration with DPI	Ensures whole-of-government adoption

9. Structural Reforms

9.1 Purpose of Structural Reform

The successful adoption of Artificial Intelligence across government and the wider economy requires a national digital ecosystem that is secure, interoperable, resilient, and capable of supporting large-scale digital services.

Papua New Guinea's digital sector has evolved over time through a number of state-owned enterprises, public institutions, and market actors established to address specific connectivity and technology needs. While these arrangements have played an important role in expanding national connectivity and digital services, the emergence of digital public infrastructure, cloud computing, data-driven governance, and artificial intelligence now requires a more coherent national architecture for the governance and management of strategic digital assets.

Structural reform is therefore necessary to align the digital sector with the objectives of the National Sovereign AI Strategy. The purpose of this reform is not to predetermine the future of any single institution, but to establish a national model that clearly distinguishes foundational public digital infrastructure, strategic utility infrastructure, and competitive digital services. This will strengthen sovereignty over critical digital systems, support open and interoperable national platforms, enable innovation and private sector participation, and improve the long-term resilience and security of nationally significant digital assets.

Through these reforms, Papua New Guinea will establish a digital sector architecture capable of supporting trusted digital government, sovereign digital public infrastructure, AI-ready infrastructure, and scalable digital services across the wider economy.

9.2 National Digital Infrastructure Implementation Framework

The implementation of Papua New Guinea's National Sovereign AI Strategy will be operationalised through a *National Digital Infrastructure Implementation Framework* structured around three coordinated and mutually reinforcing infrastructure domains: *Connectivity Utilities, Digital Public Infrastructure Utilities,* and *Competitive Digital Services.* This framework is intended to achieve five objectives.

First, it establishes a clear distinction between infrastructure that must remain under strong sovereign control, infrastructure that should operate as neutral shared national rails, and services that should remain open to innovation and competition.

Second, it defines the level and form of State participation required across each domain to protect national sovereignty, security, continuity, and public trust.

Third, it provides a governance basis for strategic shareholding partnerships with operators, users, institutional investors, and development partners so that nationally significant digital entities can attract capital and technical capability without compromising public interest.

Fourth, it ensures that the implementation of digital government remains aligned to Government's endorsed enterprise architecture and does not revert to fragmented agency-by-agency procurement.

Fifth, it creates a practical structure through which digital public infrastructure, AI-ready infrastructure, and digital government services can scale together as one national system. This is consistent with the broader logic of the strategy, which treats shared digital rails and interoperable workflows as the foundation for sovereign digital government and AI adoption.

Governance Principles Across All Three Layers

Across all three domains, the State shall pursue a balanced model of sovereign stewardship and investable governance**.**

In principle, this means the State should remain strongest where the asset or function is foundational, systemic, non-substitutable, or security-sensitive, and should become lighter where the function is contestable and innovation-led. State participation should therefore not be uniform across the stack. Instead, it should be calibrated according to strategic importance, market maturity, and risk.

To ensure sovereign interest and long-term investor confidence at the same time, each entity operating within the framework should observe the following governance principles:[1]

[1] OECD Guidelines on Corporate Governance of State-Owned Enterprises

First, the rationale for State ownership or strategic participation should be explicit and publicly defensible. The State should hold assets where continuity, neutrality, public trust, economic security, or control of nationally significant digital infrastructure requires it.

Second, policy making, regulation, and ownership should be institutionally separated. The Ministry and Department should set policy and standards; the regulator should regulate; and state-invested operating entities should operate commercially and contractually within those rules. This separation is a core condition for good governance, competitive neutrality, and investor confidence.

Third, state-invested entities should be governed through professional, merit-based boards and transparent reporting obligations. Board appointments should be based on capability, not administrative convenience, and should include the skills required for technology, finance, law, risk, and strategic infrastructure.

Fourth, where strategic partners or minority investors participate, they should receive equitable treatment, transparent information rights, and clear protections against arbitrary dilution or politically driven related-party decisions. At the same time, those protections should not prevent the State, as controlling shareholder, from exercising legitimate influence over nationally significant assets.

Fifth, where an entity is required to discharge a public service obligation, that obligation should be clearly defined, transparently costed, separately funded where appropriate, and not hidden through cross-subsidisation that weakens commercial discipline or distorts the market.

Connectivity Utilities

The *Connectivity Utilities* layer comprises the physical and network infrastructure that underpins national digital access, hosting, transmission, and compute readiness. This includes national backbone fibre, subsea cable systems, data centres, sovereign or government cloud environments, international gateways where relevant, wholesale transmission assets, Internet exchange capability, and other strategic infrastructure required to support resilient digital services and AI-ready platforms.

At this layer, the State should maintain *strong strategic participation.* Connectivity infrastructure is foundational to national sovereignty, economic resilience, and service continuity. Accordingly, the State should retain controlling influence over the most strategic assets either through majority ownership, a golden share, or equivalent reserved rights over matters of national importance. However, sovereign control does not require the State to finance or operate every asset alone. Rather, the preferred model is one where the State anchors the layer through a dedicated holding or utility structure, while crowding in co-investment

from development partners, institutional capital, operators, and other strategic investors under a transparent governance framework. World Bank guidance on DPI sustainability explicitly supports this combination of public resourcing and crowding in private investment.[2]

The State's role in this layer should therefore be to protect strategic control, define open-access obligations, ensure redundancy and resilience, and maintain policy alignment with national digital infrastructure priorities. The commercial role of the operating entities should be to build, expand, lease, and monetise infrastructure on fair and nondiscriminatory terms. Where private or minority investment is introduced, the entity should remain governed as a commercially disciplined infrastructure utility, not as a line department extension. This is the balance required to keep the entity sovereign in purpose but bankable in form.

Digital Public Infrastructure Utilities

The *Digital Public Infrastructure Utilities* layer comprises the trusted national digital rails on which both government and private sector services depend. This includes digital identity, digital payments, secure interoperability and data exchange, trust registries, authentication services, consent frameworks, and other nationally reusable public digital building blocks.

At this layer, the State should maintain decisive sovereign control over governance, standards, and neutrality, because these systems are not ordinary commercial applications; they are shared national rails that must remain interoperable, trusted, and non-discriminatory. OECD's recent DPI work underscores the central role of government in designing, developing, and managing DPI precisely because it is foundational to coherent digital government implementation.

However, sovereign control at the DPI layer should not mean closed-state monopolisation of every operational activity. The better principle is that the State should control the *rules, trust framework, certification logic, operating mandate, and neutrality obligations,* while allowing certified ecosystem participants to connect, build services, and co-invest in expansion under those rules. The entity or entities operating this layer should therefore be state-controlled, but designed to be partnership-capable. Strategic minority participation may be appropriate from ecosystem actors whose usage helps scale the utility layer, provided the State retains control over governance, access rules, standards, and the strategic evolution of the rails. This is especially important for platforms such as digital ID, data exchange, and payments, which must remain trusted across sectors.

The DPI operating function should thus be neutral across users and sectors, interoperable by design, governed through open standards, and protected from

[2] *Digital Public Infrastructure And Development: A World Bank Group Approach*

fragmentation, exclusive control, or discriminatory access arrangements. Its commercial model should reward scale and service adoption, but not permit capture of the national rails by any single operator or downstream market participant. That approach aligns with both the logic of DPI and the governance protections needed for public trust.[3]

Competitive Digital Services

The *Competitive Digital Services* layer comprises the applications, platforms, workflow systems, and sector-specific services built on top of Connectivity Utilities and DPI Utilities. This includes G2C and G2G service platforms, sectoral digital solutions, workflow systems, enterprise applications, AI-enabled public service tools, and wider market-facing services delivered by domestic firms, state-invested entities, or international partners.

As a general principle, this layer should remain open, contestable, and innovation-driven. The State should not seek to dominate every downstream digital service market. Rather, the State should set the architecture, standards, and service priorities for public-interest systems, while enabling a wide range of firms and partners to participate in delivery.

However, for core government transformation, the State should maintain an invested delivery arm within this layer. Papua New Guinea should therefore establish or designate a *National Digital Service Integrator* operating as a *government transformation integrator and project management office* for core G2C and G2G services. This entity would not exist to monopolise all service delivery. Its purpose would be to act as Government's implementation arm for nationally significant service transformation programmes that must align with the endorsed enterprise architecture, shared DPI rails, interoperability standards, cybersecurity controls, and whole-of-government delivery roadmap.

Its functions should include enterprise architecture assurance, programme management, systems integration, vendor and contract management, reuse of common components, quality assurance, migration from legacy systems through phased integration, and end-to-end oversight of the implementation of high-priority digital government services. This mirrors the role performed in different forms by central digital delivery bodies such as the UK Government Digital Service and Singapore GovTech, and aligns with World Bank recommendations for a central PMO to keep e-government implementation on time, on budget, interoperable, and strategically coherent.

The State should therefore participate in this layer in two ways. First, as *policy setter and platform steward*, through the Department and the national governance

[3] *Digital Public Infrastructure For Digital Governments Oecd Public Governance Policy Papers No. 68*

architecture. Second, as *state-invested integrator for core public service delivery*, through the National Digital Service Integrator. Outside this core public implementation function, the wider market for digital services should remain open. Private firms should be able to compete to build modules, applications, managed services, and sector-specific platforms on top of national rails. In this way, the State remains strong where coherence, architecture, and national service delivery require it, while the broader services market remains investable and innovative.[4]

Strategic Shareholding Partnerships

Across all three layers, strategic shareholding should be used selectively and differently according to the nature of the layer.

In *Connectivity Utilities*, strategic shareholding should be used primarily to mobilise long-term infrastructure capital, strategic operational expertise, and user-aligned investment, while preserving sovereign control over critical infrastructure assets.

In *DPI Utilities*, strategic shareholding should be more tightly controlled and used mainly to deepen ecosystem adoption, technical capability, and integration, not to transfer control over the national rails.

In *Competitive Digital Services*, strategic shareholding may be broader and more commercially oriented, especially where it supports scale, innovation, export potential, or industry-specific expertise. But where the State's invested integrator is concerned, its mandate should remain focused on core digital government implementation and not drift into undisciplined participation across all contestable digital markets.

For investor confidence, all such entities should operate under clear shareholder agreements, board charters, reserved matters, information rights, audit obligations, and transparent dividend and reinvestment policies. The State's sovereign interest should be protected through governance design, not through day-to-day administrative interference. That is the discipline that allows national digital entities to remain both strategic and investable. OECD's SOE guidance is clear that ownership entities should exercise shareholder rights effectively, while remaining institutionally distinct from policy and regulatory functions, and boards should be professional and shielded from undue political influence.

9.3 Single Enterprise Architectural Governance

[4] "The OECD Digital Government Policy Framework: Six dimensions of a Digital Government", OECD Public Governance Policy Papers, No. 02, OECD Publishing, Paris.

To operationalize the Single Enterprise Architecture for Core Digital Services, the governance framework will be structured to ensure clear policy authority, strong oversight, and disciplined, whole-of-government implementation. The Department of Digital Transformation and AI will be mandated as the central policy and architecture authority, responsible for defining, maintaining, and continuously evolving the national enterprise architecture framework, including technical standards, interoperability protocols, data governance requirements, cybersecurity baselines, and design principles aligned to the Digital Public Infrastructure (DPI) approach. Oversight and compliance will be exercised through the Digital Transformation and AI Board, established under the Central Agencies Coordinating Committee (CACC), which will serve as the apex governance body to approve architecture standards, enforce cross-government alignment, and resolve institutional conflicts relating to digital investments and system integration.

Kumul Digital Infrastructure Holding Ltd (KDIHL) will function as the implementation and state investment arm, responsible for translating policy into execution. In this role, KDIHL will:

- design, build, and operate core DPI platforms, including digital identity, payments, and data exchange layers;
- manage and scale shared digital infrastructure assets such as Government Cloud and national platforms;
- structure and manage strategic partnerships with private sector technology providers and development partners; and
- ensure that national digital platforms are delivered in a commercially sustainable and technically resilient manner.

To institutionalize compliance and prevent fragmentation, all government ICT investments and digital initiatives will be subject to a mandatory alignment and assurance regime. This will require that:

- all systems integrate with core DPI services, including SevisPass for identity, SevisDEx for data exchange, and national payment rails where applicable;
- all projects adhere to approved national architecture standards and technology guidelines;
- all significant ICT investments undergo centralized review and approval prior to funding and procurement; and
- all agencies progressively transition legacy systems toward interoperability with the national architecture.

This governance model ensures that Papua New Guinea achieves a unified and interoperable digital foundation, while maintaining a federated approach to sector-specific systems, thereby balancing national consistency with institutional autonomy.

10. Implementation Roadmap

11. Expected Outcomes

The National Sovereign AI Strategy is expected to deliver measurable economic value by improving productivity, reducing transaction costs, expanding formal participation in the economy, and enabling new digital markets. These outcomes will be driven by the integrated application of Digital Government, Digital Public Infrastructure (DPI), and Artificial Intelligence, positioning technology as a structural enabler of economic transformation rather than a standalone intervention.

11.1 Economic Baseline and Context

Papua New Guinea enters implementation of this Strategy with strong economic potential but a relatively low level of digital maturity. As at 2024, the economy is estimated at approximately **PGK 120–125 billion in GDP**, with an endorsed

population of **10.1 million people (December 2025)**. Despite continued economic growth, large segments of the economy and public administration remain characterized by manual processes, fragmented systems, and limited interoperability.

Digital adoption remains below global averages, constraining participation in digital services and markets, while financial inclusion—although improving—remains incomplete, particularly in rural and informal sectors. Government systems are largely siloed, resulting in duplication, inefficiencies, and elevated transaction costs. Importantly, Papua New Guinea does not yet have a formal digital economy measurement framework, limiting the ability to fully quantify the contribution of digital transformation to GDP.

The Digital Government Plan 2023–2027 previously estimated a baseline economic uplift of approximately **PGK 1.0 billion over 10 years**, demonstrating that even targeted digital reforms can yield measurable economic returns. The present Strategy builds on this foundation by introducing a broader, system-wide transformation anchored on AI and shared digital infrastructure.

11.2 Economic Impact Pathways

The Strategy will generate economic value through a set of mutually reinforcing pathways. First, productivity will be enhanced through the digitization and automation of government workflows, supported by AI-enabled decision systems that improve efficiency, accuracy, and timeliness in areas such as recruitment, procurement, budgeting, and service delivery. Second, transaction costs across the economy will be reduced through the deployment of shared digital infrastructure, including digital identity, payments, and secure data exchange, which simplify interactions between citizens, businesses, and government.

Third, the expansion of digital identity and payment systems will enable greater financial and economic inclusion, allowing more citizens and small businesses to participate in formal economic activity. Finally, the establishment of trusted national digital platforms will create a foundation for private sector innovation, enabling new services, business models, and investment opportunities to emerge on top of government-led infrastructure.

11.3 Indicative Economic and Fiscal Impact

Based on international evidence and Papua New Guinea's current economic baseline, indicative modelling suggests that the Strategy can deliver significant long-term economic gains. Using a GDP baseline of approximately PGK 120 billion, the Strategy could generate an annual economic uplift at maturity in the range of:

- **PGK 960 million per year (0.8% of GDP)** under a conservative scenario of partial implementation

- **PGK 1.8 billion per year (1.5% of GDP)** under a base scenario of successful DPI and AI deployment across government
- **PGK 3.0 billion per year (2.5% of GDP)** under an accelerated scenario of widespread adoption across both public and private sectors

In addition to broader economic gains, the Strategy is expected to deliver fiscal benefits through improved compliance, reduced leakage, and more efficient revenue collection. Indicative estimates suggest a potential annual fiscal upside in the range of **PGK 100 million to PGK 300 million**, alongside significant improvements in public sector productivity, including reduced processing times, lower administrative costs, and enhanced transparency and accountability.

11.4 Strategic Economic Outcomes

Over the medium to long term, the Strategy is expected to increase the contribution of the digital economy to national GDP, reduce transaction costs across key sectors, and expand financial inclusion and digital participation. It will improve the efficiency and effectiveness of public expenditure, strengthen domestic capacity in digital and AI-enabled services, and stimulate investment in connectivity, cloud infrastructure, and data-driven innovation.

At a broader level, the Strategy will support the development of a national digital ecosystem in which government platforms serve as a foundation for private sector growth. This includes enabling local firms, developers, and service providers to build solutions on top of national digital infrastructure, while progressively positioning Papua New Guinea as a regional node for digital infrastructure and trusted digital services.

11.5 Measurement and Evaluation Framework

To ensure that economic outcomes are systematically measured and validated, a dedicated Monitoring and Evaluation (M&E) Companion Document will be developed to support the implementation of this Strategy. This framework will adopt internationally recognized methodologies, including the establishment of a digital economy measurement baseline through Digital Supply-Use Tables and, over time, a Digital Economy Satellite Account.

Macroeconomic impacts will be assessed using scenario-based modelling calibrated to national data on connectivity, digital transactions, and technology adoption, while program-level cost-benefit analysis will be applied to key reform areas such as procurement, payroll, and service delivery to quantify efficiency gains and cost savings. In parallel, institutional performance and digital maturity will be tracked using adapted global benchmarks for digital government and GovTech.

Key indicators will include digital economy contribution to GDP, digital identity uptake, transaction volumes across national payment systems, service integration

levels, financial inclusion metrics, and improvements in government efficiency and revenue performance. Together, this framework will ensure that the Strategy is not only implemented effectively, but also delivers measurable and sustained economic impact.