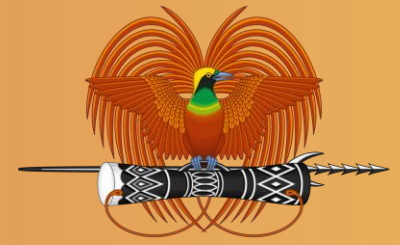




Department of Information And
Communications Technology



Business Council PNG's 7th Future's Forum

1 Day Workshop

Presented by:
Jessy Sekere

Executive Manager, Digital Government Coordination & Shared
Service

*August 14, 2025 /The Hilton Hotel
Port Moresby, National Capital District, Papua New Guinea*



Presentation Outline:



- ✓ Introduction: Mandate & Vision
- ✓ Governance Framework - GovPNG Tech Stack | DPI Approach | PAERA
- ✓ GovPNG Technology Stack: Six-Layer Architecture
 - ✓ GovTech Stack layer 1:  Governance (Policies, standards, Guidelines, etc.)
 - ✓ GovTech Stack Layer 1: Cyber Security
 - ✓ GovTech Stack layer 2: Communications
 - ✓ GovTech Stack layer 3: Hosting (Gov Leased Cloud)
 - ✓ GovTech Stack layer 3: Hosting (Website & Email Standardization)
 - ✓ GovTech Stack layer 4: Reusable Building Blocks (DPI Approach)
 - ✓ GovTech Stack Layer 5: Digital Services (G2C, G2B, G2G)
 - ✓ GovTech Stack layer 6: eGovPortals (G2G, G2B, & G2C)
- ✓ DTO Coordination: Section 9 mandate
- ✓ DTO Coordination: CoC Process (Section 14 & 15)
- ✓ Digital Future Vision
- ✓ DICT Contact Information
- ✓ End of Presentation



Introduction: Mandate & Vision



DICT's Leadership Role

The Department of Information and Communications Technology (DICT) is leading the Papua New Guinea Government's digital transformation through the **Digital Government Program**, underpinned by structured coordination with Digital Transformation Officers (DTOs) or ICT managers.



National Vision

Create a secure, inclusive, and interoperable digital ecosystem, guided by the Digital Government Act 2022 and aligned with national development objectives.



DTO Network

DTOs have become instrumental in translating policy into action across public bodies, ensuring a consistent and scalable approach to digital services rollout.



Comprehensive Approach

Our digital transformation efforts encompass cybersecurity, cloud infrastructure, GPN, data governance, and service delivery - all coordinated through a unified framework that supports both national agencies and autonomous regions like ABG.



Three National Digital Frameworks

The **Digital Government Program** is guided by three strategic frameworks that ensure cost-effective, agile, and future-ready technology delivery:



1. GovPNG Technology Stack

A six-layered technical architecture providing a common, reusable, and secure foundation for all digital services and platforms across government.



2. Digital Public Infrastructure (DPI) Principles

Ensures digital systems are secure, inclusive, citizen-centered, and rights-based, aligned to the broader public good and democratic governance.



3. PAERA Framework

Prioritizes Public Good, Accessibility, Efficiency, Reliability, and Affordability in the design and delivery of digital initiatives across all government levels.



Strategic Implementation

These frameworks serve as the strategic backbone for how we deliver technology solutions that are cost-effective, scalable, and aligned with both national objectives and regional autonomy requirements like those of government agencies and ABG.



GovPNG Technology Stack: Six-Layer Architecture



GovPNG Technology Stack

"A national framework that guides the use and adoption of technology by government agencies in Papua New Guinea"

For far too long, the Government of PNG has in the past, adopted technology through siloed approach where each agency is deploying its own technology. What is the result? Duplication of investments. Wasted Resources. Confusion in service delivery.

In 2023, the PNG Department of ICT launched the PNG Government Technology Stack — our national framework to guide how government adopts and deploys technology.



Better Experience

Enhanced user experiences across all government services



Smart Deployment

Smarter, scalable technology deployments



Certificate of Compliance Process

To ensure all government agencies are aligned to the Technology Stack, every government ICT project must pass our Certificate of Compliance process before implementation.



WoG Approach

Whole-of-Government coordinated technology deployment



Pacific First

Pacific-first solutions tailored for regional needs



Global Best Practice

Many other countries such as Singapore, Korea, and India are taking similar approach to standardized government technology frameworks.



GOVPNG TECHNOLOGY STACK

'a national framework to guide the use of technology therefore enabling a digital government for Papua New Guinea'



Better Experience



WoG Approach

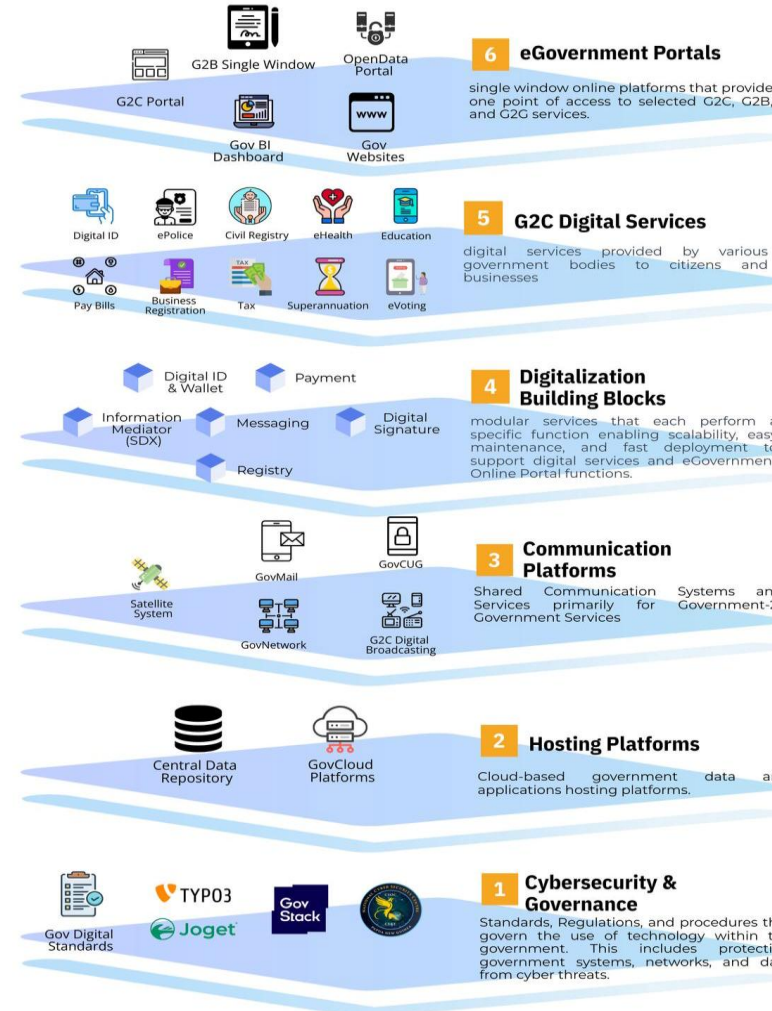


Smart Deployment



Pacific First

stack components



implementing agencies



Updated July 2024



Digital Government & ICT Policies

The Department of DICT has established a robust policy framework to guide digital transformation, cybersecurity, and data governance, aligning with national development goals and advancing digital governance through the Digital Government Act 2022.

Approved DICT Policies

- ✓  Digital Transformation Policy 2020
- ✓  National Cyber Security Policy 2021
- ✓  Government Cloud Policy 2023
- ✓  National Data Governance & Data Protection Policy 2024
- ✓  National Cyber Security Strategy 2024-2030
- ✓  National Media Development Policy 2024

Policies Under Consultation:

- ❖ Digital ID Policy (before NEC for approval)
- ❖ Social Media (e-Safety) Policy (before NEC for approval)
- ❖ Artificial Intelligence (AI) Policy (in draft)
- ❖ Universal Access and Services Policy (finalized and ready for NEC)
- ❖ National Broadband Plan (finalized and ready for NEC)

Approved Standards:

- ✓ Email standards
- ✓ Website Standards
- ✓ Social Media Standards
- ✓ Cyber Security Standards
- ✓ DTO Guidelines
- ✓ DTO Manuals

Standards under review and Draft

- ❖ Data Standards
- ❖ API Standards
- ❖ DPI Standards
- ❖ Integration/Interoperability Standards
- ❖ Digital ID Standards



Cybersecurity

Foundational policies and oversight mechanisms ensuring security, data protection, and responsible digital operations:

- ✓ Anchored on Section 16 of the Digital Government Act 2022
- ✓ Cybersecurity Policy & Strategy, Data Governance & Data Protection Policy, Cloud Policy
- ✓ National Cybersecurity Centre (NCSC)
- ✓ CERT and SOC functions
- ✓ Social Media Monitoring & Defense (SMMD)

National Cybersecurity Centre (NCSC) – Initiated during 2018 APEC Summit

Initiated during 2018 APEC Summit under the Australian Government administration until 2021 when it was transitioned to DICT under the National Cybersecurity Policy 2021 direction under NEC Decision 41/2021

At the time it Monitored cyber threats across few government agencies. This was formally established under Section 18 of the Digital Government Act 2022.

National Cybersecurity Centre (NCSC) - Established under Section 18

Monitors over **25 government agencies and 1,402 endpoints**, leveraging Shadow server's global security data lake for threat intelligence.

Agencies onboarded to NCSC have reported no cyber attacks, while non-onboarded agencies have faced recent incidents. DICT encourages all agencies to join NCSC for enhanced protection.

Security Operations Center (SOC)- Established under the NCSC

Monitors threat across more than **100 public bodies** integrated with the Government Cloud through the Checkpoint and manages firewall infrastructure for critical agencies.

Provides 24/7 cybersecurity monitoring for all national agencies, provincial governments, and autonomous regions connected to the NCSC and onboarded on the GovCloud.



Communications Layer

Establishment of Government Private Network (GPN) by leveraging on communications providers such as DataCo, Telikom, etc including satellite providers for connectivity solutions, ensuring:

- ✓ Secure inter-agency communication
- ✓ Real-time collaboration
- ✓ Encrypted data exchange facilitated through the secure network
- ✓ High-speed connectivity

Government Digital Infrastructure & Partners

We maintain a small infrastructure team under infrastructure branch within the Digital Government Wing of the Department.

We are currently partnering with DataCo through the recently signed Managed Services Agreement (MSA) in addressing data localization and sovereignty including establishment and implementation of Government Private Network (GPN)

Government Private Network (GPN) - Established under Section 22

Proof of concept completed, with a pilot phase underway for 10 agencies, starting with one district and a Government Agency.



🌐 Hosting Infrastructure

Centralized cloud hosting critical for digital service delivery:

- ✓ AWS, Oracle, Alibaba, Azure, Alibaba, etc. including DataCo among others which have been declared as CSP that Gov Agencies including provincial administrations and agencies can leverage
- ✓ 100+ public bodies on Leased GovCloud (AWS)
- ✓ DataCo MSA implementation for Hybrid DataCentre Infrastructure and GPN connectivity

🌐 **Government Cloud - Government Leased Cloud Infrastructure established under Section 25 Operational since 2023**, hosting over 100 public bodies, including national agencies, provincial authorities, Public Health Authorities (PHAs), and districts including ABG.

Upgraded in 2024 with Deloitte's assistance, incorporating advanced cloud security features ("Checkpoint") which now integrates with the SOC. Next upgrade is in progress.

🌐 Hosting of DNS, Emails, Websites on GovCloud

Under the GovCloud, DICT Centrally manages the .gov.pg domains and government websites for all public bodies, with websites developed for all 22 provinces, select districts, and PHAs.



GovTech Stack layer 3: Hosting (Website & Email Standardization)



Government Website & Email Standardization – Required under Section 38, 29, 40 & 41

Standardized digital presence ensures consistency, security, and professional representation across all government entities under the .gov.pg domain structure, including ABG agencies.

.gov.pg Domain Standards – required under Section 38

- ✓ Centralized domain management
- ✓ Consistent naming conventions
- ✓ Security certificate management
- ✓ DNS infrastructure support
- ✓ Subdomain allocation for agencies including ABG

Website Design Guidelines - – required under Section 40

- ✓ Consistent visual identity
- ✓ Accessibility compliance (WCAG)
- ✓ Mobile-responsive design
- ✓ Security best practices
- ✓ Content management systems

Email System Standards – required under Section 39

- ✓ Formal @agency.gov.pg email addresses
- ✓ Secure email infrastructure
- ✓ Anti-spam and security filtering
- ✓ Backup and archiving systems
- ✓ Mobile device compatibility

Security Requirements

- ✓ SSL/TLS encryption mandatory
- ✓ Regular security updates
- ✓ Vulnerability scanning
- ✓ Data protection compliance
- ✓ Incident response procedures

Government Agencies Implementation Support

DICT provides comprehensive technical support for agencies including ABG to implement these standards, including domain setup, email configuration, website development guidance and ongoing maintenance support. This includes standardization of social media accounts required under Section 41



GovTech Stack layer 4: Reusable Building Blocks (DPI Approach)



SevisPass (Digital ID as Verifiable Credential) – As per Digital ID Policy 2025 (Pending NEC Decision)

Secure Digital Identity System providing unique and verifiable credentials for citizens and businesses

Enables secure authentication across all government digital services and platforms including businesses, supporting both online and offline verification scenarios while maintaining privacy and security.

SevisDEx (Secure Data Exchange Platform) - Established under Section 31

Trusted Data Sharing Infrastructure facilitating secure data exchange between government agencies

Enables interoperability and data sharing while maintaining privacy, security, and compliance with data governance policies. Supports real-time and batch data exchange across all government levels.

SevisPay (Digital Payment Gateway)

Centralized Payment Gateway for all government digital transactions and fee payments. Supports multiple payment methods and provides secure, auditable transaction processing for all government services, including integration with local and international payment systems.

Integrated Digital Ecosystem

All SevisPNG components work together to create a **comprehensive digital government ecosystem**:

- ✓ **SevisPass** provides secure identity verification and authentication
- ✓ **SevisPortal** offers unified service access and citizen experience
- ✓ **SevisWallet** manages digital credentials, certificates, and transaction records
- ✓ **SevisDEx** enables secure data sharing and interoperability between agencies
- ✓ **SevisPay** processes all government and business payments and financial transactions securely

Multi-Level Government Integration

The Digital Government program is designed to serve all levels of government, from national agencies to provincial governments and autonomous regions, ensuring consistent service delivery and digital experience for all PNG citizens while respecting local governance structures.



Digital Services

What are Digital Government Services?

Digital government services represent the transformation of traditional government operations into online, accessible, and efficient digital platforms. These services are categorized into three main models based on the relationship between government and different stakeholders:

- ✓ **G2G (Government-to-Government)**
- ✓ **G2C (Government-to-Citizen)**
- ✓ **G2B (Government-to-Business)**

These three core models enable seamless interaction, improved efficiency, and enhanced service delivery across all levels of government engagement.



G2C

Government-to-Citizen

Digital services that government provides directly to individual citizens, enabling them to access government services online 24/7 without visiting physical offices.

PNG EXAMPLES:

- ✓ **MyIRC** - Online tax services
- ✓ **e-Police clearance** - Digital police certificates
- ✓ Online passport applications
- ✓ Birth/death certificate requests
- ✓ Voter registration
- ✓ License renewals



G2B

Government-to-Business

Digital platforms designed for businesses to interact with government agencies, streamlining regulatory compliance, permits, and business-related government services.

PNG EXAMPLES:

- ✓ **IPA online registration** - Investment promotion services
- ✓ **IRC online TAX** - Business tax management
- ✓ Business registration & licensing
- ✓ Permit applications
- ✓ Government procurement portals
- ✓ Import/export documentation



G2G

Government-to-Government

Internal digital systems that enable different government agencies and departments to share information, coordinate activities, and collaborate efficiently.

EXAMPLES:

- ✓ Inter-agency data sharing
- ✓ Budget management systems
- ✓ Employee management portals
- ✓ Policy coordination platforms
- ✓ Emergency response systems
- ✓ Digital document workflows



eGovPortals – Established under Section 35

Multi-stakeholder portals supporting access and collaboration:

- ✓ **SevisPortal (G2C)** - Project lead by DICT, focused on citizen facing services without visiting physical offices
- ✓ **Single Window (G2B)** - Project lead by Customs, Digital platforms designed for businesses to interact with government agencies, streamlining regulatory compliance, permits, and business-related government services.
- ✓ **G2G Portal** - Internal digital systems that enable different government agencies and departments to share information, coordinate activities, and collaborate efficiently (FMS, ALESCO Payroll)

SevisPortal (G2C eGovernment Portal) - Required under Section 31

Citizen-Centric Service Portal providing unified access to government services across all jurisdictions

Single point of access for citizens to interact with national, provincial, and local government services, ensuring consistent user experience regardless of service provider or location.

G2G eGovernment Portal (SevisPortal) – Progressive update

Supports online government service delivery across all jurisdictions. **Launched Version 1 in early 2024** with online police clearance services as a pilot.

In late 2024, DICT introduced **SevisPass (Digital ID), SevisPortal (eGovernment Portal V2), and SevisWallet (Digital Wallet) was launched**. Version 2 upgrades are in progress awaiting Digital ID policy approval by the NEC, targeting completion before the country's 50th anniversary in 2025.

SevisWallet (Digital Wallet)

Secure Digital Wallet for storing digital credentials, certificates, and transaction records

Integrates with SevisPass and SevisPay for comprehensive digital identity and payment management, allowing citizens to securely store and present their digital documents and credentials.



DTO Coordination: Section 9 mandate



Section 9 Mandate

DICT's coordination of DTOs stems from **Section 9 of the Digital Government Act 2022**, which mandates each public body to formally appoint a DTO. These officers serve as the agency's lead for digital transformation, ensuring alignment with national policies and implementation frameworks.



Monthly Coordination Sessions

- ✓ DICT hosts monthly DTO coordination sessions to:
- ✓ Share implementation updates and progress reports
- ✓ Surface operational challenges and solutions
- ✓ Introduce innovations and best practices
- ✓ Track compliance with digital government standards



Foundational Documents

- ✓ **DTO Manual:** Comprehensive guide outlining roles, responsibilities, tools and information available to DTOs
- ✓ **Compliance Manual:** Developed per Sections 14 and 15, supports evaluation, assessment and reporting of digital transformation projects



Current Participation

Today, **over 100 public bodies** are actively participating under this coordinated approach through the Digital Government program and other digital government initiatives, demonstrating the effectiveness of the DTO framework in driving Digital Transformation across government.



Coordination and Compliance - Mandated under Section 9, 14 & 15

DICT coordinates with government agencies via DTOs (Section 9) and participates in ICT steering committees for major government digital transformation projects.

Over 15 ICT projects have received Certificates of Compliance (CoC), including DCIEMS (Magisterial Services), ITAS & FMS (IRC), eBorder & IBMS (ICSA), FMIS (ABG), Bilum (DIRD), SaaS upgrade (Finance), GoLands (DLPP), NHTEM (DHERST), DataCentre Upgrade (Treasury), Digital HR Transformation (DPM), Digital Program (LCA), with several others pending deliberation by the next Public Service ICT Steering Committee Meeting.



DTO Coordination: CoC Process (Section 14 & 15)



Certificate of Compliance (COC) Overview

Mandatory certification process for major ICT projects ensuring alignment with national standards, security requirements, and best practices while supporting national agencies, subnational governments' and autonomous regions' digital initiatives.

1. Project Planning

Initial design and requirements gathering



2. COC Application

Submit to DICT through DTO coordination



3. Technical Review

DICT evaluation and steering committee assessment



4. COC Issuance

Approval, Certification and technical clearance for project implementation



COC Requirements – GovPNG Tech Stack, DPI & PAERA

- ✓ Security architecture compliance
- ✓ Data governance alignment
- ✓ Infrastructure standardization
- ✓ Cybersecurity protocols
- ✓ Interoperability standards



Benefits for All Government Levels

- ✓ Risk mitigation and security assurance
- ✓ Cost optimization through standards
- ✓ Technical support and guidance
- ✓ Integration with national systems
- ✓ Quality assurance and best practices



Multi-Level Government Integration

The DTO framework extends across all levels of government including national agencies, sub-national governments, ABG, and local government units, ensuring consistent digital transformation standards while respecting governance autonomy and local decision-making processes.



DICT Support Services



Whole-of-Government Coordination

Gov Agencies, sub-national governments including ABG can seek advisory services, business process mapping, project management support until suitable personnel are appointed to take up DTO roles within your agencies



Government Cloud Services

Gov Agencies, sub-national governments including ABG agencies are eligible to Cloud environment provisioning with secure, scalable infrastructure, esp. for Low Resource / Low Complexity Workloads while for High Resource / High Complexity Workloads will be referred to DataCo under the recently signed MSA between DICT & DataCo for hosting and Infrastructure



Infrastructure Support

.gov.pg domains, email systems, and website development assistance including infrastructure support and advice on data sovereignty solutions



Collaborative Partnership Approach

DICT recognizes Gov Agencies, sub-national governments including ABG's autonomous status and works collaboratively to provide support that enhances digital capabilities while respecting regional governance and decision-making processes. All support is provided as per the national policy frameworks with Gov Agencies, sub-national governments including ABG maintaining full control over its digital transformation priorities.



Cybersecurity Protection

Gov Agencies, sub-national governments including ABG are eligible for NCSC and SOC onboarding for comprehensive threat monitoring and firewall management



Certificate of Compliance

Assistance with COC applications and technical review processes by providing Section 14 and 15 forms for CoC application and guidance on the lodging process



General ICT and Policy Alignment Support

Guidance for Gov Agencies, sub-national governments including ABG agencies lacking specialized ICT personnel or expertise and require assistance from DICT to start their digital transformation journey and assistance in aligning their policies with national frameworks while maintaining their autonomy



Digital Future Vision



Digital Government Program Success

The Digital Government Program, driven by strong DTO coordination and underpinned by robust policy frameworks, is tangibly taking shape and progress in building a secure, inclusive, and connected digital government across Papua New Guinea.



Our Vision

Not only to modernize public service delivery but to enable **efficiency, accessibility, and economic opportunity** for all Papua New Guineans, including the people of special region of Bougainville through enhanced digital services.



Partnership Opportunities

DICT invites continued partnership with Gov Agencies, sub-national governments including ABG, private sector, civil society, and development partners as we work together to deliver a sustainable digital future.



Whole of Gov Agencies including Subnational and ABG-DICT Collaboration

The partnership with Gov Agencies, sub-national governments including ABG demonstrates how national digital transformation frameworks can successfully integrate with autonomous governance structures, creating opportunities for:

- ✓ Enhanced digital service delivery for all citizens
- ✓ Improved government operational efficiency
- ✓ Strengthened cybersecurity for critical infrastructure
- ✓ Cost-effective technology implementation
- ✓ Knowledge sharing and capacity building



Moving Forward

Through continued DTO coordination, policy alignment, capacity building, and collaborative innovation, we are building the foundation for Papua New Guinea's digital future - one that serves all citizens regardless of their location or government level while respecting regional and provincial autonomy and cultural diversity.



DICT Contact Information



Jessy Sekere

Whole-of-Government
Coordination & Compliance

 jessy.sekere@ict.gov.pg

 (675) 7317 3991

Hamilton Vagi /Nobert Wanit

Cybersecurity (NCSC and SOC
onboarding)

 hamilton.vagi@ict.gov.pg

 Nobert.wanit@ict.gov.pg

Liza Marie / Dika Davai

GovCloud (DNS, hosting)



lizarhmarie.warike@ict.gov.pg



dika.davai@ict.gov.pg

Jesse Biribudo / Joshua Pomaloh

Application Development &
Software Advisory

 jesse.biribudo@ict.gov.pg

 joshua.pomaloh@ict.gov.pg

John Pandi / Bartsch Morris

Emails and Infrastructure (GPN)

 john.pandi@ict.gov.pg

 bartsch.morris@ict.gov.pg

Allan Long /Nathan Randa / Pokana Nauairi

Policy Alignment



allan.long@ict.gov.pg



nathan.randa@ict.gov.pg



pokana.nouairi@ict.gov.pg



THANK YOU!

Advancing a Secure and Inclusive Digital Government

 visit: www.ict.gov.pg for more information

Strengthening partnerships from national to regional
levels