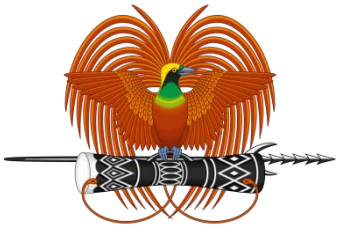

THE INDEPENDENT STATE OF PAPUA NEW GUINEA

NATIONAL CYBER SECURITY STRATEGY

2024 – 2030

Contents

MINISTER'S FOREWORD

In an era where our digital landscape shapes the very core of our nation's progress, Papua New Guinea stands at the intersection of opportunity and responsibility. As we traverse the digital frontier, the need to safeguard our cyber realms has never been more critical.

Our commitment to securing Papua New Guinea's cyber future is unwavering. This Cybersecurity Strategy serves as a blueprint, guiding us through the intricacies of the digital age. It is a testament to our dedication to protecting our citizens, fortifying our critical infrastructure, and positioning PNG as a beacon of cyber resilience in the Pacific.

As threats in cyberspace continue to evolve, so must our strategies. This document outlines not just a plan but a vision — a vision for a Papua New Guinea where every citizen is empowered, our businesses thrive securely, and our nation is a leader in the global cyber community.

Cyber resilience can play a crucial role in achieving sustainable development objectives, managing risk in national and international development investments, promoting the rule of law, contributing to international security and stability, and protecting and realizing human rights.

Through collective effort and strategic implementation, we aim to navigate the challenges ahead, creating a digital environment that fosters innovation, protects our interests, and ensures the prosperity of Papua New Guinea.

I extend my gratitude to all stakeholders, partners, and citizens whose collaboration and commitment are integral to the success of this cybersecurity journey. Together, let us secure Papua New Guinea's digital future.

Hon. Timothy Masiu, MP
Minister for Information and Communication Technology
Papua New Guinea

EXECUTIVE SUMMARY: OUR 2030 VISION

The Papua New Guinea's National Cyber Security Strategy (NCSS) delineates the nation's approach to fortifying its digital realm against cyber threats and assaults. This strategy is designed to forge a safe, resilient, and secure digital environment for citizens, businesses, and governmental entities. Embracing a risk-based methodology, the PNG NCSS harnesses technology and collaborative partnerships to bolster cybersecurity readiness across critical infrastructure and vital services.

Cybersecurity encompasses multiple stakeholders within the public domain, including policymakers, the private sector, law enforcement, academia, and civil society. Risks in cybersecurity demand analysis within a broader spectrum that incorporates legal, economic, and social elements, contributing to a more comprehensive management of cybersecurity threats and decision-making.

Technology evolves exponentially, and the threats associated with it grow increasingly sophisticated. With our escalating connectivity and reliance on Internet-based platforms and services, our vulnerabilities and exposure to cyber threats expand. While this expansion offers numerous opportunities, cyber threats have similarly advanced in recent years.

The PNG Government, through this Strategy, aims to instill trust in the online domain by bolstering businesses' cyber resilience, facilitating threat information sharing, delineating clear role expectations, and strengthening partnerships. Collaboration with industry is pivotal to safeguarding critical systems against sophisticated threats. The government pledges to confront illegal activities, leveraging offensive cyber capabilities against offshore criminals in compliance with international law.

Individuals also play a role in cybersecurity. The PNG Government pledges to enhance efforts to raise awareness of cyber threats and empower the community to adopt secure online behaviors.

Cybersecurity stands at the core of transitioning to a digital society, ensuring a trusted and secure digital economy that fosters confidence among participants and enables businesses to flourish.

The PNG NCSS seeks to mitigate risks associated with the rapid digital technology adoption across various sectors. It underscores the necessity for the government's technical and intelligence capabilities in cybersecurity to align with international standards. Priority areas include safeguarding critical infrastructure, promoting economic growth through digital technology utilization, enhancing cybersecurity skills and awareness among consumers, and fortifying public sector networks.

The strategy acknowledges the ever-changing technology landscape, recognizing that security measures can quickly become obsolete. It identifies malicious cyber activities aimed at compromising network confidentiality, integrity, or availability. The government is committed to ensuring the continuity of essential services amidst disruptive or sophisticated cyber-attacks.

The government acknowledges existing cybersecurity gaps and challenges. Recognizing that solutions require concerted efforts beyond mere documentation, key priority areas have been identified to enhance resilience and safeguard the people of PNG.

GLOSSARY OF TERMS

- **Critical infrastructure:** These are system and assets, whether physical or virtual, so vital to the Papua New Guinea. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. It includes those sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

- **Digital Assets:** Digital assets are broadly defined as any digital representation of value which is recorded, this is either on a cryptographically secured distributed ledger or any similar technology. A digital asset that has an equivalent value in real currency, or acts as a substitute for real currency, has been referred to as convertible virtual currency.

- **Cyber Education:** Includes technical and non- technical content at all levels to provide the knowledge and skills necessary to perform cybersecurity functions.

- **Cyber Awareness:** a learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure. It involves providing information about existing threats and takes into account knowledge combined with attitudes and behaviors that serve to protect digital assets and citizens online.

- **Cyber Resiliency:** The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment.

- **Cybersecurity:** The prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Cybersecurity is the process of protecting information by preventing, detecting, and responding to attacks. It takes into account the continuous and planned activities at the political, legal, economic, educational, awareness raising and technical levels to manage risks in cyberspace to ensure the ensure the confidentiality, integrity and availability of digital assets.

- **Cybercrime:** Is a crime that either uses services or applications in cyberspace are to carry out a crime or are themselves the targets of crime.

- **Cyber Incidents:** Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, and/or network.

- **Cyber Attack:** Cyberspace actions that create various direct denial effects (i.e. degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains. It is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization.

- **Electronic Evidence:** Is the information and data of investigative value that is stored on or transmitted by an electronic device.

- **Cyber bullying:** Is harassment carried out on the Internet, via social networks, video game chat, or instant messaging. This can include direct verbal or emotional abuse, exclusion from social groups, or spreading gossip and rumors, making public content that was intended to

be private, embarrassing the victim by impersonating them on social media, Posting embarrassing pictures, revenge porn.

- **Identity theft:** Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. It is the use of someone's personal information without permission for financial gain.

- **Phishing:** A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. It is the use of emails that appear to originate from a trusted source, to trick a user into entering valid credentials at a fake website. Typically, the email and the web site look like they are part of a bank the user is doing business with.

- **Ransomware**: Ransomware is a pervasive and highly destructive form of cybercrime with tangible and severe repercussions. Its reach extends across critical sectors, including hospitals, educational institutions, municipal administrations, and vital public infrastructure. Malicious actors exploit vulnerabilities in network security, holding organizations' digital assets hostage with the primary objective of financial extortion.

  It is a type of malware that renders a victim's files, data, or computer systems as a whole inaccessible until a ransom is paid, often in cryptocurrency. Ransomware attacks may leave individuals, businesses, nonprofits, and governments grappling with compromised data and disrupted operations. Ransomware uses asymmetric encryption, generating a unique pair of keys for the attacker and victim. The private key, necessary for decryption, is stored on the attacker's server, and victims are often informed that the private key will be released to them only after the ransom has been paid. Ransomware attacks also can include an additional element of threat to expose data held by the ransomware criminals unless a further ransom is paid, sometimes known as "double extortion."

- **Revenge porn:** is a form of cyber bullying where nude or sexual photos or videos of someone are publicly posted. Often, sexual images exchanged during a relationship are posted by an angry ex when the relationship ends. Other times, accounts of celebrities are hacked and sexual images found there are posted. In a recent case, revenge porn was combined with politics, when the ex of a female politician gave sexual images to the organization of a political rival. The images were published, causing her to resign, which allowed the rival to run in the election to take her place. Another name for revenge porn is Non-Consensual Pornography (NCP).

STRATEGIC CONTEXT

Acknowledge past initiatives

Papua New Guinea (PNG) has made significant strides in bolstering cybersecurity through past initiatives such as the establishment of the Cybercrime Code Act (2016) and the National Cyber Security Centre (NCSC) in 2018 with Australian support. These efforts have laid a foundation for managing cybersecurity, conducting training, exercises, and collaboration domestically and internationally.

Acknowledge present situations

As PNG becomes increasingly reliant on information and communication technologies (ICT), cybersecurity risks are evolving rapidly. Global trends indicate a surge in cyber-attacks, driven by state-sponsored entities, criminal organizations, and issue-motivated groups. PNG's digital economy faces persistent threats, demanding urgent attention to safeguard critical infrastructure, public sector networks, and citizen data.

Acknowledge current initiatives

Recent domestic efforts include the establishment the approval of the National Cyber Security Policy 2021 through NEC Decision No. 348/2021 and the establishment of the National Cyber Security Centre (NCSC) by Section 18 and 19 of the Digital Government Act 2022, which serves as a pivotal cybersecurity centre responsible for managing cybersecurity operations. The NCSC encompasses functions such as the Cyber Security Operations Center (CSOC), Computer Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT), and Social Media Management Desk (SMMD), all aimed at enhancing cybersecurity resilience and countering cyber threats.

In PNG there is both a CSOC and a CERT. Both functions provide training, exercises, and collaboration with industry sectors within the government, and houses the network operational centre and the PNG CERT (computer emergency response team). The NCSC has taken measures to protect the networks of public organizations by rolling out end-point-network protection to certain government departments and agencies, and continuously monitoring the networks for threats as well as providing incident response support.

Social Media Management Desk (SMMD) is an added function. The SMMD team basically analyses the Social Media posts made by the citizens and counteract mis and disinformation on the platforms. They use the latest available software to derive insights and counteract the mis and disinformation with close collaboration with Facebook (Meta). They also do analysis of the data and provide intelligence on possible disorder based on the statistics of the spread of misinformation and disinformation. This responsibilities are based on recent experiences that the country went through.

What are we doing now

Currently, Papua New Guinea is intensifying its efforts to bolster cybersecurity resilience through various initiatives. These include the deployment of endpoint and network security solutions, the conduct of cybersecurity audits, and the proactive management of misinformation and disinformation on social media platforms. Moreover, collaboration among key units such as the National Intelligence Unit (NIO), RPNGC Cyber Crime Unit, and Office of Censorship is facilitated through the National Cyber Coordination Centre (N3C).

N3C coordination ensures that all cyber efforts by the organizations involved operate as per their mandate. They convene as and when the need arises, rather than adhering to a fixed schedule. Comprising various security agencies, including the National Cyber Security Centre (NCSC) with units like CSOC, CSIRT, and PNG CERT, as well as SMMD, RPNGC Cybercrime Unit, NIO, and Office of Censorship, the N3C operates on principles of information sharing and collaborative action to combat cyber threats and uphold national security.

We have joined with over 400 other governments and have adopted the Accra Call for Cyber resilience Development Framework. Key actions to consolidate this multi- faceted role include:

- Encouraging decision-makers across different strategic areas, including development, security, technology, and diplomacy, to integrate cyber resilience into national, regional, and international sustainable development strategies as a cross-cutting priority;

- Promoting the mainstreaming of cyber resilience across international development programming, including the roll-out of digital risk impact assessments in the design of initiatives, accompanied by digital risk mitigation and management plans during implementation;

- Accelerating the integration of the cyber capacity building community of practice with the development field to consolidate its links and approaches with broader development goals. This can be pursued, inter alia, by creating opportunities for more structured dialogues involving the respective communities, leveraging the convening power of existing multistakeholder platforms; and

- Strengthening and promoting cyber resilience knowledge and skills among international development workforce – including donors, implementors, and partner organizations – through the development and implementation of regular training and education courses.

Additionally, PNG collaborates with regional partners such as PACSON, GFCE, Interpol, and others to prevent, deter, and learn from best practices and solutions. The structured organization and concerted efforts of units like N3C, NCSC, and SMMD are pivotal in driving forward PNG's cybersecurity agenda, mitigating overlapping responsibilities, and fortifying overall cyber resilience across the nation.

What we are trying to do through this strategy

The PNG National Cyber Security Strategy aims to leverage on the current initiatives and what we are doing now to further fortify cybersecurity defenses by adopting a risk-based approach, leveraging technological advancements, and fostering collaborative partnerships across sectors and coordiating through centralized coordination mechnisms. Key objectives include;

- protecting critical infrastructure, promoting citizen prosperity through digital technologies, and ensuring overall cyberspace security,

- designing and implementing cyber capacity building initiatives that tackle both existing and emerging gaps across policy, technology, legal, regulatory, and institutional frameworks with activities customized to PNG's unique context and absorption capacity,

- investing in capacity building that enhances the cyber resilience of significant sectors in the economy and in public service delivery (such as essential services, critical infrastructure, as well as infrastructure that is critical to the availability and integrity of the internet), promotes a holistic risk management approach, and increases opportunities to prosecute and adjudicate cybercrime, and

- ensuring that all cyber capacity building investments and programs take into account the prevalent cybersecurity skills gap and its gendered dimension and adapt as necessary to include relevant and context-based education, skilling, reskilling, and upskilling activities, components or stand-alone initiatives that are sensitive to the needs of women and girls, the youth, persons with disabilities, rural and remote communities, vulnerable and marginalized groups.

What is ahead on our current evolving cyber landscape

Looking ahead, PNG acknowledges the need for adaptable security measures to address evolving cyber threats effectively. Collaboration with international partners, investment in infrastructure and training, and establishment of a supportive legal framework for cybercrime investigations are crucial steps in safeguarding PNG's digital future and promoting prosperity in cyberspace.

Why and what We Must Do Now

In PNG, the imperative to act swiftly in fortifying cybersecurity measures is deeply rooted in the escalating cyber threats that pose significant risks to the nation's security, economic stability, and the overall well-being of its citizens. The unique geographical and demographic landscape of PNG, coupled with its rapid digitization with the rapid misuse of digital tools, underscores the critical need for immediate action.

National security is paramount, and the increasing sophistication of cyber threats poses a direct risk to PNG's sovereignty as well as domestic security. As the country becomes more interconnected through digital channels, the potential vulnerabilities in critical infrastructure, government systems, and sensitive data repositories and misues of digital tools become more pronounced. Cybersecurity breaches have the potential to compromise sensitive national information, disrupt essential services, and undermine domestic security and the foundations of the nation's security apparatus.

Economic stability is another crucial facet demanding urgent attention. PNG's Vision 2050 envisions a diversified and knowledge-based economy, making the nation globally competitive. However, this very vision is jeopardized by the growing cyber threats that target economic infrastructures, financial systems, and business enterprises as well as growing misues of digital tools. The escalating digitization of financial services, trade, commerce, and availability of digital platforms heightens the urgency to secure these channels against cyber threats that could otherwise result in financial losses, economic downturns, and hindered national progress.

The well-being of PNG's citizens is intrinsically tied to the cybersecurity landscape. With an increasing reliance on digital platforms for communication, healthcare, education, and essential services, citizens are exposed to various cyber risks including the misuse of digital platforms resulting in spreading of mis and disinformation and inciting violences as witnessed in the recent past on the 'Black Wednesday"[1]. From personal data breaches to cybercrimes impacting individuals directly, the vulnerability of citizens demands immediate and effective cybersecurity measures.

We will commit to further professionalise the cyber capacity building community of practice. This includes developing practical tools and guides that can help stakeholders put into practice established principles, notably those defined in the 2017 Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building, the 2021 consensus report of the UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, and the Global Partnership for Effective Development Cooperation.[2]

[1] https://www.postcourier.com.pg/black-wednesday-a-dark-day-to-remember/

[2] For instance, such tools and guides could offer practical guidance on how to integrate results-oriented, human rights-based, gender-responsive and inclusion- sensitive approaches across cyber capacity building strategies,

We will accelerate efforts to improve the measurement of cyber capacity building results. This can be achieved by actively and systematically integrating methodologies and good practices from the international development field, such as: leveraging nationally-led statistical and monitoring mechanisms in developing countries to strengthen their data collection, metrics, and monitoring capacities in the field of cybersecurity; systematizing project monitoring and evaluation frameworks; as well as ensuring that cyber capacity building programming is adaptable to the findings of evaluation processes.

We will also encourage other Pacific Island countries to work closely with donor governments and partners to identify and employ the full range of financial streams available to weave sustainability into the financing of national cyber resilience activities, and design for financial and development additionality and to incorporate cyber resilience in development Frameworks.

We will diversify program implementation modalities used to support developing countries in strengthening their cyber resilience capabilities, and utilize all available options – from technical assistance, grants, budget support, blended finance, and loans – after assessing the most effective approach for meeting national needs and alleviating structural barriers to local actors' access to funding.

The urgency to fortify cybersecurity in PNG arises from the evolving threat landscape that directly jeopardizes national security, economic prosperity, and the safety and well-being of its citizens. Rapid digitization necessitates proactive strategies to safeguard critical assets and information, ensuring that the nation's journey towards its Vision 2050 is resilient, secure, and aligned with the global advancements in technology.

Why PNG has an Opportunity to Lead

PNG holds a distinctive position in the Pacific region, presenting a remarkable opportunity to emerge as a leader in cybersecurity resilience. In a landscape where digital threats are evolving, PNG has the potential to pioneer a robust cybersecurity strategy, setting an example for regional partners and affirming its commitment to fostering a secure digital environment.

As the largest, most populous and strategically located Small Island Developing Stated (SID) in the Pacific, PNG wields significant influence in regional dynamics. By taking a proactive stance on cybersecurity, PNG can establish itself as a beacon of resilience, not only safeguarding its own digital landscape but also demonstrating to neighboring nations the importance of strategic preparedness against cyber threats.

Crafting a comprehensive cybersecurity strategy tailored to the unique challenges of Small Island States (SID) is paramount. The diversity of its geographical and cultural landscape necessitates an approach that is not only adaptable but also inclusive for the SIDs. By doing so, PNG can exemplify how a nation can align its cybersecurity measures with its specific context, serving as a blueprint for other Pacific nations facing similar challenges.

Moreover, PNG's leadership in cybersecurity can bolster regional collaboration. By actively sharing best practices, threat intelligence, and technological advancements with neighboring countries, PNG can contribute to the collective resilience of the Pacific region against cyber threats. This collaborative approach not only enhances regional security but also fosters a sense of solidarity among Pacific nations in navigating the digital era safely.

project cycles, and processes

In seizing this opportunity to lead in cybersecurity resilience, PNG can elevate its global standing. A nation that effectively secures its digital infrastructure, systems and data becomes an attractive destination for international partnerships and investments. By demonstrating a commitment to a secure digital environment, PNG can attract businesses, technology innovators, and international collaborations that further contribute to its economic development and global relevance.

PNG stands uniquely poised to lead in cybersecurity resilience in the Pacific region. Through the crafting of a comprehensive strategy and a commitment to collaboration, PNG can set an example for its regional partners, showcasing the power of proactive and adaptive cybersecurity measures in navigating the complexities of the digital age.

VISION, GOALS AND STRATEGIC OBJECTIVES

Vision

PNG's vision is to create a safe, resilient, and secure cyberspace that enables innovation, enhances economic prosperity for all people and for all businesses, ensures the essential services that are needed to grow, and protect the country's sovereignty.

Mission

The mission of the NCS is to protect PNG's critical infrastructure, essential services, citizens, and businesses from cyber threats and attacks through effective cybersecurity governance, risk management, and incident response with counteractive measures.

Goals

The Primary goals of the NCS is to safeguard government ICT systems, critical infrastructure, businesses, and citizens against cyber threats and ensure online safety:

Goals	**Actions**
Establish a Legal and Regulatory Framework for Cybersecurity	• Develop a comprehensive legal and regulatory framework governing the use of ICT systems, ensuring effective cybersecurity measures while upholding citizens' privacy rights. • Strengthen legislation to support cybercrime investigations and prosecutions, fostering a secure online environment for all stakeholders. • Develop a Legislation for Critical Infrastructure to protect PNG's national critical infrastructures and services and essential sectors. • Develop a Legislation for online protection to protect children online
Enhance National Cyber Resilience Infrastructure	• Develop a National Cyber Security Strategy & Legislation that will elevate the NCSC to a NCSA and define the roles of key stakeholders on cyber security and the working relationship among these stakeholders for the protection of critical infrastructure. • Strengthen the resilience of critical infrastructure and government ICT systems against cyber-attacks, enabling uninterrupted essential services delivery during cyber incidents. • Invest in cybersecurity infrastructure, tools, and training to enhance the country's capacity to detect, respond to, and recover from cyber threats effectively. • Work closely to integrate best practices from our regional partners
Build a Robust Cybersecurity, Capacity, and Capability	• Develop a national cybersecurity capability capable of timely and effective detection and response to cyber threats, mitigating risks by identifying and countering cyber threats and malicious actors' tactics. • Develop a skilled cybersecurity workforce through comprehensive training and education programs, nurturing local expertise to address evolving cyber threats.
Foster a Secure Cyber Culture	• Cultivate a culture of cybersecurity awareness and education among government agencies, workers, businesses, citizens, and students empowering them to recognize and mitigate cyber risks proactively.
Enhance International Cyber Partnerships and	• Strengthen collaboration with our international partners to address shared cybersecurity challenges, recognizing the interconnected

ecosystem	nature of global cyberspace and the importance of collective action. • Strengthen the cybersecurity ecosystem through collaboration with international partners, leveraging collective expertise and resources to enhance cybersecurity resilience globally.
Promote Online safety and Cyber Security	• Encourage responsible online behavior by promoting critical thinking about identity and content sharing, fostering safe and respectful online interactions, and protecting personal privacy and data. • Promote cyber hygiene practices across various sectors, including education, government agencies, industries, and civil society, fostering a culture of cybersecurity awareness and resilience.
Uphold Ethical Integrity	• Foster informed decision-making in technology usage by promoting understanding of rights, responsibilities, and consequences of online behaviors, promoting ethical integrity in digital interactions.
Consider Digital Impact	• Harness emerging technologies to enhance societal well-being while considering their positive and negative impacts, promoting responsible and ethical technology use for positive digital transformation.

Principles:

A comprehensive understanding of cybersecurity is paramount to keep pace with emerging technologies and more sophisticated threats. Cybersecurity capacity should not only include the protection of networks and systems, but also take into account the people that rely more and more on Internet-enabled devices to conduct basic tasks.

Government Led

As the Government is one of the largest consumers of information technology services, it commits to driving the objectives of this Strategy by adopting best practices in its operations and lead by example in the implementation of the Strategy's objectives.

Risk based approach

Understanding of the importance of Critical Infrastructure and Systems to the welfare of all citizens of PNG the Strategy seeks to mitigate cybersecurity risks to acceptable levels by encouraging the combination of benefits, acceptable risks and other approaches with the desired end result of the protection of all PNG citizens, people, and the economy. The Cybersecurity Strategy will ensure that a risk-based approach is adopted by the private sector, the government, academia and civil society in assessing and responding to cyber-related threats or issues.

Capacity development:

The Cybersecurity Strategy will seek to enable the continuous development of the the GoPNG's capacity to address fast changing cybersecurity issues and developments.

Partnership and Collaboration

Cybersecurity affects everyone and as a result it is a shared responsibility for all to exercise cybersecurity best practices. Targeted awareness raising initiatives will be implemented through the mobilization and partnership with civil society, academia and other interest groups across PNG, to enable and empower end-users to keep themselves and their organizations safer online. Alliances and partnerships are also critical.

We cannot do this alone, not only do citizens need to work with the Government and private sector but we need to work closely and collaborate with our partners in PACSON, our allies including all pacific nations and territories and our regional partners in APEC and globally though the GFCE.

Fostering an environment for economic growth and innovation

Recognizing the importance of innovation and business development to our national economy, a cyber-environment that is safe and conducive to such development will be fostered.

FOCUS AREAS

Cyber Resilience & Cyber Defence Mechanisms

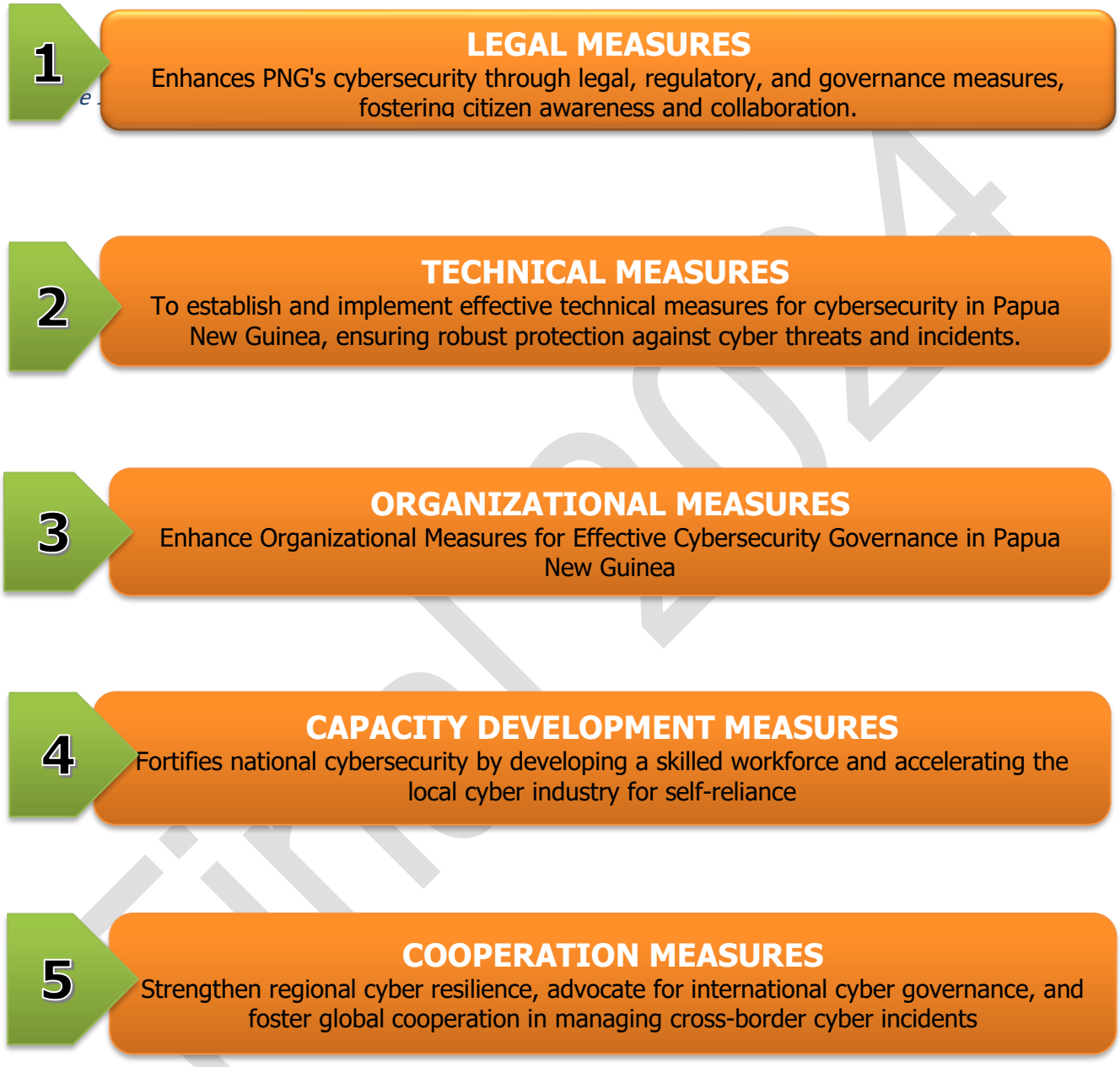

Figure 1: Strategic Focus Areas

Summary of the Strategic Objectives and Actions

Objective	Action
1: Legal Measures:	
Establish a Governance Framework and Policies for National Cybersecurity	• Strengthen coordination mechanisms and cyber security institutions to enhance capability and capacity in PNG. • Formulate and implement appropriate policies, legislation, regulations, and standards for cyber protection, addressing cybercrime and protecting citizens' rights and data. • Define the scope of critical infrastructure regulation for comprehensive coverage, enhancing cybersecurity obligations and compliance for resilient critical infrastructure. • Develop a detailed action plan and roadmap for a phased implementation of cybersecurity initiatives, with clear timelines and milestones. • Establish mechanisms for ongoing monitoring and evaluation of cybersecurity efforts, with regular reporting and feedback loops to the NCSC to track progress and address emerging challenges effectively.
Implement Legislative and Regulatory Framework for Cyber Security and Protection	• Develop and establish a legislative and regulatory framework for security and protection, ensuring conformance and compliance with international best practices and standards. • Develop national laws to recognize admissibility of electronic evidence in the courts to successfully prosecute offences. • Enforce cybersecurity obligations and compliance for resilient critical infrastructure, safeguarding citizens' rights and data against misuse and abuse.
Enhance Government Cybersecurity Uplift	• Develop and enact comprehensive legislation governing the use of ICT systems to provide a solid foundation for effective cybersecurity measures. • Clarify infrastructure regulations to ensure robust protection of critical systems and networks. • Implement measures to enhance the cybersecurity posture of the PNG Government, fostering collaboration among stakeholders to address emerging cyber threats. • Enforcement of Cyber Security, Digital Government and data Protection Standards in Government Agencies • Improve PNG's Cyber Security Ranking against Global and Regional Cyber Security Ranking.
Develop a Comprehensive Law on Online Safety	• Integrate provisions within the legal framework to address online safety concerns, including unauthorized access, interference, and interception of devices, computer systems, and data. • Ensure that the law provides clear guidelines for law enforcement, judicial clarity, and remit to those impacted by online criminal behaviors. • Incorporate regulations to combat racism, xenophobia, harassment, and abuse in the digital space, fostering a safe and inclusive online environment.
Promote National Cybersecurity Awareness	• Establish a governance framework and policies that promote national cybersecurity awareness and collaboration.

and Collaboration	• Foster collaboration among government agencies, private sector entities, civil society organizations, and academia to address cybersecurity challenges collectively. • Develop educational programs and initiatives to raise awareness about cyber threats and promote best practices for online safety and security.
2: Technical Measures	

Fully implement the National Cyber Coordination Centre (N3C)	• Formulate a Steering Committee comprising key stakeholder agencies to coordinate N3C, ensuring coordination and collaboration among various security agencies.
	• Co-lead by Security Coordination and Assessments (OSCA) and the Department of ICT, the N3C to serve as the nerve center for coordinating security agencies and implementing the cyber security policy 2021.
	• At the discretion of the National Security Council (OSCA)/DICT or in response to requests from any participating security agency, the N3C to be triggered. The activation of N3C to be subject to the following:
	  ○ When OSCA/DICT deems necessary to activate;
	  ○ During Emergencies;
	  ○ In Response to significant cyber-related crimes; and
	  ○ In response to requests from any participating security agency

Operational Units under NCSC	• Fully operationalize the established National Cybersecurity Coordination Center (NCSC) comprising operational units such as the Cyber Security Operations Center (CSOC), Computer Emergency Response Team (CERT), Cyber Safety & Security Awareness Unit (CSSAU), and Computer Security Incident Response Team (CSIRT). • The CSOC to monitor and defend whole-of-government critical infrastructures and systems, while the CERT collects and disseminates security information, • The CSSAU to drive national awareness on online safety and cyber security. • The CSIRT to respond to security incidents and conducts cybersecurity audits, and • Improve coordination among Government Aagencies on all cyber related issues combating cyber-crime. • Strengthening the monitoring and reporting processes of cyber security incidents. • Protection of Critical infrastructure for cyber security development. • Ensure to monitor all the public bodys through the CSOC under NCSC
Social Media Management Desk (SMMD)	• The SMMD to counter disinformation and misinformation and hate speech on social media.
National Intelligence Unit (NIO)	• Coordinate with the NIO for cyber intelligence analysis
RPNGC Cyber Crime Unit	• Leverage the Cyber Crime Unit of the Royal Papua New Guinea Constabulary (RPNGC) for cybercrime investigations and prosecutions.
Office of Censorship	• Collaborate with the Office of Censorship to counteract and censor

	unregulated cyber content, ensuring a safe online environment.
Enhance Technical Capabilities	• Develop and implement a national cybersecurity capability for detecting, responding to, and mitigating cyber threats in a timely manner. • Implement measures to ensure the trustworthiness of digital products and software, leveraging the GovPNG Technology Stack and encryption technologies. • Conduct regular assessments to identify and address weaknesses in critical infrastructure and government ICT systems.
Promote National Cybersecurity Awareness and Collaboration	• Establish a governance framework and policies that promote national cybersecurity awareness and collaboration. • Foster collaboration among government agencies, private sector entities, civil society organizations, and academia to address cybersecurity challenges collectively. • Develop educational programs and initiatives to raise awareness about cyber threats and promote best practices for online safety and security.
Risk Management and Compliance	• Implement measures to enhance the resilience of critical infrastructure and government ICT systems, ensuring continuity of essential services in the face of cyber-attacks. • Establish a comprehensive risk management framework for identifying, assessing, and prioritizing cybersecurity risks across critical infrastructure and essential services. • Set and enforce compliance standards, regulations, and guidelines aligned with international best practices and local cybersecurity requirements.
Cyber Threat Disruption	• Develop strategies to deter and disrupt cyber threat actors targeting PNG, collaborating with industries to dismantle ransomware business models and strengthen identity security measures.
3: Organizational Measures	
Develop a National Cybersecurity Strategy (NCS)	• Formulate a comprehensive NCS to allocate resources, identify cybersecurity objectives, and prioritize implementation efforts. • Establish a governance structure within the NCS to coordinate actions and monitor outcomes, fostering collaboration across industry, civil society, and academia. • Ensure the NCS promotes innovation, protects privacy, and enhances national cybersecurity resilience.
Establish National Cybersecurity Governance Bodies	• Create a dedicated national agency or ministry responsible for managing cybersecurity at the national level. • Designate a responsible agency as a leader in cybersecurity management, providing direction, coordination, and monitoring of cybersecurity activities and programs. • Develop organizational structures within the responsible agency to define roles, responsibilities, processes, and decision rights for effective cybersecurity posture.
Enhance Critical Infrastructure Protection	• Incorporate critical infrastructure protection into the NCS, ensuring a plan for safeguarding essential services like water, electricity, and telecommunications infrastructure and systems. • Collaborate with relevant stakeholders to prevent or mitigate disruptions to critical infrastructure, ensuring public order,

	economic stability, and national security.
Implement Lifecycle Management for NCS	• Integrate lifecycle management principles into the NCS to monitor, evaluate, and update strategies regularly. • Engage cybersecurity experts, businesses, and citizens in the NCS process to gather input, assess effectiveness, and make necessary adjustments. • Establish mechanisms for ongoing consultation and feedback to tailor the NCS to meet evolving cybersecurity challenges and national needs.
Develop Action Plans and Roadmaps	• Develop detailed action plans and roadmaps within the NCS to guide the implementation of cybersecurity strategies. • Allocate resources effectively, define roles and responsibilities, and track progress to ensure achievable and realistic cybersecurity goals. • Continuously assess and evaluate the impact of the action plans, making adjustments as needed to address emerging threats and changing environments.
Enhance Cybersecurity Metrics and Audits	• Establish cybersecurity metrics and benchmarks to measure cybersecurity development, risk assessment strategies, and audit effectiveness. • Conduct regular cybersecurity audits at the national level to identify vulnerabilities, assess risks, and prioritize corrective actions. • Utilize cybersecurity audit reports and assessments to improve cybersecurity posture and enhance resilience against cyber threats.
Cyber Safety and Security Awareness	• Develop a dedicated Child Online Protection (COP) Initiatives strategy within the NCS to protect children from online harm, abuse, and exploitation. • Establish reporting mechanisms for the identification and tracking of online issues impacting children, empowering individuals to report incidents and seek support. • Coordinate through National Cyber Coordination Centre to provide technical capabilities and support systems for child online protection • Incrase public awareness of online safety and cyber security and cyber crime in schools and on digital platforms such as social media.
4: Capacity Development Measures	
Develop Comprehensive Capacity Development Framework	• Formulate a national cybersecurity capacity development framework encompassing legal, technical, and organizational measures. • Establish clear objectives to bridge the skills gap and promote inclusivity in the technology ecosystem, focusing on building local skills, knowledge, and confidence.
Implement Public Awareness Campaigns	• Launch targeted public awareness campaigns to foster a cyber-aware society, empowering citizens to recognize and respond to cyber threats. • Tailor interventions to address specific concerns of SMEs, vulnerable populations, and other stakeholders, emphasizing identity security and ransomware prevention

Support SME Cybersecurity	• Empower small and medium-sized businesses with tailored cybersecurity support, providing resources and guidance to enhance their cyber resilience.
Develop Cyber Security capacity and capability	• Develop and implement a national cybersecurity capacity and capability to detect, respond to, and mitigate cyber threats effectively, ensuring continuity of essential services. • Strengthen law rnforcements capability or capacity to investigate and prosecute cyber criminals
Develop and Deliver Cybersecurity Training Programs	• Design and deliver training programs to enhance the skills and knowledge of PNG nationals in cybersecurity, fostering research, development, and collaboration with international partners.
Implement a Cybersecurity Workforce Development Plan	• Execute a plan to support the recruitment, training, and retention of cybersecurity professionals, ensuring a sustained and skilled cybersecurity workforce to address evolving threats.
Foster an Environment for Cybersecurity Research and Innovation and Economic Growth	• Promote and support cybersecurity research and innovation for the development and deployment of advanced cybersecurity technologies and solutions. • Encourage public-private partnerships to drive cybersecurity research and innovation within PNG, fostering an environment conducive to economic growth and self-reliance. • Stimulate local cyber industry, research, and innovation to foster economic growth, innovation, and cooperation within the public, private, civil society, technical, and academic communities.
Cyber Security Education	• Integrate cyber security education into school curriculums • Collaborate with Education Department to include cyber security/crime lessons in schools.
5: Cooperation Measures	
Establish Bilateral Cybersecurity Agreements	• Establish bilateral agreements between PNG and foreign governments or regional intergovernmental organizations that do not already exist to facilitate the exchange of cybersecurity assets, including information, expertise, policy, and technology. • Ensure that bilateral agreements promote cybersecurity capacity development by sharing best practices, upskilling personnel, enhancing collaboration, and developing operational procedures.
Promote Participation in Multilateral Agreements	• Advocate for PNG's participation in written multilateral agreements that define key cybersecurity parameters and set forward a common agenda for cybersecurity cooperation. • Encourage multilateral agreements that include capacity development components to support countries with weaker cybersecurity postures and confidence-building measures.
Facilitate Mutual Legal Assistance	• Strengthen regional and international cooperation and coordination through relevant institutions, treaties, and conventions to deal with cyber security • Aceede to the Budapest Convention and its two additional protocols, one on parliamentary of acts of a racist and xenophobic nature committed through computer systems and the second on enhanced co-operation and disclosure of electronic evidence. • Establish clear mechanisms for mutual legal assistance, including Mutual Legal Assistance Treaties (MLATs) with countries who have not signed on to the Budapest Convention, to facilitate cooperation on judicial matters related to cybersecurity. • Ensure that mutual legal assistance mechanisms cover a range of

	assistance forms, including service of documents, transmittal of evidence, and investigatory assistance.
Promote Public-Private Partnerships (PPPs)	• Encourage engagement in PPPs to harness innovations from the private sector and expedite the adoption of new cybersecurity technologies and practices. • Address challenges associated with PPPs, such as principal-agent problems and contract negotiation complexity, to maximize their effectiveness.
Foster Domestic Inter-Agency Partnerships	• Facilitate official domestic partnerships between different government agencies within PNG to enhance responsiveness to cybersecurity risks. • Encourage information and asset sharing between ministries, departments, programs, and other public sector institutions to strengthen the government's cybersecurity posture.
Regional Cyber Resilience Support and International Engagement	• Assist neighboring nations in building cyber resilience to foster regional cooperation and position PNG as a regional partner. • Advocate for and contribute to international cyber rules, norms, and standards to promote global cybersecurity governance. • Forge and foster cooperation with relevant international partners and institutions to manage cross-border cyber incidents and combat cybercrimes in alignment with applicable foreign policies, laws, treaties, and conventions.
Collaboration and Partnerships for Awareness	• Mobilize and partner with civil society, academia, and other interest groups to implement targeted awareness-raising initiatives. • Collaborate across stakeholder groups, including the private sector, civil society, academia, and the technical community, to promote cybersecurity best practices and overcome market barriers to secure technology adoption. • Improve awareness and transparency of cybersecurity practices to build market demand for more secure products and services. • Work with all Ministries, including the Ministry of Education and the Ministry of Higher Education, to integrate cybersecurity and cyber safety into future curricula, equipping students with relevant cyber knowledge and etiquette and generating interest in pursuing cybersecurity careers in PNG.

1 LEGAL MEASURES

Enhances PNG's cybersecurity through legal, regulatory, and governance measures, fostering citizen awareness and collaboration.

Policy and Legislation continue to play a key role in increasing protection and awareness of cybersecurity globally. The development and implementation of robust legal measures are essential for Papua New Guinea to effectively combat cyber threats, protect citizen rights, and foster a secure digital environment. These measures will serve as the cornerstone for enhancing cybersecurity capabilities and ensuring compliance with international standards.

The Government will take the lead to secure the digital Infrastructure and systems that powers our digital economy, and support the development of a healthy digital environment. Through the GovPNG Technology stack approach, the Government will work to make it safer, easier, and more secure to transact digital government services and also to pay for these services. Through new policies and standards the Government will be assisting citizens to secure their smart devices, use secure applications, and pay for government services.

Legislation provides the foundation for a harmonized regulatory environment, outlining roles, responsibilities, and response mechanisms to cyber threats. The legal framework ensures protection against misuse of technology, promotes cybersecurity practices, and facilitates international collaboration in combating cybercrime.

The legal measures will set basic response mechanisms to breach: through investigation and prosecution of crimes and the imposition of sanctions for non-compliance or breach of law. Laws protect general security and guarantee rights of citizens against abuse by others and ensures the protection against the misuse of the latest technologies. A legislative framework will set the minimum standards of behavior across the board, applicable to all, and on which further cybersecurity capabilities can be built.

Cybercrime Law

Cybercrime laws designate unauthorized (without right) access, interference, interception of computers, systems, and data. These laws may take the form of substantive and/or procedural law, public and/or private law, common law, case law, statutory law, administrative law, or other applicable forms of law. Legislation addressing unauthorized access, interference, and interception of computers, systems, and data. Papua New Guinea currently have a Cyber Crime Code Act (2016) which are now enforced but due to the evolving technological evolution, it the due for reviewed to adequately reflect the evolving cyber environment and address issues such as unauthorized online behaviour, illegal access, interferences, and interception including online identity.

Laws on Online Safety

Given the dampening activity of anti-social behaviors on online activities, making users and communities feel less safe, the regulation of certain behaviors is needed. Various online behaviors can negatively impact the safety and confidence of online activities. Some of these behaviors have been noted in international agreements, such as the 2011 Council of Europe Convention on Cybercrime ("Budapest Convention") as well as during PNG Parliamentary debates on online harassment, abuse character assassination against personal dignity/integrity which had significant negative effects on people.

The current Cyber Crime Code Act (2016) does not andequately addreses the online safety issues such as:

- computer-related forgery (piracy/copyright infringements),
- racist and xenophobic online material,
- online harassment and abuse against personal dignity/integrity,
- access on devices, computer systems, and data,
- illegal interferences (through data input, alteration, and/or suppression) on devices, data, and computer system,
- illegal interception on devices, data, and computer systems, and
- reliable and trustworthy online identity,

Hence, there is a need for a legislation on online safety to be developed. The legislation on online safety will be developed carefully by balancing against human rights and other values espoused by the UN Convention on Human Rights, amongst others, by using best practices, and by taking its cue from the existing mechanisms, and relevant legislations such as the Cyber Crime Code Act (2016). The legislation developed will provide clear guidelines for law enforcement, provide judicial clarity, and remit to those impacted by those behaviors.

Cybersecurity Regulations

Cybersecurity law can be defined as having five fundamental questions:

1) What are we securing?;

(2) Where and whom are we securing?;

(3) How are we securing?;

(4) When are we securing?; and

(5) Why are we securing?"[3]

Cybersecurity regulation designates rules dealing with data protection, breach notification, cybersecurity certification/standardization requirements, implementation of cybersecurity measures, cybersecurity audit requirements, privacy protection, child online protection (COP), digital signatures and e-transactions, and the liability of internet service providers. Regulations are often the implementing framework for laws, specifying how the laws should be carried out.

PNG will develop a cybersecurity legislation with clear, consistent, applicable, and up-to-date regulations by outlining the roles, duties, and responsibilities for various stakeholders. Data security is an important part of cybersecurity, but is not the only component, as cybersecurity comprises of the "systems on which data are stored and the networks on which data are transmitted".

Taking cue from the current cyber security policy 2021 and from the Electronic Transaction Act of 2021 the following legislation and regulations will be developed;

- Regulations related to personal data protection,
- Privacy protection regulations

[3] https://heinonline.org/HOL/P?h=hein.journals/ilr103&i=1022

- Cybersecurity audit requirements
- Legislation on identifying and protecting national critical infrastructures
- Regulations on Child Online Protection

Considering the implications on critical infrastructure and essential services, the Government will develop a legislation that will:

- harmonize with existing national laws;
- contain provisions compatible with international standards and best practices;
- provide a mechanism to identify PNG's critical infrastructures respective sectors and provide necessary protection of these infrastructures;
- mandate and empower relevant responsible agencies to take necessary measures towards protecting the critical infrastructures, including measures on disaster preparedness; trustworthy technology, response and recovery;
- Define the scope of critical infrastructure regulation for comprehensive coverage;
- Develop and pass the Critical Infrastructure Legislation;
- Create Critical Information Infratsructure Standards and Regulations that all agencies, private sector and others need to follow;
- Strengthen obligations and compliance for resilient critical infrastructure; and
- Understand the importance of Critical Infrastructure to the welfare of PNG.

2 TECHNICAL MEASURES

To establish and implement effective technical measures for cybersecurity in Papua New Guinea, ensuring robust protection against cyber threats and incidents.

To fortify cybersecurity defenses in Papua New Guinea, it is imperative to establish and execute effective technical measures, ensuring robust protection against cyber threats and incidents. These measures constitute the cornerstone of cybersecurity defense, furnishing capabilities to detect, prevent, respond to, and mitigate cyber threats. They are indispensable for fostering trust and security in the digital environment and facilitating the successful adoption of Information and Communication Technologies (ICTs).

A coordinated approach to national cybersecurity with Critical Information Infrastructures (CIIs) at its core is essential. This involves ensuring that government systems are secure, resilient, and safeguard citizens' data while extending protection to entities and systems beyond CIIs.

Enhancing cybersecurity resilience in Papua New Guinea necessitates the full implementation of coordination mechanisms such as the National Cybersecurity Coordination Center (N3C), National Cyber Security Centre (NCSC) composed of Computer Emergency Response Team (CERT), Cyber Security Operations Center (CSOC), Cyber Security & Safety Awareness (CSSA) Unit, and Social Media Management Desk (SMMD), along with sector-specific teams such as NIO (National Intelligence Unit), RPNGC (Cyber Crime Unit), Office of Censorship, Defence (Cyber Intelligence Unit), among others. Implementing a national framework for cybersecurity strengthens defense against cyber threats and contributes to a secure digital environment for citizens and organizations.

National Cyber Coordination Centre (N3C)

The N3C serves as the nerve center coordinating these security agencies, by fully implementing the Cyber Security Policy 2021, facilitating a unified and effective approach to cybersecurity in Papua New Guinea as and when the need arises. The partial implementation of National Cyber Coordination Centre (N3C) under the Cyber Security Policy 2021 will now be fully implemented. The N3C is the coordination mechanism for all security agencies including the NCSC, RPNGC Cybercrime Unit, National Intelligence Unit (NIO), Defence Cyber Intelligence Unit, and Office of the Censorship, among others which convene as necessary to share information and work collaboratively to deal with security threat, investigation, arrest and prosecution of cybercrime offenders.

At the discretion of the National Security Council (NSC) or in response to requests from any participating security agency, the N3C is triggered. The activation of N3C is subject to the following:

- When NSC deems necessary to activate;
- During Emergencies;
- In response to significant cyber-related crimes; and
- In response to requests from any participating security agency

The organizational structure and responsibilities of N3C plays a crucial role in enhancing cybersecurity in Papua New Guinea through central coordination. The primary roles and characteristics of the security organizations coordinated through N3C are reflected in the framework below.

Coordination Mechanism	Organization	Primary Objective	Rationale
N3C	NCSC	Ensure a unified approach to cybersecurity, responding to incidents and educating the public on safe online practices.	The NCSC coordinates the monitoring and defense of whole-of-government critical infrastructures and systems, collect and disseminate security information, drive national cyber awareness activities, and respond to security incidents, investigates, and drive audits through CSOC, CERT, CSSAU, and CSIRT, respectively.
	SMMD	Counteract Mis & Disinformation	The SMMD unit actively monitors social media accounts to identify and counter misinformation, disinformation, and hate speech. Accounts spreading false information are taken down ensuring public tension is managed.
	NIO	Analyse cyber intelligence	The NIO has a wider function on national security, however cyber intelligence unit is coordinated through the N3C for the purposes of Cyber Coordination
	RPNGC Cyber Crime Unit	Investigate and Prosecute Cyber Crime offences	RPNGC Cyber crime unit coordinates with the N3C on investigation in relation to cyber. Through the N3C, RPNGC cyber crime unit are assisted on cyber investigations and possible prosecution
	PNG Defence Cyber Intelligence Unit	Cyber Security Matters of sovereignty	The N3C as and when required will coordinate with PNG Defence Cyber Intelligence Unit on matters of soveregnty.
	Office of Censorship	Counteract and Censor unregulated content	Through the N3C, the office of censorship coordinates its efforts in counteracting and censoring unregulated cyber content.

The N3C, is governed by a Steering Committee comprising security agencies co-lead by Security Coordination and Assessments (OSCA) and the Department of ICT, ensuring coordination and collaboration.

National Cyber Security Centre (NCSC)

In the pursuit of enhancing Papua New Guinea's cyber resilience and security posture, the National Cyber Security Centre (NCSC) plays a pivotal role as the cyber security operations agency and collaborate with National Cyber Coordination Centre (N3C) as and when required. By aligning with international standards and fostering collaboration across government, industry, and society, NCSC aims to enhance its capacity to access, analyze, defend, and disseminate threat intelligence effectively while also doing awareness on cyber safety and cyber security which are essential for safeguarding personal privacy, financial security, critical infrastructure, national security, and public trust in the digital age.

This involves investing resources in specialized units such as the Cyber Security Operations Center (CSOC), Computer Emergency Response Team (CERT), Cyber Safety and Security Awareness Unit (CSSAU), and Computer Security Incident Response Team (CSIRT), which collectively monitor, defend, drive cyber awareness, and respond to cyber threats.

The CSOC focuses on continuous monitoring and defense of critical network infrastructure, while the CERT aggregates and manages security information from diverse sources. Meanwhile, the CSIRT and CSSAU stands ready to respond promptly to security incidents and conduct comprehensive audits and investigation to ensure the resilience of government systems, and drive national cyber awareness activities, respectively.

Organization	Units	Primary Objective	Rationale
NCSC	CSOC	Monitors and Defends whole of Government Critical Infrastructures & Systems	A CSOC is a unit that invests in technology and staff skilled at monitoring and defending the Critical Network Infrastructure and Systems through the installation of end points and network security installations (e.g., firewall)
	CERT	Collect and Disseminates Security Information	A CERT is a unit equipped to collect and curate security information from several sources including from Domestic, regional and international cyber security partners. This team does not respond to individual incidents.
	CSSAU	Drives national cyber awareness activities	Publishes contents to educate individuals and organizations about the importance of practicing safe and secure online behaviors
	CSIRT	Respond to Cyber Security Incidents	A CSIRT is a cross functional unit responsible for responding to security incidents and also responsible for Cyber Security Audits for the whole of Government. Some team members may not be full time but are called in as needed.

The National Cybersecurity Security Center (NCSC) serves as the cornerstone of Papua New Guinea's cyber defense strategy, encompassing four vital units:

i) **Cyber Security Operations Center (CSOC):** Dedicated to the continuous monitoring and defense of critical government infrastructures and systems, CSOC employs advanced technology and skilled personnel to safeguard against cyber threats. Through the deployment of endpoint and network security installations, such as firewalls, CSOC ensures comprehensive protection against potential breaches. Scaling up capabilities to prevent cyber-attacks through advanced technologies and establishing mechanisms for swift advice and support before cyber incidents are essential components of enhancing cybersecurity in Papua New Guinea.

ii) **Computer Emergency Response Team (CERT):** As the central repository for security information, CERT collects and disseminates curated intelligence gathered from domestic, regional, and international cyber security partners. While it does not directly respond to individual incidents, CERT plays a pivotal role in facilitating collaboration and information sharing to enhance overall cyber resilience. Expanding the dedicated CERT for a coordinated and effective response, as well as establishing a collaborative threat intelligence network for information sharing, are crucial steps in bolstering cybersecurity capabilities.

iii) **Cyber Security & Safety Awareness (CSSA) Unit:** As the drive cyber awareness, the unit publishes contents to educate individuals and organizations about the importance of practicing safe and secure online behaviors.

iv) **Computer Security Incident Response Team (CSIRT):** Tasked with responding to security incidents and conducting cyber security audits across government entities, CSIRT operates as a flexible, cross-functional unit. Its members, drawn upon as needed, enable swift and effective responses to emerging threats, ensuring the integrity and security of government systems. Establishing a comprehensive incident response plan is critical to enable timely detection, response, and recovery from cyber incidents.

The overall functions of the NCSC include but not limited to;

- Set up effective national capabilities to prevent, detect, mitigate, and respond to major cyber security incidents, improving overall cyber resilience,
- Develop and implement a national cybersecurity capability that can effectively detect, respond to, and mitigate cyber threats in a timely manner,
- Develop strategies to deter and disrupt cyber threat actors targeting PNG,
- Collaborate with industries to dismantle ransomware business models,
- Strengthen measures to protect identities and support victims of identity theft,
- Identify and establish a risk-management approach, particularly through public-private partnerships, to protect national critical infrastructure and essential services,
- Create a comprehensive risk management framework enabling the identification, assessment, and prioritization of cybersecurity risks across critical infrastructure and essential services,
- Set and enforce compliance standards, regulations, and guidelines that align with international best practices and local cybersecurity requirements,
- Implement measures ensuring the trustworthiness of digital products and software through using some of the building blocks within the GovPNG Technology Stack as well as Encryption, and
- Conduct regular assessments to identify and address weaknesses.

The NCSC employs various methods, including internal collection, private sector collaboration, and leveraging external government sources and open-source intelligence.

Threat intelligence gathered through these channels is disseminated promptly to relevant stakeholders, empowering them to take proactive measures to safeguard their infrastructure.

Furthermore, efforts are directed towards enhancing the resilience of critical infrastructure and government ICT systems, ensuring the continuity of essential services even in the face of cyber-attacks. This comprehensive approach encompasses securing digital infrastructure, devices, and applications, as well as promoting good cyber hygiene practices among citizens to foster a safer digital environment. Through the coordination facilitated by the N3C, the NCSC is better positioned to align its efforts with national cybersecurity objectives and ensure a cohesive and effective response to cyber threats.

SMMD (Social Media Management Desk)

Counteract Misinformation & Disinformation: The Social Media Management Desk (SMMD) is dedicated to combating misinformation and disinformation by actively monitoring various social media platforms. Through vigilant surveillance, the SMMD identifies instances of misinformation, disinformation, and hate speech, aiming to mitigate public tensions. By promptly taking down accounts disseminating false information, and coordinating through the N3C, the SMMD contributes to maintaining a regulated and informed online environment, fostering trust and reliability in digital discourse.

NIO (National Intelligence Unit)

Analyse cyber intelligence: The National Intelligence Unit (NIO), within its broader scope of national security functions, houses a specialized cyber intelligence unit. Coordinated through the National Cyber Coordination Centre (N3C), this cyber intelligence unit focuses on analyzing cyber threats and intelligence. By leveraging its expertise and resources, the NIO's cyber intelligence unit contributes valuable insights to the overall understanding of cyber threats, supporting proactive measures to enhance cybersecurity and safeguard national interests.

RPNGC Cyber Crime Unit

Investigate and Prosecute Cyber Crime offences: The RPNGC Cyber Crime Unit is tasked with investigating and prosecuting cybercrime offenses. As part of its operations, it collaborates with the other security agencies through the National Cyber Coordination Centre (N3C) to conduct thorough investigations and prosecutions. Leveraging the resources and assistance available through the N3C, including coordination with other relevant agencies, the RPNGC Cyber Crime Unit aims to address cybercrime effectively and ensure perpetrators are brought to justice. This coordinated approach enhances the unit's capabilities and contributes to a safer digital environment for Papua New Guinea.

Office of Censorship

Counteract and Censor Unregulated Content: The Office of Censorship oversees efforts to counteract and censor unregulated content, particularly in the realm of cyberspace. As part of the National Cyber Coordination Centre (N3C), it coordinates activities aimed at ensuring a safe and regulated online environment. This involves monitoring, identifying, and taking action against content that violates regulations or poses risks to users. By working collaboratively with other agencies within the N3C framework, the Office of Censorship contributes to maintaining integrity and safety in the digital realm.

Defence Cyber Intelligence Unit:

Coordinates Cyber intelligence on Sovereignty: The Defence Cyber Intelligence Unit is responsible for coordinating cyber intelligence activities related to sovereignty, which involves safeguarding and protecting a nation's interests, autonomy, and territorial integrity in cyberspace. This unit focuses on gathering, analyzing, and disseminating intelligence related to cyber threats and activities that may pose risks to national sovereignty. It collaborates with other defense and intelligence agencies to monitor, detect, and respond to cyber threats that may impact the sovereignty of the nation.

3 ORGANIZATIONAL MEASURES

Enhance Organizational Measures for Effective Cybersecurity Governance in Papua New Guinea

Leveraging the leadership of the N3C, the country can strengthen its cybersecurity governance framework, mitigate cyber risks, and safeguard its digital infrastructure and citizens against evolving threats. By integrating the functions and objectives of the N3C into the national cybersecurity strategy and organizational measures, Papua New Guinea can establish a unified and effective approach to cybersecurity governance and coordination. By implementing the following actions under the organizational measures, Papua New Guinea can strengthen its cybersecurity governance framework, improve coordination among stakeholders, and enhance its overall cybersecurity resilience.

Development of National Cybersecurity Strategy (NCS)

- The PNG Department of ICT and key stakeholders to develop a comprehensive NCS to address the cybersecurity challenges faced by Papua New Guinea.
- Prioritize resources within the NCSC to address critical cybersecurity objectives, such as protecting essential infrastructure, enhancing incident response capabilities, and promoting cybersecurity awareness among citizens.
- Define governance structures within the NCS to ensure effective implementation, monitoring, and evaluation of cybersecurity initiatives.
- Government to allocate resources and prioritize cybersecurity objectives as necessary.

Elevate the NCSC as the National Cyber Security Authority (NCSA)

- Ensure coordination between government agencies, industry partners, and civil society organizations under the leadership of the NCSC to ensure a cohesive and unified approach to cybersecurity governance.
- Elevate and empower the NCSC as the National Cyber Security Authority (NCSA) responsible for overseeing and managing cybersecurity initiatives at the national level in Papua New Guinea.

Implement Customized Cybersecurity Metrics and Assessments

- NCSC to develop and implement cybersecurity metrics and assessment tools to the specific cybersecurity landscape of Papua New Guinea.
- Conduct regular cybersecurity investigation and audits and risk assessments, focusing on vulnerabilities to the country's critical infrastructure and digital ecosystem, to prioritize mitigation efforts effectively.

Cyber Safety and Security

- Embed COP initiatives within the broader cybersecurity framework established by the Department of ICT in consultation with Office of Censorship to address the growing challenges of child online safety in Papua New Guinea.

- Establish reporting mechanisms and capabilities facilitated by the Department of ICT in consultation with Office of Censorship to enable swift responses to issues affecting children's online security, aligning with cultural sensitivities and local contexts.

Trustworthy Technology

Ensure trustworthiness of digital products, develop protocols for safeguarding valuable datasets, and promote secure adoption of emerging technologies with a cybersecurity focus.

Implement measures ensuring the trustworthiness of digital products and software through in compliance to Digital Government Act 2022, and in alignment to GovPNG Technology Stack Approach conforming to 8 minimum technology principles;

i) Streamlined Services,

ii) Cost effectiveness,

iii) Security and Privacy,

iv) Interoperability,

v) Scalability,

vi) Accessibility,

vii) Transparency & Accountability, and

viii) User-centric Design.

This is to minimize duplicate efforts and promoting shared digital services across government agencies, with a focus on ensuring ICT projects utilize existing shared services and integrate smoothly with the existing technology with security in the core.

Facilitate Consultation and Capacity Building

- Facilitate regular consultation sessions with local cybersecurity experts, government agencies, and community leaders to gather insights and feedback for refining the NCS and cybersecurity initiatives.
- Coordinate capacity-building efforts led by the NCSC to enhance cybersecurity skills and awareness among government officials, private sector professionals, and community members, ensuring inclusivity and participation from diverse stakeholders.

4 CAPACITY DEVELOPMENT MEASURES

Fortifies national cybersecurity by developing a skilled workforce and accelerating the local cyber industry for self-reliance

In our pursuit of a resilient cybersecurity landscape, we are embarking on a strategic journey to cultivate and sustain a skilled cybersecurity workforce tailored to our security and economic imperatives. This endeavor is anchored on fortifying the cybersecurity talent pipeline, a pivotal step amidst the global shortage of cybersecurity professionals.

Our approach hinges on bolstering the education system to incubate a proficient cybersecurity workforce, aligning with our broader objectives of fostering cyber awareness and nurturing a cyber-savvy culture. By equipping our youth with comprehensive cyber education, we are laying the groundwork for a generation primed to embrace cybersecurity careers.

To realize this vision, we are committed to supporting and empowering youths, women, and mid-career professionals to pursue cybersecurity vocations. Through strategic partnerships with international organizations and collaboration with educational institutions and industries, we aim to cultivate a dynamic workforce adept at navigating the evolving cyber landscape.

Promoting cybersecurity literacy across all sectors is integral to our strategy, encompassing tailored training initiatives and curriculum integration from primary to tertiary education levels. By instilling a culture of proactive cybersecurity practices, we are fostering a resilient workforce capable of safeguarding our digital ecosystem.

Our initiatives extend beyond the classroom, encompassing programs to combat cyberbullying and promote cyber safety among our youth. Through pilot programs and nationwide implementation, we seek to empower future generations with the skills and awareness necessary to thrive in the digital realm.

Public Cybersecurity Awareness Campaigns

Foster a cyber-aware society through educating and empowering citizens. Implement targeted campaigns to raise awareness among different sectors of society, including MSMEs, the private sector, public sector agencies, civil society, the general population, older persons, persons with disabilities, parents, educators, and children as part of Child Online Protection efforts.

Empower small and medium-sized businesses with tailored cybersecurity support by providing them links information, tools, and resources that can help them keep their business secure. The Government will work with other program to help provide toolkits to SMEs and individuals to help them to take action to reduce cyber risk. The Government will partner with Cyber capacity organizations, such as the Global Cyber Alliance, that can help provide SMES and individuals with the tools and resources they need to enhance their cyber hygiene

Training for Cybersecurity Professionals

Develop and support cybersecurity training courses, accreditation programs, and sector-specific educational programs for professionals in various sectors, including law enforcement, judicial actors, MSMEs, the private sector, public sector officials, and critical infrastructure sectors such as finance, health, telecommunications, transport, and energy. Cybersecurity professionals' retention plans will be in place to support the recruitment, training, and retention of cybersecurity professionals, ensuring a sustained and skilled cybersecurity workforce.

Cybersecurity Educational Programs in Academic Curricula

Develop the national cyber workforce through education and professionalization. Integrate cybersecurity principles into national academic curricula at primary, secondary, and higher education levels to equip students with essential cybersecure behaviors and skills.

Collaborate with the Education Department to include cyber security and cyber crime lessons in schools to ensure next generation of elites are cyber savvy.

Cybersecurity Research, Innovation & Economic Growth

Promote cybersecurity research, foster public-private partnerships, and create an environment for economic growth and innovation through collaboration across various sectors.

Design and deliver training programs to enhance the skills and knowledge of PNG nationals in cybersecurity, fostering research, development, and collaboration with international partners. Cybersecurity R&D activities will be encouraged in the public, private, and academic sectors to support the development of human capacity, new techniques, products, and better understanding of risks and mitigations in cybersecurity.

Promote, support, and fund cybersecurity research and innovation for the development and deployment of advanced cybersecurity technologies and solutions. To develop a vibrant cybersecurity ecosystem, the Government will encourage the cybersecurity industry and academia to develop advanced capabilities, and grow our cybersecurity market. The Government will invest in cybersecurity research and innovation. We will also establish a variety of different programmes, which stakeholders can leverage to develop Made-in-PNG solutions.

National Cybersecurity Industry Development

Create an environment conducive to economic growth, innovation, and cooperation within the public, private, civil society, technical, and academic communities. Foster the growth of a domestic cybersecurity industry through favorable economic, political, and social environments, supported by organizations and associations promoting industry development. Safeguards businesses and citizens by supporting SME cybersecurity, fostering a cyber-aware society, disrupting cyber threats, breaking ransomware models, and enhancing identity security.

Government Incentive Mechanisms

Encourage and support public-private partnerships that promote cybersecurity research and innovation within Papua New Guinea. Stimulate local cyber industry, research, and innovation for self-reliance. Implement incentive mechanisms to encourage capacity development, cybersecurity industry growth, and cybersecurity-related R&D activities, including grants, scholarships, fee support, loans, employment opportunities, tax alleviation, and favorable trade environments.

The Government will also work to publicize the various grant programs from our partners and allies where are SMEs, academia and other businesses can enter to fund their specific cyber research projects. The Government seeks to be at the forefront of cybersecurity research and development (R&D) to keep pace with the rapidly evolving technological landscape and leverage new technologies to stay ahead of malicious cyber actors. In this vein we will work with our partners in PACSON, GFCE, and others to bring the newest and best thinking to the country.

5 COOPERATION MEASURES

Strengthen regional cyber resilience, advocate for international cyber governance, and foster global cooperation in managing cross-border cyber incidents

To effectively address the transnational dimensions of cybersecurity incidents and leverage support for developing countries, Papua New Guinea (PNG) is committed to international cooperation. The government will collaborate closely with our allies, donors, international partners, and the technical community to strengthen PNG's capacity to prevent, respond to, and recover from malicious cyber activities, including those orchestrated by sophisticated actors.

PNG is committed to regional resilience and global leadership in cybersecurity cooperation, with a focus on fostering collaboration, advocating for responsible behavior, and actively contributing to international cybersecurity efforts.

Regional Cyber Resilience Support

- **Neighboring Nations Assistance:** PNG will play an active role in assisting neighboring nations in building cyber resilience, thus cementing its position as a regional partner dedicated to collective cybersecurity efforts. This will involve sharing expertise, resources, and best practices to fortify the entire region against cyber threats.

- **Public-Private Partnership:** Foster collaboration between the government and the private sector, recognizing their shared responsibility in cybersecurity. This entails encouraging joint initiatives, information sharing, and coordinated responses to cyber threats.

- **Intergovernmental Cooperation:** Forge partnerships with other governments to share information, best practices, and coordinate efforts in addressing global cyber challenges. PNG commits to building strong relationships with other nations to create a united front against cyber threats.

- **Regional Cooperation:** Strengthen collaboration with neighboring countries, our partners in PACSON, and regional organizations to address shared cybersecurity concerns. PNG acknowledges the interconnectedness of regional security and commits to active participation in regional cybersecurity initiatives.

- **Intra-Governmental Cooperation:** Ensure coordination and collaboration among different government agencies to create a cohesive and unified approach to cybersecurity. This involves breaking down silos and fostering a holistic approach to national cybersecurity.

International Cyber Governance Advocacy:

- **Priority of Foreign Policy:** Recognize and promote cybersecurity as a priority in foreign policy discussions. Engage in international dialogues to shape global norms and standards for cybersecurity.

- **Participation in International Cybersecurity Discussions:** Actively participate in global discussions on cybersecurity to stay informed about emerging threats, technologies, and best practices. Contribute to the development of international norms and rules in cyberspace.

- **Formal and Informal Cooperation:** Promote both formal and informal cooperation in cyberspace, acknowledging the importance of flexibility in addressing diverse cybersecurity challenges. Foster collaboration through established international frameworks and ad-hoc partnerships.

- **Capacity Building for International Cooperation:** Invest in capacity-building programs to enhance PNG's ability to engage in international cooperation effectively. Actively participate in international cybersecurity organizations and assess joining other relevant cybersecurity organizations.

Forge and Foster International Cooperation:

- **International Cyber Collaboration:** Establish, nurture, and strengthen cooperation and engagement with relevant international partners and institutions to effectively manage cross-border cyber incidents and combat cybercrimes.

- **Bilateral and Multilateral Partnerships:** Enter into partnerships on cybersecurity cooperation with other nations, focusing on areas such as governance, incident response, and capacity building for PNG's cybersecurity institutions. This involves strategic alliances to enhance PNG's cybersecurity capabilities and resilience.

PNG'S CYBER RESILIENCE AND MATURITY JOURNEY 2024-2030

Embarking on a strategic journey towards our 2030 vision, the delivery of our cybersecurity strategy spreads across three distinct horizons, reflecting a phased and systematic approach. These phases are carefully designed to fortify our cyber resilience and maturity in alignment with our overarching vision. The success of this journey hinges on the collaborative efforts between the Government and industry stakeholders, emphasizing the need for ongoing cooperation to uplift our cyber defenses.

Implementation

Effective implementation can only be achieved if a governance and monitoring process takes into account the views of all stakeholders. This collaboration by stakeholders, can take into account all the various areas that impact the successful implementation of the Strategy, this includes sourcing technical capability, budget, talent recruitment, international cooperation. Collaboration and information sharing should be mutually beneficial for all and take into account the objectives the Strategy is aiming to achieve.

The diagram below outlines all the various factors that should be taken into account for the implementation and monitoring of the Strategy.

Figure 2. Strategic framework

The implementation of this strategy will be in three phases;

Phase I: Foundational Strengthening (2024-2025)

Phase II: Scaling Cyber Maturity (2026–2028)

Phase III: Advancing Global Cybersecurity (2029–2030)

This type of approach is best used to ensure the strategy is targeted and delivered given the evolving cyber landscape.

Phase I: Foundational Strengthening (2024–2025)

In the initial phase, our primary focus will be on strengthening the foundational elements of our cybersecurity framework. This phase will include from the time the strategy is adopted. It will build from the current effort. In this phase, we will prioritize addressing critical policy and legislative gaps, fortifying vulnerabilities in our cyber defenses, and establishing robust protections mechanisms for our most vulnerable citizens and businesses. Additionally, we will extend our support to enhance cyber maturity regionally and internationally, recognizing the interconnected nature of cyber threats. This foundational strengthening is crucial to creating a resilient and secure cyber environment.

Major deliverables in Phase I are:

Deliverables	**Strategic Initiative**	**Responsible Agency**	**Funding**
The DICT will oversee the National Cyber Security Centre and provide technical support on cyber security and provide secretariat support to the National Cyber Security Centre Steering Committee. OSCA will provide chairmanship to the Committee.	Governance	DICT	GoPNG
Development of the National Cyber Security Strategy and Legislation that will elevate the NCSC to a NCSA and define the roles of key stakeholders on cyber security and the working relationship among these stakeholders	Legal	DICT	GoPNG
Development of Legislation for Critical Infrastructure to protect PNG's national critical infrastructures and services and essential sectors	Legal	DICT	GoPNG/ Partners
Maintaining and upgrading the existing National Cyber Security centre (NCSC) to meet international standards and best practice requirements;	Governance	DICT	GoPNG
Updating the Cyber Crime Policy and Legislation;	Policy/Legal	NICTA/Police /DICT/DJAG	GoPNG/ Partners
Updating the Evidence Act;	Legal	DJAG/Police NICTA/DICT	GoPNG/ Partners
Acceding to the Budapest Convention on Cyber Crime and its two additional Protocols;	Legal	DJAG/DICT	GoPNG
Begin training and capacity building on cyber security for PNG nationals to a competency level par with international experiences;	Training/ Upskilling	DICT/NCSC/Training Institutions/NICTA	GoPNG/ Partners
Facilitate necessary requirements for elevating the NCSC to a NCSA;	Policy	DICT/NCSC /OSCA/NSC	GoPNG/ Partners
Develop a Comprehensive Law on Online Safety	Legal	DICT/Censorship	GoPNG/ Partners

Implement measures to enhance the cybersecurity Posture of the PNG Government, fostering collaboration among stakeholders to address emerging cyber threats.	Cyber Security Measures	DICT/NCSC /NICTA	GoPNG/ Partners
Begin work on the enforcement of Cyber Security, Digital Government and data Protection Standards in Government Agencies	Enforcement	DICT/NCSC	GoPNG
Promote National Cybersecurity Awareness and Collaboration	Awareness	DICT/NCSC/NICTA	GoPNG/ Partners
Fully implement the National Cyber Coordination Centre (N3C)	Coordination	DICT/OSCA /RPNGC/Censorship /SMMD/NCSC /PNGDF/NIO	GoPNG
Fully operationalize SMMD	Counter measures	DICT/SMMD	GoPNG

Phase II: Scaling Cyber Maturity (2026–2028)

In this Phase, our strategy shifts towards scaling cyber maturity across the entire economy. We will emphasize further investments in the broader cyber ecosystem, with a focus on expanding the cyber industry and cultivating a diverse and skilled cyber workforce. The objective here is to extend cyber maturity comprehensively, ensuring that our nation is well-equipped to handle evolving cyber threats through sustained investments in both infrastructure and talent.

Major deliverables in Phase II are:

Deliverables	**Strategic Initiative**	**Responsible Agency**	**Funding**
Further investments in the broader cyber ecosystem, with a focus on expanding the cyber industry and cultivating a diverse and skilled cyber workforce.	Partnership and collaboration	NCSA/DICT	GoPNG/ Partners
Extending cyber maturity comprehensively, ensuring that PNG is well-equipped to handle evolving cyber threats through sustained investments in both infrastructure and talent.	Governance, Investments and Partnerships	NCSA/DICT	GoPNG/ Partners
Setting up capabilities to prevent, detect, mitigate, and respond to major cyber security incidents, improving overall cyber resilience.	Governance, Investments and Partnerships	NCSA/DICT	GoPNG/ Partners
Develop and Implement A Risk-Management Approach and Framework for Critical Infrastructure and Essential Services	Governance, Investments and Partnerships	NCSA/DICT	GoPNG/ Partners
Identify and establish a risk-management approach, particularly through public-private partnerships, to protect national critical infrastructure and essential services.	Governance, Investments and Partnerships	NCSA/DICT	GoPNG/ Partners

Create a comprehensive risk management framework enabling the identification, assessment, and prioritization of cybersecurity risks across critical infrastructure and essential services.	Governance, Investments and Partnerships	NCSA/DICT	GoPNG/ Partners
Establish Compliance Standards Aligned with International Best Practices	Governance, Investments and Partnerships	NCSA/DICT	GoPNG/ Partners
Set and enforce compliance standards, regulations, and guidelines that align with international best practices and local cyber security requirements.	Governance, Investments and Partnerships	NCSA/DICT	GoPNG/ Partners
Begin work on promoting, supporting, and funding cybersecurity research and innovation for the Development and deployment of advanced cybersecurity technologies and solutions.	Governance, Investments and Partnerships	NCSA/DICT	GoPNG/ Partners
Encourage the cybersecurity industry and academia to develop advanced capabilities, and grow our cybersecurity market.	Governance, Investments and Partnerships	NCSA/DICT	GoPNG/ Partners
Invest in cybersecurity research and innovation by working with our cluster and others to help develop a variety of different programmes, that stakeholders can leverage to develop Made-in-PNG solutions.	Governance, Investments and Partnerships	NCSA/DICT	GoPNG/ Partners

Phase III: Advancing Global Cybersecurity (2029–2030)

In this third and final phase, our vision extends beyond our national borders as we aspire to advance the global frontier of cybersecurity. We commit to spearheading the development of emerging cyber technologies capable of adapting to new risks and opportunities in the dynamic cyber landscape. Our aim is, not only to fortify our national cybersecurity, but also to position our nation as a regional leader, contributing significantly to innovations that address the evolving challenges of the cyber domain.

Major deliverables in Phase III are:

Deliverables	**Strategic Initiative**	**Responsible Agency**	**Funding**
Spearheading the development of emerging cyber technologies capable of adapting to new risks and opportunities in the dynamic cyber landscape.	Partnership and collaboration	NCSA/DICT	GoPNG/ Partners
Fortify our national cybersecurity and position our nation as a regional leader, contributing significantly to innovations that address the evolving challenges of the cyber domain.	Governance, Investments and Partnerships	NCSA/DICT	GoPNG/ Partners
Encouraging and supporting public-private partnerships that promote cybersecurity research and innovation within Papua New Guinea.	Governance, Investments and Partnerships	NCSA/DICT	GoPNG/ Partners
Publicize the various grant programs from our partners and allies where our SMEs, academia and other businesses can enter to fund their specific	Governance, Investments and	NCSA/DICT	GoPNG/ Partners

cyber research projects.	Partnerships		
Work with our partners in PACSON, GFCE, and others to bring the newest and best thinking to the country.	Governance, Investments and Partnerships	NCSA/DICT	GoPNG/ Partners
Creating an environment conducive to economic growth, innovation, and cooperation within the public, private, civil society, technical, and academic communities.	Governance, Investments and Partnerships	NCSA/DICT	GoPNG/ Partners

National Cyber Resilience Governance Framework

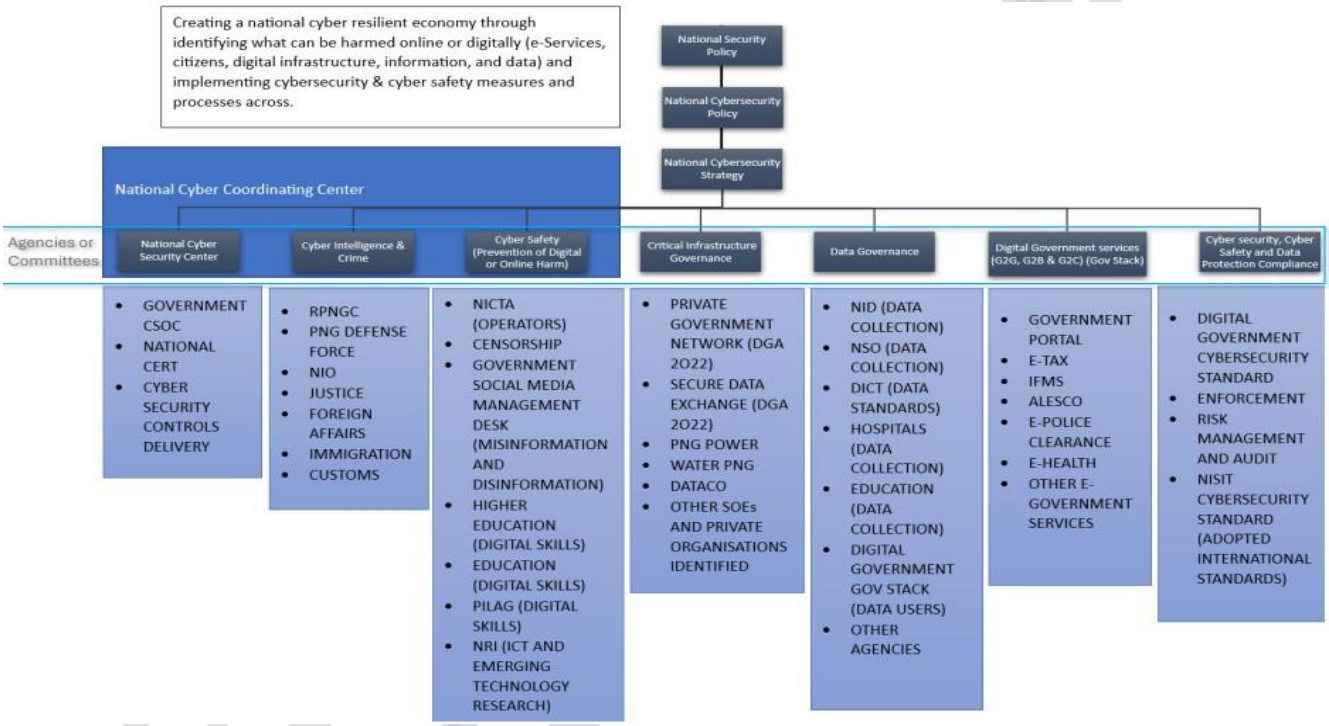

Figure 3: National Cyber Resilience Governance Framework

MONITORING AND EVALUATION

Monitoring and evaluation procedures capture the significant aspect of measuring performances based on implementation and to maintain and improve cohesive cybersecurity strategic operations. Monitoring process will enable an ongoing surveillance of the cybersecurity strategic outcomes within a year or so depending on the evolving cybersecurity landscape. Evaluation will measure annual performances and outcomes of the cyber security strategy and its implementation.

National Cybersecurity Strategic focus areas for Monitoring and Evaluation include;

- Establish a Monitoring & Evaluation mechanism for NCSA
- Monitor and evaluate delegated responsibilities to stakeholders
- Monitor and evaluate the operational and coordination body such as NCSC and N3C
- Introduce backup-strategy to stakeholders
- Identify Critical Information Infrastructures (CII) and monitor CII.
- Each sector will take leadership in monitoring and evaluating CII in their respective agencies and will be working closely with the DICT through NCSA to provide all aspects of reporting.
- Develop an approach/protection-plan to enhance protection and resilience based on reports provided by the agency's representatives.
- Establish an effective backup-strategy to allow CII data/resources retrieval when interrupted or hacked.
- Engage stakeholders and sector agencies representatives in quarterly cyber security Monitoring & Evaluation programs and workshops.
- Review and adopt global M&E best practices suitable for PNG cyber security context.
- Review, amend and harmonize existing legislative frameworks so as to sustain in addressing cybersecurity threats in Papua New Guinea.
- Strengthen regional and international cybersecurity cooperation by promoting technical cybersecurity standards as an enabler to achieving a safe and resilient cyberspace.