SAMOA
NATIONAL CYBERSECURITY STRATEGY
2025/26 - 2030/31

CONTENTS

LIST OF FIGURES

MINISTERIAL FOREWORD

In today's increasingly interconnected world, the digital landscape has become a fundamental cornerstone of our daily lives. In all areas from private enterprise to government services, social services, digital economies we rely on technology to drive progress, enhance efficiency, and foster innovation. However, this reliance on digital infrastructure also brings about new vulnerabilities and risks that we must address with urgency and foresight.

As we embark on the implementation of this National Cybersecurity Strategy, it is clear that we are facing an evolving and complex threat landscape. Cyber-attacks, data breaches, and digital disruptions have the potential to compromise our national security, economic stability, and the trust that underpins our digital systems. The rise of emerging technologies such as artificial intelligence presents both tremendous opportunities and significant risks.

This strategy sets out a comprehensive approach to safeguarding our nation's digital future. At its core, it acknowledges that cybersecurity is not just an issue for IT professionals or security experts—it is a shared responsibility that must be embedded in every level of government, industry, and society. To address the risks posed by emerging technologies, we must enhance our resilience, adapt to new threats, and foster a culture of proactive cybersecurity practices.

Our focus will be establishing legal and regulatory frameworks, strengthening incident response capabilities, and ensuring that continuous awareness and education is maintained for digital literacy uplift. Additionally, we must ensure that our workforce is equipped with the skills and knowledge to navigate and mitigate the challenges posed by an increasingly digital world.

This strategy is not only about responding to the risks we face today but also about preparing for the digital challenges of tomorrow. By adopting a forward-thinking and risk-based approach, we can create a resilient, secure, and trusted digital environment that supports the growth of our economy and protects the well-being of all citizens.

We must act now, with a sense of urgency and commitment, to ensure that our national cybersecurity infrastructure remains strong and adaptable in the face of ever-changing technological landscapes and growing threats.

Honorable Agaseata Tanuvasa Valelio Tanuvasa Peto

Minister for the Ministry of Communications and Information Technology

INTRODUCTION

Samoa has consistently demonstrated a proactive approach to cybersecurity, recognizing its critical role in protecting the nation's digital assets and maintaining the integrity of its information infrastructure. In past strategies, Samoa laid a solid foundation by implementing essential cybersecurity policies and frameworks that primarily focused on safeguarding government systems and raising public awareness.

The ever-evolving digital landscape presents both opportunity and risk, therefore the need for a comprehensive, action-oriented and forward-thinking national cybersecurity strategy has become increasingly apparent. The 2025/26 - 2030/31 strategy is designed to support Samoa's ambitious digital transformation goals by investing in a robust cybersecurity framework that not only protects government entities but also extends its protective measures to the private sector. By doing so, Samoa aims to create a secure digital environment that fosters innovation and economic growth, while also ensuring the resilience and continuity of business operations.

A key component of this strategy is the promotion of digital literacy across all sectors of society. By enhancing the cybersecurity posture of both public and private entities, Samoa seeks to build a culture of security awareness and vigilance that permeates every level of the nation's digital ecosystem. This involves equipping individuals and organizations with the knowledge and tools necessary to identify and mitigate cyber threats effectively, thereby reducing vulnerabilities and enhancing overall national security.

Moreover, Samoa is committed to improving the protection of its critical information infrastructure, recognizing its vital role in maintaining the nation's economic stability and security. By investing in cutting-edge technologies and best practices, Samoa aims to safeguard its digital infrastructure against a wide range of cyber threats, ensuring that essential services and operations remain uninterrupted in the face of potential disruptions.

In its pursuit of becoming a leader in the Pacific region, Samoa is also focused on building the capabilities of its cybersecurity workforce. By investing in the training and development of its engineers, support staff, and citizens, Samoa aims to cultivate a skilled and knowledgeable workforce that can effectively manage and respond to cybersecurity challenges. This emphasis on capacity building is crucial for achieving self-reliance in cybersecurity, empowering Samoa to independently secure its digital future.

Through these strategic initiatives, Samoa is not only enhancing its national security but also contributing to broader regional stability and resilience. By setting a benchmark for cybersecurity excellence in the Pacific, Samoa is positioning itself as a leader in the digital age, committed to protecting its digital assets and fostering a secure and prosperous future for its people.

CYBERSECURITY IN SAMOA

Situated in the Pacific region, Samoa shares similar opportunities and challenges with its neighboring small island nations. The narrative of the 'Blue Pacific Continent' weaves together these shared commonalities and amplifies the importance of regional cooperation in addressing challenges such as climate change - identified as the single greatest threat to the region. The criticality of telecommunication infrastructure especially subsea cables to the Pacific underscores the need for climate-resilient infrastructure. While increased connectivity brings benefits in furthering the digital economy and transformative impacts to service delivery it also presents other challenges to peace and security. This has led to the expanded concept of security to include cybersecurity threats and seeks to "maximize protections and opportunities for Pacific infrastructure and peoples in the digital age" (Pacific Islands Forum Secretariat, 2019)[1] as encapsulated in the Boe Declaration on Regional Security.

As a nation, Samoa is undergoing a significant digital transformation, characterized by an increasing reliance on online services and digital infrastructure. This shift is further driven by the government's commitment to enhancing connectivity and digital services through several avenues including the Digitally Connected and Resilient Samoa (DCRS) Project (effective February 2025), which aims to establish climate and disaster resilient digital connectivity infrastructure and promote an enabling environment through the development and strengthening of policy, legal and regulatory frameworks which includes cybersecurity initiatives. [2]

Samoa Computer Emergency Response Team (SamCERT)
In 2021, the Government of Samoa with the support of its development partners i.e., Government of Australia and the Government of New Zealand established under the purview of the Ministry of Communications and Information Technology (MCIT), the Samoa Computer Emergency Response Team otherwise known under its branding: 'SamCERT'. The team advises the Ministry on matters pertaining to cybersecurity both policy and technical. SamCERT is a member of the Pacific Cyber Security Operational Network (PaCSON) and Global Forum on Cyber Expertise community. SamCERT is the main hub in Samoa to ensure cybersecurity (not only establishing frameworks) as well as foster relationships with local and international stakeholders.

---

1 Pacific Island Forum Secretariat, 'Boe Declaration Action Plan', Pacific Islands Forum Secretariat, Suva, Author, 2019, 7, https://forumsec.org/sites/default/files/2024-03/BOE-document-Action-Plan.pdf, (accessed 02/04/2025)

2 https://projects.worldbank.org/en/projects-operations/project-detail/P180807

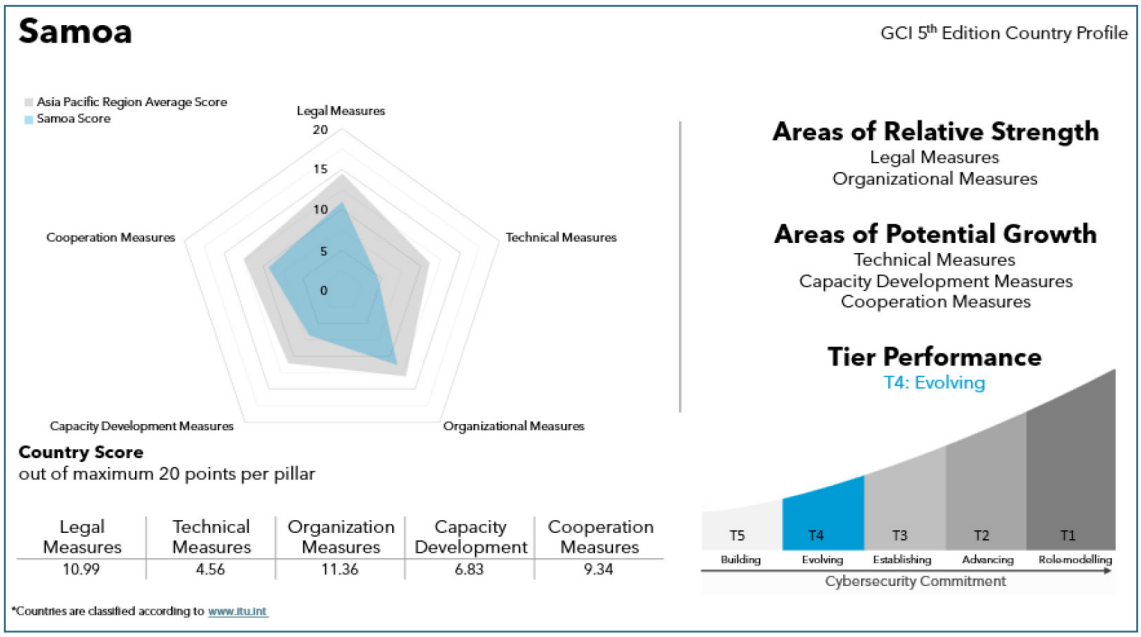

Figure 1: Samoa Country Profile - Global Cybersecurity Index

According to the International Telecommunication Union's (ITU) Global Cybersecurity Index, Samoa is classified as an Evolving Tier 4 country both globally and regionally in Asia and the Pacific (ITU 2024). The Index indicates that while Samoa has made strides in developing legal frameworks to address cybersecurity threats, it still encounters challenges in areas like technical measures, capacity building, and organizational structures. This highlights the need for substantial efforts to enhance Samoa's overall cybersecurity stance.

The following analysis examines Samoa's cybersecurity landscape through various lenses:

1. Cybersecurity Legal Framework: There is no established legal framework for cybersecurity, online safety, critical information infrastructure protection, or personal data protection. This is included in the draft "Samoa's Digital Pathway: Digital Transformation Strategy 2023 – 2030" with Cabinet. Currently Samoa does not have a standalone Cybercrime Act and instead provisions that address cyber-related offences are incorporated into the Crimes Act 2013 under Part 18 – Crimes Involving Electronic Systems. This includes offenses related to illegal access with penalties of up to seven years in prison, though these penalties are rarely enforced. The Police rarely investigate such incidents. A recent assessment by the Government of Samoa identified gaps in the legislation concerning the Budapest Convention. The Telecommunication Act 2005 Section 49 and 50 talks about the protection of personal information. All relevant legislations should be considered in developing the Cybersecurity Act. The Communications and IT Sector Plan 2022/23–2026/27 outlines strategies

to ensure the ICT sector contributes to Samoa's socioeconomic development, with a focus on cybersecurity under Goal 5: "A Safe and Secure ICT Environment." This includes promoting IT personnel security capabilities, establishing a SamCERT operating model, strengthening regional partnerships, integrating cybersecurity into education, and raising awareness through public programs. Key indicators for success include ongoing cybersecurity training, launching a national cybersecurity strategy, and establishing a helpline.

2. Cybersecurity Institutional Measures: The National Security Policy & Implementation Strategy 2024 recognizes cybersecurity as a key component of Samoa's security framework, emphasizing coordinated government action to address cyber threats. Cybersecurity is part of Pillar 3: Technology, Cyber Security, and Critical Infrastructure within Resilient Samoa. The policy highlights consolidating SamCERT operations, enhancing regional cooperation, and monitoring infrastructure vulnerabilities. MCIT, the Office of the Regulator, and the police share cybersecurity responsibilities, but their roles are not clearly defined, leading to a fragmented approach. SamCERT attempts to coordinate efforts but is limited in scope. There is a shortage of specialized cybersecurity roles, contributing to low organizational maturity in addressing cyber threats. Technical staff require further training, and a broader focus on cybersecurity is needed across all sectors.

3. Cybersecurity Implementation Measures: Cabinet approved the Information Security Policy in 2024 accompanied by guiding documents like the Information Classification and Handling Standard and Cyber Security Incident Response Standard. However, awareness of these standards is limited, and the policy lacks mandatory enforcement. Some organizations follow international security standards, but adhering to in-house standards is uncommon across sectors.

4. Partnership: There is cooperation on cybersecurity issues between government, private industry, academia, and law enforcement, but it lacks formal agreements and tends to be reactive. SamCERT collaborates with the Ministry of Police and Prison and the Office of the Regulator on awareness activities. The private sector cybersecurity market is in its early stages. Samoa is a member of PaCSON and collaborates with international partners like the National Cyber Security Centre of New Zealand and the Australian government, which has strengthened Samoa's cybersecurity capabilities. A Security Operation Center was established during the Commonwealth Heads of Government Meeting 2024, providing valuable cooperation experience on tooling and operations.

5. Awareness and Education: Cybersecurity courses are rare in schools and universities, though recognized as a future focus. The Samoa Mata'ala Roadshow and Cyber Smart Cyber Weeks have raised awareness, but overall public awareness of responsible online behaviour and past major cyber incidents remains limited. Therefore, continuous public awareness activities are needed.

Figure 2: Samoa Mataala Roadshow 2023, Salelologa Primary Schools after the cyber program activities

SAMOA'S CYBER THREAT LANDSCAPE

UNIQUE CYBERSECURITY CHALLENGES

The cybersecurity landscape points out that Samoa, as a small Pacific nation, faces unique challenges due to its geographic isolation, limited resources, and difficulty in attracting necessary expertise and infrastructure. The country also struggles with low awareness among the public and organizations, weak security practices such as poor password management and outdated software, and human errors that increase vulnerability to cyber threats like phishing and ransomware. Additionally, social engineering tactics and reliance on pirated software due to financial constraints further expose systems to cyber risks. A widespread lack of understanding of cybersecurity threats leaves many, especially in village businesses, unaware of the seriousness of these threats.

The rapid digitalization in Samoa has led to several distinct cybersecurity challenges. The country's increasing dependence on digital platforms for essential services, such as banking, healthcare, and government operations, heightens its exposure to cyber threats. The use of pirated software is prevalent, creating vulnerabilities that can be exploited by malicious actors. This issue is compounded by limited cybersecurity awareness and resources, making it imperative to prioritize cybersecurity education and infrastructure investment.

Another pressing challenge is the insufficient funding and capacity for sustainable cybersecurity practices. Many frameworks and best practices are perceived as more suitable for larger, developed countries and often irrelevant to smaller nations like Samoa. The absence of a clear leadership model and division of responsibilities in cybersecurity, coupled with limited resources, means the issue is not adequately prioritized at the government level.

KEY CYBERSECURITY THREATS

During the National Cybersecurity Strategy stakeholder consultations in November 2024, several critical cybersecurity threats were identified. Social engineering attacks, specifically phishing, are on the rise, targeting individuals and organizations alike to gain unauthorized access to sensitive information. Ransomware attacks pose a significant risk, with the potential to disrupt critical services and demand substantial financial resources for recovery. The use of outdated or pirated software further exacerbates these risks, as it often lacks necessary security updates and patches.

Samoa faces a rapidly evolving cyber threat landscape, with its government systems and critical infrastructure increasingly targeted by sophisticated malware and advanced cyberattack techniques. The recent CHOGM meeting enabled the Government to understand these risks, as threat actors sought to exploit vulnerabilities in government and event networks, potentially leading to unauthorized data access, service disruptions, and compromised communications.

In response, a collaborative Security Operation Center (SOC) was established—led by Australia's RAPID team and supported by SamCERT, SIRF, and the New Zealand Cyber Security Center to monitor and address these threats in real time. This operation revealed specific vulnerabilities in network traffic between government agencies and CHOGM systems, emphasizing the need for ongoing vigilance and rapid response.

Additionally, training on cybersecurity tools and communication strategies highlighted the importance of timely advisories and coordinated incident response. Overall, these experiences underscored the persistent and growing cyber threats Samoa faces, and the critical need for regional cooperation and robust cybersecurity measures to protect national interests.

2030/31 OUTLOOK: OUR VISION

'Secure and resilient cyber space for all in Samoa'

STRATEGIC GOALS

There are four strategic goals identified in the strategy for action to deliver on the vision.

1. Enhance partnerships, operational capacity, and governance in cyber-security.
2. Develop legal and regulatory frameworks.
3. Protect Critical Information Infrastructure
4. Promote education, awareness, and innovation.

GUIDING PRINCIPLES

The following principles aim to ensure consistency, collaboration, and alignment with Samoa's broader objectives. The collective effort in achieving the vision will be guided by the following ways of working:

- fosters and maintains *trust*.
- is people-centric and *inclusive*.
- protects *fundamental human rights* and ensures online rights are upheld.
- encapsulates *collaboration and cooperation* among stakeholders.
- ensures *transparency* (open government) and *accountability*.
- integrates a *risk-based* approach while balancing *agility and resilience*.

Figure 3: SIRF Team during the CHOGM 2024 meeting in Apia, training was provided to upskill the Public Service IT on Cybersecurity through the NCSC, New Zealand Program and RAPID, Australia Program

NATIONAL CYBERSECURITY STRATEGY GOVERNANCE

GOVERNANCE AND COORDINATION

The effective implementation of the Samoa National Cybersecurity Strategy 2025/26 - 2030/31 requires a robust governance and coordination framework to ensure leadership, accountability, and cohesive action across all sectors. Annex 3. MCIT will serve as the primary owner of the strategy, tasked with overseeing its execution, monitoring progress, and addressing challenges as they arise.

LEADERSHIP AND PRIMARY OWNERSHIP

As the primary owner, the Digital Transformation and Innovation and SamCERT Division of MCIT will be responsible for the overall execution and success of the strategy. This ministry will act as the central authority, providing leadership and ensuring that the strategy aligns with national and international priorities. This role includes setting clear objectives, structured planning, and aligning the strategy with broader development and security goals.

GOVERNANCE STRUCTURE

The governance structure is divided into four key domains, each with specific roles and responsibilities:

1. STRATEGIC GOVERNANCE

- The National Security Committee (NSC), Information Technology Advisory Committee (ITAC) along with MCIT contributes to long-term planning and goal setting.
- Ensures alignment with national and international priorities.
- Involves oversight to maintain the clarity and structure of the strategy's objectives.

2. POLICY AND LEGAL GOVERNANCE

- Represents high-level decision-making and policy-setting processes.
- Involves government leadership and legislative support to create an enabling environment.

3. OPERATIONAL GOVERNANCE

- Oversees the day-to-day execution and practical application of the strategy.
- Manages operational aspects to ensure effective implementation.
- Coordinates with stakeholders to maintain alignment with strategic goals.
- Coordinate with the SamCERT Incident Response Forum (SIRF)[3] a technical team that requires the intervention on national incidents.
- Is responsible for developing cybersecurity requirements for CII operators and other relevant entities
- Coordinate with the other CERTs in the Pacific for technical matters which requires intervention in the region.
- Coordinate with the RAPID[4] Team which requires intervention at any incident that requires assistance of the RAPID Team.
- Ensures continuous updates and improvements through collaborative stakeholder efforts.

4. TECHNICAL GOVERNANCE

- MCIT alongside its sector partners contributes to the technical aspects of the national strategy to ensure that strategic direction is translated into actionable technical guidance for national coordination efforts.
- Coordinates and manages groups to ensure technical resources and cybersecurity measures are in place.

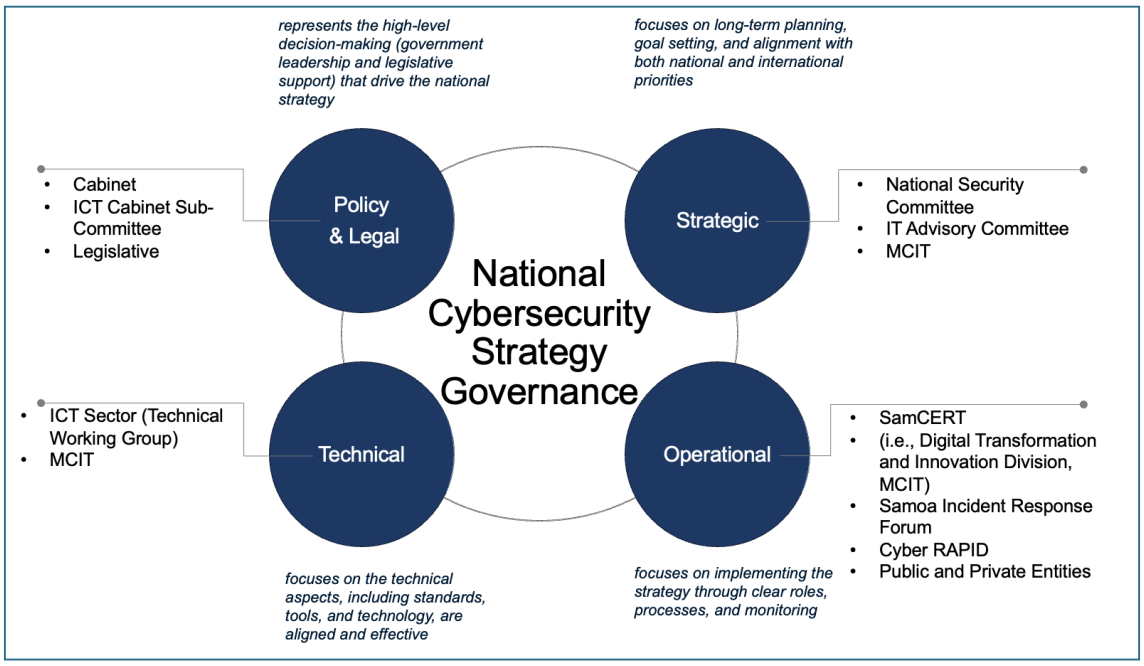

Figure 4: Samoa Country Profile - Global Cybersecurity Index

[3] SIRF will support Samoa on a national scale incident.

[4] RAPID Team will support Samoa in an event where the national team needs further assistance including SIRF.

CROSS-SECTORAL COORDINATION

Cross-sectoral coordination will be achieved through existing governance mechanisms. The NSC will provide overarching oversight, while sector-specific bodies will oversee the identification and protection of critical infrastructure. Existing structures, including the ICT Advisory Committee under the Information and Communication Technology Sector Plan as well as the Technical Working Group (TWG) for the IT Sector, already include cybersecurity within their Terms of Reference. This approach avoids establishing new committees and ensures alignment with broader digital transformation and cybersecurity objectives.

ROLES AND RESPONSIBILITIES

- ***Ministry of the Prime Minister and Cabinet*** provides leadership as chair of the ***National Security Committee (NSC)*** in areas of national security which includes cybersecurity.
- ***Ministry of Communications and Information Technology*** formulates national strategy for technology including cybersecurity and policy advice ensuring alignment with national priorities. ***SamCERT*** division provides operational support on cybersecurity incident response and awareness.
- ***The Samoa Incident Response Forum (SIRF)*** is an informal network consisting of IT professionals from various agencies across government. This forum was convened in response to the need of a platform to facilitate the dissemination of information relating to cybersecurity and enhance communications between technical personnel.
- ***Office of the Regulator (OOTR) / Government Ministries:*** Support legislative initiatives and align sector-specific goals with the national strategy.
- ***Private Sector Entities:*** Collaborate on cybersecurity initiatives, voluntarily share threat intelligence, and implement best practices.
- ***Academia:*** Contribute to research and development, and support skills development efforts.
- ***Civil Society:*** Engage in awareness campaigns and advocate for cybersecurity best practices
- ***Samoa Information Technology Association (SITA)*** focuses on building capacity building, facilitating networking, collaboration and advocacy for IT professionals in Samoa.
- ***Development Partners:*** partnership and collaboration work on advance assistance that are urgent and for recovery and post activities from cyber incidents.

By clearly defining roles and responsibilities, the governance structure ensures a clear division of tasks, avoiding overlaps and gaps. This collaborative approach leverages the strengths of all stakeholders, fostering a resilient and secure digital environment for Samoa.

PAVING THE WAY TO 2030/31: FOUR KEY STRATEGIC GOALS

To address challenges presented by the ever-changing cyber threat landscape and to be well-positioned to seize the opportunities effectively, the following four goals and corresponding priorities have been identified. A focus on these areas and its resulting implementation roadmap provides for sustainable development and positive societal impact.

STRATEGIC GOAL 1
ENHANCE PARTNERSHIP & GOVERNANCE IN CYBERSECURITY

- **Priority 1:** Strengthen the cybersecurity governance in Samoa.
- **Priority 2:** Enhance SamCERT's capacities.
- **Priority 3:** Strengthen partnerships.

STRATEGIC GOAL 2
DEVELOP LEGAL & REGULATORY FRAMEWORKS

- **Priority 4:** Development of data protection related legislation
- **Priority 5:** Update cybercrime law.
- **Priority 6:** Development of a new cybersecurity act

STRATEGIC GOAL 3
PROTECT CRITICAL INFORMATION INFRASTRUCTURE

- **Priority 7:** Development of CII identification methodology and designation of CII
- **Priority 8:** Development of CII Protection guidelines (requirements)

STRATEGIC GOAL 4
PROMOTE EDUCATION, AWARENESS, & INNOVATION

- **Priority 9:** The Information Security Policy & related standards promotion
- **Priority 10:** Cybersecurity education & skills development
- **Priority 11:** Targeted awareness raising to increase online safety.

Figure 5: Strategic Goals and Priorities for NCS 2025/26 - 2030/31

STRATEGIC GOAL 1

ENHANCE PARTNERSHIP & GOVERNANCE IN CYBERSECURITY

To develop Samoa's cybersecurity governance and enhance collaboration at both national and international levels, a series of actions will be undertaken throughout the implementation of the strategy.

PRIORITY 1: STRENGTHEN THE CYBERSECURITY GOVERNANCE IN SAMOA.

Efforts to re-align and re-define Samoa's cybersecurity governance framework will begin with a stakeholder needs assessment, identifying challenges and priorities for the cybersecurity governance framework. The relations to the functions of the National Emergency Operations Centre, Audit Office and relevant Government Bodies should be included. It is recommended that this task is done as a priority and no later than within the first six months following the strategy's approval. This will guide the drafting of a comprehensive governance framework, incorporating stakeholder feedback and best practices from international standards.

PRIORITY 2: ENHANCE SAMCERT'S CAPACITIES.

Recognizing the pivotal role of SamCERT in this governance framework, special emphasis is placed on enhancing its capacities to ensure it effectively fulfills its critical responsibilities such as incident response. The enhancement of SamCERT's capacities is crucial for ensuring cybersecurity in the country, serving as a cornerstone of national digital resilience. This priority is overarching throughout the entire strategy, reinforcing Samoa's ability to combat cyber threats, protect critical infrastructure, and safeguard digital assets.

The definition and approval of SamCERT's mandate as outlined in Goal 2 Priority 6 will clarify its roles and align them with national priorities. The development of standard operating procedures will standardize operations, while service automation will modernize its processes to improve efficiency and reliability. A well-resourced and fully operational SamCERT will not only strengthen national cybersecurity defenses but also strengthen trust in Samoa's digital ecosystem. To support these advancements, necessary software and hardware should be procured and integrated into SamCERT's operations.

In addition to the SamCERT, a team called SIRF was established during the CHOGM 2024. The main purpose of this forum is to build capabilities around SamCERT and hardening the Government Agencies networks infrastructure and staff capacity in terms of cybersecurity. This is later linked into regional initiatives and international cooperation with the RAPID Team.

PRIORITY 3: STRENGTHEN PARTNERSHIP.

Being a small island country with limited resources and capacities, fostering cooperation with national, regional, and international organizations is critical to ensure Samoa's cyber resilience. Several actions should be taken, starting with the development and implementation of a stakeholder engagement plan aimed at strengthening ties with private sector actors, academia, and government agencies to collectively address cybersecurity challenges.

Throughout the lifetime of the strategy, a regular mapping and updating of partners and partnerships should be conducted to ensure collaboration formats remain relevant and effective. Participation in cybersecurity events and training programs will enhance knowledge sharing and capacity building.

A strategic partnership workplan will be developed, focusing on key areas and prioritizing collaboration channels. An example is the formation of the SIRF and Rapid Team.

During the CHOGM 2024 Operation, access to resources from the New Zealand Cyber Security Center and RAPID Team provided much needed assistance for a national response effort to the Samoa's needs to cater for such a high secured event. It would be beneficial to use the same methodologies as the basis of this cooperation locally, regionally, and internationally.

STRATEGIC GOAL 2
DEVELOP LEGAL & REGULATORY FRAMEWORKS

To develop the legal and regulatory framework for the three priority areas of data protection, cybercrime, and cybersecurity, a structured and coordinated approach to legal framework formulation process will be adopted for each priority area. This approach will ensure consistency with stakeholder input, alignment with international and regional standards, and support for effective implementation and enforcement. The Ministry will lead priority area 4 and 6 while the Ministry of Police and Prison leads priority area 5. The OAG will support both agencies to lead develop, coordinate consultations, and monitor implementation.

The development of these legal and regulatory frameworks will also integrate online safety considerations, with particular emphasis on the protection of children from online harm and risk. In this context, the strategy will assess the feasibility and key requirements for implementing age-restriction measures for social media platforms, drawing on international best practice, including Australia's legislative approach which establishes 16 as the minimum age for holding social media accounts[5].

PRIORITY 4: DEVELOPMENT OF DATA PROTECTION RELATED LEGISLATION

Conduct a needs re-assessment in the early stages of the strategy implementation to identify current gaps in data protection. This assessment should include stakeholder consultations to gather insights into their specific requirements and challenges. The assessment will inform the drafting of a legislation, incorporation of best practices and ensuring inclusivity through feedback-driven revisions.

Stakeholder consultations will play an important role in the development of the data-protection-related legislation because they ensure that the law addresses the needs, concerns, and practical challenges of those affected, including businesses, government agencies, and the public while taking into consideration fundamental protections of human rights and freedoms.

Following governmental approval, the legislation will be implemented through widespread dissemination, training sessions for enforcement agencies, and ongoing monitoring to ensure compliance. Annual reviews will evaluate effectiveness and address emerging issues, fostering a dynamic and responsive data protection regime.

5 https://www.legislation.gov.au/F2025L00889/latest/text

PRIORITY 5: UPDATE CYBERCRIME LAW

Strengthen and update the existing laws to fully integrate the requirements of the Budapest Convention (or any other relevant documents, such as the United Nations Convention against Cybercrime). At the beginning of the strategy implementation, draft updates will undergo stakeholder consultations to ensure they address practical challenges and reflect diverse perspectives. Once the updated law secures governmental approval, its implementation will include training for law enforcement bodies and awareness campaigns to the government agencies and public to ensure compliance.

PRIORITY 6: DEVELOPMENT OF A NEW CYBERSECURITY ACT

Carry out a legal needs assessment of all existing legislation related to cybersecurity to identify areas for improvement and expansion (such as CIIP). This will lead to the drafting of a Cybersecurity Act, informed by stakeholder inputs, and aligned with national security objectives. Stakeholder consultations will ensure transparency and inclusivity, and government approval processes will finalize the act for implementation. Once enacted, the act will be disseminated, with targeted training provided to relevant agencies.

STRATEGIC GOAL 3
PROTECT CRITICAL INFORMATION INFRASTRUCTURE (CII)

The protection of CII is essential for Samoa's national security, economy, and provision of public services. The agency responsible for the CII protection should be determined either in the new Cybersecurity Act or via Government's order to define the mandate to enable this agency to guide the protection of CII as soon as possible, no later than within the first six months since the approval of the strategy.

The goal will be achieved through the development of clear methodology for CII identification, the creation of detailed protection guidelines (CII Protection, CIIP guidelines), and the integration of these measures into legal frameworks either as part of legislation or bylaws, alongside continuous monitoring and training efforts to ensure compliance.

The Government has already identified a list of Essential services where these services are a must for the government to function, refer to the Annex 1. The digital transformation of essential services has created a fundamental dependency on network availability. While manual continuity processes exist, the increasing integration of digital services means that any disruption to internet gateways now poses a significant risk to the operational resilience of these core government functions.

In this digital landscape, internet gateways serve as the primary defensive perimeter and the critical link ensuring the availability of services online; therefore, their security is paramount to national resilience.

PRIORITY 7: DEVELOPMENT OF CII IDENTIFICATION METHODOLOGY AND DESIGNATION OF CII

Following the establishment of a CII governance framework, the responsible agency will develop a methodology for identifying critical national infrastructure. This methodology will be informed by international good practice and feedback from relevant stakeholders to ensure its effectiveness.

Once the methodology is finalized, the identification process will begin, focusing on key assets and their owners. This process will involve collaboration between government agencies, regulators and critical services operators from the public and private sectors to ensure comprehensive and accurate identification of critical infrastructure.

The development of the CII identification methodology should be completed within the first twelve months following the approval of the strategy. The identification process for critical infrastructure will then

commence immediately afterward, with an estimated timeline of six to twelve months for full identification and engagement of relevant stakeholders.

PRIORITY 8: DEVELOPMENT OF CII PROTECTION GUIDELINES (REQUIREMENTS)

CII Protection guidelines are a set of operational, technical, and procedural standards and practices designed to secure and ensure the resilience of critical infrastructure against cyber threats and disruptions.

The development of CII Protection guidelines (requirements) should be completed soon after the completion of the CII identification process. Initially, a review of the existing Information Security policy will be conducted. Based on this review, a draft set of CII protection guidelines will be created, which will be validated through stakeholder workshops and feedback sessions to ensure they are tailored to stakeholders' needs and feasible for implementation.

Aligning the guidelines with best practices will be considered. Once finalized, the guidelines will be distributed to CII owners and relevant stakeholders, accompanied by training to ensure understanding and compliance. Ongoing monitoring will track adherence, and any instances of noncompliance will be addressed. These guidelines will also be integrated into the national legal framework to ensure enforcement.

STRATEGIC GOAL 4
PROMOTE EDUCATION, AWARENESS, & INNOVATION

To effectively strengthen cybersecurity posture and online safety in Samoa, it is essential to focus on education, awareness, and the promotion of key policies. Priorities in this area will include the promotion of the Information Security Policy and related standards, enhancing cybersecurity education with an emphasis of fostering innovation, and launching targeted awareness-raising initiatives. These efforts will help equip individuals and organizations with the knowledge and tools to navigate the digital world securely, fostering safer, more resilient cyberspace in Samoa.

PRIORITY 9: THE INFORMATION SECURITY POLICY & RELATED STANDARDS PROMOTION

The Information Security Policy[6] and its seven standards aims to protect the information and data within the government. To support the successful implementation of the policy, training materials will be developed to educate relevant stakeholders on the policy's requirements and its effective application. Training sessions will be conducted to ensure that government officials and other key entities understand the policy and are equipped to adhere to its guidelines. The IS Policy and its standards complement CIIP.

PRIORITY 10: CYBERSECURITY EDUCATION & SKILLS DEVELOPMENT

This priority focuses on the long-term goal of integrating cybersecurity education into Samoa's educational system and developing cybersecurity skills across the country. By integrating cybersecurity into primary, secondary, technical, and vocational education and training, and tertiary curricula, and by upskilling IT personnel across government agencies and emerging critical sectors, the goal is to foster the development of cybersecurity skills and create a broader pool of professionals equipped to tackle evolving threats. This will involve preparing and distributing teaching materials to schools and universities, integrating cybersecurity topics into existing syllabuses, and ensuring the curriculum puts emphasis on the innovation and is regularly updated to reflect the latest trends in the field. Additionally, development of programs in cybersecurity will offer advanced education and training for individuals pursuing specialized careers in the field.

Cybersecurity technical training will be offered to IT personnel across government, the essential service operators, and private sector.

6 Information Security Policy 2024, https://mcit.gov.ws/wp-content/uploads/2024/11/Information-Security-Policy_MCIT.pdf

PRIORITY 11. TARGETED AWARENESS RAISING TO INCREASE ONLINE SAFETY

This priority will focus on engaging diverse societal groups, with a particular emphasis on reaching remote villages to raise awareness about online safety. Each year, continuous awareness activities will be organized, such as the Samoa Mata'ala Roadshow and tailored campaigns, aimed at educating communities on online threats, personal security, and safe internet practices. Special attention will be given to rural and underserved areas, ensuring they are not left behind. The activities will utilize a range of platforms, from in-person events to digital tools, with regular follow-up to assess engagement and effectiveness. These efforts will be planned and executed annually, ensuring ongoing outreach, and increasing the reach and impact of cybersecurity education.

To ensure online safety, topics related to privacy breaches, harmful content, and irresponsible internet use will be addressed. The focus will be on building resilience to risks such as cyberbullying, online sexual exploitation, online threats and incitement, identity theft, and exposure to inappropriate content.

MCIT also captures Digital Child Exploitation Filter System and while the data are still at early stages of analysis, the Ministry uses such data to provide awareness on how to protect these materials from being accessed or produced in Samoa. The Childcare and Protection Bill now with the Ministry of Women, Community and Social Development is at its draft form and MCIT would like to use the opportunity to strengthen linkages and activities amongst these key stakeholders.

THEORY OF CHANGE

The logical pathway through which specific actions and interventions are expected to strengthen Samoa's Cybersecurity posture and achieve long-term resilience against evolving cyber threats through this National Cybersecurity Strategy is presented below:

ASSUMPTIONS:

- Management support, clear direction, adequate resources and communication channels.
- Access to information, stakeholder involvement, reference models, regular reviews, and availability of necessary tools and technologies.
- Sufficient budget and efficient procurement
- Quality technical expertise
- Secure, vendor support, and strong security controls
- Government support
- Subject matter expertise, curriculum standards, resource availability, stakeholder input, and ongoing course evaluation.

TARGET (VISION)	*'Secure and resilient cyber space for all in Samoa'*			
HIGH LEVEL OUTCOMES	National, regional and international stakeholders work together seamlessly, sharing information and best practices to strengthen collective cyber resilience	Comprehensive laws and regulations are in place and actively enforced, providing clear guidance and accountability for all cybersecurity activities	Essential systems and assets are protected against cyber threats, ensuring their continued operation and reliability	Individuals and organizations are well-educated on cybersecurity issues, fostering a culture of awareness and continuous innovation to address evolving cyber challenges
INTERMEDIATE OUTCOMES	Increased participation of stakeholders in cybersecurity policy formulation and operation Enhanced collective action in promoting cybersecurity best practices	Strengthened legislative foundation and improved harmonization with relevant cybersecurity conventions and standards.	Critical infrastructure are protected	Improved stakeholders' digital literacy

PROGRESS MARKERS	Established cybersecurity committees and working groups Regular governance meetings scheduled and conducted SamCERT's Operating Model requirements collected and analyzed Documentation, validation and approval of Standard Operating Model New cybersecurity SOPs tailored to Standard Operating Model drafted SOPs approved and implemented Key internal and external stakeholders mapped Stakeholders engagement plan with feedback mechanism finalized Regular stakeholder meetings and or updates scheduled and conducted	Draft Bills informed by review and analysis of legislations from comparable jurisdictions or countries Draft Bills validated through stakeholder consultations Budapest Convention requirements mapped against Existing Crime Act Finalized Bills submitted to Cabinet then Parliament	Established Methodology for Identification of Critical Information Infrastructure	Cybersecurity Communication Plan approved and implemented
INPUTS	SG1 A01 Establish Cybersecurity Governance Structure SG1 A02 Develop SamCert's Operational Modela	SG2 A06 Develop and implement a Data Protection Act SG2 A07 Amend and implement Crime Act to align with Budapest Convention	SG3 09 Develop and implement Methodology for Identification of Critical Information Infrastructure (CII)	SG4 10 Implement Information Security Policy 2024 SG4 11 Develop Cybersecurity courses (teaching learning and learning materials)

INPUTS (CONT.....)	SG1 A03 Develop and implement Cybersecurity Standard Operating Procedures SG1 A04 Support SamCert's Operatonal Model software and hardware resources and Lab SG1 A05 Develop and implement SamCert's Stakeholder Engagement Plan	SG2 A08 Develop and implement a Cybersecurity Act		SG4 12 Develop and implement Cybersecurity Communication Plan
ENABLERS	Legal and governance	Relationships with peer organizations, CSOs, private sector, professional bodies, digital service providers and networks	Technical assistance, information and resources	Efficient funding
PROBLEM	The absence of a cybersecurity governance framework and legislation, combined with limited implementation capacity, low awareness, lack of threat visibility, and increased digital transformation, significantly heightens the risk and prevalence of cyber threats.			
PRINCIPLES	››› Fosters and maintains ***trust*** ››› Is ***people-centric*** and ***inclusive*** ››› Protects ***fundamental human rights*** and ensures online rights are upheld ››› Encapsulates ***collaboration*** and ***cooperation*** among stakeholders ››› Ensures ***transparency (open-government)*** and ***accountability*** ››› Integrates a ***risk-based*** approach while balancing ***agility*** and ***resilience***			

CYBERSECURITY STRATEGY MONITORING MECHANISMS

The Monitoring, Evaluation and Learning matrix will be used to track progress, evaluate effectiveness, and ensure alignment with strategic goals. This is designed to offer real-time insights and facilitate informed decision-making, enabling MCIT and key stakeholders to adapt and respond to challenges and opportunities as they arise. Refer Annex 2

ESTABLISHMENT OF DEDICATED WORKING TEAMS

A primary aspect of monitoring mechanisms is the formation of dedicated working teams as outlined in the governance and action plan matrix. These teams are tasked with overseeing specific aspects of the strategy, ensuring that activities are executed according to plan. By taking ownership of the strategy, these teams can provide focused attention and accountability, drive progress and facilitate coordination across different Ministries. They serve as the frontline monitors, identifying potential issues early and implementing corrective measures promptly.

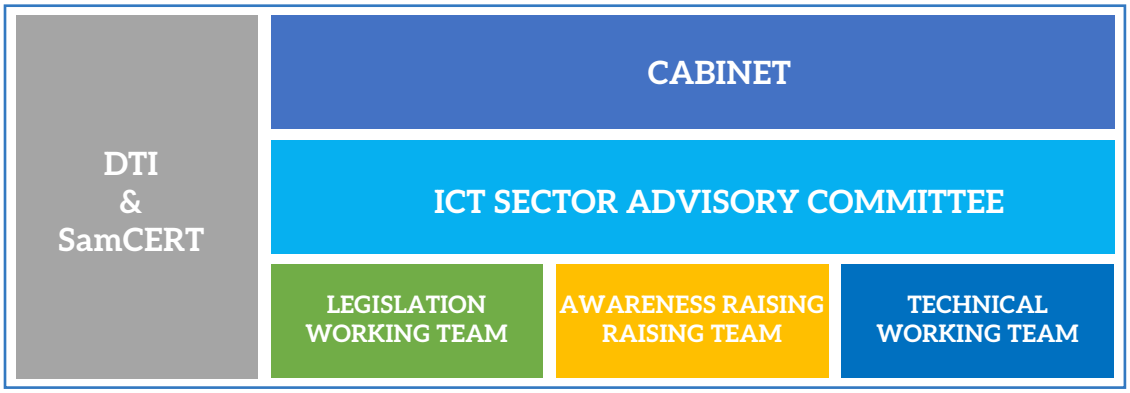

Figure 6: Monitoring Tools needed for gaining confidence for all stakeholders involved in the 2025/26 - 2030/31 on preparations and incident responses

REGULAR REPORTING AND REVIEWS

Regular reporting is a cornerstone of effective monitoring. By establishing a consistent schedule for reporting and reviewing progress, the Government can maintain transparency and accountability. These reports should include updates on KPIs, insights from working teams, and any challenges encountered. Regular reviews allow leadership to assess the overall health of the strategy, celebrate successes, and address any areas of concern.

REVIEW TIMETABLE

ACTIVITY	RESPONSIBLE	TIME
Launched National Cybersecurity Strategy	MCIT	July 2025
Mid Review	MCIT + OOTR + MPMC + MFAT + OAG	June 2027
Final Review	All	June 2030
Annual Review	MCIT	On going

FEEDBACK MECHANISMS

Incorporating feedback mechanisms such as surveys, interviews, and focus groups can provide valuable insights into the effectiveness of the strategy. These tools allow the Ministry to gather input from various stakeholders, including employees, customers, and partners. Feedback can highlight areas for improvement, reveal unforeseen challenges, and suggest innovative ideas for enhancing strategic initiatives.

Using Strategic Goal 4 as an example, the strategy aims to enhance online safety by promoting education, raising awareness, and encouraging innovation. To monitor progress, surveys and interviews will be extensively used with participants to collect insights on the effectiveness of the training and awareness sessions. This approach will enable SamCERT to conduct follow-ups, assess the long-term impact of training, and provide valuable feedback to management and executives.

TECHNOLOGY AND DATA ANALYTICS

Leveraging technology and data analytics is increasingly important in monitoring strategic progress. Advanced analytics tools can process large volumes of data, offering insights that might not be visible through traditional methods. These tools can identify patterns, predict outcomes, and provide actionable insights, enabling organizations to make informed decisions quickly.

The Ministry through its networks with PACSON and NCSC and ACSC, ITU, CTO and other regional partner also collects data, and it is hoped that the work conducted in Samoa compliments these statistics on cybersecurity. MCIT and New Zealand Department of Internal Affairs installed and launched a Digital Child Exploitation Filter System. So far, the Ministry is only using this data for training matters.

TRAINING AND CAPACITY BUILDING

Training and capacity building are integral to ensuring that monitoring mechanisms are effective. By equipping team members with the necessary skills and knowledge, the Government and its partners can enhance their ability to track and evaluate strategic progress. Ongoing training programs ensure that staff are up-to-date with the latest monitoring techniques and technologies, enabling them to implement interventions swiftly when needed.

BENCHMARKING AND COMPARATIVE ANALYSIS

Benchmarking against industry standards and conducting comparative analyses with peers can provide additional context for evaluating strategic progress. These practices help organizations understand their position within the industry, identify best practices, and set realistic targets. By learning from others, organizations can refine their strategies and improve performance.

In 2018 a Cybersecurity Maturity assessment was conducted with the Ministry and measures were in place to make sure the Government of Samoa lifts its security posture. It is also important to note that a lot has happened since then.

ADAPTIVE AND RESPONSIVE STRATEGIES

There are effective, adaptive and responsive monitoring mechanisms to allow the Ministry and its partners to pivot and adjust strategies as needed. This flexibility is crucial in today's fast-paced environment, where external factors can rapidly change the landscape. By maintaining a dynamic approach, MCIT can ensure that their strategies remain relevant and effective in achieving the goals outlined in the strategy.

Figure 7: CTF Prize Giving Opening Remarks from DFAT Staff at Falealili College. It was a successful event between the SamCERT and Retrospect Labs

ANNEX 1: List of Essential Services

Essential Services as identified under Public Service Commission are only Government Ministries:

1. **MAF** - Biosecurity, Fisheries (Monitoring Control and Surveillance duties), Regulatory Division
2. **MCIT** - Broadcasting Services (Radio 2AP)
3. **MPMC** - Immigration Services
4. **MOF** - Payroll & Budget Division
5. **MNRE** - Meteorology, Waste Management & Disaster Management Office
6. **MOH** - Public Health &Hospital Division
7. **MCR** - Customs & Border Management Division
8. **MWTI** - Maritime Division, Civil Aviation and Land Transport Division
9. **OOTR** - Spectrum Management and Technical Division (specific to interference issues)

ANNEX 2: National Planning Framework

MEL FRAMEWORK STRUCTURE						
Expected Outcome	National Indicator	Baseline	Target	Implementing Sector	Implementing Agencies	Data Source

ANNEX 3: Implementation for Results Matrix

Project Name	Timeframe	Input	Outputs	Indicators	PDS Alignment	Sector Alignment	Implementation Partner	Start Date	End Date	Budget
SG1 A01 Establish Cybersecurity Governance Structure	Short term	Budget and resources, Technical expertise, stakeholder engagement	Key stakeholders identified Stakeholder needs assessment completed Initial CNPFybersecurity governance framework drafted Cybersecurity governance framework including ToR, reporting channels approved Governance meetings scheduled and conducted	Regular governance meetings scheduled and conducted	KSO3	O4.3.4	MCIT, MPMC, OOTR, PSC			70,000.00
SG1 A02 Develop SamCert's Operational Model	Short term	Budget, software, hardware, Technical expertise	SamCERT's operational model approved Missing technologies identified and procured Standard Operating Procedures approved SamCERT's services automated	SamCert's services defined (Prevention & Response)	KSO3	O4.4.1	MCIT, OOTR, COC, SITA			100,000.00
SG1 A03 Develop and implement Cybersecurity Standard Operating Procedures	Short term	Budget, Technical expertise, updated stakeholder list, secured training opportunities	Gaps identified, existing SOPs compiled Cybersecurity SOPS tailored to SamCert's needs drafted Training on SOPs completed	Disaggregated number of staff trained on SOP Number of incidents where SOP was adhered to	KSO3	O5.1.1	MCIT, MFAT, OOTR			600,000.00
SG1 A04 Support SamCert's Operatonal Model software and hardware resources and Lab	Short term	Budget, Technical expertise, stakeholder engagement	Assessment of current software, hardware, and lab resources completed Resources gaps and requirements identified Procurement plan completed Lab environment established and configured	Required software and hardware procured and installed Lab established and operational	KSO3	O5.1.1	MCIT			500,000.00

Project Name	Timeframe	Input	Outputs	Indicators	PDS Alignment	Sector Alignment	Implementation Partner	Start Date	End Date	Budget
SG1 A05 Develop and implement SamCert's Stakeholder Engagement Plan	Short term	Budget, Technical expertise, stakeholder engagement	Key internal and external stakeholders identified and mapped Stakeholders engagement plan drafted and finalized Stakeholders meetings and updates conducted Stakeholders feedback loop established	Increased stakeholders engagement in Cybersecurity activities	KSO3	O5.1.2	MCIT, OAG, OOTR			100,000.00
SG2 A06 Develop and implement a Data Protection Act	Long term	Budget, Technical expertise, stakeholder engagement	International data protection standards and best practices reviewed Data Protection Bill drafted and presented to Cabinet	Data Protection Bill submitted to Parliament	KSO3	O4.1.4	SPPCS, OAG, MCIT, PSC, MOF			200,000.00
SG2 A07 Amend and implement Crime Act to align with Budapest Convention	Long term	Budget, Technical expertise, stakeholder engagement	Gap analysis of existing Crime Act versus Budapest Convention requirements completed Law enforcement and judiciary enaged for input on amendments Awareness and training on new provisions	Bill to amend Crime's Act submitted to Parliament	KSO3	O4.3.1 O4.3.4	MCIT, OAG, OOTR, SPPCS			200,000.00
SG2 A08 Develop and implement a Cybersecurity Act	Long term	Budget, Technical expertise, stakeholder engagement	Research and analysis of cybersecurity legislation from comparable jurisdictions completed Cybersecurity Bill drafted	Cybersecurity Bill submitted to Parliament	KSO3	O4.1.4 O4.3.1 O4.3.4	MCIT, MWTI			200,000.00
SG3 A09 Develop and implement Methodology for Identification of Critical Information Infrastructure (CII)	Long term	Budget and resources, Technical expertise	Methodology for Identification of Critical Information Infrastructure established	Number of Critical Information Infrastructure identified	KSO3	O4.4.1	MCIT, MWTI, SWA, EPC, COC, SITA, SSCC			550,000.00
SG4 A11 Develop Cybersecurity courses (teaching learning and learning materials)	Long term	Budget, Technical expertise	Cybersecurity courses and or training packages drafted	Improved Cybersecurity knowledge	KSO3	O5.1.3	MEC, NUS, MCIT SITA COC, PSC, SQA			400,000.00

Project Name	Timeframe	Input	Outputs	Indicators	PDS Alignment	Sector Alignment	Implementation Partner	Start Date	End Date	Budget
SG4 A12 Develop and implement Cybersecurity Communication Plan	Medium term	Budget and resources, communication collaterals, awareness	Cybersecurity Communication Plan approved	Increased visibility of Cybersecurity practices	KSO3	O5.1.4	OOTR, MCIT, SPPCS			400,000.00
SG4 A13 Implement and maintain robust network content filtering and monitoring systems to protect children from harmful online content	Medium term	Budget and resources, Technical expertise	Content filtering in schools and other public institutions	Increased Child Online Protection	KSO3	O5.1.8	MEC, MCIT, OOTR			300,000.00

ANNEX 4: Implementation and Budget Matrix

Project Code	Activity Name	Outcome	Budget	2025-2026				2026-2027				2027-2028				2028-2029				2029-2030			
				Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June
SG1 A01	SG1 A01 Establish Cybersecurity Governance Structure Conduct a stakeholder needs assessment Draft the cybersecurity governance framework Validate and present the framework for approval	Key stakeholders identified Stakeholder needs assessment completed Initial Cybersecurity governance framework drafted Cybersecurity governance framework including ToR, reporting channels approved Governance meetings scheduled and conducted	70,000																				
SG1 A02	SG1 A02 Develop SamCert's Operational Model Approve SamCERT's operational model (service catalogue) Define missing technologies required for the service delivery	SamCERT's operational model approved Missing technologies identified and procured Standard Operating Procedures approved SamCERT's services automated	100,000																				
SG1 A03	SG1 A03 Develop and implement Cybersecurity Standard Operating Procedures Review and approve SamCERTs Capacities Develop Standard Operating Procedures (SOPs) Purchase of the new software/hardware Automation of SamCERT's services	Gaps identified, existing SOPs compiled Cybersecurity SOPS tailored to SamCert's needs drafted Training on SOPs completed	500,000 100,000																				

Project Code	Activity Name	Outcome	Budget	2025-2026				2026-2027				2027-2028				2028-2029				2029-2030			
				Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June
SG1 A04	SG1 A04 Support SamCert's Operatonal Model software and hardware resources and Lab Continuously map and update partners, memberships in regional/ international organizations, and collaboration formats Participate in regional and international cybersecurity events Participate in regional training events Develop and implement a stakeholder engagement plan to enhance collaboration on cybersecurity with the private sector, academia, and government agencies	Assessment of current software, hardware, and lab resources completed Resources gaps and requirements identified Procurement plan completed Lab environment established and configured (Security Operations Center)	500,000																				
SG1 A05	SG1 A05 Develop and implement SamCert's Stakeholder Engagement Plan Conduct a needs assessment Draft the legislation Conduct public consultations Secure approval by the government Implement a legislation Continuously monitor and evaluate implementation	Key internal and external stakeholders identified and mapped Stakeholders engagement plan drafted and finalized Stakeholders meetings and updates conducted Stakeholders feedback loop established	100,000																				

Project Code	Activity Name	Outcome	Budget	2025-2026				2026-2027				2027-2028				2028-2029				2029-2030			
				Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June
SG2 A06	SG2 A06 Develop and implement a Data Protection Act Develop and approve working plan on legal alignment to Budapest Convention Secure approval by the government Implement legislation	International data protection standards and best practices reviewed Data Protection Bill drafted and presented to Cabinet	200,000																				
SG2 A07	SG2 A07 Amend and implement Crime Act to align with Budapest Convention Conduct a legal needs assessment Draft the legislation Conduct public consultations Secure approval by the government Implement legislation Continuously monitor and evaluate implementation	Gap analysis of existing Crime Act versus Budapest Convention requirements completed Law enforcement and judiciary enaged for input on amendments Awareness and training on new provisions	200,000																				
SG2 A08	SG2 A08 Develop and implement a Cybersecurity Act Determine agency responsible for CII in Samoa Develop CII identification methodology Identify CII and CII owners using the methodology developed Continuously review CII identification methodology	Research and analysis of cybersecurity legislation from comparable jurisdictions completed Cybersecurity Bill drafted	200,000																				

Project Code	Activity Name	Outcome	Budget	2025-2026				2026-2027				2027-2028				2028-2029				2029-2030			
				Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June
SG3 A09	SG3 09 Develop and implement Methodology for Identification of Critical Information Infrastructure (CII) Review of the existing information security standards Establish a CII working group Draft CII protection guidelines Validate and finalize protection guidelines Disseminate protection guidelines to CII owners Training on CII Protection Guidelines Voluntary Compliance Monitoring (12 months) Monitor and ensure compliance with CII Protection Guidelines	Methodology for Identification of Critical Information Infrastructure established	550,000																				
SG4 A10	SG4 10 Implement Information Security Policy 2024 Prepare training materials for training on the Information Security Policy and its implementation Training on the Information Security Policy and its implementation	Inclusive Cybersecurity awareness conducted	200,000																				

Project Code	Activity Name	Outcome	Budget	2025-2026				2026-2027				2027-2028				2028-2029				2029-2030			
				Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June	Jul-Sep	Oct-Dec	Jan-Mar	Apr-June
SG4 A11	SG4 11 Develop Cybersecurity courses (teaching learning and learning materials) Make cybersecurity a part of the curriculum at the primary, secondary, and tertiary levels of education Develop and launch cybersecurity programs Create and implement cybersecurity skills development program for IT personnel	Cybersecurity courses and or training packages drafted	400,000																				
SG4 A12	SG5 12 Develop and implement Cybersecurity Communication Plan Conduct continuous awareness-raising activities Develop and conduct targeted cybersecurity awareness campaigns for different audiences Continue working on existing cybersecurity awareness programs (e.g., Samoa Mata'ala Roadshow)	Cybersecurity Communication Plan approved	400,000																				
SG4 A13	Implement content filtering in schools	Increased Child Online Protection	300,000																				

GLOSSARY

Term	Definitions	Reference
Cyber safety	The practices and precautions taken to protect individuals and their information when using the internet and digital devices. It involves being aware of online risks—such as cyberbullying, scams, identity theft, and exposure to inappropriate content—and knowing how to avoid or respond to them. Cyber safety includes using strong passwords, not sharing personal information, recognizing suspicious emails or messages, keeping software updated, and understanding privacy settings on social media and other platforms.	Australian Government, eSafety Commissioner. (n.d.).
Cybersecurity	The practice of protecting computer systems, networks, and digital data from unauthorized access, attacks, damage, or theft. It involves the use of technologies, processes, and policies to safeguard information and ensure the confidentiality, integrity, and availability of data. Cybersecurity covers a wide range of activities, including securing networks, protecting devices, managing user access, and responding to cyber threats such as malware, phishing, and hacking.	National Institute of Standards and Technology (NIST). (2022). Cybersecurity Framework.
Online safety	refers to the measures and practices that individuals use to protect themselves and their personal information while using the internet. It involves being aware of potential risks such as cyberbullying, scams, identity theft, and exposure to inappropriate content, and knowing how to avoid or respond to these dangers. Online safety includes actions like using strong passwords, not sharing sensitive information, recognizing suspicious links or emails, and understanding privacy settings on websites and apps.	UK Safer Internet Centre. (n.d.).
Cybercrime	refers to criminal activities that are carried out using computers, networks, or the internet. These crimes can target individuals, organizations, or governments and often involve the theft of personal information, financial fraud, hacking, spreading malware, or illegal online activities such as cyberbullying and identity theft. Cybercrime can be committed by individuals or organized groups and can have serious financial, personal, and societal impacts.	Interpol. (n.d.). Cybercrime.
Critical Information Infrastructure (CII)	refers to computer systems, networks, and digital assets that are essential for the functioning of a country's critical services, such as energy, water, transportation, healthcare, finance, and government operations. Disruption or damage to these infrastructures could have a significant impact on national security, public safety, the economy, or the well-being of citizens.	National Critical Information Infrastructure Protection Centre (NCIIPC), Government of India. (n.d.).
Social engineering	refers to a manipulation technique that exploits human psychology to trick individuals into revealing confidential information or performing actions that compromise security. Instead of attacking technical vulnerabilities, social engineering targets people, often through methods such as phishing emails, pretexting, baiting, or impersonation. The goal is typically to gain unauthorized access to systems, data, or physical locations.	Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). Social Engineering Attacks.
Ransomware	is a type of malicious software (malware) that encrypts a victim's files or locks them out of their computer system, making the data inaccessible. The attacker then demands a ransom payment, usually in cryptocurrency, in exchange for providing a decryption key or restoring access. Ransomware attacks can target individuals, businesses, or organizations and often cause significant financial and operational damage.	National Cyber Security Centre (NCSC). (n.d.). Ransomware.

Term	Definitions	Reference
Essential Services	In Samoa, refer to services that are critical for the health, safety, and well-being of the population, as well as the functioning of society and the economy. These typically include services such as healthcare, water supply, electricity, law enforcement, emergency response, and telecommunications. According to the *State of Emergency Orders* issued by the Government of Samoa (for example, during the COVID-19 pandemic), essential services have specifically included: • Hospitals and health services • Police and fire services • Electricity and water supply • Telecommunications • Banking services • Supermarkets and food supply • Fuel supply	Government of Samoa. (2020). State of Emergency Orders (COVID-19).
Malware (short for "malicious software")	is any software intentionally designed to cause damage to computers, servers, networks, or users. Malware can steal, encrypt, or delete data, alter or hijack core computer functions, and monitor users' activity without their permission. Common types of malware include viruses, worms, trojans, ransomware, spyware, and adware.	National Institute of Standards and Technology (NIST). (2020). Glossary: Malware.
Tradecraft	refers to the techniques, methods, and procedures used in espionage and intelligence operations to accomplish missions and protect agents. It encompasses skills such as surveillance, counter-surveillance, secure communications, disguise, clandestine meetings, and the use of codes or ciphers. Tradecraft is essential for intelligence officers and spies to operate covertly and avoid detection.	U.S. Department of Defense. (2010). Dictionary of Military and Associated Terms (JP 1-02).
Security Operation Center (SOC)	A centralized unit within an organization that is responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents in real time. The SOC is staffed by security analysts and engineers who use a variety of tools and processes to protect the organization's information systems from threats such as malware, unauthorized access, and data breaches. The SOC typically operates 24/7 to ensure continuous protection.	National Institute of Standards and Technology (NIST). (2022). Security Operations Center (SOC). In NIST Special Publication 800-172A.
Cyberspace	A term used to describe the virtual environment created by interconnected computer networks, including the internet, telecommunications networks, and computer systems. It is the domain where digital communication, data exchange, and online activities occur. Cyberspace encompasses all the hardware, software, and data that enable digital interactions and is fundamental to modern information technology and communication.	National Institute of Standards and Technology (NIST). (2019). Cyberspace. In NIST Special Publication 800-37 Rev. 2.
RAPID Team Rapid Assistance for Pacific Incidents and Disasters.	In Australia and the Pacific, RAPID team generally refers to a group of specialists—often within national CERTs (Computer Emergency Response Teams) or the Australian Cyber Security Centre (ACSC)—who are tasked with quickly responding to, investigating, and mitigating cyber incidents. These teams may be deployed to assist organizations, government agencies, or Pacific Island nations in the event of significant cyber threats or attacks.	Australian Cyber Security Centre. (2023). Incident Response.