Tonga National Cybersecurity Framework

Cyber Security Consultancy Services for Developing and Supporting Information Systems

Contract number: TO-MFNP-128783-CS-CQS
Project duration: 12 November 2020 – 11 May 2022

4 January 2022

Change history

Version	Date	Summary of changes
1.0	4 January 2022	First version for approval

Document status

Draft	
For approval	X
Approved	

Authors

Name	Role
Epp Maaten	Team Leader
Rünno Reinu	Security Analyst
Janno Kase	Security Consultant/Specialist
Toomas Lepik	Security Engineer
Marit Lani	Project Manager

Table of Contents

Glossary

Acronym	Explanation
DGSP	Tonga Digital Government Strategic Plan 2018–2023
DGSF	Tonga Digital Government Strategic Framework 2019–2024
G2C	Government to citizen
G2B	Government to business
G2G	Government to Government
ICT	Information and Communication Technologies
ITU	International Telecommunication Union
MDA	Ministries, departments, agencies
SDG	UN Sustainable Development Goals
SGN	Tonga Secure Government Network
TSDF	Tonga Strategic Development Framework 2015-2025
TCC	Tonga Communications Company
UN	United Nations

Preface

Purpose

The Tonga National Cybersecurity Framework provides strategic goals and supporting objectives to guide the Government and public enterprises on how to build and strengthen government processes and workflows. The National Cybersecurity Framework outlines the prioritized actions that ministries, departments and agencies (MDAs), but also private sector companies and citizens, when applicable, must apply to reduce their vulnerability to cyber threats.

Scope

At the national level, cybersecurity is a shared responsibility that requires coordinated action for prevention, preparation, response, and incident recovery on the part of government authorities, but also from the private sector and civil society. A comprehensive National Cybersecurity Framework is necessary, which is in line with the Tonga Digital Government Strategic Framework 2019-2024 (DGSF). The current framework follows the holistic (whole-of-government) approach of the DGSF according to which all IT and digital government initiatives should acknowledge and be aware of the potential impact on G2G, G2B, and G2C interactions. However, the main focus is on the governmental sector with the task to develop and safely manage the data and information systems used for improving government services.

The current framework is part of strategic planning, which, first of all, has an important impact on how the overall system operates and which priorities drive decision-making and resource allocation. A robust framework is a critical enabler of long-term success and provides relevant mandates to identify the roles of various stakeholders, as well as institutes laws that protect data and privacy (e.g. through use-purpose specification) and information security (cyber security).

Target audience

The Tonga National Cybersecurity Framework **is targeted for Tongan Government agencies** to improve the overall security profile and ICT capabilities across the government. The framework also addresses the general public and enterprises through raising risk awareness and improving personal cyber hygiene.

Executive Summary

The Tonga Strategic Development Plan 2018–2023 (DGSP) sets among its National Outcomes the aim of successful provision and maintenance of infrastructure and information technology together with a dynamic knowledge-based economy. The closely aligned Tonga Digital Government Strategic Framework 2019–2024 sets the direction for the Government's use of Information and Communication Technologies (ICTs), with the ultimate intent of improving Government decision making, business process and workflow efficiency, improving the quality and timeliness of services for the people of Tonga, while reducing the complexity and cost of Government services. The DGSP relies on the digitization of information and data to provide the basis for more efficient process automation, interagency workflows, with the intent of improving the cost and efficiency, and utility of Government information and decision support systems. Personal privacy, security, disaster recovery and continuity of operations, and data protection and sovereignty are all assigned high priority within the DGSP.

The National Cybersecurity Framework establishes objectives to help guide the often complex requirements to develop and safely manage the data and information systems used for improving government services. Cybersecurity is closely linked to the architecture and frameworks required within the DGSP, such as the Tonga Enterprise Architecture Framework, and the information exchange model that will help facilitate the integration and exchange of data across agencies.

The Cybersecurity Framework does not prescribe any technologies, individual standards, or international best practices – a multitude of aspects must be taken into consideration when making specific policy or regulatory decisions which will impact the implementation and operations of ICTs in Tonga. The current framework provides a system of stakeholder requirements, which is transformed into national and organizational objectives and outcomes. The Implementation Plan defines key success factors, or compliance metrics, which need to be officially set by the key stakeholders and parliament, and followed by all MDAs when implementing their ICT activities.

The Cybersecurity Framework document is structured in four main chapters. In the first chapter, the vision and goals for Tonga are set for the next years in the cybersecurity domain. Next, the Framework describes the environment of today's trends in digital development. The second chapter introduces cyber threats and trends in cybercrime, and the national capacities to address these. The essence of the Cybersecurity Framework is in Chapter 3, which describes the main strategic actions and targets in six areas. Chapter 4 covers the implementation mechanism as well as the monitoring and evaluation of the strategy.

1. Vision and Approach

1.1. Vision

The Cybersecurity Framework envisions to provide a more reliable and safe digital environment for the Kingdom of Tonga.

The vision is aligned with the vision and mission of the main strategic documents of Tonga – the Tonga Strategic Development Framework 2015-2025 (TSDF) and the Digital Government Strategic Plan 2018-2023 (DGSP).

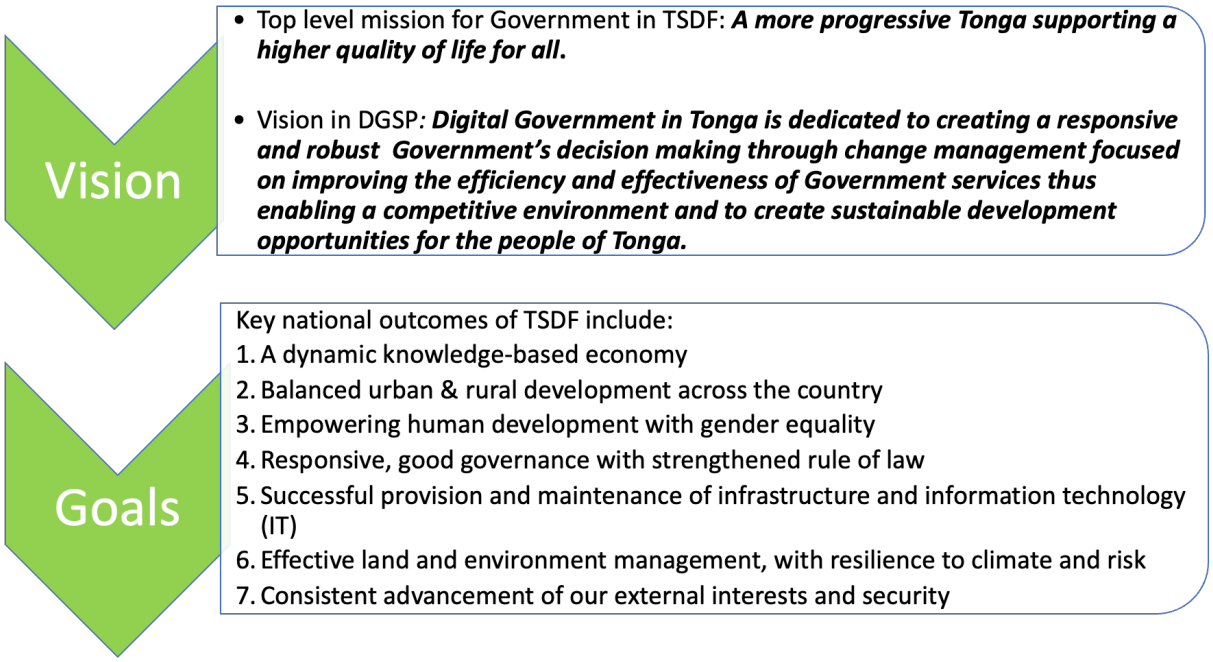

Figure 1. Strategic visions and goals in TSDF 2015-2025 and GDSP 2019-2024.

1.2. Basic principles

The Tonga Digital Government Strategic Plan 2019-2024 sets the basic principles that each information technology (IT) infrastructure project or information Systems (IS) project should consider. These principles are applicable also when protecting the confidentiality, integrity and availability of governmental e-services and IT systems:

1. Security
2. Connectivity
3. Interoperability
4. Portability
5. Innovation
6. Accessibility
7. Customer focus
8. Standardization
9. Redundancy
10. Holistic (whole-of-government) approach

2. Overview of the Environment

2.1. Cyber Threat Environment

Vulnerability in cyberspace

Tongan citizens, public and private organizations are increasingly dependent on the use of cyberspace. The rapid process of digital transformation changes the way people work, communicate and spend their leisure time. At the same time, the increased dependence on the cyberspace brings out several risks, including the risk of cyber threats. The complexity and interdependency of technology in cyberspace makes its protection against cyber threats a very challenging task.

The severity of cyber threats

Malicious cyber activities can be carried out by a wide array of actors – individuals or criminal hacker groups, but even by state supported terrorist groups. Cyber criminals are becoming better organized and well-funded to execute such malicious activities. At the same time, barriers to enter the cybercrime landscape are getting even lower, thus enabling high income for low-risk criminal activities. Cyber attacks may affect the Tongan Government and other public organizations, businesses of all size and even all of the individuals who are connected to the digital world.

Cyber attack goals and methods

The goal of cyber attacks is usually linked to financial earnings (theft, blackmailing, et.) and gaining power (infrastructure disruptions, social unrest, etc.).

There are several methods to perform successful cyber attacks. Information systems could be intruded to steal business information or personal confidential information that can lead to blackmailing activities. Furthermore, malicious cyber actors can infiltrate communication systems of governments and can collect financially and politically sensitive information. Another method of blackmailing includes deployment of ransomware that makes personal or business files unusable until ransom is paid. The increase in harassment campaigns in social media has led to malicious political influencing activities.

2.2. Protection of Critical Infrastructure

Critical infrastructure can be seen as a backbone for the whole Tongan society, enabling national security, government activities, economic growth and social wellbeing of the citizens. Infrastructure consists of human-made physical and organisational structures and facilities such as buildings, roads, air and marine ports, utilities, sports facilities, schools, hospitals, etc. that are required for a society and economy to function. Disruptions in the operation of critical infrastructure can seriously and negatively affect Tonga's ability to function as a successful society.

It is vital to bear in mind that malicious cyber attackers are able to infiltrate connected critical infrastructure objects. Later, they may be able to take control of the information systems that are controlling the operations of the critical infrastructure, including remotely interrupting or even destroying the infrastructure objects. In other countries, there have

been several serious and successful attacks against the industrial control systems of critical infrastructure objects, namely power grids and power plants, aviation and marine systems, health care and national databases. The variety of attack vectors has been wide, including malware through emails, poorly protected wireless networks, websites and even social media.

A Secure Government Network (SGN) and a consolidated Data Center infrastructure has been prepared for the Tongan MDAs. However, many agencies either continue to operate independent server rooms or outsource their IT systems to commercial vendors. In the framework of the World Bank supported project "Cyber Security Consultancy Services for Developing and Supporting Information Systems", in September 2021, a report on "Cybersecurity audit and risk assessment of Tongan Government agencies" was delivered and a survey on information security and risk management was carried out. The survey pointed out several weaknesses discovered in the current solutions concerning the security of perimeters and other physical controls of server rooms. Thus, the use of the consolidated Data Center should be further encouraged.

2.3. Awareness of Cybersecurity

Rapid development of ICTs is always accompanied by risks related to the public awareness of cybersecurity. For example, the lack of cybersecurity awareness is one of the most important factors in successful cybercrime cases. In response to these emerging risks, the Tongan government sector has implemented plans and actions to raise awareness of the importance of cybersecurity.

The public sector of Tonga approaches cybersecurity awareness on a number of levels:

- Awareness related to cybersecurity incidents is covered by CERT Tonga
- Awareness related to the behavior of public servants in relation to social media is handled by the Public Service Commission
- Cross-sectoral awareness through "advocacy at regional and national level key events"[1] is the responsibility of three working groups:
    - Cybersafety Working Group
    - Cybersecurity Working Group
    - Cybercrime Working Group.

CERT Tonga together with other government and private organisations is active in the area of awareness-raising. They cooperate with the Tonga Police and Attorney General's Office to carry out cyberhygiene events. For example, in 2021 a series of training events on "Social Media and the Law" were held, highlighting the existence of the "Electronic Communication Abuse Offences Act 2020", which came into force on 1 July 2021.

As cybersecurity awareness-raising is an ongoing process, many steps are yet to be performed to minimize the gap between secure use of ICT and current practices.

The survey on information security and risk management carried out as part of the report on "Cybersecurity audit and risk assessment of Tongan Government agencies" addressed Tongan Government Agencies and resulted in a number of recommendations for increased

[1] Cybersaftey Working Group Terms of Reference (ToR), 2021; Cybersecurity Working Group Terms of Reference (ToR), 2021; Cybercrime Working Group Terms of Reference, 2021

awareness related to information security and incident management within those agencies. In particular, awareness should be increased in the following areas:

- secure use of mobile devices and remote work for the staff of the agencies
- secure ways of using information systems, internet and email
- clear employee responsibilities (including responsibilities related to incident management and incident reporting).

Among the obstacles to increased awareness are the insufficient quality of network connections in remote locations and a lack of resources, such as personnel or awareness materials.

2.4. Cybersecurity Control Environment of Tongan MDAs

Based on international standards such as ISO 27001 and ISO 27005, the aforementioned survey aimed at obtaining a picture of how the individual Tongan authorities govern cybersecurity risks, and which organizational and technical measures are in place to manage security risks posed to networks, information systems and their usage.

The results of the survey revealed that the majority of the government agencies have implemented a general information security policy and information security guidelines for end-users, which is definitely necessary when setting common IT security principles in the organisation. Furthermore, policies covering access management, logging and monitoring, network security and physical/environmental security were generally implemented at least to some extent in the majority of the institutions who responded.

On the other hand, certain areas of information security are not widely covered with policies and procedures. Such areas include mobile devices and remote access, backup of systems and data, vulnerability and patch management, business continuity, disaster recovery and IS outsourcing. Furthermore, one fifth of the institutions reported having no written IT security policies in place.

Regarding the implementation of information security measures in Tongan public sector organisations, biggest gaps were detected in the secure usage of mobile devices, segregation of access controls, responsibilities of vulnerability and patch management and awareness raising of employees.

3. Strategic Tasks

The strategic tasks of Tonga outlined in this chapter are set to improve the efficiency and effectiveness of government services and make them more reliable and safe by using ICTs. ICTs can make a major contribution to mitigating the difficulties of remoteness and distance; they can provide accessible communications formats that enhance the engagement of vulnerable and excluded groups. ICTs can help improve knowledge, services delivery and trade. In times of disaster, reliable communications can play a critical role both before and after. The rapidly falling costs of communications technology and the increasingly small scale at which it can operate, are particularly important for addressing our small economies of scale and the need for inclusive communications and access to the Internet. Therefore the reliable and safe use of ICTs is essential when delivering key services by government and businesses, and drawing communities more closely together.

The proposed Cybersecurity Framework is based on the the "Guide to Developing a National Cybersecurity Strategy"[2] that introduces a set of good practice elements that can make the strategy comprehensive and effective, while allowing for tailoring it to the national context. The seven strategic areas listed in the Guide are adjusted to the Tongan environment based on the existing cybersecurity interventions, public strategies, related policies and frameworks, and current practices.

3.1. Implement Safe Digital Governance

The Tonga Digital Government Strategic Framework 2019–2024 sets directions for the Government's use of ICT, with the ultimate intent to transform and simplify the way Government does business through digitization, innovation, and automation of Government processes. However, digital governance involves areas of great concern such as personal privacy, security, disaster recovery and continuity of operations. The strategic objective of the DGSF is to ensure the compliance of information systems' with laws and regulations concerning privacy and protection of national information.

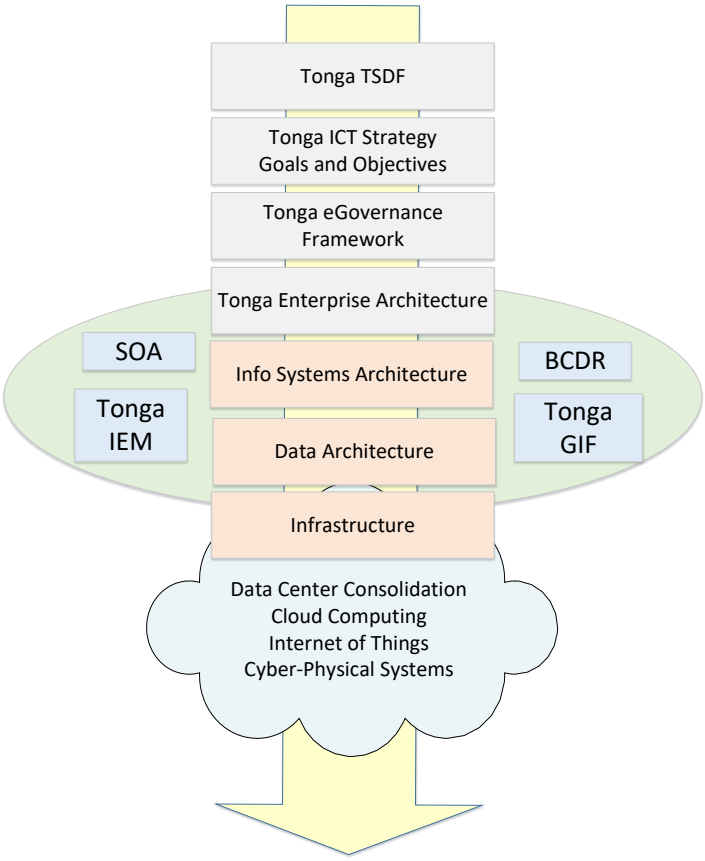

Figure 2. e-Governance Integrated Frameworks of Tonga DGSP. TSDF - Tonga Strategic Development Framework, BCDR – Continuity of operations plan, SOA – Service Oriented Architecture, IEM – Information Exchange Model, GIF – Government Interoprability Framework

Cybersecurity of e-governance is closely tied to the architecture and frameworks required within the DGSP, such as the Tonga Enterprise Architecture Framework, data interoperability framework, and a Tonga information exchange model that will help facilitate the integration

[2]ITU, *Guide to Developing a National Cybersecurity Strategy – Strategic engagement in cybersecurity* 2018

and exchange of data across agencies.

The DGSP foresees the development of a National Digital Government Security Standard. However, as an introduction, a **Cybersecurity Manual** for Tongan government agencies should be developed and adopted. The manual would serve as a basis for the future Digital Government Security Standard and would enable ensuring the confidentiality, integrity and availability of data and services.

The Government of Tonga is currently preparing upgrades to the Civil Registration and National Identity systems, including a new electronic linkage between the two that will contribute to Tonga's progress towards the UN Sustainable Development Goals (SDGs) agreed in 2015 by all UN Member States. The provision of a 'legal identity for all' is a target of the SDGs, and is also key to achieving many other SDGs, such as access to basic services.

Tonga MDAs currently connect to each other, and internally within the agencies, using public Internet services. Not having a communications technology standard or standard vendor service agreements, as well as security risks from exposing government data to the public Internet present high operational and security risks. The Tonga **Secure Government Network** (SGN) will allow better end-user performance allowing implementation of more efficient, innovative applications and services as it connects Government agencies to the national data center and to standardized cloud computing resources.

The **consolidated data center** environment offers all government agencies **cloud computing** resources and interconnection or interoperability tools. The consolidated data center will also ensure disaster recovery and continuity of operations for MDAs, once the backup data center environment is made available. Therefore, transitioning information systems of the MDAs into a cloud computing environment ensures the interoperability, portability, and better security to protect the confidentiality, integrity, and availability of Tonga's data resources.

Actions:

1. Develop and adopt a Cybersecurity Manual for Tongan government agencies
2. Carry out the upgrade of Civil Registration and National Identity systems.
3. Transition all MDAs to the Secure Government Network (SGN).
4. Implement the Data Center Consolidation Program and Tongan Government Cloud Computing Transition

3.2. Risk management

It is important to realize that cybersecurity incidents can never be completely prevented. The rapid development of technology and its accelerated spread also increases the potential for security incidents in information systems and critical IT infrastructure. Therefore, in addition to preventing incidents, focus must also be on **cyber resilience** – i.e. on the **control and reduction of damage caused by incidents**. This requires two types of actions: firstly, proactive measures aimed at preventing incidents, and secondly, reactive measures to control and reduce damage as shown in Figure 3.

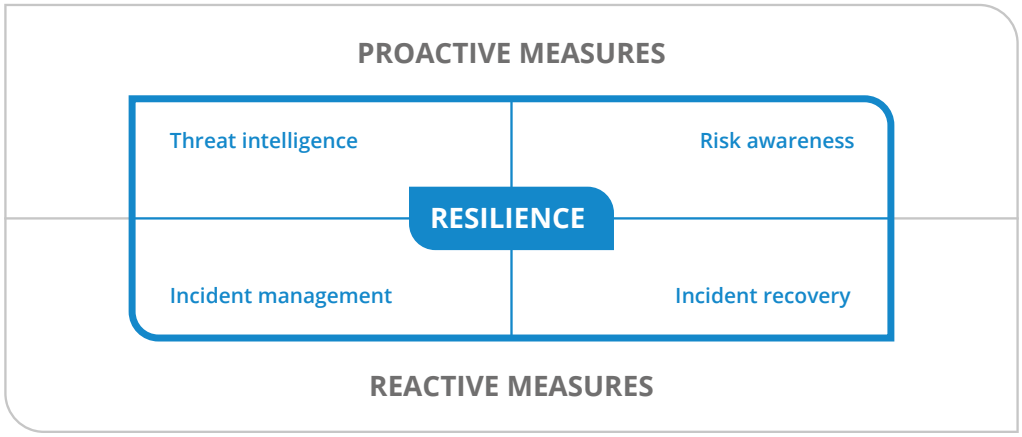

Figure 3. Measures to achieve cyber resilience

According to the ISO/IEC 27005 standard on information security, risk management assessment of consequences of a security incident is part of the risk analysis process. First, all relevant ICT assets of an organisation should be identified and valuated. Asset valuation begins with the classification of assets according to their criticality, in terms of their importance for fulfilling the main objectives of the organization. Valuation is then determined using two measures:

- the replacement value of the asset: the cost of recovery clean-up and replacing the information (if at all possible);
- the business consequences of loss or compromise of the asset, such as the potential adverse business and/or legal or regulatory consequences from the disclosure, modification, non-availability and/or destruction of information, and other information assets.[3]

Continuous monitoring and analysis of information on security incidents both domestically and internationally makes the rapid identification of threats possible and the resolution of incidents more effective. Therefore, Tonga will put continuous effort into **identifying and understanding potential threats** (threat intelligence) **and the risks** associated with these threats (risk awareness). There is also a need for resources to **detect and cope with incidents** (incident management) and to plan activities and resources to **deal with the damage** caused by incidents (recovery). The existence of such measures will, on the one hand, increase the ability to prevent incidents by increasing the overall security and, on the other hand, significantly reduce the adverse impact of incidents on society.

To improve Tonga's resilience against such incidents, it is essential to **detect, analyse, understand, and mitigate cybersecurity risks**.

Cybersecurity risks involve three components as shown in Figure 4:

- **Threat**. Threats can be either technological, such as malware, or geopolitical, such as adversary nation states, criminal, such as an organized crime group, or even environmental, such as extreme weather conditions.
- **Vulnerability**. Vulnerability is often described as a weakness of a computer system that can be exploited. In the cyber ecosystem, vulnerability is more complex, and the nature can either be technological, organizational, administrative, or anything else that might leave the ecosystem open to cyberthreats.

[3] Chapter B.2 Asset valuation, ISO/IEC 27005 Information Security Risk Management

- **Impact** (consequence). Impact can be assessed when combining the likelihood of the cyber incident with the potential impact to the ecosystem or its components.

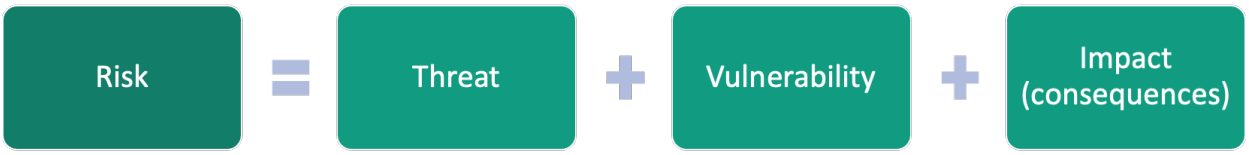

Figure 4. Three components of cybersecurity risk.

To mitigate cybersecurity risk and minimize the negative impact of cyber threats, the Government of Tonga shall introduce the **procedure of regular risk assessment in every public institution and critical private enterprises.** The assessment findings shall be recorded in a format of a combined security risk register that assists in the preparation of risk mitigation plans for Tongan MDAs and critical private enterprises. These plans will detail the activities necessary to be carried out for IT and cybersecurity risk mitigation, including activity description, priority, responsible stakeholders, and time of completion.

Both national level and sector oriented cyber risk repositories improve the understanding of current cybersecurity risks and allow to forecast and model trends. It is important that all considerable changes in technological risks are included in the risk mapping. New risks related to major shifts in technology such as the use of artificial intelligence, quantum computing, etc. should also be considered. Similarly, risks that are related to the growing use of existing technologies such as cloud computing and IoT should also be considered in the risk landscape.

Actions:

1. Identify threats and vulnerabilities of public sector information systems and critical IT infrastructure.
2. Perform regular risk assessments in public organisations and critical private enterprises.
3. Prepare risk mitigation and disaster recovery plans.

3.3. Threat preparedness and incident response

The information security and risk management survey also pointed out that many Tonga MDAs do not have a dedicated policy for incident management, let alone a process defined. **Defining the incident management process** becomes one of the areas for improvement to avoid that the responsibilities and even the consequences are not formally clear.

All MDAs should have a full overview of their cybersecurity incidents. Without an **incident reporting requirement** Tonga MDAs will not get a clear picture of the threats and vulnerabilities they are facing. The same applies to critical private sector enterprises. Therefore, improvement in this area is desired and starts with setting the requirement to report any ICT incidents to the Ministry of MEIDECC. The partnership between public and private sector should be enhanced as well and the reporting of cybercrime and cybersecurity incidents has to be consistently promoted. The lessons learnt should be captured and analyzed by the responsible officials. Based on reporting, incidents can be centrally analysed and appropriate awareness and training can be organized to prevent future incidents.

The main body responsible for preventing and solving cybersecurity incidents in Tonga is currently CERT Tonga. The team provides the public sector with a portfolio of computer emergency response services and focuses on educating public and private sectors alike. CERT Tonga carries out forensics and analysis of digital evidence in cooperation with law enforcement authorities.

As of today, electronic evidence is an element in almost all crimes. Therefore, increasing the resources of CERT Tonga and their ability to **investigate and analyze digital evidence** is crucial for Tonga. There is also a need to develop **standardized procedures of electronic evidence management** both for Tonga Police and CERT Tonga.

While the mission of CERT Tonga is related more to increasing the awareness and the level of education among the Tongan public and private sectors, the IT team of the Ministry of MEIDECC is dealing with the more technical aspects of information security and incident response. This separation of tasks is further reinforced by MEIDECC analysing the needs and planning a governmental CSIRT in the future.

Actions:

1. Define the incident management process in all MDAs
2. Introduce the requirement for reporting incidents for MDAs
3. Enhance Public-Private-People Partnerships on cybercrime and promote the reporting of incidents
4. Enhance the investigation and forensic capability of CERT Tonga
5. Develop standardized procedures of electronic evidence management both for Tonga Police and CERT Tonga.

3.4. Enhanced skills

With the rapid growth of internet connectivity in Tonga, many citizens are getting access to the internet, while often lacking knowledge of how to protect themselves online. The Digital Government Strategy Framework 2019-2024 (DGSF) emphasizes that training (among other areas) accelerates the benefits of the DGSF goals, such as advancing digital inclusion for all (i.e. cultivating activities that ensure all individuals and communities – including those disadvantaged – access and use ICT). Tonga is aware of the financial support and the long-term planning that these national priorities require. Two specific objectives in cultivating digital literacy and digital inclusion according to the DGSF are:

- 3.2 Incorporate digital literacy skills development into all educational programs
- 3.6 Promote adult and professional education programs to develop Enterprise Architecture, Governance and management-oriented ICT capabilities.

While reaching these objectives, Tongan authorities ought to assign a high priority to "personal privacy, security, disaster recovery and continuity of operations, and data protection and sovereignty" as the ICT implementation and operation gain momentum.[4]

[4] The 2019-2024 Digital Government Strategic Framework. January 2019. Kingdom of Tonga. P. 19, 28, 31, 41

In 2021, CERT Tonga launched a cooperation with the cybersecurity services provider Trustwave on the enhancement of CERT Tonga services and incident management for the public sector, which has resulted in a meticulous list of training courses, exercises and awareness-raising opportunities that are planned to be delivered in 2022. In cooperation with law enforcement agencies, CERT Tonga conducted training courses around the country in 2021 on the safe use of social media. The training opportunities provided by international organisations such as ITU or APNIC are also very valuable for Tonga.

In the framework of the World Bank supported project "Cyber Security Consultancy Services for Developing and Supporting Information Systems", in September 2021 the cybersecurity capacity-building and training needs for Tonga were also collected through surveys (see the project's deliverable 'Cybersecurity audit and risk assessment'). The result was that **training and awareness raising** can help to address 18 modelled risks scenarios, which correspond to 34 unique threats. Furthermore, the survey revealed that Tongan MDAs as well as the general public (including the educators) have a suitable number of training opportunities and cybersecurity related curricula at their disposal to enhance (cyber)security incident management and response. However, there are also shortcomings that prevent them from fully taking advantage of the available opportunities as well as further building up their existing skills. Among these are:

- Cybersecurity curricula exist only for classes 9-13 and do not exist for the youth (early primary, middle primary and secondary levels should be improved) or for the more mature population (continuing education)
- Remote studies are not available to the population in more remote areas due to connectivity issues
- Often resources such as teachers or classes are missing – but even where these resources can be found, organisers struggle with low turnout
- Public service employees from different ministries are used to working in silos. Cooperation, especially on matter of information security remains sparse.

At the same time, some of the opportunities were identified in the area of skills. For instance, the issue of turnout and logistics of training courses can be addressed with remote studies. In addition, the non-governmental sector often steps in where governmental resources are not sufficient (e.g. church, donors).

Inclusion of cybersecurity topics in the national ICT **curricula** in all educational institutions across **primary, secondary and tertiary levels** should be the goal. The Government of Tonga should support the establishment of specialised training facilities such as laboratories and develop appropriate training materials that enable to conduct practical training courses. Allocation of additional resources to **train the trainers** is necessary. Dedicated programs should be introduced to teach the teachers at schools and lecturers at universities.

Actions:

1. Continue awareness building
2. Incorporate digital literacy skills development into all educational programs
3. Allocate additional resources to train the trainers

3.5. Active and reliable partner of the international community

Tonga relies heavily on international organisations for capacity building, sponsorship and mutual assistance. **Strengthening international cooperation** enables to benefit of formal cooperation (e.g. Mutual Legal Assistance) and informal cooperation (e.g. information sharing between CERTs but also between law enforcement authorities in neighbouring countries).

Oganisations like FIRST and Asia Pacific Computer Emergency Response Team's (APCERT) aim to maintain a trusted contact network of computer security experts to improve the region's awareness and competency related to computer security incidents. CERT Tonga under the Ministry of MEIDECC was the first from the Pacific Islands region to become an Operational Member of APCERT. The capacity building through APCERT includes:

- Jointly developing measures to deal with large-scale or regional network security incidents
- Facilitating information sharing and technology exchange, including information security, computer virus and malicious code among its members
- Promoting collaborative research and development on subjects of interest to its members
- Assisting other CERTs in the region to conduct efficient and effective computer emergency response.

International networks include organisations such as Interpol and G7. Tonga also takes part in the GLACY+ Project that is a joint initiative of the European Union and the Council of Europe, aimed at strengthening the global response to cybercrime and the challenges posed by electronic evidence. This project supports Tongan authorities in their legislation harmonization and capacity building initiatives. Tonga MDAs represent the country also in the Pacific Islands Law Officers' Network (PILON) Cybercrime and Sexual and Gender Based Violence (SGBV) Working Groups, in the Pacific Cyber Security Operational Network (PaCSON) and other thematic working groups.

Actions:

1. Increase both bi-lateral and multilateral dialogues and continue networking with other countries to enter into partnership agreements.
2. Continue the capacity and confidence building through international collaboration

3.6. Provide an enabling cybersecurity governance framework

Common cybersecurity governance framework is a key element in achieving the desired state of cybersecurity in Tonga. Such framework comprises of four vital elements that are described below.

First element is a clear establishment of cybersecurity roles and responsibilities of each and every stakeholder in Tongan cybersecurity ecosystem. The evolvement of the cybersecurity governance framework includes reviewing of cybersecurity roles and responsibilities amongst public and private sector stakeholders. Furthermore, commitment of executive management is enhanced regarding cybersecurity plans, activities and decisions.

Second element is an effective national cooperation between the cybersecurity stakeholders. This element includes cross-agency information sharing (including threat information sharing platform) and setting common cybersecurity goals. Established cybersafety, cybersecurity and cybercrime working groups dedicated to raise awareness, build the community and conduct training in their own areas is a good example of inter-agency cooperation in cybersecurity.

Third element of the cybersecurity governance framework are **common initiatives and projects**. Initiatives like Secure Government Cloud and Secure Government Network help to centralise services to competent authorities, thus making the securing of services more efficient.

Fourth element considers principles, policies, directives, and other common cybersecurity guidance that should be in place to implement and govern cybersecurity. The current state of written and management approved policies and other guidance documents will be approved. To make the development of such **guidance documents** more efficient, common templates are developed to align cybersecurity principles at different stakeholders.

Actions:

1. Review and clarify cybersecurity roles and responsibilities among public and private sector stakeholders
2. Enhance cybersecurity cooperation between national stakeholders
3. Promote common cybersecurity initiatives and projects
4. Develop common templates for cybersecurity related policies and guidance documents.

4. Implementation Plan

Strategic Action	Activity	Output /KPI	Lead Agency	Supporting institutions	Priority
1. Implement a Safe Digital Governance					
Develop and adopt Cybersecurity Manual for Tongan government agencies	Cybersecurity Manual for Tongan government agencies should be developed and adopted. The manual will serve as a basis for the Digital Government Security Standard to be and enables to ensure the confidentiality, integrity and availability of data and services of Tonga Government authorities.	Cybersecurity Manual is developed and adopted	MEIDECC		
Upgrade of Civil Registration and National Identity systems	Tonga shall establish a unique persistent identier for its citizens and residents that can be used as an authentication base for the provision of public services. The provision of legal identity for all is the key to enable safe and secure access to basic services.	Unique identifier that is a precondition for the provision of online services	Ministry of Justice	MEIDECC	
Transition of all MDAs to Secure Government Network (SGN)	All agencies which create and analyze data, refer to data and information, or use data for decision making must be connected to the Secure Government Network (SGN).	% of MDAs connected to SGN	MEIDECC		
Implement Data Center Consolidation Program and Tongan Government Cloud Computing Transition	Government of Tonga needs to carry out the analysis and selection of information systems to be reorganised and migrated to the Data Center. New systems should be deployed only on Government Cloud. Existing systems should be ranked first based on their criticality and dependence on external IT services and then migrated based on ranking. Government of Tonga monitors the Data Center and prepares disaster recovery plans.	Mapping of the system to be migrated. A detailed migration plan with order of steps and dates has been created. ICT systems hosted in the Data Center and Government Cloud are under constant monitoring.	MEIDECC	TCC	

2. Risk management					
Identification of threats and vulnerabilities	Identify and understand potential threats (threat intelligence) and the risks associated with these threats (risk awareness) of public sector information systems and critical IT infrastructure. This activity is required to be performed prior to conducting risk assessments in each MDA. Update of the scenarios of national cybersecurity risk register is regular	The national cybersecurity risk register is regularly updated	MEIDECC		
Perform regular risk assessments in public organizations and critical private enterprises	Introduce the procedure of regular risk assessment in every public organization and critical private enterprises. The assessment findings are recorded in a format of a combined security risk register. Pilots in ministries are conducted and based on the pilots risk assessment guidelines delivered to MDAs. Training courses to all MDAs are conducted.	Pilots in ministries are conducted and based on the pilots risk assessment guidelines are delivered to MDAs. Regular cybersecurity risk assessments are carried out by MDAs.	MEIDECC All MDAs		
Prepare risk mitigation and disaster recovery plans	After risk assessments have been performed, it is followed by the preparation of risk mitigation and disaster recovery plans for Tongan MDAs and critical public organisations.	Risk mitigation and disaster recovery plans are prepared by all MDAs	All MDAs		
3. Threat preparedness and incident response					
Define the incident management process for MDAs	Defining the incident management process is improved in MDAs to recover quickly and avoid serious consequences. The description of the process shall include the responsibilities of stakeholders involved.	Incident management process is defined in every MDA	All MDAs		
Introduce the requirement for reporting incidents for MDAs	Government of Tonga introduces the requirement for reporting incidents to create the picture of threats and vulnerabilities of Tonga cyberspace.	The requirement to report cybersecurity incidents is established	MEIDECC		
Enhance public-	Promote the reporting of incidents among private	Cybersecurity	MEIDECC		

private partnership in fighting cybercrime and promote the reporting of incidents	companies.	incidents are reported by private companies			
Enhance the investigation and forensic capability of CERT Tonga	Increase the resources of CERT Tonga and their ability to carry out the analysis digital evidence and investigation and digital forensics. Law enforcement agencies and CERT Tonga continue to be a part of different capacity building training courses and fora in the region and internationally.	CERT Tonga is equipped and trained to carry out analysis of digital evidence	Tonga Police MEIDECC (CERT Tonga) Attorney General's Office		
Develop standardized procedures of electronic evidence management both for Tonga Police and CERT Tonga.	Law enforcement agencies to develop standardized procedures of electronic evidence management following the concept of the 'chain of custody', which is fundamental to ensuring the integrity of evidence brought before the courts.	Digital evidence is collected based on the International best practice.	Tonga Police MEIDECC (CERT Tonga) Attorney General's Office		
4. Enhanced skills					
Continue awareness building	As most of the population is using mobile and smart devices for social media purposes, courses and awareness campaigns on the safety on social media should be continuously provided. The awareness campaigns should be focused not only to MDAs but also to children and young people including their parents as well.	Awareness raising events and cyberhygience courses are carried out continuously	MEIDECC (CERT Tonga) Ministry of Education and Training		

Incorporate digital literacy skills development into all educational programs	Incorporate digital literacy skills development into all educational programs, establishing basic levels of digital literacy needed for school graduates to successfully enter the workforce.	Enhanced cybersecurity curriculum is rolled out	Ministry of Education and Training		
Allocate additional resources to train the trainers	To provide good training courses, the focus should be on training the trainers. Dedicated programs should be introduced to teach the teachers at schools and lecturers at universities. Additionally, the Government of Tonga should support cybersecurity classes for the unemployed and people interested in changing the profession as part of continuing education.	Specialized courses on cybersecurity trainers are provided. Government supports professional certification schemas.	Ministry of Education and Training MEIDECC		
5. Active and reliable partner of the international community					
Increase bilateral and multilateral dialogues and continue networking with other countries to enter into partnership agreements.	Continue networking with other countries and enter partnership agreements. International collaboration aims to strengthen cyber-capacity and expertise in Tonga for the government, businesses, as well as for community. Participate in international cybersecurity exercises to improve information exchange and competency in relation to resolving computer security incidents.	Increased and improved partnerships. Number of regional and international organizations that Tonga is a member of or partners in.	MEIDECC		
Continue capacity and confidence building through international collaboration	International collaboration aims to strengthen cyber-capacity and expertise in Tonga for the government, businesses, as well as for community. Law Enforcement Agencies and CERT Tonga continue to be a part of different capacity building training courses and fora in the region and internationally.	Enhanced international collaborations on cybersecurity, and improved participation of relevant national stakeholders in cybersecurity programs and	Tonga Police MEIDECC (CERT Tonga) Attorney General Office		

		initiatives in the wider global arena. Improved access to technical support and outreach.			
6. Provide an enabling governance framework					
Review and clarify roles and responsibilities	Review and clarify cybersecurity roles and responsibilities amongst public and private sector stakeholders.	Roles and duties of government agencies and critical private sector companies concerning the enhancement of cybersecurity in Tonga are transparent and supervised	MEIDECC		
Enhance cooperation in cybersecurity	Enhance cooperation in cybersecurity between national stakeholders, including cross-agency information sharing (including threat information sharing platform) and setting common cybersecurity goals.	Appropriate information sharing mechanisms are established	MEIDECC		
Promote common cybersecurity initiatives and projects	Promote common cybersecurity initiatives and projects, e.g. Secure Government Cloud and Secure Government Network	% of MDAs connected to SGN Number of information systems on Secure Government Cloud	MEIDECC		
Develop common templates for cybersecurity related policies and guidance documents	The current state of written and management approved policies and other guidance documents will be approved by developing common templates to align cybersecurity principles at different stakeholders.	Templates for common cybersecurity guidance documents are available to all MDAs	MEIDECC		