CYBERSECURITY CAPACITY REVIEW

Independent State of Samoa

July 2018

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

DEPARTMENT OF COMPUTER SCIENCE

OCSC Oceania Cyber Security Centre

ITU

CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers: Dr Eva Nagyfejeo, Dr James Boorman, Dr Jeb Webb

Reviewed by: Professor Sadie Creese, Professor William Dutton, Professor Michael Goldsmith, Associate Professor Carsten Rudolph, Professor Basie Von Solms

Approved by: Professor Michael Goldsmith

Version	*Date*	*Notes*
1	*1 June 2018*	*First draft to Technical Board*
2	*3 July 2018*	*Second draft to ITU*
3	*17 July 2018*	*Third draft to ITU and MCIT*

LIST OF ABBREVIATIONS

ADB	Asian Development Bank
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CNSS	Committee on National Security Systems
CSL	Computer Services Limited
DNS	Domain Name System
HIDS	Host Intrusion Detection Systems
ICT	Information Communications Technology
IPS	Intrusion Prevention System
ISPs	Internet Service Providers
IT	Information Technology
ITU	International Telecommunication Union
MCIT	Ministry of Communications and Information Technology
NIDS	Network Intrusion Detection Systems
OOTR	Office of the Regulator
PaCSON	Pacific Cyber Security Operational Network
SAS-ASH	Samoa American Samoa - American Samoa Hawaii cable
SPF	Sender Policy Framework
SSCC	Samoa Submarine Cable Company
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security

EXECUTIVE SUMMARY

In collaboration with the International Telecommunication Union (ITU), the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') together with its regional partner, the Oceania Cyber Security Centre (OCSC) undertook a review of the maturity of cybersecurity capacity in the Independent State of Samoa at the invitation of the Ministry of Communications and Information Technology (MCIT). The objective of this review was to enable the government of Samoa to benchmark national cybersecurity capacity and set priorities for strategic investment and capacity development.

Over the period 18-20 April 2018, the following stakeholders participated in roundtable consultations: academia, criminal justice, law enforcement, information technology officers and representatives from public-sector entities, critical-infrastructure owners, policy makers, information-technology officers from the government and the private sector (including financial institutions), the banking sector, as well as international partners.

The consultations took place using the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five *dimensions* of cybersecurity capacity:

- Cybersecurity Policy and Strategy
- Cyber Culture and Society
- Cybersecurity Education, Training and Skills
- Legal and Regulatory Frameworks
- Standards, Organisations, and Technologies

Each dimension comprises *factors* which describe what it means to possess cybersecurity capacity. Factors present a number of *aspects* and for each aspect there are *indicators*, which describe steps and actions that, once observed, define the state of maturity of that aspect. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations. For more details on the definitions, please consult the CMM document.[1]

Figure 1 below provides an overall representation of the cybersecurity capacity in Samoa and illustrates the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' is placed at the perimeter.

[1] Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition (assessed 25 February 2018)

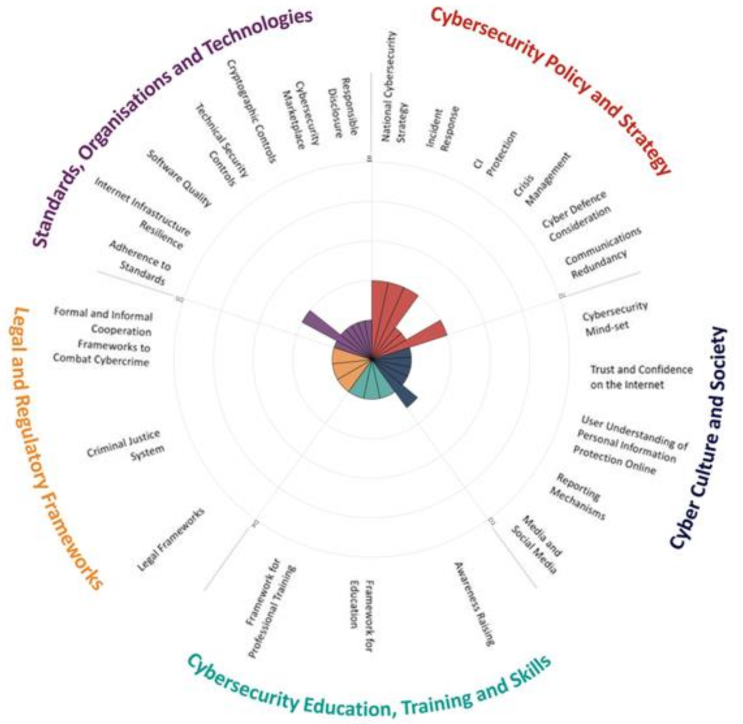

Figure 1: Overall representation of the cybersecurity capacity in Samoa

The following CMM report provides a detailed description of findings and recommendations regarding the research team's understanding of the current situation in Samoa, providing guidance on how to drive maturity against CMM indicators in all five dimensions as detailed in each section.

To highlight the recommendations seen as critical for Samoa to consider, key findings and key recommendations for each dimension have been selected using the research team's professional judgement as summarised below.

Cybersecurity Policy and Strategy

Samoa has published a national cybersecurity strategy, though the specifics of the process leading up to the production of this strategy document remain unclear.

Samoa's national cybersecurity organisation is currently in its formative stages, although the MCIT has reported that significant progress toward the development of a national cybersecurity programme has been made to date. Statements from MCIT participants and others suggested that MCIT is the recognised coordinating body for the nation's cybersecurity policy. The MCIT has been given the mandate to consult across public and private sectors, as well as with civil society.

The content of the national cybersecurity strategy does provide some linkage between cybersecurity, national risk priorities and business development within the nation, but this is at a high level of abstraction and lacking in specific detail regarding the risks, priorities, and objectives concerned. The strategy content technically fulfils one of the CMM's strategic-level maturity indicators in that it aims to protect critical infrastructure from internal threats, i.e. "…cyber-threats including but not limited to infrastructure impairment and criminal activities"[2], but participant comments strongly suggested that Samoa is not yet well placed to do this.

Samoa is currently in the process of developing a national incident-response capability. Most focus-group participants could think of ways in which incidents within their organisations could constitute national-level issues but, as yet, it appears that there is no register or catalogue of incidents that is centrally maintained by the Samoan government.

While it is virtually certain that some who have been involved with development of the cybersecurity strategy have defined the nation's critical infrastructure, some participant comments suggested that there might not be a complete and common understanding of which organisations are considered critical infrastructure and which are not. This may indicate that, if a list of general CI assets has been created, it may not have been widely distributed.

The Government of Samoa has recognised that crisis management is necessary for national security. However, there is no evidence of any cybersecurity dimension to national crisis management and participants were unaware of any crisis management plan that involves coordination on national cybersecurity incidents.

Much of the CMM assessment content pertaining to cyber-defence is not applicable to Samoa in any direct sense because Samoa does not have its own standing military.

There was no evidence and insufficient participant representation for the researchers to be able to establish the extent to which redundancy of critical systems has been achieved within Samoa's key organisations.

Key recommendations:

- Because cybersecurity is both a fundamental and a perennial concern, it is important that the cybersecurity programme remains a permanent dimension of governance and management throughout Samoa. The program needs robust legal backing, and technological development and security initiatives should be given their own budgets with equal priority given whatever funds are currently available. Samoa's international partners should provide the funding and resources required to make Samoa a strong link in the global information security chain.

[2] Government of Samoa 2016, Samoa National Cybersecurity Strategy 2016-2021, Ministry of Communications and Information Technology, Apia (Samoa). Available at: http://www.samoagovt.ws/wp-content/uploads/2017/02/MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021.pdf (accessed 22 May 2018).

- A mechanism for reporting detected cybersecurity incidents needs to be established, which all organisations considered key to national security are expected to use.

- Critical Infrastructure organisations should be tasked with mapping their business processes to understand organisational or personal information assets (types of information, people with kinds of knowledge, kinds of hardware to include personal devices, software, organisational or virtual processes, etc.). Consideration should be given to how these assets are vulnerable to different kinds of purposive or incidental threats that can result in negative consequences for the organisation or the nation as a whole. The information assets linked to the most serious consequences for the nation are ranked highest priority for protection, and so on down, depending on the funding and resources available. One potentially helpful discussion of information security from a business process perspective can be found in Nebauer, Klemen and Biffl (2006).[3]

Cyber Culture and Society

Overall, the cyber-ecosystem in Samoa is still in its very early stages. The review found that cybersecurity has not yet become a priority across the public and private sectors or among end-users. Focus-group discussions suggest that Samoa, like most other Pacific Island countries has a very low level of awareness of cybersecurity. A participant noted that people are less interested primarily due to the fact that cybersecurity is fairly new to the country, not widely used, and there is a general lack of knowledge about any national cyber-attacks or personal bad experiences with cyber-incidents.

Overall, the general cybersecurity awareness within government agencies remains still very low. Due to the limited representation of the private sector, it was difficult to determine or get a clear picture of the extent to which private entities recognise the need to prioritise a cybersecurity mind-set.

Most people in Samoa access the Internet via their mobile phones (not via desktop computers) and based on focus-group discussions, it seems to be quite common that most phone users have a nearly blind trust regarding what they see or receive online via their phones. Participants in our discussions believed that users are unaware of many risks and the required skills to use mobile Internet. Most users do not have the ability to critically assess content they see and receive online, nor the applications they use.

With e-government services in the very early stages of implementation, there is a need to build trust in order to move government agencies and citizens to online services. That said, the trust in online services offered by the government (e.g.: e-Tax system) is generally very low.

[3] Neubauer, T., Klemen, M. and Biffl, S., 2006, April. Secure business process management: a roadmap. In *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on* (pp. 8-pp). IEEE, viewed 23 May 2018, <http://www.academia.edu/download/5829469/pub-inf_3650.pdf>.

Online banking is the only form of e-commerce that is currently available, since Samoa is still very much a cash society and has a culture of face-to-face interaction this is unlikely to change significantly in the near future.

Participants noted that public awareness of the issues surrounding the protection of personal information and the relationships between privacy and security concerns regarding personal data is very low. Participants suggested that this is because Samoa does not have a tradition or legislation regarding privacy and data protection. As a consequence, mobile Internet users are not aware of the kinds of data they share with operators, nor do they know what is done with the information they do provide on popular social media channels such as Facebook or Twitter.

No central, dedicated reporting framework exists in Samoa for users to report computer-related or online incidents. Participants noted that people generally report online threats to the police in person (as opposed to initiating some process online).

Cybersecurity issues are reported in an ad-hoc manner in the media in Samoa, with insufficient coverage in mass media both online and offline. Traditional media seldom provide coverage on cybersecurity when compared to social media. Despite the popularity of social media via mobile phones, there is limited awareness raising and discussions for cybersecurity via the social media channels. One participant mentioned that allegedly school fights (cyber-enabled bullying) have been triggered by and discussed on social media.

Key recommendations:

- Develop and implement campaigns that promote the safe use of online services across the general public, enabling users to critically assess online content they consume social media or smart-phone applications.

- Consider educating the public (including High Chiefs (Matai), Chiefs of village councils and the Church) on the nature and consequences of cybercrime and cyberbullying.

- Establish coordinated mechanisms within the public and the private sectors that allows citizens to report cybercrime cases, including online fraud, cyber-bullying, child abuse online, identify theft, privacy and security breaches, and other incidents, in particular for women and other vulnerable groups.

Cybersecurity Education, Training and Skills

A national programme for cybersecurity awareness raising, led by a designated organisation (from any sector) which addresses a wide range of demographics is yet to be established. Due to the lack of a national awareness programme, cybersecurity awareness amongst the general public is low.

The awareness on cyberbullying and the protection of children online is driven by the Office of the Regulator, the Ministry of Police and the Attorney General's Office. Under the leadership of the MCIT and in partnership with the Ministry of Police, new provisions have been made for the government to move forward and re-introduce the Cyber Safety Pasifika awareness campaign.

Focus-group discussions suggest that awareness of cybersecurity issues is very limited among executive managers both in public and private sectors, which could be one of the reasons why cybersecurity awareness-raising has not yet been perceived as a priority. There are currently no efforts to raise the cybersecurity awareness of executive staff in any sector.

The need for enhancing cybersecurity education in schools and universities has been identified by leading government and academic stakeholders. The Samoa National Cybersecurity Strategy (2016-2021) under Goal 4 recognizes the need to enhance education and skills such as the 'development of School Curriculums concerning Computer Studies in the primary and secondary levels' and 'development of Tertiary level Computer Science Curriculum to include Cybersecurity measures'[4]. Overall, cybersecurity education only occurs as part of the curriculum for a more general computing and information systems program.

There is currently no formal cybersecurity education in place in Samoa. The country has very limited options for cybersecurity qualifications and there is a shortage of qualified cybersecurity educators to improve the situation. There are no elective or mandatory cybersecurity specific courses offered.

The need for training professionals in cybersecurity has been recognized by the government. The strategy statement of Goal 4 of the Samoa National Cybersecurity Strategy (2016-2021) seeks as part of the national cybersecurity capacity-building efforts to 'ensure that all relevant stakeholders including citizens, students, businesses, judiciary, and law enforcement receive sustainable trainings.'[5] However, focus-group discussions failed to confirm if any distinct budget to reach these goals exists.

No cybersecurity framework for certification and accreditation of public-sector professionals exists. Likewise, there are no vocational trainings and providers of ICT equipment (e.g.: CISCO academy) are the ones transferring instructions and information to staff in Samoa. Otherwise, there is no other level of education in this regard yet.

Key recommendations:

- Appoint a dedicated organisation (e.g.: National ICT Steering Committee) which has the mandate to develop and implement a national cybersecurity awareness-raising programme with initial target groups focusing on the most vulnerable users, such as children and women, based on international good practice. Coordinate and cooperate with key stakeholders, in particular including those who participated in the review, including the private sector, civil society and international partners. Some of the tasks of the organisation would be to:
    - Create a single online portal linking to appropriate cybersecurity information and disseminate materials for various target groups via the cybersecurity awareness programme and social media.
    - Develop a dedicated awareness-raising programme for executive managers within the public and private sectors as this group is usually the final arbiters on investment into security.

[4] Government of Samoa (2016)
[5] Government of Samoa (2016)

- Develop qualification programmes for cybersecurity educators and start building a cadre of existing and new professional educators to ensure that skilled staff is available to teach newly formed (and existing) cybersecurity courses.

- Establish regular mandatory training for IT employees and general employees regarding cybersecurity issues.

Legal and Regulatory Frameworks

Samoa currently lacks any cybersecurity-specific legislation, although several legal instruments touch upon cybersecurity-related activities. The government are aware of this issue and are currently working towards ratifying the Budapest Convention on Cybercrime, including thoroughly examining and re-evaluating domestic legislation in terms of what amendments or new cybersecurity related laws are required.

With regards to privacy, personal expression, and other human rights online there is no specific legislation in Samoa. However, these issues are dispersed under several legal instruments. While Samoa has not adopted specific legislation on human rights online, Article 13 of the Constitution of Samoa (1960) refers to the fundamental human-rights protection of freedom of speech and expression.

Concerning data protection, there is no overall national legislation or regulation that adequately addresses this aspect, as mentioned earlier. However, it is scattered under various legislations such as the Telecommunications Act (2005), the Statistics Act (2015), the Electoral Act (1963) and the National Provident Fund Act (1972).

The protection of children online is covered under the Crimes Act (2013) that provides the following provisions for the safeguard of children online: Section 82 ‘Publication, distribution or exhibition of indecent material on a child or on a child through an electronic system is an offence’ and Section 218 ‘makes it an offence for any person to carry out any act of solicitation of children’.

There is no comprehensive legal framework that regulates consumer protection online. With regards to intellectual property legislation, Samoa has a Copyright Act (1998) in place that is administered by the MCIT, however it is not applicable to online content.[6] Samoa is currently undergoing steps to amend its legal framework on cybercrime in line with the Budapest Convention on Cybercrime.

Overall, the legislative framework regulating cybersecurity and related topics is still in the start-up stage of development, as adopted or amended legislation does not cover all aspects of cybersecurity, such as: the protection of human rights online; data protection; consumer protection online; and digital evidence regulations. Legislation is not yet sufficiently enforced,

[6] Copyright Act (1998) Available at http://www.wipo.int/wipolex/en/details.jsp?id=5760 (accessed 16 May 2018)

despite Samoa being one of the most advanced in the region according to UNCTAD's Cyberlaw Tracker.[7]

Across the criminal justice system of Samoa, capacities are at start-up stages of development.

There is no single institution or special unit that deals with cybercrime issues, nor does Samoa have digital forensics capability or skills to handle digital evidence. Participants expressed several concerns that the law-enforcement community faces such as lack of facilities and tools to monitor cybercrime. Participants noted that the following issues with the current system: reliance on complaints to trigger investigations; lack of active search or identification of cyber-threats; and lack of an adequate level of training and certifications in many of the institutions which are needed to carry out prosecutions.

The authorities in Samoa have recognised the need to improve informal and formal cooperation mechanisms, both domestically and across borders, but they remain ad-hoc and are only in their very initial stages. The existing provisions under the Mutual Assistance in Criminal Matters Act (2007) facilitates international assistance in criminal matters and criminal investigations between Samoa and foreign states[8] however, the act does not consider cybercrime. There are no provisions that allow law enforcement to preserve computer data or traffic data on behalf of a foreign state in cybercrime investigations.

Key recommendations:

- Consider setting up a periodic process of reviewing and enhancing Samoa's laws relating to cyberspace to address the dynamics of cybersecurity threats (e.g.: hate speech online, cyber-bullying).

- Consider creating a National Cybercrime Laboratory under the auspices of the Ministry of Police in order to facilitate digital forensics. This will provide a platform to all law enforcement agencies to carry out cybercrime investigations.

- Consider establishing institutional capacity building programmes for judges, prosecutors and police personnel from security agencies to acquire new ICT skills needed for cybercrime investigations (for e.g.: digital evidence gathering) and effective ways of enforcing cyber-laws.

Standards, Organisations, and Technologies

Samoa has yet to adopt defined standards and good practices for information risk management for securing data, technology and infrastructure. However, the Government of Samoa is aware of this and has included establishing standards as a key goal in the National

[7] UNCTAD Cyberlaw Tracker: The case of Samoa. Available at http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/CountryDetail.aspx?country=ws (accessed 16 May 2018)

[8] Mutual Assistance in Criminal Matters Act (2007) Available at https://www.unodc.org/res/cld/document/wsm/2007/mutual_assistance_in_criminal_matters_act_2007_html/Samoa_Mutual_Assistance_in_Criminal_Matters_Act_2007.pdf (accessed 16 May 2018)

Cybersecurity Strategy: Goal 2: "*Establish relevant technical measures (Entities and Standards) to eliminate Cyber Threats and Attacks, enhance Cybersecurity and promote Cyber Safety*"[9]. As part of the implementation of the national strategy, the Ministry of Communications and Information Technology (MCIT) and the Office of the Regulator (OOTR) are leading the assessment and development of suitable cybersecurity standards.

There is no publicly available evidence or participant discussion to suggest that the public sector currently develop software. In terms of the private sector, no defined cybersecurity standards or good practices could be publicly identified in Samoa. The Government of Samoa does not currently provide guidance on standards or good practices to other sectors. Participants from both the private and public sectors noted that there is no specific cybersecurity standard in use locally in Samoa by any sector.

Samoa currently has two submarine cables as part of the country's Internet infrastructure to improve the bandwidth and availability (redundancy) of international Internet service: The Samoa American Samoa - American Samoa Hawaii (SAS-ASH) cable connecting Samoa to American Samoa and Hawaii; and the Tui-Samoa cable, connecting Samoa to Fiji[10].

Participants noted that the resiliency of the Internet infrastructure (in terms of redundancy) is seen to be provided to the country via the combination of the two submarine cables and the Internet services that rely on satellite based infrastructure. Participants noted that, in the private sector, some organisations obtain redundancy of Internet service via the use of multiple ISPs, or by mixing both mobile and fixed line technology from the same ISP.

The Samoa National Broadband Policy 2012 outlines the roadmap to increase the speed and affordability of Internet access and increase penetration in rural and urban areas, to 30% and 40% respectively by 2020[11]. Samoa is currently serviced by multiple ISPs for both domestic and business customers. When asked to consider the usability of Samoa's Internet infrastructure, a wide variety of participants across all sectors noted that their domestic services lack sufficient speed and have a high cost. When asked about their experiences for business use, participants had fewer speed complaints across both the private and public sectors, with these connections generally seen to be faster, but still costly. There are currently no publicly available Service Level Agreements (SLAs) from the ISPs for domestic or business use and no publicly available statistics on the frequency or cause of service outages.

The Government Internet and Email Policy 2016[12] requires the IT department in all government agencies to maintain lists of approved software and test new software for compatibility with their environment. However, there is no identified centrally managed catalogue of secure software platforms and applications or process for monitoring software quality across agencies. The public sector does not use a common operating environment,

[9] Government of Samoa (2016), p8.
[10] Telegeography. (2018) 'Submarine cable map 2018'. Available at: http://submarine-cable-map-2018.telegeography.com/ (Accessed 14 May 2018).
[11] MCIT. 2012 ''. Available from: http://www.mcit.gov.ws/images/mcit/POLICY%20Samoa%20National%20Broadband%20Policy%202012%20_approved_.pdf (Accessed 23 May 2018).
[12] MCIT. (2016) 'Government Internet & Email Policy 2016'. Available at: http://www.mcit.gov.ws/publications/134-government-internet-email-policy-2016 (Accessed 14 May 2018).

agencies decide which operating systems and applications to run across their chosen end user and server environments.

The Government Internet and Email Policy 2016 from the MCIT provides guidance on mandatory minimal security requirements for all government agencies. In terms of technical controls, the policy covers the requirement for all agencies to have perimeter firewall, web content filtering and antivirus controls. However, the policy does not cover additional controls and there is no supporting guidance on selecting suitable products, secure configuration or deployment. There is no evidence of wider promotion of the use of technical security controls, nor incentives being offered to any sector for the use of up-to-date security controls. There is no evidence that ISPs are offering upstream controls or antimalware software as part of their services.

Samoa does not currently have defined standards or good practice guidance for cryptographic controls for protecting data at rest or in transit. Participants noted that in the public sector initial work is underway to deploy certificates as controls for protecting web traffic in transit across all government websites, but this is not currently reflected in policy. In terms of the private sector, participants noted that certificates are deployed across the finance sector for protecting web traffic in transit only.

Participants from the public and private sectors noted that Samoa does not currently produce cybersecurity technologies, but relies on international offerings.

Samoa does not currently have a responsible disclosure policy. The need for a responsible disclosure policy was not acknowledged by participants from any sector. When asked about how users can report bugs and vulnerabilities to service providers, participants noted that currently local service providers do not have a mechanism in place.

Key recommendations:

- Adopt a nationally agreed baseline of cybersecurity related standards and good practices that address identified risks across the public and private sectors, including: risk management and information risk management; managing Internet infrastructure; software development; procurement; ecommerce; electronic business transactions; and authentication.

- Identify and describe all ICT assets in use by the public sector and critical infrastructure to inform risk assessments. This should include, but not be limited to: applications; platforms (environment in which applications are executed); and how information is exchanged and stored.

- Revise the technical security control framework based on regular risk assessments that include the assessment of the effectiveness of controls, informed by the National CIRT and penetration tests where possible.

INTRODUCTION

At the invitation of Ministry of Communications and Information Technology (MCIT), and in collaboration with International Telecommunication Union (ITU), the Global Cyber Security Capacity Centre (GCSCC) together with its regional partner, the Oceania Cyber Security Centre (OCSC) have conducted a review of the cybersecurity capacity of the Independent State of Samoa. The objective of this review was to enable the Government to gain an understanding of its cybersecurity capacity in order to strategically prioritise investment in cybersecurity capacities.

Over the period 18-20 April 2018, stakeholders from the following sectors participated in a three-day consultation process:

Commented [E1]: @Tala: please provide info from participants list. Need to be updated.

- Public-sector entities
    - Ministry of Education, Sports & Culture
    - Samoa Qualifications Authority (?)
    - Department of Foreign Affairs & Trade
    - National Health Services
    - Ministry of Health
    - Ministry of Police
    - Ministry of Public Enterprises
    - Ministry of Agriculture & Fisheries
    - Samoa National Kidney Foundation (?)
    - Ministry of Public Enterprises
    - Ministry of Agriculture & Fisheries
    - Public Service Commission
    - Ministry of Commerce, Industry & Labour
    - Ministry of Communications & Information Technology
    - Ministry for Revenue
    - Ministry of Finance
    - Samoa International Finance Authority (?)
    - Office of the Regulator (?)
- Criminal-justice sector
    - Attorney General's Office
    - Office of the Electoral Commission
- Finance sector
    - Bank of the South Pacific
    - Samoa Commercial Bank
    - FEXCO Samoa
- Critical-infrastructure owners
    - Samoa Water Authority
    - NetVO Samoa

- Academia
    - National University of Samoa

- International community
    - United States Embassy
    - NZ High Commission
    - UNDP
    - Australia High Commission
    - Food & Agriculture Organisation

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were based on the GCSCC Cybersecurity Capacity Maturity Model (CMM)[13] which is composed of five distinct *dimensions* of cybersecurity capacity.

Each dimension consists of a set of factors, which describe and define what it means to possess cybersecurity capacity therein. The table below shows the five dimensions with the five dimensions together with the factors of which they are comprised:

DIMENSIONS	FACTORS
Dimension 1 **Cybersecurity Policy and Strategy**	D1.1 National Cybersecurity Strategy D1.2 Incident Response D1.3 Critical Infrastructure (CI) Protection D1.4 Crisis Management D1.5 Cyber Defence D1.6 Communications Redundancy
Dimension 2 **Cyber Culture and Society**	D2.1 Cybersecurity Mind-set D2.2 Trust and Confidence on the Internet D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Social Media
Dimension 3 **Cybersecurity Education, Training and Skills**	D3.1 Awareness Raising D3.2 Framework for Education D3.3 Framework for Professional Training
Dimension 4 **Legal and Regulatory Frameworks**	D4.1 Legal Frameworks D4.2 Criminal Justice System D4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime
Dimension 5 **Standards, Organisations, and Technologies**	D5.1 Adherence to Standards D5.2 Internet Infrastructure Resilience D5.3 Software Quality D5.4 Technical Security Controls D5.5 Cryptographic Controls D5.6 Cybersecurity Marketplace D5.7 Responsible Disclosure

[13] Global Cyber Security Capacity Centre, Cybersecurity Capacity Maturity Model for Nations (CMM) https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition (accessed 24 May 2018)

STAGES OF CYBERSECURITY CAPACITY MATURITY

Each dimension comprises factors which describe what it means to possess cybersecurity capacity. Factors present a number of aspects and for each aspect there are indicators, which describe steps and actions that once observed define which state of maturity this specific element of aspect is. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to dynamically adapt or change against environmental considerations. The five stages are defined as follows:

- **Start-up:** at this stage either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There is an absence of observable evidence of cybersecurity capacity at this stage.
- **Formative:** some aspects have begun to grow and be formulated, but may be ad-hoc, disorganised, poorly defined – or simply new However, evidence of this aspect can be clearly demonstrated.
- **Established:** the indicators of the aspect are in place, and functioning. However, there is not well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in this aspect. But the aspect is functional and defined.
- **Strategic:** at this stage, choices have been made about which indicators of the aspect are important, and which are less important for the particular organisation or state. The strategic stage reflects the fact that these choices have been made, conditional upon the state's or organisation's particular circumstances.
- **Dynamic:** At this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technological sophistication of the threat environment, global conflict or a significant change in one area of concern (e.g. cybercrime or privacy). Dynamic organisations have developed methods for changing strategies in-stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

The assignment of maturity stages is based upon the evidence collected, including the general or average view of accounts presented by stakeholders, desktop research conducted and the professional judgement of research staff. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of Samoa and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

METHODOLOGY - MEASURING MATURITY

During the country review specific dimensions are discussed with the relevant group of stakeholders. Each stakeholder cluster is expected to respond to one or two dimensions of the CMM, depending on their expertise. For example, Academia, Civil Society and Internet-Governance groups would all be invited to discuss both Dimension 2 and Dimension 3 of the CMM.

In order to determine the level of maturity, each aspect has a set of indicators corresponding to all five stages of maturity. In order for the stakeholders to provide evidence on how many indicators have been implemented by a nation and to determine the maturity level of every aspect of the model, a consensus method is used to drive the discussions within sessions. During focus groups, researchers use semi-structured questions to guide discussions around indicators. During these discussions stakeholders should be able to provide or indicate evidence regarding the implementation of indicators, so that subjective responses are minimised. If evidence cannot be provided for all of the indicators at one stage, then that nation has not yet reached that stage of maturity.

The CMM uses a focus-group methodology since it offers a richer set of data compared to other qualitative approaches.[14] Like interviews, focus groups are an interactive methodology with the advantage that during the process of collecting data and information diverse viewpoints and conceptions can emerge. It is a fundamental part of the method that rather than posing questions to every interviewee, the researcher(s) should facilitate a discussion between the participants, encouraging them to adopt, defend or criticise different perspectives.[15] It is this interaction and tension that offers advantage over other methodologies, making it possible for a level of consensus to be reached among participants and for a better understanding of cybersecurity practices and capacities to be obtained.[16]

With the prior consent of participants, all sessions are recorded and transcribed. Content analysis – a systematic research methodology used to analyse qualitative data – is applied to the data generated by focus groups.[17] The purpose of content analysis is to design “replicable and valid inferences from texts to the context of their use”.[18]

There are three approaches to content analysis. The first is the inductive approach which is based on “open coding”, meaning that the categories or themes are freely created by the researcher. In open coding, headings and notes are written in the transcripts while reading them and different categories are created to include similar notes that capture the same

[14] Relevant publications:
Williams, M. (2003).Making sense of social research. London: Sage Publications Ltd. doi: 10.4135/9781849209434
Knodel, J. (1993). The design and analysis of focus group studies: a practical approach. In Morgan, D. L. SAGE Focus Editions: Successful focus groups: Advancing the state of the art (pp. 35-50). Thousand Oaks, CA: SAGE Publications Ltd. doi: 10.4135/9781483349008
Krueger, R.A. and Casey, M.A. (2009). Focus groups: A practical guide for applied research. London: Sage Publications LTD.

[15] Relevant publications:
J. Kitzinger. ‘The methodology of focus groups: the importance of interaction between research participants.’ Sociology of Health & Illness, 16(1):103–121, 1994.
J. Kitzinger. ‘Qualitative research: introducing focus groups’. British Medical Journal, 311(7000):299– 302, 1995.
E.F. Fern. ‘The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality.’ Journal of Marketing Research, Vol. 19, No. 1, pages 1–13, 1982.

[16] J. Kitzinger. ‘Qualitative research: introducing focus groups’. British Medical Journal, 311(7000):299– 302, 1995.

[17] K. Krippendorff. Content analysis: An introduction to its methodology. Sage Publications, Inc, 2004. H.F. Hsieh and S.E. Shannon. ‘Three approaches to qualitative content analysis.’ Qualitative Health Research, 15(9):1277–1288, 2005.
K.A. Neuendorf. The content analysis guidebook. Sage Publications, Inc, 2002.

[18] E.F. Fern. ‘The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality.’ Journal of Marketing Research, Vol. 19, No. 1, Volume and Number? pages 1–13, 1982.

aspect of the phenomenon under study.[19] The process is repeated and the notes and headings are read again. The next step is to classify the categories into groups. The aim is to merge possible categories that share the same meaning.[20] Dey explains that this process categorises data as "belonging together".[21]

The second approach is deductive content analysis which requires the prior existence of a theory to underpin the classification process. This approach is more structured than the inductive method and the initial coding is shaped by the key features and variables of the theoretical framework.

In the process of coding, excerpts are ascribed to categories and the findings are dictated by the theory or by prior research. However, there could be novel categories that may contradict or enrich a specific theory. Therefore, if deductive approaches are followed strictly these novel categories that offer a refined perspective may be neglected. This is the reason why the GCSCC research team opts for a blended approach in the analysis of our data, which is a mixture of deductive and inductive approaches.

After conducting a country review, the data collected during consultations with stakeholders and the notes taken during the sessions are used to define the stages of maturity for each factor of the CMM. The GCSCC adopts a blended approach to analyse focus-group data and use the indicators of the CMM as our criteria for a deductive analysis. Excerpts that do not fit into themes are further analysed to identify additional issues that participants might have raised or to tailor our recommendations.

In several cases while drafting a report, desk research is necessary in order to validate and verify the results. For example, stakeholders might not be always aware of recent developments in their country, such as whether the country has signed a convention on personal data protection. The sources that can provide further information can be the official government or ministry websites, annual reports of international organisations, university websites, etc.

For each dimension, recommendations are provided for the next steps to be taken for the country to enhance its capacity. If a country's capacity for a certain aspect is at a formative stage of maturity then by looking at the CMM the indicators which will help the country move to the next stage can be easily identified. Recommendations might also arise from discussions with and between stakeholders.

Using the GCSCC CMM methodology, this report presents results of the cybersecurity capacity review of Samoa and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

[19] S. Elo and H. Kyng¨as. 'The qualitative content analysis process.' Journal of Advanced Nursing, 62(1):107–115, 2008.
H.F. Hsieh and S.E. Shannon. 'Three approaches to qualitative content analysis.' Qualitative Health Research, 15(9):1277–1288, 2005.

[20] P.D. Barbara Downe-Wamboldt RN. 'Content analysis: method, applications, and issues.' Health Care for Women International, 13(3):313–321, 1992.

[21] I. Dey. Qualitative data analysis: A user-friendly guide for social scientists. London: Routledge, 1993.

CYBERSECURITY CONTEXT IN SAMOA

In 2017, the ITU ICT Development Index ranked Samoa as the 127th economy in terms of access and use of ICT and ICT skills.[22,23] Mobile phone subscribers accounted for 69.19% of the population compared with 3.7% with fixed line phones in 2017, but not all these subscribers had access to the Internet.[24] In 2017, 29.1% of households had access to the Internet, with mobile broadband as the main method of access.[25]

Focus-group participants noted that domestic Internet services currently lack sufficient speed and come at a high cost. However, the government of Samoa is working to improve this and realise the economic, social and potential environmental benefits of continuing to develop the Internet infrastructure of the country, through the Samoa National Broadband Policy 2012[26]. Targets include improving Internet access speed, affordability and penetration in rural and urban areas to 30% and 40% respectively by 2020.[27] The newly completed Tui-Samoa cable, connecting Samoa to Fiji aims to reduce the costs of Internet access and provide a needed boost in speed for accessing content outside Samoa.[28,29] The recently announced Manatua cable that will link "*Tahiti, Cook Islands and Niue and possibly Tonga to Samoa*"[30], with construction due to be completed by early 2019[31], may open up opportunities for Samoa to become digital hub in the region.

[22] ITU. 2017. 'ICT Development Index 2017', Available at: http://www.itu.int/net4/ITU-D/idi/2017/#idi2017economycard-tab&WSM (Accessed 23 May 2018).
[23] ITU. 2018 'The ICT Development Index (IDI): conceptual framework and methodology'. Available from: https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017/methodology.aspx (Accessed 23 May 2018).
[24] ITU 2017.
[25] ITU 2017
[26] MCIT. 2012 'Samoa National Broadband Policy 2012'. Available from: http://www.mcit.gov.ws/images/mcit/POLICY%20Samoa%20National%20Broadband%20Policy%202012%20_approved_.pdf (Accessed 23 May 2018).
[27] MCIT. 2012.
[28] Telegeography. (2018) 'Submarine cable map 2018'. Available at: http://submarine-cable-map-2018.telegeography.com/ (Accessed 14 May 2018).
[29] The World Bank. (2017) 'Samoa to Have Faster, Cheaper Internet as Submarine Cable Project Starts in Savai'I'. Available at: http://www.worldbank.org/en/news/press-release/2017/02/24/samoa-to-have-faster-cheaper-internet-as-submarine-cable-project-starts-in-savaii (Accessed 14 May 2018).
[30] Samoa Observer. (2018) 'Work for $5m Cable Depot begins'. Available at: http://www.samoaobserver.ws/en/01_03_2018/local/30590/Work-for-$5m-Cable-Depot-begins.htm (Accessed 14 May 2018).
[31] Cook Island News. (2018) 'Manatua cable project set to start'. Available at http://www.cookislandsnews.com/item/67313-manatua-cable-project-set-to-start (Accessed 14 May 2018).

Focus-group participants noted that social media and messaging are the main use of the Internet in Samoa. Facebook (49.79%) and Pinterest (29.05%) have continued to be the main social media platforms used by Samoans from April 2017 to April 2018, with an increasing interest in YouTube (11.62%).[32]

Focus-group participants noted that the use of the Internet for e-commerce in Samoa is low and focused on overseas suppliers. According to The Pacific Financial Inclusion Programme, in 2016, 49% of Samoans did not use any formal financial system, with only 39% of the population having a bank account.[33] Participants theorised that given the low use of banks, the use of e-commerce is unlikely to increase significantly in the near future.

Cybersecurity is firmly on the agenda in Samoa with the release of the National Cybersecurity Strategy 2016-2021. The strategy takes a multidimensional approach and aims to '*strengthen existing cyber systems and critical infrastructure sectors, support economic growth and protect the public*'[34] through:

- defining organisation roles and responsibilities for cybersecurity;
- adopting technical standards;
- establishing a National Computer Incident Response Team (CIRT);
- revising existing and introducing new legislation;
- building capacity through training and awareness; and
- strengthening local and regional cooperation

The Government of Samoa's commitment to strengthening cybersecurity is further underlined by the recent announcement that the CEO of MCIT has been elected as Chairman Elect of the Pacific Cyber Security Operational Network (PaCSON) Executive Committee[35].

[32] Statcounter. 2018. Available at: http://gs.statcounter.com/social-media-stats/all/samoa (Accessed 23 May 2018)

[33] Pacific Financial Inclusion Programme. 2016 'Financial Services Sector Assessment for Samoa'. Available at: https://www.cbs.gov.ws/index.php/dmsdocument/5408 (Accessed 23 May 2018).

[34] Government of Samoa. (2016) 'MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021'. Available at: http://www.samoagovt.ws/wp-content/uploads/2017/02/MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021.pdf (Accessed 14 May 2018), p2.

[35] Samoa Observer. (2018) 'Samoa to Chair for Pacific Cyber Security Operational Network'. Available at: http://www.samoaobserver.ws/en/17_05_2018/local/33192/Samoa-to-Chair-for-Pacific-Cyber-Security-Operational-Network.htm (Accessed 18 May 2018).

REVIEW REPORT

OVERVIEW

In this section, we provide an overall representation of the cybersecurity capacity in Samoa. Figure 2 below presents the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' at the perimeter.

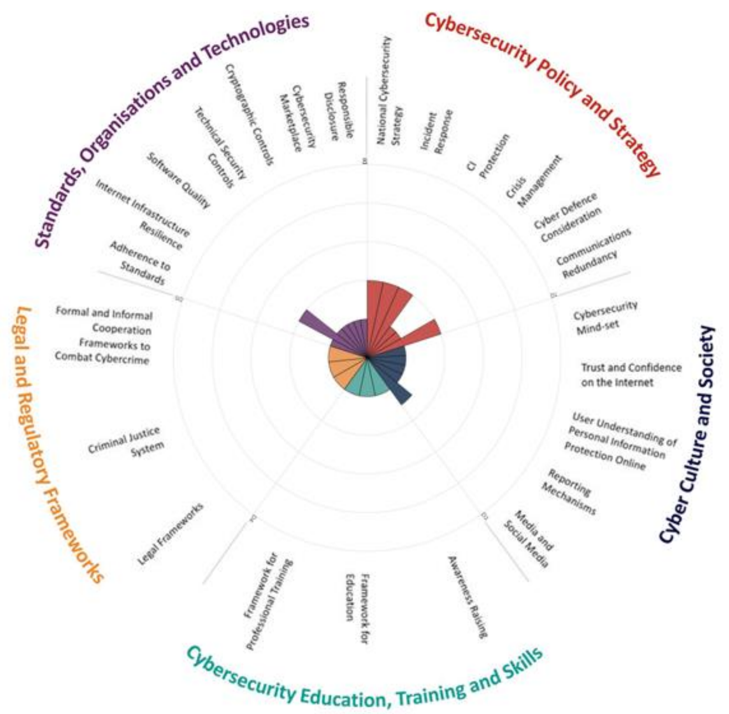

Figure 2: Overall representation of the cybersecurity capacity in Samoa

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

The factors in Dimension 1 gauge Samoa's capacity to develop and deliver cybersecurity policy and strategy and to enhance cybersecurity resilience through improvements in incident response, crisis management, redundancy, and critical infrastructure protection capacity. The Cybersecurity policy and strategy dimension also includes considerations for early warning, deterrence, defence and recovery. This dimension considers effective policy in advancing national cyber-defence and resilience capacity, while facilitating the effective access to cyberspace increasingly vital for government, international business and society in general.

D 1.1 NATIONAL CYBERSECURITY STRATEGY

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government, because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key government and non-governmental cybersecurity actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities

Stage: Formative

Samoa has published a national cybersecurity strategy, though the specifics of the process leading up to the production of this strategy document remain unclear. The extent to which advice was sought from international partners is unknown. It was reported that key stakeholder groups were identified in the process of drafting the strategy, but some statements made by participants suggested that the list of groups involved may not have been complete.

Some consultation with national stakeholders was reported by the MCIT. Some consultation was also reported having occurred by some Samoan participants, though those present either did not personally attend or were unable to remember details of this consultation process. No one asked could recall what kinds of input was collected from the stakeholders consulted. Participants from the financial sector indicated that nothing seemed to have come from the previous consultation(s) they were aware of. The specifics of whatever consultation process actually took place could not be recalled by any participants present.

None of the international organisation representatives who participated in this study believed his or her organisation to have been consulted during the strategy-drafting process, and some of these participants' comments suggested that doing so would not have been within their organisation's mandate.

Some participants suggested that strategic plans for cybersecurity exist and that some priorities have been set for capacity building and assessment, however the specifics of this were not known to the participants. It was unclear how the strategy might have been, to date, operationalised for implementation by the various stakeholders concerned.

Participants indicated that they had not participated in any real-time cyber-incident management exercises, and that to their knowledge none had taken place. However, there was interest expressed in making such exercises a priority in the future. Still, it appears that the conditions required to meet the CMM strategic-level maturity indicator, "cybersecurity strategic plans, aligned with national strategic priorities, drive capacity-building and investments in security" have been met, as the decision-makers who devised these plans are the same decision-makers directing capacity-building and investment efforts within the country.

The CMM currently lists "Relevant metrics, measurement, and monitoring processes, data, and historic trends are evaluated and inform decision-making" as an indicator of strategic-level maturity within the aspect of cybersecurity strategy development. Although Samoa's general cybersecurity capacity maturity is not at this level, it would be fair to acknowledge that it is likely that some public and private organisations within Samoa use some kinds of metrics, measures, data, and awareness of current and past situations to inform decision-making on cybersecurity-related issues. Some participants did report their organisations having information- and cybersecurity measures in place that were administered by more mature organisations or service providers.

When asked whether there were any plans in place for strategy revision, a representative from the MCIT indicated that there were not. It remains to be seen whether Samoa's experience with cybersecurity-strategy development will result in future international or regional leadership that will shape the development of global cybersecurity strategy.

Samoa's national cybersecurity organisation is currently in its formative stages, although the MCIT has reported that significant progress toward the development of a national cybersecurity programme has been made to date.

Statements from MCIT participants and others suggested that MCIT is the recognised coordinating body for the nation's cybersecurity policy. The MCIT has been given the mandate to consult across public and private sectors, as well as with civil society. However, while the MCIT reported past efforts to engage in a multi-stakeholder consultative process to develop this programme, it was noted that participation in this process had been lacking, for reasons that remain unclear.

The goals and objectives of Samoa's national cybersecurity program have been outlined in the nation's cybersecurity strategy, but at the time this study was conducted, participants from the MCIT were unable to describe what metrics will be used to measure the progress of this programme.

What budget is available for the cybersecurity programme, or how this budget is planned to be distributed over the long term was not established during the current study. Unless a budget for the cybersecurity program is secured over the long term, its prospects for further development and future sustainability are obviously in question.

The cybersecurity programme has yet to be fully instantiated and statements made by various participants suggested that metrics are not yet being applied to monitor and measure the functionality of the programme for the purpose of allocating or reallocating resources.

The provisions of Samoa's *National Information and Communication Technology Policy 2012-2017* make one reference to the need for protecting "the security of information shared and access[ed] using ICT"[36]; the *Samoa National Cybersecurity Strategy 2016-2021* outlines the current goals of the cybersecurity programme, which are:

1) Develop necessary organizational structures with a focus on utilizing existing structures in Samoa as well as in the region;
2) Establish relevant Technical Measure (Entities and Standards) to eliminate Cyber Threats and Attacks, enhance Cybersecurity and promote Cybersecurity;
3) Strengthen the legal framework to meet highest regional and international standards with regard to protection of fundamental rights as well as criminalization, investigation, electronic evidence and international cooperation;
4) Build digital citizens capacity, raising awareness and attaining resources to enhance Cybersecurity, combat Cybercrime activities and promote Cyber safety to the highest levels; and
5) Cooperation; Responding to the global nature of Cybersecurity threats and attacks through a multi-stakeholders approach and strengthening local and global partnerships[37].

The content of the national cybersecurity strategy does provide some linkage between cybersecurity, national risk priorities and business development within the nation, but this is at a high level of abstraction and lacking in specific detail regarding the risks, priorities, and objectives concerned. The strategy content technically fulfils one of the CMM's strategic-level maturity indicators in that it aims to protect critical infrastructure from internal threats, i.e. "…cyber-threats including but not limited to infrastructure impairment and criminal activities"[38], but participant comments strongly suggested that Samoa is not yet well placed to do this.

The extent to which the provisions of the strategy represent actionable directives may be contingent upon other communications to which the research team was not privy.

A statement from a participant from the MCIT suggested that some metrics and measurements may have been adopted in the interest of monitoring the cybersecurity

[36] Government of Samoa 2012, *National Information and Communication Technology Policy 2012-2017*, Ministry of Communications and Information Technology, Apia (Samoa), viewed 22 May 2018, <http://www.mcit.gov.ws/images/mcit/NICTPOLICY2012-2017.pdf>.
[37] Government of Samoa 2016, *Samoa National Cybersecurity Strategy 2016-2021*, Ministry of Communications and Information Technology, Apia (Samoa), viewed 22 May 2018, <http://www.samoagovt.ws/wp-content/uploads/2017/02/MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021.pdf>.
[38] Samoa Government (2016)

programme. However, another comment from the same participant, when asked whether there were plans to update the strategy, suggested that there were not yet any plans to update or otherwise incorporate new content into the strategy. It is therefore not clear whether any metrics currently in use might be applied toward resource investment or adjustment of the strategy in response to the evolving threat landscape.

D 1.2 INCIDENT RESPONSE

This factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, coordinate, and operationalise incident response.

Stage: Formative

Samoa is currently in the process of developing a national incident-response capability. Most focus-group participants could think of ways in which incidents within their organisations could constitute national-level issues but, as yet, it appears that there is no register or catalogue of incidents that is centrally maintained by the Samoan government.

Samoa is in the process of standing up a national CIRT, but at the time our study was conducted future funding sources were yet to be determined, as were membership roles and responsibilities within the CIRT or within the local incident-response capabilities of Samoa's key organisations. Some key members from the communications sector had been identified as core members of the CIRT, but comments from these participants suggested that no formal coordination or information-sharing mechanisms are currently in place between organisations within that sector.

Some participants from the public and private sectors reported having cybersecurity incident-response processes within their organisations. However, other participants described incidents where they had been unsure what to do and had had to make decisions in the moment. From these mixed statements it can be gleaned that incident-response processes vary from organisation to organisation, and that many of these processes are unclear or otherwise inadequate.

Comments from focus-group participants suggested that incident-response efforts are not currently being coordinated across organisations. While some participants described steps that they took to handle incidents, the extent to which leads for incident response have been formally designated within organisations is unclear.

As no coordinating national incident-response organisation was yet established at the time this study was conducted, the associated roles, responsibilities and lines of communication or platforms required for broad collaboration on issues were not yet established. Some participants reported having had international support for some kinds of incidents. A participant from the banking sector reported enlisting help from their central branch, located outside of Samoa. Another participant from a critical-infrastructure service reported having to fly in experts from abroad to investigate and resolve an incident which had resulted in both a loss of confidentiality and availability of a core business system for at least two months.

As the national CIRT had not yet been stood up at the time our study was conducted, the extent to which key processes and tools for incident response had been defined by the Samoan government was unclear from participant commentary, but it was clear that most participants present at the focus groups we conducted were not personally familiar with cybersecurity incident response. Participant accounts suggested that many were unfamiliar with key concepts pertaining to incident management, which may indicate that the extent to which IR processes have been identified, documented, and operationalised within these organisations is limited; that training in this area should be improved; or both.

Some participants reported incidents in which international cooperation was required. Depending on the accepted definition of "cybersecurity incident", some participants also referenced instances of international cooperation on cybercrime issues which they thought might also be considered national cybersecurity-related incidents (e.g. the leaking of confidential government information combined with allegations against government officials, or civil disputes connected to online activities).

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

This factor studies the government's capacity to identify CI assets and the risks associated with them, engage in response planning and protection of critical assets, facilitate quality interaction with CI asset owners, and enable comprehensive general risk-management practice including response-planning.

Stage: Formative

While it is virtually certain that some who have been involved with development of the cybersecurity strategy have defined the nation's critical infrastructure, some participant comments suggested that there might not be a complete and common understanding of which organisations are considered critical infrastructure and which are not. This may indicate that, if a list of general CI assets has been created, it may not have been widely distributed. Nevertheless, the government's very invitation of representatives from certain organisations to take part in this study could be taken as an indication that these organisations have recognised roles to play in the national cybersecurity strategy.

Representatives from critical-infrastructure organisations indicated that cybersecurity was a concern, but it was unclear whether standardised, detailed cybersecurity audits were taking place that required granular audits of information assets. It was also unclear to what extent cybersecurity risk assessments were being conducted, if assets were being appraised to assign relative priority or criticality, or whether the outcomes of cybersecurity risk assessments were guiding investment or resource allocation. When asked if risk-management approaches were being used in their organisations, participants from various sectors indicated that they were.

The majority of focus-group participants from CI organisations were IT staff who may have had limited visibility in regard to the MCIT's interactions with their organisations, but their comments suggested that the amount of interaction between the government and CI organisations on cybersecurity issues was relatively low. We were unable to establish the extent to which people with responsibility for ensuring that the CI assets are managed appropriately engaged in activities around cybersecurity, because these people were under-represented. Participants informed us that cybersecurity is an ongoing concern, however the specifics of how CI organisations manage cybersecurity, such as the scope of reporting requirements or the mechanisms for vulnerability disclosure, were often absent from the discussion.

While participants did indicate that communications strategies were in place for crisis situations such as natural disasters, they were unaware of any coordination between their organisations on cybersecurity issues. It was unclear how the management of general threats to CI organisations are managed (i.e. what kinds of problems are managed locally versus what kinds require additional assistance), but some participants described situations in which they required assistance from outside the organisation to resolve a cybersecurity issue or incident.

Although the people with responsibility for ensuring that the CI assets are managed appropriately were generally not present for questioning, participant comments suggested that CI organisations in Samoa are not presently equipped to respond rapidly to changes in the risk environment as far as cybersecurity is concerned.

We were unable to establish the extent to which cybersecurity requirements and vulnerabilities in CI supply chains have been identified, mapped and managed; or the extent to which trust has been established between the government and CI organisations on the exchange of threat information. However, participant commentary suggested that many interdependencies had probably not been identified, given the current reported lack of coordination between organisations. Still, there was no reason to suspect that CI organisations and the government would be reluctant to share information regarding identified threats due to a lack of trust.

Participant comments suggested that some risk management is going on within organisations that can be considered part of the critical infrastructure, but it was unclear what cybersecurity risk-management practices within these organisations currently entail (e.g. what standards are being used by whom), but some comments did suggest low maturity in the areas of threat awareness and cybersecurity incident-response planning.

While several participants referenced the existence of a crisis- or disaster-management plan that guides response efforts across CI organisations during such events, none of the participants believed this plan to have a cybersecurity incident-response dimension.

It seems likely that some degree of physical and logical access control has been implemented within all CI organisations. It also seems from participant commentary that there is some basic capacity to detect, identify, respond to and recover from cyber-threats in most CI organisations, but that the capabilities involved are uncoordinated and probably of varying quality from organisation to organisation.

D 1.4 CRISIS MANAGEMENT

This factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, coordinate, and operationalise incident response.

Stage: Start-up

The Government of Samoa has recognised that crisis management is necessary for national security. The Ministry of Natural Resources and Environment has developed a National Disaster Management Plan[39] and allocated responsibility for "*ensuring the ongoing coordination, development and implementation of Disaster Risk Management programmes and activities in Samoa*"[40] to the Disaster Management Office (DMO). The DMO actively communicate updates on current situations and provide guidance through their Facebook page[41]. However, there is no evidence of any cybersecurity dimension to national crisis management and participants were unaware of any crisis management plan that involves coordination on national cybersecurity incidents.

[39] Ministry of Natural Resources and Environment (MNRE) 2011, Samoa's National Disaster Management Plan 2011-2014, viewed 27 June 2018, available from: https://www.mnre.gov.ws/wp-content/uploads/2017/08/27077_ndmpfinal20111215endoresedbydac.pdf

[40] MNRE 2018, Disaster Management Office, viewed 27 June 2018, available from: https://www.mnre.gov.ws/about-us/divisions/disaster-management-office/

[41] Disaster Management Office 2018, Disaster Management Office – Samoa, viewed 27 June 2018, available from: https://www.facebook.com/DMOSamoa/

D 1.5 CYBER DEFENCE

This factor explores whether the government has the capacity to design and implement a cyber-defence strategy and lead its implementation, including through a designated cyber-defence organisation. It also reviews the level of coordination between various public and private sector actors in response to malicious attacks on strategic information systems and critical national infrastructure.

Stage: Start-up

Much of the CMM assessment content pertaining to cyber-defence is not applicable to Samoa in any direct sense because Samoa does not have its own standing military. That said, some of the associated capabilities might be cultivated within Samoa's future CIRT, or provided by an international partner under an agreement. In a focus group consisting of participants from international organisations, when asked whether anyone was aware of a cyber-defence arrangement between Samoa and another country, a participant from the Australian High Commission stated that a threat to Samoa is considered a threat to Australia, and that Australia is well-placed to respond to such a threat. Given the potentially sensitive nature of this topic, this portion of the discussion consisted of only general language. It was not clear from this what kinds of cyber-defence capabilities Australia might provide or under what circumstances they might be provided.

Samoa has published a cybersecurity strategy and participant comments indicated that this strategy is considered to be a subset of Samoa's broader national security strategy. We were unable to determine the extent to which Samoa's general national security strategy identifies specific threats in terms of external threat actors (state or non-state), insider threats, or supply chain vulnerabilities; or is concerned with incident scenarios in which critical infrastructure is intentionally disrupted.

Samoa's national cybersecurity strategy does not outline the country's position in response to different types or levels of cyber-attack. Participant commentary suggested that attacks by foreign powers were not currently much of a concern. Some participants opined that limited connectivity and slow Internet connection speeds have probably spared Samoa from many kinds of attack to date. However slow Internet access may make organisations particularly vulnerable to Denial of Service (DoS) attacks. Participants suggested that people will probably not become concerned about attacks until a major cybersecurity incident occurs. A participant from the Samoan Water Authority explained that their systems are not currently connected to the Internet but will be soon. It appears that much of Samoa's critical infrastructure is not yet especially vulnerable to cyber-attack for the simple reason that many of the control systems concerned are not connected to the Internet.

It is unclear in the case of Samoa where the line might be drawn between cybersecurity incident response and "cyber-defence." Samoa's cyber-defence needs can be met through a combination of internal capacity-building and operational support from international partners.

As Samoa's CIRT was not yet operational at the time of our study, and participant comments suggested that coordination on cybersecurity issues was not yet taking place across Samoa's key organisations, Samoa’s current capacity for coordinated cyber-defence is understandably low.

D 1.6 COMMUNICATIONS REDUNDANCY

This factor reviews a government’s capacity to identify and map digital redundancy and redundant communications among stakeholders. Digital redundancy foresees a cybersecurity system in which duplication and failure of any component is safeguarded by proper backup. Most of these backups will take the form of isolated (from mainline systems) but readily available digital networks, but some may be non-digital (e.g. backing up a digital communications network with a radio communications network).

Stage: Formative

One finance sector participant noted that their organisation used a second local data centre for limited redundancy, restoring from offline backup to re-establish service in the event of prolong outage (cold site). However, it was noted that there is no hardware redundancy within this architecture. There was no discussion of high availability solutions and only limited use at the organisational level of redundant Internet service through either mixing fixed line and 4G technology, or obtaining service from two different local providers. Participants cited funding limitations as the chief barrier to establishing redundant business systems within most organisations. There was no evidence and insufficient participant representation for the researchers to be able to establish the extent to which redundancy of critical systems has been achieved within Samoa’s key organisations.

During the response to Cyclone Gita in February 2018, the ability for the government to broadcast disaster information via AM radio was degraded, even though FM radio was still active the signal could not be received in rural areas[42]. The DMO Facebook page provides limited redundancy for this kind of dissemination communication, however the low Internet penetration in the community and the dependence on cell towers limits the redundancy offered.

Participant commentary indicated that communications redundancy for emergency assets is assured via emergency radios and satellite phones. While efforts to integrate and coordinate emergency services into a national emergency communication network were cited, some participant commentary suggested that there was room for improvement, i.e. that the process of connecting people to the appropriate emergency service does not always go smoothly. Participant commentary indicated that standard operating procedures (SOPs) are currently in place for emergency response assets, but the extent to which these SOPs accommodate the possibility of disrupted communications to varying degrees was unclear. Though some participants did allude to past emergency response drills that would presumably have involved the use of emergency communications channels, we were unable to establish

[42] RNZ 2018, Concerns in the Samoas over state of emergency communications, available from: https://www.radionz.co.nz/international/programmes/datelinepacific/audio/2018632777/concerns-in-the-samoas-over-state-of-emergency-communications (accessed 28 June 2018).

the extent to which the communications plans in place are tested or whether there are systematic efforts to improve upon them.

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cybersecurity Policy and Strategy*, the Global Cyber Security Capacity Centre has developed the following set of recommendations for consideration by the Government of Samoa. These recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model. The recommendations are provided specifically for each factor.

NATIONAL CYBERSECURITY STRATEGY

R1.1 A thorough and potentially helpful high-level discussion of national cybersecurity issues is offered in Klimburg (2012).[43]

R1.2 Samoa should develop its own internal cybersecurity risk-analyst capacity. Cybersecurity risk-analyst skills are required for monitoring operations and developments in the risk environment (within specific organisations as well as within the world at large). These analysts should be able to bring together available data and information from various sources, such as system and user logs, reports from staff, news sources, service providers, and domestic and international partners, to create "risk profiles" specific for their organisational contexts. Ideally, every organisation that has a computer network should have someone with these skills, and cybersecurity management decisions should take into account findings from these analyses. A basic 12-step process for intelligence-driven information security risk management is summarised at the end of the discussion section in Webb, Ahmad, Maynard and Shanks (2014).[44]

R1.3 Analysts should be given standardised procedures for monitoring and reporting observations and developments that cybersecurity policies (organisational and national) might need to be revised to accommodate.

[43] Klimburg, Alexander (ed.) 2012, *National Cybersecurity Framework Manual*, NATO Cooperative Cyber Defence Centre of Excellence publication, Tallinn 2012, viewed 23 May 2018, <https://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf>.

[44] Webb, J., Ahmad, A., Maynard, S.B. and Shanks, G., 2014. A situation awareness model for information security risk management. *Computers & security*, *44*, pp.1-15, viewed 24 May 2018, <http://www.academia.edu/download/44214181/A_Situation_Awareness_Model_for_Informat20160330-21085-1o6ebqv.pdf>.

R1.4 Establish a regular cycle for re-evaluating and updating the national cybersecurity policy in response to recognised developments (e.g. every six months).

R1.5 Once personnel with cybersecurity skill sets have been placed within Samoa's key public- and private-sector organisations, consult with international partners to establish an ongoing program for the conduct of cybersecurity readiness exercises in which key organisations are required to participate. The program created should be a matter of national security policy.

R1.6 Samoan organisations should be consulted to understand what kinds of risks they perceive themselves to be faced with, what kinds of incidents they have experienced, and what kinds of lessons they have learned or ideas they have had in the wake of these experiences. The control strategies required to defend against these risks should then be referenced (in high level language that is not conducive to the development of effective countermeasures by criminals or other adversaries) in the national cybersecurity strategy.

R1.7 Once a general collection of control strategies appropriate for the risks being faced has been compiled, organisations need to be consulted on how these high-level strategies can be operationalised within their own organisational contexts. This might be achieved by having representatives from these organisations write down their understanding of what their implementation of these control strategies should entail.

R1.8 Government personnel should be available via some form of telecommunication to advise practitioners who are unsure of how they should implement the government's recommended control strategies.

R1.9 Deep consultation between government and representatives from Samoa's key organisations needs to take place to ensure a common picture of who does what and why within the national cybersecurity program. It is necessary for understanding risk from general and context-specific perspectives, as well as for allocating realistic roles and responsibilities to the stakeholders involved.

R1.10 Samoa needs to decide upon and endorse the use of specific metrics for use in monitoring the performance of the cybersecurity programme; otherwise it is impossible to know how well it is working or where it needs to be improved. A recent survey of systems security metrics is offered in Pendleton Garcia-Lebron, Cho, and Xu (2017).[45]

R1.11 Special attention needs to be applied toward assuring effective communication between the cybersecurity programme's coordinating body and points of contact within Samoa's key organisations to ensure that risk pictures and corresponding resource requirements are current.

R1.12 The cybersecurity programme's coordinating body needs to maintain a good relationship with the general public in the interest of awareness raising and incident reporting from individual users to the authorities. An aware and educated public is a distributed sensing environment that can yield important insights into the types of threats Samoa is facing.

R1.13 Because cybersecurity is both a fundamental and a perennial concern, it is important that the cybersecurity programme remains a permanent dimension of governance and management throughout Samoa. The program needs robust legal backing, and technological development and security initiatives should be given their own budgets with equal priority given whatever funds are currently available. Samoa's international partners should provide the funding and resources required to make Samoa a strong link in the global information security chain.

R1.14 In order to assure that national-level cybersecurity risk assessments are updated continuously, an intelligence cycle approach can be adopted in which data about the risk environment is collected and analysed on a continuous basis. Collaborative partnerships will be important to ensure that information on the risk environment is captured at the local, national, regional and global levels. Analyst findings should be structured into standardised report formats that can be integrated into decision-making at different levels of the programme. Ideally, the cybersecurity analysts within organisations will pass findings to analysts at the strategic level who can then consolidate them to support national policymaking.

R1.15 The policy should identify specific requirements for specific sectors that organisations within those sectors are required to operationalise after a process of consultation. The purpose of the consultation should be at least twofold: to establish organisational context (for the purpose of identifying risks and suitable control strategies) and to facilitate guidance from the government where

[45] Pendleton, M., Garcia-Lebron, R., Cho, J.H. and Xu, S., 2017. A survey on systems security metrics. *ACM Computing Surveys (CSUR)*, *49*(4), p.62, viewed 23 May 2018, <http://www.cs.utsa.edu/~shxu/socs/A%20Survey%20on%20Systems%20Security%20Metrics.pdf>.

organisations are unsure about how to go about planning, implementation, monitoring, or reporting.

R1.16 It could be helpful if a future version of the national cybersecurity strategy (or other policy document) were to describe the nation's security priorities as different types of high-level control strategy types (technical controls, training and education, law enforcement powers and capabilities, etc.) that relate to Samoa's priorities for progress and business development, e.g. "Minimum cybersecurity standards need to be enforced across the banking and financial sectors, followed by public awareness campaigns that will help build trust and confidence in the very online financial services that will make Samoan businesses more efficient and life easier for the average Samoan."

R1.17 If it has not already done so, Samoa needs to either develop or adopt information- and cybersecurity performance metrics that will help the government to monitor the performance of the cybersecurity programme and make adjustments to the strategy behind it where required in the interest of improving this performance.

R1.18 The strategy should be revised regularly to reflect posture changes in response to changes in the risk environment. Situation awareness over this environment should be supported by intelligence from international partners, reports from security analysts within Samoan organisations, and reports by security analysts who have been tasked by the Samoan government with monitoring developments in Samoa and in the world at large.

INCIDENT RESPONSE

R1.19 A mechanism for reporting detected cybersecurity incidents needs to be established, which all organisations considered key to national security are expected to use.

R1.20 Standard criteria need to be established or adopted for prioritizing and escalating reported cybersecurity incidents, and incidents reported to the government should be interpreted by personnel who possess the skill set required to understand the nature of an incident. These personnel should also have the communication skills necessary to elicit (from those who report an incident) the types of information required to classify the incident.

R1.21 Information on reported incidents needs to be logged into a secure registry upon receipt, according to a standardised format, by qualified personnel who are charged with maintaining this registry.

R1.22 Incident reports should be aggregated at regular intervals to inform the government's risk picture and make corresponding changes to strategy or resource allocation.

R1.23 A national incident response capability should be a distributed but concerted effort. If it is not possible to standardise incident response processes across Samoa's key organisations, their different approaches need to be translated into common terminology for sharing information about threats, vulnerabilities, and observed impacts or consequences. A collection of best practices for incident response at the national level has been compiled by the Organization of American States (2016).[46]

R1.24 All organisations considered key to the national interest should have membership in (or a formal relationship with) the national incident response organisation.

R1.25 A national CIRT requires building up cybersecurity management capability within all the nation's key organisations. Organisations should have the capacity to handle most kinds of incidents themselves, with the roles of the CIRT being oriented more toward the issuance of consistent practical guidance and the facilitation of information sharing and cooperative problem solving.

R1.26 At its highest stage of maturity, functions of the national CIRT should be focussed on aggregating intelligence fed forward from both distributed sensing technologies and the cybersecurity analysts within individual organisations. The CIRT can then serve an early warning function which supports coordinated prevention efforts across the country.

R1.27 Whatever funding is available for development projects that involve information systems, the application of funds should be divided between achieving the aim of the project itself and implementing the necessary countermeasures against identified cybersecurity risks (i.e. control strategies such as user education and awareness, skills education and training, policies, security technologies, etc.). This is in addition to whatever funds are required to develop general cybersecurity capacity within the nation, though the security costs for individual projects will become less as general security capacity increases. Unfortunately, there is no universally appropriate percentage of funding that should be allocated for security, but it can be significant in cases where the risks are high in terms of probability or consequence. If uncontrolled, some risks may lead to

[46] Organization of American States, 2016, *Best Practices for Establishing a National CSIRT*, General Secretariat of the Organization of American States, Washington, DC, viewed 23 May 2018, <https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf>.

serious negative consequences that detract significantly from the anticipated benefits of the project, or even the failure of the project itself.

R1.28 The Samoan government should work to ensure that there are qualified information- and cybersecurity professionals embedded in all organisations considered key to the national interest, and that each organisation has a designated lead for incident response.

R1.29 As it seems that many organisations may not currently have formalised incident response processes, the Samoan government is well placed to standardise these practices across organisations.

R1.30 Cybersecurity practitioners within organisations should be given clear guidance concerning the government's minimum performance standards for incident response, and clear guidance concerning what kinds of information should be shared with the CIRT and how.

R1.31 Once established, the CIRT should collect incident related information from supported organisations in a standardised format. The CIRT should then analyse and fuse this information as necessary to provide early warning where possible, and to produce appropriate general guidance and recommendations (to include advice which has been tailored for different sectors, types of organisations, or even specific organisations when necessary).

R1.32 Once established, the CIRT should share information and processed intelligence on threats and incidents with international partners, as appropriate, to support coordinated international response to identified issues.

R1.33 Once established, the CIRT should continuously support the information sharing and collaborative problem-solving efforts of its supported organisations, to include connecting Samoan practitioners with other international experts.

R1.34 Once established, the CIRT should administer a secure online platform for communication and collaboration on prevention and response issues.

R1.35 The Samoan government should ensure that all key organisations have lines of communication for communicating directly with the CIRT in a time of crisis.

R1.36 The mission scope of Samoa's national CIRT is ultimately at the discretion of the Samoan government. The Samoan government should adopt its own definitions for cybersecurity incidents and cybercrimes, as well as its own threshold for escalating cybersecurity or cybercrime issues to the status of "national cybersecurity incidents" that require CIRT involvement. Just as "there is no single universal definition of cybercrime"[47] there is also no universally agreed upon definition for the term "cybersecurity incident"[48]. Examples of terminological ambiguity can be found in NIST publications. Cichonki, Millar, Grance, and Scarfone (2012)[49] define a "computer security incident" as "violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices" (6). However, Kissel (2013)[50] defines a "cyber incident" as "actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein" (57). The NIST definition of "computer security incident" is broader than the NIST definition of "cyber-incident" because the former includes patterns of human behaviour that can be considered violations while the latter only concerns effects on data and networked technology that can be considered violations. Switching contexts from that of organisational policy to that of national law, we can imagine online bullying translating to criminal laws relating to unacceptable use (a "computer incident") but not to criminal laws relating to adversely affecting data or technology (a "cyber-incident").

R1.37 The CIRT itself should be staffed by the highest performing, most capable cybersecurity incident response personnel available and should endeavour to match the capabilities of international partners as soon as possible.

R1.38 The Samoan government should endorse the adoption of specific standards and guidance, to include monitoring requirements, performance metrics, reporting requirements, and minimum performance standards by all organisations considered key to the national interest.

R1.39 The results of performance audits and tests should be processed into actionable guidance for the organisations being evaluated, and these organisations should be free to request support (or exception) where compliance is too challenging due to current resource constraints.

R1.40 The Samoan government should organise or facilitate training programs that will enable every key Samoan organisation to have personnel capable of conducting

[47] INTERPOL 2018, *Cybercrime*, *International Criminal Police Organisation website*, viewed 24 May 2018,< https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>

[48] Ab Rahman, N.H. and Choo, K.K.R., 2015. A survey of information security incident handling in the cloud. *Computers & Security*, *49*, pp.45-69, viewed 24 May 2018, <http://search.ror.unisa.edu.au/record/UNISA_ALMA51109762230001831/media/digital/open/9915914113201831/12142882480001831/13142967130001831/pdf>.

[49] Cichonki, P., Millar, P., Grance, T. and Scarfone, K., 2012. SP 800-61 rev. 2. *Computer Security Incident Handling Guide*, viewed on 24 May 2018, <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>.

[50] Kissel, R. ed., 2013, NISTIR 7298 Rev. 2 *Glossary of Key Information Security Terms*, viewed on 24 May 2018, <https://www.nist.gov/publications/glossary-key-information-security-terms-1>.

cybersecurity prevention and response activities at or beyond a reasonable minimum standard.

R1.41 Once IR capabilities have been built up in key Samoan organisations, the Samoan government should facilitate (and eventually conduct itself) incident readiness exercises and drills to test capabilities within organisations.

R1.42 Findings from incident management should be translated into guidance on preventative controls.

R1.43 Once established, the CIRT should establish and administer a secure online environment for information sharing and general collaboration by cybersecurity incident response professionals in Samoa and abroad.

R1.44 The government of Samoa should work with international partners to identify and address any skill shortages that might currently impede participation in international collaboration on incident response issues.

R1.45 The CIRT should facilitate coordination between incident response personnel and international partners in emergency situations that meet agreed upon criteria.

R1.46 The CIRT should play a proactive role by maintaining situation awareness over the national and international risk environments. This means some personnel should be assigned to strategic analyst roles, where information collected from various sources (distributed sensor technologies, incident reports received, trusted news outlets, online forums for practitioners, etc.) is processed into concise guidance for practitioners in supported or partner organisations.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.47 If it has not already done so, the Samoan government should clearly specify which organisations are considered "critical infrastructure" and outline the kinds of risks that face these organisations.

R1.48 CI organisations should be tasked with mapping their business processes to understand organisational or personal information assets (types of information, people with kinds of knowledge, kinds of hardware to include personal devices, software, organisational or virtual processes, etc.). Consideration should be given to how these assets are vulnerable to different kinds of purposive or incidental threats that can result in negative consequences for the organisation or the nation as a whole. The information assets linked to the most serious consequences for the nation are ranked highest priority for protection, and so on down, depending on the funding and resources available. One potentially helpful discussion of information security from a business process perspective can be found in Nebauer, Klemen and Biffl (2006).

R1.49 Audits of information assets being used within CI organisations should be updated at regular cycles or whenever there has been any significant change of personnel, modification of business process, or emergence of new and serious type of threat.

R1.50 The audit lists distributed to and completed by organisations should be in a standardised format.

R1.51 The Samoan government needs to promote and institutionalise a routine process for information sharing and coordination on cybersecurity issues which includes all organisations connected to critical infrastructure. Each CI organisation needs a point of contact who will be involved in this process. The process should be supervised by the government and should enable the constant maintenance of security across all CI assets.

R1.52 CI organisations should map their information systems architecture in terms of all information assets (IT, data, software applications, business sub-processes, and people with special skills or knowledge required), involved in all of that organisation's business processes. Core business processes (including their points of linkage to other less central business processes, and any concerns related to the use of personal devices) should then be given the highest priority for security resource allocations.

R1.53 The government body tasked with facilitating coordination on cybersecurity (e.g. the CIRT) should forward vulnerability intelligence and advice from reputable sources, ideally filtered for relevance to recipients (if possible), to the teams tasked with the cybersecurity management of different CI assets.

R1.54 CI organisations should be encouraged to share information about discovered vulnerabilities and incidents without threat of penalty. Incidents involving CI assets need to be analysed to establish root causes and eliminate points of vulnerability where possible.

R1.55 The cybersecurity skill set required to identify, respond to, and recover from incidents needs to be built up to a working standard across all CI organisations. This can be done by requiring CI organisations to comply with a government issued list of specific practices, guidelines, or standards; but this obviously requires having qualified personnel. Training to develop cybersecurity skills in

Samoan personnel (and retention programs to keep these people in Samoan organisations) should be funding priorities for Samoa and its international aid partners.

R1.56 A detailed framework for improving the cybersecurity of critical infrastructure in the US was recently published by the National Institute of Standards and Technology (Barret 2018).[51]

R1.57 The risk management systems in place within all CI organisations should include the identification and control of cybersecurity risks linked to threats of all types: internal and external to the organisation; incidental (arising from accidents or acts of nature) or purposive (intentional policy violations, attacks in the interest of fraud, sabotage, espionage, etc.).

R1.58 The cybersecurity risk scenarios considered should be linked to different kinds of potential negative impacts, to include harm to the public; reputational damage for the government or for CI organisations; direct and opportunity costs (i.e. the costs associated with incident management as well as opportunities that could be missed due to an incident; impact on revenue; and hindrance to innovation (e.g. due to the theft or destruction of intellectual property), etc.

R1.59 Cybersecurity risk control strategies (to include asset allocations required for executing these strategies) within CI organisations should be updated in accordance with lessons learned from incidents and their business impacts, to ensure that such incidents can be avoided or better mitigated in the future. In some cases, the resources required for control strategies may include assets that will enable redundancy or contingency planning in the event of an incident that results in a denial of service within a certain business process.

R1.60 Rigorous approaches to physical and virtual access control can be used to avoid or mitigate many kinds of risks.

R1.61 A National cybersecurity incident response plan that details who does what in the event of an incident involving the ICT dimension of multiple CI organisations should be drafted, and then drilled and tested through readiness exercises on a regular basis.

[51] Barrett, M.P., 2018. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* (No. NIST Cybersecurity Framework), viewed 23 May 2018, <https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-1>.

CRISIS MANAGEMENT

R1.62 The Samoan government needs to designate an authority responsible for designing, planning and executing cybersecurity crisis management exercises.

R1.63 The cybersecurity crisis management authority should draw on the knowledge and expertise of stakeholders such as critical infrastructure asset owners; core business process owners and cybersecurity practitioners from other key Samoan organisations; academics; civil leaders and consultants.

R1.64 Cybersecurity crisis management preparedness exercises should only be undertaken after cybersecurity capacity has been built up to a minimum standard within Samoa's key organisations. Subjecting unprepared or untrained personnel to performance testing can impact morale in negative, counterproductive ways.

R1.65 Exercise designs should be based on realistic incident scenarios that will test information flows, techniques and measures currently in use, decision-making, and future resource investment planning in the wake of the test incident.

R1.66 Appropriate resources need to be allocated for cybersecurity crisis preparedness exercises. Where funding or resources are currently lacking, requests should be forwarded to international aid partners.

R1.67 The planning process for cybersecurity crisis preparedness exercises should include a promotional communications campaign that provides future participants with explanations of what their roles within the exercise will entail, and what the benefits and incentives are for participation.

R1.68 The performance of people recruited to participate in cybersecurity crisis preparedness exercises should be kept confidential to the greatest possible extent, and the participants should be reminded of this assurance from recruitment through to the issuance of constructive feedback on performance.

R1.69 Feedback on performance should be provided in a sector-specific report that rates performance according to key performance indicators (KPIs) that agree with international crisis management good practice standards and guidance.

R1.70 Evaluation should be followed up with training that aims to correct identified problems. The cybersecurity crisis management authority should provide guidance on cybersecurity crisis management planning to ensure that it comprises tasks and objectives that are specific, measurable, attainable, relevant, and time-bound (SMART).

R1.71 When exercises are conducted, they should be monitored by trained personnel from the cybersecurity crisis management authority or, ideally, another external body.

R1.72 The monitors who evaluate the cybersecurity crisis preparedness exercises should provide constructive feedback to the participants once the exercise has been completed.

CYBER DEFENCE

R1.73 Through coordination with international partners, the Samoan government should develop unambiguous criteria for conditions under which their assistance can be assured.

R1.74 It may be advisable that Samoa delay the adoption of Internet-connected supervisory control and data acquisition (SCADA) systems for critical infrastructure management until sufficient cybersecurity management capacity has been developed within critical infrastructure organisations.

R1.75 Samoa should invest in its CIRT rather than attempting to stand up a separate cyber-defence capability. Once fully operational, the Samoan CIRT may be able to meet most of Samoa's cyber-defence needs through the facilitation of coordinated response across sectors. In situations where assistance from international partners is required, the CIRT should be able to provide support as necessary.

R1.76 A mechanism needs to be set up for organisations to report information to the CIRT. Once cybersecurity-related analytic capacity has been developed and embedded in Samoa's key organisations, these personnel should serve as nodes within a distributed intelligence network that shares information on discovered threats, vulnerability, incident scenarios and known business impacts. Though their attention should be principally inward facing (monitoring the risk environments of their own organisations), these personnel may also gather intelligence information from external/global sources to support the CIRT's intelligence fusion and guidance production efforts. Jasper (2017) provides a good overview of US cyber-threat intelligence sharing frameworks and the kinds of information inputs involved.[52]

[52] Jasper, S.E., 2017. US cyber threat intelligence sharing frameworks. *International Journal of Intelligence and CounterIntelligence*, *30*(1), pp.53-65, viewed 23 May 2018, <https://calhoun.nps.edu/bitstream/handle/10945/50768/Jasper_US_Cyber_Threat_2017.pdf?sequence=1>.

R1.77 Samoa should endeavour to support international partners with cybersecurity relevant intelligence information where possible.

R1.78 To become a leader in the region, Samoa should aim for eventually having its own cybersecurity and cyber-defence research centre, possibly within a university Computer Science or Information Systems department.

R1.79 Samoa's CIRT should be capable of coordinating the management of cybersecurity issues domestically (across law enforcement and the public and private sectors), as well as internationally (with allied or neutral states).

R1.80 Any CIRT activities involving active countermeasures intended to affect adversary capability need to be carefully risk-managed and coordinated with key partners within Samoa and Abroad, to limit the possibility of unintentional, possibly cascading consequences (STUXNET being one well-reported example of how malware intended for a specific target ended up affecting numerous other systems globally). (These kinds of potentially high-risk activities are typically illegal unless strictly controlled and in response to threats meeting very specific criteria.[53])

COMMUNICATIONS REDUNDANCY

R1.81 Establishing redundancy where it does not currently exist for systems supporting the core functionalities of critical infrastructure organisations should become a priority for international partners. Identification of these systems should be the product of asset mapping during risk assessment.

R1.82 Crisis and disaster-response drills should rigorously test the ability of emergency response assets to communicate and coordinate effectively using the selected radio frequency bands and satellite phones, especially under simulated conditions of these communications themselves being impaired or unavailable. No doubt many lessons have already been learned from Samoa's real-world experiences managing natural disasters, and it is largely just a matter of making sure that this knowledge is relayed during training and tested during response exercises and drills.

[53] *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations* 2017, Cambridge: Cambridge University Press, 2017.

R1.83 Shortcomings identified during the conduct of emergency response exercises and drills should be remedied through training and resource allocations where possible, with outstanding/unmet needs cited in funding and resource requests lodged with international partners.

R1.84 Where approaches have proven effective toward assuring communications redundancy under challenging conditions in Samoa, these approaches should be shared with international partners, e.g. via publicly available reports (or secure communications channels where the subject matter is sensitive for some reason).

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

Forward-thinking cybersecurity strategies and policies entail a wide array of actors, including Internet users. The days in which cybersecurity was left to experts formally charged with implementing cybersecurity have passed with the rise of the Internet. All those involved with the Internet and related technologies, such as social media, need to understand the role they can play in safeguarding sensitive and personal data as they use digital media and resources. This dimension underscores the centrality of users in achieving cybersecurity, but seeks to avoid conventional tendencies to blame users for problems with cybersecurity. Instead, cybersecurity experts need to build systems and programmes for users – systems that can be used more easily and be incorporated in everyday practices online.

This dimension reviews important elements of a responsible cybersecurity culture and society such as the understanding of cyber-related risks by all actors, developing a learned level of trust in Internet services, e-government and e-commerce services, and users' understanding of how to protect personal information online. This dimension also entails the existence of mechanisms for accountability, such as channels for users to report threats to cybersecurity. In addition, this dimension reviews the role of media and social media in helping to shape cybersecurity values, attitudes and behaviour.

D 2.1 CYBERSECURITY MIND-SET

This factor evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society-at-large. A cybersecurity mind-set consists of values, attitudes and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem that increase the resilience of users to threats to their security online.

Stage: Start-up

Overall, the cyber-ecosystem in Samoa is still in its very early stages. The review found that cybersecurity has not yet become a priority across the public and private sectors or among end-users. Focus-group discussions suggest that Samoa, like most other Pacific Island countries has a very low level of awareness of cybersecurity. A participant noted that people are less interested primarily due to the fact that cybersecurity is fairly new to the country, not widely used, and there is a general lack of knowledge about any national cyber-attacks or personal bad experiences with cyber-incidents. Participants were not aware of any research conducted to measure to what extent Internet users are concerned with cybersecurity issues. Some participants suggested that concern is low because people often consider that it is the IT providers' job to protect, not the responsibility of the user.

However, the government of Samoa has recognised the problem of low awareness of cybersecurity issues across sectors, with the introduction of the *Samoa National Cybersecurity Strategy 2016-2021* (see D1.1) in February 2017 by the MCIT.[54] The strategy sets capacity building (e.g.: building of digital citizens capacity, awareness raising and the promotion of Cyber Safety) as one of the main objectives in order to enhance cybersecurity in the country.[55] Cybersecurity in Samoa is currently driven by the communications sector, primarily the MCIT with the assistance of all its relevant stakeholders.

Overall, the general cybersecurity awareness within government agencies remains very low. In terms of Internet security within the Government, the MCIT conducted two separate surveys regarding the review and monitoring of the *Government Internet and Electronic Mail Policy* (2016)[56] - specifically for government organizations only - which covered: 1) configured firewall and filtering systems, 2) hardware & software firewall, 3) virus protection, 4) software installation, 5) backup and recovery. In addition, the Office of the Regulator also conducted a survey in collaboration with the Samoa Bureau of Statistics regarding the level of ICT accessibility and affordability.

Commented [E2]: @Tala: Followed up with Office of Regulator, waiting for response. Could you please elaborate on that?

Due to the limited representation of the private sector, it was difficult to determine or get a clear picture of the extent to which private entities recognise the need to prioritise a cybersecurity mind-set.

D 2.2 TRUST AND CONFIDENCE ON THE INTERNET

This factor reviews the level of user trust and confidence in the use of online services in general, and e-government and e-commerce services in particular.

[54] Ministry of Communication and Information Technology (2017) 'Samoa National Cybersecurity Strategy 2016-2021', Available at http://www.samoagovt.ws/2017/02/national-cybersecurity-strategy-launched/mcit-samoa-national-cybersecurity-strategy-2016-2021/ (accessed 7 May 2018)

[55] Ministry of Communication and Information Technology (2017) 'Samoa National Cybersecurity Strategy 2016-2021', Available at http://www.samoagovt.ws/2017/02/national-cybersecurity-strategy-launched/mcit-samoa-national-cybersecurity-strategy-2016-2021/ (accessed 7 May 2018)

[56] Ministry of Communication and Information Technology (2016) 'Government Internet and Electronic Mail Policy', Available at http://www.mcit.gov.ws/images/Final-Draft_Govt-Internet-and-Email-Policy-2016_Final.pdf (accessed 7 May 2018)

Stage: Start-up

Most people in Samoa access the Internet via their mobile phones (not via desktop computers) and based on focus-group discussions, it seems to be quite common that most phone users have a nearly blind trust regarding what they see or receive online via their phones. Participants in our discussions believed that users are unaware of many risks and the required skills to use mobile Internet. Most users do not have the ability to critically assess content they see and receive online, nor the applications they use.

That said, participants highlighted that there is a general lack of trust in mobile payments. According to UNCTAD's e-trade readiness assessment 'only 3.7% of mobile phone owners have a mobile money account.'[57] Also, participants noted that a primary concern with regard to cybersecurity in the country has been social friction and distrust relating to controversial content on an unofficial Facebook page (OLP) which pretends to be speaking for the Prime Minister[58].

With e-government services in the very early stages of implementation, there is a need to build trust in order to move government agencies and citizens to online services. That said, the trust in online services offered by the government (e.g.: e-Tax system) is generally very low.

Online banking is the only form of e-commerce that is currently available, since Samoa is still very much a cash society and has a culture of face-to-face interaction this is unlikely to change significantly in the near future. One participant expressed that 'it would be a surprise if people were using their phones to pay bills. An estimate would be way less than 10 % of the population'. The fact that there is no national ID system in place yet makes record keeping and trusted transactions difficult, but on the other hand there is the perception that 'no one can do anything to me online because I don't have a credit card'. One of the requirements to open a bank account is to provide two photo IDs, however participants suggested that most people do not have an ID, passport or driver's license, presenting real obstacles to obtaining bank accounts. Also, some participants mentioned that it is quite common for Samoans living abroad to transfer money back to Samoa through Western Union, with the recipient going to the Western Union office in person to pick up the cash with a reference number used for identification. One participant noted that page design often makes banking via mobile phone difficult and therefore few people trust the security of their phones for financial transactions.

[57] UNCTAD (2016) *Rapid e-Trade Readiness Assessment*. Available at http://unctad.org/en/PublicationsLibrary/dtlstict2017d10_en.pdf (accessed 7 May 2018)
[58] Young, L.W. (2018) *Anonymous blogger's page shut down by Facebook*. Available at http://www.samoaplanet.com/anonymous-bloggers-page-shut-down-by-facebook/ (accessed 7 May 2018)

D 2.3 USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

This factor looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protection of personal information online, and whether they are sensitised to their privacy rights.

Stage: Start-up

Participants noted that public awareness of the issues surrounding the protection of personal information and the relationships between privacy and security concerns regarding personal data is very low. Participants suggested that this is because Samoa does not have a tradition or legislation regarding privacy and data protection. As a consequence, mobile Internet users are not aware of the kinds of data they share with operators, nor do they know what is done with the information they do provide on popular social media channels such as Facebook or Twitter. Further discussions proposed that the majority of users are too willing to give away personal details, and also remain unaware and not alert to such issues such as the privacy settings they use, or the terms and conditions of the websites. Participants made reference to the current 'Digital Identities Project' that aims to introduce a national ID card to address the problem that many people do not have forms of personal identification. Participants noted that the lack of formal identification is causing problems across sectors with storing and processing personal data. One example given discussed the case where one patient was found to have multiple patient numbers and multiple health records.

Commented [E3]: @Tala: could you please confirm?

D 2.4 REPORTING MECHANISMS

This factor explores the existence of reporting mechanisms functioning as channels for users to report Internet related crime such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.

Stage: Start-up

No central, dedicated reporting framework exists in Samoa for users to report computer-related or online incidents. Participants noted that people generally report online threats to the police in person (as opposed to initiating some process online). Participants noted that the police try to mediate charges between citizens and reconcile the issue first before referring the matter to court. Some participants noted that one of the reasons why people do not report more frequently is that Samoa is a very religious country that has a culture that promotes 'forgiveness' rather than discipline (punishment) towards offenders. The Samoan Way was described during the review as 'talk, forgive, and move on'.

Despite the lack of reporting mechanisms to report incidents, participants noted that users sometimes report incidents directly to the platform providers, such as Facebook. Participants suggested that many Facebook users perceive this platform as ‘the Internet’ and use it frequently. Building on this reporting mechanism could be a crucial step for mobile Internet users in Samoa to develop a more general sense of how to report problems. Many participants referred to the incident regarding the OLP Facebook page that targeted the Prime Minister and government departments, mixing falsehoods with the truth to mislead. Participants discussed that the OLP Facebook page has created a lot of anger with Samoans, particularly those living abroad, causing reputational damage for families. Participants noted that a complaint was filed with Facebook resulting in the deactivation of the OLP account, however the page was reactivated again upon appeal to Facebook by the account owner.

D 2.5 MEDIA AND SOCIAL MEDIA

This factor explores whether cybersecurity is a common subject across mainstream media, and an issue for broad discussion on social media. Moreover, this aspect speaks about the role of media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.

Stage: Start-up- Formative

Cybersecurity issues are reported in an ad-hoc manner in the media in Samoa, with insufficient coverage in mass media both online and offline. Traditional media seldom provide coverage on cybersecurity when compared to social media. When covered, such reporting refers to high-level events, such as the government’s launching of the National Cybersecurity Strategy[59] or successful cybercrime cases such as the ATM hacking by Chinese nationals or the sophisticated theft by a Romanian man[60,61]. Based on desk research, the Samoa Observer covered cybersecurity related issues (e.g.: cyber-abuse, cyber-bullying) more than ten times in 2017-2018. However, media provides readers limited information and suggestions on how to protect themselves against cyber-threats.

[59] Loop Pacific (2017) *Samoa’s government launches cyber safety*. Available at http://www.loopsamoa.com/samoa-news/samoa%E2%80%99s-government-launches-cyber-safety-strategy-51403 (Accessed 11 May 2018)

[60] Feagaimaali’i-Luamanu, J. (2018) *Romanian guilty of “sophisticated” theft.* Available at http://sobserver.ws/en/06_05_2018/local/32881/Romanian-guilty-of-%E2%80%9Csophisticated%E2%80%9D-theft.htm (Accessed 16 May 2018).

[61] Feagaimaali’i-Luamanu, J. (2017) *More suspected involved in A.T.M. skimming theft*. Available at http://www.samoaobserver.ws/en/10_07_2017/local/22057/More-suspected-involved-in-ATM-skimming-theft.htm (Accessed 9 May 2018).

Despite the popularity of social media via mobile phones, there is limited awareness raising and discussions for cybersecurity via the social media channels. One participant mentioned that allegedly school fights (cyber-enabled bullying) have been triggered by and discussed on social media.

RECOMMENDATIONS

Based on the consultations, the following recommendations are provided for consideration regarding the maturity of C*yber Culture and Society*. These aim to provide possible next steps to be followed to enhance existing cybersecurity capacity as per the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

CYBERSECURITY MIND-SET

R2.1 Intensify efforts in leading government agencies to prioritise cybersecurity and enhance efforts at all levels of government to promote understanding of cyber-risks and threats.

R2.2 Design coordinated training programmes for employees in the public organisations in cooperation with the private sector. Training should include:

a) web security (for e.g.: protection of personal information online, social media, social engineering, secure web browsing, malware, passwords)
b) email security (for e.g.: identify a phishing email, sending an email securely)
c) data security (for e.g.: handling and classifying sensitive information, back-up and recovery)
d) mobile device security (for e.g.: portable data storage)
e) remote access security (for e.g.: working from home/while travelling)

R2.3 Consider educating the public (including High Chiefs (Matai), Chiefs of village councils and the Church) on the nature and consequences of cybercrime and cyberbullying.

R2.4 Consider in collaboration with NGOs providing the youth social programmes (for e.g.: in schools and universities) that will teach students about safe and responsible behaviour online (for e.g.: the risks of using social media), including how to prevent any uncompromising behaviour.

R2.5 Consider setting up a multi-stakeholder group (including business, government, law enforcement agencies, and academia) to run joint projects and initiatives as well as facilitating on-going discussions on cybercrime and cybersecurity issues.

R2.6 Design online programmes and training materials (for e.g.: cybersecurity best practices, cyber-threat landscape in Samoa, risk management) in consultation with the multi-stakeholder group and make them freely accessible for the public. This will equip the public with the right skills needed for their everyday use of the Internet and online services.

R2.7 Identify vulnerable groups and high-risk behaviour across the public, in particular children and women, to inform targeted, coordinated awareness campaigns.

R2.8 Promote prioritisation of risk and threat understanding for private-sector entities by identifying high-risk practices.

R2.9 Enhance efforts in the private sector, in particular telecommunication and e-commerce services, to employ cybersecurity good (proactive) practices.

R2.11 Promote the sharing of information on incidents and good practices among organisations and across sectors to promote a proactive cybersecurity mind-set.

TRUST AND CONFIDENCE ON THE INTERNET

R2.12 Develop and implement campaigns that promote the safe use of online services across the general public, enabling users to critically assess online content they consume social media or smart-phone applications.

R2.13 Promote the implementation of user-consent policies by Internet operators.

R2.14 Encourage ISPs to establish programmes that promote trust in their services based on measures of effectiveness of these programmes.

R2.15 When introducing e-government services for citizens, implement security measures from the beginning to build trust and uptake by citizen, companies and other users.

R2.16 When introducing e-government services for citizens promote their use through a coordinated programme, including the compliance to web standards that protect the anonymity of users.

R2.17 To promote trust of users in e-services inform users about the utility of deployed security solutions.

R2.18 Encourage the development of e-commerce services with emphasising the need for a security (e.g.: use of encryption, post trust certificates/logos of third-party authentication services on the homepage).

R2.19 Employ processes for gathering user feedback within government agencies in order to ensure efficient management of online content.

R2.20 Ensure that security measures are in place for existing e-government services for businesses and public organisations.

R2.21 Ensure that the private sector applies security measures to establish trust in e-commerce services, including informing users of the utility of deployed security solutions.

R2.22 Encourage that users can easily access the terms and conditions for using e-commerce services.

R2.23 Encourage CEOs to use social media platforms in order to create trust with their customers and increase transparency. Customers more likely to use e-commerce services and products if the CEO uses social media.

R2.24 To promote trust of customers in e-commerce services, post customer reviews (both good and bad) and testimonials.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.25 Establish programmes with NGOs and support existing efforts by stakeholders to raise user awareness of online risks. Promote measures to protect privacy to enable users to make informed decisions on when and how to share personal information online.

R2.26 Develop and implement a data protection legislation, including monitoring mechanisms of its application.

R2.27 Encourage a public debate on social media platforms (also in the traditional media) regarding the protection of personal information and about the balance between security and privacy to inform policy-making.

R2.28 Develop a Code of Practice on Protecting Personal Information Online in consultation with multiple stakeholders that can be distributed within the public (for e.g.: in primary and secondary schools).

The Code of Practice should include:

a) guidelines regarding Internet safety and the dangers of misuse of personal information online
b) why personal data is important, how it is processed and how can users protect their privacy

REPORTING MECHANISMS

R2.29 Establish coordinated mechanisms within the public and the private sectors that allows citizens to report cybercrime cases, including online fraud, cyber-bullying, child abuse online, identify theft, privacy and security breaches, and other incidents, in particular for women and other vulnerable groups.

R2.30 Provide manuals to educate the public, teachers and parents about the types of cybercrime that can be reported, how to exercise their rights when falling victim to such crimes and how to report it.

R2.31 Raise awareness about new and existing reporting channels among the wider public and across stakeholder groups and cooperate with the private sector in this regard.

R2.32 Once the Cybercrime Unit of the Ministry of Police is created, consider setting up a secure website of the Cybercrime Unit where victims of cybercrime can report to the police by choosing different options: 1) dialling a number in case it is an emergency or the crime is in progress 2) completing an online form for non-emergency crimes or reporting via social media/email. It is important that all reporting channels should offer the victim the option to report anonymously (for e.g.: anonymous online forms).

R2.33 Consider turning the Cybercrime Unit of the Ministry of Police into Samoa's national fraud and cybercrime reporting centre, providing a central point of contact for citizens and businesses.

R2.34 Consider establishing secure two way of information sharing between the Cybercrime Unit of the Ministry of Police and the High Chiefs of village councils.

MEDIA AND SOCIAL MEDIA

R2.35 In cooperation with civil society and media organisations develop programmes and campaigns to raise awareness among media providers and leading social media actors, for instance during the dedicated cybersecurity awareness month or dedicated web or social media sites on this topic.

R2.36 Enhance the understanding of cybersecurity among media providers (for e.g.: journalists) and facilitate a more active role of media in conveying information about cybersecurity to the public.

R2.37 Encourage media content providers to disseminate information on good (proactive) cybersecurity practice that users can pursue to protect themselves or to respond to cyber-incidents. This could stimulate social media discussions on the topic.

DIMENSION 3

CYBERSECURITY ECUATION, TRAINING AND SKILLS

This dimension reviews the availability of cybersecurity awareness-raising programmes for both the public and executives. Moreover, it evaluates the availability, quality, and uptake of educational and training offerings for various groups of government stakeholders, private sector, and the population as a whole.

D 3.1 AWARENESS RAISING

This factor focuses on the prevalence and design of programmes to raise awareness of cybersecurity risks and threats as well as how to address them, both for the general public and for executive management.

Stage: Start-up

A national programme for cybersecurity awareness raising, led by a designated organisation (from any sector) which addresses a wide range of demographics is yet to be established. Due to the lack of a national awareness programme, cybersecurity awareness amongst the general public is low.

The awareness on cyberbullying and the protection of children online is driven by the Office of the Regulator, the Ministry of Police and the Attorney General's Office. In 2016, the cabinet approved a policy on *Filtering System to prevent access to child sexual abuse material on the Internet*.[62] The policy includes a section on education and public awareness that indicates that the Office of the Regulator will jointly work 'with the ISPs and other relevant stakeholders to promote child online safety and raise awareness', informing the public about the potential

Commented [E4]: @Tala: Waiting for response from the Office of the Regulator as they have been conducting awareness campaign of the potential dangers associated with internet use. Could you please follow up on that with the Office of Regulator?

[62] Attorney General's Office, the Office of the Regulator and the National Prosecution Office (2016) *Filtering System to prevent access to child sexual abuse material on the Internet.* Available at https://www.regulator.gov.ws/images/Policies/Policy---Filtering-System-for-CSAM-APPROVED.pdf (accessed 12 May 2018)

dangers associated with Internet use and promote the use of tools that assist in safe Internet use.[63]

One participant mentioned that in the past five years the Ministry of Police, with assistance from the Australian Department of Foreign Affairs and Trade (DFAT) and the Australian Federal Police, had conducted annual Cyber Safety Pasifika awareness campaigns aimed at educating young people about cyberbullying. However, this annual campaign no longer exists due to lack of funding typically sourced from Australia. Therefore, there is no national cybersecurity awareness programme currently in place. Participant discussions confirmed this finding during the review. However, under the leadership of the MCIT and in partnership with the Ministry of Police, new provisions have been made for the government to move forward and re-introduce the Cyber Safety Pasifika awareness campaign.

Another participant noted that the Ministry of Education is planning a campaign related to the introduction of tablet computers to schools and homes in order to 'raise awareness of what children are doing with their devices and to help parents and children understand that not all Internet access is bad and not everything on the Internet is true.' However, participants emphasized that cybersecurity awareness raising campaigns generally are still at the very initial stages.

Focus-group discussions suggest that awareness of cybersecurity issues is very limited among executive managers both in public and private sectors, which could be one of the reasons why cybersecurity awareness-raising has not yet been perceived as a priority. There are currently no efforts to raise the cybersecurity awareness of executive staff in any sector. However, participants suggested that community elders and chiefs should receive cybersecurity training, or at least be the targets of some awareness programs in order to drive change. Moreover, several participants seemed to agree that the Church should have a central role in cybersecurity awareness and education.

D 3.2 FRAMEWORK FOR EDUCATION

This factor addresses the importance of high quality cybersecurity education offerings and the existence of qualified educators. Moreover, this factor examines the need for enhancing cybersecurity education at the national and institutional level and the collaboration between government, and industry to ensure that the educational investments meet the needs of the cybersecurity environment across all sectors.

Stage: Start-up

[63] Attorney General's Office, the Office of the Regulator and the National Prosecution Office (2016) Filtering System to prevent access to child sexual abuse material on the Internet. Available at https://www.regulator.gov.ws/images/Policies/Policy---Filtering-System-for-CSAM-APPROVED.pdf (accessed 12 May 2018)

The need for enhancing cybersecurity education in schools and universities has been identified by leading government and academic stakeholders. The Samoa National Cybersecurity Strategy (2016-2021) under Goal 4 recognizes the need to enhance education and skills such as the 'development of School Curriculums concerning Computer Studies in the primary and secondary levels' and 'development of Tertiary level Computer Science Curriculum to include Cybersecurity measures'[64]. Overall, cybersecurity education only occurs as part of the curriculum for a more general computing and information systems program. However, it was not clear from focus-group discussions how these objectives will be prioritized in the implementation of the strategy since there is no national budget to reach the goals.

There is currently no formal cybersecurity education in place in Samoa. The country has very limited options for cybersecurity qualifications and there is a shortage of qualified cybersecurity educators to improve the situation. There are no elective or mandatory cybersecurity specific courses offered. Samoa plans to integrate cybersecurity subject areas into existing IT and related education programs in the future. In terms of schools, initial work is underway on introducing basic ICT skills through the provision of 1500 tablet computers to primary schools, with some aspects of security included as part of the project. One participant mentioned that 15 years ago so few people had access to a computer in Samoa that there was no need for cybersecurity training.

In terms of higher education, there are no specific programmes at the Bachelor or Master level available at the only University in Samoa. There was no evidence of competitions for students.

Similarly, it was not clear from focus-group discussions to what extent cooperation between the private sector and the university exists.

During the review, some participants remarked that children should be trained on the devices they receive through support programs. For example, children could be trained on how technology can be used as a tool for learning and carrying out tasks, as opposed to something solely for entertainment. When recommending potentially effective agents of change, participants suggested Samoa could achieve change by involving: 'teachers and women'; Church Youth Groups; Matai (High Chief of the village council) and mobile phone companies. One participant offered that women's associations should be more involved in training, education and awareness.

[64] Government of Samoa (2016) Samoa National Cybersecurity Strategy 2016-2021, Ministry of Communications and Information Technology, Apia (Samoa). Available at http://www.samoagovt.ws/wp-content/uploads/2017/02/MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021.pdf (accessed 22 May 2018)

D 3.3 FRAMEWORK FOR PROFESSIONAL TRAINING

This factor addresses the availability and provision of cybersecurity training programmes building a cadre of cybersecurity professionals. Moreover, this factor reviews the uptake of cybersecurity training and horizontal and vertical cybersecurity knowledge transfer within organisations and how it translates into continuous skills development.

Stage: Start-up

The need for training professionals in cybersecurity has been recognized by the government. The strategy statement of Goal 4 of the Samoa National Cybersecurity Strategy (2016-2021) seeks as part of the national cybersecurity capacity-building efforts to 'ensure that all relevant stakeholders including citizens, students, businesses, judiciary, and law enforcement receive sustainable trainings.'[65] However, focus-group discussions failed to confirm if any distinct budget to reach these goals exists.

No cybersecurity framework for certification and accreditation of public-sector professionals exists. Likewise, there are no vocational trainings and providers of ICT equipment (e.g.: CISCO academy) are the ones transferring instructions and information to staff in Samoa. Otherwise, there is no other level of education in this regard yet.

However, participants suggested that there is a demand for more cybersecurity professionals in Samoa. During focus-group discussions it was acknowledged that computer science and cybersecurity professionals are often educated abroad, e.g.: in New Zealand or Australia. Participants recognised that there is a need for professional training and certification offerings both in the public and private sectors. Also, some participants expressed the desire for more formal training (including awareness and IT staff training) to complement the existing practice of self-learning via freely available online resources and discussion forums. Participants from the private sector referred to CAM (anti-money-laundering) courses that are being offered locally. In terms of technical training, participants noted that although CISCO certifications such as CCNP and CCNA are offered, they are often considered prohibitively expensive. Opinion was given that the private sector is currently 'too reactive—not proactive.'

Recently, Samoa has hosted a week-long workshop focused on firewall configuration, run by the Internet Service Provider (ISP) BlueSky and the Pacific Network Operators Group (PacNOG). However, the regularity and full scope of this training, including who attended, is unknown. In 2017 APNIC delivered training on WireShark and Spoofing – mainly for private-sector participants, although some government officials participated.[66] One participant

Commented [E5]: @Tala: could you please elaborate on that training?

[65] Government of Samoa (2016) Samoa National Cybersecurity Strategy 2016-2021, Ministry of Communications and Information Technology, Apia (Samoa). Available at http://www.samoagovt.ws/wp-content/uploads/2017/02/MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021.pdf (accessed 22 May 2018)

[66] APNIC. Network Security and Internet Resource Management workshop. Available at https://blog.apnic.net/2017/11/09/register-network-security-workshop-samoa/ (accessed 22 May 2018)

mentioned that the Australia Pacific Technical College (APTC) has been approached to provide some certificate level training due to demand from the government and private sector, however the level of progress was not clear (it is probably under development).

Commented [E6]: @Tala: could you please provide more information on that?

A more structured national initiative to develop a cybersecurity workforce has yet to be developed, with limited training programmes on cybersecurity issues offered for the public and private-sector employees or the public.

RECOMMENDATIONS

Following the information presented on the review of the maturity of *cybersecurity education, training and skills*, the following set of recommendations are provided to Samoa. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

AWARENESS RAISING

R3.1 Appoint a dedicated organisation (e.g.: National ICT Steering Committee) which has the mandate to develop and implement a national cybersecurity awareness-raising programme with initial target groups focusing on the most vulnerable users, such as children and women, based on international good practice. Coordinate and cooperate with key stakeholders, in particular including those who participated in the review, including the private sector, civil society and international partners. Some of the tasks of the organisation would be to:

- Create a single online portal linking to appropriate cybersecurity information and disseminate materials for various target groups via the cybersecurity awareness programme and social media.
- Develop a dedicated awareness-raising programme for executive managers within the public and private sectors as this group is usually the final arbiters on investment into security.

R3.2 Speed up the Awareness aspects as contained in the Goal 4 of the Samoa National Cybersecurity Strategy (specifically Action Item 2). For example, the establishment and fostering of links with village council about recent ICT developments; the use of Government media outlet to publicize Cybersecurity information; the development of Tertiary level Computer Science Curriculum to include Cybersecurity measures.

R3.3 Coordinate awareness-raising effort, for instance through a dedicated cybersecurity awareness month (e.g.: Cyber Safety Pasifika awareness campaign) and develop material for specified target groups and sectors, based on international good practice.

R3.4 Integrate cybersecurity awareness-raising efforts into ICT literacy courses and initiatives that could provide established vehicles for cybersecurity awareness-raising campaigns.

R3.5 Establish metrics and ensure that evidence of application and lessons learnt feed into existing and new developed programmes.

FRAMEWORK FOR EDUCATION

R3.6 Develop qualification programmes for cybersecurity educators and start building a cadre of existing and new professional educators to ensure that skilled staff is available to teach newly formed (and existing) cybersecurity courses.

R3.7 Integrate specialised cybersecurity courses in the all computer science degrees at universities and offer specialised cybersecurity courses in universities and other bodies.

R3.8 Make an introductory course in Cybersecurity Awareness a component of ALL University courses.

R3.9 Create cybersecurity education programmes for non-IT specialists and make them available at universities and other bodies in the public sector

R3.10 Collect and evaluate feedback from existing students for further development and enhancement of cybersecurity course offerings.

R3.11 Design specific cybersecurity programmes at the Bachelor or Master levels. Also, consider hosting annual cybersecurity competitions for students.

R3.12 Ensure that all cybersecurity education efforts are coordinated and optimized to maximize the available teaching capacity.

R3.13 Investigate the job market in cybersecurity and emphasize and advance the creation of more job opportunities.

FRAMEWORK FOR PROFESSIONAL TRAINING

R3.14 Train general IT staff on cybersecurity issues so that they can react to incidents as they occur.

R3.15 Identify training needs and develop training courses, seminars and online resources for targeted demographics, including non-IT professionals. Cooperate with the private sector to develop those offerings.

R3.16 Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, models, and operation of these tools.

R3.17 Document national training needs so that the professional needs of society can be adequately met.

R3.18 Develop metrics to evaluate the take up and success of cybersecurity training courses (e.g.: seminars, online resources, and certification offerings).

R3.19 Create a knowledge exchange programme targeted at enhanced cooperation between training providers and academia.

R3.20 Establish regular mandatory training for IT employees and general employees regarding cybersecurity issues.

R3.21 Create specific measures to help government and companies to retain skilled cybersecurity staff.

R3.22 Ensure that professional cybersecurity certification courses are offered across sectors within the country.

R3.23 Establish job creation initiatives for cybersecurity within organisations and encourage employers to train staff to become cybersecurity professionals.

R3.24 Consider investigating the provision of more affordable cybersecurity courses.

R3.25 Ensure that students who study computer science abroad return to the country on completion of their studies.

R3.26 Conduct train the trainer programmes in cybersecurity in order to increase the pool of experts who could provide capacity building sessions in the cybersecurity filed at national level.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

This dimension examines the government's capacity to design and enact national legislation directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, and other cybercrime-related issues. The capacity to enforce such laws is examined through law enforcement, prosecution, and court capacities. Moreover, this dimension observes issues such as formal and informal cooperation frameworks to combat cybercrime.

D 4.1 LEGAL FRAMEWORKS

This factor addresses legislation and regulation frameworks related to cybersecurity, including: ICT security legislative frameworks; privacy; freedom of speech and other human rights online; data protection; child protection; consumer protection; intellectual property; and substantive and procedural cybercrime legislation.

Stage: Start-up

Samoa currently lacks any cybersecurity-specific legislation, although several legal instruments touch upon cybersecurity-related activities. The government are aware of this issue and are currently working towards ratifying the Budapest Convention on Cybercrime, including thoroughly examining and re-evaluating domestic legislation in terms of what amendments or new cybersecurity related laws are required.

The most relevant legislative frameworks related to Samoa's Internet landscape are:

- the Electronic Transactions Act[67] (2008) – that recognises the validity of electronic transactions according to the requirements set out in the Act

[67] Electronic Transactions Act (2008) Available at http://www.paclii.org/ws/legis/consol_act/eta2008256/ (accessed 17 May 2018)

- the Crimes Act[68] (2013) – that covers some aspects of cybercrime under 'Crimes Involving Electronic Systems' Part 18. (XVIII)

With regards to privacy, personal expression, and other human rights online there is no specific legislation in Samoa. However, these issues are dispersed under several legal instruments. For instance, privacy is partially covered under Sections 19-21 of the Statistics Act[69] (2015) that obliges the Government Statistician to ensure the confidentiality of information collected for statistical purposes only. Similarly, agencies that collect and store personal information of individuals are required to take privacy and confidentiality measures such as the Office of the Electoral Commissioner under Section 94 'Infringement of secrecy' of the Electoral Act[70] (1963), the National Provident Fund under Section 8 'Confidentiality' of the National Provident Fund Act[71] (1972). Further, Sections 48 'Confidentiality of customer information' and 50 'Protection of Personal Information' of the Telecommunications Act[72] (2005) refer to the protection of personal information and privacy of customers stored by Internet Service Providers (ISPs):

50. (2)

> *A service provider shall operate the service provider's telecommunications network* ***with due regard for the privacy of the service provider's customers****. Except as permitted or required by law, or with the consent of the person to whom the personal information relates,* ***a service provider shall not collect, use, maintain or disclose customer information or customer communication for undisclosed purposes.***

While Samoa has not adopted specific legislation on human rights online, Article 13 of the Constitution of Samoa (1960) refers to the fundamental human-rights protection of freedom of speech and expression. In addition, Samoa is a signatory to several international instruments on human rights such as:

- the Universal Declaration of Human Rights (1992)
- the Convention on Elimination of All Forms of Discrimination Against Women (CEDAW) (1971)
- the Convention on the Rights of the Child (1989)
- the International Convention on Civil and Political Rights (1966)
- the International Covenant on Economic Social and Cultural Rights (1966)

[68] Crimes Act (2013) Available at http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=93579&p_country=WSM&p_classification=01.04 (accessed 16 May 2018)
[69] Statistics Act (2015) Available at http://www.sbs.gov.ws/index.php/new-document-library?view=download&fileId=1635 (accessed 16 May 2018)
[70] Electoral Act (1963) Available at https://www.oec.gov.ws/wp-content/uploads/2017/08/Electoral-Act-1963-1.pdf (accessed 17 May 2018)
[71] National Provident Fund Act (1972) Available at https://www.npf.ws/sites/default/files/docs/SNPF%20Act%201972.pdf (accessed 17 May 2018)
[72] Telecommunications Act (2005) Available at http://mcit.gov.ws/images/mcit/Telecom-Act-2005.pdf (accessed 17 May 2018).

According to the US Department of State's *Samoa Human Rights Report*[73] (2017), there have not been any violations by the government with regards to Internet access, Internet censorship or the monitoring of private communications online.

Concerning data protection, there is no overall national legislation or regulation that adequately addresses this aspect, as mentioned earlier. However, it is scattered under various legislations such as the Telecommunications Act (2005), the Statistics Act (2015), the Electoral Act (1963) and the National Provident Fund Act (1972).

The protection of children online is covered under the Crimes Act (2013) that provides the following provisions for the safeguard of children online: Section 82 'Publication, distribution or exhibition of indecent material on a child or on a child through an electronic system is an offence' and Section 218 'makes it an offence for any person to carry out any act of solicitation of children'. However, none of these address issues such as cyberbullying and sexual grooming, nor do they define responsibilities of ISPs and the authorities. Samoa has ratified the Convention on the Rights of the Child[74] in 1994, with participants noting that the government are in the process of finalising a bill in line with the obligations set out in the Convention.

There is no comprehensive legal framework that regulates consumer protection online. Focus-group discussions support the findings of the UNCTAD's e-trade readiness assessment,[75] suggesting that consumer protection online is a key concern. However, as mentioned above, Samoa lacks legislation that specifically addresses data protection and privacy. Consumer protection is limited to online fraud via the Crimes Act, Section 215 'Identity Fraud'[76]:

215 (4)

> *A person is liable to imprisonment for a term not exceeding seven (7) years who intentionally, without authorisation and with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person, causes a loss of property to another person by:*
>
> *a) any input, alteration, deletion or suppression of electronic data; or*
> *b) any interference with the functioning of an electronic system.*

In other words, prosecutions can be pursued for theft and fraud if committed online. Also, this section is compliant with Article 8 "Computer-related Fraud" of the Convention on Cybercrime.[77]

[73] US Department of State. Samoa Human Rights Report (2017) https://www.state.gov/documents/organization/277357.pdf (accessed 16 May 2018)

[74] UNICEF (2006) A situation analysis of children, women and youth. Available at https://www.unicef.org/pacificislands/Samoa_sitan.pdf (accessed 18 May 2018)

[75] UNCTAD (2017) Samoa Rapid eTrade Readiness Assessment. Available at http://unctad.org/meetings/en/SessionalDocuments/dtlstict2017d10_en.pdf (accessed 18 May 2018)

[76] Crimes Act (2013) Available at http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=93579&p_country=WSM&p_classification=01.04 (accessed 16 May 2018)

[77] Council of Europe, Convention on Cybercrime, 23 November 2001, available at: http://www.refworld.org/docid/47fdfb202.html (accessed 16 May 2018)

With regards to intellectual property legislation, Samoa has a Copyright Act (1998) in place that is administered by the MCIT, however it is not applicable to online content.[78] Also, Samoa being a member of the World Trade Organization (WTO) has obligations stated in the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) that entered into force in 2012[79]. Participants noted that specific reference to intellectual property online will be addressed under the legislative reforms, making Article 10 of the Convention on Cybercrime applicable to offences related to infringement of copyright and related rights by means of a computer system.

As already mentioned above, Samoa is currently undergoing steps to amend its legal framework on cybercrime in line with the Budapest Convention on Cybercrime. Like most jurisdictions in the region, Samoa does not have a specific law that is solely concerned with cybercrime such as the Computer Crimes Act[80] (2003 revised in 2006) of the Kingdom of Tonga. However, there are certain legislations that currently offer some assistance to law enforcement. For example, Part 18 of the Crimes Act (2013) which outlines offences such as skimming (under Sections 206 and 207) and harassment (under Section 219) have been successfully prosecuted in Samoa. Furthermore, there are 'traditional' offences such as fraud, theft and offences against children that can still be pursued and prosecuted, if the offences are committed online.

Samoa's cybercrime provisions are contained under the following legislations:

- **Crimes Act** [81](2013) that covers some aspects of cybercrime under 'Crimes Involving Electronic Systems' Part 18. (XVIII)
- **Telecommunications Act**[82] (2005) that covers some aspects of cybercrime under
  - 'Interpretation' (Section 2)
  - 'Telecommunications And Computer Offences' (Section 74)
  - 'Other Offences and Penalties' (Section 75)
- **Broadcasting Act**[83] (2010) that covers some aspects of cybercrime under
  - 'Interpretation' (Section 2)
  - 'Broadcasting And Computer Offences' (Section 65)
  - 'Offences And Penalties' (Section 66)
- **Copyright Act**[84] (1998) that covers some aspects of cybercrime under
  - 'Reproduction and Adaptation of Computer Programs' (Section 13)
  - 'Criminal Sanctions' (Section 27)

[78] Copyright Act (1998) Available at http://www.wipo.int/wipolex/en/details.jsp?id=5760 (accessed 16 May 2018)

[79] Samoa IP Laws and Treaties. IP-related Multilateral Treaties (Entry into force of the Treaty for the Contracting Party). World Trade Organization) - Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) (1994). Available at http://www.wipo.int/wipolex/en/profile.jsp?code=WS (accessed 16 May 2018)

[80] Computer Crimes Act (2003) Kingdom of Tonga. Available at https://ago.gov.to/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0014/ComputerCrimesAct_2.pdf (accessed 16 May 2018)

[81] Crimes Act (2013) Available at http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=93579&p_country=WSM&p_classification=01.04 (accessed 16 May 2018)

[82] Telecommunications Act (2005) Available at http://mcit.gov.ws/images/mcit/Telecom-Act-2005.pdf (accessed 17 May 2018)

[83] Broadcasting Act (2010) Available at http://www.wipo.int/wipolex/en/text.jsp?file_id=311112 (accessed 17 May 2018)

[84] Copyright Act (1998) Available at http://www.wipo.int/wipolex/en/details.jsp?id=5760 (accessed 16 May 2018)

The existing provisions under Samoa's legislation – Police Powers Act[85] (2007) and the Criminal Procedure Act[86] (2016) – do not fully consider cybercrime. For instance, Samoa's procedural laws only provide for traditional search and seizure of evidential material which partially extends to computers. However, there are no clear procedural powers that extend to obtaining and accessing electronic evidence for cybercrime related investigations (e.g.: stored computer data in a computer system). There are also no clear procedural powers to allow law enforcement to issue preservation orders on an Internet Service Provider (ISP), requiring the preservation of stored computer data or traffic data to assist cybercrime investigations. The same issue applies to production orders to empower law enforcement to issue such orders on an ISP to disclose partial traffic data for specific cybercrime related activities. Similarly, there are also no clear safeguards and conditions in place for handling sensitive electronic evidence throughout investigations. Participants suggested expanding and clarifying existing provisions to include cybercrime and safeguard measures, which will be part of the legislative reform once Samoa eventually ratifies the Convention on Cybercrime.

Overall, the legislative framework regulating cybersecurity and related topics is still in the start-up stage of development, as adopted or amended legislation does not cover all aspects of cybersecurity, such as: the protection of human rights online; data protection; consumer protection online; and digital evidence regulations. Legislation is not yet sufficiently enforced, despite Samoa being one of the most advanced in the region according to UNCTAD's Cyberlaw Tracker.[87]

D 4.2 CRIMINAL JUSTICE SYSTEM

This factor studies the capacity of law enforcement to investigate cybercrime, and the prosecution's capacity to present cybercrime and electronic evidence cases. Finally, this factor addresses the court capacity to preside over cybercrime cases and those involving electronic evidence.

Stage: Start-up

Across the criminal justice system of Samoa, capacities are at start-up stages of development.

There is no single institution or special unit that deals with cybercrime issues, nor does Samoa have digital forensics capability or skills to handle digital evidence. Participants expressed several concerns that the law-enforcement community faces such as lack of facilities and tools

[85] Police Powers Act (2007) Available at http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=&p_isn=102756 (accessed 16 May 2018)
[86] Criminal Procedure Act (2016) Available at https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/102763/124340/F-1072562110/WSM102763.pdf (accessed 15 May 2018)
[87] UNCTAD Cyberlaw Tracker: The case of Samoa. Available at http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/CountryDetail.aspx?country=ws (accessed 16 May 2018)

to monitor cybercrime. Participants noted that the following issues with the current system: reliance on complaints to trigger investigations; lack of active search or identification of cyber-threats; and lack of an adequate level of training and certifications in many of the institutions which are needed to carry out prosecutions.

The capacity of prosecutors and judges to handle cybercrime cases and cases involving digital evidence was considered by the participants to be very limited. One participant estimated that the Attorney General's Office currently has less than ten prosecutors trained abroad to prosecute cybercrime cases. Participants noted that very few cybercrime cases have been brought to court and at the national level prosecutors do not receive any training on cybercrime or digital evidence. Further discussions suggested that the training received is mainly focusing on awareness, without specific details on how to actually investigate or prosecute cybercriminals.

Commented [E7]: @Tala: could you please elaborate on the trainings received abroad? Who delivered the trainings?

Commented [E8]: @Tala: could you please specify the trainings?

Similarly, participants perceived the capacity of courts to handle cybercrime cases as very low, with no specialised training available to judges at the national level, who often lack the knowledge to use ICT themselves. Participants referred to the limited funding and the absence of technical equipment. Based on desk research, in September 2017, judges from Samoa attended the first 'Introductory Cybercrime and Electronic Evidence Training of Trainers Course for the Pacific Region' that was delivered by the Council of Europe in Tonga.[88]

The participants highlighted the role of village councils who create local bylaws and hand out fines to community members. Chiefs from each family form the village council, with a Matai (High Chief) who leads the village council. Regarding threats, the Samoan way is to reconcile and usually not to prosecute the crime (e.g.: the police encourages that the issue is resolved before it has to go to court). Much of what was being referred to as cybercrime concerned defamation cases, e.g. someone saying negative things about another person on Facebook. To illustrate, one participant explained a case where the village council fined a perpetrator for insulting someone else on social media as opposed to a criminal prosecution. Therefore, it was suggested that village councils (and High Chiefs) could play a vital role by providing guidance to village citizens to abide by cybersecurity bylaws. As a result, village citizens will be protected from cyberbullying. However, there is a lack of awareness and training of High Chiefs and chiefs of the village councils regarding new technologies and cyber-threats.

During the review, participants recommended the followings: the creation of a cybercrime division within law enforcement ('cybercrime is a new creature for Samoa'); guidance on how to provide support to victims of cybercrime; trainings on investigating and prosecuting cybercrime should be given a high priority; and keeping ISP's involved by ensuring they understand the legal mutual requirements of cybercrime offences.

Overall, Samoa's capacity is very limited due to the lack of experts, funding, and technical equipment to tackle cybercrime cases. It is currently unclear whether the CIRT will have a role in managing cybercrime issues (e.g. providing support to law enforcement).

Commented [E9]: @Tala: Is the CIRT expected to be involved in investigations and prosecutions?

[88] Council of Europe (2017) Introductory Cybercrime and Electronic Evidence Training of Trainers Course for the Pacific Region. Available at https://www.coe.int/web/cybercrime/-/jud-trainin (accessed 16 May 2018)

D 4.3 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

This factor addresses the existence and functioning of formal and informal mechanisms that enable cooperation between domestic actors and across borders to deter and combat cybercrime.

Stage: Start-up

The authorities in Samoa have recognised the need to improve informal and formal cooperation mechanisms, both domestically and across borders, but they remain ad-hoc and are only in their very initial stages.

The existing provisions under the Mutual Assistance in Criminal Matters Act (2007) facilitates international assistance in criminal matters and criminal investigations between Samoa and foreign states.[89] However, the act does not consider cybercrime, in other words, it only covers traditional requests for mutual assistance in criminal matters with a foreign state and does not extend to cybercrime assistance, hence the lack of cross-border cybercrime investigations. There are no provisions that allow law enforcement to preserve computer data or traffic data on behalf of a foreign state in cybercrime investigations. Furthermore, the act does not cover trans-border access to stored computer data with consent or where publicly available, nor the establishment of a 24/7 network to ensure expeditious assistance of mutual-assistance requests. The need to expand and clarify existing provisions to include cybercrime was acknowledged during the review. Participants noted that this will also be addressed under the legislative reform in order to ratify the Budapest Convention on Cybercrime.

Samoa is currently a member of the following organisations that provide various forms of information sharing and cooperation on cybercrime issues and investigations:

- **The Pacific Cyber Security Operational Network**[90] (PaCSON) – 'is a network of government-designated cybersecurity incident response officials from across the Pacific who share information on cybersecurity threats, tools, techniques and ideas between nations.' [91]

- **The Cyber Safety Pasifika Program** (CSP)[92] - is a 'partnership between the Australian Federal Police (AFP) and the Pacific Islands Chiefs of Police, representing an opportunity to be truly proactive in preventing cyber-crime by sharing knowledge gained in Australia and globally with colleagues throughout the Pacific. It works with

[89] Mutual Assistance in Criminal Matters Act (2007) Available at https://www.unodc.org/res/cld/document/wsm/2007/mutual_assistance_in_criminal_matters_act_2007_html/Samoa_Mutual_Assistance_in_Criminal_Matters_Act_2007.pdf (accessed 16 May 2018)
[90] CERT Australia (2018) Pacific Cyber Security Operational Network. https://www.cert.gov.au/news/pacific-cyber-security-operational-network (accessed 16 May 2018)
[91] CERT Australia (2018) Pacific Cyber Security Operational Network. https://www.cert.gov.au/news/pacific-cyber-security-operational-network (accessed 16 May 2018)
[92] Cyber Safety Pasifika Program. Available at http://www.cybersafetypasifika.org/ (accessed 17 May 2018)

the Pacific Islands Chiefs of Police and aims to raise awareness for safe online behaviour in the region.'[93]

- **The Pacific Transnational Crime Coordination Centre** (PTCCC) – is 'based in Samoa and tackles transnational crime in the region (including cybercrime threats). It performs the central coordination role of managing, enhancing, and disseminating law enforcement intelligence products produced by the PTCCC, the Pacific Transnational Crime Network (PTCN) member countries and other international law enforcement partners.' [94]

- **Pacific Islands Law Officer's Network (PILON) Cybercrime Working Group** – is 'a network of senior law officers of the pacific countries who focus on the development and implementation of best practice legislations including the Budapest Convention on Cybercrime. Also, it serves as a forum to allow countries to share information and experiences on cybercrime related issues.'[95]

Some of the participants noted that there has always been a strong respect and working relationship between all three institutions (police, prosecutors and judiciary). Together they uphold the rule of law and ensure justice is served. Participants expressed the need to introduce enhanced and specific cybercrime legislations to improve law-enforcement cooperation and the criminal justice system. A formal relationship exists between the Ministry of Communications and Information Technology, the Office of the Regulator, and the police, on at least the documentation of cybercrime issues, whereby law-enforcement initiates the cybercrime investigations and provides the files to the prosecutors to present in court, while the judiciary assess the evidence and determine a judgment. A participant cited that there is currently 'no budget for cybercrime processing' and that the costs associated with this can be massive.

Among the different available international cooperation channels, the 'police-to-police' coordination via INTERPOL[96] was described as an important channel to facilitate cross-border cooperation and information sharing that is handled by the Transnational Crime Unit (TCU), however it does not include the police.

Commented [E10]: @Tala: could you please confirm?

Samoa is currently looking at coordinating workshops to provide training for law-enforcement, prosecutors and judiciary on cybercrime and electronic-evidence gathering this July, with the assistance of the Council of Europe. The government is in the process of taking steps to bring Samoa into a legislative position to ultimately ratify the Budapest Convention on Cybercrime.

[93] Pacific Islands Chiefs of Police. Available at https://picp.co.nz/our-work/cyber-safety-pasifika/ (accessed 17 May 2018)
[94] Pacific Islands Chiefs of Police. Available at https://picp.co.nz/our-work/cyber-safety-pasifika/ (accessed 17 May 2018)
[95] Pacific Islands Law Officer's Network (PILON). Available at http://pilonsec.org/about (accessed 17 May 2018)
[96] INTERPOL. Samoa. Available at https://www.interpol.int/Member-countries/Asia-South-Pacific/Samoa (accessed 17 May 2018)

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Legal and Regulatory Frameworks*, the following set of recommendations are provided to Samoa. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

LEGAL FRAMEWORKS

R4.1 Consider setting up a periodic process of reviewing and enhancing Samoa's laws relating to cyberspace to address the dynamics of cybersecurity threats (e.g.: hate speech online, cyber-bullying).

R4.2 Revise and adapt the established legislative framework addressing cybersecurity and cybercrime.

R4.3 Review the Crimes Act (2013) to ensure offences cover cyber-criminality and responsive to technological advances.

R4.4 Consider developing a Computer Misuse Act or Cybercrime legislation (e.g.: similar to the Computer Crimes Act 2003 in Tonga) that holistically addresses cybercrime offences and legal procedures.

R4.5 Develop new legislative provisions through multi-stakeholder consultation processes on children's safety online, data protection, consumer protection online, intellectual property online and human rights online.

R4.6 Consider developing a separate strategy covering cybercrime specifically that would also clarify the roles and responsibilities of the actors (CERT, CIRTs, law enforcement, Ministries) involved in handling computer security incident response and cybercrime investigations.

R4.7 Dedicate resources to ensure full enforcement of existing and new cybersecurity laws and monitor implementation.

R4.8 Consider revising the Police Powers Act (2007) and the Criminal Procedure Act (2016) with respect to the procedural powers for investigations of cybercrime and evidentiary requirements to deter, respond to and prosecute cybercrime. Also, revise and enforce legislative provisions that obliges ISPs to provide technical assistance for law enforcement when they conduct lawful electronic surveillance.

CRIMINAL JUSTICE SYSTEM

R4.9 Consider creating a National Cybercrime Laboratory under the auspices of the Ministry of Police in order to facilitate digital forensics. This will provide a platform to all law enforcement agencies to carry out cybercrime investigations.

R4.10 Consider creating a Cybercrime Division/Unit under the Ministry of Police.

R4.11 Strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources, full investigative measures and digital chain of custody.

R4.12 Consider turning the Cybercrime Unit of the Ministry of Police into Samoa's central point of contact to carry out cybercrime investigations both domestically and internationally.

R4.13 Consider establishing institutional capacity building programmes for judges, prosecutors and police personnel from security agencies to acquire new ICT skills needed for cybercrime investigations (for e.g.: digital evidence gathering) and effective ways of enforcing cyber-laws.

R4.14 Consider establishing standards for the training of law enforcement officers, village councils and the Matai (High Chief) on cybercrime.

R4.15 Dedicate sufficient human and technological resources in order to ensure effective legal proceedings regarding cybercrime cases.

R4.16 Consider requesting reliable and accurate cybercrime statistics from the Ministry of Police in order to better inform decision-makers about the current cybercrime threat landscape in Samoa when developing policies and legislations to address this matter.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS

R4.17 Strengthen international cooperation to combat cybercrime based on existing legal assistance frameworks and enter further bilateral or international agreements.

R4.18 Facilitate informal cooperation mechanisms within the police and criminal justice system, and between police and third parties, both domestically and across borders, in particular ISPs.

R4.19 Consider establishing a 24/7 point of contact within the Cybercrime Unit of the Ministry of Police in order to provide instant assistance for mutual legal assistance requests.

DIMENSION 5
STANDARDS, ORGANISATIONS AND TECHNOLOGIES

This dimension addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

D 5.1 ADHERENCE TO STANDARDS

This factor reviews government's capacity to design, adapt and implement cybersecurity standards and good practice, especially those related to procurement procedures and software development.

Stage: Start-up

Samoa has yet to adopt defined standards and good practices for information risk management for securing data, technology and infrastructure. However, the Government of Samoa is aware of this and has included establishing standards as a key goal in the National Cybersecurity Strategy: Goal 2: "*Establish relevant technical measures (Entities and Standards) to eliminate Cyber Threats and Attacks, enhance Cybersecurity and promote Cyber Safety*"[97]. As part of the implementation of the national strategy, the Ministry of Communications and Information Technology (MCIT) and the Office of the Regulator (OOTR) are leading the assessment and development of suitable cybersecurity standards.

[97] Government of Samoa (2016) 'MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021'. Available at: http://www.samoagovt.ws/wp-content/uploads/2017/02/MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021.pdf (Accessed 14 May 2018), p8.

When discussing the situation in the public sector, participants noted that the Government Internet and Email Policy 2016[98] from the MCIT provides guidance on mandatory minimal security requirements for all government agencies, including acceptable use. However, guidance is limited on how security controls should be applied and there are no details of recommended products or configurations. Discussions with participants suggests that both the depth and breadth of additional security controls vary across agencies. Some public-sector participants suggested that the practice of sharing passwords amongst colleagues was commonplace in order to ensure tasks are completed on time, despite this being strictly forbidden in the Government Internet and Email Policy 2016. There was no discussion or evidence of further guidance around digital-identify management, including authentication.

The public sector sets a standard for procurement practices through legislation, policy, guidance and operating procedures, overseen by the Ministry of Finance: "*Public Finance Management Act 2001; Treasury Instructions 2013; Operating Manuals; Treasury Circulars; Cabinet Directives and specifically Cabinet Directive reference FK(12)29 dated 05 October 2012 concerning Financial Delegation Thresholds*"[99]. The scope of the legislation and policy includes public entities where the government has "*50 percent share or voting rights*"[100]. Policy and guidance is provided for goods, works, general services and consulting services to "*ensure that procurement is carried out with due diligence, efficiency and in conformity with sound engineering or other appropriate professional practices*"[101]. However, there is no mention of cybersecurity standards or good practices to guide agencies or public entities in their procurement decisions.

There is no publicly available evidence or participant discussion to suggest that the public sector currently develop software. Computer Services Limited (CSL) is the only local service provider that was identified as currently advertising software development services in Samoa[102]. However, participants were not aware of any software development within Samoa or any specified standard or good practices to guide developers.

In terms of the private sector, no defined cybersecurity standards or good practices could be publicly identified in Samoa. The Government of Samoa does not currently provide guidance on standards or good practices to other sectors. Participants noted that security policy and guidance is provided by International head offices, including the purchasing of information technology products.

Participants from both the private and public sectors noted that there is no specific cybersecurity standard in use locally in Samoa by any sector. Participants theorised that Samoa could benefit from the adoption of recognised cybersecurity standards and good practices, including the setting of a minimum standard for cybersecurity across all sectors.

[98] Government of Samoa. (2016) 'Government Internet & Email Policy 2016'. Available at: http://www.mcit.gov.ws/publications/134-government-internet-email-policy-2016 (Accessed 14 May 2018).
[99] Ministry of Finance. (2016) 'Amended Procurement Guidelines: Goods, Works & General Services'. Available at: https://www.mof.gov.ws/Portals/195/Procurement%202017/Amended%20Procurement%20Guidelines%20for%20GWGS.pdf (Accessed 14 May 2018), p1.
[100] Ministry of Finance. (2016), p2.
[101] Ministry of Finance. (2016), p2.
[102] CSL. (2018) 'About us'. Available at: https://www.csl.ws/mesmerize/about-us/ (Accessed 14 May 2018).

D 5.2 INTERNET INFRASTRUCTURE RESILIENCE

This factor addresses the existence of reliable Internet services and infrastructure in the country as well as rigorous security processes across private and public sectors. Also, this aspect reviews the control that the government might have over its Internet infrastructure and the extent to which networks and systems are outsourced.

Stage: Formative

Samoa currently has two submarine cables as part of the country's Internet infrastructure to improve the bandwidth and availability (redundancy) of international Internet service: The Samoa American Samoa - American Samoa Hawaii (SAS-ASH) cable connecting Samoa to American Samoa and Hawaii; and the Tui-Samoa cable, connecting Samoa to Fiji[103]. The SAS-ASH cable is managed by Bluesky[104] and the Tui-Samoa cable is managed and operated by the Samoa Submarine Cable Company (SSCC) on behalf of the government[105]. SCCC shareholders include three of the current Internet Service Providers (ISPs): Bluesky, CSL and DigiCel[106]. Samoa has received key funding for the construction and operation of the Tui-Samoa cable from the Asian Development Bank (ADB), the World Bank, and the Government of Australia[107].

A regional partnership between Samoa, the Cook Islands, French Polynesia and Niue (the Manatu Cable Consortium) has recently been formed to oversee the construction of a third cable – the Manatu cable[108]. The Manatua cable will link "*Tahiti, Cook Islands and Niue and possibly Tonga to Samoa*"[109], with construction due to be completed by early 2019[110].

[103] Telegeography. (2018) 'Submarine cable map 2018'. Available at: http://submarine-cable-map-2018.telegeography.com/ (Accessed 14 May 2018).
[104] Office of the Regulator. 2017 'ITU PITA Workshop on: Enhancing access to submarine cables for Pacific Island Countries'. Available from: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2017/Submarine%20Cable/submarine-cables-for-Pacific-Islands-Countries/Samoa%20-%20Country%20Report-Suva%2CFinal-1.pdf (Accessed 24 May 2018).
[105] SSCC. (2018) 'ABOUT US'. Available at: http://ssccsamoa.com/about/ (Accessed 14 May 2018).
[106] SSCC. (2018)
[107] The World Bank. (2017) 'Samoa to Have Faster, Cheaper Internet as Submarine Cable Project Starts in Savai'I'. Available at: http://www.worldbank.org/en/news/press-release/2017/02/24/samoa-to-have-faster-cheaper-internet-as-submarine-cable-project-starts-in-savaii (Accessed 14 May 2018).
[108] Cook Island News. (2018) 'Tender open for telecoms cable project'. Available at: http://cookislandsnews.com/national/local/item/67588-tender-open-for-telecoms-cable-project/67588-tender-open-for-telecoms-cable-project (Accessed 14 May 2018).
[109] Samoa Observer. (2018) 'Work for $5m Cable Depot begins'. Available at: http://www.samoaobserver.ws/en/01_03_2018/local/30590/Work-for-$5m-Cable-Depot-begins.htm (Accessed 14 May 2018).
[110] Cook Island News. (2018) 'Manatua cable project set to start'. Available at http://www.cookislandsnews.com/item/67313-manatua-cable-project-set-to-start (Accessed 14 May 2018).

Independent of the submarine cables, ISPs Bluesky, NetVo and Digicel offer services that use satellite infrastructure[111,112,113]. NetVo use their own infrastructure[114], Digicel use infrastructure provided by 03b[115] and Bluesky use Intelsat[116]. A new entrant, Kacific Broadband Satellites is looking to provide satellite infrastructure for use by ISPs in 2019[117]. On land, Bluesky is the only provider who offers fixed line broadband[118]. Mobile broadband is offered by Bluesky, NetVo and Digicel[119].

Samoa's National Cybersecurity Strategy includes the goal of establishing a National Computer Incident Response Team (CIRT) to "*identify, combat, respond and manage Cyberspace Threats or Attacks*"[120]. Working with their private-sector partners, the CIRT will play a critical role in securing Samoa's Internet infrastructure, with regional support to develop this capacity further from the Pacific Cyber Security Operational Network (PaCSON) funded by the Australian Government. PaCSON, aims to bring together National CIRT and CERT teams in the region to build capacity for managing the security of national Internet infrastructure[121]. Samoa's commitment to this regional cybersecurity initiative is demonstrated by the recent election of the CEO of MCIT as Chairman Elect of the PaCSON Executive Committee[122]. This initiative will assist Samoa in defining standards and good practices for the management of the Internet infrastructure in terms of availability of service, maintaining confidentiality of the traffic and the integrity of the infrastructure and the traffic that traverses it.

Participants noted that the resiliency of the Internet infrastructure (in terms of redundancy) is seen to be provided to the country via the combination of the two submarine cables and the Internet services that rely on satellite based infrastructure. Participants noted that, in the private sector, some organisations obtain redundancy of Internet service via the use of multiple ISPs, or by mixing both mobile and fixed line technology from the same ISP.

[111] Office of the Regulator. 2017 'ITU PITA Workshop on: Enhancing access to submarine cables for Pacific Island Countries'. Available from: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2017/Submarine%20Cable/submarine-cables-for-Pacific-Islands-Countries/Samoa%20-%20Country%20Report-Suva%2CFinal-1.pdf (Accessed 24 May 2018).

[112] Samoa Observer. (2016a) 'Netvo Samoa Launches Samoa's most advanced 4G LTE Network is here!'. Available at: http://www.samoaobserver.ws/en/31_07_2016/local/9366/Netvo-Samoa-Launches-Samoa%E2%80%99s-most-advanced-4G-LTE-Network-is-here!.htm (Accessed 14 May 2018).

[113] Samoa Observer. (2016b) 'Global satellite service provider backs Digicel'. Available at: http://www.samoaobserver.ws/en/20_07_2016/local/8893/Global-satellite-service--provider-backs-Digicel.htm (Accessed 14 May 2018).

[114] Samoa Observer. (2016a).

[115] Samoa Observer. (2016b.

[116] Office of the Regulator 2017.

[117] Kacific. (2015) 'Products and Services'. Available at: http://kacific.com/business-model/ (Accessed 14 May 2018).

[118] Office of the Regulator 2017.

[119] Office of the Regulator 2017.

[120] Government of Samoa. (2016) 'MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021'. Available at: http://www.samoagovt.ws/wp-content/uploads/2017/02/MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021.pdf (Accessed 14 May 2018), p9.

[121] IT Brief. (2018) 'The Pacific Cyber Security Operational Network is now in action'. Available at: https://itbrief.com.au/story/pacific-cyber-security-operational-network-now-action/ (Accessed 15 May 2018).

[122] Samoa Observer. (2018) 'Samoa to Chair for Pacific Cyber Security Operational Network'. Available at: http://www.samoaobserver.ws/en/17_05_2018/local/33192/Samoa-to-Chair-for-Pacific-Cyber-Security-Operational-Network.htm (Accessed 18 May 2018).

The Samoa National Broadband Policy 2012 outlines the roadmap to increase the speed and affordability of Internet access and increase penetration in rural and urban areas, to 30% and 40% respectively by 2020[123]. Samoa is currently serviced by multiple ISPs for both domestic and business customers. In 2017, 29.1% of households had access to the Internet, with mobile broadband as the main method of access[124] out of a population in 2017 of 197,448[125]. Participants suggested that Internet access in Samoa is mainly from mobile devices and that usage is focused on messaging and social media, with any ecommerce activity directed to overseas suppliers and no significant use for electronic business transactions.

When asked to consider the usability of Samoa's Internet infrastructure, a wide variety of participants across all sectors noted that their domestic services lack sufficient speed and have a high cost. When asked about their experiences for business use, participants had fewer speed complaints across both the private and public sectors, with these connections generally seen to be faster, but still costly. Participants theorised that speed issues may be caused by: rain reducing the throughput of mobile services; limited capacity of the infrastructure to cope with demand; and upstream issues outside of the Samoan networks. Turning to the reliability of services, participants have varied experiences with the availability (outages) of Internet services, suggesting that there are still opportunities to improve the reliability of the Internet infrastructure for end users. However, there are currently no publicly available Service Level Agreements (SLAs) from the ISPs for domestic or business use and no publicly available statistics on the frequency or cause of service outages.

[123] MCIT. 2012 ''. Available from: http://www.mcit.gov.ws/images/mcit/POLICY%20Samoa%20National%20Broadband%20Policy%202012%20_approved_.pdf (Accessed 23 May 2018).
[124] ITU. 2017. 'ICT Development Index 2017', Available at: http://www.itu.int/net4/ITU-D/idi/2017/#idi2017economycard-tab&WSM. (Accessed 23 May 2018).
[125] Samoa Bureau of Statistics. (2018) 'Population & Demography Indicator Summary'. Available at: http://sbs.gov.ws/index.php/population-demography-and-vital-statistics (Accessed 15 May 2018).

D 5.3 SOFTWARE QUALITY

This factor examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this factor reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the criticality of services.

Stage: Start-up

The Government Internet and Email Policy 2016[126] requires the IT department in all government agencies to maintain lists of approved software and test new software for compatibility with their environment. However, there is no identified centrally managed catalogue of secure software platforms and applications or process for monitoring software quality across agencies. The public sector does not use a common operating environment, agencies decide which operating systems and applications to run across their chosen end user and server environments.

The Government Internet and Email Policy 2016 includes the requirement for agencies to configure antivirus software to automatically install updates, but no requirements are mentioned in terms of updating and patching operating systems or applications. When asked about their practices, participants from the public sector gave varying responses when discussing updating and patching operating systems and applications, suggesting that the practice is variable across agencies. One public-sector participant noted that they were not always able to deploy operating system patches to their end-user environment due to reaching the monthly data limit with their ISP. Another public-sector participant noted that their organisation managed operating-system updates via Windows Server Update Services (WSUS). There are currently no defined standards or good practices in place for updating and patching operating systems and applications in the public service.

Participants from the private sector commented that platforms and applications are commonly managed and provided via head offices outside of Samoa, with updating and patching carried out remotely by international teams or patching onsite by local teams. However, it was noted that local patching is limited and mainly focused on the operating system and not applications.

Participants did not discuss concerns regarding functional requirements of software from any sector.

[126] MCIT. (2016) 'Government Internet & Email Policy 2016'. Available at: http://www.mcit.gov.ws/publications/134-government-internet-email-policy-2016 (Accessed 14 May 2018).

D 5.4 TECHNICAL SECURITY CONTROLS

This factor reviews evidence regarding the deployment of technical security controls by users, public and private sectors and whether the technical cybersecurity control set is based on established cybersecurity frameworks.

Stage: Start-up

The Government Internet and Email Policy 2016 from the MCIT provides guidance on mandatory minimal security requirements for all government agencies. In terms of technical controls, the policy covers the requirement for all agencies to have perimeter firewall, web content filtering and antivirus controls. However, the policy does not cover additional controls and there is no supporting guidance on selecting suitable products, secure configuration or deployment.

One public-sector participant noted that remote work in their organisation is carried out using personal devices and flash drives to exchange information with institutional systems, without breaching policy. Participants also noted that organisations have experienced ransomware incidents, with malware introduced into systems via flash drives from personal devices or through end users opening infected attachments. During further discussion, participants indicated that more than one organisation has experienced domain blacklisting. Participants theorised that this was due to compromised email accounts or compromised public-facing systems being abused to distribute spam, though there was no discussion of the use of SPF DNS records as a control for domain spoofing. Participants noted that the government is considering moving the public sector to Google's G-Suite as a measure to improve security, especially around messaging. However, there was no discussion of what controls would apply to Cloud environments. There is no publicly available statistical data on the use and deployment of technical security controls by users, private or public sectors.

Participants suggested that the practice of patching operating systems and performing backups are widespread across sectors, but noted that there are no defined standards or good practices to guide these activities. The discussion of more advanced controls was limited to a single public-sector entity which is using an Intrusion Prevention System (IPS) to protect their network, supported by Host Intrusion Detection Systems (HIDS) with limited functionality. However, there was no evidence that controls are reviewed and assessed for their effectiveness. Participants noted that in the finance sector, controls are typically deployed and managed by overseas head office teams.

There is no evidence of wider promotion of the use of technical security controls, nor incentives being offered to any sector for the use of up-to-date security controls. There is no evidence that ISPs are offering upstream controls or antimalware software as part of their services. ISPs did not discuss the need to establish policies for technical security control deployment as part of their services. There is no evidence of a defined standard or good practices for up-to-date security controls, including backup and patching, in any sector.

D 5.5 CRYPTOGRAPHIC CONTROLS

This factor reviews the deployment of cryptographic techniques in all sectors and users for protection of data at rest or in transit, and the extent to which these cryptographic controls meet international standards and guidelines and are kept up-to-date.

Stage: Start-up

Samoa does not currently have defined standards or good practice guidance for cryptographic controls for protecting data at rest or in transit. Participants noted that in the public sector initial work is underway to deploy certificates as controls for protecting web traffic in transit across all government websites, but this is not currently reflected in policy. In terms of the private sector, participants noted that certificates are deployed across the finance sector for protecting web traffic in transit only. The discussion of wider use of encryption for protecting data in transit through cryptographic protocols was limited to the use of Secure Shell (SSH) in some organisations. A visual inspection of a sample (N=29) of public-sector and private-sector websites demonstrated that the use of current TLS controls varies in both sectors, with most sites having no TLS controls in place and one site using an obsolete version of TLS.

When considering other cryptographic controls, participants noted that the government is exploring digital-signature controls for proving the authenticity of documents and communications. However, there was no discussion of controls for protecting data at rest from any sector. One public-sector participant suggested that the main barrier to wider adoption of cryptographic controls was the cost of implementation, theorising that one approach to tackle the problem would be to lower the government tariffs on enabling products.

D 5.6 CYBERSECURITY MARKETPLACE

This factor addresses the availability and development of competitive cybersecurity technologies and insurance products.

Stage: Start-up

Participants from the public and private sectors noted that Samoa does not currently produce cybersecurity technologies, but relies on international offerings. Participants noted that in the finance sector, some organisations have first-party cyber-insurance through their head offices outside of Samoa, though this insurance is seen as having a high cost.

There was no discussion amongst participants that a market for insurance has been identified in Samoa. Participants noted that their organisations had nothing to cover financial losses in the event of a serious cybersecurity incident, theorising that in the future the Government of Samoa could provide services to protect business in Samoa from such events.

D 5.7 RESPONSIBLE DISCLOSURE

This factor explores the establishment of a responsible-disclosure framework for the receipt and dissemination of vulnerability information across sectors and, if there is sufficient capacity, to continuously review and update this framework.

Stage: Start-up

Samoa does not currently have a responsible disclosure policy. The need for a responsible disclosure policy was not acknowledged by participants from any sector. When asked about how users can report bugs and vulnerabilities to service providers, participants noted that currently local service providers do not have a mechanism in place.

There was no discussion or evidence of the informal sharing of newly discovered or known vulnerabilities with a group who can further disseminate the information across sectors. However, Samoa is in the process of establishing a CIRT as part of the National Cybersecurity Strategy to "*identify combat, respond and manage Cyberspace Threats or Attacks*"[127]. With

[127] MCIT. (2016) 'MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021'. Available at: http://www.samoagovt.ws/wp-content/uploads/2017/02/MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021.pdf (Accessed 14 May 2018), p8.

the recent membership of PaCSON, Samoa will establish the capacity to sharing vulnerability information with other CIRT teams across the region[128].

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Standards, Organisations, and Technologies*, the following set of recommendations are provided to Samoa. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

ADHERENCE TO STANDARDS

R5.1 Adopt a nationally agreed baseline of cybersecurity related standards and good practices that address identified risks across the public and private sectors, including: risk management and information risk management; managing Internet infrastructure; software development; procurement; ecommerce; electronic business transactions; and authentication.

R5.2 Ensure that defined standards and guidance include: consideration of cybersecurity risks in all procurements of goods and services; secure configuration of networks, devices, systems and applications; digital identify management, including authentication; and secure software development practices (including websites) where applicable.

R5.3 Define and revise a list of endorsed cybersecurity products for government agencies to use that address identified requirements and risks.

R5.4 Establish a software development forum for the discussion and sharing of methodologies that focus on data integrity and resilience.

R5.5 Promote defined cybersecurity standards, good practices and the use of endorsed products across all sectors.

R5.6 Revise existing public-sector awareness campaigns regarding policy and guidelines and actively communicate requirements and expectations.

[128] IT Brief. (2018) ‘The Pacific Cyber Security Operational Network is now in action’.
Available at: https://itbrief.com.au/story/pacific-cyber-security-operational-network-now-action/ (Accessed 15 May 2018).

R5.7 Actively enforce policy, especially regarding digital identity management, including authentication.

R5.8 Measure and evaluate the implementation of defined standards, good practices and endorsed products in the public and private sectors.

R5.9 Revise the agreed baseline of cybersecurity related standards and good practices based on regular risk assessments that are informed by stakeholders, including the National CIRT.

INTERNET INFRASTRUCTURE RESILIENCE

R5.10 Establish or assign an institution responsible for developing Internet infrastructure policy and assessing the deployment of technology and processes.

R5.11 Enhance coordination and collaboration regarding resilience of Internet infrastructure across public and private sectors.

R5.12 Encourage ISPs to establish and publish service level agreements for services and report on service outages.

R5.13 Define metrics for continuously measuring service reliability, collect data and publish reports to show trends.

R5.14 Identify, describe and revise assets, processes, roles, responsibilities and skills required for formally managing National infrastructure, informed by a national risk assessment that minimises single point of failure.

R5.15 Conduct regular assessments of the assets, processes, roles, responsibilities and skills required for managing Internet infrastructure to ensure that practices follow international standards, guidelines, good practices and address identified risks.

R5.16 Raise awareness with end users to enable them to identify services that have successfully implemented defined standards and good practices.

R5.17 Measure and evaluate the use of use of ecommerce, electronic transactions and authentication for analysing trends.

SOFTWARE QUALITY

R5.18 Establish or assign an institution responsible for developing software quality policy and assessing practices across sectors.

R5.19 Enhance coordination and collaboration regarding software quality, functional requirements and security across the public and private sectors.

R5.20 Identify and describe all ICT assets in use by the public sector and critical infrastructure to inform risk assessments. This should include, but not be limited to: applications; platforms (environment in which applications are executed); and how information is exchanged and stored.

R5.21 In collaboration with public, critical infrastructure and private-sector partners, develop and revise a catalogue of applications and platforms that have been evaluated for software quality, functional requirements and security risks across sectors.

R5.22 Address gaps in identified applications and platforms that have not been evaluated for software quality, functional requirements and security risks.

R5.23 Revise policies for assessing software for deficiencies to include guidance on measuring, evaluating and reporting the impact on usability and performance.

R5.24 Develop and revise policies and processes for regular updating and patching operating systems and applications for all government agencies to use.

R5.25 Promote across all sectors the policies and practices regarding: use of the catalogue of evaluated platforms and applications; updating and patching; and assessing software for deficiencies.

R5.26 Measure and evaluate the implementation of: evaluated platforms and applications; regular updating and patching; and assessment of software for deficiencies.

R5.27 Regularly review and share collected findings on software deficiencies and use the data to inform revisions of the catalogues of evaluated platforms and applications.

TECHNICAL SECURITY CONTROLS

R5.28 Establish or assign an institution responsible for developing technical control policy and assessing the deployment of such controls across sectors.

R5.29 Adopt standards and good practices for selecting, configuring and deploying technical controls based on risk assessments for private and public sectors and end users.

R5.30 Expand technical security controls to include, but not be limited to: using centralised software update services (for example, Windows Server Update Services); Sender Policy Framework (SPF) DNS records; daily off-line backup; encryption; network segmentation; centralised logging; configuration management; media sanitisation; Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS); host based firewalls; application white listing; hardening user applications; restricting administrative privileges; and using multi-factor authentication where possible[129].

R5.31 Revise the technical security control framework based on regular risk assessments that include the assessment of the effectiveness of controls, informed by the National CIRT and penetration tests where possible.

R5.32 Consider use cases in risk assessments that include, but are not limited to: removable media; cloud services; remote work; and use of personal devices.

R5.33 Consider using Data Loss Prevention controls in areas dealing with sensitive and confidential information.

R5.34 Develop incentives for the use of defined standards and good practices for technical controls in all sectors, including the offering of antimalware software by ISPs and banks as part of their services.

R5.35 Promote standards and good practices for technical controls for use by private and public sectors and end users.

R5.36 Measure and evaluate the implementation of defined standards and good practices by users, private and public sectors.

[129] Australian Signals Directorate. (2017) 'STRATEGIES TO MITIGATE CYBER SECURITY INCIDENTS – MITIGATION DETAILS'. Available at: https://asd.gov.au/infosec/top-mitigations/mitigations-2017-details.htm (Accessed 15 May 2018).

CRYPTOGRAPHIC CONTROLS

R5.37 Establish or assign an institution responsibility for developing cryptographic control policy and assessing the deployment of such controls across sectors.

R5.38 Adopt standards and good practices for the configuration and implementation of cryptographic controls for protecting information in transit and at rest, including the use of algorithms detailed in the CNSS's Advisory Memorandum on Information Assurance 02-15 (CNSSAM 02-15) where possible.

R5.39 Embed the requirement for the defined standards and good practices for protecting information in transit and at rest in procurement policy.

R5.40 Promote the use of defined standards and good practices for protecting data in transit and at rest across all sectors.

R5.41 Consider incentives to promote the adoption of cryptographic controls across sectors.

R5.42 Measure and evaluate the implementation of cryptographic controls for protecting data in transit and at rest across all sectors.

CYBERSECURITY MARKETPLACE

R5.43 Establish or assign an institution responsible for assessing the local cybersecurity market place.

R5.44 Assess the need to develop a local cybersecurity market place based on a national risk assessment, including the availability, affordability and supply chain of cybersecurity goods and services.

R5.45 Adopt standards and good practices that are informed by regular risk assessments for: the assessment of cybersecurity related financial risk; the development of secure software (including websites); and infrastructure development.

R5.46 Promote across all sectors the use of the defined standards and good practices for: the assessment of cybersecurity related financial risk; the development of secure software (including websites); and infrastructure development.

R5.47 Measure and evaluate the implementation of defined standards and good practices.

RESPONSIBLE DISCLOSURE

R5.48 Establish or assign an institution responsible for developing responsible disclosure policy and assessing the processes in place.

R5.49 In consultation with key sector stakeholders, develop and implement a responsible disclosure policy and processes for reporting bugs and vulnerabilities across sectors.

R5.50 In consultation with key sector stakeholders, develop and implement a policy and processes for sharing bug and vulnerability reports across sectors.

R5.51 Promote the adoption of the bug and vulnerability policies and processes across all sectors.

R5.52 Measure and evaluate the use of the bug and vulnerability policies and processes.

ADDITIONAL REFLECTIONS

Even though the level of stakeholder engagement in the review was more limited than we might have hoped, which limits the completeness of evidence in some areas, the representation and composition of stakeholder groups was, overall, balanced and broad.

This was the 24th country review that we have supported directly.

Global Cyber Security Capacity Centre

Oxford Martin School, University of Oxford

Old Indian Institute, 34 Broad Street, Oxford OX1 3BD,

United Kingdom

Tel: +44 (0)1865 287430 • Fax: +44 (0) 1865 287435

Email: cybercapacity@oxfordmartin.ox.ac.uk

Web: www.oxfordmartin.ox.ac.uk

Cybersecurity Capacity Portal: www.sbs.ox.ac.uk/cybersecurity-capacity