



JANUARY 2020

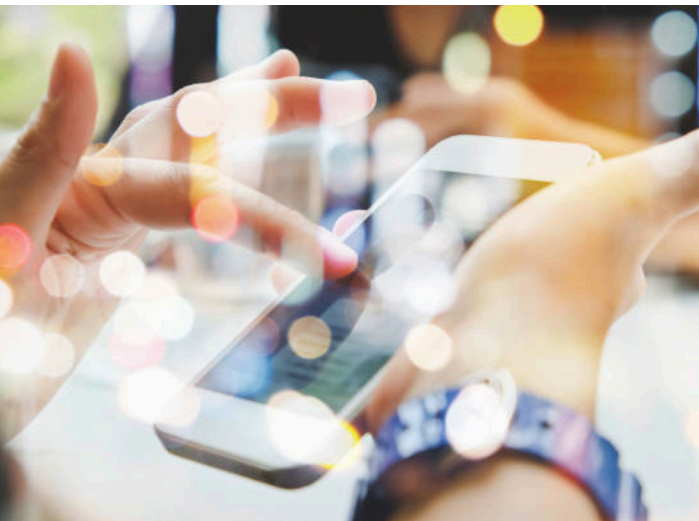
Pacific Islands Cyber Security Standards Cooperation Agenda



Foreword

There is a long and robust history of collaboration between Standards Australia and its Pacific neighbours, which has paved the way for one of the most important discussions of our generation, that is cyber security.

The area of cyber security has exploded onto the scene in recent years as technology continues to expand its reach and capability at an extraordinary rate. This has resulted in an estimated 5 billion people owning mobile phones by 2017,¹ with these devices becoming much cheaper and much more powerful each year. In 2018, the Australian Bureau of Statistics found that 85% of households have access to the internet.² As of 2019, around 4.4 billion people across the world are active internet users, representing



58% of the global population.³ The world is very well connected to the cyber sphere, and those who are not are catching up quickly. But this connectivity comes with many dangers and can make anyone more vulnerable to the ever-increasing cyber security threats today. This is particularly so when cyber progress is not accompanied with equal appreciation for cyber standardisation, regulation and safety.

As the peak standards development organisation in Australia and the national member of international standards bodies such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), Standards Australia is well equipped to deliver essential cyber security

assistance to Pacific nations undergoing impressive digital transformation. Hence, the Cyber Security Regional Standardisation Enhancement Program was developed out of a desire to understand the current cyber ecosystem in the Pacific, and to see how international standards could help enhance the security and stability in the region.

Through close collaboration and consultation, Standards Australia – along with various industry experts, organisations and country representatives – was able to help each Pacific nation identify their priorities in terms of cyber security and standardisation, and to develop comprehensive plans for the future. The ultimate goal of the program and this accompanying agenda is to ensure that the Pacific region continues to thrive, and in doing so is able to protect its industries, governments and citizens from the ever-increasing cyber security threats.

On behalf of Standards Australia, I would like to thank the various organisations, experts and government officials who contributed their invaluable time and expertise to the program and the publication of this agenda. This program demonstrates the immense power of bringing together people with such a variety of backgrounds who all share a common interest: cyber security.

Adrian O'Connell

Chief Executive Officer
Standards Australia

1 <https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/05/The-Mobile-Economy-2018.pdf>

2 <https://www.abs.gov.au/Technology-and-Innovation>

3 <https://www.statista.com/statistics/617136/digital-population-worldwide/>

Executive Summary

Vision

The Cyber Security Regional Standardisation Enhancement Program was designed to strengthen cyber security in the Pacific region by enhancing each country's engagement with the ISO/IEC 27000 Information Security Management System series of international standards.⁴

Over time and after several consultations with country representatives, this vision was revised to reflect the overriding priority of the Pacific region; to harmonise with and implement these standards.

This document, the *Pacific Islands Cyber Security Standards Cooperation Agenda*, outlines the way forward for the project. It describes how each country intends to continue to engage and collaborate with relevant stakeholders to progress this vision and reach their stated goals.

Enablers and Stakeholders

The project was centred around the five nominated Pacific Island Countries of Fiji, Papua New Guinea, Solomon Islands, Tonga and Vanuatu.

Standards Australia consulted with partners including various national standards bodies (NSBs), the Australian Federal Police and the Australian Cyber Security Centre (ACSC) to develop the first cyber security standards agenda of its kind for the Pacific Islands. Funding was provided by the Department of Foreign Affairs and Trade (DFAT) for the Cyber Security Regional Standardisation Enhancement Program.⁵

Key Priorities

Each country came to the table with an open mind and a willingness to instigate change. Naturally the program changed over time and hence its priorities and values followed suit. However, there were three major outcomes that remained key tenants of the program, which were:

- To enhance the Pacific region's access to funding, resourcing and technical assistance to promote market awareness and participation in cyber security standards development, adoption and use across the Pacific region;
- To help the Pacific nations gain a greater understanding of the value of cyber security standards, and ensure that projects under development in the ISO/IEC JTC 1/SC 27 take into account each country's specific needs and priorities; and
- To facilitate ongoing dialogue, information sharing and relationships between the Pacific nations, Australia, Australian industry and others such as cyber security experts and peers.

While cyber security has been a somewhat emergent topic amongst the Pacific Island countries before now, the impressive level of engagement in the Cyber Security Regional Standardisation Enhancement Program from all participants is one indication of a promising future for the topic.

⁴ <https://www.iso.org/isoiec-27001-information-security.html>

⁵ **Disclaimer:** This publication has been funded by the Australian Government through the Department of Foreign Affairs and Trade. The views expressed in this publication are the author's alone and are not necessarily the views of the Australian Government.

Contents

Foreword	2
Executive Summary.....	3
About This Agenda.....	6
Background and Context	6
Introduction.....	6
What is cyber security?	7
Why is cyber security important in the region?.....	7
What is ISO/IEC JTC 1 and SC 27?	8
Why are cyber security standards important?.....	8
What is the ISO/IEC 27000 series?	8
Methodology	12
Cyber Security Standards in Fiji.....	13
Purpose.....	13
Background and Trade Information	13
Information Technology Uptake.....	14
Cyber Security and ICT: Policy and Legislative Environment	14
Standards Uptake and Engagement.....	15
Standards Gaps and Challenges.....	15
SWOT Analysis	16
Conclusion.....	16
Cyber Security Standards in Papua New Guinea.....	17
Purpose.....	17
Background and Trade Information	17
Information Technology Uptake	17
Cyber Security and ICT: Policy and Legislative Environment	18
Standards Uptake and Engagement	20
Standards Gaps and Challenges.....	21
SWOT Analysis	21
Conclusion.....	26
Cyber Security Standards in Solomon Islands.....	27
Purpose.....	27
Background and Trade Information	27
Information Technology Uptake	28
Cyber Security and ICT: Policy and Legislative Environment	29
Standards Uptake and Engagement	29
Standards Gaps and Challenges.....	30
SWOT Analysis	30
Conclusion.....	34

Continues...

Cyber Security Standards in Tonga.....	35
Purpose.....	35
Background and Trade Information	35
Information Technology Uptake	36
Cyber Security and ICT: Policy and Legislative Environment	37
Standards Uptake and Engagement	38
Standards Gaps and Challenges.....	39
SWOT Analysis	39
Conclusion.....	43
Cyber Security Standards in Vanuatu	44
Purpose.....	44
Background and Trade Information	44
Information Technology Uptake.....	44
Cyber Security and ICT: Policy and Legislative Environment	45
Standards Uptake and Engagement.....	46
Standards Gaps and Challenges.....	46
SWOT Analysis.....	47
Conclusion.....	51
Conclusions and Next Steps.....	52
Annex A – Cyber Security Standards	53
Annex B – Forum Attendees.....	55

About This Agenda

This agenda is the product of extensive engagement with five nominated Pacific Island countries. The purpose was to develop and deliver a program that is capable of strengthening cyber security in the Pacific region by enhancing information technology (IT) security infrastructures and harmonising each country's national standards with the ISO/ IEC 27000 Information Security Management System series of international standards.



Together, the participants – Fiji, Papua New Guinea, Solomon Islands, Tonga and Vanuatu – participated in the Cyber Security Regional Standardisation Enhancement Program, including a two-day forum held in April 2019 led by Standards Australia, with support from DFAT, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The objective of the forum was primarily to build market understanding of cyber security and develop the participants' knowledge on the ISO/

IEC 27000 series of standards. The forum also provided an invaluable opportunity to share information, network and develop gap assessments in relation to each country's current cyber security ecosystem.

This agenda plots the course taken to achieve these objectives during the Cyber Security Regional Standardisation Enhancement Program. The program involved extensive stakeholder engagement, numerous country visits, a needs analysis process and a two-day forum with guest speakers ranging from the Australian Cyber Security Centre (ACSC), the Australian Federal Police to the Australia Pacific Business Council and more.

The aim of this agenda is to explore what was learned during the program, and more importantly what strategies need to be implemented in the future to improve the participants' IT security infrastructure and harmonise cyber security standards. This document presents the context, the methodology, the findings and the next steps required to achieve the goals of the Cyber Security Regional Standardisation Enhancement Program.

Background and Context

Introduction

The growth of the digital economy is unprecedented and is providing Australia and our Pacific neighbours with enhanced access to the global market.

The digital economy contributed AUD 79 billion, or 5.1 per cent of Australia's Gross Domestic Product (GDP) in 2017. This is estimated to continue to grow rapidly to hit \$139 billion or 7.3 per cent of GDP by 2020.⁶ In the Pacific, regional digital trade is growing at an exponential rate, with transactions in Asia and the Pacific region increasing at an average of 50 per cent annually and making up nearly half of global transactions. In our region, Current Average Growth Rate (CAGR) of new digital

⁶ <https://www.afr.com/technology/australian-digital-economy-valued-at-79b-20150324-1m6gxn>

economy-enabling technologies could create up to USD 625 billion in economic activity per year by 2030, representing 12 per cent of the region's total projected GDP.

With up to 80 per cent of global trade (USD 4 trillion annually) affected by standards or associated technical regulations, it is important that Australia and our Pacific neighbours participate in national and international standardisation processes. Standards provide a global architecture for defining both general and sectorial market referentials and are critical for supporting and enabling regional and global trade. The standards also foster deeper international economic integration, promote international market competitiveness, innovation, efficiency and support consumer health and wellbeing.

In the digital economy, cyber security is becoming an increasingly complex and difficult challenge. While the digital economy is opening up new opportunities for Australia and our region to boost productivity and grow innovation, it has also made Australia one of the world's most targeted countries for cyber crime. Australia is the fourth most nominated country in the world for spear-phishing attacks, the ninth most nominated country for ransomware and 1.5% of all cyber-attacks in the world are launched out of Australia.⁷ The same threats exist for our Pacific counterparts, yet they are not as well positioned to deal with these threats.

In 2017, DFAT launched its first International Cyber Engagement Strategy, in which Standards Australia is listed as the lead agency for supporting the development of international standards that improve cyber security and encourage harmonisation of standards of digital products. As part of this, Standards Australia also has a critical cyber security standards capacity building role within the Pacific region.

What is cyber security?

Cyber security encapsulates measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means. According to the Department of Home Affairs, effective cyber security keeps information safe and networks and systems secure. It also allows the technology industry to thrive and is fundamental to growth in the global economy. All of us – citizens, businesses and government – have a role to play when it comes to cyber security.

Why is cyber security important in the region?

Cyber security is an ever-growing issue for the Pacific region. With the struggle for economies to keep pace with the rapidly evolving cyber security technologies, products and solutions become a primary barrier of cyber protection. This risk is further compounded by the fact that cyber security is still a relatively nascent sector, with infrastructure and knowledge severely lacking. Very few countries in our region have implemented national cyber security strategies, and not many organisations are equipped to keep up with ever-evolving threats and regulations. The Pacific is an ideal environment for cyber criminals to thrive in due to high digital connectivity, contrasted with low cyber security awareness, growing cross-border data transfers and weak regulations. A recent CISCO study found that in the Asia-Pacific, many companies receive up to 10,000 threats a day.⁸ That means 6 threats are received every minute. Of the companies surveyed, 69% receive more than 5,000 threats a day. However, only 50% of the total numbers of alerts are investigated.⁹

7 <https://www.businessinsider.com.au/heres-how-important-cyber-security-is-to-australia-2016-4>

8 [The Cisco 2018 Asia Pacific Security Capabilities Benchmark Study.](https://www.cisco.com/c/en/us/solutions/cyber-security/capabilities-benchmark-study.html)

9 <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/overview>



What is ISO/IEC JTC 1 and SC 27?

The joint technical committee of ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission), ISO/IEC JTC 1, Information Technology, is the place where the basic building blocks of new technologies are defined and where the foundations of important ICT infrastructures are laid.

In addition to this well-established focus of work, ISO/IEC JTC 1 positions itself as a system integrator to complement its current program, especially in areas of standardisation where many consortia/fora are active.

Currently there are over 3,100 published ISO/IEC standards developed by committees in JTC 1 comprised of some 4,500 registered technical experts from around the world.

ISO/IEC JTC 1/SC 27, IT Security Techniques, is the subcommittee of ISO/IEC JTC 1 responsible for helping the fight against the growing problems of cyber security attacks, information and identity theft and online fraud. It provides organisations with solutions to protect their sensitive and critical information and personal data, regardless of the business sector and organisational structure.

Why are cyber security standards important?

Information security is of paramount importance to all organisations. With the increasing development of, and reliance on, information technology, it is imperative that organisations protect their critical data assets both for their own operational needs and to ensure the continuing confidence of their clients, customers and partners. Alignment with the ISO/IEC 27000 series can secure their critical assets, manage risks more effectively, and improve and maintain customer confidence. In doing so, they increase the trust and confidence of users, underpinning continued investment in innovative technologies and driving continued economic growth. Also, by sharing best practices and by specifying state of the art techniques and mechanisms, they can assist in improving the quality of processes and also the quality of solutions to help businesses, administrations and individuals.

What is the ISO/IEC 27000 series?

The ISO/IEC 27000 series of standards provides best practice recommendations on information security management – the management of information risks through information security controls – within the context of an overall information security management system (ISMS). These standards outline general methods, management systems requirements, techniques and guidelines for information security and privacy.

The standards are considered critical for:

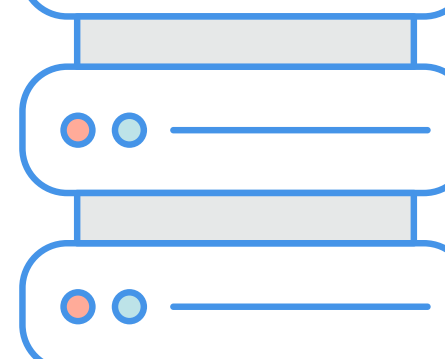
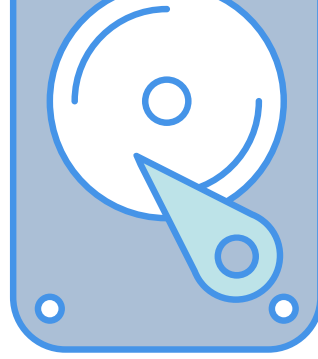
- building trust and assuring security and privacy in the Information and Communications Technology (ICT) domain, particularly for supporting cross border transactions and enabling digital trade;
- building business, consumer and government confidence and trust in digital services; and

- helping organisations keep information assets secure through the management of security. Assets include financial information, intellectual property, employee details or information entrusted by third parties.

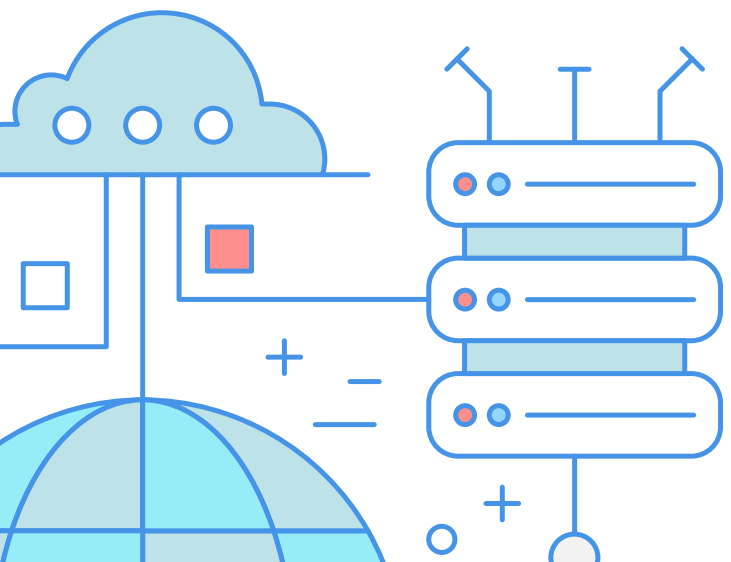
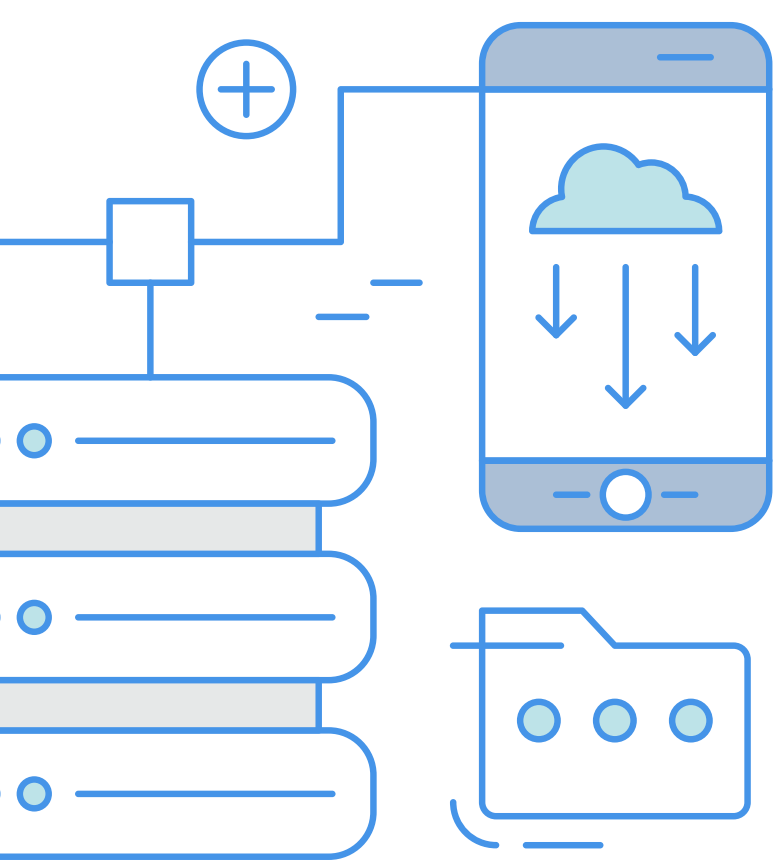
For example, as a foundation of the series, the ISO/IEC 27001 is the best-known standard, providing requirements for an information security management system (ISMS). An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It considers people, processes and IT systems by applying a risk management process. It can help small, medium and large businesses in any sector keep information assets secure.

The ISO/IEC 27000 series is published by ISO and IEC. The ISO/IEC JTC 1/SC 27 subcommittee is responsible for the maintenance of the ISO/IEC 27000 series. Like other ISO management system standards, certification to individual ISO/IEC 27000 standards is optional, not mandatory. The number differs depending on the source, but according to one there are currently 45 standards included in the [ISO/IEC 27000 series](#), which are listed in “Annex A – Cyber Security Standards” on page 53. It is important to note that the area of cyber security is constantly evolving with new technological advances and this will be factored into consultations and the needs assessment process.

Key



deliverables⁺





The intended deliverables for this project include:

1. To build awareness of the ISO/IEC 27000 series, identify country cyber security standardisation needs and conduct a regional **cyber security standards needs analysis** process with nominated NSBs and stakeholders.
2. Convene a **two-day regional Cyber Security Forum** in Sydney to build understanding, knowledge and information sharing opportunities on the ISO/IEC 27000 series.
3. Produce a **regional cyber security standards “agenda”** with tangible country-specific recommendations for further engagement and participation, adoption and development of international information security standards; and identify capacity building activities based on the standards agenda.

The outcomes of this initiative for nominated countries include:

1. Access to funding, Standards Australia’s resourcing and technical assistance to promote awareness and participation in cyber security standards development, adoption and use across the Pacific region;
2. Helping organisations secure financial, intellectual property, employee details entrusted by third parties through the use of internationally aligned cyber security standards;
3. Building trust and assuring security and privacy in the ICT domain, particularly for supporting cross border transactions and unlocking future digital trade;
4. Building business, consumer and government confidence and trust in digital products and services;
5. Increasing the Pacific region’s engagement in the growing work of ISO/IEC JTC 1/SC 27 to gain a greater understanding of the value of cyber security standards, and also ensure that projects under development take into account countries’ specific needs and priorities; and
6. Facilitating ongoing dialogue, information sharing and relationships with cyber security experts and peers.

Methodology

1	Preparation and project planning	<ul style="list-style-type: none"> a Develop project concept note (background, scope, objectives, benefits/value, context, nominated countries identified, methodology, timelines, stakeholder analysis, risks, deliverables and outcomes). b Secure partners, sponsors and supporters. c Project organisation established. d Project implementation plan developed (based on point a. above). e Operationalise project implementation plan.
2	Engagement, communications and on-boarding	<ul style="list-style-type: none"> a Invitation letters and information memorandum sent to nominated countries. b Partners, sponsors and supporters' briefings and presentations. c Follow-up nominated countries as necessary. d Nominated countries accept the offer to participate e Nominated countries on-boarded.
3	Needs analysis	<ul style="list-style-type: none"> a Initial research and fact-finding to understand gaps and needs. b Questionnaire to nominated countries (addressing information gaps from the initial research). c In-country visits and stakeholder interviews (to gain support, clarify any outstanding issues from the questionnaire and prepare representatives from the nominated countries for the forum). d Detailed needs analysis conducted (using information from initial research, questionnaire and in-country visits). e Draft agenda developed.
4	Initial interventions and refinement of needs analysis	<ul style="list-style-type: none"> a Regional cyber security forum designed and planned (including agenda, keynote presenters, logistics and other details). b Meeting notice and agenda sent to nominated country representatives including travel arrangements and details of any support offered. c Confirm attendees for the forum. d Forum held (key capacity building delivered, and ongoing needs identified during the forum). e Forum outcomes analysed and documented.
5	Finalisation	<ul style="list-style-type: none"> a Refine the standards agenda as a result of the needs identified during the forum. b Issue the draft agenda to nominated countries for comments and feedback (particularly recommendations). c Update agenda as a result of the feedback. d Issue final agenda. e Project close and debrief.



Cyber Security Standards in Fiji

Purpose

This document outlines an approach to cooperation and collaboration between Fiji and Standards Australia in progressing the application of cyber security standards within the Pacific region. This is an unofficial document.

Background and Trade Information

The Republic of Fiji consists of over 300 islands with a combined population of approximately 905,502 people. In recent years, Fiji has experienced the best growth cycles since its independence, recording nine years of consecutive growth between 2009 and 2018. This upward trajectory is expected to continue this year, making it ten straight years of growth.

The fundamental contributing factors to Fiji's sustained growth include major structural and economic reforms, the promotion of trade and economic growth, the creation of business-friendly environments and government initiatives (such as tax breaks and incentives) combined with accommodative policies. In 2015, Fiji developed a Trade Policy Framework to guide its trade, industry, investment and economic agenda to 2025.

Fiji has also dedicated itself to a programme of wider integration and participation. Fiji is an active member of the following organisations:

- Melanesian Spearhead Group (MSG).
- African and Caribbean Group of States (ACP).
- World Trade Organization (WTO – members since 1996).
- UN Human Rights Council.
- Pacific Islands Forum.

Fiji also has the following trade agreements in place:

- United Kingdom-Pacific Interim Economic Partnership Agreement (UK-Pacific IEPA).
- European Union-Pacific Interim Economic Partnership Agreement (EU-Pacific IEPA).
- Melanesian Spearhead Group Trade Agreement (MSGTA).
- Pacific Closer Economic Relations (PACER).
- Pacific Island Countries Trade Agreement (PICTA).
- South Pacific Regional Trade and Economic Co-operation Agreement (SPARTECA).
- World Trade Organisation Agreement.

Classified as an upper-middle-income country,¹⁰ the Fijian government continues to focus on the alleviation of poverty, social empowerment, rural development and expansionary fiscal policies. The country's service, construction, manufacturing, retail and tourism sectors continue to grow, with the latter being the main driver for growth.

¹⁰ <https://data.worldbank.org/country/fiji>

Information Technology Uptake

Fiji is an established hub of the Pacific and has positioned itself to become an attractive country for ICT investments. The country is connected to the Southern Cross Cable fibre optic networks, which affords it world-class connectivity.

Recently, the country has demonstrated a significant focus on incentivising the ICT sector. For example:

- Income tax exemptions apply for operators who set up Internationally Accredited ICT Training Institutions;
- Income tax exemptions also apply for any Communication Technology (ICT) operator that is operating in the declared Kalabu Tax Free Zone; and
- Small ICT start-ups can access a 150 per cent deduction on all start-up costs.

These policies have placed Fiji in a competitive position to attract ICT investment at all levels. The country has leveraged its geographic location (between Asia and the United States), its high-end IT infrastructure and competent workforce to promote Fiji as a capable, connected and dynamic society.



Fiji is a leader in the area of ICT development in the Pacific region. After the Savusavu Cable landing station was unveiled in late 2018, around 95% of the country gained access to a fast and durable internet connection, which was reflected in the World Bank's 2017 statistics showing that 50 per cent of the Fijian population uses the internet.¹¹ This statistic is predicted by some to grow to 99% by 2030.¹²

The country has consistently invested heavily in the ICT industry and has seen rapid infrastructure growth in recent

years. In Fiji's 2019-2020 National Budget, almost \$40 million was allocated for the development of the ICT sector, and a number of tax incentives were announced in the 2018-2019 Budget, such as a 250 per cent tax deduction policy for ICT Research and Development expenditure.¹³ The 2019-2020 Budget further added to the existing incentive package in the ICT industry by removing the minimum employee and export requirements, and by removing the \$1,000 license fee.

Cyber Security and ICT: Policy and Legislative Environment

Fiji has been quite active in recent years when it comes to cyber security, and further work is being done. For example, Fiji was elected 2nd Vice-Chair of the Executive Committee of the Commonwealth Telecommunications Organisation (CTO) in 2016. Fiji was elected as the 1st Vice-Chair in 2017 and is currently the Chair of CTO.

With regard to the institutions that have been established within Fiji, the Director of Public Prosecutions and the Fiji Police Force play important roles. The Financial Intelligence Unit (FIU) is the leading agency in Fiji that is primarily responsible for preventing and detecting money laundering and terrorist funding activities.

11 <https://data.worldbank.org/indicator/IT.CEL.SETS?start=1960>

12 <http://www.parliament.gov.fj/wp-content/uploads/2018/05/Standing-Committee-on-JLHR-Report-on-the-Online-Safety-Bill-No-7-of-2018-part-1.pdf>

13 <https://www.frsc.org.fj/wp-content/uploads/2018/11/merged.pdf>

The Fijian Government is currently working with the Council of Europe on the finalisation of the cybercrime legislation, which is aligned to the provisions in the Budapest Convention.

The Fijian criminal justice authorities have hitherto used the current laws along with international best practices adopted by courts to obtain telephone records and other forms of electronic evidence to successfully prosecute cybercrimes and electronic evidence cases. These laws include the Crimes Act 2009, Mutual Assistance in Criminal Matters 1997, and the Telecommunications Act 1999. Fiji also has an Online Safety Act 2018 which establishes the Online Safety Commission and promotes online safety, deters harmful electronic communications including cyberbullying, and creates criminal offences.¹⁴

These policy and development efforts are notable and have been complemented by an increase in enhanced training and education in the sector.

Standards Uptake and Engagement

Fiji is yet to take up and engage in national or international cyber security standards. Notably, Fiji is an active, observing member of the ISO through its Department of National Trade Measurement and Standards (DNTMS) and is a member in various ISO Technical Committees and Policy Development Committees.

Fiji is ranked at 121 out of 175 countries on the ITU Global Cybersecurity Index (2018), the second highest of all the participating Pacific Island Countries.¹⁵ Fiji is also one of two Pacific countries in this project to be a full member of the Pacific Area Standards Congress (PASC). As mentioned earlier, Fiji actively participates in Asia-Pacific CERT Cyber Security Forums such as Pacific Cyber Security Operational Network (PACSON).

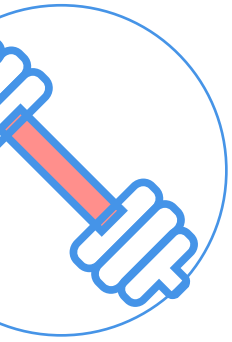
Standards Gaps and Challenges

Fiji has been able to undertake ICT development and international engagement. However, there is a need to develop equivalent cyber security standards and regulation. The notable gaps are:

- There is no specific cyber security legislation;
- There are no national, sector-specific cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals;
- There are no national cyber security standards; and
- Fiji is not a member of IEC or a participant in ISO/IEC JTC 1.

14 <https://www.laws.gov.fj/Acts/DisplayAct/2462#>

15 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf



SWOT Analysis

Through consultation with stakeholders in Fiji the decision was made not to publish the findings from the SWOT Analysis, including the recommendations and objectives for the short, medium and long term.

DNTMS and stakeholders in Fiji remain committed to these objectives and will continue to work closely with relevant stakeholders like Standards Australia to progress standards development activities related to cyber security.

Conclusion

Fiji has been recognised for leading the way in ICT development amongst the Pacific nations, a hard-won title achieved through impressive and consistent government policies and active community engagement.

Given the steps taken by the Fijian government in continuing to address the connectivity issues, the next step is to match this development with appropriate cyber security policies and standards.

The Fijian government has been aware of the importance of implementing cyber security standards and conducting constant and effective legislative reviews and this is evident in the implementation of consistent and steady policies. Through its network and partnerships, Fiji has already made strides to improve its standards uptake and address the gaps in its cyber legislation. Fiji can leverage its ICT infrastructure and investments to overhaul its cyber security policies efficiently and effectively.





Cyber Security Standards in Papua New Guinea

Purpose

This document outlines an approach to cooperation and collaboration between Papua New Guinea and Standards Australia in progressing the application of cyber security standards within the Pacific region. This is an unofficial document.

Background and Trade Information

Papua New Guinea lies in the southwestern Pacific, consisting of a mainland and six hundred islands that span across 452,860 square kilometres. With a population of around 8.3 million, life in Papua New Guinea ranges from traditional village-based centres to modern urban cities such as Port Moresby, although to this day around 80 to 85 per cent of the population rely on farming as their livelihood.

Classified as a Small Island Developing State (SIDS), Papua New Guinea is an active member of the international realm and sustains membership with the Melanesian Spearhead Group (MSG), the South Pacific Regional Trade and Economic Cooperation Agreement (SPARTECA), the Pacific Island Countries Trade Agreement (PICTA) and – since 1996 – the World Trade Organisation. The country's major import partners are Australia, Singapore, China, Japan and Malaysia.

Papua New Guinea experienced a decade of impressive economic growth in the mid-2000's, driven by formal employment opportunities, strong government expenditure and revenue, conservative fiscal policies, activities such as the Papua New Guinea LNG project and high international prices for its exports.

However, this growth peaked in 2014, after which Papua New Guinea suffered from budget deficits and falling commodity prices. Currently, the government continues to implement macroeconomic stability policies and growth has slowed, with GDP decreasing in 2018 from its five-year average of 7 per cent to 2.9 per cent. The country faces other challenges, for example, the estimated 2 million citizens living in poor conditions or facing hardship, and the high urban unemployment rate, particularly amongst young people.^{16,17,18}

Information Technology Uptake

A participant in several multilateral forums including APEC, International Telecommunication Union (ITU), the Asia-Pacific Telecommunity (APT) and the Pacific Island Telecommunications Association (PITA), Papua New Guinea has taken a leading role in championing ICT development and has done so through cooperation and persistence. The uptake of ICT in Papua New Guinea has increased significantly in the last decade; for example, the usage of mobile phones in the country rose from 4.7 per cent to 47 per cent between 2007 and 2015 alone.¹⁹ An estimated 4,018,000 citizens today have mobile cellular subscriptions, and the numbers continue to rise.

16 2015 Pacific Regional MDG Tracking Report; https://rrrt.spc.int/sites/default/files/resources/2019-01/2015_Pacific_Regional_MDGs_Tracking_Report.pdf

17 <https://dfat.gov.au/geo/papua-new-guinea/Pages/papua-new-guinea-country-brief.aspx>

18 <https://dfat.gov.au/trade/resources/Documents/png.pdf>

19 <https://data.worldbank.org/indicator/IT.CEL.SETS>

Because of the uniquely challenging terrain of Papua New Guinea, improvements like these are only possible with dedicated government input into ICT infrastructure and policies. In July 2012, the country connected to a 10GBps fibre-optic gateway from Madang to Sydney and in late 2018 agreed to join the Coral Sea Cable System, an undersea fibreoptic cable connected between Sydney, Port Moresby and Solomon Islands. According to DFAT, “the Coral Sea Cable System (CS2) will deliver faster, cheaper and more reliable communications infrastructure, affording both countries significant economic and development benefits.”²⁰

The country’s Vision 2050 National Plan focusses heavily on ICT development and education. It sets out imperatives including:

- For community colleges, vocational schools and technical colleges to expand and increase the ICT knowledge and skills within the country;
- To establish an Industrial Technology and Development Institute (ITDI) for the promotion of aggressive and cooperative research amongst institutions and higher education;
- To bridge the digital and technology divide and using political will to direct the appropriate agencies towards reducing the significant gap in socioeconomic inequalities.

Papua New Guinea is clearly dedicated to advancement in the ICT sector. In May 2017 the first Neutral Internet Exchange Point (IXP) was opened, representing a huge step in enhancing the affordability and quality of internet connectivity in local communities. Again, in March 2018 the Government teamed up with the University of Papua New Guinea, the Government of India and the United Nations Development Programme (UNDP) to create the Centre for Excellence in Information Technology (CEIT), enabling a model learning environment and enhancing education software, curriculum and teaching facilities. Later that year the country also held its first significant and successful ICT event, the Papua New Guinea Digital Economy Forum.²¹

There is still plenty of room for improvement. Papua New Guinea’s cost of data ranks among the highest in the world, with a study in 2015 showing that a 2GB per month broadband costs more than 100% of the average monthly income.²² Indeed, due to affordability constraints and the continued challenge of infrastructure, only 11 per cent of the population uses the internet.²³

Cyber Security and ICT: Policy and Legislative Environment

In 1992, the government of Papua New Guinea tabled the National Policy on Information and Communications (NPIC), focussing on the spread of information capabilities across the country. At the time, cyber security was not an anticipated threat and was mentioned sparingly. Over the years, the increased uptake of ICT and the liberalisation of the ICT market meant that Papua New Guinea was more connected to the world through cyber space, utilised more advanced technology and increased social interaction tenfold. The country also became more exposed to cybercrime threats from around the world.

With this, the government saw the need to develop a new policy, producing the National ICT Policy 2008. However, apart from a few cybercrime recommendations, there has been little progress in the country towards cyber security. That is until the government launched the Cybercrime Policy in October 2015, designed to define the instruments

20 <https://dfat.gov.au/about-us/publications/Pages/supporting-the-future-digital-economies-of-papua-new-guinea-and-solomon-islands.aspx>

21 <http://www.looppng.com/tech/first-successful-ict-event-png-76867>

22 <http://strategies.nzl.com/industry-comment/affordability-of-internet-access-in-the-pacific-2015>

23 <https://data.worldbank.org/indicator/IT.NET.USER.ZS?start=1960>

and mechanisms that may be used to address cybercrime in the country, and to determine general principles and considerations related to future legislative and policy responses to cybercrime.

Additionally, the Cybercrime Act 2016 was passed, which built on pre-existing policies and supported other legislative pieces such as the National Information and Communications Technology Act 2009 (NICTA). It was criticised for its unnecessary penalties and lack of effective enforcement capacity. A 2017 study by the Australian Strategic Policy Institute (ASPI) found that the country's approach to cyber governance continues to be limited and patchy, citing issues such as lack of public awareness and limited infrastructure.²⁴

However, it is noted that the criticism of the Cybercrime Act led to comparatively vibrant public discussion around cyber security. With free media commentary and growing access to community blogging, awareness around cyber security was brought to more areas of the country, which signified an important step in the right direction.

Other areas of cyber maturity have also been recognised. For example, the creation of a specialised Intelligence Unit and a cybercrime taskforce in the Royal Papua New Guinea Police in 2014 has made considerable impacts on the detection and prevention of cybercrime. Similarly, Papua New Guinea Customs has notably cooperated with the National Information and Communications Technology Authority (NICTA) to prevent illegal ICT importation.

The Integrated Government Information System (IGIS)²⁵ program is a development of centralised and shared government information system, for all of government. As phase one of the program commissioned back in 2014, National Capital District based agencies are integrated to a centralised government national data centre, providing shared services of voice, internet access and email hosting as phase 1, with the view to standardise government services. Phase two and three is to extend connectivity to more sub-national level agencies in provinces and districts. Part of the IGIS vision is to enhance departmental integration and coordination, which is vital if the country truly hopes to develop a robust cyber security environment. Currently, groups ranging from the Department of Communication and Information (DCI), NICTA, the Police Force, the Office of the Public Prosecutor, the Department of Prime Minister and Papua New Guinea Customs are responsible for different aspects of cyber security. However there is a greater need to synchronise not only cyber security efforts within the country, but also with international standards, legislation and best practices. Despite considerable efforts to tackle the rising cyber security challenges the country continues to face issues that are common among the Pacific islands, including a low level of awareness and education and lack of training and resources.



Nevertheless, these challenges have not deterred the government from pursuing its cyber security vision. For example, when establishing the country's Computer Emergency Response Teams (CERT), Papua New Guinea held a two-day workshop for network operators, financial, legal and academic representatives and government

24 <https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017>

25 <http://gopngicttalk.org/category/igis>

agencies to discuss the nation's cyber security future and to gain input in the development of an action plan. Papua New Guinea has also been part of and held successful events, including the Connected Papua New Guinea Technology Summit (CPNGTS19)²⁶ and the Girls in ICT events. Papua New Guinea also launched the country's National Cyber Security Centre in November 2018, and the government is currently formulating a National Cybersecurity Policy and Strategy.

Standards Uptake and Engagement

With the recognised need for better cyber security policies within the country, Papua New Guinea is working hard to catch up to the requisite level of standards implementation that comes hand in hand with the growing level of ICT usage.

An essential part of this effort is the creation of relevant bodies to oversee and implement the government's policies. For example, the National Institute of Standards and Industrial Technology of Papua New Guinea (NISIT) is a government statutory national standards body that was established under the NISIT Act 1993. It covers technical standards, conformity assessment schemes and productivity and technical barriers to trade within the country.



Established in 2010, the National Information & Communications Technology Authority (NICTA) is responsible for the regulation and licensing of ICT in Papua New Guinea. The Authority's goal is to actively collaborate with NISIT, as well as other regional and international standards organisations and academia, in order to develop effective conformity and interoperability (C&I) systems and processes within Papua New Guinea.²⁷ Then in 2017, the government unveiled a Computer Emergency Response Team (CERT), which works to promote awareness

and provide assistance and coordinated responses to cyber security incidents within Papua New Guinea. Other important engagements have occurred in the area of cyber security standardisation, including the recent Memorandum of Understanding made between Papua New Guinea and Australia in relation to cyber security cooperation²⁸

In terms of international standards, Papua New Guinea is a member of the following:

- International Organization for Standardization (ISO) – Correspondent Member.
- International Electro-technical Commission (IEC) – Affiliate Member.
- International Telecommunication Union (ITU) – Full Member.
- Pacific Islands Forum – Full Member.
- APEC's Sub-Committee on Standards and Conformance (SCSC) – Full Member.
- APEC TEL – Full Member.
- The Pacific Area Standards Congress (PASC) – Full Member.
- Pacific Accreditation Cooperation (PAC) – Associate Member (PAC and APLAC have been merged into the new regional body called the Asia-Pacific Accreditation Cooperation or APAC).
- Asia-Pacific Telecommunity (APT) – Full Member.

²⁶ <http://www.connectedpng.com/technology-summit-2019/>

²⁷ <https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2016/Oct-CandI2016/CAICT2016/PNG.pdf>

²⁸ <https://dfat.gov.au/international-relations/themes/cyber-affairs/Pages/mou-between-papua-new-guinea-and-australia-relating-to-cyber-security-cooperation.aspx>

Standards Gaps and Challenges

Taking into consideration the country's appropriate legal, technical and organisational measures as well as their capacity building and cooperation, the ITU Global Cybersecurity Index ranked Papua New Guinea 139 out of 175 countries in 2018.²⁹ Papua New Guinea has no cyber security professional certification, no national standards or cyber security frameworks³⁰ and does not participate in any ISO Technical or Policy Development Committees³¹ nor does it hold a membership with IEC.

While the country has made strides in developing bodies to oversee the standardisation of cyber security, there is an opportunity to improve the internal capacities of these bodies and the collaboration between government departments and relevant stakeholders.

There is a long way to go before Papua New Guinea reaches cyber maturity, and the country has recognised the imperative to work on formulating and adopting relevant international cyber security standards, although this will be a lengthy process that requires stakeholder input, the establishment of working groups and a supporting national cyber security policy.

SWOT Analysis

During the forum, key participants from Papua New Guinea were asked to analyse their country's strengths, weaknesses, opportunities and threats (SWOT). Below is a summary of their response.

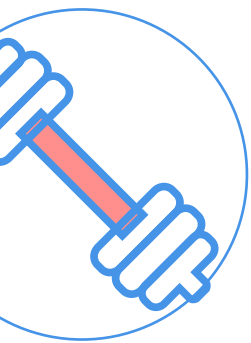
Strengths:

- Papua New Guinea Computer Emergency Response Team (PNGCERT) already established in February 2018.
- Papua New Guinea state of art National Cyber Security Centre is operational as of October 2018.
- Papua New Guinea Cybercrime Act established in 2016.
- National ICT Sector Coordinating Committee was established in October 2018, with a National ICT Roadmap guiding Digital Transformation, which covers cyber security under Digital Safety as one of six pillars.
- Government is prioritising and supporting cyber security development.
- Government supports National Institute of Standards and Industrial Technology (NISIT) and recognises the value of standards.
- Improved skills and knowledge of cyber security in ongoing development programs, with development partners including Cyber Security Regional Standardisation Enhancement Program and PaCSON.
- Increase in ICT graduates in educational institutions and in other ICT initiatives, including 'Women in ICT' program.
- High digital illiteracy in PNG that limits Papua New Guinea being exposed to the cyber space and hence cyber incidences.

29 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

30 Note, the country is currently drafting cybersecurity policy and strategy.

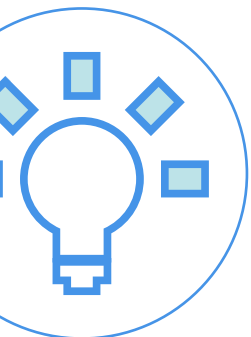
31 Note, the country is an observer in some of these.





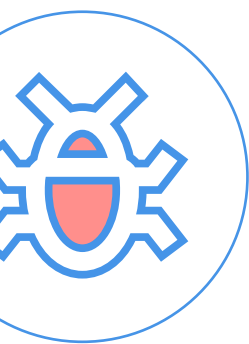
Weaknesses:

- Lack of in-country resources and expertise.
- Lack of public communication or awareness plan and unclear demarcation of responsibilities.
- No public awareness, or awareness from the police force.
- Lack of unified coordination across the whole of government due to lack of overarching policy.
- Lack of government cyber security standards, guideline or policy.
- Lack of enforcement and prosecution capabilities with the mandated law and justice sector agencies, including digital forensic in police, prosecution capability in courts.
- Lack of police capacity (more of a focus on traditional crime).
- Lack of fundamental enabling policies and guidelines, including electronic evidence guidelines and general data protection policies.
- Lack of centralised government procurement policies.
- Lack of established business continuity planning or incident response plan in the event of cyber attacks or incidents. These capacities are currently under development.
- High digital illiteracy resulting in users being comprised, misinformed or misrepresented due to the low level of online awareness and education of cyber safe practices and how and where to seek assistance.
- Government lacks the resources to fully participate in international standards; currently, Papua New Guinea is only a correspondent member of the ISO and an affiliate member of IEC.



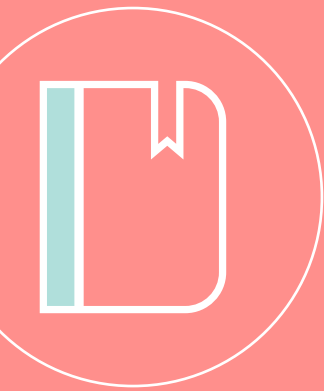
Opportunities:

- Papua New Guinea's cooperation with the Australian Federal Police and organisations such as the Pacific Islands Law Officers' Network (PILON) has given the country an opportunity to build its enforcement and investigations capacity.
- The country is continuing to build a network of 'best practice' standards and certification with organisations such as APEC, Standards Australia and ISO/IEC.
- The government and public sectors of Papua New Guinea have recognised that the sharing of resources for a common goal is an invaluable process and must be prioritised.
- By continuing to provide training and development, there is a great opportunity to unlock vital skills and expertise in the ICT and cyber security sector.
- With numerous university and school programs available that focus on ICT and cyber security, the message will reach younger generations and help to improve the future of cyber security in the country.
- The Coral Sea Cable System, linking Sydney to Port Moresby and Honiara, creates shared interests between Papua New Guinea and Australia in protecting and enhancing the country's connectivity and cyber safety.
- Papua New Guinea is dedicated to continuing to work with Australia through organisations such as DFAT, Standards Australia and Department of Communication and Arts to reach the ultimate goal of national and region and international standards and ICT security cooperation.



Threats:

- Once again, the lack of whole of government coordinated approach between government bodies and organisations means initiatives and programs are not effective or sustained after development partners' assistance ends.
- Without strong central government procurement guidelines, there is a threat that received ICT solutions may be substandard or vulnerable and exploited in future (especially ICT solutions that donated or provided as aid under bilateral arrangements)
- Without procurement guidelines and central coordination, ICT systems from a multitude of sources and donor agencies may be costly to integrate or support interoperability, resulting in high total cost of ownership to the recipient post installation.
- Where there is lack of accredited and relevant national curriculum for ICT or technology in the country, many highly talented nationals complete training overseas and many are known to have not returned, resulting in country elite 'brain drain'. The drain is compounded with exposure to better employment conditions and living environments outside of Papua New Guinea. Further for those ICT talents in Papua New Guinea, many better talents are found in the industry and not the government as comparatively, the government remuneration conditions are less attractive.
- Inevitably, Papua New Guinea's enhanced ICT infrastructure, such as increasing connectivity and internet speed and quality of service, may now provide a more cyber conducive environment, which may see an increase in internet based opportunity as well as threats.
- Papua New Guinea is not a part of the Budapest Convention on Cybercrime treaty is missing out on much potential initiatives enjoyed under this cooperation.



Agenda Recommendations

Out of this SWOT analysis process, a number of key findings emerged, which were turned into recommended action plans for the country moving forward. These were:

- 01 Raise Awareness of Cyber Security Standards:** A Coordination Unit is being established by NISIT and the Department of Communication and Information with the goal of identifying and collating other cyber security initiatives and priorities and aligning them into a clear, whole of government action plan within respective agencies.
- 02 Establish a Technical Committee:** NISIT will develop a Technical Committee focused on Cyber Security Standards and best practice, bringing together experts from a variety of sectors in order to set priorities for the adoption and development of standards in Papua New Guinea. Target by July 2019.
- 03 Develop Awareness Materials with Australian Federal Police and relevant active agencies:** This goal leverages off existing materials and relationships in order to build awareness amongst the public and business sector. It will be the responsibility of the Department of Communication and Information.
- 04 Disseminate Awareness Materials:** The Department of Communication and Information as a mandated government agency is responsible for government media communication to lead awareness in collaboration with other agencies, including Office of Censorship, PNGCERT and NICTA to promote public awareness.
- 05 Finalise National Cyber Security Policy and Strategy:** This Policy will soon be finalised by the Department of Communication and Information. This will involve developing a framework and/or guide for relevant stakeholders to follow.
- 06 Ensure Third-Party Review of National Cyber Security Policy and Strategy:** In order to ensure the Policy effectively captures all elements of cyber security and standardisation, NISIT and NICTA are given the responsibility to ensure third parties are able to review and submit commentary on the Policy.

In addition to this, the participants acknowledged broader objectives for the short, medium and long term.

Short term

- Establish an effective Central Coordination Unit that can utilise strong implementation mechanisms;
- Effectively utilise existing training and awareness building programs, for example, AFP PILON;
- Establish NISIT's Technical Advisory Committee with a focus on cyber security standards development and engage in collaboration with other ongoing cybersecurity initiatives; and
- Engage with the National Procurement Commission to assess and develop central procurement guidelines.

Medium term

- Monitor and evaluate the new Central Coordination Unit and ensure it has established future work plans;
- Ensure the training and awareness building programs focus on standard and international best practices and are tailored to the Papua New Guinea context;
- Using the new NISIT Technical Advisory Committee, build a work program for the potential adoption of the ISO/IEC 27000 series, and perhaps other relevant standards;
- Work further with the National Procurement Commission to develop national procurement guidelines;
- Develop an Incidence Response and Business Continuity Framework; and
- Follow up status with Papua New Guinea's Foreign Affairs and Trade (FAT) and drive Papua New Guinea's membership to Budapest Convention.

Long term

- Build and integrate cyber education and awareness into local curriculums and training programs in collaboration with other relevant community members;
 - Implement the ISO/IEC 27000 series and other relevant international standards that were identified as necessary by the NISIT Technical Advisory Committee;
 - Review the Cybercrime Act 2016 to address any gaps;
 - Support the development of education and awareness programs around procurement practices and the implementation of national procurement guidelines; and
 - Increase the monitoring of all cable networks and their activity.
-

Conclusion

Papua New Guinea understands and recognises the importance of increased connectivity and ICT uptake, leading the way in a rise of economic and social development and inclusion and enhancing the country's growth and prosperity in the face of many unique challenges. However, there is an opportunity to respond with enabling policies, legislation, standards and guidelines, technical capacity, education and awareness to systematically manage the inherent risks that follow; that is the growing threats from cyber security and exposure to cybercrime. There have been a number of important, small steps taken in recent years, including the introduction of the Cybercrime Act and the development of a CERT. However, to date Papua New Guinea still lacks cyber security standards, both from the policy and operational standpoint.

Driven by APEC preparation as the APEC host in 2018 and including the increased awareness on the digital economy, the government has now recognised digital safety as an important agenda with future development and hence has increased its efforts and priorities towards cyber security. This is evident in increased development initiatives and participation in forums and programs with the aim of enhancing its understanding of cyber security and developing a minimum baseline for cyber defence and awareness, inline international standards and best practices. Developing cyber security standards is one of the key focus areas to reach Papua New Guinea's ambitions of cyber safety. There are many environmental, political and economic challenges the country shall face; however, the Papua New Guinea government has demonstrated that it is serious and focused on making Papua New Guinea a modern, cyber-safe digital economy.





Cyber Security Standards in Solomon Islands

Purpose

This document outlines an approach to cooperation and collaboration between Solomon Islands and Standards Australia in progressing the application of cyber security standards within the Pacific region.

The document is not an official document and has not been endorsed by the government of Solomon Islands. It is focused on current government initiatives to progress cyber security in Solomon Islands. Despite this, it still has application for the private sector.

Background and Trade Information

Solomon Islands lies in the southwest of the Pacific Ocean, an archipelagic state that spans across nearly 1,000 islands and totals approximately 28,400 square kilometres of land mass. The population is estimated at 611,343 and consists of 63 distinct languages and varying communities.

After many years of unrest and violence, the country has now stabilised. Both the economy and trade have balanced out and grown, with the GDP reaching 7.9 per cent in 2010. Although this number has tended to decline over the years, growth rates have remained relatively stable, sitting at 3.5 per cent in 2017.

Solomon Islands developed its first National Development Strategy in 2016, setting out the country's strategic direction for development and its efforts to build capacity in areas such as trade, infrastructure and disaster resilience. Other helpful reforms have also been initiated, for example, the Customs Act review that is aimed at improving compliance measures, and reforms in areas such as competition and investment that are hoped to result in benefits for the general public and businesses. The National Transport Plan (2007-2026) and the National Infrastructure Investment Plan (2013) demonstrate the country's dedication to improving its transport and infrastructure sectors.

Solomon Islands has been a member of the World Trade Organisation since 1996 and, as a small island state with limited domestic capacity, it relies heavily on trade. The country created a Trade Policy Framework (TPF) to guide its trade, industry, investment and economic agenda over the coming years and has begun focussing on improving its commodity facilities in areas such as cocoa, fisheries and forestry.

One of the Pacific's poorest countries, Solomon Islands faces challenges including the high service delivery costs caused by its small and geographically dispersed population, ethnic conflict, poor infrastructure, volatile property ownership and under-developed labour skills. The country was rated 4th in the 2018 World Risk Index, facing severe environmental issues caused by climate change and natural disasters including cyclones, earthquakes, tsunamis and volcanoes. Indeed, the country incurs an estimated \$20 million in damage per year from earthquakes and cyclones alone.^{32,33}

32 <https://www.gfdrr.org/en/solomon-islands>

33 <https://dfat.gov.au/trade/resources/Documents/solo.pdf>

Information Technology Uptake

The ICT sector within Solomon Islands had a slow start but has made significant progress. The government recognised the need to remove barriers to investment and competition in the ICT sector and to implement soft regulations. As a result, the Telecommunications Act 2009 was enacted to reduce barriers to entry, facilitate interconnection and access and prohibit anti-competitive conduct. The ICT market was liberalised, and soon the total population covered by ICT networks rose from 11 per cent in 2010 to 89 per cent in 2015.³⁴ The Act also established the Telecommunications Commission of Solomon Islands (TCSI), an independent expert regulatory body responsible for the economic and technical management of the country's ICT sector.

Since this time, mobile penetration has grown rapidly, and the government has continued its path towards ICT growth. For example, in 2011 Solomon Islands Government Information and Communication Technology Support Unit (ICTSU) was mandated to coordinate and deliver all government ICT projects, and the 2013 National Infrastructure Investment Plan had a strong focus on addressing the continued ICT gap.

Solomon Islands is also signed on to the Coral Sea Cable System. This project is designed to not only connect Honiara to Sydney and Port Moresby but also build enhanced domestic network links that will connect the capital to the rest of the country through provincial hubs such as Auki, Noro and Taro.

In September 2017, Solomon Islands Minister of Communication and Aviation, Mr Peter Shanel Agovaka, launched the country's National Information Communication and Technology Policy. The framework for this policy was drafted using the Telecommunications and ICT Development Program, which ran from August 2010 to March 2015 in collaboration with the World Bank Group and DFAT. Other outcomes of this program included the submission of draft ICT policies and the introduction of a National Numbering Plan in 2014. The program also helped to increase the number of mobile subscribers per 100 people from 8 per cent to 66 per cent between 2010 to 2015.³⁵



Solomon Islands has been focused on facilitating the increased access to reliable and affordable ICT services to the general population and regulating competition in the market. Departments have been commissioned and policies implemented to improve connectivity and social inclusion through ICT. However, there is still a significant gap despite reasonable improvements in areas such as mobile phone penetration; as of 2017, only 12 per cent of the population uses the internet.³⁶ What is more, there is the growing threat from cybercrime.

34 <http://documents.worldbank.org/curated/en/253541468296466114/pdf/ICRR-Disclosable-P113148-06-10-2016-1465565211071.pdf>

35 <http://documents.worldbank.org/curated/en/253541468296466114/pdf/ICRR-Disclosable-P113148-06-10-2016-1465565211071.pdf>

36 <https://data.worldbank.org/indicator/IT.NET.USER.ZS>

Cyber Security and ICT: Policy and Legislative Environment

Cyber security has been increasing in importance within Solomon Islands for a few years. There are no specific laws on cybercrime, electronic transfers, data privacy or security; however, the government has indicated an intent to introduce these soon. The Ministry of Communication and Aviation is responsible for developing and coordinating the country's cyber policies. They have been actively working with the recently formed National Cyber Security Working Group to improve cyber security.

In the international sphere, Solomon Islands has engaged with various initiatives and forums around cyber security, such as the Melanesian Spearhead Group (MSG), Cyber Safety Pasifika, Pacific ICT ministerial meetings and the Asia-Pacific Network Information Centre (APNIC). The country signed a Memorandum of Understanding with Indonesia in late 2017, agreeing to cooperate in preventing, detecting, and combating issues including cybercrime and corruption. In 2018, the Australia Solomon Islands Technology for Development Challenge was launched, seeking ideas on how the country can connect to and support its young people to maximise their skills and education, and to access jobs across the country and internationally.

Unlike most other Pacific nations in this Cyber Security Standards Agenda, Solomon Islands does not have a specialised Cyber Crime Unit. However, various members of the Police Force have undergone in-depth cybercrime training programs, have actively participated in initiatives such as Cyber Safety Pasifika and have indicated clearly that the Force is aware of the increasing threat and is aiming to engage internationally to address it.

There is evidence of inter-departmental collaboration on cyber security issues, but representatives from Solomon Islands have confirmed that the dialogue is limited. There is an opportunity to improve collaboration between government and stakeholders including schools, businesses and consumers.

The digital world is progressing steadily in Solomon Islands. Fortunately, the country has shown that it understands the importance of matching any ICT development with equivalent security policies and regulations, and not letting the technology get ahead of the government. However, the country faces challenges in acting on this awareness and implementing appropriate strategies.

Standards Uptake and Engagement

There is a lack of engagement when it comes to regulating and enforcing standards for cyber security in Solomon Islands. The current rank on the ITU Global Cybersecurity Index (2018) is 160 out of 175 countries.³⁷ The country has shown that it is willing to engage in this area and many opportunities lie ahead..

Importantly, the country has showcased its desire to implement a framework for the certification of organisations and infrastructure in accordance with the ISO/IEC 27000 series. Solomon Islands also hopes to develop a National Cyber Security Strategy or Framework, which will include an approach for implementing relevant cyber security standards, and discussions have been made around building a Cyber Security Centre and a Cyber Security Operation Centre for the country.

37 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Standards Gaps and Challenges

There is an important opportunity for Solomon Islands to implement strong and effective cyber security standards. Currently, the most notable gaps in standards uptake and engagement for Solomon Islands include:

- It has no national CERT.
- It has no cyber security regulation.
- There are no national, sector-specific cyber security frameworks for the certification and accreditation of national agencies and public sector professionals.
- There are no national, sector-specific cyber security frameworks for implementing internationally recognised cyber security standards.
- It has no national standards or cyber security frameworks.
- It is not a member of ISO, nor is it a participant in any ISO Technical Committees or Policy Development Committees.
- It is not an IEC member.
- It is not an ISO/IEC JTC 1 participant.
- It is not a member of the Pacific Area Standards Congress (PASC).
- It is not a member of the Pacific Accreditation Cooperation (PAC).
- It is not a member of the APEC – Sub-Committee on Standards and Conformance (SCSC).
- Solomon Islands was a member of the Pacific islands' PacCERT. However, it ceased operation due to lack of funding.

SWOT Analysis

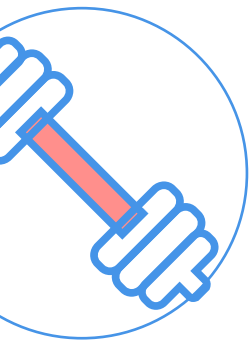
During the forum, key participants from Solomon Islands were asked to analyse their country's strengths, weaknesses, opportunities and threats (SWOT). Below is a summary of their response.

Strengths:

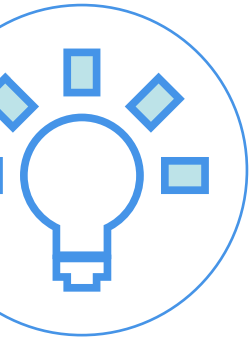
- A Disaster Recovery Site has been established for the government.
- The government has established a Centralised Data Centre to manage all government systems and applications.
- Additionally, a Demilitarised Zone (DMZ) has been established to protect the internal network nodes in these Data Centres, adding another security layer to the local area network.
- Solomon Islands' inclusion in the Coral Sea Cable network has elevated the significance of cyber security for the country and increased the focus.
- Funding is provided by DFAT to upskill ICT government employees through cyber security skills and knowledge.

Weaknesses:

- There is a continued lack of accredited, skilled experts and professionals around cyber security.
- There is a lack of coordination between the bodies and departments involved in cyber security, including the Royal Solomon Islands Police, the Attorney General Chamber, the Ministry of Communication and Aviation, Solomon Islands Government ICT Support Unit, the Prime Minister's Office and regulatory bodies.
- The country lacks a Cyber Security Strategy or Framework as well as specific legislation to address cyber security.
- Solomon Islands has no official cyber security standards.
- There is minimal public awareness around cyber security issues.

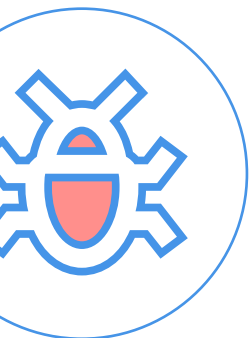


- There is no National Standards Body.
- 80 per cent of the population live in rural areas, with limited access and knowledge of cyber security issues and geographic challenges to the communication of information and spreading of awareness.



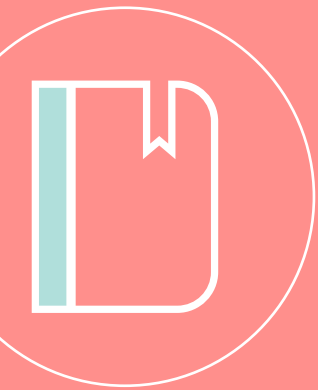
Opportunities:

- The country hopes to adopt the ISO/IEC 27000 series of standards.
- The continued engagement and networking with international standards bodies and experts such as Standards Australia.
- Building trust with the general public and delivering robust systems to protect and educate them.
- A Cyber Security Centre has been proposed in collaboration with the Australian Government.
- A project is underway to build a Security Operation Centre in collaboration with Solomon Islands Government ICT Support Unit.
- The country hopes to integrate cyber security education into the curriculum of tertiary and secondary schools.
- The government plans to work with Solomon Islands Chamber of Commerce to discuss cyber security issues and address the needs for business and investments.
- The Coral Sea Project will help the country to promote public awareness around cyber security.



Threats:

- Coming hand-in-hand with the Coral Sea Project is the increased exposure to cybercrime and attacks.
- Changes in the Australian government policy could affect Solomon Islands' funding for cyber security projects.



Agenda Recommendations

Out of this SWOT analysis process, several key findings emerged, which were turned into recommended action plans for the country moving forward. These were:

01 Consult with Relevant Stakeholders: To obtain their view on the country's cyber security needs and standards and specific comments on sectors, the Ministry of Communication and Aviation and the Government ICT Support Unit should consult with Solomon Islands Cyber Security Working Group and industry stakeholders.

02 Develop a Standard Network Security Guideline: This guideline will help the network to operate on a more cohesive and effective level, potentially reducing the risk of cybercrime through attacks like Denial of Service (DoS).

03 Investigate a Potential ISO/IEC 27000 Series Framework: In collaboration with Standards Australia, the Government ICT Support Unit, the Ministry of Communication and Aviation and Solomon Islands Cyber Security Working Group must discuss the development of a framework for the certification of organisations and infrastructure, establishing the baseline and identifying any weaknesses.

04 Investigate a Cyber Security Incident Reporting tool: This tool could be developed by the Police Cyber Security team with the Government ICT Support Unit and Internet Service Providers (ISP's) in order to help respond to incidents and manage risks in time to address them and reduce their impact.

05 Establish a National Cyber Security Standards Taskforce: This Taskforce would be responsible for planning and developing a cyber security standards framework, enabling the country to have a coordinated approach to cyber security initiatives. This taskforce may be a subcommittee of Solomon Islands Cyber Security Working Group.

In addition to this, the participants acknowledged broader objectives for the short, medium and long term.

Short term

Continue the cyber security professional training program;

Bring together all the key decision-makers and stakeholders in order to coordinate a cyber security strategy, including the Royal Solomon Islands Police, the Attorney General Chamber, the Ministry of Communication and Aviation, Solomon Islands Cyber Security Working Group, Solomon Islands Government ICT Support Unit, the Prime Minister's Office and regulatory bodies;

Develop a National Cyber Security Strategy or Framework and develop an approach for implementing standards;

Create a standards implementation guide for (a) the government, (b) critical infrastructure and (c) businesses; and

Discuss the potential for a framework for certification of organisations and infrastructure in accordance with the ISO/IEC 27000 series.

Medium term

Prepare a cyber security awareness program to spread amongst government employees, schools and the general public; and

Conduct a cyber security audit with assistance from appropriate experts for the Data Centre and all government departments.

Long term

Develop and implement specific cyber security legislation and regulations; and

The Ministry of Communication and Aviation and Solomon Islands Cyber Security Working Group to liaise with the Ministry of Education to develop a program on cyber security in Solomon Islands National University as well as primary and secondary curriculums.

Conclusion

There are opportunities ahead for Solomon Islands to grow in digital maturity. The levels of connectivity and social inclusion across the country have been impressively growing in recent years, and the government has made improvements in its cyber security governance. Government initiatives have proven that awareness of cyber security is spreading, and the country's international engagement and networking are commendable. However, the general public's awareness is still extremely limited and centred mainly around the increase of connectivity and infrastructure.

The government through the Ministry of Communication and Aviation and Solomon Islands Cyber Security Working Group must continue to push for a cyber security focus and open dialogue between its departments and relevant stakeholders including businesses and schools to communicate the importance of this topic. With a lack of skills and training, a lack of standards or legislative frameworks and minimal coordination between relevant bodies, Solomon Islands may face challenges ahead in bolstering its cyber security environment. However, the country has shown many positive indications that it can reach its goals.





Cyber Security Standards in Tonga

Purpose

This document outlines an approach to cooperation and collaboration between Tonga and Standards Australia in progressing the application of cyber security standards within the Pacific region. This is an unofficial document.

Background and Trade Information

Tonga is an archipelago in the South Pacific made up of 176 islands that are divided into four main groups: Tongatapu, Ha'apai, Vava'u and the Niua. The Polynesian population totals approximately 106,000 and is spread across only 36 of the Islands, while roughly another 100,000 Tongans live abroad mainly in Australia, New Zealand and the United States.

With the GDP currently lying at 3.2 per cent, Tonga is classified as a middle-income developing country and relies heavily on foreign aid and remittances from expatriates. Although Tonga's economy is quite open and vulnerable to external shock, the country is stable, particularly since embarking on several political reforms in the aftermath of civil unrest in 2006. Tonga then acceded to the World Trade Organisation in July 2007 and has been a strong supporter of the system, despite being one of the smallest member economies.

The country's goods exports are valued at around \$2 million, consisting mostly of agriculture and fisheries but also including a small manufacturing sector, tourism and other services. While the former is relatively modest, it has potential for expansion particularly with the increased use of technology and social media. Tonga's primary trading partners are Australia, Fiji, New Zealand, Japan and the United States.

Some state-owned enterprises have been established in several sectors including telecommunications, transport, utilities and banking. However, the country has a backlog of reforms and reviews that are necessary to modernise and make relevant its legal and regulatory frameworks, from agriculture to transport to ICT.



Importantly, however, Tonga has been pushing through a period of rapid change in its economic and regulatory environment in recent years. The government committed itself to achieving positive results and acknowledging the unique challenges and complexities the country faced in terms of improving its infrastructure and industry and boosting its economy. Despite these challenges, Tonga has made some of the best progress in the Pacific with the Millennium Development Goals, the United Nations strategy aimed at combatting poverty, hunger, disease, illiteracy, environmental degradation and gender discrimination.^{38,39}

38 https://www.who.int/topics/millennium_development_goals/about/en/

39 <https://dfat.gov.au/geo/tonga/Pages/tonga-country-brief.aspx>

Information Technology Uptake

The government of Tonga understands the inherent value of ICT development, especially in a country that is relatively isolated. The hope for many years has been to improve the affordability and accessibility of telecommunications and to utilise this to mitigate some of the country's economic constraints, particularly considering how important high-speed internet has become to the functioning of modern economies around the world. Indeed, Tonga was amongst the first Pacific Island countries to deregulate its telecommunications sector in 2003. Essentially, ICT development offers new economic opportunities within Tonga, as well as the opportunity to make connections to larger markets and utilise new avenues for delivery of services both regionally and internationally.

However, prior to 2013 Tonga was dependant on satellite connectivity that was not only expensive by comparison but also unable to meet the growing demands for connectivity. Hence, in 2013 Tonga invested in a new submarine fibre-optic cable, connecting to the Southern Cross Cable Network (SCCN) in Fiji. Along with the project, a 'Fibre Optic Awareness' media campaign was also launched in 2013 in conjunction with Tonga's National ICT Day.

The Tonga-Fiji cable was commissioned in 2013 and the domestic cable to Tonga's outer Islands was completed in 2018, providing substantially higher bandwidth capacity and reduced international bandwidth costs. However, there have been issues with the cable, including a 12-day outage in January 2019 which plunged the country in isolation, and the lack of rural distribution. In addressing these issues, the Tongan government signed a 15-year deal in April 2019 with Kacific Broadband Satellites Group, granting the country access to higher-speed connectivity and giving 89 outer islands access to bandwidth from the high-speed Kacific1 satellite.



In May 2009, a major step towards ICT development came the creation of the Ministry of Information and Communications (MIC). This government body is responsible for, among other things, the promotion of ICT as an enabler of national development and as a platform for ensuring that ICT services meet national needs and international standards.

In 2012 the government embarked on an e-government initiative aimed at equipping its departments with the latest technology and tools to advance ICT development in Tonga. Then in 2013, efforts to reform the

ICT sector and its regulatory regime began in earnest with the Tongan government and the MIC, with significant support also coming from the World Bank.

In 2009, the National ICT Policy was approved, recognising that a connected society has invaluable benefits but also poses new challenges and threats. This Policy "outlines the National ICT Vision and the key objectives that are to be achieved through effective use of ICT and the development of new skills and jobs that will enable our country, and our

people, to participate in and benefit from the global networked economy” and sets out six supporting pillars for Tonga’s ICT programme.⁴⁰

Over the years, Tonga has actively sought to develop its ICT capabilities, both through domestic policy efforts and through international networking and initiatives. Tonga has been part of the Pacific Regional ICT Ministerial Meetings for several years, and in May 2016 the country held an Asia-Pacific Network Information Centre (APNIC) Workshop on Computer Emergency Response Teams. Earlier in 2016 Tonga’s first Computer Emergency Response Team (certTonga) was established to ensure a safe and secure digital environment by providing incident response, vulnerability testing and security consultation and advice.

Nevertheless, there is plenty of room for improvement in Tonga’s ICT development and uptake. The country is still suffering from a skills shortage, and education around information technology is limited. While some ICT-related legislation already exists, it is not specific enough to tackle current technology issues, let alone future ones, and the government has struggled to properly enforce these laws.

Some sectors, such as the tourism industry, have already come to rely on technology without the equivalent regulations and understanding that is necessary to protect consumers and industry. The country was ranked at 110 out of 165 countries on the ICT Development Index (2017) and internet usage in Tonga sits at 41%, a figure which will continue to rise.

Cyber Security and ICT: Policy and Legislative Environment

While the country of Tonga is still in the early stages of developing and implementing specific cybercrime legislation, policies and strategies, there has been an impressive level of engagement with the topic in recent years, particularly on the international platform.

In 2010, a meeting of Pacific Ministers responsible for ICT was convened by the Secretariat of the Pacific Community (SPC) and held in Tonga. Together, the Pacific ICT Ministers endorsed a Framework for Action on ICT for Development in the Pacific and set out a target for the Pacific Island countries to have cybercrime legislation in place by 2015.

In April 2011, Tonga hosted the Pacific Cybercrime Legislation Workshop in collaboration with the Australian Attorney-General’s Department, the Council of Europe and the SPC, with a focus on supporting the plight to strengthen cybercrime legislation in the Pacific Island countries.

Between 2013 and 2016, Tonga was part of the GLACY Project (Global Action on Cybercrime) and reaped the benefits of judicial training, legislative advice and law enforcement capacity building. To this day, Tonga continues to be one of the priority countries under the updated GLACY+ Project. The dedication to such forums led Tonga to become the first Pacific Island to accede to the Convention on Cybercrime (Budapest Convention) in May 2017, and the country is currently in the process of drafting a bill to align with the Convention.

At the same time, Tonga hosted the Pacific Islands Law Officers’ Network Cybercrime Workshop, a workshop focussed on enhancing the effectiveness of law enforcement in tackling cybercrime. While Tonga does not have a specific Cybercrime Unit in the Police Force, its Transnational Crime Unit (TCU) was established in 2003 and was later transformed into the Serious Organized Transnational Crime Unit (SOTCU) in 2010, which is currently responsible for tackling cybercrime.

40 <http://pippr.victoria.ac.nz/bitstream/handle/123456789/27/Tonga%20-%20national%20ICT%20policy.pdf?sequence=1>

Domestically, Tonga has also developed cyber security initiatives. For example, the Cyber Challenge Taskforce was created in December 2013 and tasked with providing a coordinated approach to technology concerns in the country. The Taskforce includes a committee made up of various government ministries, key stakeholders, private sector businesses and non-government organisations (NGO's), a unique partnership that has allowed Tonga to "mobilize its resources, identify key challenges, and coordinate relevant programmes, working groups [and] review laws."⁴¹

Tonga has only one piece of legislation that specifically deals with cybercrime, being the Computer Crimes Act 2003. The Acts covers the combatting of computer crime, governs the collection and use of electronic evidence and gives the Tonga Police the authority to investigate, detect and prosecute computer crimes. Just recently, an updated Computer Crimes Bill 2019 will be introduced to the Legislative Assembly.

Other Tongan legislation that touches on or may impact cybercrime includes:

- The Communications Act 2000;
- Communications Act 2015;
- Communications Commission Act 2015;
- The Evidence Act 2000;
- Tonga Police Act;
- Criminal Offences (Amendment) Act 2012;
- Pornography Control Act 2002;
- Defamation Act 1988;
- Copyright Act 2002; and
- Tongan Internet Corporation Registration Act 2000.

Standards Uptake and Engagement

Currently, the only regulatory control of cyber security is conducted by the Ministry responsible for Communications (MEIDECC), and even this is only aimed at the telecommunications industry. Additionally, the country has no recognised national or international standards, and there is no standards certification bureau responsible for implementation and enforcement.



Nevertheless, in recent years, Tonga has been engaging with standards bodies and discussions and has made it clear that it recognises the importance of standardisation in cyber security. Indeed, standards have been on the table since the early ICT National Policy which highlighted the importance of ensuring "appropriate levels of security and privacy standards for ICT practices, resources and data" and developing "a robust policy and regulatory framework that ensures competition and standardisation and encourages growth throughout the ICT sector".⁴²

⁴¹ http://www.mic.gov.to/index.php?option=com_content&view=article&id=4913&lang=en

⁴² <http://pippr.victoria.ac.nz/bitstream/handle/123456789/27/Tonga%20-%20national%20ICT%20policy.pdf?sequence=1>

Tonga has cooperated with international assistance programs and bodies, including the Pacific Cyber Security Operational Network (PaCSON) and the Pacific Islands Forum (PIF). The current rank on the ITU Global Cybersecurity Index (2018) is 116 out of 175 countries, the highest rank of the five Pacific Islands assessed in this agenda.⁴³

Standards Gaps and Challenges

Nevertheless, gaps remain in Tonga's standards uptake which leave the country more vulnerable to cybercrime and external threats. These gaps include:

- No Cyber security professional certification.
- No National Standards or Cyber Security Frameworks.⁴⁴
- Not a member of ISO.
- Not participant or observer in the ISO Technical Committee or Policy Development Committee.
- Not a member of IEC or part of the IEC Committee.
- Does not participate in ISO/IEC JTC 1 or ISO/IEC 27000.
- Not a member of Pacific Area Standards Congress (PASC).
- Not a member of the Pacific Accreditation Cooperation (PAC).
- Not a member of APEC – Sub-Committee on Standards and Conformance (SCSC).

SWOT Analysis

During the forum, key participants from Tonga were asked to analyse their country's strengths, weaknesses, opportunities and threats (SWOT). Below is a summary of their response.

Strengths:

- The country has established an ICT Tonga Taskforce.
- Various pieces of legislation have addressed aspects of cyber security, for example, the Computer Crimes Act 2003.
- In November 2016, Tonga became the first Pacific Island country to be a party to the Convention on Cybercrime (Budapest Convention) and has drafted an updated Bill to align with the Convention.
- An E-Government has been introduced and backed by international support such as the Digital Government Support Project.
- The country has drafted an Electronic Transaction Bill and a Privacy Bill.
- Tonga's Computer Emergency Response Team has been running since July 2016.
- Tertiary education has introduced cyber security post-graduates, masters and PhD programs.
- The country has seen positive growth in some sectors due to online/social media platforms (for example, tourism).
- Internet usage and penetration continues to rise.
- The country receives grants from DFAT and the Council of Europe to build capacity and support its bodies such as CERT and the Attorney-General's Department.
- Tonga has been an active member and recipient of various APNIC initiatives, for example hosting the APNIC Workshop in May 2016.
- Under the Budapest Convention, Tonga has participated in activities for capacity building in the legislative enforcement space.
- The country has run a National Cyber Week since 2014 in collaboration with UNESCO/UNICEF.

43 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

44 [However, the Cyber Challenges Taskforce established in 2013 has helped provide guidance.](#)

- Internet Service Providers (ISP's) have been offering security training.
- The ITU conducts assessments of Tonga's cyber security maturity.

Weaknesses:

- There is a resistance to change, and the general population lacks awareness, understanding and education of cyber security issues.
- There is a lack of clarity around Tonga's strategic direction for policy and activities
- There is no National Standards Body.
- There is a lack of standards around ICT procurement and cyber security.
- Tonga has limited resilience or capacity for contingency planning and implementation.
- Tonga also has a lack of reviews and updating system for vital sectors.
- The cost of cyber security access and implementation is high.
- Human resources and skills are limited, and those with expertise have somewhat outdated qualifications.
- Proper implementation is a persistent issue, particularly with legislation that exists but is not well enforced.
- Some sectors have come to economically rely on online/social media platforms (for example, tourism).
- The rise in internet usage and penetration is also strength and a weakness.
- There is a lack of contextualised ICT solutions.

Opportunities:

- There is the potential to open up the Tongan market to international commerce, for example through call centres based in Tonga.
- Regional agreements and partnerships are invaluable for Tonga, for example, the MoU signed between Tonga and Netsafe Inc in May 2017.
- Local experts can become certified through international partners and programs.
- Tonga's data centres and other infrastructure can become certified to existing international standards.
- It is not too late for Tonga to develop its standards, commerce and implementation capacity before businesses around the country begin using technology more expansively.
- Education represents a vital opportunity to build capacity, expertise and spread awareness.

Threats:

- There has been a broad rise in cybercrime and increasingly sophisticated cybercrime activities
- The development of the Asia-Pacific Information Superhighway may increase Tonga's exposure to criminal activity.
- Tonga is vulnerable due to (a) non-compliance with legislation, standards and regulation and (b) the perception of lower level protections amongst Tonga making it an easier target.
- Proprietary technologies are currently in use but can be exploited by anyone because of the lack of open and effective standards.



Agenda Recommendations

Out of this SWOT analysis process, several key findings emerged, which were turned into recommended action plans for the country moving forward. These were:

01 Work with Standards Australia and other bodies: Seek advice from these bodies and establish a collaborative relationship with them to help the country set up a National Standards Body under a Public-Private Partnership (PPP) model. Create a National Standards 'Working Group' made up of the government, private sector and public enterprise to coordinate this relationship.

02 Develop an Awareness Campaign: This campaign should be directed at top-level decision makers as well as the wider community, aimed at increasing the pressure to develop relevant policies and instruments and to provide resources to the general public. It should be the responsibility of Tonga's CERT and other relevant government agencies and stakeholders.

03 Develop a Cyber Security National Strategy/Roadmap: Focussing on the country's cyber challenges – such as security, crime and safety – this agenda will provide direction and help with the prioritisation of activities, allocation of resources and the protection of key assets and information.

04 Enhance Localised Education, Training and Certification: In order to increase the country's cyber security capacity, it needs to focus on aligning curriculums, training programs and certification with the ISO/IEC 27000 series and other relevant standards, including auditing and risk assessments. Those responsible for this action include Tonga's ICT Taskforce, CERT and relevant education providers in collaboration with Standards Australia.

05 Adopt ICT Procurement and Security Standards: This initiative will ensure the viability of cyber security initiatives and must be spearheaded by Tonga's businesses community and government.

In addition to this, the participants acknowledged broader objectives for the short, medium and long term.

Short term

- Establish a working relationship with Standards Australia;
- Initiate activities to increase awareness in the business and general community;
- Use these activities to increase the pressure on the government to develop effective and specific cyber policies and instruments and provide resources;
- Encourage CERT to build relationships and increase communications to businesses and industries;
- Leverage external party relationships and initiatives to promote cyber security;
- Encourage the review of existing contingency plans through testing and drills;
- Develop a National Strategy for Cyber Security; and
- Develop a process for incident reporting, collection and analysis of data.

Medium term

- Enhance Tonga's contingency planning capacity and ensure there are limited to no service interruptions;
- Implement ICT procurement standards;
- Enhance the provision of training and certification to build immediate capabilities;
- Increase the private sector's participation in cyber security activities and initiatives;
- Refine the country's messaging and awareness building programs;
- Develop and implement an awareness campaign for top-level decision makers; and
- In doing so, prioritise dedicated funding for cyber security, encourage economic modelling/other quantitative analysis and leverage the G2G relationship.

Long term

- Set up a National Standards Body and increase the adoption of standards;
- Enhance localised education, training and certification through (a) scholarships, (b) capacity building for education providers and (c) building cyber security into the primary and secondary curriculum;
- Reduce the cost of ICT access;
- Look at the government's past activities and initiatives and use this to inform future activities and build on them; and
- Align Tonga's standards with other regional government structures, for example the Cyber Centre as a dedicated agency.

Conclusion

Tonga is a growing and stable country, with a government that is focussed on bringing the rest of the world to its doorstep through ICT growth. It has made commendable efforts to liberalise and expand the ICT industry, and connectivity continues to grow each year. However, like many countries before it, Tonga has struggled to keep its legislative and regulatory frameworks up to date as technology continues to stride ahead.

There is a lack of awareness across the general population on the dangers of the cyber space. Specialists or experts in cyber security are dwindling due to outdated skills and training. However, the government of Tonga continues to face these challenges head-on and is striving to address them through policy, networking, awareness campaigns, curriculum overhauls and more. Indeed, the country has shown a unique proclivity for bringing together national and international stakeholders to discuss, prepare and implement strategies to tackle the growing threat from cyber space, and it does not show any signs of slowing down.





Cyber Security Standards in Vanuatu

Purpose

This agenda outlines the preliminary cybersecurity initiatives in Vanuatu. It provides the basis and requirements to help design and develop Vanuatu's National Cyber Security Roadmap. The current developed policies, Vanuatu's National Sustainable Development plan, National Security Strategy and proposed Digital Roadmap plans and documents, will help set the required information and route to derive the Cyber Security Roadmap. With these milestones achieved, this agenda will help consolidate all various works into one central location to support the development of Cyber Security Roadmap.

Background and Trade Information

Vanuatu is a South Pacific island nation with a population of 281,000 which currently ranks at 147 out of 155 countries on the 2018 Global Cybersecurity Index.⁴⁵ The country joined the World Trade Organisation in 2012 and adopted a trade policy framework the same year, both which have led to considerable achievements in its economic and trade performance in the following years. Vanuatu has achieved reasonable growth rates in recent years, with its GDP growing by 3.8% from 2017 to 2018. It launched a national development strategy in 2017 known as Vanuatu 2030, which focuses, among other things, on enhancing trade and investment in the area.

However, Vanuatu faces other challenges. One-third of its population lacks access to basic services, while over 12 per cent live below the national basic needs poverty line,⁴⁶ representing the country's struggle to promote social inclusion and alleviate poverty. Vanuatu is one of the world's most vulnerable countries to natural hazards,⁴⁷ incurring an average loss of \$48 million per year due to earthquakes and cyclones. Its economic growth is severely restrained by its distance to major markets, narrow market base and infrastructure needs.

Despite these challenges, Vanuatu continues to maintain strong economic growth and has made impressive strides in enhancing the economic and social stability of the region.

Information Technology Uptake

In the past decade, Vanuatu has experienced significant growth in the ICT sector, spearheaded by a resilient dedication to strengthening the regulatory framework around ICT, improving and utilising government support and investing significantly in the sector from both public and private stakeholders.

Vanuatu has demonstrated a strong desire to improve the efficiency and effectiveness of its ICT infrastructure and frameworks hence wanting to contribute to and utilise technology more in order to improve the livelihood of its communities. Vanuatu's ICT sector has been transformed in recent years in many ways. For example, the

45 The International Telecommunication Union (ITU) Global Cybersecurity Index (GCI) is a multi-stakeholder initiative to measure the commitment of countries to cyber security. Cyber security has a wide field of application that cuts across many industries and sectors. Each country's level of development is analysed within five categories: Legal Measures, Technical Measures, Organizational Measures, Capacity Building and Cooperation.

46 <https://dfat.gov.au/geo/vanuatu/development-assistance/Pages/development-assistance-in-vanuatu.aspx>

47 <https://www.gfdr.org/en/vanuatu>

liberalisation of the telecommunications market; the creation of a multi-stakeholder National ICT Development Committee; and several projects including the country's first international submarine cable which was installed on 15 January 2014. This was a project executed by Interchange Ltd whereby the deployment of the submarine cable system linking Port Vila (Vanuatu) to Suva (Fiji) under the 'ICN1' - a US \$32 million project involving French telecommunications corporation Alcatel-Lucent. It is a milestone cable project linking Vanuatu directly into the high capacity Southern Cross cable between Sydney and USA. In 2008, Vanuatu committed into setting up its eGovernment Broadband Network. Since 2012 Vanuatu has celebrated an Annual ICT Day, which sees experts and government officials come together to collaborate and champion the country's ICT achievements and what is to come.

Cyber Security and ICT: Policy and Legislative Environment

As the country continues to enhance its ICT uptake, it has also recognised the growing threat from cyber security. For example, in 2017, while there were around 82 mobile cellular subscriptions per 100 citizens in Vanuatu and around 92% of the population covered by a mobile network, only 51 secure internet servers existed. As it stands, the rapid increase in the use of technology such as mobile phones in Pacific countries like Vanuatu is being exploited by cyber criminals because of the growing gap between prevalence and security.



The existing regulations and policies surrounding cyber security are coupled with a lack of awareness amongst the public as to how to use technology safely and what the consequences of failing to do so are. Thus, there is a need to increase cyber security awareness throughout all government and private sector organisations.

However, authorities in Vanuatu are catching up with cyber security. Since August 2018, the country has been revising and adapting new cybercrime

legislation, collaborating with working groups compiled of national experts, international consultants, law enforcement agencies and more to develop a new Cybercrime Bill that aligns more effectively with international standards like the Budapest Convention on Cybercrime.

The Office of the Government Chief Information Officer (OGCIO) was established by the Vanuatu Council of Ministers in November 2011. The purpose of this office is to efficiently and effectively encourage the spread of ICT throughout Vanuatu to promote an educated, healthy and wealthy Vanuatu.⁴⁸ It is committed to delivering better ICT services and e-government solutions to the country's ministries, agencies and ultimately to all citizens and businesses.

In May 2014, the OGCIO released Vanuatu's National ICT Policy, Cybersecurity Policy and Universal Access Policy. Each policy identifies individual goals, priority areas and outlines the country's commitment to programs such as the Pacific Cyber Security Operational Network (PaCSON) and the Cyber Safety Pasifika (CSP) Program.

Other legislative pieces that are used to address cyber security concerns include the *Telecommunications Act 1989* and the *Telecommunications (Amendment) Act 2007*,

48 <https://ogcio.gov.vu/index.php/about-us/purpose>

the *Electronic Transactions Act 2000*, the *E-Business Act 2000* and the *Police Power Act of 2017*.

Vanuatu then launched its Computer Emergency Response Team (CERT) in June 2018 as part of a new cyber security initiative. This initiative aims to strengthen Vanuatu's National Security. The establishment of its CERT Vanuatu has led to the development of Vanuatu's National Security Strategy. These new initiatives are the core components of Vanuatu's entire security infrastructure thus enabling the country to step up its response to cyber crime. Individuals can report any cyber threats to a central team that is responsible for the management, control and mitigation of these threats. This team also has the capability to analyse the findings and then provide accumulated expert advice and guidance to the government, businesses and individuals who are using the internet.

Other strides have been made that have implications for Vanuatu in terms of cyber security, such as the establishment of the first-ever Vanuatu Bureau of Standards office in August 2017, the work of the country's National Disaster Management Office (NDMO) and the introduction of a Policing Cybercrime Unit.

Standards Uptake and Engagement

Vanuatu has developed a national vision: for everyone – citizens, businesses, tourists and more – to be able to fully enjoy the benefits of a secure and efficient cyber space. To achieve this, a National Cyber Security Policy was drafted in 2013 to create cyber resilience and enhance understanding throughout the country.

A part of this policy is Vanuatu's continued effort to define and control "technical minimum standards for operators of national critical infrastructure to ensure basic security standards".⁴⁹

This goal was reiterated and refined in a 2014 Strategy and Implementation Plan for Mobile Governance in Vanuatu,⁵⁰ developed in cooperation with the OGCIO. This plan outlined the country's goal to define the minimum cyber security standards for critical infrastructure operations and to produce cyber security tools and services for citizens, business and government.

An essential part of this process is Vanuatu's cooperation with assistance programs including the Cyber Security Regional Standardisation Enhancement Program and the Pacific Cyber Security Operational Network (PaCSON). A significant step towards standards engagement was made in August 2017 with the creation of Vanuatu Bureau of Standards (VBS), which is responsible for the facilitation, promulgation, promotion and implementation of regional and national standards for goods, services, practices and processes.

Standards Gaps and Challenges

While the importance of cyber security standardisation within Vanuatu has been recognised, there is still progress to be made. The fast increase in technologies, introduces new cyber security issues and challenges.

Vanuatu's historical engagement with international standards is limited. The ITU Global Cybersecurity Index is a measurement tool used to rate a country's level of commitment to cyber security by analysing their legal measures, technical measures, organisational measures, capacity building and cooperation. In 2018, Vanuatu ranked 147 out of 175 countries on this Index.⁵¹

49 <https://ogcio.gov.vu/images/Cybersecurity-Policy-EN-FR-BI.pdf>

50 <http://www.cto.int/media/research/projects/Strategy%20and%20Implementation%20Plan%20Report.pdf>

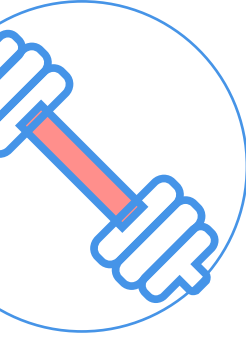
51 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Currently, the country has no National Standards or Cyber Security Frameworks and implements no international cyber security frameworks. However, Vanuatu has recently joined as a member of ISO and the introduction of the country's National Cyber Security Policy and ICT Policy is a significant step towards developing standards and best practices.


SWOT Analysis

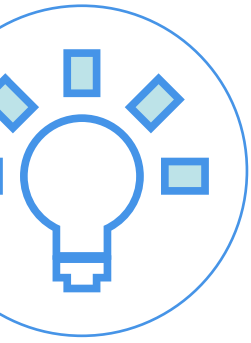
During the forum, key participants from Vanuatu were asked to analyse their country's strengths, weaknesses, opportunities and threats (SWOT). Below is a summary of their response.

Strengths:

- 
- A regulated Community Awareness Program.
 - The inclusion of ICT and cyber security issues in the national government policy (the National Sustainable Development Plan known as the '2030 People's Plan').
 - Greater cyber security awareness and collaboration with the Vanuatu Police Force and the enhancement of cybercrime awareness through the new Police Cybercrime Unit.
 - Enhanced education awareness programs (for example, the Annual ICT Day).
 - The transfer of information between the population through greater communication networks has been well received.
 - The country's internet access is well established and continues to improve each year;
 - Establishment of the following:
 - Computer Emergency Response Team (CERT);
 - Vanuatu Bureau of Standards (VBS);
 - National Disaster Emergency Management Committee (NDEMC);
 - The Office of the Government Chief Information Officer (OGCIO), which created national central database control.

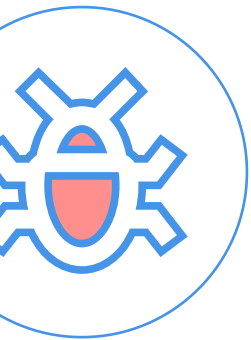
Weaknesses:

- 
- There are too few awareness campaigns that can assist in educating consumers and businesses, and there is not enough funding to finance these awareness campaigns.
 - The country faces a lack of training and knowledge around cyber security, ICT and technology.
 - The minimal cyber security knowledge and practical skills amongst the population continue to transcend generations, as parents are not able to educate their children as they themselves do not have the requisite information or skills.
 - The country has a deficit of human resources and technical ability in cyber security and ICT.
 - The country is spread across 83 islands and extends over 1000 kilometres, making communication across the country a significant issue.
 - Vanuatu has no established consumer commission.
 - The country recognises that it will take a significant amount of time and resources to implement the types of ICT infrastructures, government policies, programs and standards that are necessary to establish a strong and effective cyber security environment.



Opportunities:

- Vanuatu can work collaboratively with Non-Government Organisations (NGO's), private and regional bodies to address the issues it faces around cyber security, for example with:
 - Standards Australia;
 - ISOC;
 - APNIC; and
 - APRIGF.
- The National Government is ardently focusing on tackling the policy and financing issues, for example:
 - It is emphasising the need to enhance ICT utilisation and education within primary and secondary education.
 - It is also aiming to deliver awareness campaigns to local communities.
- A consumer commission is being developed, which will enable greater amounts of information to be spread amongst the community.
- The deficit in skills and knowledge amongst the Vanuatu population can be remedied through a dedication to training programs and continued cooperation with assistance programs.
- Vanuatu's Cybercrime Act is set to be passed in Parliament soon.



Threats:

- The Cybercrime Act is a first of its kind and has no policy foothold to base itself off.
- Every day more of the Vanuatu population goes online or buys a mobile device without having the requisite knowledge of how to behave online or how to stay secure.
- Mobile phones are difficult to trace as there are no IP addresses allocated to them.
- Children do not have the proper training either at home or in school, leaving them vulnerable.
- The population is experiencing a spike in cybercrime victims, as internet usage continues to rise but is not met with an equal amount of knowledge and information about how to stay safe online.
- Weaker visa and visa-free requirements within Vanuatu also allows for an increase in cybercrime.
- Along with the country's increased bandwidth capabilities comes the risk of more cybercrime and the need for enhanced security, standards and policies.



Agenda Recommendations

Out of this SWOT analysis process, several key findings emerged, which were turned into recommended action plans for the country moving forward. These were:

01 Enhance awareness of ISO/IEC 27000: This is an essential recommendation as it will assist in enhancing awareness of cyber security across the country and could also be used as a basis for further policies. It was decided that the Vanuatu Bureau of Standards (VBS) would be primarily responsible for this, by designing and distributing pamphlets to the general public.

02 Increase training on cyber security and standards: The country wants to communicate the importance of standards in cyber security and help individuals and businesses understand how to implement these standards. Once again, VBS will be primarily responsible for this.

03 Form a Cyber Security Working Group: By bringing together relevant government, public and private stakeholders, Vanuatu hopes to reach the common goal of setting up effective guidelines and frameworks for cyber security standards in the country. Here, participants agreed the Vanuatu Chamber of Commerce and Industry (VCCI) would work in conjunction with VBS to develop this working group.

In addition to this, the participants acknowledged broader objectives for the short, medium and long term.

Short term

Begin designing and distributing awareness campaigns to the broader community; and

Create and update the website and social media platforms with cyber security tips and information.

Medium term

Organise a discussion about forming a Technical Committee and/or Commission for cyber security;

Implement awareness programs;

Gather all stakeholders to discuss cyber security standards;

Ensure there is ongoing stakeholder collaboration whereby common goals, challenges and strategies are shared;

Promote ICT career paths and training; and

Focus on training and awareness for cyber security standards and regulations.

Long term

Implement further awareness programs;

Develop an Annual Cyber Security Plan and Budget in conjunction with relevant stakeholders;

Develop and implement a 5 Year Plan Roadmap; and

Generate a greater awareness on the ISO/IEC 27000 series for the private sector.

Conclusion

Cyber security in Vanuatu is a relatively nascent topic, yet many efforts are being made to address it. Given the fast evolving nature of ICT, this transition will take time and coordination. Key challenges include lack of ICT and security infrastructure, low levels of awareness, minimal security procedures within organisations, a lack of trained security professionals and lack of cyber security standards present and enforced in Vanuatu.

However, the country has demonstrated a strong dedication to improving its cyber security outlook and utilising technology and the internet in a safe and effective manner. The way forward is to focus on networking – sharing and using best practices, discussing challenges and learning from mistakes – and setting benchmark goals that have been developed by the government in cooperation with relevant stakeholders and consumers. Finally there needs to be an understanding of the need to adopt and implement cyber security standards in the eGovernment services and organisations operating in Vanuatu.



Conclusions and Next Steps

Cyber security will continue to play an essential role in the future of the Pacific region for many years to come, as companies and individuals alike continue to embrace innovation and digital transformation. Considering this, it is imperative that governments play their part in properly shaping the ICT industry and ensuring it is supported by a stable regulatory and investment environment. This not only involves proactively investigating areas of growth but accompanying that growth with the most effective and internationally recognised standards possible.

This agenda sets out how each participating Pacific nation plans to do exactly that. For many years, ISO/IEC JTC 1/SC 27 has been an internationally recognised centre of information security expertise that serves the needs of a diverse range of industries and governments. Hence, the Cyber Security Regional Standardisation Enhancement Program was run to enhance the countries' understanding and use of the ISO/IEC 27000 series of standards. It also provided a valuable opportunity to share information and develop long-term relationships between a diverse range of people and organisations.

Whilst each country is experiencing digital transformation and cyber security in its own unique way, common themes did begin to emerge when it came to priorities and plans moving forward. These were:

- Developing awareness campaigns for the whole community;
- Creating a working group, committee or commission for cyber security;
- Enhancing ICT career paths and education;
- Enhancing ICT training and certification;
- Continuing to work with organisations such as Standards Australia; and
- Developing a cyber security national strategy, roadmap or policy.

Importantly, this agenda has no prescribed destination and is not an official plan for any of the participating countries. Rather, it offers important guidance and outlines the starting point for the Pacific nations in terms of reaching their individual cyber security goals. Indeed, it can be used to inform decision-making, to map progress or to simply outline the way forward towards cyber safety in the Pacific region.

Annex A – Cyber Security Standards

The published ISO/IEC 27000 series standards are:

Designation	Title
ISO/IEC 27000	Information security management systems – Overview and vocabulary
ISO/IEC 27001	Information technology – Security Techniques – Information security management systems
ISO/IEC 27002	Code of practice for information security controls
ISO/IEC 27003	Information security management system implementation guidance
ISO/IEC 27004	Information security management – Monitoring, measurement, analysis and evaluation
ISO/IEC 27005	Information security risk management
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007	Guidelines for information security management systems auditing (focused on auditing the management system)
ISO/IEC TR 27008	Guidance for auditors on ISMS controls (focused on auditing the information security controls)
ISO/IEC 27009	Essentially an internal document for the committee developing sector/ industry-specific variants or implementation guidelines for the ISO27K standards
ISO/IEC 27010	Information security management for inter-sector and inter-organizational communications
ISO/IEC 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
ISO/IEC 27013	Guideline on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 (derived from ITIL)
ISO/IEC 27014	Information security governance
ISO/IEC TR 27015	Information security management guidelines for financial services – Now withdrawn
ISO/IEC TR 27016	Information security economics
ISO/IEC 27017	Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC TR 27019	Information security for process control in the energy industry
ISO/IEC 27031	Guidelines for information and communication technology readiness for business continuity
ISO/IEC 27032	Guideline for cybersecurity
ISO/IEC 27033-1	Network security – Part 1: Overview and concepts
ISO/IEC 27033-2	Network security – Part 2: Guidelines for the design and implementation of network security
ISO/IEC 27033-3	Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues
ISO/IEC 27033-4	Network security – Part 4: Securing communications between networks using security gateways

Designation	Title
ISO/IEC 27033-5	Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
ISO/IEC 27033-6	Network security – Part 6: Securing wireless IP network access
ISO/IEC 27034-1	Application security – Part 1: Guideline for application security
ISO/IEC 27034-2	Application security – Part 2: Organization normative framework
ISO/IEC 27034-6	Application security – Part 6: Case studies
ISO/IEC 27035-1	Information security incident management – Part 1: Principles of incident management
ISO/IEC 27035-2	Information security incident management – Part 2: Guidelines to plan and prepare for incident response
ISO/IEC 27036-1	Information security for supplier relationships – Part 1: Overview and concepts
ISO/IEC 27036-2	Information security for supplier relationships – Part 2: Requirement
ISO/IEC 27036-3	Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security
ISO/IEC 27036-4	Information security for supplier relationships – Part 4: Guidelines for security of cloud services
ISO/IEC 27037	Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27038	Document redaction
ISO/IEC 27039	Intrusion prevention
ISO/IEC 27040	Storage security
ISO/IEC 27041	Investigation assurance
ISO/IEC 27042	Analyzing digital evidence
ISO/IEC 27043	Incident investigation
ISO/IEC 27050-1	Electronic discovery – Part 1: Overview and concepts
ISO 27799	Information security management in health using ISO/IEC 27002 – guides health industry organizations on how to protect personal health information using ISO/IEC 27002



Annex B – Forum Attendees

Fiji	Asenaca Kevu	Dept. of National Trade Measurement & Standards Ministry of Industry, Trade & Tourism
Fiji	Haroon B. Khan	Ministry of Industry, Trade and Tourism Fiji
Fiji	Tupoutua'h Baravilala	Office of the Attorney General
Fiji	Savenaca Siwatibau Waqa	Fiji Police, Criminal Investigation Headquarters
Fiji	Jemesa Lave	Fiji Police, Criminal Investigation Headquarters
Papua New Guinea	Flierl Shongol	Department of Communication & Information (ICT Policy).
Papua New Guinea	Felix Rupokei	National Information & Communications Technology Authority
Papua New Guinea	Dominic Moros	National Information & Communications Technology Authority
Papua New Guinea	Jimmy Son	Papua New Guinea Computer Society (Industry Group)
Papua New Guinea	Dan Yansom	National Institute of Standards & Industrial Technology (NISIT)
Papua New Guinea	Robertson Asari	Office of the Secretary, Department of Communication and Information
Papua New Guinea	Joseph Loi Steven	Department of Prime Minister & National Executive Council
Papua New Guinea	Jack Tomon	Department of Communication and Information
Solomon Islands	Jerome Rivogani	SI Telekom Company Ltd
Solomon Islands	John Stanley	
Solomon Islands	Richard Nokia	Ministry of Finance & Treasury
Tonga	Edwin Liava'a	Tonga Cable Limited
Tonga	Paul Taumoepeau	Tonga Chamber of Commerce and Industry
Tonga	Sam Ve'a	Tonga Chamber of Commerce and Industry
Tonga	Siosaia Vaipuna	Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications and Climate Change (MEIDECC)
Tonga	Brenda Átoa	Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications and Climate Change (MEIDECC)
Vanuatu	Cainton Milroy	Interchange Ltd/Tek Tok (Tech Talk)
Vanuatu	George Hapsai	Telecommunications Radiocommunications and Broadcasting Regulator
Vanuatu	Ruth Amos	Vanuatu Bureau of Standards

