Pacific Region
Infrastructure Facility

Strengthening Cybersecurity in the Pacific Islands

MAPPING CYBERSECURITY IMPROVEMENT INITIATIVES AND STAKEHOLDERS

The report was prepared by external consultant, Elvin Prasad, with the support of the Pacific Region Infrastructure Facility (PRIF).

The report is published by the PRIF, a multi-partner coordination and technical assistance facility for improved infrastructure in the Pacific region. The PRIF development partners are the Asian Development Bank, the Australian Department of Foreign Affairs and Trade, the European Union, the European Investment Bank, Japan International Cooperation Agency, the New Zealand Ministry of Foreign Affairs and Trade, the United States Department of State, and the World Bank Group.

PRIF Coordination Office
c/o Asian Development Bank
Level 20, 45 Clarence Street
Sydney, NSW 2000, Australia

Phone: +61 2 8270 9444
Email: enquiries@theprif.org
Website: www.theprif.org

Published February 2024

Photos courtesy of the Asian Development Bank.
All tables and figures are provided by the author, unless otherwise specified.
Note: In this publication, "$" refers to United States dollars unless otherwise state.

Table of Contents

Tables

Figures

Abbreviations

ADB	Asian Development Bank
DFAT	Australian Government Department of Foreign Affairs and Trade
EU	European Union
FSM	Federated States of Micronesia
JICA	Japan International Cooperation Agency
MFAT	New Zealand Ministry of Foreign Affairs and Trade
PRIF	Pacific Region Infrastructure Facility
RMI	Republic of Marshall Islands
US	United States
ACSC	Australian Cyber Security Centre
A4AI	Alliance For Affordable Internet
APCICT	Asian and Pacific Training Centre for Information and Communication Technology for Development
APT	Asia-Pacific Telecommunity
ASPI	Australian Strategic Policy Institute
APNIC	Asia Pacific Network Information Centre
APTC	Australia Pacific Training Coalition
CERT NZ	Computer Emergency Response Team New Zealand
CTO	Commonwealth Telecommunications Organisation
CROP	Council of Regional Organisations of the Pacific
GFCE	Global Forum on Cyber Expertise
ICANN	Internet Corporation for Assigned Names and Numbers
ICDP	International Centre for Democratic Partnerships
IGO	Intergovernmental organization
ITU	International Telecommunication Union
NGO	Nongovernment organization
OCSC	Oceania Cyber Security Centre
PaCSON	Pacific Cyber Security Operational Network
PICISOC	Pacific Islands Chapter of the Internet Society
PILON	Pacific Islands Law Officers' Network
PITA	Pacific Islands Telecommunications Association
PTC	Pacific Telecommunications Council
SPC	Secretariat of the Pacific Community.
TAFE	Technical and Further Education
UNICEF	United Nations International Children's Emergency Fund
UNODC	United Nations Office on Drugs and Crime
WWW	World Wide Web

Executive Summary

Overview

The Pacific Region Infrastructure Facility (PRIF), a multi-partner coordination and technical assistance facility for improved infrastructure in the Pacific, identified the need to develop a central, shared mapping of cybersecurity improvement initiatives undertaken by all stakeholders and PRIF's member countries.[1]

This mapping exercise involved 46 stakeholders and 14 countries in the Pacific – PRIF members, together with Papua New Guinea (PNG), which is an associate member. The survey was undertaken in June 2022, and the results presented in this Report are a snapshot of cybersecurity initiatives in the region at that time. Out of these countries, just a few have established some form of a guiding framework or have strategized long term for cybersecurity. Most are highly dependent on external technical and financial support for information and communications technology (ICT) and cybersecurity capabilities, resulting in many stakeholders active across the region.

Coordination on cybersecurity across the Pacific plays a significant role in supporting overall security goals and objectives, as this mapping also intends to improve effectiveness and minimize potential duplication in cybersecurity initiatives.

This mapping exercise was aimed at identifying cybersecurity initiatives that have recently been implemented, are ongoing, or are planned for the Pacific region and populating them in a database. It is intended to support PRIF members by identifying gaps and overlaps, as well as areas for future cooperation. The survey was undertaken in June 2022, and the results presented in this Report are a snapshot of cybersecurity initiatives in the region at that time. It is intended that survey results be updated as needed.

Approach

The mapping process involved the identification of relevant stakeholders and government agencies that deal with cybersecurity across the 14 Pacific countries, establishing contacts, and developing and distributing a survey. The collated responses from countries and stakeholders capture cybersecurity initiatives across five key focus areas in the Pacific – cybersecurity, online safety, cybercrime, laws and policies, and training and education. Survey results were captured in a database, summarized in the following table.

Database summary

	Number of survey responses	Number of initiatives reported	**Other stakeholders identified**
PRIF Development Partners	7	81	-
Other international, regional, or national stakeholders	39	90	34
Subtotal	**46**	**171**	**34**
PRIF member countries	14	71	2
Total	**60**	**242**	**36**

Source: Survey responses. Note: The European Union responded on behalf of the European Investment Bank which had no initiatives, resulting in seven PRIF Development Partners in the reported counts.

[1] PRIF's Pacific member countries are Cook Islands, Federated States of Micronesia, Fiji, Kiribati, Nauru, Niue, Palau, Republic of the Marshall Islands, Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu. Papua New Guinea is an associate member.

Results

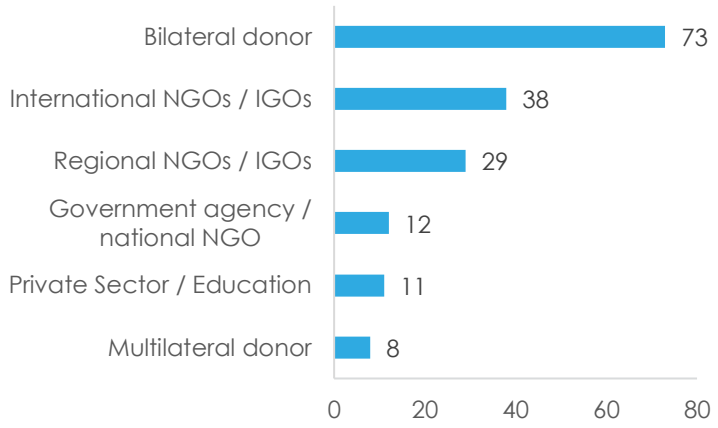
The Study identified 96 stakeholders active in the region and 242 initiatives.

Stakeholders' participation typically spans several sectors, beyond a core cybersecurity focus, including telecommunications, internet, governance, legal and regulatory, training and education.

Most initiatives are delivered by bilateral donors, NGOs and IGOs.

Regional technical organizations and international nongovernment organizations (NGOs) or intergovernmental organizations (IGOs) play a considerable role and should be a key focus for future coordination.

Initiatives reported by stakeholders (count of initiatives)



NGO = nongovernment organization, IGO = intergovernmental organizations.

Source: stakeholder survey responses. Note: Counts include initiatives reported by multiple funders and implementing agencies.

Most initiatives reported by stakeholders were regional (n = 46).

Tonga, Vanuatu, Fiji, and Samoa were the focus of the most initiatives (n > 20), followed by PNG (n = 19), Solomon Islands (n = 17), and Kiribati (n = 14). Fewer initiatives targeted Nauru, Tuvalu, and Federated States of Micronesia (n < 10). Very few were reported for Cook Islands, Niue, and Palau (n=2) and none were reported for Republic of the Marshall Islands. Most country-specific initiatives focused on general cybersecurity, with apparent gaps in many countries across cybercrime, law, and policy.

Categories addressed by stakeholder initiatives (by country)

Country	Cybersecurity (other)	Training And Education	Online Safety	Law And Policy	Cybercrime
Tonga	22	15	10	8	7
Vanuatu	22	15	6	10	6
Samoa	21	14	7	7	4
Fiji	20	14	8	7	3
PNG	20	14	8	4	3
Solomon Islands	22	10	8	5	2
Kiribati	12	11	4	4	1
Tuvalu	10	6	4	2	1
Nauru	8	5	3	2	1
FSM	4	4	2	4	3
Niue	3	3	1	1	1
Cook Islands	4	2	-	-	-
Palau	2	1	-	-	-
RMI	-	-	-	-	-

PNG = Papua New Guinea, FSM = Federated States of Micronesia, RMI = Republic of Marshall Islands.

Source: Stakeholder survey responses. Excludes initiatives where beneficiary countries were not reported.

Most country-reported initiatives focus on foundational legal and policy frameworks, and embryonic capabilities.

In their response to the survey questionnaire, PRIF member countries identified initiatives that were own-national funding (n = 13). These were reported by PNG, Fiji, Nauru, Niue, Tuvalu, and Vanuatu.

Key findings

1. **Continued coordination and visibility of initiatives is important** given the large number of organizations active in the region.

2. **Smaller countries rely heavily on regional support.** Most initiatives are delivered through regional programs. Country-specific programming is focused on larger countries. Few country-specific initiatives addressed online safety, law and policy, and cybercrime.

3. **Many initiatives are relatively short term** and / or responsive to immediate needs (e.g., support for staffing of computer emergency response teams). Evidence of mainstreaming or sustainability is limited. Few programs addressed specific industry and physical infrastructure vulnerabilities.

4. **International and regional NGOs and IGOs similarly play an important role in delivery, but planned initiatives to be delivered by these organizations may lack visibility due to reliance on external funding.** The lack of visibility about planned initiatives from this group is a significant gap – and potential area for a risk of overlaps in the future.

5. **National government agencies and institutions are important implementing partners, particularly for Online Safety initiatives.** However, few countries reported initiatives independent of donors.

6. **More granular analysis of initiatives is needed to better identify capability gaps.** The categories adopted in this study are high-level for initial mapping, but further detail will better support targeting.

Recommendations

Further work on information sharing and investment coordination should focus on the following areas.

1. **Emphasize more programmatic approaches for funding and resourcing of the nascent cybersecurity capacity development in the region.** More consistent models for multi-year support are needed to develop a more self-sustaining cybersecurity capacity.

2. **Mainstreaming of cybersecurity capacity development into donor funded initiatives** to catch up with accelerating internet penetration, digital government, and e-commerce initiatives. Key gaps include: programs focused on industry and critical infrastructure, e-transactions, cybercrime and ccTLD administration.

3. **Provide ongoing access to regional programs and mechanisms for support for smaller countries,** which lack the scale to develop national technical capacity. Examples include pairing of national ICT agencies and industry operators with trusted regional partners.

4. **Strengthen information sharing and awareness through relevant institutions.** Undertake periodic updates, and boost awareness and dissemination, for example, through platforms such as the Global Forum for Cyber Education's Cybil Knowledge Portal, as well as continued coordination and information sharing via regional and international working groups and events.

5. **Cybersecurity industry strategy should cultivate long-term engagement with NGOs and IGOs.** As key implementing partners, and hosts to technical skills and expertise in the region, maintaining engagement and the sustainability of participating in cybersecurity in the region should be a key consideration for development partners.

6. **Standardize reporting for future information-sharing initiatives.** Align with relevant capability models and standards, as well as additional breakdowns on activities and outcomes.

1 Introduction

1.1 Background

Addressing cybersecurity has become a key challenge for social, political, and economic development in the Pacific. Increasing connectivity across the Pacific Island countries (PICs), alongside the evolution of global threats in the cyber domain, has resulted in range of emerging economic, safety, disruption, and reputational risks that need to be managed.

Evolving global threats in the cyber domain

Many of these risks are not unique to the Pacific. Issues related to openness, accessibility, security, diversity, and critical internet resources have become key points of discussions at global information and communication technology (ICT) forums. Expanded connectivity and accessibility has also led to a greater need to safeguard critical internet infrastructure of every nation as the global threat landscape continues to grow. In the last 3–5 years, there has been significant growth in global cyber-attacks, many of which have targeted large corporations and governments in the Pacific. Mitigation efforts have largely been limited to cybersecurity mechanisms and user awareness for online safety practices. Cyber-attacks have devastating consequences and are specifically crafted to affect various sectors and industries.

Unique challenges compound the exposure of Pacific Island countries to cyber-risks as connectivity and accessibility improve

Many of the unique challenges faced by the countries in the region – remoteness, small populations, low income and digital literacy levels – compound their exposure to the risk, and constrain their capacity to respond. The Global Cybersecurity Index (GCI) issued by the International Telecommunications Union (ITU) in 2020[2] demonstrated that many PICs have made insufficient progress in improving their cybersecurity, with most PICs scoring less than 30 out of 100 on the index.

Until recently, improving internet connectivity and accessibility was the main ICT concern in the Pacific, but improving cybersecurity has not been a priority for many countries. Over the last decade, the digital divide and gaps in connectivity have been closing in the region through investments in submarine cable projects and satellite connectivity. This has connected many new groups of Pacific citizens, including schools and rural and outer-island communities, to the internet. However, many of these groups, and their respective national governments, are vulnerable to the threats in the online world, and other internet safety and privacy concerns. As such, the Pacific is particularly exposed to cyber-crimes.[3]

It is increasingly recognized that digital connectivity is an important opportunity for the region, and that cybersecurity risks need to be managed more effectively.

It is increasingly recognized that digital connectivity is a key driver of economic, social, and political development for the region. For example, the recently released Pacific Island Forum *2050 Strategy*

[2] ITU. 2020. Global Cybersecurity Index. https://www.itu.int:443/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[3] See Pacific Region Infrastructure Facility. 2019. Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands. https://www.theprif.org/document/regional/information-and-communications-technology-ict/cybersecurity-and-safeguarding

for the Blue Pacific Continent[4] identifies Technology and Connectivity as one of five key thematic areas for delivering on the Pacific leaders' vision for "enabling all Pacific peoples to participate in and benefit from development". The Peace and Security thematic of the 2050 Strategy, as well as the *2018 Boe Declaration on Regional Security*[5] highlight cybercrime and cybersecurity as key risks to Pacific infrastructure and peoples.

It is also increasingly recognized that threats in the cyber domain are a risk to this vision. A safer cyber environment has now become a priority, alongside other national development objectives. The 2018 Boe Declaration on Regional Security from Pacific Island Forum leaders called for an increasing emphasis on cybersecurity. Many leaders in the region have also called for stricter controls on the use of the internet. However, most countries have struggled to develop effective responses to these emerging risks, making cybersecurity one of the leading security challenges in the Pacific.

Many PICs, often with assistance from development partners and other nongovernment organizations (NGOs), have now established their own national strategies to manage cybersecurity risks. Examples include development of cyber-resiliency plans, cybersecurity legislation and policy, establishment of computer emergency response teams (CERTs) and other security measures.

Despite these efforts, PICs remain a long way from having comprehensive and sustainable policies and frameworks in place to manage cybersecurity.

Further, as Pacific citizens become more online, effective online safety programs and awareness campaigns will need to address a broader range of users, including a specific focus on the younger age groups.

More effective coordination can improve the targeting and effectiveness of cybersecurity initiatives in the region

PRIF's 2019 report *Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands*[6] identified the following insights about initiatives to improve cybersecurity:

- there are difficulties in achieving sustainability;
- there is a lack of visibility and coordination of efforts; and
- most attempts to reduce cyber-risks rely heavily on pan-regional approaches.

PRIF's report provided a cyber-risk assessment and policy and legal gap analysis to inform discussions with participating countries, donor agencies, and other stakeholders on the development of cyber and electronic transaction frameworks.

Following this report, PRIF's ICT Sector Working Group, together with participants from the ITU, Commonwealth Telecommunications Organization, Global Forum for Cyber Education (GFCE), Pacific Cyber Security Operational Network (PaCSON) and the Council of Regional Organisations of the Pacific (CROP) ICT Sector Working Group, concurred that gaps and overlaps in initiatives and failure to achieve synergies were undermining achievement of their objective of improved cybersecurity. In addition, development projects have been placed at risk. They identified the need to develop a central, shared mapping of cybersecurity improvement initiatives between development agencies (including PRIF's development partners) and the PICs.

[4] Pacific Islands Forum. 2022. '2050 Strategy for the Blue Pacific Continent', https://www.forumsec.org/2050strategy/

[5] Pacific Islands Forum. 2018. 'Boe Declaration on Regional Security', https://www.forumsec.org/2018/09/05/boe-declaration-on-regional-security/

[6] Pacific Region Infrastructure Facility. 2019. Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands. https://www.theprif.org/document/regional/information-and-communications-technology-ict/cybersecurity-and-safeguarding

1.2 Study objectives

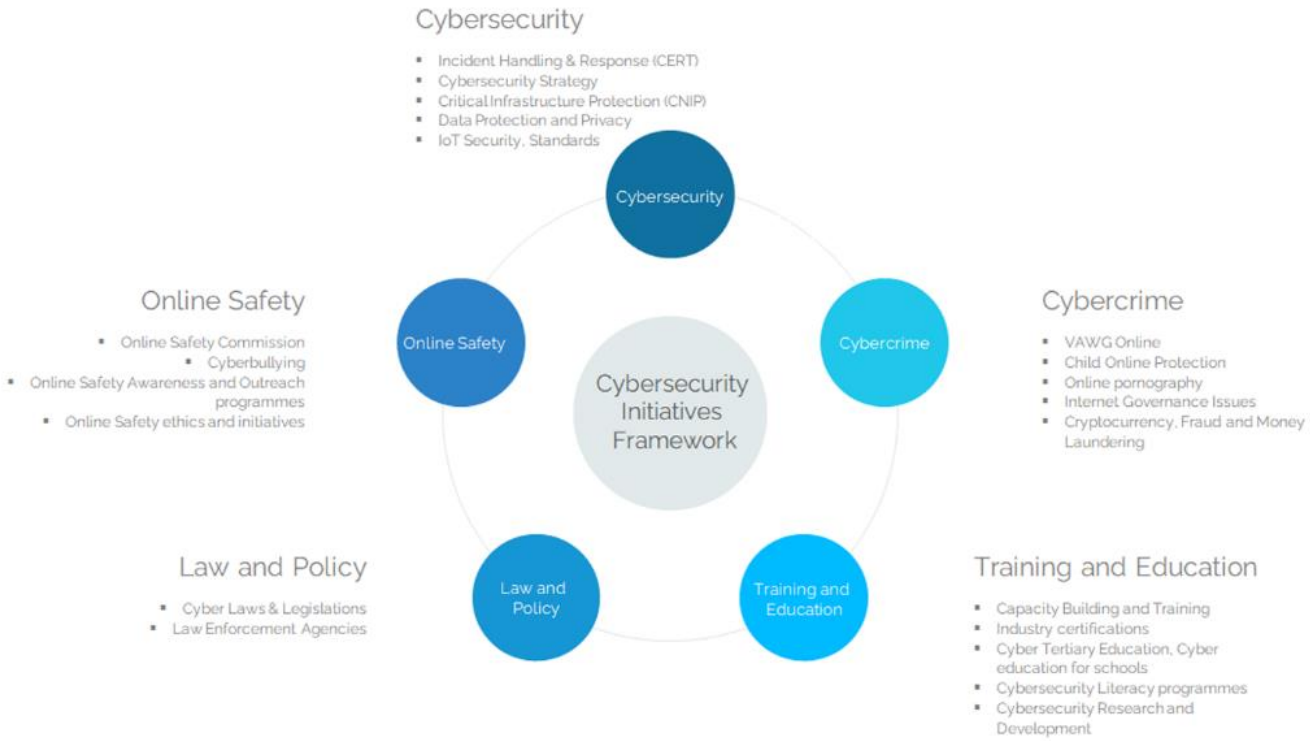
This Report builds on the findings in the 2019 Report and brings together information from a range of sources and stakeholders in order to develop a central, shared snapshot of cybersecurity initiatives in the region. In the future, further surveys may be undertaken to periodically update the data presented in this Report. Any updated data will be available via the PRIF website.

1.3 Scope

The scope of the mapping exercise included cybersecurity initiatives of PRIF's development partners, PRIF member countries, including associate member Papua New Guinea (PNG), and other key agencies and NGOs active in PRIF member countries.

Cybersecurity initiatives across five key focus areas were considered: cybersecurity, cybercrime, training and education, online safety, and law and policy, as summarized in Figure 1.

Figure 1: Cybersecurity Initiatives Framework Showing the Five Key Focus Areas



IOT = Internet Of Things, VAWG = Violence Against Women & Girls
Source: Authors.

1.4 Approach and methodology

The following section provides a summary of the approach and methodology adopted for the study. Further detail is included at Appendix A: Study methodology.

1.4.1 Mapping process

The mapping process involved four steps:

1. Identification of key country contacts and stakeholders
2. Data gathering
3. Data validation and augmentation
4. Compilation and processing

Each of these steps is discussed under the following headings.

1.4.2 Identification of key country contacts and stakeholders

Relevant stakeholder groups were identified regarding capturing the key stakeholders with active initiatives in the region. These primarily fall into three groups:

- PRIF member development partners
- PRIF member countries
- Other international, regional, or national stakeholders

This resulted in a starting stakeholder group of 14 member countries, and 46 other stakeholders (including eight PRIF development partners) who were sent survey questionnaires.

Additional funding agencies and implementation partners identified in questionnaire responses (discussed further in Section 4.2) bring the total number of stakeholders in the database to 96.

1.4.2.1 PRIF member development partners

PRIF's development partners consist of the major multilateral and bilateral donors in the Pacific, summarized in Table 1.

Table 1: PRIF Member Development Partners

Development partner
Asian Development Bank
Australian Department of Foreign Affairs and Trade
European Union
European Investment Bank
Japan International Cooperation Agency
New Zealand Ministry for Foreign Affairs and Trade
United States Department of State
World Bank Group

Source: Authors.

For bilateral partners, some cybersecurity initiatives will be undertaken by national agencies other than the PRIF member; for example, Australia is a member of PRIF through the Department of Foreign Affairs and Trade (DFAT), but has cybersecurity initiatives that may be undertaken by other agencies, such as the Australian eSafety Commissioner.

1.4.2.2 PRIF member countries

PRIF's 14 member countries and PNG were included in the study. Based on the most recent assessments, most countries have low cybersecurity maturity, with the exception of Fiji and Samoa, which were assessed as "established", and PNG, Tonga, and Vanuatu, which were assessed as "intermediate".[7]

The lead agency on cybersecurity in each country was identified as the point of contact, as summarized in Table 2.

Table 2: PRIF Member Countries, Cybersecurity Maturity and Lead Agencies

Country	Lead agency	Areas of oversight	Population (2020)	Fixed Internet Broadband Subscriptions (2019, per 100 inhabitants)	Cybersecurity maturity level
Cook Islands	Office of the Prime Minister	Various	15,281	15.14	Starting
Federated States of Micronesia	Department of Transportation, Communications, and Infrastructure,	ICT, Transport, Infrastructure	105,503	3.39	Starting
Fiji	Ministry of Communications	ICT	894,961	1.48	Established
Kiribati	Ministry of Information, Communications, and Transport	ICT, Transport	118,744	0.06	Starting
Nauru	Department of ICT	ICT	11,690	9.50	Starting
Niue	Ministry of Infrastructure	Infrastructure	1,562	Not reported	Starting
Palau	Division of Communication, Ministry of Public Infrastructure, Industries, and Commerce	ICT, Infrastructure, Trade	17,930	6.93	Starting
Papua New Guinea	Department of Information and Communications Technology	ICT	8,934,475	0.21	Intermediate
Republic of the Marshall Islands	Ministry of Transportation and Communications	ICT, Transport	54,590	1.72	Starting
Samoa	Ministry of Communications and Information Technology	ICT	198,646	0.87	Established
Solomon Islands	Ministry of Communication and Aviation	ICT, Aviation	712,071	0.16	Starting
Tonga	Ministry of Communication	ICT	99,780	3.54	Intermediate
Tuvalu	Department of ICT	ICT	10,580	3.96	Starting
Vanuatu	Officer of the Government Chief Information Officer	ICT	294,688	1.59	Intermediate

ICT = information and communications technology.

Source: Various national cybersecurity capability maturity assessments (unpublished); PRIF 2021 Pacific Infrastructure Performance Indicators.

1.4.2.3 Other international, regional, or national stakeholders

This third stakeholder group was identified from previous PRIF and the CROP ICT Working Group studies in the region. This was supplemented with desktop research. In some cases, this will include

[7] See https://ocsc.com.au/cmm-and-capacity-initiatives/

implementing partners, delivering projects on behalf of development partners funded or co-funded projects. Several other stakeholders were identified from country responses and are discussed further in Section 4.2.

All stakeholder survey respondents are listed in Table 3.

Table 3: Other International, Regional, or National Stakeholders

Name	Stakeholder Type
Asia Pacific Network Information Centre (APNIC)	Regional NGO
Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT)	International NGO
Asian Development Bank (ADB)	Multilateral Donor
Asia-Pacific Telecommunity (APT)	Regional NGO
Australia Government eSafety Commissioner	Government Agency
Australia Pacific Training Coalition (APTC)	Technical, Vocational Education and Training
Australian Cyber Security Centre (ACSC)	Government Agency
Australian Government Department of Foreign Affairs and Trade (DFAT)	Bilateral Donor
Australian Government Department of Infrastructure Transport Regional Development and Communication	Government Agency
Australian Strategic Policy Institute (ASPI)	National NGO
Christ's University in Pacific (CUP)	University
Commonwealth Telecommunications Organisation (CTO)	International IGO
Computer Emergency Response Team New Zealand (CERT NZ)	Government Agency
Council of Europe	International IGO
Council of Regional Organisations of the Pacific (CROP) ICT Working Group	Regional IGO
Cyber Safety Pasifika (CSP)	Regional IGO
e-Governance Academy (eGA) Foundation	International NGO
European Union (EU)	Bilateral Donor
Fiji National University (FNU)	University
Get Safe Online (GSO)	Public Private Partnership
Global Forum on Cyber Expertise (GFCE)	International NGO
Global Partners Digital (GPD)	International NGO
International Centre for Democratic Partnerships (ICDP)	International NGO
International Telecommunication Union (ITU)	International NGO

Name	Stakeholder Type
Internet Corporation for Assigned Names and Numbers (ICANN)	International NGO
Japan International Cooperation Agency (JICA)	Bilateral Donor
New Zealand Ministry of Foreign Affairs and Trade (MFAT)	Bilateral Donor
Oceania Cyber Security Centre (OCSC)	National NGO
Pacific Cyber Security Operational Network (PaCSON)	Regional IGO
Pacific Fusion Centre	Regional IGO
Pacific Islands Chapter of the Internet Society (PICISOC)	Regional NGO
Pacific Islands Forum Secretariat (PIFS)	Regional IGO
Pacific Islands Law Officers' Network (PILON)	Regional IGO
Pacific Islands Telecommunications Association (PITA)	Regional NGO
Pacific Technical and Further Education (Pacific TAFE)	Technical, Vocational Education and Training
Pacific Telecommunications Council (PTC)	Regional NGO
Save the Children	International NGO
Secretariat of the Pacific Community (SPC)	Regional IGO
Standards Australia	National NGO
The Asia Foundation	International NGO
United Nations International Children's Emergency Fund (UNICEF)	International NGO
United Nations Office on Drugs and Crime (UNODC)	International NGO
United States Agency for International Development Digital Connectivity and Cybersecurity Partnership (DCCP)	Bilateral Donor
United States Department of State (DOS)	Bilateral Donor
University of South Pacific (USP)	University
Welchman Keen	Private Sector
World Bank	Multilateral Donor
World Wide Web Foundation / Alliance for Affordable Internet (A4AI)	International NGO
The Asia Foundation	International NGO
United Nations International Children's Emergency Fund (UNICEF)	International NGO
United Nations Office on Drugs and Crime (UNODC)	International NGO
United States Agency for International Development Digital Connectivity and Cybersecurity Partnership (DCCP)	Bilateral Donor

Name	Stakeholder Type
United States Department of State (DOS)	Bilateral Donor
University of South Pacific (USP)	University
Welchman Keen	Private Sector
World Bank	Multilateral Donor
World Wide Web Foundation / Alliance for Affordable Internet (A4AI)	International NGO

IGO = intergovernmental organization, NGO = nongovernment organization.

Source: Authors.

1.4.3 Data gathering

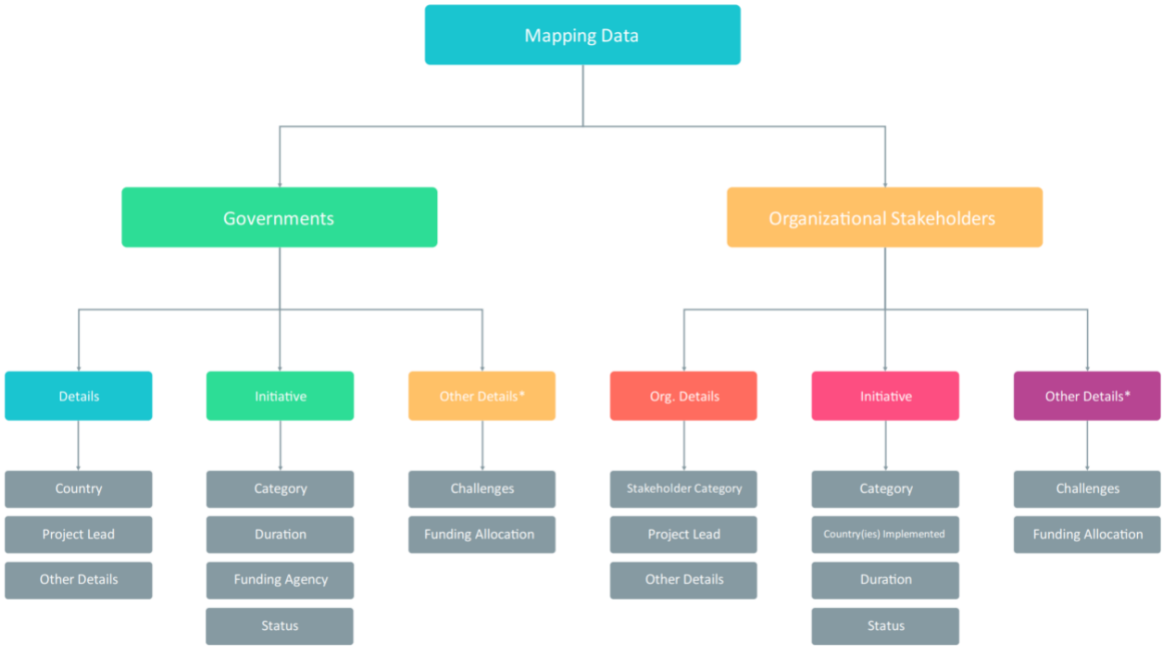
The data gathering exercise was conducted using secondary research methods through interviews, questionnaires, and desk research. The main sources for desk research involved development partner status reports, academic journals, third-party industry and country assessments, indexing, website information, reports, information requests, etc.

Key sources that were used to identify stakeholders included the ITU Global Cybersecurity Index, Global Cyber Alliance (GCA), and the Global Forum on Cyber Expertise (GFCE) Cybil Portal.

Separate questionnaires were developed and distributed – one for member countries, and one for development partners and other stakeholders. The questionaries can be found in Appendices B and C.

The data were gathered through the questionnaires and other sources to populate the framework shown in Figure 2.

Figure 2: Data Collection Framework



Source: stakeholder survey responses.

This split between Country Initiatives and Stakeholder Initiatives is used throughout the report.

A total of 60 (100%) responses to the questionnaire were received, providing information on of 242 initiatives, as shown in Table 4.

Table 4: Questionnaire Responses

Stakeholder Group	Number of questionnaires distributed	Number of responses	Number of initiatives reported
Stakeholders			
PRIF development partners	7	7	81
Other international, regional, or national stakeholders	39	39	90
Subtotal	**46**	**46**	**171**
PRIF member countries			
PRIF member countries	14	14	71
Total	**60**	**60**	**242**

Source: stakeholder survey responses.

The total number of initiatives reported may include duplicates, via country, funding agency, and implementing partner reports. These are discussed further in Section 1.4.4.

1.4.4 Data validation and augmentation

In some cases, other secondary data were added to augment or fill gaps in responses. Examples include:

- project status;
- start / end dates;
- beneficiary country(ies) where a project was described as regional; and
- validating project information provided by multiple respondents.

Responses were cleaned to align descriptive data like agency and country names, as well as dates, status, and duration.

For the analysis, duplicate initiatives have not been removed so as to preserve detail on donor activities. Instead, results are typically reported separately for development partners, countries and other stakeholder respondents in this Report.

In the supporting database, initiatives are flagged as a “Child”, where there is an obvious “Parent” funding agency. These Child and Parent cases are also flagged as being related, alongside other types of “Related” initiatives, such as jointly funded initiatives. Where countries have reported a stakeholder-funded initiative, these have been flagged as related in the country record.

Table 5 summarizes the number of these initiatives in the responses provided by stakeholders and member countries.

Table 5: Child and Related Initiatives

Stakeholder Group	Number of "Child" initiatives	Number of "Related" initiatives[8]	Number of country initiatives without other funding agency	Total number of initiatives reported
PRIF development partners and other stakeholders	8	47	n/a	171
PRIF member countries	24	37	15	71
Total	**32**	**84**	**15**	**242**

PRIF = Pacific Region Infrastructure Facility.

Source: stakeholder survey responses.

In summary, 47 (27%) of the 171 initiatives reported by stakeholders were related to other initiatives. For the 71 initiatives reported by countries, 37 (52%) were related to initiatives also reported by stakeholders. A small number of cases of Child initiatives were identified.

Only a small number (15, or 21%) of the initiatives reported by PRIF member countries did not involve an external funding agency. However, the related stakeholder initiative was not identifiable for all of the externally funded initiatives.

1.4.5 Compilation and processing

Questionnaire responses were analyzed to produce relevant indicators, such as total number of initiatives in the Pacific, and to map the reported initiatives by country, category, and donor.

Several summaries were tabulated based on this data set. The results include aggregated counts of initiatives, the number of initiatives by category, and breakdown of individual categories.

These are discussed in Section 2 of this Report onward.

1.4.6 Database

A key output of the study is a database that includes all 242 initiatives reported in stakeholder and member country responses and represents a snapshot of cybersecurity in the region.

1.5 Limitations

This mapping exercise was limited in certain aspects due to time and scope. This included relying on the information provided by respondents, the correctness (or otherwise) of information provided by stakeholders and country representatives, how up to date the information on initiatives provided was, and limitations related to the specific experience and knowledge of respondents (for example where knowledge transfer and record keeping of development initiatives by focal points may not be comprehensive, or where limited responses have been provided).

Another key limitation is the sharing or release of sensitive information related to cybersecurity. Some governments have cybersecurity functions overseen by the defense and national security agencies and there may be initiatives that not warranted for public disclosure.

[8] Count includes Child initiatives, and each related initiative.

1.6 Report structure

The report is structured as follows:

Section 2. Who is Working on Cybersecurity in the Pacific

Section 3. What Initiatives Are They Working on

Section 4. Which Countries?

Section 5. Country Survey Results

Section 5. Analysis and Discussion

Section 6. Conclusion

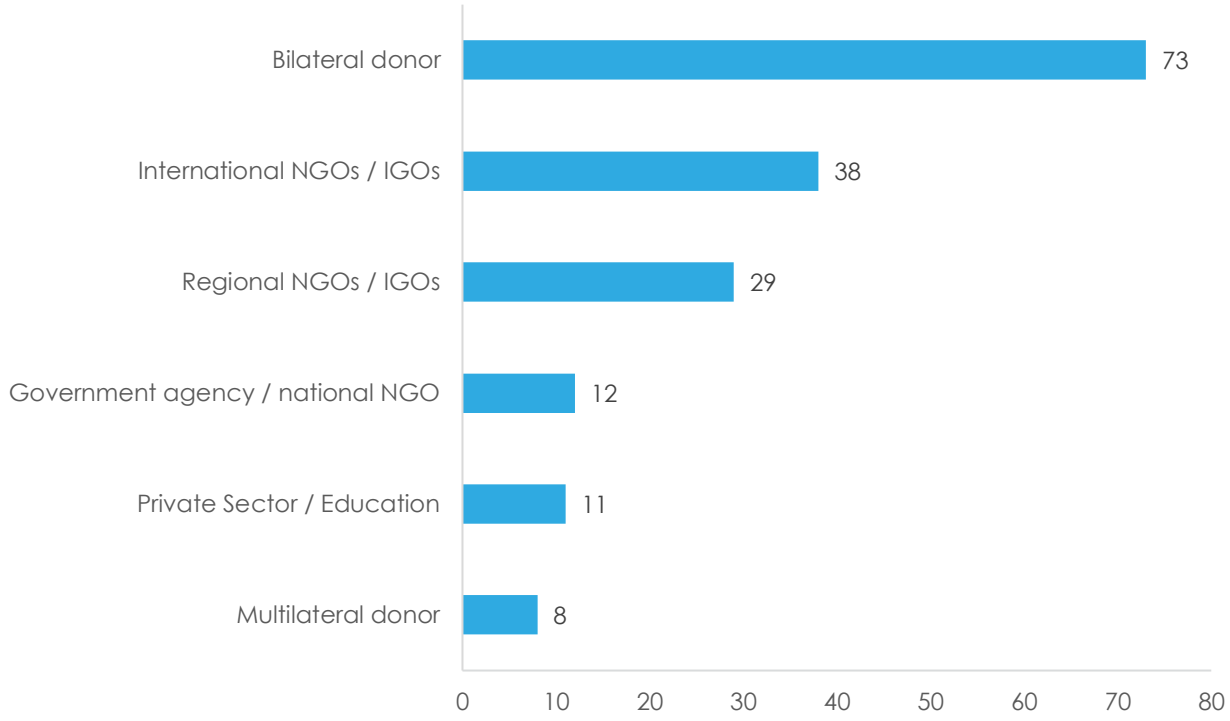
Appendices include questionnaires distributed to respondents, and a database of responses.

2 Who is Working on Cybersecurity in the Pacific?

2.1 All initiatives reported by stakeholders

171 initiatives were reported by 46 stakeholders (including PRIF Development Partners). Bilateral donors accounted for the most initiatives (n = 73), followed by international NGOs and IGOs (n = 38). Government agencies and national NGOs (n = 12), and private sector / education stakeholders (n = 11) contributed relatively few initiatives. The types of stakeholders are summarized in Figure 3.

Figure 3: Initiatives Reported by Stakeholders (Count of Initiatives)



IGO = intergovernmental organization, NGO = nongovernment organization.

Source: stakeholder survey responses.

Notes: Counts include initiatives reported by multiple funders and implementing agencies.

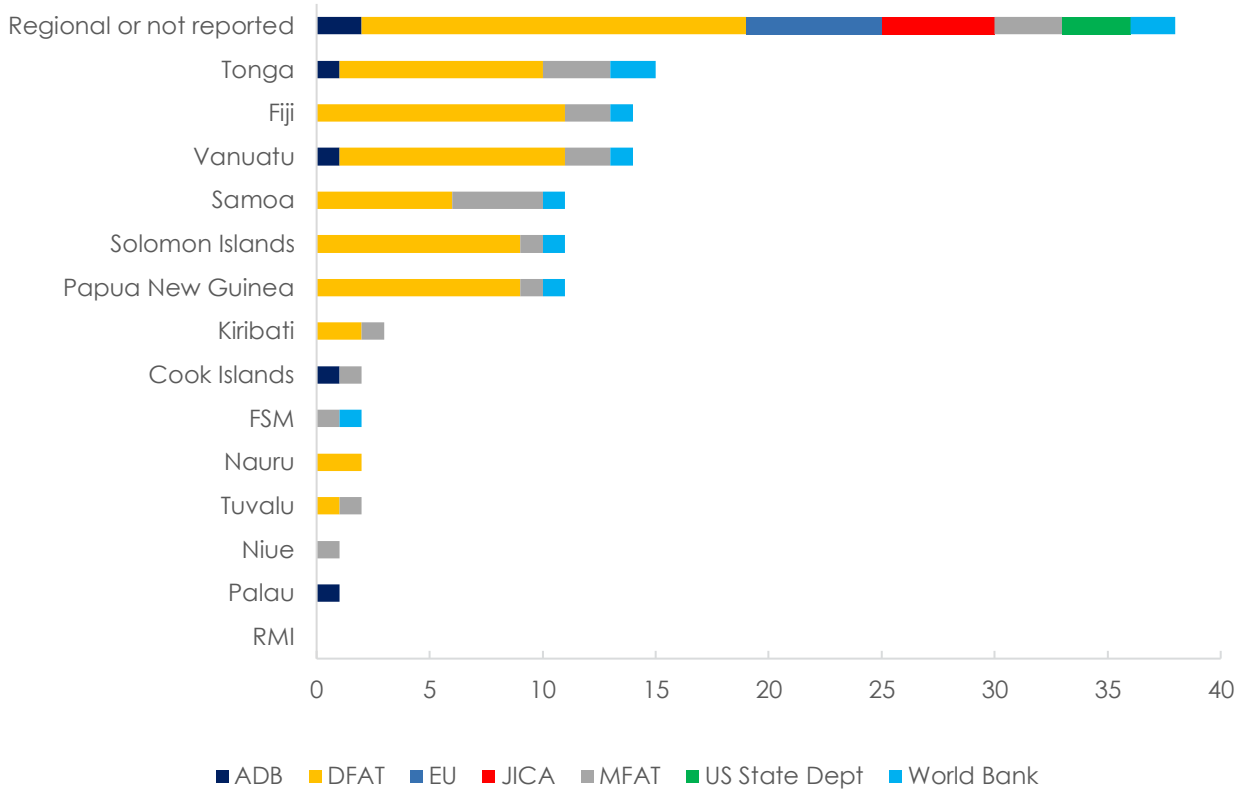
2.2 Initiatives reported by PRIF development partners

Most initiatives appear to be delivered through regional or multi-country programs. In many cases, country-specific programming funded by donors was reported by implementing partners.

Partners with country initiatives reported across five or more countries include the Asian Development Bank, DFAT, the New Zealand Ministry of Foreign Affairs and Trade, and the World Bank. Partners where engagement was reported as concentrated in regional (or country not reported) initiatives include the European Union (EU), Japan International Cooperation Agency, and the US State Department (noting that country-specific programming may be in development).

No European Investment Bank initiatives on cybersecurity were reported.

Figure 4: Initiatives Reported by PRIF Development Partners (Count Attributed by Country)



ADB = Asian Development Bank, DFAT = Australian Government Department of Foreign Affairs and Trade, EU = European Union, FSM = Federated States of Micronesia, JICA = Japan International Cooperation Agency, MFAT = New Zealand Ministry of Foreign Affairs and Trade, PRIF = Pacific Region Infrastructure Facility, RMI = Republic of Marshall Islands, US = United States.

Source: stakeholder survey responses

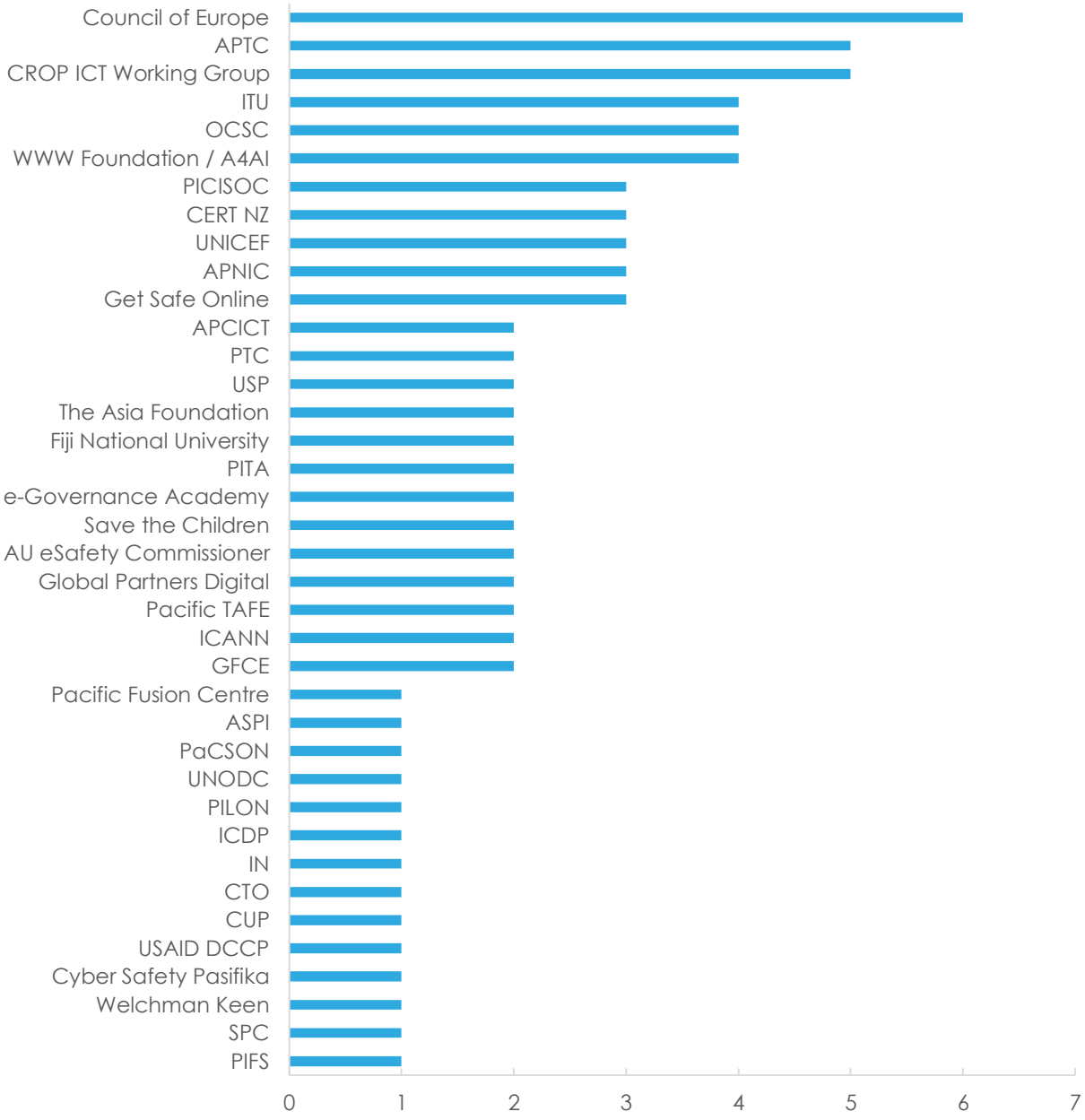
Notes: [1] Counts include single initiatives reported for multiple countries; [2] Excludes bilateral initiatives reported by other government agencies (e.g., PaCSON / NZ CERT).

2.3 Initiatives reported by non-member stakeholders

Many other organizations are active on cybersecurity in the region, highlighting the importance of continued coordination. These stakeholders include several implementing partners, technical IGOs, and universities and other educational institutions.

Most reported two or fewer initiatives; however, a larger number of initiatives were reported by groups such as the Council of Europe, Asia-Pacific Telecommunity (APT), the ITU and Pacific Islands Chapter of the Internet Society (PICISOC).

Figure 5: Initiatives Reported by Other Regional Stakeholders (Count)



ACSC = Australian Cyber Security Centre, A4AI = Alliance For Affordable Internet, APCICT = Asian and Pacific Training Centre for Information and Communication Technology for Development, APT = Asia-Pacific Telecommunity, ASPI = Australian Strategic Policy Institute, APNIC = Asia Pacific Network Information Centre, APTC = Australia Pacific Training Coalition, CERT NZ = Computer Emergency Response Team New Zealand,

CTO = Commonwealth Telecommunications Organisation, CROP = Council of Regional Organisations of the Pacific, GFCE = Global Forum on Cyber Expertise , ICANN = Internet Corporation for Assigned Names and Numbers, ICDP = International Centre for Democratic Partnerships, IGO = intergovernmental organization, ITU = International Telecommunication Union, NGO = nongovernment organization, OCSC = Oceania Cyber Security Centre, PaCSON = Pacific Cyber Security Operational Network, PICISOC = Pacific Islands Chapter of the Internet Society, PILON = Pacific Islands Law Officers' Network, PITA = Pacific Islands Telecommunications Association, PTC = Pacific Telecommunications Council, SPC = Secretariat of the Pacific Community, WWW = World Wide Web, TAFE = Technical and Further Education, UNICEF = United Nations International Children's Emergency Fund, UNODC = United Nations Office on Drugs and Crime

Source: Stakeholder survey responses.

Note: [1] Counts include initiatives reported by multiple funders and implementing agencies.

2.4 Other stakeholders identified

2.4.1 Country survey responses

In their response to the survey questionnaire, PRIF member countries identified initiatives (n = 71) that were mostly funded by stakeholders also identified in the survey (n = 47), or where their own national funding source was reported (n = 13). In most cases, the country-reported initiatives appear to be related to those already identified in stakeholder surveys.

A small number of additional funding sources were identified. These included bilateral support from the following sources:

- The Australian Government Attorney General's Department (n =1)
- The People's Republic of China (n = 1)

As well as support from international NGOs:

- The United Nations Development Programme (n = 1)

A further breakdown of these initiatives from other funding sources is included in Section 3.

A further eight initiatives reported by PRIF member countries had no funding source reported – however, many of these may benefit from in-kind support, or indirect budget support. For example, Federated States of Micronesia (FSM) noted in its response that INTERPOL membership provides national law enforcement agencies with support on cybercrime, among other issues; however, they were not reported as a funding agency or delivery partner.

Several countries also identified bilateral support via agency-to-agency partnerships brokered through international NGOs, such as the APT.

2.4.2 Stakeholder survey responses

In their response to the survey questionnaire, stakeholders identified additional funding agencies and/or delivery partners not identified elsewhere.

The other stakeholders from both the country and stakeholder surveys are summarized in Table 6 below.

Table 6: Other Stakeholders Identified in Country and Stakeholder Survey Responses

Stakeholder	Type
Asian Development Bank Private Sector Development Initiative (PSDI)	Multilateral Donor
Australian Federal Police (AFP)	Law Enforcement
Australian Government Attorney-General's Department	Government Agency
Australian Government Department of Communications and the Arts	Government Agency
Bill & Melinda Gates Foundation	International NGO
Computer Emergency Response Team Vanuatu (CERT VU)	Government Agency
Estonia Development Cooperation	Bilateral Donor
Estonian Centre for International Development (ESTDEV)	Bilateral Donor
Estonian Government Ministry of Foreign Affairs	Government Agency
European Commission Service for Foreign Policy Instrument (FPI)	Government Agency
Facebook	Private Sector
Federal Republic of Germany	Bilateral Donor
Federal Republic of Germany Foreign Office	Bilateral Donor
French Ministry for Europe and Foreign Affairs	Bilateral Donor
Global Cyber Security Capacity Centre (GCSCC)	International NGO
Government of India (GOI)	Government Agency
Government of Israel Ministry of Economy and Industry	Government Agency
Government of Israel National Cyber Directorate	Government Agency
Government of Japan Ministry of Foreign Affairs	Government Agency
Government of Japan Ministry of Internal Affairs and Communication (MIC)	Government Agency
Government of Republic of Korea (GOK)	Bilateral Donor
Government of Thailand	Bilateral Donor
Government of Estonia	Bilateral Donor
International Multilateral Partnership Against Cyber Threats (IMPACT)	International IGO
Korea Internet & Security Agency (KISA)	Government Agency
Ministry of Foreign Affairs of the Netherlands	Government Agency
Monash University	University
Network Startup Resource Center (NSRC)	International NGO
Oxfam	International NGO
People's Republic of China (PRC)	Government Agency
Protection Group International (PGI)	Private Sector
United Kingdom Foreign Commonwealth and Development Office (FCDO)	Bilateral Donor
United Nations Development Programme (UNDP)	International IGO
United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP)	International NGO
University of Oregon	University
Vanuatu Bureau of Standards (VBS)	Government Agency
Vanuatu Internet Governance Forum (VanIGF)	National NGO
Vanuatu Police Force (VPF)	Law Enforcement
Vanuatu Telecommunications Radiocommunications and Broadcasting Regulator (TRBR)	Government Agency
Victoria State Government	Government Agency

IGO = intergovernmental organization, NGO = nongovernment organization.

Source: Country and stakeholder survey responses.

3 What Types of Initiatives Are They Working on?

3.1 Stakeholder initiatives by category

3.1.1 PRIF Development Partners

Initiatives reported by PRIF Development Partners primarily addressed Cybersecurity, followed by Training and Education, and Cybercrime. Bilateral Development Partners also reported Law and Policy initiatives. DFAT and the World Bank were the only donors reporting initiatives targeting Online Safety. DFAT also reported the most initiatives (n= 50) overall, and was the only Development Partner reporting initiatives across categories.

Table 7: Development Partner initiatives by category

Stakeholder	Total initiatives	Of which, address the following categories				
		Cybersecurity (other)	Online Safety	Cybercrime	Law And Policy	Training And Education
ADB	3	3	-	1	-	-
DFAT	50	26	10	8	10	19
EU	6	4	-	3	2	1
JICA	5	5	-	-	-	3
MFAT	9	8	-	3	1	7
US	3	3	-	-	1	-
World Bank	5	4	1	2	-	-
Total	81	53	11	17	14	30

ADB = Asian Development Bank, DFAT = Australian Government Department of Foreign Affairs and Trade, EU = European Union, FSM = Federated States of Micronesia, JICA = Japan International Cooperation Agency, MFAT = New Zealand Ministry of Foreign Affairs and Trade, PRIF = Pacific Region Infrastructure Facility, RMI = Republic of Marshall Islands, US = United States.

Source: Stakeholder survey responses

Notes: [1] Counts include initiatives reported by multiple funders and implementing agencies; [2] Initiatives can address more than category, therefore counts by category may exceed totals.; [3] USAID DCCP included here under US Department of State.

3.1.2 Stakeholder survey responses

Government agency / national NGOs reported a narrow focus by institution, except for the Oceania Cyber Security Centre (OCSC), which reported initiatives covering all categories.

International NGOs / IGOs likewise tended to focus on specific categories. For example, Council of Europe initiatives are focused on cybercrime and law and policy. Most international NGOs / IGOs are focused on general cybersecurity and / or online safety, and training and education.

Regional NGO / IGO initiatives are mostly focused on general cybersecurity improvements, followed by cybercrime, online safety and training and education. APT and PICISOC reported initiatives covering all categories.

Across all stakeholders, fewer initiatives addressed the cybercrime and law and policy categories.

Stakeholder initiatives reported by category are shown in Table 8.

Table 8: Stakeholder Initiatives by Category

Stakeholder	Total initiatives	Of which, address the following categories				
		Cybersecurity (other)	Online Safety	Cybercrime	Law And Policy	Training And Education
Government agency / national NGO						
OCSC	4	3	2	3	3	3
CERT NZ	3	3	-	-	-	3
eSafety Commissioner	2	-	2	1	-	-
Government of India	1	-	-	-	-	1
ASPI	1	1	-	-	-	-
Standards Australia	1	1	-	-	-	-
International NGOs / IGOs						
Council of Europe	8	-	-	8	8	-
ITU	5	5	-	-	-	2
WWW Foundation / A4AI	4	1	4	-	-	1
Get Safe Online	3	2	1	-	-	3
GFCE	2	2	-	-	-	2
UNICF	3	-	3	-	-	1
Global Partners Digital	2	1	-	-	2	-
ICANN	2	2	-	-	-	1
Save the Children	2	-	2	-	-	1
The Asia Foundation	2	1	2	-	-	-
APCICT	3	-	-	-	-	3
UNODC	1	1	-	1	-	1
e-Governance Academy	2	2	-	-	-	-
ICDP	1	1	1	-	-	-
CTO	1	1	-	-	-	-
Regional NGOs / IGOs						
APT	5	2	2	2	5	4
PICISOC	4	4	4	2	2	1
CROP ICT Working Group	5	4	4	3	-	1
Pacific Fusion Centre	2	2	-	1	-	1
Cyber Safety Pasifika	1	1	1	1	-	-
APNIC	3	2	-	-	-	1
ACSC / PaCSON	1	1	1	-	-	-
Pacific Island Forum	1	1	-	1	-	-
PITA	2	1	-	-	-	1
PTC	2	1	-	-	-	1
PILON	1	-	-	1	-	-
SPC	1	-	-	-	1	-
Private Sector / Education						
Pacific TAFE	2	-	-	-	-	2
Welchman Keen	1	1	-	-	-	1
Fiji National University	2	-	-	-	-	2
USP	2	1	-	-	-	1
APTC	1	-	-	-	-	1
Christ's University in Pacific	1	-	-	-	-	1
Total	90	n/a	n/a	n/a	n/a	n/a

ACSC = Australian Cyber Security Centre, A4AI = Alliance For Affordable Internet, APCICT = Asian and Pacific Training Centre for Information and Communication Technology for Development, APT = Asia-Pacific Telecommunity, ASPI = Australian Strategic Policy Institute, APNIC = Asia Pacific Network Information Centre, APTC = Australia Pacific Training Coalition, CERT NZ = Computer Emergency Response Team New Zealand, CTO = Commonwealth Telecommunications Organisation, CROP = Council of Regional Organisations of the Pacific, GFCE = Global Forum on Cyber Expertise , ICANN = Internet Corporation for Assigned Names and Numbers, ICDP = International Centre for Democratic Partnerships, IGO = intergovernmental organization, ITU = International Telecommunication Union, NGO = nongovernment organization, OCSC = Oceania Cyber Security Centre, PaCSON = Pacific Cyber Security Operational Network, PICISOC = Pacific Islands Chapter of the Internet Society, PILON = Pacific Islands Law Officers' Network, PITA = Pacific Islands Telecommunications Association, PTC = Pacific Telecommunications Council, SPC = Secretariat of the Pacific Community, WWW = World Wide Web, TAFE = Technical and Further Education, UNICEF = United Nations International Children's Emergency Fund, UNODC = United Nations Office on Drugs and Crime

Notes: [1] Counts include initiatives reported by multiple funders and implementing agencies; [2] Initiatives can address more than category, therefore counts by category may exceed totals.

Source: Stakeholder survey responses.

4 Which Countries Are Stakeholders Working in?

4.1 Categories addressed by initiatives in each country

Most initiatives reported by stakeholders are focused on core cybersecurity activities, followed by training and education. Fewer initiatives address online safety, law and policy, and cybercrime. Smaller countries, in particular, appear to have only limited support in these areas. The number of initiatives by category and country are shown in Figure 6.

Figure 6: Categories Addressed by all Stakeholder Initiatives, by Country

Country	Cybersecurity (other)	Training And Education	Online Safety	Law And Policy	Cybercrime
Regional or not reported	52	18	22	16	36
Tonga	22	15	10	8	7
Vanuatu	22	15	6	10	6
Samoa	21	14	7	7	4
Fiji	20	14	8	7	3
PNG	20	14	8	4	3
Solomon Islands	22	10	8	5	2
Kiribati	12	11	4	4	1
Tuvalu	10	6	4	2	1
Nauru	8	5	3	2	1
FSM	4	4	2	4	3
Niue	3	3	1	1	1
Cook Islands	4	2	-	-	-
Palau	2	1	-	-	-
RMI	-	-	-	-	-

FSM = Federated States of Micronesia, PNG = Papua New Guinea, RMI = Republic of Marshall Islands.

Notes: [1] Counts include initiatives reported by multiple funders and implementing agencies; [2] Initiatives can address more than category, therefore counts by category may exceed totals.

Source: Stakeholder survey responses.

4.2 Which stakeholders are active in each country?

4.2.1 PRIF Development Partners

Most initiatives reported by PRIF Development Partners were regional in nature or otherwise did not report targeting specific countries (n = 38). Tonga, Fiji, Vanuatu, Samoa, Solomon Islands and Papua New Guinea were the focus of the most initiatives (n > 10 each). None were reported for RMI, and only a small number reported for most other countries. NZ MFAT, AG DFAT and the World Bank had the most initiatives targeting specific countries. The US DOS, EU and JICA reported initiatives which were all Regional / Not Reported to be targeting specific countries.

PRIF Development Partners initiatives by country are shown in Table 9.

Table 9: Development Partner initiatives by country

Stakeholder	Total initiatives	Of which, target the following countries															Number of countries
		Regional / Not reported	Tonga	Fiji	Vanuatu	Samoa	Solomon Islands	PNG	Kiribati	Cook Islands	FSM	Tuvalu	Nauru	Niue	Palau	RMI	
MFAT	9	3	3	2	2	4	1	1	1	1	1	1	-	1	-	-	11
DFAT	50	17	9	11	10	6	9	9	2	-	-	1	2	-	-	-	9
World Bank	5	2	2	1	1	1	1	1	-	-	1	-	-	-	-	-	7
ADB	3	2	1	-	1	-	-	-	-	1	-	-	-	-	1	-	4
US	6	6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
EU	5	5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
JICA	3	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

ADB = Asian Development Bank, DFAT = Australian Government Department of Foreign Affairs and Trade, EU = European Union, FSM = Federated States of Micronesia, JICA = Japan International Cooperation Agency, PNG = Papua New Guinea, MFAT = New Zealand Ministry of Foreign Affairs and Trade, RMI = Republic of Marshall Islands, US = United States Department of State.

Notes: [1] Counts include initiatives reported by multiple funders and implementing agencies; [2] Initiatives can target more than country, therefore counts by country may exceed totals.

Source: Stakeholder survey responses

4.2.2 Stakeholder survey responses

Most initiatives reported by stakeholders were regional in nature or otherwise did not report targeting specific countries (n = 46). Tonga, Vanuatu, Fiji, and Samoa were the focus of the most initiatives (n > 20), followed by PNG (n = 19), Solomon Islands (n = 17), and Kiribati (n = 14). Fewer initiatives targeted Nauru, Tuvalu, and FSM (n < 10). Very few were reported for Cook Islands, Niue, and Palau (n = 2) and none were reported for RMI.

The most prolific stakeholders were national government agencies and NGOs operating bilaterally, in particular, CERT NZ (12 countries), the OCSC (10 countries) and the ACSC / PaCSON (nine countries). This was followed by international NGOs and IGOs, such as Get Safe Online, GFCE and Global Partners Digital (nine countries, respectively) and the ITU (seven countries).

Regional IGOs reported fewer country-specific initiatives, led by Asia Pacific Network Information Centre (APNIC, eight countries), Secretariat of the Pacific Community (SPC, seven countries) and PICISOC (four countries). Of education stakeholders, Fiji National University (seven countries) reported the most country-specific initiatives.

Stakeholder initiatives by country are shown in Table 10.

Table 10: Stakeholder Initiatives by Country

Stakeholder	Total initiatives	Of which, target the following countries															Number of countries
		Regional / Not reported	Tonga	Vanuatu	Fiji	Samoa	Papua New Guinea	Solomon Islands	Kiribati	Nauru	Tuvalu	FSM	Cook Islands	Niue	Palau	RMI	
Government agency / national NGO																	
OCSC	4	-	2	1	1	1	2	-	2	-	2	2	1	1	-	-	10
CERT NZ	3	2	1	1	1	1	1	1	1	1	1	-	1	1	1	-	12
ACSC/ PaCSON	1	-	1	1	1	1	1	1	1	1	1	-	-	-	-	-	9
eSafety Commissioner	2	-	1	-	1	-	-	-	-	-	-	-	-	-	-	-	2
Government of India	1	-	-	1	-	1	-	-	-	-	-	-	-	-	-	-	2
ASPI	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Standards Australia	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
International NGOs / IGOs																	
Get Safe Online	3	-	3	2	2	2	2	2	2	2	2	-	-	-	-	-	9
ITU	5	1	2	3	1	2	3	2	2	-	-	-	-	-	-	-	7
GFCE	2	1	1	1	1	1	1	1	1	1	1	-	-	-	-	-	9
Global Partners Digital	2	1	1	1	1	1	1	1	1	1	1	-	-	-	-	-	9
ICDP	1	-	1	1	1	1	1	1	1	1	1	-	-	-	-	-	9
Council of Europe	8	4	-	2	1	-	-	-	-	1	-	-	-	-	-	-	3
The Asia Foundation	2	1	1	1	1	-	1	1	-	-	-	-	-	-	-	-	5
Save the Children	2	1	1	-	1	1	1	-	-	-	-	-	-	-	-	-	4
WWW Foundation / A4AI	4	3	-	-	1	-	-	-	-	-	-	-	-	-	-	-	1
UNICEF	3	1	-	-	-	1	-	1	-	-	-	-	-	-	-	-	2
APCICT	3	1	1	-	-	1	-	-	-	-	-	-	-	-	-	-	2
ICANN	2	1	-	-	1	-	-	-	-	-	-	-	-	-	-	-	1
e-Governance Academy	2	1	-	1	-	-	-	-	-	-	-	-	-	-	-	-	1
CTO	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
UNODC	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Regional NGOs / IGOs																	

Stakeholder	Total initiatives	Of which, target the following countries															Number of countries
		Regional / Not reported	Tonga	Vanuatu	Fiji	Samoa	Papua New Guinea	Solomon Islands	Kiribati	Nauru	Tuvalu	FSM	Cook Islands	Niue	Palau	RMI	
APNIC	3	-	2	2	2	2	2	2	1	1	-	-	-	-	-	-	8
SPC	1	-	1	1	1	1	1	1	1	-	-	-	-	-	-	-	7
PICISOC	4	2	1	1	-	1	-	2	-	-	-	-	-	-	-	-	4
CROP ICT Working Group	5	4	-	-	1	-	-	-	-	-	-	-	-	-	-	-	1
APT	5	3	-	-	-	-	-	-	-	-	-	2	-	-	-	-	1
Pacific Island Forum	1	-	1	-	-	1	1	-	-	-	-	-	-	-	-	-	3
Pacific Fusion Centre	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
PITA	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
PTC	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Cyber Safety Pasifika	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
PILON	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Private Sector / Education																	
Fiji National University	2	1	1	1	1	1	1	1	1	-	-	-	-	-	-	-	7
Pacific TAFE	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
USP	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
APTC	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Christ's University in Pacific	1	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	1
Welchman Keen	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

ACSC = Australian Cyber Security Centre, A4AI = Alliance For Affordable Internet, APCICT = Asian and Pacific Training Centre for Information and Communication Technology for Development, APT = Asia-Pacific Telecommunity, ASPI = Australian Strategic Policy Institute, APNIC = Asia Pacific Network Information Centre, APTC = Australia Pacific Training Coalition, CERT NZ = Computer Emergency Response Team New Zealand, CTO = Commonwealth Telecommunications Organisation, CROP = Council of Regional Organisations of the Pacific, GFCE = Global Forum on Cyber Expertise , ICANN = Internet Corporation for Assigned Names and Numbers, ICDP = International Centre for Democratic Partnerships, ITU = International Telecommunication Union, OCSC = Oceania Cyber Security Centre, PaCSON = Pacific Cyber Security Operational Network, PICISOC = Pacific Islands Chapter of the Internet Society, PILON = Pacific Islands Law Officers' Network, PITA = Pacific Islands Telecommunications Association, PTC = Pacific Telecommunications Council, SPC = Secretariat of the Pacific Community, WWW = World Wide Web, TAFE = Technical and Further Education, UNICEF = United Nations International Children's Emergency Fund, UNODC = United Nations Office on Drugs and Crime.

Notes: [1] Counts include initiatives reported by multiple funders and implementing agencies; [2] Initiatives can target more than one country, therefore counts by country may exceed total initiatives.

Source: stakeholder survey responses

5 Country Survey Results

5.1 PRIF member countries' own initiatives

In their response to the survey questionnaire, PRIF member countries identified initiatives that reported own-national funding (n = 13). These were reported by PNG, Fiji, Nauru, Niue, Tuvalu, and Vanuatu, and are shown in Table 11.

Table 11: Country Initiatives, Own-Funding Agency

Funding Agency	Reporting Country	Category	Initiative Name	Status
Department of Information and Communications Technology	Papua New Guinea	Cybersecurity, Law and Policy,	Cybersecurity Bill	Completed
Department of Information and Communications Technology	Papua New Guinea	Cybersecurity, Law and Policy	National Cybersecurity policies, Digital Transformation activities, Data Protection plans, etc.	Ongoing
Government of Fiji	Fiji	Cybersecurity, Law and Policy	Critical Infrastructure – National Cyber Incident Response and Recovery Framework	Ongoing
Government of Fiji	Fiji	Cybercrime, Law and Policy	Cybercrime Act 2021	Completed
Government of Fiji	Fiji	Online Safety, Law and Policy	Establishment of Online Safety Commission, through the introduction of the Online Safety Act 2018	Completed
Government of Fiji	Fiji	Cybersecurity, Law and Policy	National Cybersecurity Strategy	Completed
Government of Nauru	Nauru	Cybersecurity	Cyber Security Awareness Team – focus on security of government infrastructure	Ongoing
Government of Niue	Niue	Cybersecurity	Niue ICT Committee – ICT technical advisory and Cybersecurity	Ongoing
Government of Tuvalu	Tuvalu	Law and Policy	Regulatory Activities	Ongoing
Office of the Government Chief Information Officer; CERT Vanuatu	Vanuatu	Online Safety	Introduce new legislations to support the Cybercrime Act of 2021 – Against harmful online content	Ongoing
Office of the Government Chief Information Officer; CERT Vanuatu	Vanuatu	Cybersecurity, Law and Policy	ISO 27000 Certification Standards	Ongoing
Vanuatu Internet Governance Forum	Vanuatu	Online Safety	TV/Radio Campaigns	Ongoing
Vanuatu Internet Governance Forum; Office of the Government Chief Information Officer	Vanuatu	Online Safety, Training and Education	Community Outreach (with CERT Vanuatu; Vanuatu Bureau of Standards; Vanuatu Police Force; TRBR Vanuatu)	Ongoing

CERT = Computer emergency response team, TRBR = Telecommunications Radiocommunications and Broadcasting Regulator.

Source: Country survey responses.

Of note is that these own-funding agency initiatives are mostly in the countries with more mature cybersecurity arrangements, and do not obviously address the gap in coverage of regional and bilateral stakeholder initiatives for the Cook Islands, Niue, Palau, and the RMI.

Most initiatives by own-funding agencies are focused on foundational activities to introduce legal and policy frameworks, and embryonic development of cybersecurity / response capabilities. No programs were identified that focus on industry and physical infrastructure vulnerabilities.

5.2 Other funding agencies identified in country responses

In their response to the survey questionnaire, PRIF member countries identified initiatives that were mostly funded by stakeholders also identified in the stakeholder survey. A small number of initiatives were identified by countries as being undertaken with the support of other funding agencies. These initiatives, and the categories addressed are summarized in Table 12 below.

Table 12: Country Initiatives, Funding Agency not Reported Elsewhere

Funding Agency	Reporting Country	Category	Initiative Name	Status
Attorney General's Department, Australia	Solomon Islands	Cybercrime, Law and Policy	Cybercrime bill	Not reported
People's Republic of China	Kiribati	Training and Education	Cybersecurity Training	Not reported

Source: Country survey responses.

5.3 Status and duration of initiatives

5.3.1 Status of initiatives

As at June 2022, initiatives reported by stakeholders mostly have a status of In Progress or Ongoing (49.7%), and a smaller cohort of planned projects (13.5%) – most of which were identified by bilateral donors. 63 of the initiatives reported by stakeholders had a status of Complete (36.8%). These results are summarized in Table 13.

Table 13: Stakeholder Initiatives by Status

Stakeholder type	Completed	In progress / Ongoing	Planned	Total
Bilateral donor	29	27	17	73
Multilateral donor	3	5	0	8
Government agency / national NGO	4	7	1	12
International NGOs / IGOs	22	13	3	38
Regional NGOs / IGOs	4	24	1	29
Private Sector / Education	1	9	1	11
Other / Not reported	0	0	0	0
Total	**63**	**85**	**23**	**171**
Total (% of initiatives)	**36.8%**	**49.7%**	**13.5%**	**100.0%**

IGO = intergovernmental organization, NGO = nongovernment organization.

Source: Stakeholders survey responses.

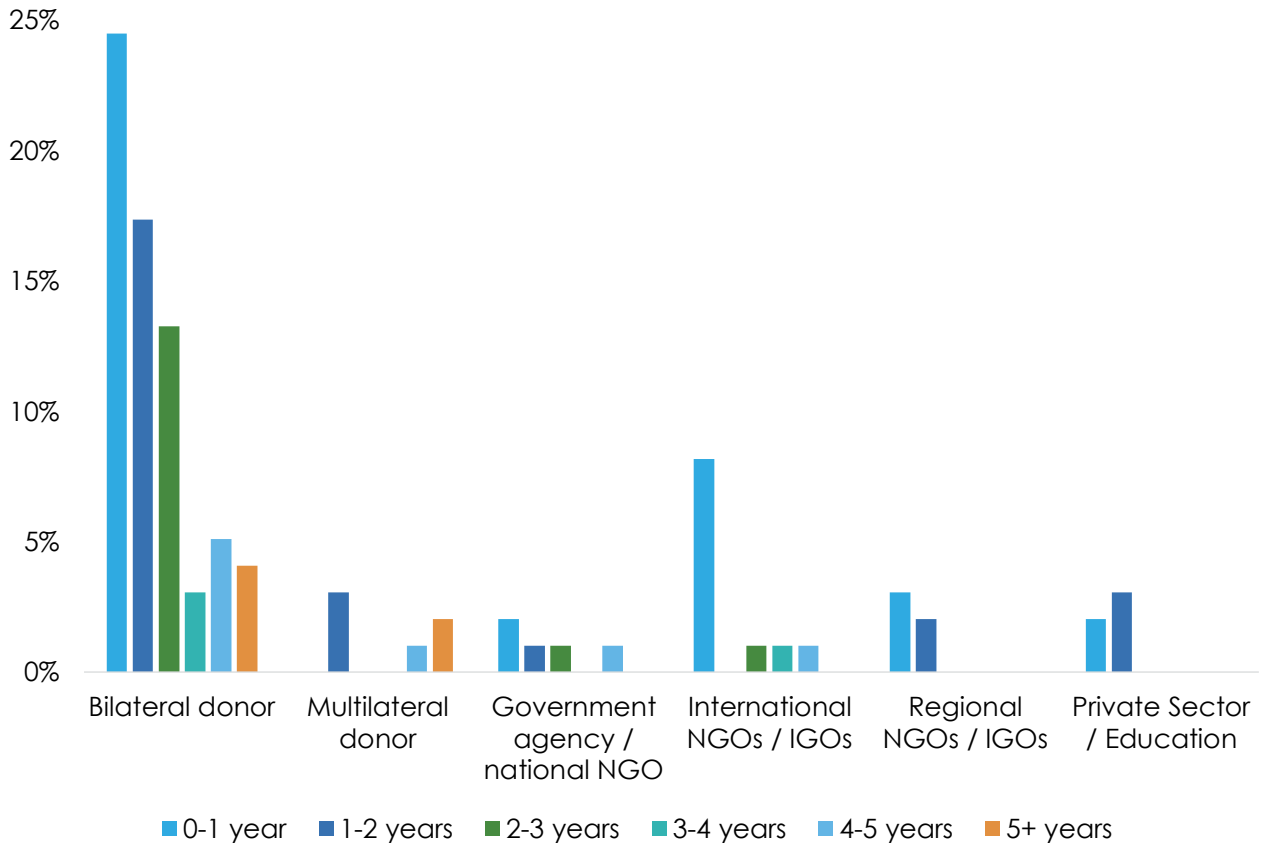
The low number of planned initiatives reported by NGOs and IGOs is likely reflective of their dependence on access to external funding. Many initiatives undertaken by these groups are typically either responsive to member demand and/or driven by funding provided by third parties. Given the significant role of these groups in delivering initiatives in the region, the lack of visibility about planned initiatives is a significant gap – and a potential risk area for overlaps in the future.

5.3.2 Duration of initiatives

Initiatives reported by stakeholders tended to be short term, with most initiatives having a reported duration of 1—2 years.

Of the 171 stakeholder initiatives reported, a duration estimate was provided for 98 (57.3%). Many initiatives with no duration estimated were reported to be "ongoing" but are excluded from the analysis of duration shown in Figure 7.

Figure 7: Duration of Initiatives by Stakeholder Group (%, Initiatives with Reported Duration)



IGO = intergovernmental organization, NGO = nongovernment organization.

Source: stakeholder survey responses.

As can be seen, medium-term initiatives, with a duration of 2 or more to 5 years are few, and were primarily reported by bilateral and multilateral donors. Interestingly, while fewer overall, initiatives reported by government agencies / national NGOs tended to be proportionally higher in the number of these medium-term projects. This may reflect greater stability in funding relatively to regional and international NGOs / IGOs.

Private Sector / Education respondents appear to have reported duration of courses provided (e.g., a 3-day training course offered on a recurring basis). As such, comparisons of reported duration with

the time bound funding of programmatic initiatives reported by other stakeholders are not recommended.

For initiatives where an expected completion date was provided, none are expected to occur beyond 2025.

5.4 How well do initiatives address gaps and risks?

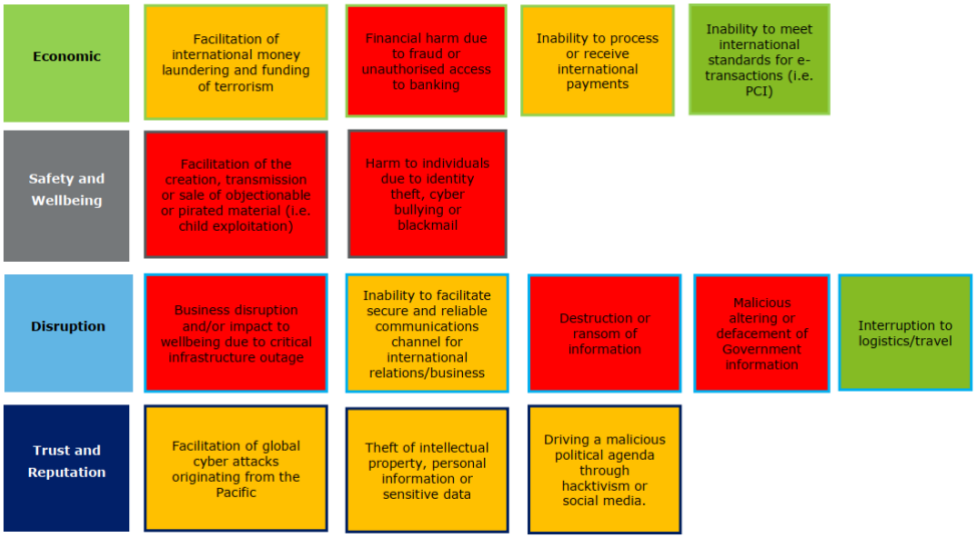
5.4.1 Gaps and risks identified in PRIF's 2019 Cybersecurity study

To provide context to the stakeholder survey responses, key gaps and risks identified in earlier reports are summarized below. The 2019 PRIF study on *Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands*[9] included both a 'Cyber Risk Assessment' and 'Policy and Legal Gap Analysis' which highlighted key cybersecurity gaps and risks across PRIF Member Countries. The highest rated risks were:

- **Economic**: 'Financial harm due to unauthorised access to banking'
- **Safety and Wellbeing**: 'Facilitation of the creation, transmission or sale of objectionable or pirated material'; and 'Harm to individuals due to identity theft, cyber bullying or blackmail'.
- **Disruption**: 'Business disruption and/or impact to wellbeing due to critical infrastructure outage'; 'Destruction or ransom of information; Malicious altering or defacement of Government information'

The 2019 'Cyber Risk Assessment' identified fourteen key types of cyber risks across four harm areas, and rated on their potential impact and likelihood (Figure 8).

Figure 8: Cyber Risk Assessment



Source: PRIF 2019 Cybersecurity and Safeguarding Electronic Transaction in The Pacific Islands

[9] Pacific Region Infrastructure Facility. 2019. Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands. https://www.theprif.org/document/regional/information-and-communications-technology-ict/cybersecurity-and-safeguarding

The report noted that Financial losses through fraud/scams, and the protection of children from cyber bullying and exploitation are the highest current realized cyber risks for the region

However, it was also noted that the need to address growing cyber risks was critical. Cyber incidents being experienced by PRIF member countries included financial harm, disruption of system resilience, severe harm to well being, and reputational harm.

A key observation of the 2019 study was the reliance of many countries on pan-regional mechanisms for support on cyber issues.

Similarly, the 'Policy and Legal Gap Analysis' considered challenges and opportunities in existing legal and regulatory frameworks at both a country and regional level. Key regional opportunities were identified as:

- implementing cybersecurity and digital strategy in the region and developing a consistent approach to coordinating strategy across the Pacific, where interconnectedness requires a coordinated and consistent approach;
- preparing a legal framework which sets out key functions and responsibilities of cyber stakeholders, deals with cybercrime, and allocates funding;
- building capacity at a regulatory, enforcement and technical level and identifying a clear strategy or funding to develop regional resource and capacity;
- improving cybersecurity safeguards for critical infrastructure; and
- increasing public awareness of cybersecurity and digital issues.

Overall it was recommended that urgency should be attached to implementing cybersecurity building blocks in each country, over commercial law frameworks.

At the most basic level it was recommended that developing cybersecurity strategies, capacity and awareness building and safeguarding critical infrastructure across the region are high priority needs, to ensure Pacific countries are not left vulnerable as the region becomes more connected, digitally focused and, consequently, a potential target for hackers and fraudulent digital operators.

The 'Policy and Legal Gap Analysis' in the 2019 report involved a review of the policy and legal frameworks in place in each of the participating countries. It highlighted the challenges and opportunities in existing legal and regulatory frameworks and offered recommendations on a way forward (at both a domestic and regional level).

The report noted the low level of cyber security maturity across the region was highlighted as significant challenge. Many countries had no strategy or work plan to uplift cyber security, and key roles and institutions had not been established/defined.

The country level key findings are shown in Figure 9.

Figure 9: Policy and Legal Gap Analysis

Stage of development	None	Initial	Established	Sophisticated

Country	CI	FJ	FSM	KI	RMI	NR	NU	PW	PNG	WS	SB	TO	TV	VU
Strategy and governance														
National cybersecurity strategy	I	E	I	I	N	I	N	N	E	E	N	I	I	E
Governance	I	E	I	E	I	E	I	N	E	E	N	E	E	E
Security														
Institutions	I	I	I	I	I	I	I	N	E	E	N	E	I	E
Critical infrastructure	I	N	N	N	N	N	N	N	N	I	N	E	N	I
Vigilance														
Incident reporting	I	I	I	N	N	I	I	I	I	N	I	I	I	I
Domestic cooperation	I	E	N	I	N	E	N	N	I	E	N	I	N	I
International cooperation	E	I	I	I	I	E	I	I	I	I	I	E	I	E
Resilience														
Cybercrime (substantive)	I	E	N	E	I	S	N	I	S	E	I	E	I	I
Cybercrime (child protection)	I	N	N	E	I	S	I	E	E	E	N	E	N	E
Cybercrime (procedural)	I	I	I	E	I	S	I	I	S	I	I	E	I	I
Law enforcement	I	I	I	I	I	I	I	I	I	I	I	I	I	I
Prosecution	I	I	I	I	I	I	I	I	I	I	I	I	I	I
Courts	I	I	I	I	I	I	I	I	I	I	I	I	I	I
Legal and regulatory frameworks														
Electronic transactions	I	E	N	N	N	N	N	N	N	E	N	N	N	E
Privacy, freedom of speech and other human rights online	I	I	I	I	E	I	N	I	I	I	I	N	I	I
Data protection	N	I	N	N	I	N	N	I	I	I	N	I	N	I
Digital authentication	I	N	N	N	I	N	N	N	I	I	N	I	N	N
ccTLD administration	E	E	E	E	I	E	E	E	I	E	I	I	E	I
Consumer protection	S	E	N	E	E	I	I	E	E	E	I	E	N	I
Intellectual property legislation	E	E	E	I	I	I	E	E	E	E	N	E	I	E
Access to information	E	E	N	I	I	I	N	E	N	I	N	I	I	E

Note: "Initial" means that the country is in the process of developing or implementing the concept measured and "Established" refers to a state where the relevant framework or concept is implemented and operates. Each of these ratings refers to the particular concept measured, and not the country's overall capacity to respond to cyber-risk.

Source: PRIF 2019 Cybersecurity and Safeguarding Electronic Transaction in The Pacific Islands

5.4.2 Comparison of initiatives with gaps and risks

Drawing on the gaps and risks identified in the PRIF 2019 study, the following analysis compares the initiatives identified in the Stakeholder surveys, based on key word matching.

Referring to heatmap in Table 14, gaps in initiatives addressing highest rated risks identified in the 2019 Cyber Risk Assessment include:

- Financial harm due to fraud or unauthorised access to banking
- Facilitation of objectionable or pirated material
- Business disruption and/or impact to wellbeing due to critical infrastructure outage

In most cases at least some initiatives are being undertaken to address these highest rated risks in a number of countries, as well as via regional initiatives. However the medium and low rated risks appear to have more broad based gaps in initiatives in addressing the following risks:

- Facilitation of international money laundering
- Inability to process or receive international payments
- Driving a malicious political agenda through hacktivism or social media
- Inability to meet international standards for e-transactions

Even where coverage is better, many initiatives are likely to be nascent, with capabilities remaining at an early stage e.g. e-KYC initiatives to address risks of financial harm or money laundering.

Table 14: Comparison of initiatives with Cyber Risk Assessment

Cyber Risk Assessment (2019)	Regional /	Cook	Fiji	FSM	Kiribati	Nauru	Niue	Palau	Papua	RMI	Samoa	Solomon	Tonga	Tuvalu
High														
Financial harm due to fraud or unauthorised access to banking														
Facilitation of objectionable or pirated material														
Harm to individuals through theft, bullying, blackmail														
Business disruption due to critical infrastructure outage														
Destruction / Ransom of Information														
Malicious altering or defacement of Government information														
Medium														
Facilitation of int'l money laundering														
Inability to process or receive intl. payments														
Inability to facilitate secure and reliable communications														
Facilitation of global cyber attacks originating from the Pacific														
Theft of IP, personal or sensitive data														
Driving a malicious political agenda through hacktivism or social media														
Low														
Inability to meet international standards for e-transactions														
Interruption to logistics/travel														

Source: Stakeholder survey responses; Dark Blue= Highest count, Light Blue = Lowest count, Red = None

For the 'Policy and Legal Gap Analysis', and referring to the heatmap in Table 15, gaps in initiatives include the following areas by stage of development.

None — Initial

- Critical infrastructure
- Electronic transactions

Initial — Established

- Governance
- Incident reporting
- International cooperation
- Courts
- Privacy, freedom of speech, and other human rights online

Established — Sophisticated

- Cybercrime (all types)
- ccTLD administration
- Consumer protection

Consistent with the earlier analysis in Sections 3 and 4 of this Report, gaps in country specific initiatives are most obvious in smaller countries, such as Cook Islands, Kiribati, Niue, Palau, RMI and Tuvalu.

In many cases, work on incident reporting is likely to be rolled up in support of CERT and cooperation initiatives.

Note that the observations here reflect a high level comparison only based on survey responses, and are presented without counts as keyword matching is imprecise. Many initiatives may target a number of areas, not obvious from the description or comments provided in survey responses. To support better targeting and cooperation, it is recommended that future information sharing initiatives adopt standardized reporting across more detailed categories – such as those used in relevant cybersecurity standards or capability frameworks.

Table 15: Comparison of initiatives with Policy and Legal Gap Analysis

	Regional	Cook Islands	FSM	Fiji	Kiribati	Nauru	Niue	Palau	Papua New	RMI	Samoa	Solomon	Tonga	Tuvalu	Vanuatu
Strategy and Governance															
National cybersecurity strategy															
Governance															
Security															
Institutions															
Critical infrastructure															
Vigilence															
Incident reporting															
Domestic cooperation															
International cooperation															
Resilience															
Cybercrime (substantive)															
Cybercrime (child protection)															
Cybercrime (procedural)															
Law enforcement															
Prosecution															
Courts															
Legal and regulatory frameworks															
Electronic transactions															
Privacy, freedom of speech, and other human rights online															
Data protection															
Digital authentication															
ccTLD administration															
Consumer protection															
Intellectual property legislation															
Access to information															

Source: Stakeholder survey responses; Dark Blue= Highest count, Light Blue = Lowest count, Red = None

6 Analysis and Discussion

The exercise was intended to establish an initial mapping of cybersecurity initiatives in the Pacific. As per the tabulated initiatives in Sections 2 through 5, the supporting database contains various attributes that are associated with each of the listed initiatives such as country of implementation, duration, etc. Other secondary attributes such as name and details of responders, email contact, etc., are included separately as an annexure.

The mapping is intended to improve the targeting and effectiveness of cybersecurity initiatives by development partners, funding agencies, and other implementation partners in the future.

As mapping has previously not been widely available for cybersecurity initiatives in the Pacific, many of the initiatives identified in the study appear to have been developed on an ad hoc basis – either in response to short-term needs, or as when funding and resourcing were made available for a limited number of countries in the region. Many countries, especially smaller countries, appear to rely on regional programs.

6.1 Key findings

The key findings of the study include the following.

1. **Continued coordination and visibility of initiatives is important** given the large number of organizations active in the region.

2. **Smaller countries rely heavily on regional support.** Most initiatives are delivered through regional or multi-country programs. Country-specific programming is focused on larger countries. Fewer country-specific initiatives addressed online safety, law and policy, and cybercrime.

3. **Many initiatives are relatively short term** and / or responsive to immediate needs (e.g., support for staffing of CERTs). Evidence of mainstreaming or ongoing sustainability of this model is limited as few member countries report initiatives that are self-funded. Few programs were identified which appear to focus on industry and physical infrastructure vulnerabilities.

4. **International and regional NGOs and IGOs similarly play an important role in delivery, but planned initiatives to be delivered by these organizations may lack visibility due to reliance on external funding.** The lack of visibility about planned initiatives from this group is a significant gap – and potential area for a risk of overlaps in the future.

5. **National government agencies and institutions are important implementing partners, particularly for online safety initiatives.** However, few countries reported initiatives independent of donor support.

6. **More granular analysis of initiatives is needed to better identify capability gaps.** The categories adopted in this study are high-level for the purpose of developing an initial mapping, but further detail will better support targeting and coordination on key gaps.

6.2 Recommendations

Further work on information sharing and investment coordination should focus on the following areas.

1. **Emphasize more programmatic approaches for funding and resourcing of embryonic cybersecurity capacity development in the region.** Less reactive, and more consistent models for multi-year support is needed to develop a more self-sustaining cybersecurity capacity in the region.

2. **Mainstreaming of cybersecurity capacity development into donor-funded initiatives** to catch up with accelerating internet penetration, digital government, and e-commerce initiatives. Key gaps in the initiatives identified are industry and critical infrastructure focused programs, electronic transactions, cybercrime, and ccTLD administration. **Provide ongoing access to regional programs and mechanisms for support for smaller countries,** which lack the scale to develop national technical capacity. Examples could include pairing of national ICT agencies and industry operators with trusted regional partners.

3. **Strengthen information sharing and awareness through relevant institutions.** Undertake periodic updates, and seek to boost awareness and dissemination among PRIF development partners and member countries – as well as other regional stakeholders. Examples include platforms such as GFCE's Cybil Knowledge Portal, as well as continued coordination and information sharing via regional and international working groups and events, such as the Pacific Cyber Capacity and Coordination Conference, and industry groups such as APT.

4. **Cybersecurity industry strategy should cultivate long-term engagement with International and regional NGOs and IGOs.** As key implementing partners, and hosts to technical skills and expertise in the region, maintaining engagement and the sustainability of participating in cybersecurity in the region should be a key consideration for development partners. Examples include better pipeline visibility, and early engagement on program design.

5. **Standardize reporting for future information-sharing initiatives.** This should include aligning with relevant capability models and standards – such as the Global Cyber Security Capacity Centre's Cybersecurity Capacity Maturity Model for Nations, the National Institute of Standards and Technology Cybersecurity Framework, and ISO/IEC 27000 Information Security Management Systems – as well as additional breakdowns of activities and outcomes aligned to these frameworks to support better targeting and design.

.

7 Conclusions

There have been numerous initiatives related to cybersecurity among PRIF's member countries; however, these have not always been widely shared, leading to risks of overlaps or gaps.

Since 2015, when the ITU launched its Global Cybersecurity Index (GCI) initiative to measure the cybersecurity commitment of 193 member states around the world, Pacific member countries have been introduced to the assessment questionnaire that requires them to provide responses based on the five strategic pillars - (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Development, and (v) Cooperation.

Many PRIF member countries have not maintained a comprehensive register of cybersecurity initiatives, or ICT initiatives more generally. This is very much reflected in their responses, or the lack thereof, to previous GCI questionnaires, and the survey distributed for this study.

This mapping exercise also highlights the extent mutual and indirect assistance provided to Pacific countries by development partners and a range of other stakeholders.

Continued and timely information sharing is imperative to ensure that efforts are focused on keeping pace with the exposure of the Pacific to cybersecurity risks.

There has been progress in number of areas, with several initiatives addressing key gaps identified in the 2019 PRIF study on *Cybersecurity and Safeguarding Electronic Transaction in The Pacific Islands*[10] . There are now a range of mechanisms in place to improve information sharing and coordination on cybersecurity. Most notably, through the recently established GFCE Pacific Hub.

Continued information sharing and coordination should remain a priority, and supports research, market studies, decision making by development partners, and for future mainstreaming of cybersecurity across other infrastructure sectors.

[10] Pacific Region Infrastructure Facility. 2019. Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands. https://www.theprif.org/document/regional/information-and-communications-technology-ict/cybersecurity-and-safeguarding

8 References

Bulletproof Cyber Limited. 2021. *Bulletproof Annual Cyber Security Industry Report 2021*. https://www.bulletproof.co.uk/industry-reports/bulletproof-annual-cyber-security-report-2021

International Telecommunication Union. 2015. *Global Cybersecurity Index 2014*, *Measuring Commitment to Cybersecurity*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

International Telecommunication Union. 2019. *Global Cybersecurity Index 2018*, *Measuring Commitment to Cybersecurity*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

International Telecommunication Union. 2021. *Global Cybersecurity Index 2020*, *Measuring Commitment to Cybersecurit*y. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Kuerbis, B. and F. Badiei. 2017. *Mapping the Cybersecurity Institutional Landscape*, *Digital Policy, Regulation and Governance*. Emerald Publishing Limited.

Sambuli, N., J. Maina and T. Kamau. 2016. *Mapping the Cyber Policy Landscape: Kenya*. Global Partners Digital.

Appendix A: Study methodology

Overview

A complete and inclusive policy approach needs to be taken in the Pacific that would a) capture comprehensively all aspects of security to ensure improvements in cybersecurity capabilities; b) establish trust and partnership with private and public entities; and c) strengthen an economy's engagement in risk management and response planning of their critical asset protection.

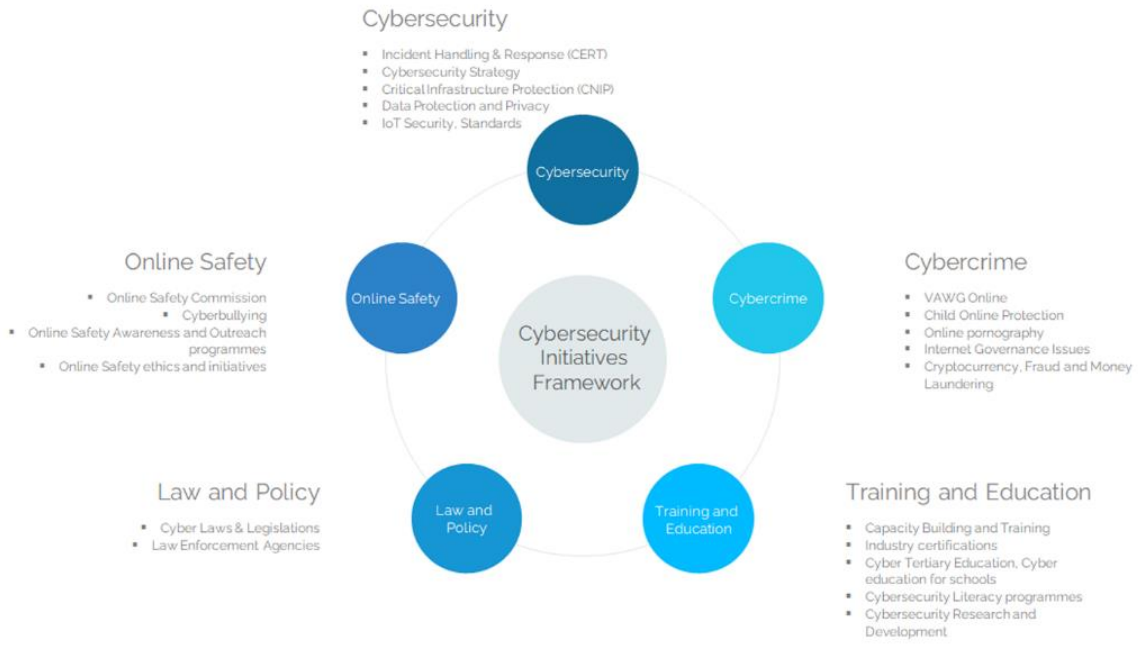
Establishing a proper understating of the cyber-landscape in the Pacific will present a detailed view of key initiatives, who is implementing them, and where all the development initiatives are focused.

Through the mapping exercise, this study will create synergies within all relevant stakeholders and identify gaps and overlaps in initiatives, something that will also allow donor agencies to focus on resourcing and assisting where it is really needed. Examples include:

- **Through better targeted development initiatives and capacity-building programs** in the Pacific, cyber-social concepts need to be embedded within security strategies and education programs, and most importantly, in the school systems vis-à-vis online safety ethics.
- **Increasing cybersecurity commitment levels** in the Pacific with more funding resources that need to be allocated toward the Pacific action on building cyber-resiliency.
- **Progressing the Pacific's cyber-landscape will require commitments from Pacific leaders** as well. Big steps need to be taken to develop regional cyber-constructs, driving growth in cyber-convergence for industries, and investing in cyber-research and development.
- **Allocating and mobilizing donor funding for cybersecurity initiatives** such as CERT setup and related technical assistance, mainly for smaller developing countries in the Pacific are equally needed.
- **Building partnerships and collaborative efforts** play a vital role in further progressing the regional cybersecurity works with relevant international organizations and agencies to develop policy guidance on the legislative, standards and operational requirements.
- **Ultimately working towards aligning the Pacific's cybersecurity to the global cybersecurity agenda**, to build a safer and trustworthy ICT and digital ecosystem for all Pacific citizens.
- **Creating opportunities for the ICT sector that makes an impact across the Pacific region** and seeing that ICT developments are also aligned with the United Nations Sustainable Development Goals.

To map cybersecurity initiatives across these outcomes, a cybersecurity initiative framework was developed for the study, addressing five key focus areas, as shown in Figure A1.1.

Figure A1.1: Cybersecurity Initiatives Framework Showing the Five Key Focus Areas.



IoT = Internet Of Things, VAWG = Violence Against Women & Girls

Source: Authors.

These focus areas are:

1. **Cybersecurity**
   Incident Handling & Response (CERT), Cybersecurity Strategy, Critical Infrastructure Protection (CNIP), Data Protection and Privacy, Internet Of Things Security, Standards

2. **Online Safety**
   Online safety commission, Cyberbullying, Online safety Awareness and outreach programs, Online Safety ethics and initiatives

3. **Cybercrime**
   Violence Against Women & Girls Online, Child Online Protection, Online pornography, Internet Governance Issues, Cryptocurrency, Fraud and Money Laundering,

4. **Laws and Policies**
   Cyber Laws & Legislations, Law Enforcement Agencies,

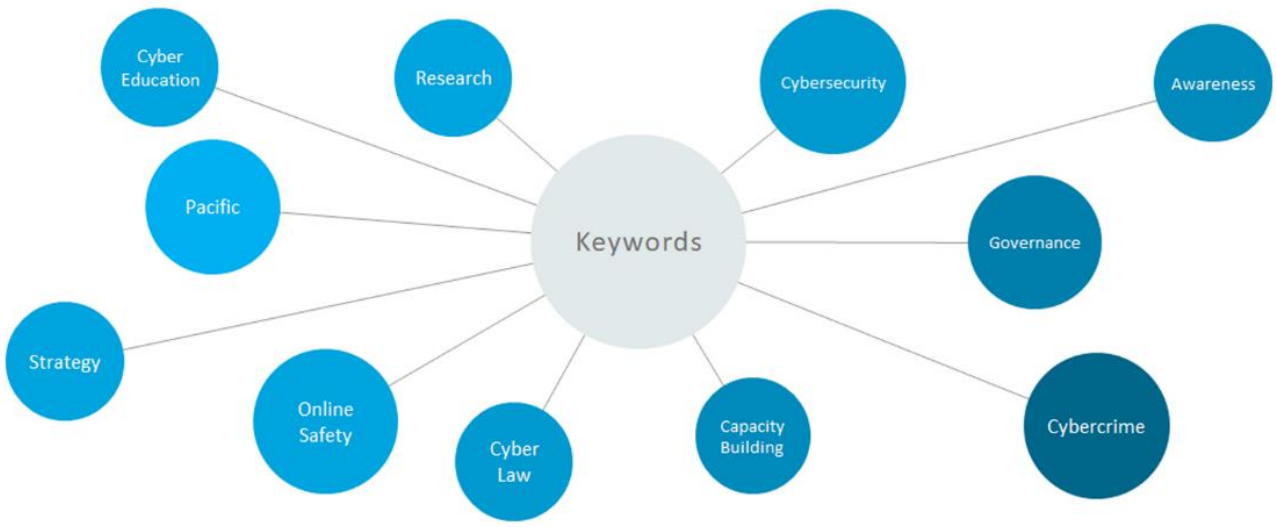
5. **Training and Education**
   Capacity Building and Training, Industry certifications, Cyber Tertiary Education, Cyber education for schools, Cybersecurity Literacy programs, Cybersecurity Research and Development

Data collection

The research data gathering employed a qualitative approach, which consisted of a literature review, and key informant interviews to establish the current and planned cybersecurity initiatives in the Pacific.

- The mapping and data collection exercise was conducted using secondary research methods through interviews, questionnaires, desk research, and other methods as necessary.
- The main sources for desk research involved status reports, journals, assessments, indexing, website information, new reports, information requests, etc.
- Keywords/Phrases were used to search for resources online such as:
  - Pacific Cybersecurity
  - Cybersecurity status of Pacific countries
  - Cybersecurity development in the Pacific region
  - Key sources that were used for identifying stakeholders included: International Telecommunications Union, Global Security Index, Global Cyber Alliance, Cybil Portal Computer Emergency Response Team Frameworks, etc.

Figure A1.2: List of Keywords and Phrases Used in the Research Process



Source: Authors.

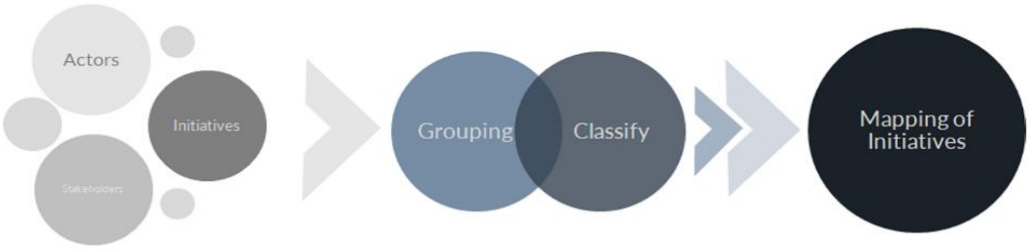
Data analysis

To map the cybersecurity developments in the Pacific region, the study referenced the works conducted by major stakeholders that have been implemented or have planned some form of initiative with Pacific member countries, either directly or indirectly through partners or donor agencies.

The mapping process phases involved the identification of actors and all relevant organizations and stakeholders across the region who are working in the cybersecurity space, identifying relevant government ministries and departments that deal with national cybersecurity development matters

across the 14 Pacific countries, establishing contacts, grouping, or classifying the key focus areas into five unique categories before the final mapping activities were initiated.

Figure A1.3: Mapping Process Phases



Source: Authors.

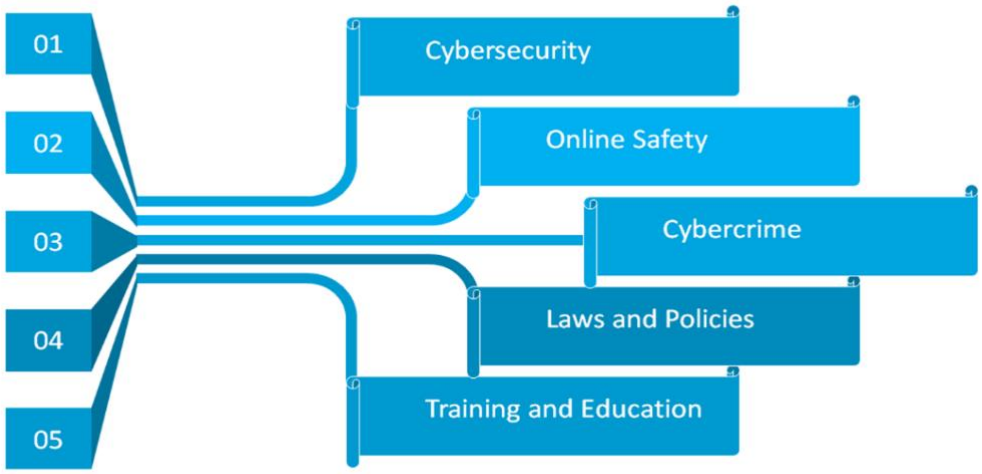
Overall goal

Conduct a mapping exercise, ensuring that all development activities related to cybersecurity in the Pacific are captured precisely, and in later phases, periodically update information on initiatives being fostered, funded, and implemented by development partners, agencies, and PIC governments.

Main areas of focus

The five main areas of focus as listed below, all with an emphasis of getting a broader range of information and as much detailed as possible, of all relevant stakeholders and the development initiatives undertaken in the Pacific.

Figure A1.4: Key Areas of Focus for the Mapping Exercise



Source: Authors.

Methodology

1. Component: Approved implementation plan
   1.1. Terms of reference developed and finalized
   1.2. Scope of work and work assignments defined
   1.3. Contract is signed

2. Component: Stakeholder engagement
   2.1. Building on stakeholder involvement, communications, and feedback processes, learning and integration

3. Component: Define the scope of the cybersecurity mapping
   3.1. Scope of development areas, countries and stakeholders involved

4. Component: Finalization of inception report detailing the implementation plan for consultancy
   4.1. Analyze the current cybersecurity landscape, determine objectives
   4.2. Status of cybersecurity projects in the Pacific
   4.3. Identify the priority areas

5. Component: Identify the cybersecurity relevance of the policy problem and research objectives
   5.1. Strategizing for effective research data, data collection methods

6. Component: Prepare and implement the mapping exercise
   6.1. Coordinating data requests and collection

7. Component: Project completion
   7.1. Closing
   7.2. Final reports

Figure A1.5: Steps and Stages of the Overall Project

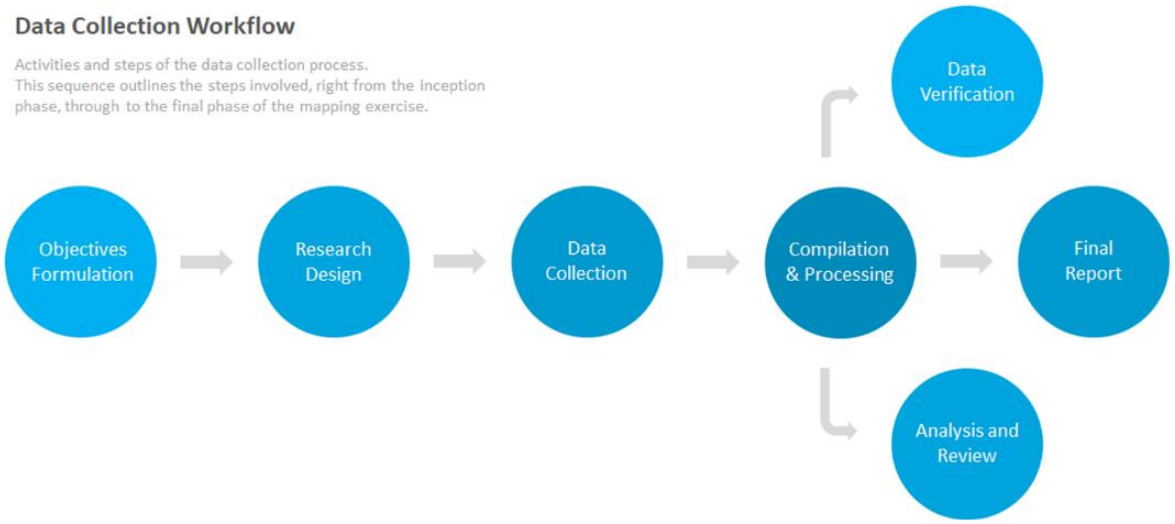
Source: Authors.

Research data collection

The data collection process plays a very critical role in this mapping exercise in order to accurately capture cybersecurity developments in the Pacific region. The aim of our researched and collected data is to have a widened scope, to target the broader stakeholder groups across the region and beyond, and to gather as much data and information from respondents as possible. Similarly, we will try to capture data from other secondary sources such as reports and assessments conducted in the past by other entities that may need to be supplemented with refreshed and updated data.

The workflow diagram below illustrates the various activities that constitute the data collection process. A major element of this process also involves the data verification and validation process, ensuring that the collected and compiled data would be subjected to stringent checks to establish an accurate representation of the development initiatives in the Pacific.

Figure A1.6: Workflow Diagram Showing the Core Activities of the Data Mapping Process



Source: Authors.

Appendix B: Questionnaire for Pacific Island Countries

Information Sharing on Cybersecurity Initiatives - Technical Assistance Study

The purpose of this questionnaire is to gather information from Pacific Island Governments on Cybersecurity in the region.

Our aim is to improve the targeting and effectiveness of cybersecurity initiatives in the PICs by mapping, sharing and periodically updating information on initiatives being fostered, funded, and implemented by development partners, agencies and PIC governments.

The feedback and responses that we gather will allow us to identify key development initiatives, implementers and focus areas, and the challenges faced. This will eventually give us more insight into the specifics related to Cybersecurity development, allowing us to create synergies and better engage with various stakeholders.

It might take around 8-10 minutes to complete this questionnaire.

Stakeholder Details

Your Name

Organization Name

Email Address

Details of Cybersecurity Initiatives in the Pacific

- Which Cybersecurity related initiatives are you currently working on or have already been implemented in your country?
- Which category do these initiatives belong to?
- What is the estimated duration of these initiatives?

- Who are the donors or funding agencies for these initiatives?
- What is the status of these current initiatives?

For the questions above, please fill in the details as per table below:

Initiative	Category	Funding Agency	Duration	Status
e.g., Project 1	e.g., Cybersecurity, Online Safety, Cybercrime, Law and Policy, or Training and Education	e.g., ADB	e.g., 1 year	e.g., Planned, In progress, Completed, On hold or Overdue
e.g., Project 2				
***fill in as many initiatives as seen relevant				

Optional Questions

What do you think are the major Cybersecurity challenges faced in your country? *(Optional)*

Please provide any other details relevant to Cybersecurity developments in your country *(Optional)*

Appendix C: Questionnaire for other stakeholders

Information Sharing on Cybersecurity Initiatives - Technical Assistance Study

The purpose of this questionnaire is to gather information from development partners and other stakeholders on Cybersecurity initiatives in the Pacific region.

Our aim is to improve the targeting and effectiveness of cybersecurity initiatives in the PICs by mapping, sharing and periodically updating information on initiatives being fostered, funded and implemented by development partners, agencies and PIC governments.

The feedback and responses that we gather will allow us to identify key development initiatives, implementers and focus areas, and the challenges faced. This will eventually give us more insight into the specifics related to Cybersecurity development, allowing us to create synergies and better engage with various stakeholders.

It might take around 8-10 minutes to complete this questionnaire.

Stakeholder Details		
Your Name		**Organization Name**
Email Address		
Stakeholder Category		

☐ **Intergovernmental** ☐ **Private Sector** ☐ **Technical Community**

☐ **Civil Society** ☐ **Donor Agency** ☐ **Academia**

☐ **Others (please specify)**

Details of Cybersecurity Initiatives in the Pacific

- Which Cybersecurity initiatives are you currently working on or have already implemented in the Pacific?
- Which category do these initiatives belong to?
- In which Pacific country(ies) are these initiatives being implemented?
- What is the estimated duration of these initiatives?
- Who are the donors or funding agencies for these initiatives?
- What is the status of these current initiatives?

For the questions above, please fill in the details as per table below:

Initiative	Category	Country Implemented	Funding Agency	Duration	Status
e.g., National cybersecurity strategy assistance	e.g., Cybersecurity, Online Safety, Cybercrime, Law and Policy, or Training and Education	e.g., Kiribati	e.g., ADB	e.g., 1 year	e.g., Planned, In progress, Completed, On hold or Overdue
e.g., Cybersecurity capacity building					
***fill in as many initiatives as seen relevant					

Optional Questions

Which key Cybersecurity priority areas do you think should be the target of development for the Pacific? *(Optional)*

What are some of the challenges that your organization has faced in relation to Cybersecurity development projects in the Pacific? Why? *(Optional)*

Please provide any other details relevant to Cybersecurity developments by your organization *(Optional)*

Appendix D: Contact list for country representatives

Organization Name	Ministry of Contact	Contact Person	Designation
1. Cook Islands	Office of the Prime Minister	Ms. Pua Hunter	Director of ICT
2. Federated States of Micronesia	Department of Transportation, Communications and Infrastructure,	Mr. Edward Albert	IT Manager
3. Fiji	Ministry of Communications	Mr. Varun Chaudhary Mr. Vivek Anand	Engineer Senior Engineer
4. Kiribati	Ministry of Information, Communications and Transport	Mr. Wayne Reiher - Mr. Domingo Kabunare	Director of ICT
5. Nauru	Department of ICT	Mr. Geoffrey Harris - Ms. Nadia Ika - Mr. Daicos Jeremiah	Secretary of ICT Director of ICT Admin
6. Niue	Ministry of Infrastructure	Mr. Clinton Chapman	ICT regulatory oversight, Utilities
7. Palau	Ministry of Public Infrastructure, Industries and Commerce	Mr. Takkon Chin	Chief, Division of Communication
8. Papua New Guinea	Department of Information and Communications Technology	Mr. Flierl Shongol Mr. Russell Matia Woruba Ms Georgina Kiele	Deputy Secretary for Policy Director of Informatio Acting Executive Manager for Cybersecurity and Digital Standards
9. Republic of the Marshall Islands	Ministry of Transportation and Communications	Mr Phil Phillipo - Mr. Rommel Natividad -	Secretary Director of Communications
10. Samoa	Ministry of Communications and Information Technology	Mr. Suetena Loia - Mr. Fualau Talatalaga Matau Matafeo -	ACEO ICT Division Chief Executive Officer
11. Solomon Islands	Ministry of Communication and Aviation	Mr. Alwyn Danitofea	Director Communication

Organization Name	Ministry of Contact	Contact Person	Designation
12. Tonga	Ministry of Communication	Mr. Andrew Toimoana	Director of Information
13. Tuvalu	Department of ICT	Mr. Opetaia Opet Simati -	Director at Department of ICT
14. Vanuatu	Officer of the Government Chief Information Officer (OGCIO)	Mr. Gerard Metsan - Mr. John Jack Mr Jackson Miake –	Chief Information Officer Director Vanuatu IGF

Appendix E: Catalogue of initiatives reported by Pacific Island Countries

Initiative	Category	Funding Agency	Duration	Status
1 Cook Islands				
i. Cyber Awareness	Cybersecurity, Online Safety	PaCSON, Get Safe Online (GSO), Cyber Safety Pacifika, Cook Islands Government	Ongoing	Ongoing
ii. Cyber Security Capacity Maturity Model for Nations (CMM)	Cybersecurity	Oceania Cyber Security Centre, Cook Islands Government	4 months (June – September 2022)	In progress
2 Federated States of Micronesia (FSM)**				
i. Establishment of FSM Cyber Security and Intelligence Bureau (CSIB) - Special Division within the Department of Justice	Cybersecurity	Governments of the United States of America and Australia		Completed
ii. Cybersecurity Capacity Maturity Model Workshop	Cybersecurity, Cybercrime, Law and Policy	World Bank, the Asia-Pacific Telecommunity (APT), and the Oceania Cyber Security Centre (OCSC)		Completed
iii. Member of the International Criminal Police Organization (INTERPOL) - provides investigative support, expertise, and training to law enforcement worldwide, with focuses on terrorism, cybercrime, and organized crime	Cybercrime			Completed
3 Fiji**				
i. Readiness Assessment Report to Establish a National CIRT	Cybersecurity	Inernational Telecommunications Union/IMPACT		Completed

Initiative	Category	Funding Agency	Duration	Status
ii. Cybersecurity Capacity Review	Cybersecurity	Commonwealth Telecommunications Organisation (CTO), the Global Cyber Security Capacity Centre		Completed
iii. Cybersecurity Assessment & Strategy Consultation	Cybersecurity, Law and Policy	Commonwealth Telecommunications Organisation (CTO), the Global Cyber Security Capacity Centre		Completed
iv. National Cybersecurity Strategy	Cybersecurity, Law and Policy	Fiji Government	1 year	Completed
v. Establishment of Online Safety Commission, through the introduction of the Online Safety Act 2018	Online Safety, Law and Policy	Fiji Government		Completed
vi. Cybercrime Act 2021	Cybercrime, Law and Policy	Fiji Government		Completed
vii. Get Safe Online	Cybersecurity, Online Safety, Training and Education	GSO	Ongoing	Ongoing
viii. Update of Digital Forensics Lab – Cybercrime Unit, Fiji Police	Cybercrime	Australian Federal Police (AFP)		Ongoing
ix. Formulation of Critical Infrastructure Incident Response Framework	Cybersecurity, Cybercrime	Australian Government, Fiji Government		Ongoing
x. Capacity building - Cyber Safety Pasifika	Cybersecurity, Online Safety, Training and Education	Australian Federal Police (AFP)		Ongoing
xi. Critical Infrastructure – National Cyber Incident Response and Recovery Framework	Cybersecurity, Law and Policy	Fiji Government		In progress
4 Kiribati				
i. Computer Emergency Response Team Kiribati	Cybersecurity	World Bank	4 years	In progress
ii. Cybercrime Law implementation	Law and Policy	Council of Europe	Ongoing	Planned
iii. Cybersecurity Training & Education	Online Safety, Training and Education	Get Safe Online	3 years	In progress

Initiative	Category	Funding Agency	Duration	Status
iv. Cybersafety training and education	Online Safety, Training and Education	Facebook & Save The Children Foundation	3 years	In progress
v. Cybersecurity Training	Training and Education	PaCSON (DFAT)	Ongoing	In progress
vi. Cybersecurity Training	Training and Education	People's Republic of China	Ongoing	Planned
5 Nauru				
i. CSAT – Cyber Security Awareness Team - focus on security of government infrastructure	Cybersecurity	Government of Nauru (GON)	Ongoing	Ongoing
ii. PaCSON Member	Cybersecurity		Ongoing	Ongoing
iii. Security Awareness Training	Training and Education	Welchman Keen		Completed
iv. Establishing a national CIRT	Cybersecurity			Planned
6 Niue**				
i. PaCSON Member - through Telecom Niue Ltd	Cybersecurity		Ongoing	Ongoing
ii. Niue Center for Excellence in Information Technology (CEIT)	Training and Education	Government of India		Ongoing
iii. Niue ICT Committee – ICT technical advisory and Cybersecurity	Cybersecurity	Government of Niue		Ongoing
7 Palau**				
i. PaCSON Member - through Bureau of Public Safety	Cybersecurity		Ongoing	Ongoing
ii. Agreement Establishing the Micronesian Regional Transnational Crime Unit - cybercrime detection and	Cybercrime			Ongoing

Initiative	Category	Funding Agency	Duration	Status
prevention, and sharing information concerning national and regional criminal activity trends.				
8 Papua New Guinea**				
i. National CERT – restructured through the new Bill and expanded Cybersecurity and Digital Projects workforce.	Cybersecurity			In progress
ii. Cybersecurity Bill	Cybersecurity, Law and Policy,	Department of Information and Communications Technology (DICT)		Completed
iii. National Cyber Security Centre	Cybersecurity, Law and Policy, Training and Education	Australian and PNG governments		Completed
iv. National Cybersecurity policies, Digital Transformation activities, Data Protection plans, etc.	Cybersecurity, Law and Policy	Department of Information and Communications Technology (DICT)		Ongoing
v. Get Safe Online	Cybersecurity, Online Safety, Training and Education	GSO		Ongoing
vi. Cybersecurity Capacity Building	Cybersecurity, Online Safety, Law and Policy, Training and Education	Welchman Keen		Ongoing
9 Republic of the Marshall Islands (RMI)				
i. RMI Central Email System - Cybersecurity Taskforce	Cybersecurity	State Department Funding	5 years	In progress
ii. Reviewing Computer Crimes Bill	Cybersecurity, Cybercrime Law and Policy	State Department Funding	1 year	Planned
iii. Strategy Workshop - Cybersecurity Strategy Plan	Cybersecurity, Law and Policy	State Department Funding	1 year	In progress
iv. Government Workers Training	Cybersecurity	State Department Funding	1 year	Planned
10 Samoa				
i. Cybersecurity Strategy	Law and Policy	ITU	3 years	Completed

Initiative	Category	Funding Agency	Duration	Status
ii. Cybersecurity Policy	Law and Policy	NIL	NIL	Planned
iii. Cybersecurity Trainings (Technical Trainings for all Technicians in Govt and some private institutions)	Training and Education	DFAT	2 years	Ongoing
iv. Cybersecurity Materials	Cybersecurity, Online Safety	NZ CERT	Ongoing	Ongoing
v. SamCERT website	Cybersecurity	DFAT	12 months	Planned
vi. SamCERT Operation	Cybersecurity	DFAT	3 years	Ongoing
11 Solomon Islands				
i. Cybersecurity Policy	Cybersecurity, Law and Policy	ITU	Since 2019 till current	To be completed this year 2022- In Progress
ii. Cybersecurity training	Training and Education	ITU	Ongoing	Ongoing
iii. Cybersecurity Training for CERT staff	Training and Education	DFAT- Australian Government	Since 2021	Ongoing
iv. Cybersecurity training	Training and Education	Asia Pacific Telecommunity (APT)	Ongoing	Ongoing
v. Cybercrime bill	Cybercrime, Law and Policy	Australian Attorney General's Department	1 year	Completed
12 Tonga				
i. Revised Cybercrime Bill	Cybercrime, Law and Policy	World Bank	1 year	In progress
ii. Revised of Cybersecurity curriculum for schools	Cybersecurity, Training and Education	World Bank	1 Year	In Progress
iii. National Cybersecurity Framework	Cybersecurity, Law and Policy	World Bank	1 Year	In Progress
iv. Cybersecurity Manual	Cybersecurity, Law and Policy	World Bank	1 year	In progress
v. Cybersecurity Training	Training and Education	World Bank	1 Year	In Progress

Initiative	Category	Funding Agency	Duration	Status
vi. CERT Cybersecurity Training	Training and Education	DFAT Australia	2 years	In progress
vii. Cybersecurity Awareness Training	Training and Education	ITU	1 year	In Progress
13 Tuvalu				
i. CMM Review	Cybersecurity, Online Safety, Cybercrime, Law and Policy, Training and Education	OCSC	1 year	Near completion, awaiting on Tuvalu feedback for final report- In Progress
ii. PaCSON	Cybersecurity, Online Safety, Cybercrime, Law and Policy, Training and Education	PaCSON	Ongoing	Following PaCSON and affiliate CERTs for advisories on malware outbreaks and perceived vulnerabilities
iii. Regulatory Activities	Law and Policy	Tuvalu Government	Ongoing	Needing technical assistance for regulatory strengthening
iv. Get Safe Online (GSO)	Cybersecurity, Online Safety, Cybercrime, Law and Policy, Training and Education	Get Safe Online	Ongoing	Following the global GSO initiatives
v. Digital Readiness Assessment	Cybersecurity, Online Safety, Cybercrime, Law and Policy, Training and Education	UNDP	Upcoming	Initial workshop and survey to be held on July 6th
14 Vanuatu				
i. Online Human Rights Advocacy Program	Online Safety	SPC	12 months	Completed

Initiative	Category	Funding Agency	Duration	Status
ii. Child Online Protection	Cybercrime	UNICEF	12 Months	In progress – completed by December 2022
iii. TV/Radio Campaigns	Online Safety	Vanuatu IGF	June – July 2022	Ongoing
iv. Community Outreach	Online Safety, Training and Education	Vanuatu IGF/OGCIO/CERT Vanuatu/TRBR/Vanuatu Bureau of Standards/Vanuatu Police Force	Ongoing	Ongoing
v. Online Portal	Cybercrime	Vanuatu IGF/UNICEF	12 Months	In Progress - December 2022
vi. Introduce new legislations to support the Cybercrime Act of 2021 – Against harmful online content	Online Safety	OGCIO/CERT Vanuatu	Ongoing	Ongoing
vii. ISO 27000 Certification Standards	Cybersecurity, Law and Policy	OGCIO/CERT Vanuatu	Ongoing	Ongoing

Appendix F: Catalogue of initiatives reported by other stakeholders

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
1 Asia Pacific Network Information Centre (APNIC)					
i. Security community engagement - CSIRT Support, Technical Awareness, LEA Engagement, Network Operators community	Cybersecurity, Law and Policy, Training and Education	PNG, Vanuatu, Tonga, Samoa, Solomon Islands, Fiji	APNIC, APNIC Foundation	On-going	Ongoing
ii. National CERT establishment - Regional activities to promote collaboration among organizations with CERT responsibilities	Cybersecurity	Fiji, PNG, Tonga, Solomon Islands, Vanuatu, Kiribati, Marshall Islands, Nauru, Samoa	DFAT & APNIC	2 years	Completed
iii. Technical capacity building - Network infrastructure, Capacity building for network/IT engineers	Training and Education	Not specific countries but regionally focused – i.e., via academy.apnic.net, Fellowship program, Mentoring	APNIC, APNIC Foundation	On going	Ongoing
2 Asia-Pacific Telecommunity (APT)					
i. Assessment of Cybersecurity Readiness	All dimensions of cybersecurity, such as, institutional arrangement, Online Safety, Cybercrime, Law and Policy, or Training and Education	Federated States of Micronesia (FSM)	In collaboration with Oceania Cyber Security Centre (OCSC)	1 year	Completed
ii. National cybersecurity roadmap assistance	All dimensions of cybersecurity, such as, institutional arrangement,	Federated States of Micronesia (FSM)	In collaboration with Oceania Cyber Security Centre (OCSC)	1 year	Completed

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
	Online Safety, Cybercrime, Law and Policy, or Training and Education				
iii. National Cybersecurity Personnel Development Plan Assistance	Law and Policy, Training and Education	All APT members	In collaboration with PGI International	1 year	Completed
iv. A number of training courses on cybersecurity	Law and Policy, Training and Education	All APT members	In collaboration with Partner Training Institutions (in People's Republic of China, India, Thailand, Japan, and Rep. of Korea)	Through the year	Ongoing
v. A Research project on unsolicited commercial messages	Law and Policy, Training and Education	All APT members	KISA / Korea	2 years	Ongoing
3 Australia Pacific Training Coalition (APTC)					
i. Short Courses Micro-Credentials - Cyber Security Essentials and Digital Literacy Essentials	Training and Education	Fiji, Nauru, Kiribati, Papua New Guinea, Samoa, Solomon Islands, Timor-Leste, Tonga, Tuvalu, and Vanuatu	Australian Government		Ongoing
4 Australian Cyber Security Centre (ACSC)/ Pacific Cyber Security Operational Network (PaCSON)					
i. Cybersecurity capacity building	Cybersecurity, Online Safety, Training and Education	Australia, Cook Islands, Fiji, Kiribati, Marshall Islands, Nauru, New Zealand, Niue, Palau, Papua New Guinea, Samoa, The Solomon Islands, Tokelau, Tonga, Tuvalu, Vanuatu	Australian Department of Foreign Affairs and Trade (DFAT) Cyber and Critical Tech Cooperation Program (CCTCP)	Ongoing	Ongoing
5 CERT NZ					
i. Annual Cyber Smart Pacific campaign	Cybersecurity, Training and education)	PaCSON member countries	MFAT	Ongoing	In progress

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
ii. Monthly Remote Session Series	Cybersecurity, Training and education)	PaCSON member countries	MFAT	Ongoing	In progress
iii. In-country visits with training	Cybersecurity, Training and education)	PaCSON member countries	MFAT	Ongoing	In progress
6 Commonwealth Telecommunications Organisation (CTO)					
i. Commonwealth Approach for Developing National Cybersecurity Strategies - Commonwealth Cybergovernance Model - National Cybersecurity Strategies	Cybersecurity	Fiji			Completed
7 Council of Europe					
i. Budapest Convention on Cybercrime – facilitate works and activities to assist Pacific countries to accede to the convention	Cybercrime, Law and Policy	All Pacific	Council of Europe (CoE) member states		Ongoing
ii. Global Action on Cybercrime Extended (GLACY)+ Initiatives focus on policies, legislation and prosecution	Cybercrime, Law and Policy	All Pacific	Council of Europe (CoE) member states	5 year (2017–2021)	Completed
iii. GLACY+: Legislative support on cybercrime in Nauru Workshop under the framework of the GLACY+ project-consolidating the support on cybercrime and electronic legislation and assessment	Cybercrime, Law and Policy	Nauru	Council of Europe (CoE) member states		Completed

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
iv. GLACY+: Cooperation on cybercrime in the Pacific: Vanuatu focusing on the international sharing of electronic evidence	Cybercrime, Law and Policy	Vanuatu	Council of Europe (CoE) member states		Completed
v. GLACY+: Combatting Online Child Abuse in the Pacific: Regional workshop	Cybercrime, Law and Policy	15 Pacific countries	Council of Europe (CoE) member states		Completed
vi. GLACY+: Support for Drafting Data Protection Legislation in Vanuatu – Introductory workshop	Cybercrime, Law and Policy	Vanuatu	Council of Europe (CoE) member states		Completed
vii. GLACY+: Webinar on Countering Disinformation in the Pacific region	Cybercrime, Law and Policy	10 Pacific countries	Council of Europe (CoE) member states		Completed
viii. GLACY+: Webinar – The effects of COVID-19 on cybercrime in the Pacific	Cybercrime, Law and Policy	All Pacific	Council of Europe (CoE) member states		Completed
8 Council of Regional Organisations of the Pacific (CROP) ICT Working Group					
i. Pacific Cybersecurity Center of Excellence (CoE)	Cybersecurity, Online Safety, Law and Policy, Training and Education	Laucala Campus Fiji, All Pacific	USP		Planned
ii. Capacity Building for the Pacific	Training and Education	All Pacific	Various partners	Ongoing	Ongoing
iii. CROP ICT Cyber Security Task Force	Cybersecurity, Online Safety, Cybercrime, Law and Policy, Training and Education	All Pacific	CROP agencies and various partners		Ongoing
iv. Framework for Action on ICT for Development in the Pacific (FAIDP)	Cybersecurity, Online Safety, Cybercrime, Law and Policy, Training and Education	All Pacific	CROP agencies and various partners		Ongoing

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
v. Pacific Regional ICT Strategic Action Plan (PRISAP)	Cybersecurity, Online Safety, Cybercrime, Law and Policy, Training and Education	All Pacific	CROP agencies and various partners		Ongoing
9 Cyber Safety Pasifika (CSP)					
i. Pacific Police Development Program – Cyber Safety Pasifika (CSP) Program Three pillars of focus: Cyber Safety Awareness and Education, Development of Cybercrime Legislation and Policy and Up-skilling of Pacific Police in Cybercrime Investigations	Cybersecurity, Online Safety, Cybercrime, Law and Policy, Training and Education	All Pacific	DFAT Australia		Ongoing
10 Department of Foreign Affairs and Trade (DFAT) Australia					
i. Girls Online (GO!): Participating Meaningfully and Safely in Cyberspace	Online safety; Training and Education	Tonga, Vanuatu	DFAT	2.5 years	Ongoing
ii. Cybercrime Legislation and Implementation	Cybercrime, Law and policy	Pacific (regional)	DFAT	4.5 years	Ongoing
iii. National Bank of Vanuatu cybersecurity uplift	Cybersecurity	Vanuatu	DFAT	2 years	Ongoing
iv. Understanding Technology-Facilitated Domestic Violence in the Pacific and Building Support Services for Victim-Survivors	Online safety	Fiji, Tonga, Vanuatu	DFAT	3 years	Planned

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
v. Executive Cybersecurity Seminar Series	Training and education	Papua New Guinea, Fiji	DFAT	1 year	Planned
vi. Expanding the eSafety Women model in the Pacific	Online Safety, Training and Education	Australia, Fiji, Kiribati, Nauru, New Zealand, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu	DFAT	2 years	Ongoing
vii. Building Online Safety Capabilities in the Indo-Pacific Region	Online Safety, Training and Education	Fiji	DFAT	3 years	Ongoing
viii. Pacific Law Officer's Network (PILON) Cybercrime Workshop	Cybercrime, Law and policy	Pacific (regional)	DFAT	5 years	Ongoing
ix. National Cyber Strategy Development & Implementation Planning	Cybersecurity, Law and policy	Timor-Leste	DFAT	1.5 years	Planned
x. Cyber Security Training Services	Training and education	Timor-Leste	DFAT	1 year	Planned
xi. Pacific Cyber Security Operational Network (PaCSON)	Cybersecurity, Online Safety, Training and Education	Pacific (regional)	DFAT	6 years	Ongoing
xii. Pacific Cyber Security Operational Network Cyber Upskill Program (PaCSON CUP)	Cybersecurity, Online Safety, Training and Education	Pacific (regional)	DFAT	2 years	Planned
xiii. Enhancing cyber capacity building and regional coordination of efforts in the Pacific (GC3B)	Training and Education, Law and policy	Pacific (regional)	DFAT	1 year	Planned
xiv. UN Cyber Diplomacy in the Pacific	Cybersecurity, Law and Policy	Pacific (regional)	DFAT	2 years	Ongoing

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
xv. Strengthening Online Safety for Young People in the Pacific	Online safety, Training and Education	Solomon Islands	DFAT	3 years	Ongoing
xvi. Cyber Security Advisory and Mitigation Services for the Meteorology Division	Cybersecurity	Samoa	DFAT	1 year	Planned
xvii. Cyber Security Defensive Readiness Program	Cybersecurity	TBC – two Pacific countries	DFAT	2 years	Planned
xviii. Fostering National Practice Exchange in Ransomware in Southeast Asia and the Pacific	Cybercrime, Cybersecurity	Pacific (regional)	DFAT	6 months	Ongoing
xix. UNSW Cyber Bootcamp Project	Training and Education	Solomon Islands	DFAT	3 months	Completed
xx. Cybercrime Investigative Training (Cyber Safety Pasifika (CFP))	Cybersecurity, Online Safety, Cybercrime, Training and Education	Pacific (regional)	DFAT	4.5 years	Ongoing
xxi. Pacific threat environment and capability analysis	Cybersecurity	Pacific (regional)	DFAT	6 months	Planned
xxii. Cyber Security Maturity Model for Nations review (CMM) plus roadmap assessment	Cybersecurity	Nauru	DFAT	1.5 years	Planned
xxiii. Support to PNG Social Media Management Desk	Cybersecurity	Papua New Guinea	DFAT	2 years	Planned
xxiv. Cyber Security Services in the Pacific	Cybersecurity	Fiji, Tonga, Samoa, Vanuatu and Solomon Islands	DFAT	3 years	Ongoing

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
xxv. Fiji Cyber Security Strategy Development	Cybersecurity, Law and Policy	Fiji	DFAT	8 months	In progress
xxvi. Pacific Telecommunications Security Expert Forum	Training and Education	Pacific (regional)	DFAT	10 months	Planned
xxvii. Continuing support to PNG National Cyber Security Centre - Technical training	Training and Education	Papua New Guinea	DFAT	3 years	Planned
xxviii. Continuing support to PNG National Cyber Security Centre - operational extension	Cybersecurity	Papua New Guinea	DFAT	1 year	Planned
xxix. Pacific Cybercrime Workshop in Tonga	Cybercrime, Training and Education	Tonga	DFAT	2 months	Completed
xxx. Support to develop National CERT (Tonga CERT)	Cybersecurity	Tonga	DFAT	4 years	Completed
xxxi. Assist Tonga implement legislation relevant to the Budapest Convention on Cybercrime	Cybercrime, Law and Policy	Tonga	DFAT	2 years	Completed
xxxii. Support PICISOC to establish a Pacific Internet Government Forum	Online Safety	Vanuatu	DFAT	1 month	Completed
xxxiii. Review and Reform of Cyber Security and Cybercrime Legislation	Cybercrime, Law and Policy	Samoa	DFAT	3 years	Completed
xxxiv. Enhanced Capacity of a Security Operations Centre in	Cybersecurity	Solomon Islands	DFAT	3 years	Completed

	Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
	the Solomon Islands Government Information, Communication and Technology Support Unit					
xxxv.	Supporting cyber security capacity in Papua New Guinea	Cybersecurity	Papua New Guinea	DFAT	2 months	Completed
xxxvi.	Supporting Efficient Internet Connectivity in Pacific (PacTraining)	Cybersecurity, Training and Education	Fiji, Samoa, Solomon Islands, Tonga, Vanuatu	DFAT	2 years	Completed
xxxvii.	Cyber Breach Workshop for the Pacific	Cybersecurity	All Pacific	DFAT	1.5 years	Completed
xxxviii.	Supporting a technology for development challenge to connect youth with job opportunities in Solomon Islands	Training and Education	Solomon Islands	DFAT	2 years	Completed
xxxix.	Cybersecurity analyst training program - project sensor pilot (Fiji)	Cybersecurity, Training and Education	Fiji	DFAT	1 year	Completed
xl.	Strengthening Cyber Security Capacity in Fiji	Cybersecurity, Law and Policy, Training and Education	Fiji	DFAT	1 year	Completed
xli.	Building CERT Capacity in the Pacific	Cybersecurity, Training and Education	All Pacific	DFAT	2 years	Completed
xlii.	Cybercrime training workshops for the Pacific	Cybercrime, Training and Education	All Pacific	DFAT	1.5 years	Completed

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
xliii. Interim Support for Papua New Guinea CERT	Cybersecurity	All Pacific	DFAT	1 year	Completed
xliv. Cyber Security Regional Standardisation Enhancement Program (Asia Pacific)	Law and Policy	Papua New Guinea, Fiji, Vanuatu	DFAT	1 year	Completed
xlv. e-Governance workshops and training in the Indo-Pacific	Training and Education	PNG; Solomon Islands; Vanuatu; Fiji, Samoa; Tonga; Kiribati	DFAT	1.5 years	Completed
xlvi. Women in Cyber Fellowships	Training and Education, Law and Policy	All Pacific	DFAT	2 years	Ongoing
xlvii. Cyber security training and capability uplift	Cybersecurity, Training and Education	Solomon Islands, Vanuatu	DFAT	6 months	Completed
xlviii. Developing a National CERT in Vanuatu	Cybersecurity	Vanuatu	DFAT	3 years	Completed
xlix. Blockchain and Digital Innovation in Papua New Guinea	Training and Education	Papua New Guinea	DFAT	1 year	Completed
l. Web Application Secure Development Training in Vanuatu	Online safety, Training and Education	Vanuatu	DFAT	1 month	Completed
11 e-Governance Academy (eGA)					
i. National Cyber Security Index (NCSI), database, evidence materials	Cybersecurity, Law and Policy, Training and Education	All Pacific	Estonia Development Cooperation, e-Governance Academy Foundation	Ongoing	Completed
ii. Cyber Security Consultancy Services for Developing and Supporting Information Systems in Tonga	Cybersecurity	Tonga	World Bank		Completed

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
12 Get Safe Online (GSO)					
i. Media campaigns This has involved the following activity: - Developing monthly campaigns on key topics (as identified by the countries we operate in) using social media, videos, radio and TV advertising, public relations, and local influencers. - Keeping content relevant, up to date and topical on dedicated country websites & driving traffic to these websites.	Online Safety, Training and Education	Fiji, Kiribati, Nauru, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu, Vanuatu	UK Foreign, Commonwealth and Development Office	We have been working in the Pacific since July 2020. We have run two substantial projects to date, the first lasting around 9 months and the second around 6 months which finished at the end of March 2022. From April 2022 – August 2022 we have been provided with funding to run basic media campaigns only. We are hopeful that future funding will be secured to start our work again and run substantial media campaigns from Autumn 2022 onwards.	In progress
ii. The Get Safe Online Ambassador Scheme. - We train local citizens on basic cyber safety techniques and provide presentation training also if needed.	Cybersecurity, Training and Education	Fiji, Kiribati, Nauru, Papua New Guinea, Samoa, Solomon Islands. Tonga, Tuvalu, Vanuatu	UK Foreign, Commonwealth and Development Office	We have been working in the Pacific since July 2020. We have run two substantial projects to date, the first	In progress

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
- These ambassadors are then encouraged to go out into their communities to run (free) online safety awareness sessions. - We also provide ongoing mentoring and resources.				lasting around 9 months and the second around 6 months which finished at the end of March 2022. This involved identifying and training local citizens to become Ambassadors. From April 2022 – August 2022 we are concentrating on identifying opportunities for our trained Ambassadors to conduct sessions in their local communities rather than training new people.	
iii. Relationship building - This has involved identifying and building relationships with key cybersecurity personnel in governments and/or CERT's, other key NGOs and relevant organizations involved with cybersecurity development work in the Pacific.	Cybersecurity, Training and Education	Fiji, Kiribati, Nauru, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu, Vanuatu	UK Foreign, Commonwealth and Development Office	We have been working in the Pacific since July 2020. We have run two substantial projects to date, the first lasting around 9 months and the second around 6 months which finished at the end of March 2022.	In progress

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
				From April 2022 – August 2022 we are continuing to nurture our relationships helping colleagues with challenges they may have (where we can assist) and identifying opportunities for our ambassadors to run awareness sessions.	
13 Global Forum on Cyber Expertise (GFCE)					
i. Pacific Regional Meeting	Cybersecurity, Training and Education	All Pacific	GFCE		Planned
ii. GFCE Pacific Hub	Cybersecurity, Training and Education	All Pacific	Members or Partners		Planned
14 Global Partners Digital (GPD)					
i. Report on Human Rights in the Digital Age and Civic Engagement in the Pacific	Law and Policy	Fiji, Kiribati, Nauru, PNG, Samoa, Solomon Islands, Tonga, Tuvalu, Vanuatu	UK Foreign and Commonwealth Office	6 months	Completed (finalized March 2021)
ii. Inclusive Approach for Cyber Security Strategies [Involved facilitating a workshop in Fiji in November 2019 to discuss cybersecurity priorities in the region]	Cybersecurity, Law and Policy	Fiji, Kiribati, Nauru, PNG, Samoa, Solomon Islands, Tonga, Tuvalu, Vanuatu	UK Foreign and Commonwealth Office	1 year	Completed (Finalized March 2020)
15 International Centre for Democratic Partnerships (ICDP)					

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
i. Pacific Connect - webinar/dialogue relating to cybersecurity and literacy in the Pacific	Cybersecurity, Online Safety	Australia, Fiji, PNG, Samoa, Solomon Islands, Tonga, and Vanuatu	DFAT Australia		Planned
16 International Telecommunication Union (ITU)					
i. Country Assistance on Computer Incident Response Team (CIRT) Assessment and Capacity Building	Cybersecurity	Papua New Guinea, Samoa, Tonga, and Vanuatu, Kiribati	Australian Government Department of Infrastructure, Transport, Regional Development and Communication		Ongoing in Kiribati; Complete in other countries
ii. CIRT Capacity Building	Cybersecurity, Training and Education	Papua New Guinea, Vanuatu	Australian Government Department of Communications and the Arts		Completed
iii. Promotion of Child Online Protection Guidelines to Pacific regionally, including to Pacific Islands Telecommunications Association (PITA) Strategy Forum	Cybersecurity	Pacific Regional	ITU		Ongoing
iv. National Cybersecurity Strategy	Cybersecurity	Kiribati, Solomon Islands	ITU		Completed
v. 2020 ITU Pacific Cyberdrill	Cybersecurity, Training and Education	Pacific Regional	ITU	8–10 December 2020	Completed
17 Internet Corporation for Assigned Names and Numbers (ICANN)					
i. Cybersecurity capacity development - DNS security, DNSSSEC training	Cybersecurity, Training and Education	Fiji	Joint collaborations – ICANN/USP	2 weeks	Completed
ii. Support DNS root zone resiliency among ISPs in Pacific countries to host root server instances -	Cybersecurity	Australia, Federated States of Micronesia, Fiji, Palau, Guam, Marshall Island, New Caledonia, New Zealand,	Joint partnerships between ICANN and ISP hosts.	3-6 months	Completed

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
DNS resiliency, stability, and security		PNG, Samoa, Solomon Islands, Vanuatu			
18 Ministry of Foreign Affairs and Trade (MFAT)					
New Zealand Cyber Security Support to the Pacific Programme	Cybersecurity, Cybercrime, Law and Policy, Training and Education	All Pacific	NZ Government	5 years	Ongoing
CERT NZ / SamCERT Technical Equipment Cooperation	Cybersecurity, Training and Education	Samoa	New Zealand Government	June 2021 to 2024	Ongoing
CERT NZ Trial Translation Project of Good Practices Guides (11 Pacific Island languages for eight economies)	Cybersecurity, Training and Education	Cook Islands, Fiji, Kiribati, Niue, Samoa, Tonga, Tuvalu, Vanuatu	New Zealand Government	March 2021 to May 2022	Complete
CERT NZ Tonga workforce development programme	Cybersecurity, Training and Education	Tonga	New Zealand Government	2021-2024	Ongoing
CERT NZ support for Cyber Smart Pacific awareness raising campaign	Cybersecurity, Training and Education	All Pacific	New Zealand Government	2020-2025	Ongoing
Cyber Safety Pasifika New Zealand Police secondment	Cybersecurity, Cybercrime, Training and Education	All Pacific	New Zealand Government	March 2021 to 30 April 2023	Ongoing
Extension of New Zealand's Digital Child Exploitation Filtering System (DCEFS)	Cybersecurity, Cybercrime	Samoa, Tonga	New Zealand Government	March 2020 to March 2023	Ongoing
Legal Assistance to Develop Tokelau Cyber Rules	Cybercrime, Law and Policy	Tokelau	New Zealand Government	Nov-20	Ongoing
Niue Information Security Technology Project	Cybersecurity, Training and Education	Niue	New Zealand Government	November 2021 to December 2022	Ongoing

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
CERT NZ / SamCERT Technical Equipment Cooperation	Cybersecurity, Training and Education	Samoa	New Zealand Government	June 2021 to 2024	Ongoing
Women and International Security in Cyberspace Fellowship	Cybersecurity, Law and Policy	Fiji, Indonesia, Lao People's Democratic Republic (the), Malaysia, Papua New Guinea, Philippines (the), Samoa, Thailand, Vanuatu, Viet Nam	Australia – Department of Foreign Affairs and Trade (DFAT), Canada, United Kingdom –Foreign, Commonwealth & Development Office (FCDO), Netherlands (the) – Ministry of Foreign Affairs, New Zealand – Ministry of Foreign Affairs and Trade (MFAT)	Oct 2019 to Dec 2021	Completed
19 Oceania Cyber Security Centre (OCSC)					
i. National cybersecurity assessment (strategy and policy, cybersecurity culture, education training awareness, regulatory and legislative frameworks, tech controls)	Cybersecurity, Online Safety, Cybercrime, Law and Policy, Training and Education	Samoa, Tonga, Vanuatu, PNG, Cooks, Tuvalu, FSM, Kiribati together with others including Australia and NZ	Victoria Government (Aus), APT (for FSM) ITU (Samoa, Tonga Vanuatu, PNG)	Ongoing activity	Ongoing
ii. Roadmap (CCM informed NSC and capacity building)	Cybersecurity, Online Safety, Cybercrime, Law and Policy, Training and Education	FSM	APT, Victoria Government (Aus)	6 months	Completed
iii. OCSC Conference (Melbourne, 2020) Pacific focused. Panels on challenges facing the Pacific (OCSC); coordination of capacity building (GFCE); developing national cybersecurity strategy (ITU); cybercrime (AFP); CERT (APNIC).	Cybercrime, Law and Policy, Training and Education	Tonga, Kiribati, Cook Islands, Tuvalu, Fiji and PNG.	Victorian Government, GFCE, GPD	3 days	Completed

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
iv. Research into a framework for CERTs in the Pacific	Cybersecurity	Ideally all, but under development	Victorian Government and Monash University	3 to 6 years (PhD research)	In progress
20 Pacific Islands Chapter of the Internet Society (PICISOC)					
i. Promoting awareness and educating our people on responsible cyber behavior	Cybersecurity, Online Safety, Training and Education	Pacific Island Countries who attended the Girls in ICT Day 2022	ISOC Chapter Admin Fund	Annual event and can be part of careers day event in schools that have requested assistance, e-talanoa sessions	Ongoing
ii. Internet Governance awareness during the Pacific Internet Governance Forum 2021 (PacIGF21)	Cybersecurity, Online Safety, Cybercrime, Law and Policy	Vanuatu, Solomon Islands, Tonga, Samoa	APTLD, ISOC Chapter Admin, APNIC	3 days and can be a yearly event	Ongoing
iii. Facilitating national cybersecurity policies workshops and discussions	Cybersecurity, Online Safety, Cybercrime, Law and Policy	Solomon Is and other Pacific Island Countries	Participating on Voluntary basis and initiated by National Government responsible Ministry		Ongoing
iv. Online gender-based violence, Pacific Gender Scorecards (Gender and ICT Research)	Cybersecurity, Online Safety	Members from Samoa, PNG and Tonga are part of this program	Participation on voluntary basis but support by Alliance for Affordable Internet, ADB PSDI & World Wide Web Foundation	1 year	Ongoing
21 Pacific Islands Forum Secretariat (PIFS)					
i. Boe Declaration – Sub-Committee on Regional Security (SRS) – Initiatives on 6 Strategic Focus Areas (SFA) - Under the Boe Declaration, Pacific Leaders have prioritized Cybersecurity and Cyber-Enabled Crimes	Cybersecurity, Cybercrime, Law and Policy, Training and Education	All Pacific	Various	Ongoing	Ongoing

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
as key emerging security challenges for the region					
22 Pacific Islands Law Officers' Network (PILON)					
i. Cybercrime Working Group – facilitate webinars, trainings, and capacity building on countering cyberbullying, cybercrime, disinformation, etc	Cybercrime, Law and Policy, Training and Education	19 member countries and territories and PILON partners and observers	Various sources	Ongoing	Ongoing
23 Pacific Technical and Further Education (Pacific TAFE)					
i. Development of the Certificate IV in Cyber Security Qualification	Training and Education	All member countries of USP	Private and donor agencies such as Australian Federal Police	10 – 12 months	Three cohorts of this training are completed. Out of the three, one cohort was delivered at Emalus Campus. Currently on the fourth cohort.
ii. Advance Diploma of Cyber Security	Training and Education	All member countries of USP	Private	1.5 – 2 Years	Planned. Initial discussions have started.
24 Save the Children					
i. Online Safety Campaign – I Am Digital	Online Safety, Training and Education	Fiji, Papua New Guinea, Samoa and Tonga	Facebook		Ongoing
ii. Pacific Islands Digital Citizenship and Safety Advisory Group	Online Safety	Fiji, Papua New Guinea, Samoa, Tonga, Kiribati, Solomon Islands and Vanuatu	Facebook		Ongoing
25 Secretariat of the Pacific Community (SPC)					

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
i. Data Governance for CROP Agencies – Initiatives on Data Governance policy, storage, (re)use, license and security of data and data governance awareness workshops	Law and Policy, Training and Education	CROP Members	SPC		In progress
26 Standards Australia					
i. Pacific Islands Cyber Security Standards Cooperation Agenda - Cyber Security Regional Standardisation Enhancement Program - focused on building market awareness and use of the ISO/IEC 27000 series	Cybersecurity	Fiji, Papua New Guinea, Solomon Islands, Tonga, and Vanuatu	Australian Government		Completed
27 The Asia Foundation					
i. Pacific Cyber Dialogue	Cybersecurity, Online Safety	All Pacific	DFAT, MFAT, The Asia Foundation		Completed
ii. Countering Online Misinformation	Online Safety	All Pacific			Ongoing
28 United States Embassy – Department of State					
i. Pacific Islands Cyber Conference – under the United States' Digital Connectivity and Cyber Partnership (Digital Partnership)	Cybersecurity, Training and Education	All Pacific	U.S. Department of State		Completed
ii. Pacific Islands Cyber Capacity Building Engagement Strategic	Cybersecurity, Training and Education	All Pacific	US Department of State		Completed

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
Cyber Planning and Implementation					
29 University of South Pacific (USP)					
i. Postgraduate Diploma in Cybersecurity programme	Training and Education	14 Pacific countries	USP	2 year program	Ongoing
ii. Establishment of a Pacific Regional CERT - PacCERT	Cybersecurity	All Pacific	USP, JICA		Completed. (PacCERT no longer in operation)
30 USAID - Digital Connectivity and Cybersecurity Partnership (DCCP)					
i. Digital Connectivity and Cybersecurity Partnership (DCCP) – Pacific	Cybersecurity, Law and Policy, Training and Education	All Pacific	US Government	5 years	Planned
31 Welchman Keen					
i. Cybersecurity Capacity Building in the Pacific	Cybersecurity, Training and Education	All Pacific		2 years	Ongoing
32 World Wide Web Foundation / Alliance for Affordable Internet (A4AI)					
i. Get Safe Online Initiative	Online Safety, Training and Education	Pacific Countries and Territories	UK Commonwealth Programme	2 to 3 years	Ongoing
ii. Online Gender Based Violence	Online Safety	Pacific Countries and Territories	Web Foundation	3 to 4 years	Ongoing
iii. eSafety and Online Safety	Online Safety	Fiji and Pacific	e-safety Australia	Ongoing	Ongoing
iv. Digital Skills Programme and Child Online Protection – Cybersecurity	Cybersecurity, Online Safety	All Pacific	ITU, Web Foundation, A4AI	Ongoing	Ongoing
33 UNICEF					

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
i. Training of U-Ambassadors on how to stay safe online	Online Safety, Training and Education	Solomon Islands	UNICEF and Oxfam		Completed
ii. Cyber Safety Programme	Online Safety	Samoa	UNICEF		Completed
iii. Outreach activities in schools on cyber-bullying	Online Safety	Tonga	UNICEF		Completed
34 eSafety Commissioner (Australia)					
i. Building Online Safety Capabilities in the Pacific	Online Safety	Fiji	DFAT	3 years	In progress
ii. eSafety Women in the Pacific	Online Safety, Cybercrime	Regional	DFAT	2 years	In progress
35 Pacific Fusion Centre					
i. Capacity building and internship programme	Cybersecurity, Training and Education	All Pacific	Australian Government		Ongoing
ii. Boe Declaration on Regional Security - assessments and advice on Pacific regional security challenges – Cybersecurity and Cyber-enabled crimes	Cybersecurity, Cybercrime, Law and Policy, Training and Education	All Pacific	Australian Government		Ongoing
36 United Nations Office on Drugs and Crime (UNODC)					
i. Training on Cybercrime and Ransomware for the Pacific	Cybersecurity, Cybercrime, Training and Education	6 Pacific countries – Fiji, PNG, Solomon Islands, Samoa, Tonga, and Vanuatu	Australian Government	Less than 1 year	Ongoing
37 World Bank					
i. Pacific Regional ICT Regulatory Development Project - Cybersecurity support	Cybersecurity, Law and Policy, Training and Education	All Pacific	World Bank	5 years	Completed

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
ii. Cybersecurity Multi-Donor Trust Fund	Cybersecurity, Online Safety, Cybercrime, Law and Policy, Training and Education	All Pacific	Estonia, Gates Foundation, Germany, Israel, Japan, The Netherlands, U.S. Department of State		Ongoing
iii. Pacific Regional Connectivity Program	Cybersecurity, Law and Policy	Tonga	World Bank	7 years	Completed
iv. Pacific Regional Connectivity Program 2	Cybercrime, Law and Policy	Federated States of Micronesia	World Bank	8 years	Ongoing
v. Cyber Security Consultancy Services for Developing and Supporting Information Systems in Tonga – focused on the expansion of the Cybersecurity Program of the government of Kingdom of Tonga	Cybersecurity, Training and Education	Tonga	World Bank		Completed
38 Christ's University in Pacific					
i. Master of Cyber Security (MCS) program	Training and Education	Tonga	CUP		In progress
39 United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP)/ Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT)					
i. Pacific Information Security and Privacy Capacity Building Programme - Cybersecurity capacity building for policymakers and civil servants	Training and Education	Samoa, Sub-regional (Pacific Countries)	APCICT/UNESCAP	24-25 Feb. 2021 (Samoa)	Ongoing
ii. Capacity Building Webinar on Information	Training and Education	All Pacific	APCICT/UNESCAP	28 Sept. – 1 Oct. 2021 (Sub-regional)	Completed

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
Security and Privacy for Pacific Countries					
iii. Development of Training Modules - Academy of ICT Essentials for Government Leaders - Information Security and Privacy provided through APCICT Virtual Academy	Training and Education	All Pacific	APCICT/UNESCAP		Ongoing
40 Pacific Islands Telecommunications Association (PITA)					
i. Telecommunications & Cybersecurity regulations and Capacity Building in the Pacific Island - facilitate webinars, trainings, and capacity building for members	Cybersecurity, Law and Policy, Training and Education	PITA members	Various sources		Ongoing
ii. Pacific Network Operators Group (PacNOG) Meeting, Conference and Educational Workshop - capacity development program for the IP-ISP network operators from the Pacific Islands	Training and Education	PITA members, operators, industry	APNIC, ICANN, USP, University of Oregon, NSRC	Twice every year	Ongoing
41 Pacific Telecommunications Council (PTC)					
i. PTC Conference – that involves global telecoms security, data protection, and research	Cybersecurity	All PTC members	Various sources		Ongoing
ii. PTC Academy Courses	Training and Education	All PTC members	Various partners		Ongoing
42 European Union (EU)					

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
i. EU-Japan Connectivity Partnership – EU Strategy for Cooperation in the Indo Pacific	Cybersecurity, Law and Policy, Training and Education	Indo-Pacific Region	Japan, United States and the European Union (EU)		Ongoing
ii. GLACY (Global Action Cybercrime)	Cybercrime	Global	European Union (EU)	3 years	Completed
iii. GLACY+ (Global Action on Cybercrime Extended)	Cybercrime, Law and Policy	Global	European Union (EU), Council of Europe	2016–2024	Ongoing
43 Japan International Cooperation Agency (JICA)					
i. PacCERT - Technical assistance, equipment and staff capacity building	Cybersecurity	All Pacific	JICA, USP		Completed
ii. JP-US ICS Cybersecurity Training for the Indo-Pacific Region JP-US Energy-sector Cybersecurity Workshop for the Indo-Pacific Region JP-US-EU Seminars on Cybersecurity in the post-COVID environment: Suggestions to the Indo-Pacific Region	Cybersecurity, Law and Policy, Training and Education	Indo-Pacific Region	Japan, US, and the European Union	1 week	Completed
iii. Defense Practice Against Cyber Attacks	Cybersecurity, Training and Education	Global	JICA		Completed
iv. Industrial Control Systems Cybersecurity Training for Indo-Pacific Region	Cybersecurity, Training and Education	Global	JICA	3 days	Planned in 2022

Initiatives	Category(ies)	Country(ies) Implemented	Funding Agency(ies)	Duration	Status
v. Capacity Building in International Law and Policy Formation for Enhancement of Measures to Ensure Cybersecurity	Cybersecurity, Training and Education	Global	JICA	12 days	Planned in 2022
44 Australian Strategic Policy Institute (ASPI)					
i. e-Governance in the Pacific: Mapping a Way Forward - Cyber Security Policy and Strategy	Cybersecurity, Law and Policy	Fiji, Kiribati, Papua New Guinea, Samoa, Solomon Islands, Tonga, Vanuatu	DFAT Australia, Estonia Development Cooperation	1.5 years	Completed
45 Fiji National University (FNU)					
i. Certificate of Attainment in IT Security Awareness	Training and Education	All Pacific		2 days course	Ongoing
ii. ISO/IEC 27001 – Information Security Management – Lead Implementer	Training and Education	All Pacific		5 days course	Ongoing
46 Asian Development Bank (ADB)					
i. Pacific Information and Communication Technology Investment Planning and Capacity Development Facility-Phase 2 - Technical Assistance	Cybersecurity, Cybercrime	Cook Islands, Palau, Marshall Islands, Tonga, Vanuatu	ADB	2022 - 2024	Ongoing
ii. Supporting Finance Sector and Private Sector Development in the Pacific	Cybersecurity	Regional	ADB	2021 - 2022	Ongoing
iii. Supporting Finance Sector and Private Sector Development in the Pacific - eKYC pilot	Cybersecurity	Samoa, Vanuatu	ADB	2021 - 2022	Ongoing

Pacific Region
Infrastructure Facility

www.theprif.org

ADB

Australian Aid

NEW ZEALAND
FOREIGN AFFAIRS & TRADE

European Union

European Investment Bank

JICA

WORLD BANK GROUP