UK Government

Australian Government
Department of Foreign Affairs and Trade

NEW ZEALAND
FOREIGN AFFAIRS & TRADE
Manatū Aorere

The Partners in the Blue Pacific P4C Outcomes Report

2023 | Nadi, Fiji.

OCSC
Oceania Cyber Security Centre

GFCE
Global Forum on Cyber Expertise

Contents

Executive Summary

The inaugural Partners in the Blue Pacific (PBP) Pacific Cyber Capacity Building and Coordination Conference (P4C) was held in Nadi, Fiji from 2nd to 4th of October 2023. Over 80 representatives gathered from Pacific island countries, PBP member countries and non-government stakeholders to facilitate a Pacific centred dialogue to inform future Cyber Capacity Building (CCB) efforts in the region.

Pacific island countries represented included: Cook Islands; Fiji; Kiribati; Marshall Islands; Nauru; Niue; Palau; Papua New Guinea; Samoa; Solomon Islands; Tonga; Tuvalu and Vanuatu. All PBP member countries were represented: Australia; Canada; Germany; Japan; New Zealand; the Republic of Korea; the United Kingdom; and the United States of America.

Five key themes emerged from the discussions at P4C:

- **Pacific Leadership:** The Pacific leading the co-design of CCB activities in the Pacific, for the Pacific and in the Pacific way. CCB efforts should not only be co-designed to address country specific priorities, but also align with and support the achievement of established regional priorities as defined in: (1) the Boe Declaration Action Plan; (2) the implementation plan for the 2050 Strategy for the Blue Pacific Continent; and (3) the forthcoming Pacific ICT and Digital Transformation Action Plan.

> Enhancing a common understanding on the unique context of the various Pacific island countries so that capacity building efforts are tailored

> Coherent and consistent coordination across the various partners will be key to the effectiveness to the support in this sector.

- **Contextualised Capacity Building:** One size does not fit all. A tailored approach is required for CCB in the Pacific that considers each country's identified and chosen priorities in addition to unique cultural, economic, and geographical contexts.

- **Improved Pacific Cyber Ecosystem:** The need for better coordination between all stakeholders. Improving the way stakeholders work together to deliver results by dismantling silos, developing a regional framework, adopting a holistic approach, enhancing trust and promoting knowledge sharing across all levels.

- **Embedded sustainability:** Working to ensure that Pacific island countries are properly equipped to not only receive the right assistance but to also be able to retain the capacity that is developed. CCB should shift away from an ad hoc approach, to longer-term commitments that build resilience strategically and holistically.

- **Inclusive Development:** adhering to the Pacific way of not leaving anyone behind, no matter the size of the economy. Each island is part of the Pacific family. CCB must be mindful not to widen existing gaps in equality, taking a whole of society approach and incorporating more than just the technical aspects of cyber.

Introduction

The inaugural Partners in the Blue Pacific (PBP) Pacific Cyber Capacity Building and Coordination Conference (P4C) was held in Nadi, Fiji from the 2nd to the 4th of October 2023. The Oceania Cyber Security Centre (OCSC) and the Global Forum on Cyber Expertise (GFCE) Pacific Hub were invited to organise the P4C on behalf of the PBP. Over 80 representatives gathered from Pacific island countries, PBP member countries and non-government stakeholders to facilitate a Pacific-centred dialogue to inform future Cyber Capacity Building (CCB) efforts in the region.

The Pacific Islands Forum's 2018 Boe Declaration, 2019 Boe Declaration Action Plan, the 2050 Strategy for the Blue Pacific Continent, and the 2023 Lagatoi Declaration all recognise cybersecurity as a regional priority and emphasise its central role in securing the Pacific's future security and prosperity. The Partners in the Blue Pacific (PBP), in collaboration with the OCSC and GFCE, structured the content and format of the P4C to align with and help fulfil these regional priorities by improving CCB program design and delivery.

The discussions that were held during the P4C were anonymised and documented by the OCSC, with the knowledge of all delegates, to capture the issues raised throughout the event and share them through this outcomes report with the wider CCB community. These notes have been analysed by the OCSC Research and Capacity Building team, identifying five key themes that will be explored in this report from the perspectives of the P4C attendees. Finally, the report will conclude with recommendations to improve coordination of current and future CCB efforts in the Pacific.

Pacific island countries represented that contributed to these discussions included: Cook Islands; Fiji; Kiribati; Marshall Islands; Nauru; Niue; Palau; Papua New Guinea; Samoa; Solomon Islands; Tonga; Tuvalu and Vanuatu. The Federated States of Micronesia, French Polynesia, New Caledonia and Tokelau were invited but unable to attend.

All PBP member countries were represented: Australia; Canada; Germany; Japan; New Zealand; the Republic of Korea; the United Kingdom; and the United States of America. PBP private sector partners included: BAE Systems Australia and Cyber CX.

Other stakeholders included representatives from: the Asia Pacific Network Information Centre (APNIC) Foundation; Asian Development Bank (ADB); Cyber Safety Pasifika (CSP); Digicel Pacific; Forum of Incident Response and Security Teams (FIRST); Global Forum on Cyber Expertise (GFCE) Secretariat and Pacific Hub; Internet Corporation for Assigned Names and Numbers (ICANN); Monash University; Pacific Cyber Security Operational Network (PaCSON) Secretariat; Pacific Island's Chief's of Police (PICP); Pacific Islands Forum (PIF - Secretariat and Fisheries Agency); Pacific Islands Law Officers' Network (PILON) Cybercrime Working Group; Pacific Telecommunications Security Expert Forum (PTSEF), United Nations Development Programme (UNDP); the University of Oxford; and Websafe Samoa.

Other stakeholders invited but unable to attend included: Asia Pacific Telecommunity (APT); Cadmus; International Telecommunication Union (ITU); Pacific Islands Telecommunications Association (PITA); Pacific Regional Infrastructure Facility (PRIF); Pacific Security College; University of the South Pacific (USP); and the World Bank.

Discussion

Delegates at the P4C recognised and discussed the requirement for change within Pacific cyber capacity building and coordination caused by the oversaturation of programs. Pacific delegates further acknowledged cyber assistance and support in the region lacks coordination.

Furthermore, existing monitoring and evaluation practices are limited and lack independent measurement of long-term impact, typically focused on self-reporting of project outcomes. Knowledge of longer-term impact from the perspective of Pacific island countries is limited to confidential assessments which are often not shared with donors. Under certain program agreements, it is the implementor who provides self-assessment to comply with program guidelines which generally do not involve any assessment of impact.

Instead of continuing to repeat the same actions and expecting a different outcome, the P4C recognised that a new approach was required. This involved recalibrating and realigning the needs and aspirations of the Pacific with the policies and strategies of development partners, thus propelling the region to move forward more effectively. The P4C provided an opportunity for stakeholders in the region to meet and discuss what's working, what's not and why, while planning contextualised actions that sustainably strengthen cyber capacity for the future.

These issues were explored throughout the conference and five themes emerged, and are discussed in more detail in the following section:

- Pacific Leadership.
- Contextualised Capacity Building.
- Improved Pacific Cyber Ecosystem.
- Embedded Sustainability.
- Inclusive Development.

Theme 1: Pacific Leadership

Capacity building, or people working together to share knowledge, skills and resources toward a common goal, is not a new concept for the Pacific, it is embedded in the Pacific way. However, delegates reflected that historically the Pacific has not usually led CCB and were clear that this must change. There is a clear demand to shift from donor-led CCB to the Pacific taking the lead to co-design future CCB efforts for the Pacific, with the Pacific and in the Pacific way.

The Pacific Islands Forum is already playing an important leadership role in the region and has highlighted the importance of cyber in both the 2018 Boe Declaration and 2050 Strategy for the Blue Pacific Continent. The Pacific ICT Ministers have recently built upon this further with the 2023 Lagatoi Declaration. Discussions confirmed that future CCB efforts should not only address country-specific priorities but demonstrate how they align with and support the achievement of goals defined in the 2019 Boe Declaration Action Plan, the 2030 Implementation Plan for the 2050 Strategy for the Blue Pacific Continent and the forthcoming Pacific ICT and Digital Transformation Action Plan. Given the considerable political support for addressing cyber in the region, delegates identified the pressing need to act swiftly to achieve change while they have the support of their national leaders.

On a practical level, the Pacific cyber community is strong, collaborative and showing leadership regionally by supporting peers to develop their own capability, especially in the incident response community. In accordance with the PBP principles of being Pacific-led, there is a desire for future CCB efforts to be co-designed by recipients to ensure they are tailored to meet their needs and delivered in the Pacific way. Furthermore, there was a request for existing relationships to be strengthened and widened to include other stakeholders beyond incident response teams for a more holistic approach to CCB. Suggestions included wider stakeholder engagement and increasing information sharing of what is working, what is not and why.

Pacific delegates communicated that they need to push back and say no to offers of support that are not aligned with their needs, cannot be absorbed within existing capacity, or do not fit their schedule. This extends beyond projects to events and workshops, with a call from the Pacific community that it is better to say no to meetings and workshops rather than sending the wrong staff and participating for the sake of it when such participation might not necessarily be required. This may also support the notion of less talk and more action by pushing back on attending meetings that may not be necessary or of low value to achieving Pacific goals.

Delegates stated that, in the past, international donors and implementers have played a role in perpetuating misaligned capacity building assistance. While it was recognised that these stakeholders continue to play an important part in the CCB ecosystem, there is a perception that they are not always acting in the recipient's best interest or following Pacific leadership.

Finally, there is a desire from the Pacific community for a common framework to help address regional priorities set by leaders to relieve some of the burden on limited resources for developing national policies, legislation, and standards. There was also a request that this should be supported by a platform for sharing knowledge and tools; therefore, strengthening relationships between countries by building the people network for wider collaboration.

Theme 2: Contextualised Capacity Building

Embodying the notion that one size does not fit all, a consistent issue raised throughout the conference was the need for CCB efforts to be tailored to each country's unique circumstances. This included the need for countries to understand where they stand now and identify their own priorities for next steps. Delegates suggested that CCB efforts should look to build upon what has been successfully achieved, as opposed to lifting and shifting solutions developed in larger economies outside the Pacific context, which are often not fit for purpose for Pacific island countries and need to be adapted. In support of this issue, delegates also raised the need for taking a 'filtered approach' to repackage global information and knowledge into the Pacific context so it can be better understood and absorbed.

It was noted that national priorities vary between countries, which can impact political will to support CCB over national and regional challenges such as climate change. Delegates stated that different countries are at different levels of cyber maturity. Combined with the varying levels of trained staff this impacts their ability to absorb CCB efforts in addition to their existing responsibilities and commitments.

Some identified variables that may shift the scope and delivery of capacity assistance in different jurisdictions may include geographic location; levels of linguistic diversity; cultural and economic factors; existing levels of maturity; affordability, reliability, and availability of high-speed connectivity; local human capacity and skills within the private and public sectors; user habits; and other non-cyber-related national priorities.

Examples of tailoring within the Pacific community embodied the notion of making use of what you already have and streamlining requirements from guidance and standards designed for bigger economies. This included establishing incident response capabilities without a formal national Computer Emergency Response Team (CERT); making use of existing governance structures; and taking a more agile approach to policymaking.

There is interest from both the Pacific community and the PBP to not only use an evidence base to identify needs but also to assess implementation and its impact on maturity. This includes a need for sharing priorities identified by assessments and any recommendations for action with partners where possible. Pacific delegates emphasised the importance of improving the sharing of success stories and lessons learnt across the Pacific community as a source of evidence of what is working, what is not and why.

Tailored and targeted training was specifically raised by several delegates as a key issue at both the national and regional levels. This included a request for resources that provide specific technical guidance for recipients to apply in their own environments over resources that embed a reliance on external ad hoc support that does not improve their sovereign capability. More in-country training that is tailored to the needs, context, and cultural norms of each country, extending to other stakeholder groups beyond incident responders, was seen as key to building the skills of a larger cohort. Such an approach may also provide some relief for the government staff who are often juggling existing multiple operational commitments with attendance at regional workshops and events. This currently requires significant travel and time away from work and home. Delegates also noted that this current practice of 'death by workshops' often leaves teams with either no, or degraded operational capability as there is no, or limited redundancy for key human resources when they are away.

Theme 3: Improved Pacific Cyber Ecosystem

The current ad hoc and piecemeal nature of existing CCB efforts was a consistent issue raised by delegates, who underscored the need for improved coordination between all stakeholders in the Pacific cyber ecosystem. Fundamental changes were requested to how capacity building stakeholders work together to enhance this ecosystem, so it can achieve successful cyber maturity uplift across the Pacific.

A consistent message from delegates was that the principal challenge undermining the existing cyber ecosystem is a lack of coordination between the Pacific island countries and the donors who provide or fund assistance. Delegates noted that the variety of support in the region is unclear and that there is a lack of clarity regarding who is doing what and what they are willing and able to support. Conversely, understanding which Pacific island countries are currently seeking what assistance has also been unclear for donors.

Pacific and PBP delegates agreed that the issue of poor coordination has previously been exacerbated by a lack of collaboration between the different external donor governments, which has produced an overcrowded, confusing, and often duplicative system of capacity building. PBP delegates noted that they have spread themselves thin trying to simultaneously lift maturity in multiple areas across multiple Pacific island countries at once, only to discover that they have repeated the work of alternative donor governments. While there has been goodwill on both sides to meaningfully uplift the Pacific's cyber capacity, the lack of alignment between the different stakeholder groups has inhibited substantial progress to date.

Governance challenges in the Pacific were raised by several attendees as having inhibited capacity building coordination. In some circumstances, it has historically been unclear who has had ownership of the different aspects of cyber in each Pacific island country (awareness, legislation, incident response etc.) and who the point of contact on the ground should be for international stakeholders. A lack of dialogue between the right people has subsequently led to duplicated and defunct assistance initiatives. Addressing this issue may assist in both: a) partners engaging with the right people; and b.) recipients knowing when to involve or defer to other teams, departments, or ministries within government.

Trust also emerged as a central component of the regional cyber ecosystem that needed strengthening. Relationships were described as fundamental to all successful capacity building work in the Pacific and these relationships are predicated on trust.

A number of Pacific delegates discussed that, on occasion, mistrust between Pacific stakeholders, external governments and implementers has arisen due to occasional perceptions of geo-politicking and pursuits of self-interest. While it was acknowledged that not every stakeholder has shared mutual priorities and interests, delegates expressed a desire for a process through which commonalities can be identified and stakeholders can work together and build a sustainable capacity building system.

Trying to set individual geopolitical agendas and profit motives aside, and instead prioritising areas of mutual interest, was also suggested as a possible solution. Another proposed strategy involved engaging Pacific 'Cyber Heroes' in workshops and events to showcase local and regional capacity, build trust and confidence in this capacity, and reduce the reliance on external experts.

In addition to improving coordination and developing greater trust between stakeholders, adopting a holistic approach to capacity building was another identified solution to enhancing the Pacific cyber ecosystem.

With rapid digital advances across Pacific island countries, cyber has become a whole of nation issue that covers a broad range of people and areas. Consequently, delegates discussed that effective capacity building and incident response now requires a whole of nation response. Such an approach must go beyond the traditional focus on incident response and technical personnel, and actively include all the policy makers, educators, law enforcement officials and community members affected and responsible for managing cyber incidents and maturity uplift.

It was communicated that some stakeholders who have a significant role in enabling successful cyber capacity building and incident response have been insufficiently involved with the topic through either a lack of understanding of its applicability to them and their role, or because they have been excluded from greater participation. A holistic and inclusive approach to cyber capacity building was therefore identified as a necessity, without it these stakeholders will continue to be excluded and progress will be limited.

Streamlined and improved events were also presented as an ongoing challenge to the Pacific cyber community. There was resounding recognition amongst the Pacific cyber community present at the P4C that there is an oversaturation of events that are exhausting, of limited value, and prevent attendees from doing their day jobs. While community and peer learning are fundamental components of the regional cyber ecosystem, and these are facilitated by events, there was a collective desire articulated by Pacific delegates for greater coordination that would allow Pacific cyber leaders to attend necessary events consecutively and avoid unnecessary time travelling. Pacific delegates also noted that there was a current gap in knowledge sharing, with those attending workshops and events rarely sharing knowledge gained with their teams when returning home.

Many Pacific cyber stakeholders wear multiple different hats and cannot afford to take long, unproductive trips away from home. More practical arrangements around scheduling, program content, and resources were asked for to maximise not only the utility of events but also people's time. Furthermore, there was a request that a stronger emphasis be placed on getting the right people to attend events. It was agreed that Pacific and non-Pacific stakeholders can only add or take value from opportunities if they are the right people for that opportunity.

Through the discussions held at the P4C, it was established that the exchange of capacity building information and knowledge within the region needs to be improved. The Pacific cyber community relies heavily on one other to help guide their individual capacity building strategies and priorities. Peer-to-peer learning within and between countries is a fundamental component of how delegates have historically built their capacity building agendas. However, delegates also reported that information is not as free-flowing as they would like. Consequently, there was an identified need to simplify and ease the sharing of knowledge between and within Pacific island countries.

Geographic disparity, limited ability to attend offshore training, and gatekeeping of information, were all identified limitations to enhanced knowledge sharing. As discussed under Theme 2, when training sessions/workshops are held overseas often there are only a select few people who can attend due to financial and capacity constraints, and those that do attend do not always share what they have learned freely. Subsequently, there was a call for more accessible education materials, scholarships for formal higher education and certified training, more reliable knowledge-sharing mechanisms and the establishment of knowledge exchange focal points to help address this issue.

Theme 4: Embedded Sustainability

Resilient and sustainable CCB programs and assistance were another frequently raised topic throughout the conference. Too often it has been the case that assistance initiatives are not set up to last long-term and Pacific island countries are left with only short-term benefits, rather than sustained advancements. Improving the Pacific cyber ecosystem, as discussed above, will increase the sustainability and resilience of regional capacity building. However, it was discussed that on top of improving inter-stakeholder relationships, systems of governance and advancing coordination to better match resources to the Pacific's needs and priorities, work must be undertaken to ensure that Pacific island countries are properly equipped to not only receive the right assistance but be able to retain it.

While there is a strong appetite for the PBP suggested program of legacy replacement for ageing equipment and software or the replacement of unlicensed or cracked software, there was concern expressed around the local sustainability of such support for the total cost of ownership for the life of new software or equipment which is typically absent from offers of support. The challenge of the increased cost of climate-resilient digital infrastructure (including data centres), availability and affordability of cyber insurance, cost of forensic tools, and the ability to pay ransoms and identify the origin of such attacks were also raised as concerns, which should be factored into future CCB efforts.

Human resources were also raised as an ongoing challenge; public sector salary bands and budgetary constraints make it difficult for Pacific governments to compete with the private sector when hiring and retaining skilled workers, both domestically and internationally. 'Brain drain', or the poaching of Pacific skilled workers to higher paying jobs in wealthier economies such as New Zealand and Australia, is a universally felt burden that amplifies workforce instability. Pacific ministries and agencies need robust, reliable, and agile digital workforces. However, the required skillsets needed to fully operate and maintain a healthy digital workforce in most Pacific island countries are scarce, which subsequently constrains ongoing resilience. Those who do have the right skills are forced to wear multiple hats within their system and are often overworked, an issue that further undermines workforce sustainability.

In addition to challenges with affordability, there was also a clear message that emerged from the conference that while short-term interventions had their benefits, short-termism was undermining effective regional capacity building. 'Tick-the-box' exercises and interventions that are siloed, uncoordinated, and with limited long-term vision, were reported to have been prominent in the regional capacity building space and have tended to produce limited impact. For instance, delegates cited that in circumstances that require external expertise to overcome an immediate challenge, the trend has been to employ international vendors or implementers from outside the region to quickly fill the identified gap and resolve the issue. While in the interim this fixes the problem, these vendors and implementers often then leave without sharing their knowledge or contributing to meaningful local capacity improvements. The local context is therefore no better prepared to mitigate or overcome a similar issue in the future.

Rather than building capacity, it was said that short-term interventions instead build a cycle of dependence. Alternatively, it was canvased that if necessary short-term actions could be incorporated into long-term strategic initiatives that seek to build resilience and maturity and form part of a broader regional capacity building framework, the Pacific may experience more efficient outcomes.

When designing long-term programs, several attendees discussed that it is important to build in flexibility and adaptability so that these programs can adjust as they go and remain fit for purpose. Furthermore, there was an expressed concern that capacity building activities should have tangible, measurable results, and that programs that can point to their successful outcomes are preferable. It was seen that such evidence would allow stakeholders to keep track of what is working and what is not, and inform appropriate adjustments to the design and delivery of capacity building programs as they unfold. Real results can take time to materialise, and delegates believed that the region would benefit from a strategic, balanced approach to program delivery that incorporates complementary short and long-term objectives and employs a coordinated approach to identifying priorities and assessing achievements.

Integrated within the issue of impactful localised capacity building were concerns around sovereignty and the ability of Pacific island countries to protect their sovereign interests. Developing sustainable cyber capacity is not just an employment or financial issue, it is also related to maintaining sovereign capabilities and protecting sovereign assets. Purely short-term interventions, fail to improve local expertise and do not accommodate for the total cost of ownership, do nothing to alleviate Pacific island countries' dependency on external parties to develop, maintain, restore, or replace their digital systems and their subsequent sovereign interests. The inclusion of Non-Disclosure Agreements (NDAs) in all CCB activities was suggested as a means of preserving Pacific sovereignty and building trust as covered under Theme 3.

Theme 5: Inclusive Development

The Pacific cyber ecosystem is built around community and within this community there is a strong emphasis on inclusive development and ensuring that no one is left behind. Pacific delegates at the P4C collectively voiced support for a comprehensive approach that sufficiently helped all communities simultaneously instead of a chosen few. This sentiment exists both regionally, in a desire to look after the smallest and most isolated nations, and nationally, in a desire to look after the most vulnerable social and cultural groups that extend beyond the main islands to those living on outer islands.

It was recognised that digital development can have both positive and negative impacts and that some groups are more vulnerable to negative impacts than others. Therefore, it is crucial capacity building efforts in the region account for, and actively address, these divides so that they do not inadvertently exacerbate them. Socio-economic, linguistic, gender, disability, and geographical divisions were highlighted as inclusive development challenges that both the PBP and Pacific island countries needed to accommodate in their future capacity building program design and delivery to avoid the broadening of existing inequalities. Diverse stakeholders and perspectives need to have active input into the broad spectrum of themes and challenges highlighted at the conference and within this report, ensuring that the entire region has the opportunity to advance cyber maturity and resilience collectively.

Recommendations

The OCSC has analysed the P4C deliberations and has compiled the following recommendations for further consideration by PBP governments, Pacific island countries, and other relevant stakeholders.

These recommendations have been split into short-term and long-term priorities. Short-term recommendations are designed to be progressed and reported on at the 2024 P4C. Longer-term recommendations address sustainability goals to be achieved over the coming years, with progress reported on at subsequent P4Cs.

The OCSC acknowledges that a number of the recommendations will require further evaluation and the initiation of separate actions to achieve their implementation. Therefore, these recommendations should be taken as a starting point for delivering longer-term impact.

Short-Term Recommendations

R1 To support the notion of less talk more action, the next P4C event must include a focus on what actions have been taken and how progress was achieved. This should be supported by a discussion of next steps for the following year, aligned to the existing Pacific cyber priorities defined by the Pacific Islands Forum and ICT Ministers.

R2 Consider what tools, knowledge and resources can be rapidly shared and deployed to meet the most urgent needs, mindful of sustainable principles such as support for the total cost of ownership. Examples include:

- mobile digital forensics kits which can be deployed to countries without existing digital forensic capability;
- table-top exercises to inform risk assessments, develop and test response plans to ransomware and other serious incidents; and
- identifying and sharing points of contact.

R3 To avoid duplication, adopt an existing assessment and evaluation approach to measure progress of PBP cyber programmes on cyber maturity and determine impact from the perspective of Pacific island countries and their priorities.

R4 Consult with existing regional bodies regarding what, if any, consolidation or co-location can occur regarding regional events. For example: PaCSON; CSP; PILON; PRFP; P4C; ICT Ministers Meeting; ICANN and IGF. This should include consideration of what events must be regional and what can be targeted at the country level.

R5 Develop and implement a confidential mechanism for recipients to provide frank and fearless feedback to donors and implementers, while protecting future opportunities for support aligned to recipient's needs.

Long-Term Recommendations

R6 Pacific governments should consider working to formalise and communicate their national cyber governance structures and mandates. This will help ensure that stakeholders are connecting with the right people when managing cyber issues, capacity building initiatives and events.

This should include consideration of:

1. a fit for purpose approach that considers the national context and size of the economy; and
2. identifying which entities, people or person should lead:
    a. formulation and implementation of policy and strategy;
    b. incident response;
    c. online safety, awareness, training and education;
    d. drafting cyber legislation and regulations;
    e. guidance for good practices and use of standards; and
    f. requesting assistance.
3. how to share this structure internally and with partners.

Furthermore, to support regional commitments to Cyber security challenges, Pacific governments may want to consider how domestic governance structures align to regional governance and reporting arrangements, for example as defined in the PIF 2030 Implementation Plan for the 2050 Strategy.

R7 To complement activities, deconflict and reduce duplication, all donors, implementers, and multilateral organisations are encouraged to coordinate CCB activities with and between regional bodies. For example, by aligning activities with and between the Pacific Islands Forum and the GFCE Pacific Hub. To assist with coordination and funding of longer-term initiatives, donor and Pacific governments should consider pooling or 'warm handovers' of funding for CCB where possible.

R8 To improve CCB sustainability and outcomes in the region, stakeholders should consider including the following requirements in future CCB proposals, mindful of not overburdening already stretched resources in recipient Pacific island countries:

1. a flexible plan that sufficiently balances the need for short-term interventions to respond to immediate needs with long-term maturity uplift;
2. evidence that there is an identified need for the activity, including a request from the recipient for the activity to occur, and confirmation that the activity is not a duplication of existing efforts;
3. co-design of the activity with the recipient at the scoping or initiation phase before implementation is approved;
4. stage-gate funding with recipient-led feedback determining progression, corrective action or termination between project phases. This process should empower Pacific governments to correct or stop projects that are not delivering desired outcomes without fear of missing out on future support. The lessons learnt should be shared with all parties concerned to improve practice and future efforts;
5. a sustainability plan that addresses concerns surrounding long-term affordability (including total cost of ownership for the life of the product or service), national sovereignty (such as the use of non-disclosure agreements), local workforce capacity and capability uplift through knowledge sharing;
6. any assessment component to be tied to a donor funding mechanism to fund recipients chosen identified priorities;
7. approved projects to be listed on public databases and these databases should be regularly reviewed to ensure they are accurate and up to date to remain of value. The GFCE's Cybil Portal is an example of an existing public database for global capacity building activities. This will help to avoid duplicated efforts; and
8. consider how to build on what has been successfully achieved to date and not overburden the Pacific cyber ecosystem with too many additional initiatives.

R9 Offerings of tailored education and professional training programs to the broad Pacific community, supported by scholarships, should be considered. These training programs should be coordinated and include a sustainability plan that ensures a broad range of stakeholders can participate. This will help to build a cohort of trained staff and develop a regional skills base, limiting the impact of 'brain drain'.

Education, training, workshops, and best practice resources should:

1. include Pacific relevant examples to filter the content to the Pacific context. For example, including case studies (real or fictitious) to apply concepts in the context of Pacific island countries;
2. where possible, partner with local or regional educational institutions to develop materials that are tailored to the Pacific context;
3. encourage participation of the local private sector to assist in holistic uplift of maturity; and
4. encourage knowledge sharing between participants and their teams at home.

R10 Focus on strengthening existing relationships to achieve long-term goals. This should include considering:

1. building the cultural capacity of donors and implementors;
2. providing politically agnostic support;
3. increasing transparency around donor priorities to enable increased collaboration on shared interests; and
4. utilising existing local and regional experts to help share knowledge and build up Pacific Cyber Heroes to sustain capacity in the Pacific, for the Pacific and in the Pacific way.

Acknowledgments

The P4C Outcomes Report was authored by Dr. James Boorman (OCSC) and Mr. Joe Fulwood (OCSC). The authors thank Mr. Md Ekramul Islam for note-taking throughout the conference which was essential to inform this report.

Reviewed by and feedback incorporated from: Prof. Carsten Rudolph, OCSC and Monash University; the Global Forum on Cyber Expertise (GFCE); and the Partners in the Blue Pacific (PBP).

Approved by: Mr. Cameron Boardman, OCSC.