PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK

PaCSON Capacity Building

Action Plan 2025-2028

From the Convenors

Since 2017 PaCSON members have worked together to make significant strides in lifting cyber security capabilities and readiness across the Pacific. The foundations of PaCSON enable cooperation and collaboration by empowering members to share cyber security threat information, tools, techniques and ideas.

A key part of PaCSON is the Capacity Building Working Group. Over the years, we have seen a rapid increase in the delivery of various cyber capacity building initiatives, which has translated into positive changes at the national level. To help shape future efforts in the Pacific and noting the increase of partners wanting to engage in capacity building efforts, members have agreed to the establishment of the PaCSON Capacity Building Action Plan 2025-2028. This resource will signal the needs of the Pacific at a regional level.

We would like to thank the PaCSON Capacity Building Working Group members for their valuable contribution to this Action Plan. The five strategic focus areas will channel our focus, to help build capacity in areas that matter most to our PaCSON members and chart a tangible and measurable way forward. We are grateful this opportunity has also allowed us to look back, in order to move forward, in a purposeful Pacific way, as a region.

Ngā mihi mahana

Lefaoali'i Meremine Auelua

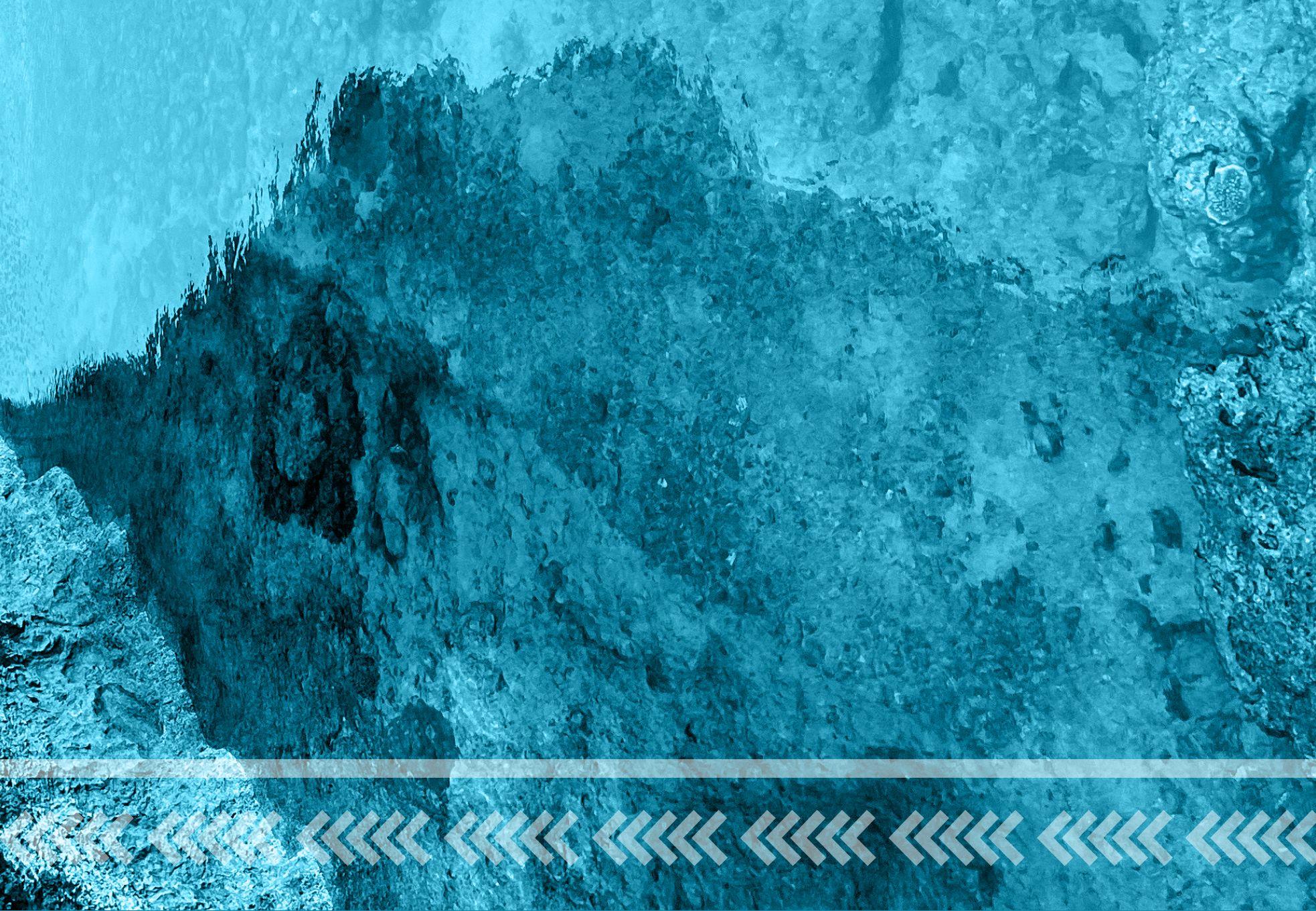
NCSC New Zealand

Malo 'aupito

'Otukolo Tokai

CERT Tonga

Contents



Key considerations

What is the Cyber Security landscape in the Pacific?

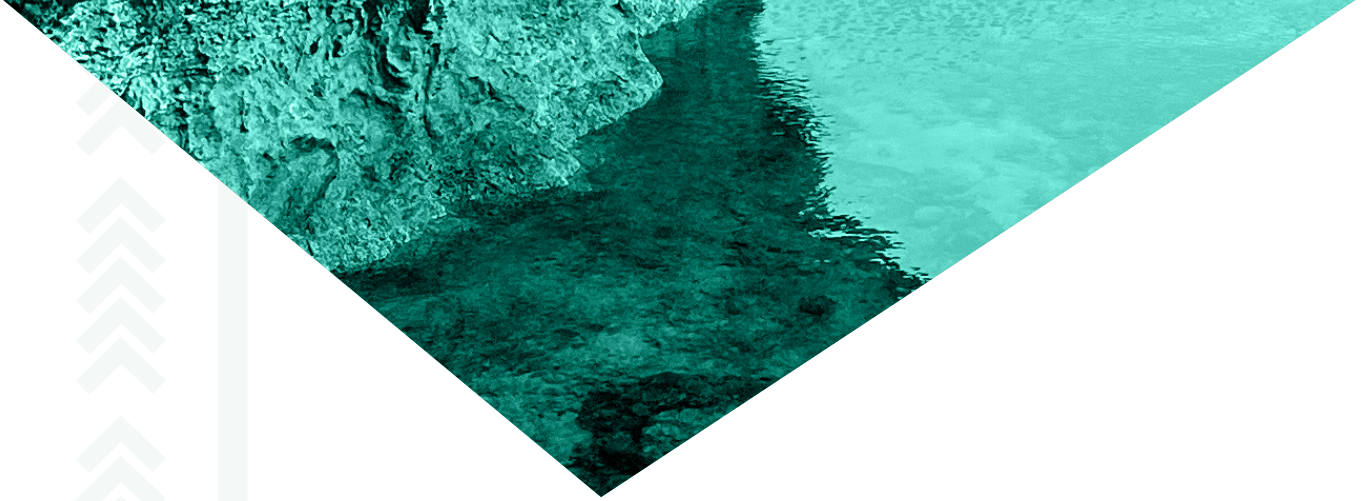
The Pacific region is increasingly targeted by a wide range of malicious cyber actors as shown by the proliferation of ransomware incidents, phishing expeditions and sophisticated scams. The Boe Declaration accurately identified cybercrime and cyber security as emerging security threats that we must address to ensure the safety and security of Pacific peoples and the viability of our economies, critical infrastructure, data and information. The impact of cyber threats can be devastating for nations of all sizes, and it is imperative we work together to set goals, agree on actions and implement initiatives that build a safe and secure region.

What is the PaCSON Capacity Building Working Group doing to help build Cyber resilience?

The PaCSON Capacity Building Working Group (PaCSON CBWG) is committed to highlighting the needs of our members and ensuring their vision for regional collaboration is realised. The PaCSON CBWG aims to be more aligned with the commitments leaders have underscored in regional forums, including the Lagatoi Declaration. Digital transformation provides opportunities, whether it be economic growth, improved health services or access to better educational services. However, to protect the systems we use, we need to measure the success of the actions we take as a community.

What is the pathway forward?

This new Action Plan is owned by PACSON members. Convenors have shaped the content based on the views of the members and will monitor the implementation of this plan. This Action Plan signals the focus areas for partners that want to deliver capacity building in the Pacific – the actions are the initiatives members want to see implemented. This is a step change in how this community has approached capacity building in the past – it's a about building together the Pacific way. The five strategic focus areas can also assist current and future partners to tailor their assistance accordingly at the regional level.



INSTITUTIONAL GOVERNANCE

Institutional Governance underscores the importance of foundation building. New approaches and guidance on future thinking will help strengthen cyber resilience in the Pacific. As emerging threats become more persistent, Pacific countries are moving towards building Computer Emergency Response Teams (CERTs), CERT-like functions or National Cyber Security Centres. Establishment support and policy guidance are fundamental in building effective institutions in the Pacific region.

Level of Ambition

- PaCSON members can access reliable support and information to establish relevant mechanisms, to uplift cyber security resilience within respective countries.
- Pacific CERTs have a clear mandate, with delegated authority, by respective governments.
- Pacific countries understand how the 11 norms of responsible state behavior in cyber space can support national interests.
- PaCSON members can support their respective countries to build sustainable livelihoods in a fast-changing world.

1

STRATEGIC FOCUS

Actions

- Work collaboratively with other regional infrastructure to build legislation and regulatory support.
- Readiness assessments conducted yearly to understand national gaps.
- Support the development of national cyber security policies and mechanisms.
- Specific support on building CERTs, national cyber centres and CSIRT functions.
- Enhanced formal information sharing mechanisms.
- Deliver study tours to strengthen understanding of governance processes, cross agency collaboration on cyber related issues.
- Regional SOC with 'break-glass' incident response function, supported by relevant partners.

Measure of Success

- An increase in the number of countries with established CERTs/ CERT-like functions or national cyber security capabilities.
- Number of requests supported under this pillar.
- Gradual increase in cyber legislation and policy implementation.
- Tailored policy support for Pacific countries.
- Deliver at least one study tour in the next three years to help shape the future of cyber security functions in the Pacific.

Potential Partners

- Partners and Friends of PaCSON.
- Relevant development partners.

Alignment

- 2050 Strategy for the Blue Pacific Continent.
- Boe Declaration Action Plan.
- Sustainable Development Goal 4, 8, 9 and 17.
- Lagatoi declaration on digital transformation of the Pacific priority four.
- Budapest convention.
- United Nations 11 responsible norms of state behavior.
- ITU global cybersecurity index.

WORKFORCE DEVELOPMENT

The cyber skilled workforce in the Pacific region is facing significant challenges. A decrease in professionals at a time when the Pacific is looking to increase its digital footprint is impacting governments and local private sector. With the reliance on digital infrastructure, local capability and capacity are crucial. This pillar will focus on initiatives that will help address the skills gap and provide growth opportunities.

Level of Ambition

- The Pacific region has a highly skilled cyber security workforce to support national initiatives and regional cooperation. Increased capability and capacity will support the uplift of the Pacific response to cyber threats and the ability to provide informative cyber security advice to leaders.

2

STRATEGIC FOCUS

Actions

- Yearly secondments, internships or scholarship opportunities for PaCSON members.
- Deliver train-the-trainer model training on CERT functions.
- Seek investment in establishing workforce development plans or implementation of initiatives to increase number of staff where resources are low.
- Support for professional certifications or micro-credentials.
- Support for attendance at regional and global conferences / symposiums.
- Partnerships with academic institutions for training on AI / cyber security.

Measure of Success

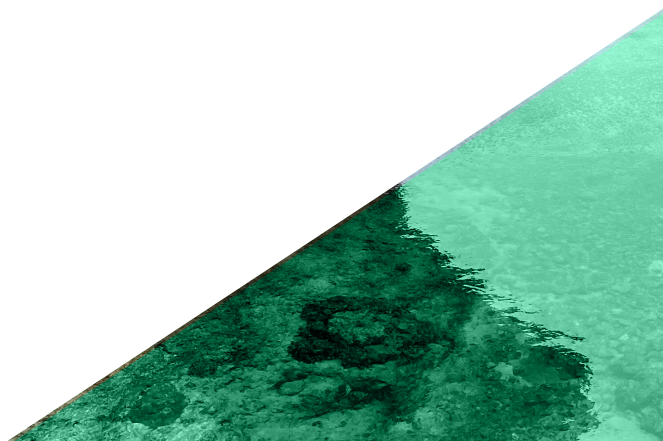
- Increase number of PaCSON partners participating in secondment or placement opportunities.
- Number of training courses delivered locally by Pacific PaCSON members.
- At least three training opportunities per year for PaCSON countries.
- Number of workforce development plans and the number of staff are increased by initiatives to support CERT-like functions.

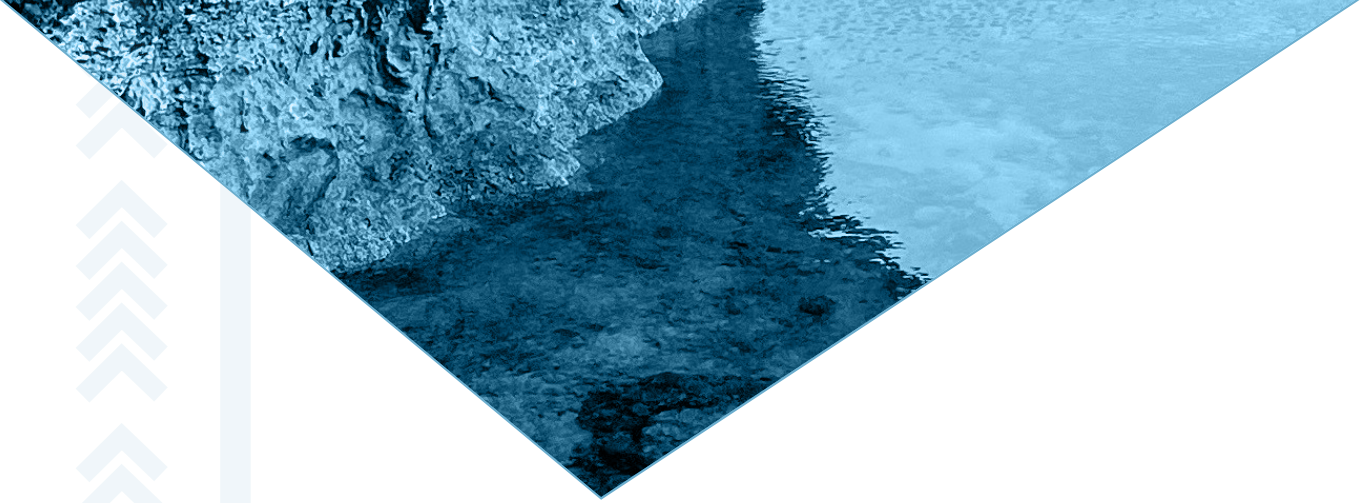
Potential Partners

- Friends of PaCSON.
- Partners of PaCSON.
- Relevant industries (Public and private).
- International development donors.
- Academia.
- Civil society groups.

Alignment

- 2050 Strategy for the Blue Pacific.
- Boe Declaration Action Plan.
- Sustainable Development Goal 4, 8, 9 and 17.
- Lagatoi declaration on digital transformation of the Pacific priority four.





INCIDENT RESPONSE

Cyber incidents have increased in severity in the Pacific. Limited resources remind us of the need to be vigilant and build local capability. Malicious actors often exploit weaknesses in systems including server exploitation, phishing campaigns and web compromises, to gain initial access to networks. Continuous improvement and upskilling are required to arm each PaCSON member with tools and initiatives over the next three years, to respond to cyber incidents to the best of their ability.

Level of Ambition

- PaCSON members have the capacity and capability to respond to cyber incidents in a timely manner. Furthermore, members are provided with support to address state sponsored cybercrime and online cyber bullying related issues.

3

STRATEGIC FOCUS

Actions

- Specific threat hunt and remediation information and training is provided at a bilateral or regional level.
- Regional tabletop exercises and CTFs.
- Training on incident response tools.
- Incorporation of incident communication and advisory training in every PaCSON related initiative.
- Training in cyber security incident management.
- Creation and implementation of incident response plans and playbooks.
- Explore legal frameworks for cross-border cooperation e.g. sub regions.
- Deployment of PaCSON cyber security team for supporting major events (PIFLM, CHOGM, etc.).

Measure of Success

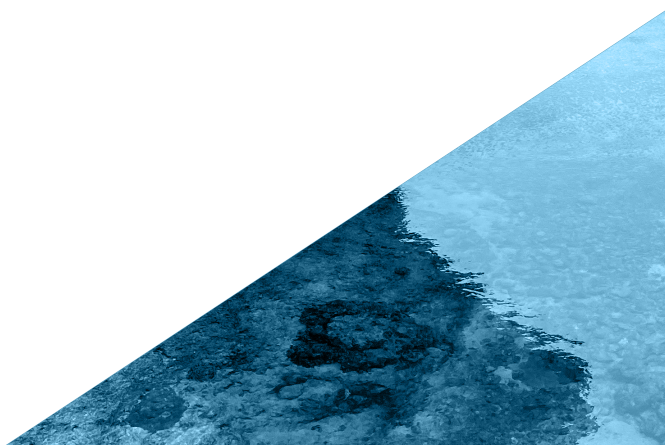
- The responsiveness of Pacific partners to future cyber incidents.
- Number of trainings provided over the course of three years.
- The number of alerts and advisories established by partners.
- At least one TTX delivered in the Pacific.
- Responsibilities are shared among members.
- Members are reporting activities.
- Implementation of Standard Operating Procedures and incident response plans that are tested.

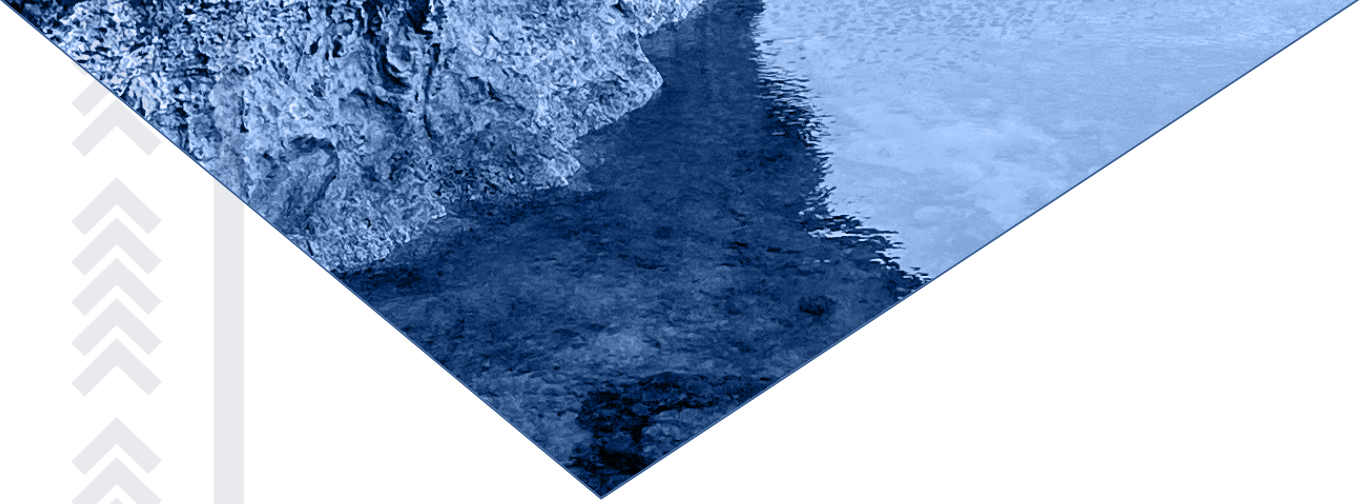
Potential Partners

- Friends of PaCSON.
- Partners of PaCSON.
- Relevant industries.
- Relevant regional groupings such as PILON and PICP.
- International development donors.
- Senior leaders.
- APCERT/FIRST.

Alignment

- 2050 Strategy for the Blue Pacific Continent.
- Boe Declaration Action Plan.
- Sustainable Development Goal 4, 8, 9 and 17.
- Lagatoi declaration on digital transformation of the Pacific priority four.





CRITICAL TECHNOLOGY

Investment in infrastructure and innovation are crucial drivers of economic growth and development. Critical infrastructure supports the provision of services that are essential to the growth of PaCSON members. Loss, damage or disruption to these services can adversely affect Pacific economies, security and greatly impact on the livelihoods of Pacific peoples. With the growth of new industries, including information and communication technologies, it is important to find lasting solutions to both economic and environmental challenges and underscore the importance of information sharing and innovation, to facilitate sustainable development.

Level of Ambition

- PaCSON members are well informed of products, services and procurement processes to assist with future bilateral decisions on critical technology.
- Establishing trusted and secure systems which help create a stable cyber environment underpinned by policy and regulatory frameworks.
- Pacific partners build the resilience of critical infrastructure to be able to manage cyber incidents, recover from disruptions, adapt to the changing conditions and provide the same level of service.
- Have best practice and guidelines in place.

4

STRATEGIC FOCUS

Actions

- Create opportunities for PaCSON members to engage with technology providers to understand their products. This could include engagement with Amazon and Google.
- Share advice on procuring large scale infrastructure and licenses. This includes understanding what support can be provided at a regional scale.
- Developing regulatory frameworks or processes to support critical infrastructure assets and providers.
- PaCSON may join conferences, host side events, or have an AGM together with Vendor Expo or Pacific Cyber Drill.
- Receiving advice from trusted partners regarding equipment / critical infrastructure.
- Training on a secure by design / secure by default framework.

Measure of Success

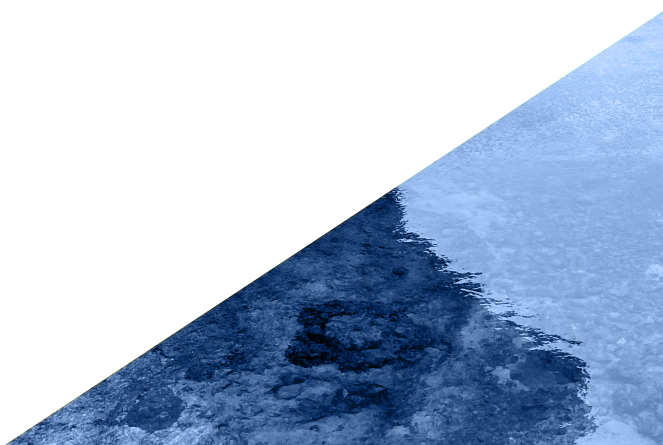
- Number of engagements between PaCSON members and vendors.
- Implementation of critical technology related processes or mechanisms over the course of three years.
- Number of global best-practice initiatives delivered.
- Ensure emerging technologies are secure, reliable and affordable (For example, AI).

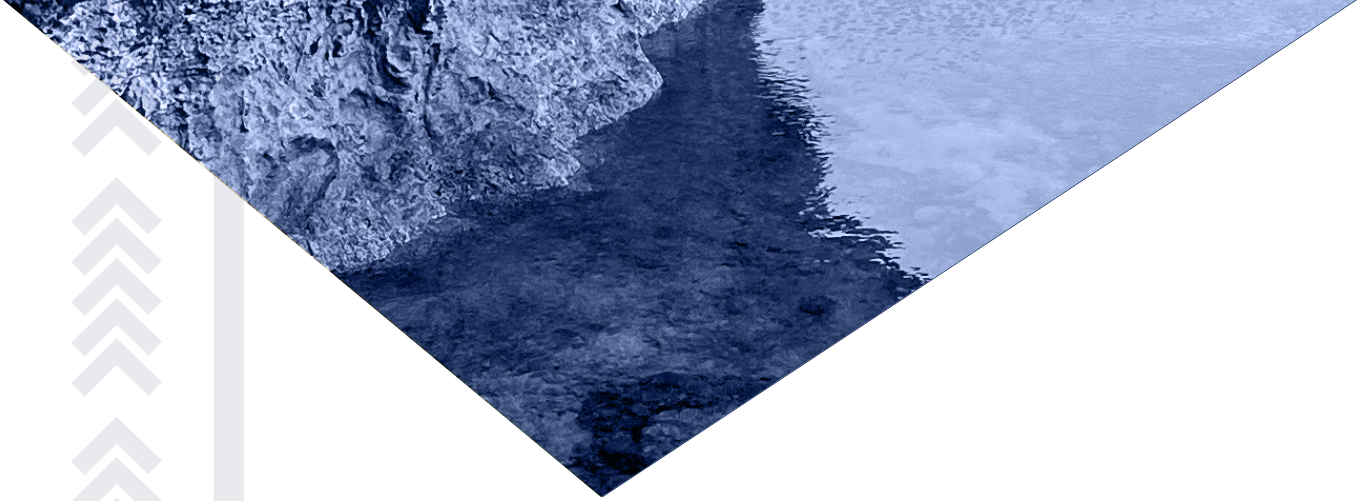
Potential Partners

- Partners of PaCSON.
- Relevant industries and tech/ telecommunication providers.
- Partners of the Blue Pacific partners.
- APT, ITU, APCERT.
- CISA and Shadowserver.
- PRIF.
- Intelligence community.
- Big tech (Meta, Amazon, Google, Microsoft, SpaceX, social media, etc.).

Alignment

- 2050 Strategy for the Blue Pacific.
- Boe Declaration Action Plan.
- Sustainable Development Goal 4, 8, 9 and 17.
- Lagatoi declaration on digital transformation of the Pacific priority four.
- United Nations Disaster Risk Reduction Database.
- ISO & NIST international standards.





REGIONAL UPLIFT

Pacific regionalism and the 'Pacific way' are well known concepts to PaCSON members. It is one that transcends all boundaries and is used to address challenges together, including cyber security. We are committed to building upon our respective cyber journeys and are committed to building a prosperous, safe and secure cyber environment for our Pacific region. We have seen the success of the Pacific deployment to the Commonwealth Heads of Government Meeting and the impact our Pacific missions have had during the UN Open-Ended Working Group Meetings on ICT.

Level of Ambition

- Foster the strengths of each Pacific country and explore tangible ways to support each other to ensure no one is left behind.
- Reinforce PaCSON's role amongst regional architecture and reaffirm its support to the Pacific Island Forum on cyber related matters.
- Work towards building regional expertise that can be used by PaCSON members to work through any challenges and share lessons learnt.

5

STRATEGIC FOCUS

Actions

- Identify ways to continue the deployment of a Pacific technical team to support regional events and forums.
- Support representation at global international forums/conferences and relevant cyber weeks.
- Provide relevant information to the Pacific Island Forum on cyber security matters for leader's consideration.
- Deployment of child exploitation filters at a regional level through Internet Service Providers (ISPs).
- Empower/mandate PaCSON members to implement changes quickly.
- Reaffirm PaCSON as a part of the regional architecture.

Measure of Success

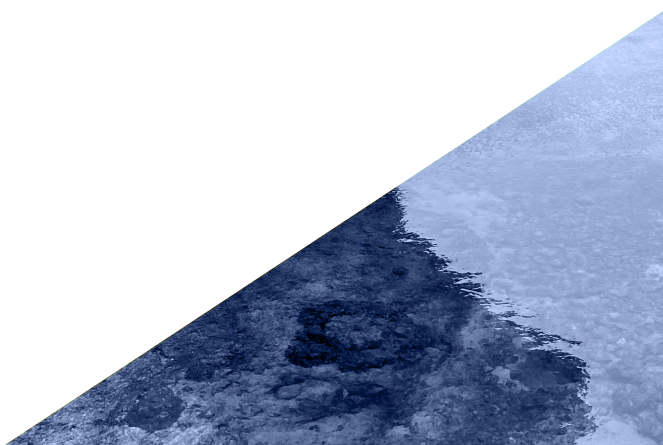
- Number of deployments over the course of three years.
- International forums/conferences speaking roles offered to PaCSON members.
- Number of papers provided or requested by the Pacific Island Forum.
- National policies published.
- Develop measurement criteria for pacific cyber maturity.
- Less incidents across PaCSON member countries.
- Cyber Maturity Models.
- PILON (Assessments, legislation, laws & guides).

Potential Partners

- Partners of PaCSON.
- Relevant industries.
- Academia.
- PaCSON working groups and members.
- PITA.
- PacNOG.
- PILON.
- International development donors.

Alignment

- 2050 Strategy for the Blue Pacific Continent.
- Boe Declaration Action Plan.
- Sustainable Development Goal 4, 8, 9 and 17.
- Lagatoi declaration on digital transformation of the Pacific priority four.



PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK