Report on Intersessional Consultations of Caribbean Internet Governance Policy Framework On Data Governance & Cybersecurity

TABLE OF CONTENTS

1. INTRODUCTION

The Caribbean Internet Governance Policy Framework is the region's principal statement of shared policy direction for the internet. Now in its fourth edition, published in January 2024, it is coordinated by the Secretariat of the Caribbean Telecommunications Union (CTU) and developed through the Caribbean Internet Governance Forum (CIGF), which serves as the region's primary multi-stakeholder assembly on internet governance. The Framework is reissued periodically so that it continues to reflect technological and social change, to guide governments and users and to amplify Caribbean perspectives in global internet governance spaces.

Two developments since the fourth edition gave particular urgency to this review cycle: the adoption of the Global Digital Compact (GDC) in September 2024 and the approval of the WSIS+20 outcome document in December 2025. Both call for resilient digital infrastructure and for emerging technologies that are safe and secure by design. Alongside these, the region has seen the rapid rise of generative and agentic artificial intelligence, the emergence of post-quantum cryptography as a practical concern and a continuing pattern of ransomware and data-extortion incidents affecting government ministries, health systems, utilities and financial institutions across the Caribbean.

To prepare the ground for the 22nd CIGF, the CTU Secretariat convened two open, virtual intersessional consultations. The first, held on 2 June 2026, examined data governance and whether it belongs within the Framework. The second, held on 6 August 2026, examined cybersecurity, using the CARICOM Cybersecurity and Cybercrime Action Plan (CCSCAP) as its point of departure. This report consolidates the discussion from both sessions.

2. CONSULTATION ONE — DATA GOVERNANCE (2 JUNE 2026)

The first consultation opened with an overview of the current Framework, its six strategic areas, the WSIS definition of internet governance and the relationship of the Global Digital Compact and the WSIS+20 review to both internet governance and data governance. The Secretariat also advised that a specialised Caribbean AI task force is being formed to report on the implications of artificial intelligence for the region.

2.1 WHY DATA GOVERNANCE MATTERS FOR THE CARIBBEAN

Data governance was defined for the purposes of the session as the frameworks, policies, rules and institutions that govern the collection, storage, processing, sharing, transfer and use of data. Its constituent parts were identified as legal and regulatory frameworks; policies on data quality and security; standards and interoperability; ethics and the protection of rights; and oversight mechanisms.

The regional stake is substantial. Because most Caribbean data is processed outside the region, questions of data sovereignty and economic dependency arise directly. A comparison of data governance with internet governance identified three areas where the current Framework is largely silent:

- Data ownership.
- Cross-border data flows.
- Data generated outside of internet transactions.

2.2 ONE FRAMEWORK OR TWO?

The central question of the session was whether data governance should be absorbed into the existing Framework or developed as a separate instrument. Participants leaned towards a single mechanism, on the reasoning that splitting the material across two documents risks losing the audience the Framework has taken years to build.

A counterpoint was raised that data governance is in significant part a matter of content rather than carriage and may therefore fall outside the portfolio of telecommunications regulators — which in turn raises the practical question of which regulators, telecommunications or data protection, are the relevant interlocutors in each territory.

The discussion also worked through terminology. A hierarchical structure was proposed in which digital governance is the broadest term, with internet governance and data governance sitting beneath it. This connects to a question the Secretariat had already placed before the meeting: whether the scope of the Framework should expand from internet governance to digital governance. Participants were invited to review the digital governance framework published at wdg.org and to send comments to the CTU.

2.3 HARMONISATION, UNIVERSAL ACCEPTANCE AND LANGUAGE

Three further threads emerged. First, the difficulty of harmonisation across Caribbean territories, given differing legal and institutional starting points. Second, a proposal that the principles of universal acceptance be integrated into the data governance discussion. Third, a matter of accessibility: the Framework is written in English, yet the CTU's membership increasingly includes non-English-speaking countries. Participants asked the Secretariat to explore language interpretation and translation for CTU products, events and processes, so that the region's multilingual character is properly served.

3. CONSULTATION TWO — CYBERSECURITY (6 AUGUST 2026)

The second consultation assessed the Framework against the CARICOM Cybersecurity and Cybercrime Action Plan. First drafted in 2006 and updated in November 2025, the CCSCAP is organised around six thematic areas: public awareness, capacity building, technical standards, policy, incident management and regional and international cooperation.

A scoring matrix was developed to assess how fully the Framework addresses each area, on a scale from 0 to 4:

Score	Level of coverage
0	No mention
1	Mentioned
2	Policy assigned
3	Funded plans in place

Score	Level of coverage
4	Implementation underway

The sections below summarise the discussion under each thematic area.

3.1 PUBLIC AWARENESS AND EDUCATION

Participants agreed that awareness work must be multi-pronged and multi-layered, operating at global, regional and national levels simultaneously. The global character of the internet system should not be lost from view and regional sessions should not inadvertently exclude participants.

Regional delivery was widely seen as more efficient than country-by-country effort. ICANN's virtual Domain Name Systems Security Extensions (DNSSEC) training, coordinated through CANTO with Internet Service Providers (ISPs) across multiple territories, was cited as a model that achieved better economies of scale. A train-the-trainers approach at regional level was recommended as a cost-effective way to cascade knowledge into national communities, alongside online delivery such as MOOCs.

A candid note was struck about reach and durability: initiatives often fail to touch ordinary citizens and are frequently not sustained and on that basis the accuracy of a coverage rating of 3 in this area was questioned. Because human error remains the leading cause of breaches, the human element deserves proportionate attention, with targeted and sustained effort directed at vulnerable groups — children, the elderly and persons with disabilities. Civil society groups and Internet Society chapters were identified as instrumental in grassroots delivery.

On institutional roles, it was argued that the CTU has a more pivotal part to play than CANTO in community education, given CANTO's potential conflicts of interest and that the CTU should convene open, pedagogical public forums — not merely awareness campaigns — covering cybersecurity, artificial intelligence, large language models and the environmental and health impacts of large data centres. Practical channels suggested included radio programming and the embedding of cybersecurity awareness in school curricula. The CTU's own history of more than twenty ICT roadshows, which reached beyond typical audiences to the elderly and to youth, was recalled, as was the Caribbean Youth ICT Network; an analogous network for senior citizens was proposed for future consideration.

On funding, participants pointed to the Internet Society Foundation, which offers grants to NGOs and chapters, to ESG-type funds operated by telecommunications providers such as the Liberty Foundation and the Digital Foundation and to European Union mechanisms. The prevailing view was that sustainability must be designed into programmes from the outset: well-designed, comprehensive and durable programmes should be developed before funding is sought, since one-off activities not built for longevity will not achieve lasting impact.

3.2 TECHNICAL STANDARDS

The question posed was whether adoption of standards such as RPKI, DNSSEC, IPv6 and ASPA should be mandated against SMART timelines of, say, eighteen to twenty-four months, or encouraged voluntarily. Organisations including LACNIC, ARIN and ICANN already promote these standards.

The consultation came down clearly in favour of incentivisation over mandate. "Mandatory" was described as a very strong term that raises the unresolved question of who holds authority over ISPs and IT companies; awareness-building that demonstrates the value of these technologies was judged more effective. It was further noted that ISPs do not make decisions on technical merit alone and that telecommunications regulators do not reach every relevant entity — universities operating their own networks being one example.

Capacity building was seen as the practical lever, with the important qualification that it must include structured follow-through to ensure implementation, not merely knowledge acquisition. LACNIC's online MOOC campus was highlighted as cost-effective, though most of its content is in Spanish, with only three MOOCs available in English; the meeting suggested that Caribbean demand for more advanced English-language material on RPKI and DNSSEC be expressed collectively. ARIN indicated that it offers largely funded RPKI and ASPA training at national and regional level and is willing to coordinate sessions tailored to the Caribbean community.

Participants also cautioned that technical standards are not static. Quantum computing threatens current cryptographic methods, including those underpinning RPKI and the United States government has set a 2027 deadline for quantum-resilient measures. The conclusion was that standards should be cited in the Framework as examples rather than as binding requirements and that broader frameworks such as NIST and the ISO 27000 series should also be referenced.

Two structural points closed the discussion. First, the internet ecosystem comprises three layers — telecommunications, protocols and applications — and any discussion of technical standards should specify which layer it addresses. Second, DNS resilience metrics need greater focus. DNS stability sits within ICANN's fourth strategic objective and evidence-based data on the status of DNS implementation across the Caribbean would materially assist decision-making, though the collection methodology remains to be determined. A joint Caribbean–Pacific project was proposed as a possible vehicle.

3.3 POLICY AND REGULATORY FRAMEWORKS

This session addressed which legal instruments should be prioritised for fast-tracked adoption, how multilateral agreements and mutual legal assistance treaties should be standardised and the perennial difficulty of translating regional policy into national action.

Experience suggests that regional harmonisation initiatives stall when the impetus originates outside the countries themselves and HIPCAR was cited as emblematic of this pattern. Two remedies were proposed. First, prioritisation criteria must be explicit and instruments should be considered within the context of the CARICOM Single ICT Space. Second — and identified as the decisive factor — the true economic value to each country of adopting a given instrument must be clearly articulated, since it is that argument which generates political will and secures parliamentary adoption. Participants observed that economic development is an underemphasised dimension of internet governance in the Caribbean relative to other regions and that national sovereignty will always sit in tension with regional approaches, leaving persuasion and demonstrated benefit as the primary tools available.

The awareness of the legal and judicial community was raised as a related gap. The CTU holds a memorandum of understanding with the Caribbean Agency for Justice Solutions and engages with it at least annually on ICT adoption in the judicial sector, but no recent initiative has focused specifically on cybersecurity.

3.4 CAPACITY BUILDING AND CSIRT DEVELOPMENT

Research presented to the consultation found that at least nine Caribbean territories have no national CSIRT. Some territories, including the ABC Islands, rely instead on foreign equivalents such as the Dutch NCSC — arrangements that are not adapted to local contexts and that become points of contention during national-level cyber incidents. The CTU is working with a partner organisation on CSIRT development in the region, details of which are not yet public.

The clearest recommendation of the session was structural: the region should pursue a federated cybersecurity response ecosystem rather than an exclusively centralised model. Under this approach, national CSIRTs provide national coordination while distributed, sector-based capabilities operate across critical sectors, major operators and key institutions. Organisations such as the CTU, ARIN, LACNIC, ICANN and CaribNOG contribute policy coordination, technical capacity and community development, while CARICOM IMPACS provides regional security coordination and mutual assistance. A recent national consultation process in three Caribbean countries indicated a preference for sector-based CSIRTs operating alongside an all-encompassing national CSIRT, on the reasoning that government, manufacturing and healthcare each require tailored incident response.

Information sharing between national teams was identified as a significant obstacle, frequently because the enabling national legislation does not exist. Participants recommended that minimum standards for CSIRTs be defined and that coordination recommendations and model legislation be explored to facilitate CSIRT operations where legal frameworks remain incomplete.

3.5 INCIDENT MANAGEMENT

On operational readiness, the consultation recommended that CSIRT playbooks include, as a minimum, a defined scope, a RACI matrix setting out who is responsible, accountable, consulted and informed, standardised incident response documentation and sign-off by all relevant parties. Standardisation of documentation was emphasised as what allows a process to execute smoothly under pressure.

A second, human-centric dimension of resilience was raised through a concrete example: a citizen unable to fill a prescription because a pharmacy's system was offline. When internet-dependent services fail, ordinary citizens are frequently left without recourse. The consultation therefore proposed that policy oblige service providers and governments to maintain fallback procedures for when automated systems are unavailable, whatever the underlying cause.

A point of drafting discipline accompanied this. Broad language such as "the internet is not working" was cautioned against, since outages are commonly caused by local connectivity, building networks or end-user devices rather than by the internet itself; the more precise formulation, "a service is not available," is both more accurate and more appropriate to a policy document.

Finally, restrictions on social media access for children — implemented in some jurisdictions on safety and mental health grounds — were flagged as a policy area the Caribbean framework may wish to consider.

3.6 REGIONAL AND INTERNATIONAL COOPERATION

Participants asked that the Framework reflect the division of labour between the CTU, which operates at the policy level and CARICOM IMPACS, which operates at the level of implementation and that the interface between regional and national levels be more fully articulated.

On engagement with international organisations, the guidance was that Caribbean participation must be intentional and strategic. The region should define clearly what change its participation is intended to bring and how its activities align with each organisation's strategic goals, recognising that not every Caribbean need can be met by every international body. The recently created ICANN space for Small Island Developing States was cited as an example requiring exactly this clarity of intended outcome. Collaboration with ARIN, LACNIC, ICANN and others is ongoing, but the Framework should offer policy-level guidance on what to pursue and with whom. Adequate and diversified resourcing of regional cooperation was treated as a precondition rather than an afterthought.

3.7 EMERGING AND CONVERGING THREATS

The consultation closed its substantive discussion by looking beyond the CCSCAP matrix. Policy attention, it was argued, tends to settle on visible, above-the-surface challenges, while the greater danger lies in converging forces below the surface — in particular the consolidation of artificial intelligence capability among a small number of companies. For the Caribbean this raises questions of data sovereignty, cultural influence, intellectual capacity and trade. A small number of mega-companies now command more resources than entire countries, which sharply limits the leverage available to small Caribbean governments and AI consolidation compounds that asymmetry.

The consultation's conclusion was that the Framework should address these risks directly and that a forward-looking, future-casting approach to governability is required alongside reactive policy measures. Quantum computing and AI convergence were identified as the two most prominent near-term threats warranting proactive attention.

4. CROSS-CUTTING THEMES

Read together, the two consultations converge on a small number of propositions that cut across subject matter:

- Scope is widening. Both sessions pressed at the boundary of "internet governance," whether through data governance, artificial intelligence, or the environmental footprint of data centres. The proposition that digital governance is the broader container for internet and data governance is now squarely on the table.
- Persuasion over prescription. On technical standards and on legal harmonisation alike, participants preferred incentives, demonstrated value and articulated economic benefit to mandates the region has limited capacity to enforce.
- Sustainability must be designed in, not added later. Programmes should be built for longevity before funding is sought and capacity building should carry structured follow-through to implementation.
- Federation over centralisation. Distributed, sector-based capability coordinated nationally and regionally was preferred to single points of authority — a pattern visible in the CSIRT discussion and echoed in the layered approach to awareness.

- Reach the people the region usually misses. Children, the elderly, persons with disabilities, rural communities, non-technical citizens and non-English-speaking members of the CTU were all raised, in different sessions, as constituencies the region's processes do not yet serve well.
- Sovereignty and dependency are the underlying question. Data processed abroad, foreign CSIRTs responding to national incidents and AI capability concentrated in a handful of firms are three expressions of a single structural concern.
- Precision matters in policy language. Distinguishing service unavailability from internet outage and naming which layer of the ecosystem a standard addresses, were both raised as drafting requirements rather than pedantry.

5. NEXT STEPS

The inputs from both consultations will be compiled and used to prepare proposed amendments to the Caribbean Internet Governance Policy Framework and to structure the agenda of a workshop at the 22nd CIGF. The CCSCAP gap analysis prompted follow-up questionnaire will be circulated to capture input from the wider community beyond those able to attend the sessions.

Stakeholders are invited to take part in the following ways:

- Complete the follow-up cybersecurity questionnaire distributed by the CTU Secretariat: https://form.jotform.com/CTUnion/cigpf-cybersecurity
- Review the digital governance framework published at wdg.org and send comments to the CTU via cigf@ctu.int.
- Submit any further comments or recommendations on cybersecurity, data governance and internet governance to cigf@ctu.int.
- Attend the 22nd Caribbean Internet Governance Forum in Grenada, 24–26 August 2026, in person or online.

APPENDIX A: CCSCAP VS CIGPF EVALUATION TABLE MATRIX

CCSCAP Area	CIGPF Coverage Summary	Gap Rating	Evidence from CIGPF	Consultation Questions
Public Awareness & Education	Strategic emphasis on awareness campaigns, inclusive capacity building, and national IG fora.	3	"Promote Internet awareness building events … Ensure capacity building efforts are appropriately inclusive."	1. Which awareness activities should be regional vs national; 2. What accreditation should regional cyber training carry; 3. How should public awareness campaigns be funded and sustained?
Technical Standards	Endorses IPv6, RPKI, DNSSEC, IXPs and technical fora but lacks binding timelines and compliance metrics.	2	"Promote the deployment of RPKI … minimum of one Internet exchange point (IXP) per country with local DNS root server and IPv6 routing capability."	1. Which three technical standards should be mandated regionally within 24 months; 2. What minimum IXP and DNS resilience metrics should be required per country; 3. How should compliance be monitored and enforced?
Policy & Regulatory Frameworks	Calls for harmonization, model laws, dispute resolution and judicial training; adoption pathways under-specified.	3	"Examine, compare, document and analyze existing national strategies … and make recommendations for regional harmonization."	1. Which legal instruments should be prioritized for fast-track adoption; 2. What incentives or conditional finance would speed national legislative adoption; 3. How should MLATs and mutual assistance be standardized regionally?

Capacity Building	Commits to training, tertiary capacity and technical fora; CSIRT funding and sustainable certification pathways are under-specified.	2	"Organize and/or host appropriate training programs … Equip regional and local tertiary institutions…"	1. What minimum CSIRT staffing and budget should each Member State aim for within 18 months; 2. How should regional training be financed sustainably; 3. What accreditation and career pathways should be created for cyber professionals?
Regional & International Cooperation	Encourages cooperation with ARIN/LACNIC/ICANN and international bodies; lacks formal CSIRT federation terms and pooled governance mechanisms.	2	"Pursue and capitalize on formal cooperation agreements … Ensure coordinated and sustained national and regional approaches … CARICOM IMPACS."	1. What governance model should a regional CSIRT federation adopt; 2. What data-sharing and mutual assistance protocols are acceptable to Member States; 3. How should regional cooperation be resourced and governed?
Incident Management	Mentions of incident response and CSIRT models but lacks playbooks, exercise schedules and dedicated financing lines.	1	"Evaluate and adopt appropriate models for computer security incident response teams (CSIRTs) for cyber-security and attack mitigation."	1. What minimum incident response playbook elements must every national CSIRT have; 2. How often should regional incident response exercises be held and who funds them; 3. What SLAs and reporting timelines should be mandated for national incident reporting?

APPENDIX B: GLOSSARY OF ACRONYMS AND ABBREVIATIONS

Terms are listed as they appear in this report and in the two consultation summaries on which it is based.

Acronym	Meaning
ABC Islands	Aruba, Bonaire and Curaçao — the Dutch Caribbean islands referred to in the CSIRT discussion.
AI	Artificial intelligence.
ARIN	American Registry for Internet Numbers — the regional internet registry serving the United States, Canada and parts of the Caribbean.
ASPA	Autonomous System Provider Authorisation — a routing security mechanism used alongside RPKI.
CAJS	Caribbean Agency for Justice Solutions — the body with which the CTU holds a memorandum of understanding on ICT in the judicial sector.
CANTO	Caribbean Association of National Telecommunication Organizations.
CARICOM	Caribbean Community.
CaribNOG	Caribbean Network Operators Group.
CCSCAP	CARICOM Cybersecurity and Cybercrime Action Plan — first drafted in 2006 and updated in November 2025; the point of departure for the August consultation.
CIGF	Caribbean Internet Governance Forum — the region's primary multi-stakeholder assembly on internet governance.
CSIRT	Computer Security Incident Response Team.
CTU	Caribbean Telecommunications Union.
DNS	Domain Name System.
DNSSEC	Domain Name System Security Extensions — protocols that authenticate DNS responses.
ESG	Environmental, social and governance — used here to describe corporate funds of that type held by telecommunications operators.
EU	European Union.
GDC	Global Digital Compact — adopted in September 2024.
HIPCAR	Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures — the regional project cited as emblematic of stalled harmonisation efforts.
ICANN	Internet Corporation for Assigned Names and Numbers.
ICT	Information and communication technology.
IMPACS	CARICOM Implementation Agency for Crime and Security.

Acronym	Meaning
IPv6	Internet Protocol version 6.
ISO	International Organization for Standardization. The ISO/IEC 27000 series covers information security management.
ISP	Internet service provider.
LACNIC	Latin American and Caribbean Internet Addresses Registry — the regional internet registry serving Latin America and much of the Caribbean.
LLM	Large language model.
MLAT	Mutual legal assistance treaty.
MOOC	Massive open online course.
MOU	Memorandum of understanding.
NCSC	National Cyber Security Centre — in this report, the Netherlands' national centre, on which some Dutch Caribbean territories rely.
NGO	Non-governmental organisation.
NIST	National Institute of Standards and Technology — the United States standards body whose cybersecurity frameworks were recommended for reference.
RACI	Responsible, Accountable, Consulted, Informed — the matrix recommended for assigning roles in an incident response playbook.
RPKI	Resource Public Key Infrastructure — a framework for validating the authority to announce internet routes.
SIDS	Small Island Developing States — the grouping for which ICANN recently created a dedicated space.
SMART	Specific, Measurable, Achievable, Relevant, Time-bound — the criteria proposed for standards adoption timelines.
WDG	World Digital Governance — the organisation whose digital governance framework, published at wdg.org, participants were asked to review.
WSIS	World Summit on the Information Society.
WSIS+20	The twenty-year review of the World Summit on the Information Society; its outcome document was approved in December 2025.

The CTU Secretariat thanks all participants in both consultations for their contributions.