Edit article
View stats
View post

Caribbean CTO Brief
841 subscribers
Subscribed

Issue 10

Irwin Williams
Head of Software Development at iGovTT

January 10, 2026

1. CTU's Q1 ICT Forecast

CTU held its 1st International ICT Forecast and Industry Watch Meeting on 9 January 2026, a virtual session that walked governments through the full Q1 2026 decision calendar: ARIN fellowships, ITU Council Working Groups cluster, TTIGF 2026, CANTO Connect & 42nd AGM, CTU Spectrum Management Task Force, MWC Barcelona, ICANN 85, CITEL Assembly, LACNIC 44/LACNOG and CTU Executive Council 54. It closed with a Global Industry Watch on space sustainability and LEO satellite congestion.

Pilot Watch: Yes – "External Representation Pipeline"

- Nominate a single external-events lead (Digital Ministry / PMO / regulator) to own the CTU calendar and coordinate briefs and debriefs.
- For each Q1 event (TTIGF, CANTO, ITU cluster, Spectrum TF, MWC, ICANN, CITEL, LACNIC), assign named reps and 1–2 clear positions (e.g. AI safeguards at ITU, spectrum/LEO strategy, IXPs, OTT rules).
- Require a 1-page debrief template after each: key decisions, risks, opportunities, and "what we change at home" – and feed that directly into your IDB/CDB/World Bank/EU conversations so donor asks and external positions line up.

Time-sensitive: January–March 2026 – the TTIGF, CANTO, ITU cluster, Spectrum TF, MWC (2–5 March), ICANN 85 (7–12 March) and CITEL Assembly (16–19 March) window is where your 2026–2028 connectivity and governance landscape gets negotiated.

Source: CTU – *1st International ICT Forecast and Industry Watch Meeting* (9 January 2026)

1st International ICT Forecast and Industry Watch Meeting

The CTU's International ICT Forecast and Preparatory Meeting will take place on 9th January 2026, the first for 2026 in a series of quarterly...

Caribbean Telecommunications Union

2. ECLAC "Data Embassies": a new, fundable tool for an old resilience theme

ECLAC's 135-page study, *"Data embassies: an innovative approach to strengthening digital resilience in the Caribbean"* (10 December 2025), proposes that Caribbean states host copies of their most critical government systems and databases (civil registry, ID, tax, treasury, customs, cadastre, justice) in treaty-based "data embassies" abroad, so the state can keep operating when local infrastructure is lost to hurricanes, cyberattacks or connectivity failures. The study is part of the EU–LAC Digital Alliance / Global Gateway and explicitly frames digital continuity for Caribbean PEIDs as a "strategic imperative" and a matter of state survival.

Why it matters: In earlier issues we've talked about cloud, DR, IXPs and sovereignty. This is the first concrete, UN-backed playbook for cross-border continuity – combining law, diplomacy, cloud and DR architecture. It upgrades DR from a "good IT practice" to critical state infrastructure that needs the attention of Finance, AG/Justice, Foreign Affairs, National Security and ICT, not just the CIO.

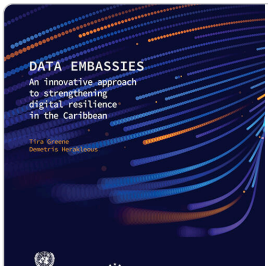
Impact Rating: High – it's the clearest path yet to keeping **IDs, salaries, taxes and trade running** during a national-scale outage.

Pilot Watch: Yes – early-mover, multi-country data embassy pilot

- Form a cross-ministry steering group (Finance, AG/Justice, Foreign Affairs, ICT, National Security/Disaster) to shortlist 1–2 "crown-jewel" systems for data-embassy treatment.
- Commission in 2026 a costed concept note sized for IDB/CDB/World Bank/EU funding: bilateral host vs regional facility vs hybrid, with legal and governance options.
- Through CTU/ECLAC, advocate a regional Data Embassy Working Group mandated to deliver a model treaty + technical templates within 12 months – making this plug-and-play for small states.

Time-sensitive: 2026–2027 – vendors and donors are shaping Caribbean cloud, subsea and LEO offerings now; if data-embassy requirements aren't in the conversation, architectures will harden without our continuity needs built in.

Source: ECLAC – *Data embassies: an innovative approach to strengthening digital resilience in the Caribbean* (10 December 2025)



Data embassies: an innovative approach to strengthening digita...

In view of the accelerating pace of digital transformation, data have become the backbone of state functionality, economic development and...

Economic Commission for Latin America and the Caribbean

3. Jamaica's digital postal codes: location joins identity and payments as core DPI

On 6 January 2026, Jamaica Post and Yassuh Jamaica Limited announced a partnership to develop a digital postal code system assigning a unique, navigable code to every home and building in Jamaica. Minister of Efficiency, Innovation and Digital Transformation Audrey Marks described it as a critical step in modernising public services, improving efficiency and strengthening Jamaica's logistics ecosystem under Vision 2030.

Why it matters: In earlier briefs we treated digital public infrastructure (DPI) mainly through identity and payments, and we've noted existing addressing work in countries like Trinidad and Tobago's S-42-based postal code system and national spatial data infrastructure efforts. Jamaica's initiative is the first new, high-profile "digital postal code" programme in this current wave that is being framed explicitly as national logistics and service-delivery infrastructure, not just a mail project. If Jamaica gets standards, governance and openness right, digital postal codes can become a location rail alongside ID and payments: powering last-mile delivery, e-commerce, ride-hailing, property taxation, disaster response and geospatial planning. For other Caribbean states – including T&T – it sharpens the strategic choice: treat postal/geospatial data as closed operational tooling, or intentionally open it up as shared DPI (standards-aligned, proprietary, or regional). "Do nothing" on that question is no longer neutral.

Impact Rating: High for Jamaica; **Medium–High** as a regional signal.

Time-sensitive: 2026–2027 – as Jamaica designs and tests the system, other states still have leverage to influence standards and governance rather than retrofitting compatibility later.

Sources: Jamaica Observer – "Digital postal codes initiative aims to modernise Jamaica's national delivery system" (6 January 2026)

Digital postal codes initiative aims to modernise Jamaica's national...

KINGSTON, Jamaica — Minister of Efficiency, Innovation and Digital Transformation Audrey Marks has endorsed a landmark partnership...

jamaicaobserver.com

4. Barbados' Trident ID: sequel focused on delivery risk, not design

Barbados has confirmed that 2026 will be a year of acceleration for *Trident ID* and broader public-sector digitisation: more services digitised monthly, expanded cybersecurity investments, and a nationwide sensitisation campaign to address misconceptions about the ID. New Trident ID features are expected by mid-2026, aimed at

smoother access to both public and private-sector services and deeper GovTech modernisation.

Why it matters: We've already treated Barbados in earlier issues as part of the Caribbean eID and GovTech playbook, alongside Jamaica's NIDS and OECS e-ID efforts. This is the sequel: after delays, government is recommitting with new timelines and clearer integration ambitions. The key question is no longer "do we have a digital ID design?" but "will Trident ID show up in real transactions on a visible schedule?" That makes Barbados a live small-state test case for turning ID from a card into an access rail.

Impact Rating: High – success here would create one of the region's clearest proof-points for ID-enabled service delivery in a small-state context, sitting alongside Jamaica's NIDS and emerging OECS e-ID work as a key reference.

Pilot Watch: Yes – anchor it in a public integration roadmap

- Launch a monthly public dashboard (IDs issued, digital logins, services accessed) so citizens and partners can track progress – and so donors see a credible results framework.
- For other states, build this into your donor asks: when talking to IDB/World Bank/EU about ID and GovTech, insist funds be tied to service integration and change management, not just credential production and core platform licences.

Time-sensitive: Mid–late 2026 – if citizens and ecosystem partners don't see Trident ID embedded in key services by year-end, they will keep investing in parallel KYC and manual verification instead.

Source: Biometric Update – "Barbados to expedite digital ID, public sector digitization this year" (5 January 2026)

Barbados to expedite digital ID, public sector digitization this year

Digitizing public services aligns with the digital technology pillar of his ministry which is expected to boost national development and the digital...

Biometric Update

---

5. Dominican Republic / Indotel: online harms, AI and "fake news" hit the regulatory stack

The Dominican Telecommunications Institute (Indotel) has announced that from 2026 it will implement a national strategy to combat digital blackmail, online extortion and the spread of "fake news", working with the high-tech crimes unit (Dicat), National Police and Public Prosecutor. The move responds to the Dominican Republic registering the highest number of digital fraud victims in the Americas in the second half of 2024, and officials explicitly reference AI-manipulated images and content as tools in these crimes.

Why it matters In earlier issues we've built a digital-trust narrative around cyber, data protection, AI risk and platform governance. Indotel's plan is the first explicit "online harms + AI + regulator" bundle in the region. Done well, it can become a model for tackling AI-enabled extortion, deepfake sexual abuse and fraud; done badly, it can turn into a broad

"fake news" mechanism that chills speech and is easily politicised. It underlines that trust infrastructure is legal + technical + governance, not just better SOC tooling.

Impact Rating: High – this will shape how safe and how free Dominican online spaces feel for years.

Pilot Watch: Yes – but only with strong guardrails

- Any Caribbean government considering similar moves should:
- In discussions with security/justice donors (EU, USAID-type, IDB citizen-security windows), position this as a rights-sensitive online harms framework where governance design is a funded deliverable, not an afterthought.

Source: Dominican Today – "Indotel to launch national strategy against digital extortion and fake news in 2026" (8 January 2026)

Indotel to launch national strategy against digital extortion and fake...

Santo Domingo.- Starting in 2026, the Dominican Telecommunications Institute (Indotel), together with other state agencies, will implement a nation...

Dominican Today

6. Mastercard's SME cyber card: financial rails quietly adding security for MSMEs

On 2 December 2025, Mastercard announced from Miami that it has enhanced its SME card offering for Latin America and the Caribbean, integrating cybersecurity tools My Cyber Risk and Identity Theft Protection directly into SME credit cards, with additional digitalisation tools (such as a Digital Presence Optimizer) rolling out across LAC markets in 2026. The suite targets SMEs that increasingly rely on digital payments but lack dedicated cyber capacity.

Why it matters: We've repeatedly flagged that Caribbean MSMEs are digitally exposed and under-served on cyber, even as we push more e-commerce and digital payments – and a lot of that discussion has focused on homegrown and public rails (DCash, JAM-DEX, fast-pay/RTGS upgrades, CARICOM cross-border work). This Mastercard move is a reminder that global card schemes are quietly bundling security features, while the region is still designing its own account-based and real-time systems. Strategically, it only matters if Caribbean banks and MSME agencies treat it as a bridge – something that complements, not crowds out, efforts to embed cyber, fraud analytics and KYC support into local and regional payment infrastructure. On its own, it's just another vendor bundle that can sit buried in a card brochure.

Pilot Watch: Maybe – but only via banks, MSME programmes and national payment councils

- Ask your state bank, development bank and major SME issuers if and when they'll enable these features locally and how they'll be surfaced to MSMEs.
- When building or refreshing MSME and digital-economy projects with IDB/CDB/World Bank, explore whether card-based cyber tools

can complement grants/training instead of developing overlapping tools from scratch.

- As you design domestic and regional fast-payment systems, make sure *your* rails also ship basic cyber/fraud tooling to MSMEs — don't outsource that vision entirely to card schemes.

Time-sensitive: 2026 – issuers are deciding now how to package SME offerings; if Caribbean governments and DFIs don't push for the cyber stack, it may roll out in minimalist form or not at all.

Source: Mastercard Newsroom (Latin America) – "Mastercard unveils SME card with built-in cybersecurity solutions to help small and medium businesses thrive in the digital economy" (2 December 2025)

Mastercard unveils SME card with built-in cybersecurity solutions t...

Mastercard enhanced its credit card value proposition for small and medium-sized enterprises (SMEs) in Latin America and the...

newsroom.mastercard.com

Trendline – From "more portals" to "who owns continuity and trust?"

Across **Issues 1–9**, we tracked AI pilots, GovTech, cloud moves, IXPs, data protection, cyber, and early identity/payment rails. In **Issue 10**, those threads converge into one hard question:

> **Who actually owns digital continuity and trust in your state – and what budget line pays for it?**

- External agenda as a coherent system
- Continuity as national security, not IT hygiene
- DPI as coordinated rails – identity, payments, now location
- Trust infrastructure = law + tech + governance + rails

Verified Future – Trust & Continuity Stack, now with map, tool and test cases

In previous issues we've highlighted digital ID (Barbados and others), cloud and IXPs, cyber and data protection, MSME digitalisation. This week adds three missing pieces:

- A regional map of where decisions get made (CTU Forecast + 2026 ICT Calendar).
- A concrete continuity tool backed by ECLAC and EU–LAC (data embassies).
- Real Caribbean pilots in location DPI (Jamaica), ID adoption (Barbados) and online harms (Dominican Republic), plus a first move to embed cyber into MSME finance (Mastercard).

Together they sketch a Caribbean Trust & Continuity Stack that can actually be built by 2030:

1. Identity Layer – who you are
2. Location Layer – where you are

3. Continuity Layer – how the state survives disruption
4. Safety Layer – how abuse is constrained and SMEs are protected

Caribbean CTO Brief

Building technology from within the Caribbean has unique challenges. Let's navigate them as a community.


Nirvan, Marilyn and 577 connections are subscribed

841 subscribers

✓ Subscribed