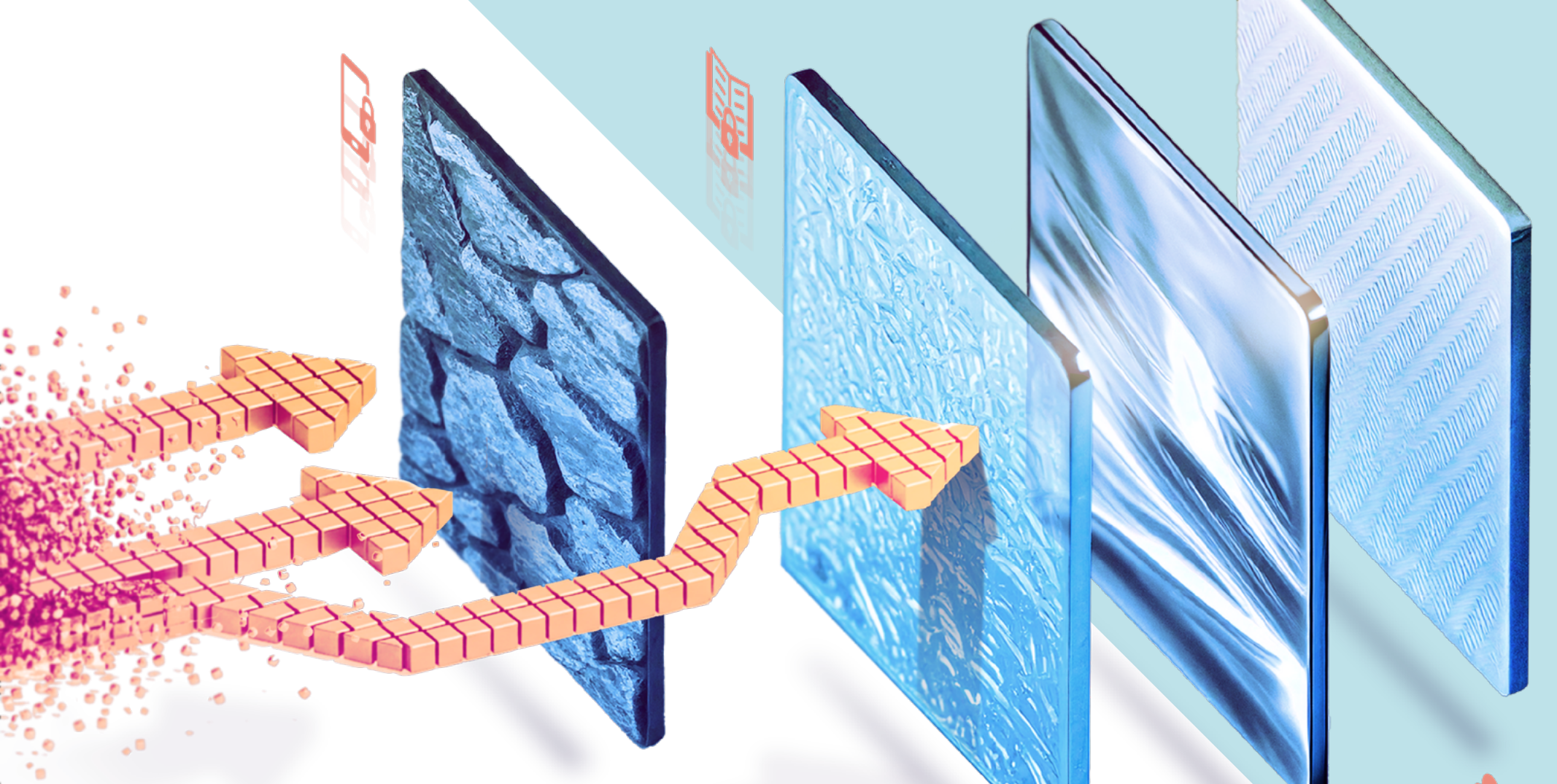


CARICOM CYBER SECURITY AND CYBERCRIME ACTION PLAN

October, 2025

IMPACS

Global Gateway

EXPERTISE FRANCE
GROUPE AFD

EL PACCTO 2.0
EU-LAC Partnership on justice and security

Message from the Executive Director, CARICOM IMPACS

The vision of a secure, prosperous and deeply integrated Caribbean Community (CARICOM) is inextricably linked to our ability to navigate the digital landscape safely. Over the past decade, the rapid acceleration of digital government services, e-commerce and regional data exchange has fundamentally reshaped our economies and societies. This progress, while monumental, has simultaneously exposed our critical infrastructure and citizens to an increasingly sophisticated and pervasive array of transnational cyber threats.

It is against this critical backdrop that I proudly present the **updated CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP).**

More than just a policy directive, the CCSCAP represents our collective strategic commitment to ensuring cyber resilience throughout the CARICOM Region. Its framework is the carefully distilled product of extensive regional consultation, in-depth threat analyses and robust collaboration with our Member States, global partners and technical authorities.

The original framework was foundational, but the threat matrix has evolved dramatically. This updated CCSCAP reflects that reality by embedding a greater focus on operational resilience. Notably, we have strengthened the core pillars and introduced a crucial emphasis on coordinated incident response - the ability to swiftly and effectively recover from a major cyber disruption and maintain the continuity of essential services across the Region.

Furthermore, this document serves as the essential blueprint for the harmonisation of cybercrime legislation and the strategic elevation of our collective technical capacity. The success of this CCSCAP will depend on our shared governance, the swift implementation of national-level frameworks and the pooling of regional and international resources and expertise.

I urge all practitioners, policymakers, law enforcement agencies and technical stakeholders across the Caribbean region to utilise the CCSCAP as the definitive guide for our collective actions over the coming years. The security of our digital future is a shared responsibility; unified implementation of this Action Plan is essential. Its successful implementation will ensure that CARICOM remains not only connected but also robust, resilient, and secure for generations to come.

Michael Jones
Executive Director
CARICOM Implementation Agency for Crime and Security (IMPACS)

Foreword

The update of the CARICOM Cybersecurity and Cybercrime Action Plan (CCSCAP) marks a significant achievement in the partnership between the European Union and CARICOM in advancing cybersecurity and combatting cybercrime. This strategic framework reflects joint efforts to secure the Caribbean's digital future, through collaboration, innovation, and shared commitment.

The CCSCAP, born from consultations initiated in October 2024, is enriched by the expert contributions from the EU Programme of Assistance against Transnational Organized Crime for Latin America and Caribbean (EL PACCTO) and the EU LAC Digital Alliance. This comprehensive plan outlines pathways for public awareness, capacity building, policy frameworks, and incident management, setting the stage for enhanced digital defences in the region over the next five years.

A pivotal aspect of the CCSCAP is the set up of regional responses to online menaces, thus complementing and strengthening national mechanisms for the protection of the Caribbean cyberspace. This is precisely the approach adopted by the European Union and its Member States for the buildup of cyber-resilience in our continent, and I am sure that we will be able to cooperate on the safeguard of digital infrastructures and the combat cybercrime from both sides of the Atlantic Ocean.

The dialogue with the Caribbean is centred on bi-regional collaboration between our regions, and shall not be limited to state actors such as the judiciary and law enforcement agencies. It must also include academia, civil society organizations, and private-sector actors. The CCSCAP places a premium on involving society as a whole in the pursuit of its goals, and accentuates public-private partnership as a foundation for success. The EU Global Gateway, which aims to mobilize investments, can certainly be leveraged to enhance these collaborative efforts and contribute to achieve the priorities listed in the Action Plan.

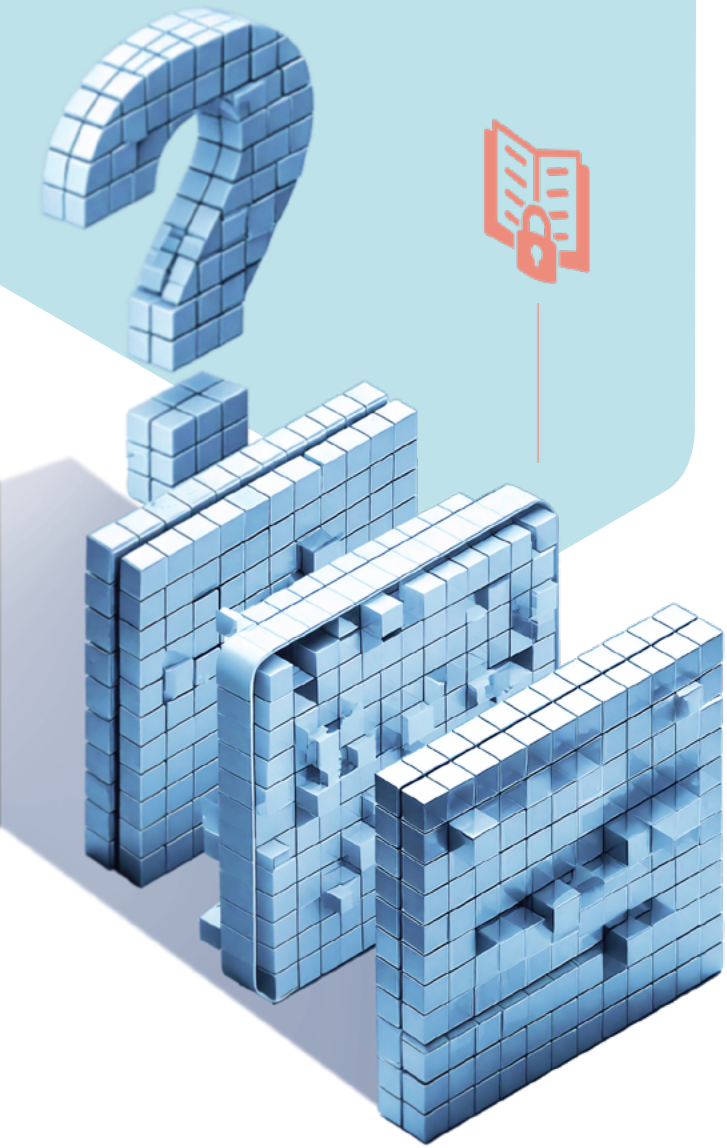
CARICOM and its Member States can rely on a long-term European support for improving standards and raising cyber awareness across the Caribbean. the Latin America and Caribbean Cyber Competence Centre (LAC4), a hub for training and knowledge-exchange, can play a crucial role in this endeavour by providing expertise and specialized training for the different areas of intervention identified in the Action Plan. It can foster an environment that encourages continuous learning and innovation, ensuring that CARICOM nations are well-equipped to address emerging cyber risks and establish resilient digital.

Bilateral cooperation between CARICOM and EU Member States is another key factor for the identification and fostering of rule of law based solutions against online threats. Our countries share a common vision inspired by democratic values, which needs to be transposed in the regulatory framework guaranteeing data protection and digital privacy laws. I am confident that the years to come will bring further synergies in our policy making processes, placing the Caribbean and Europe ahead of the challenges deriving from ever evolving technologies. The updated CCSCAP has been launched, and it is now time to pass to action. I look forward to seeing the tangible implementation of the strategies outlined within the plan, driving meaningful progress in cybersecurity across the Caribbean. By collectively advancing these initiatives, we can ensure a safer digital environment that benefits all.

H.E. Cécile Tassin
Ambassador of the European Union to the Republic of Trinidad and Tobago

TABLE OF CONTENTS

EXECUTIVE SUMMARY



Launched in 2016, the Caribbean Community (CARICOM) Cyber Security and Cybercrime Action Plan (CCSCAP) has been updated in 2025 to confront a rapidly evolving threat landscape. This updated CCSCAP provides a coordinated, forward-looking framework to safeguard the Region's digital infrastructure, strengthen cooperation and align with international best practices. Drawing on extensive stakeholder consultations, it addresses critical gaps – from fragmented laws to under-resourced incident response – through concrete measures and regional coordination. The Plan also introduces an enhanced governance structure and robust monitoring and evaluation to ensure effective execution. Organised around six strategic pillars, the CCSCAP outlines key initiatives to bolster cyber resilience across CARICOM and includes:

Public Awareness & Education:

- Launch region-wide cyber security awareness campaigns targeting youth, seniors, businesses and the general public.
- Integrate cyber security into school curricula and higher education programmes.
- Deliver specialised training workshops for small businesses and vulnerable sectors on practical cyber hygiene measures and mandate cyber awareness training for public officials to foster informed decision-making.

Policy & Regulatory Frameworks:

- Harmonise and strengthen cybercrime laws, electronic evidence and digital forensics legislation and data protection/privacy regulations across Member States.
- Establish clear protocols for mutual legal assistance and extradition in cybercrime cases.
- Implement national cyber security strategies and risk management frameworks to ensure a consistent, robust legal and policy environment Region-wide.

Capacity Building:

- Develop a sustainable regional cyber workforce by establishing a talent pool and training repository.
- Standardise cyber security job profiles, training curricula and certification programmes across CARICOM to professionalise skills.

- Partner with academia and industry to provide hands-on training, internships and public-private initiatives that build local expertise in cyber security and cybercrime investigation.

Technical Standards:

- Adopt minimum cyber security standards and baseline controls for critical networks and services, aligned with internationally recognised frameworks.
- Strengthen protection of critical information infrastructure (energy, telecom, finance, etc.) through mandatory risk assessments, regular vulnerability testing and secure configuration guidelines.
- Enforce secure procurement and supply-chain standards for ICT vendors and promote certification of products to ensure only trusted, secure technologies are deployed**.**

Incident Management:

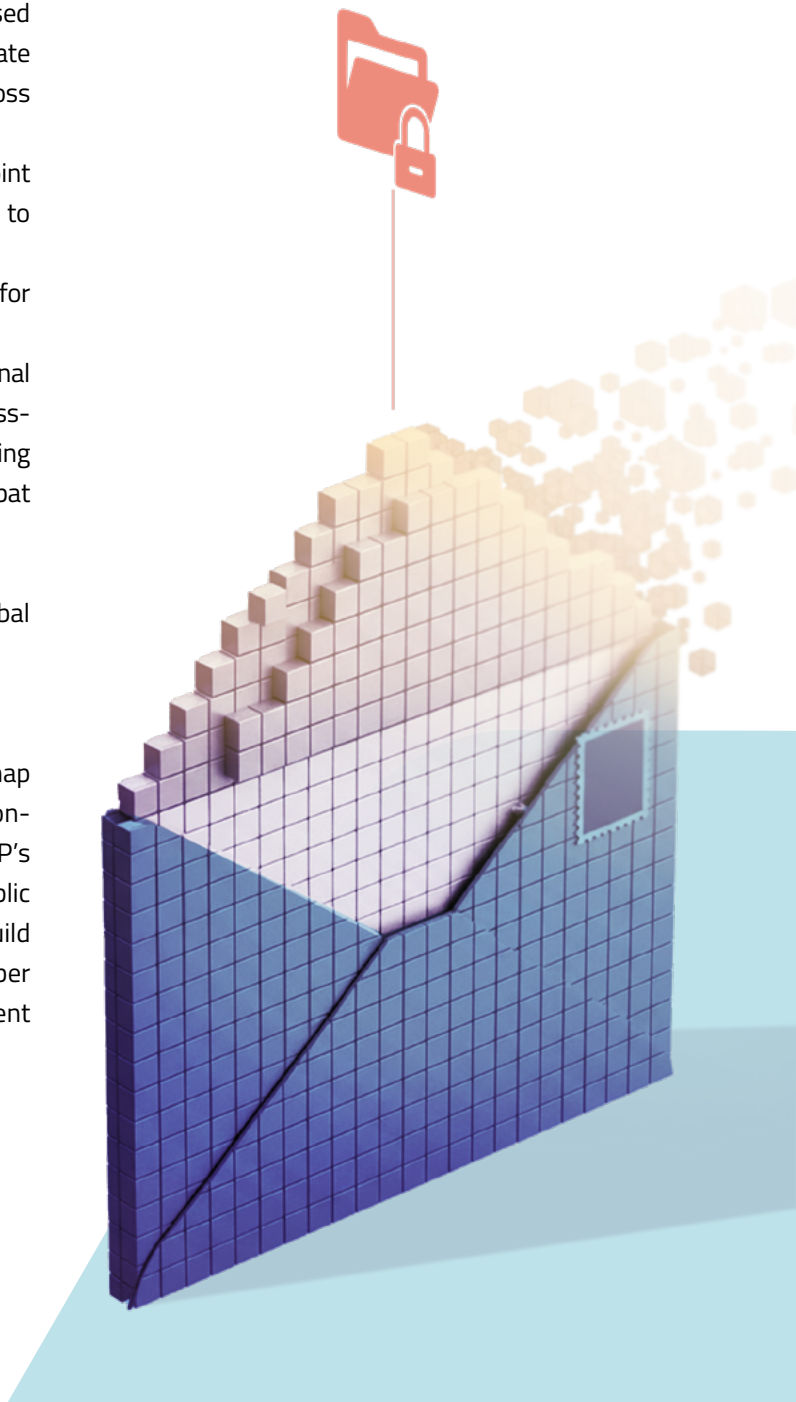
- Improve cyber incident readiness by establishing or enhancing national Computer Security Incident Response Teams (CSIRTs) in every Member State and a coordinated regional incident response framework.
- Implement standardised incident reporting protocols and threat intelligence-sharing mechanisms across CARICOM.
- Conduct regular incident response drills and simulation exercises to test and refine readiness.
- Additionally, develop an incident response support fund or resource mechanism to assist in managing major cyber emergencies.

Regional & International Cooperation:

- Strengthen collective defenses through a proposed Regional Cyber Fusion Centre (RCFC) to coordinate threat intelligence and incident analysis across CARICOM.
- Establish information-sharing networks and joint cyber security exercises among Member States to foster trust and rapid assistance.
- Promote regional public-private partnerships for cyber security innovation and resource sharing.
- Align CARICOM cyber initiatives with international standards and best practices, and deepen cross-border law enforcement collaboration (including shared training and mutual assistance) to combat cybercrime.

The Plan also encourages active participation in global cyber diplomacy and forums to ensure Caribbean interests are represented.

Collectively, these six pillars provide a clear roadmap for action, focusing on practical steps that decision-makers can champion. By implementing the CCSCAP's initiatives, CARICOM states will enhance public cyber awareness, modernise legal frameworks, build technical capacity and improve readiness for cyber threats – thereby creating a more secure and resilient digital Caribbean.

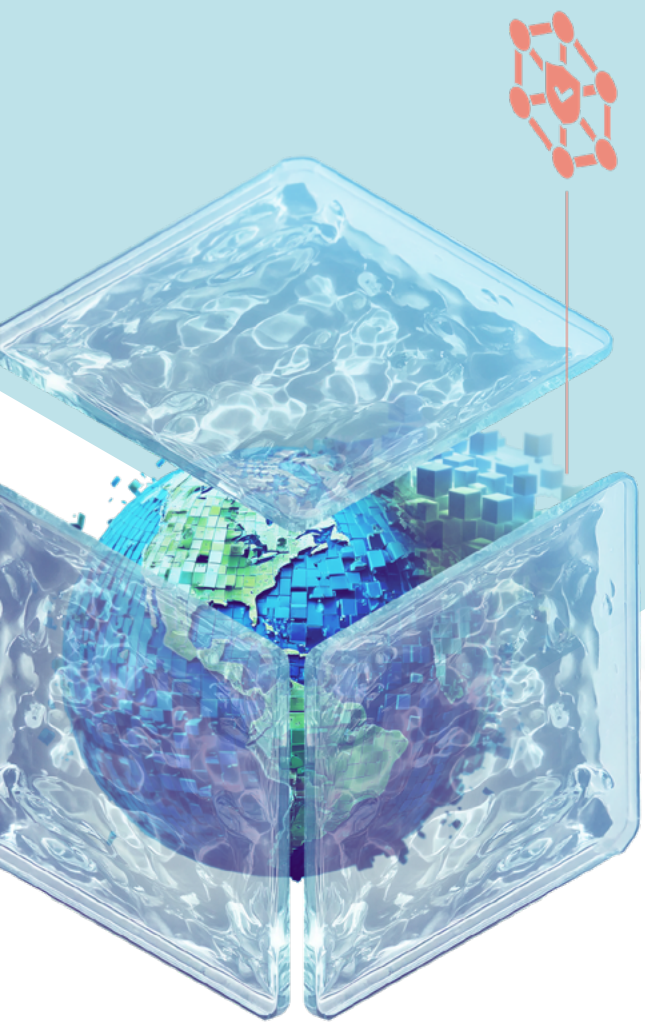


LIST OF ACRONYMS

ACRONYM	Full Name
APT	Advanced Persistent Threat
CARICOM	Caribbean Community
CARICOM IMPACS	CARICOM Implementation Agency for Crime and Security
CBSI	Caribbean Basin Security Initiative
CEH	Certified Ethical Hacker
CFU	Cyber Fusion Unit
CIU	Cybercrime Investigation Unit
CII	Critical Information Infrastructure
CLPSU	Cyber Legislation, Policy & Strategy Unit
CSAM	Child Sexual Abuse Material
CSIRTs	Computer Security Incident Response Teams
C3SC	CARICOM Cybersecurity and Cybercrime Steering Committee
CSU	Cybersecurity Unit
CTU	Caribbean Telecommunication Union
DPIA	Data Protection Impact Assessment
EU CyBERNET	European Union Cybersecurity Network of Expertise
FIRST	Forum of Incident Response and Security Teams
GDPR	General Data Protection Regulation
GFCE	Global Forum on Cyber Expertise
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISAC	Information Sharing and Analysis Centre
ISO	International Organisation for Standardisation
IoT	Internet of Things

ACRONYM	Full Name
LACNIC	Latin American and Caribbean Internet Addresses Registry
LAC4	Latin America and Caribbean Cyber Competence Centre
MLA	Mutual Legal Assistance
M&E	Monitoring and Evaluation
NCPOC	National Cyber Points of Contact
NCO	National Cybersecurity Office
NIST	National Institute of Standards and Technology
OAS CICTE	Inter-American Committee Against Terrorism of the Organisation of American States
OEWG	Open-Ended Working Group
OWASP	Open Web Application Security Project
PPP	Public-Private Partnership
PPT	People, Processes and Technology
PTES	Penetration Testing Execution Standard
RCFC	Regional Cyber Fusion Centre
RIFC	Regional Intelligence Fusion Center
RSS	Regional Security System
SOP	Standard Operating Procedure
SSDF	Secure Software Development Framework
TTX	Tabletop Exercise
UWI	University of the West Indies
UNODC	United Nations Office on Drugs and Crime
VAPT	Vulnerability Assessment and Penetration Testing

BACKGROUND AND CONTEXT



In an increasingly digitised world, cyber resilience has become a foundational pillar not only of national security but of economic competitiveness, social development and public trust. Across the Caribbean, the accelerating pace of digital transformation is deeply reshaping how governments operate, businesses function and citizens engage with society. As the Region advances toward a single ICT space and expands e-government services, its growing digital footprint also increases exposure to cyber threats. From mobile banking and online education to critical infrastructure and public services, the vulnerability of digital systems undermines trust, disrupts development and poses cross-border challenges. However, efforts to secure this digital future remain constrained by fragmented legal frameworks and uneven institutional readiness. Strengthening regional coordination towards cyber resilience and in the fight against cybercrime is therefore essential to safeguarding digital growth, ensuring data protection and unlocking the full potential of the Caribbean's digital economy.

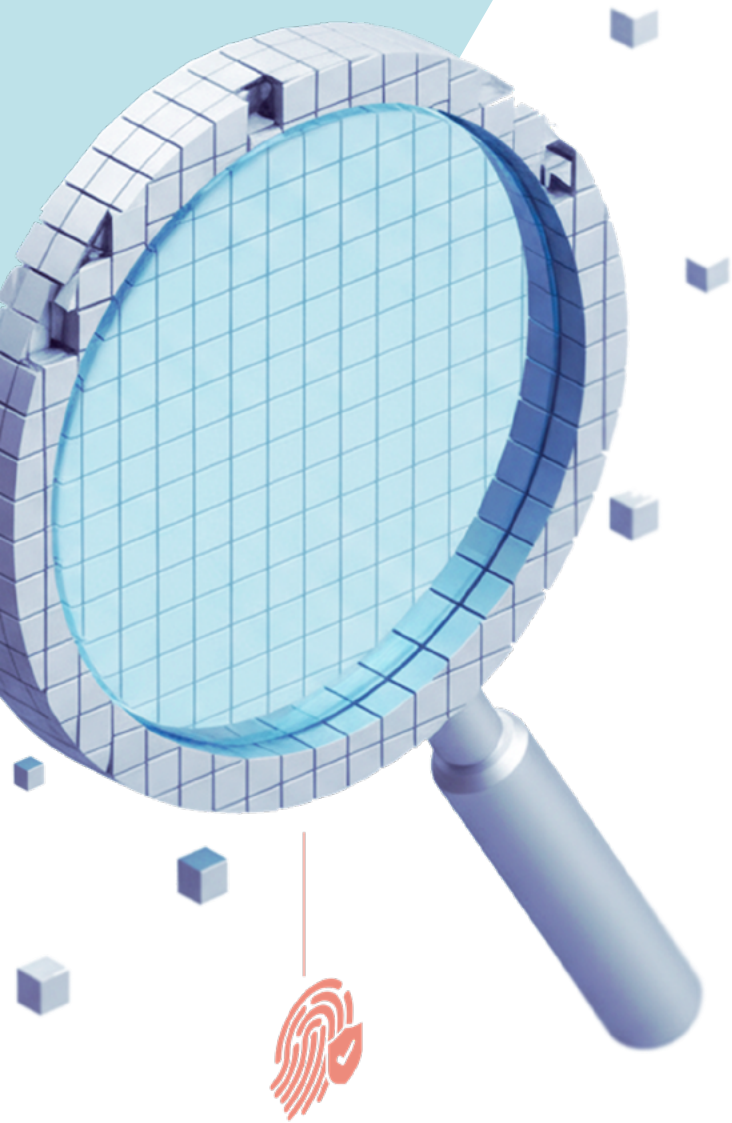
In its 2025 *Global Risks Report*, the World Economic Forum (WEF) highlighted cyber-threats among the top immediate global risks, underscoring the growing significance of cyber security threats in the coming decade. As digital systems underpin more of our critical infrastructure and daily life, the scale and sophistication of cyberattacks have skyrocketed. If cybercrime were measured as a national economy, it would rank as the third largest in the world, just behind the United States and China. According to Cybersecurity Ventures' *Cybersecurity Almanac 2024* and *Boardroom Cybersecurity Report 2024*, global damages from cybercrime are projected to reach approximately US$10.5 trillion annually by 2025, rising from about US$9.5 trillion in 2024 — encompassing losses from ransomware, data breaches, fraud, business disruption, intellectual property theft and incident recovery costs. This staggering figure reflects how deeply cyber threats have become woven into the fabric of our global economy -and underscores the urgent need for stronger cyber security awareness and capacity to detect and respond in a timely manner across every sector.

The CCSCAP emerged in 2016 as a pivotal regional initiative to address the mounting cyber threats facing CARICOM Member States. Acknowledging the

escalating risks posed by cybercrime and vulnerabilities in digital infrastructure, the CCSCAP aimed to establish a harmonised approach across the Caribbean to tackle cyber threats, reinforce cyber resilience and foster international collaboration in an increasingly digital world. Since its inception, however, the landscape has evolved significantly, with rapid technological advancements, digitisation across critical sectors, and new forms of cyber threats underscoring the need for a more comprehensive, updated strategy.

The initial CCSCAP laid the foundation for a regional response to cyber threats through five key priority areas including public awareness, capacity building, technical standards, legal environment, and international cooperation. These pillars enabled significant progress, guiding Member States in securing their digital infrastructure and creating foundational frameworks for combating cybercrime. A review of the previous Plan was conducted, the results of which are attached as Annex I. Among the most notable achievements were:

- The establishment of the CARICOM IMPACS Cyber Fusion Unit (CFU) on 1 February 2024. Housed at the Regional Intelligence Fusion Center (RIFC) under CARICOM IMPACS, the CFU serves as a vital hub for intelligence gathering, threat detection, analysis and proactive defence, dedicated to protecting the Region's critical infrastructure, fostering trust and cooperation and enhancing the overall cyber resilience posture of CARICOM Member States.
- The successful delivery of training programmes for judges and prosecutors in electronic evidence handling and cybercrime investigation, enhancing judicial efficiency. A total 334 law enforcement and judicial officers were trained in cybercrime investigations and cyber security. With a total of 58 persons trained under a train-the-trainers programme.
- The establishment and upgrading of State owned/ law enforcement cyber forensic laboratories in several CARICOM Member States including Antigua and Barbuda, Barbados, Guyana, Jamaica, Trinidad and Tobago and the Regional Security System (RSS) complemented by the adoption of updated cyber forensic software.
- The development and partial dissemination of national cybers security strategies by numerous Member States, increasing overall strategic alignment within the Region.
- The enhancement of a 24/7 network of law enforcement points of contact for cybercrime investigations, bolstering cross-border collaboration and developing informal operational networks for cybercrime investigation and law enforcement.
- Recognition of cyber security and cybercrime within national threat assessments and integration into crisis management frameworks in several States.



However, the assessment also revealed key areas requiring further action:

- The lack of a standardised regional training curriculum for law enforcement, first responders and prosecutors, with training efforts remaining fragmented and donor-dependent.
- The non-establishment of a regional Academy of ICT Essentials for Government Leaders based on UN standards, leaving senior government officials without a consolidated training platform.
- Limited regional collaboration with tertiary institutions, such as UWI, for structured cyber security and cybercrime education programmes.
- Variations in the development and enactment of cybercrime and data protection legislation across Member States, with inconsistent alignment to international best practices.
- A need for enhanced change management to ensure cyber security is integrated into organisational culture, especially within the public sector.
- Incomplete implementation of cyber forensic infrastructure in all Member States, despite progress in key jurisdictions.
- Gaps in the establishment of CSIRTs or dedicated cyber units at national level.
- Fragmented landscape of public awareness initiatives on cyber security risks and best practices.
- Limited international and regional cooperation mechanisms on cyber security and on cybercrime matters.
- The lack of reference to the inclusion of a gender perspective as well as a specific focus on youth and vulnerable groups to promote actions that are inclusive, sustainable and socially responsive.

The CCSCAP's 2025 update builds on these successes while directly integrating the outcomes of in-depth bilateral consultations conducted with nine CARICOM Member States and a representative from Latin America. These engagements revealed implementation challenges and national priorities which are reflected in an expanded and refined set of action points across all pillars. Notably, the updated CCSCAP introduces new activities and funding strategies for CSIRT operations.

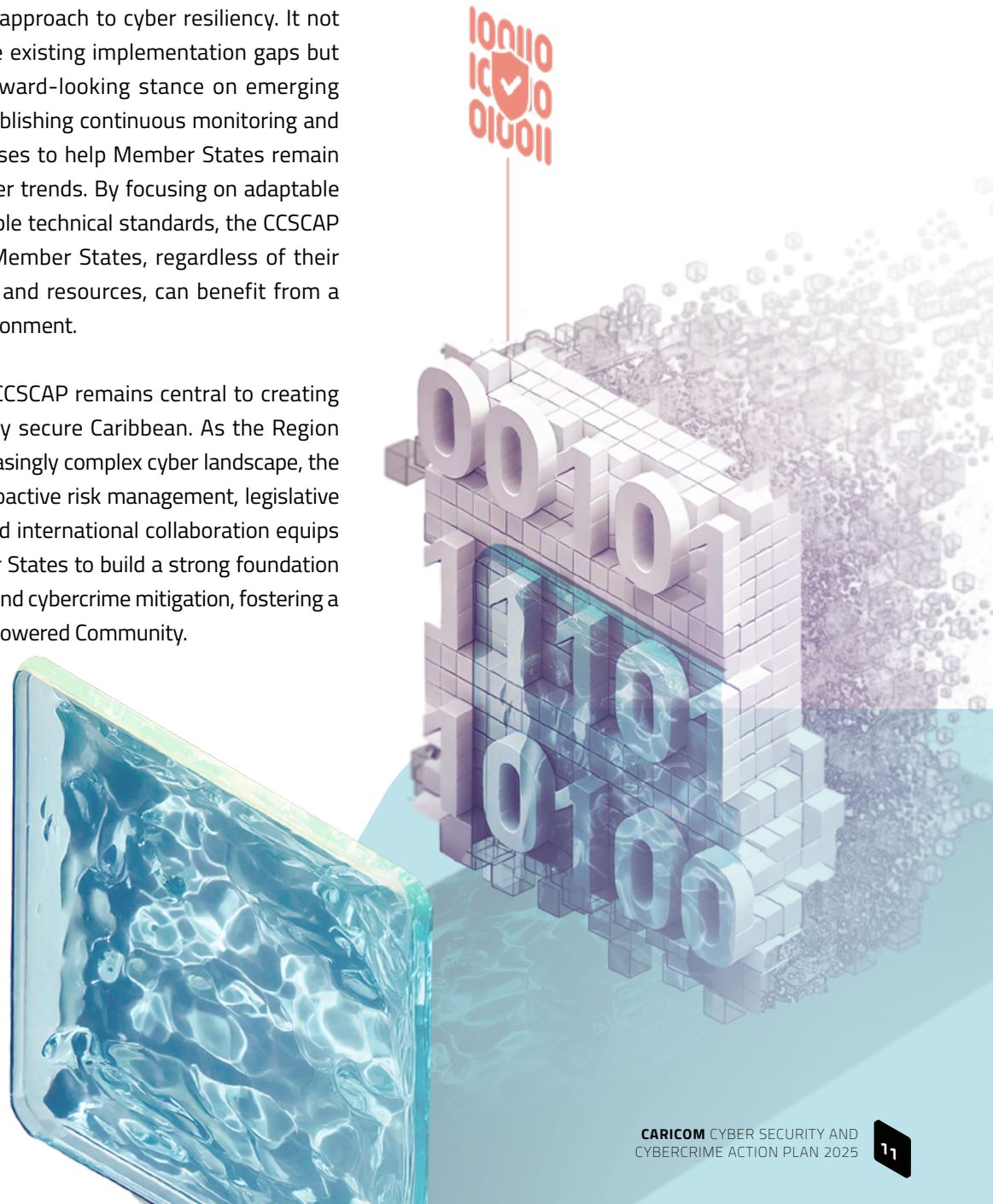
A consultation meeting was also held in Trinidad and Tobago at the CARICOM IMPACS headquarters in October 2024, attended by representatives from CARICOM IMPACS, CARICOM Secretariat, the Commonwealth Secretariat, Caribbean Telecommunication Union (CTU), INTERPOL, RSS, LACNIC, Organization of American States (OAS), consultants from EL PACCTO 2.0 and EU-LAC Digital Alliance, regional CSIRTs, and government stakeholders (Trinidad and Tobago and the Dominican Republic). It resulted in an agreement on the priorities

in this phase of elaboration of the Plan, and were subject to further refinement based on subsequent analysis and in-depth interviews with cyber units from Member States, ensuring that the strategies are both comprehensive and contextually relevant. The main priorities were:

1. **Public Awareness, Education, and Advocacy:** Raising public awareness and promoting education are critical for creating a culture of cyber security and anti-crime.
2. **Capability Development and Capacity Building:** Strengthening organisational capabilities and human resources is essential for addressing the dynamic nature of cyber threats.
3. **Enhancing and Harmonising Technical Standards and Infrastructure:** The Plan underscores the importance of unified technical standards and infrastructure improvements.
4. **Policy, Institutional and Regulatory Framework:** To create a robust and adaptable legal environment.
5. **Cyber Incident Management:** To create a security posture that can anticipate, withstand and recover from a broad spectrum of cyber threats.
6. **Regional and International Cooperation:** Recognising the transnational nature of cyber threats, the Plan prioritises collaboration at regional and global levels.

The revised CCSCAP reflects CARICOM's commitment to a future-proof approach to cyber resiliency. It not only aims to close existing implementation gaps but also adopts a forward-looking stance on emerging technologies, establishing continuous monitoring and evaluation processes to help Member States remain responsive to cyber trends. By focusing on adaptable training and scalable technical standards, the CCSCAP ensures that all Member States, regardless of their unique capacities and resources, can benefit from a secure digital environment.

In summary, the CCSCAP remains central to creating a resilient, digitally secure Caribbean. As the Region confronts an increasingly complex cyber landscape, the Plan's focus on proactive risk management, legislative harmonisation, and international collaboration equips CARICOM Member States to build a strong foundation for cyber security and cybercrime mitigation, fostering a safer, digitally empowered Community.



CURRENT CYBERCRIME AND CYBERSECURITY LANDSCAPE

In the Caribbean, the cyber security landscape reflects a complex matrix of strengths, vulnerabilities, and evolving threats. As CARICOM Member States advance their digital economies and invest in e-governance, they are confronted by increasingly sophisticated cyber threats that target critical infrastructure, public services, financial institutions and private enterprises. The rapid digital adoption across sectors such as healthcare, education and finance has amplified the Region's exposure to cyber risks, highlighting an urgent need for coordinated and robust cyber resiliency measures across the Caribbean.

The Region's threat landscape now encompasses a broad range of cyber incidents, with ransomware, data breaches, phishing, and cyber-enabled fraud being particularly prevalent. Ransomware attacks have become highly disruptive, crippling essential systems and demanding cryptocurrency payments to unlock data. These incidents, which have caused significant operational downtime and financial losses, are particularly concerning in the healthcare sector, where data breaches compromise patient confidentiality and disrupt essential services. Phishing and social engineering tactics also contribute to the rise in cyber-enabled financial crime, targeting financial institutions, e-commerce platforms, and individual consumers. "Pig butchering" scams, which combine romance fraud with financial deception, are on the rise, as are scams aimed at vulnerable populations, such as elderly fraud and tech support scams.

Another growing concern is the use of digital platforms for the distribution and production of child sexual abuse material (CSAM). The ease of access to these networks through streaming services and the use of artificial intelligence (AI) to generate illicit content pose new challenges for authorities, requiring them to adapt their investigative and enforcement capabilities to these evolving criminal dynamics.

Recent advances in AI have amplified both the scale and speed of many of the cyber risks already identified, particularly those linked to disinformation and influence

operations. Threat actors are increasingly automating phishing campaigns, tailoring social-engineering efforts on a population scale, generating convincing deepfakes, and probing systems using AI-assisted discovery. At the same time, defenders can utilise AI for anomaly detection, triage and incident response, with opportunities to integrate AI into existing cyber security systems for faster and more adaptable detection. However, AI is not inherently good, bad or neutral. Its development and deployment require safeguards to prevent bias, misuse and the generation of harmful or misleading content. For CARICOM, these dual-use realities necessitate a balanced approach. Accordingly, societies must strengthen preparedness for AI-enabled attacks (such as deepfakes, influence operations, and automated compromise), support responsible adoption of AI for defence (threat-intelligence enrichment, anomaly detection, incident response), and embed safeguards for transparency, accountability, and ethics in all AI-related initiatives.

The challenges do not stop there; insider threats are an additional concern as trusted personnel, whether intentionally or unintentionally, may expose organisations to cyber risk. Moreover, the use of emerging technologies like AI has introduced new vulnerabilities. While AI can enhance cyber security defences, it is increasingly used by cybercriminals to automate attacks, evade detection and manipulate online behaviour. The rapid adoption of Internet of Things (IoT) devices, from medical equipment to smart home systems, further complicates the landscape, as many of these devices lack adequate security controls, making them prime targets for exploitation. Advanced Persistent Threats (APTs) and supply chain attacks add further complexity, enabling attackers to infiltrate networks and remain undetected for extended periods. These stealthy tactics pose risks not only to intellectual property and critical infrastructure, but also to national and regional sovereignty through cyber espionage activities.

CARICOM Member States' digital infrastructure remains vulnerable due to substantial disparities in state-level cybersecurity readiness: while some States have fully established CSIRTs and enacted data protection and privacy laws, others continue to lag in institutional capacity and regulatory framework maturity (See: *"The State of Data Protection and Privacy Laws in the Caribbean," Corlane Barclay, Jan 2024; and OAS-CIC-TE report "National Cybersecurity Strategies: Lessons Learned,"* 2023). While some States have established CSIRTs and enacted data protection laws, others lag in institutional capacity and regulatory frameworks. This lack of harmonisation – exacerbated by fragmented legal traditions across the Caribbean (common law in most anglophone states vs. civil law in others) – complicates cross-border incident response, weakens regional resilience, and limits CARICOM's ability to combat cyber-incidents effectively. While some countries have updated cybercrime legislation aligned with the Budapest Convention, others lag behind or have gaps in their laws, which criminals eagerly exploit. Strengthening legal convergence and cross-border cooperation is therefore essential to build a more effective and resilient regional response.

Physical threats to digital infrastructure also present a growing concern. The Caribbean's vulnerability to natural disasters, exacerbated by climate change, underscores the importance of resilience planning for ICT infrastructure. Hurricanes, floods, and other environmental events can disrupt power grids, data centres, and communications systems, weakening cyber defences and complicating recovery efforts. Building resilience requires a proactive approach that integrates both physical and digital security, with protocols for backup systems, disaster recovery, and business continuity planning.

Furthermore, CARICOM faces significant challenges in public-private partnerships, regulatory frameworks, capacity building, and incident response and recovery. Public-private partnerships are essential for sharing threat intelligence and resources, yet they remain underdeveloped in some areas. Additionally, there is a need for a comprehensive and harmonised regulatory framework to enforce consistent cyber security standards across Member States. This is not only a technical requirement but also a legal harmonisation imperative – aligning national laws under shared standards (for example, model cybercrime laws reflecting the provisions of the Budapest Convention) is essential to close jurisdictional gaps and enable an effective collective response to cyber threats. Ongoing capacity-building and training programmes are also

vital to equip local professionals with the skills to handle cyber-incidents, and further international cooperation is crucial for enhancing the Region's overall cyber security posture.

The Caribbean's cyber security landscape underscores the necessity for a harmonised, regionally coordinated approach to address shared challenges and vulnerabilities. By prioritising cross-border cooperation, CARICOM Member States can pool resources, share intelligence and develop unified incident response strategies to strengthen collective cyber resilience. This cooperative approach should be supported by comprehensive cyber security legislation, public awareness campaigns and capacity-building programs to enhance digital literacy and skill development across all sectors. CARICOM faces a dynamic and evolving cyber security environment shaped by emerging threats, technological advancements and resource limitations. Addressing these challenges requires a coordinated strategy that strengthens legal frameworks, cultivates local cyber security expertise and promotes a culture of cyber awareness and responsibility throughout the Caribbean. By proactively addressing these vulnerabilities, the updated CCSCAP aims to foster a resilient, secure digital environment that supports economic growth, public safety and regional stability.

As part of the updated CCSCAP, a strategic plan incorporates a public awareness campaign to educate individuals, businesses and institutions on cyber-risks and cybercrimes. These efforts focus on preventing fraud, phishing and exploitation by promoting safe online practices. Another key aspect is public–private collaboration in cybercrime prevention: strengthening cooperation between governments, financial institutions, technology companies, and internet service providers to improve threat intelligence sharing and incident response. Joint training initiatives and real-time data exchange mechanisms will enhance the region's ability to detect and mitigate cyber-threats.

GOVERNANCE STRUCTURE

The effectiveness of the CCSCAP depends on a well-defined governance structure that fosters accountability, encourages cross-border coordination and ensures the sustainable implementation of its initiatives. This Governance Structure section aims to design a comprehensive framework for decision-making, coordination and accountability within the CCSCAP, supporting an integrated approach to cyber security across the Region.

Strategic Objectives

The Governance framework is designed to:

1. Provide strategic leadership and oversight through a regional body that sets direction, priorities.
2. Ensure operational delivery through a dedicated technical centre responsible for daily coordination, capacity development and threat management.
3. Establish independent monitoring and evaluation (M&E) mechanisms that guarantee transparency, objective performance assessment and continuous improvement.
4. Integrate national coordination points to strengthen Member State engagement and streamline information flow.
5. Promote inclusive participation by incorporating perspectives from government, private sector, academia, and civil society.

CARICOM Cyber Security and Cybercrime Steering Committee (C3SC)

The CARICOM Cyber Security and Cybercrime Steering Committee (C3SC) shall serve as the central authority within the governance structure for the CCSCAP, acting as the principal oversight body responsible for strategic direction, setting regional cyber security priorities and ensuring cohesive implementation of action plan initiatives.

Comprising senior representatives[1] from CARICOM Member States alongside several key entities, the C3SC includes a core group of permanent members as follows CARICOM IMPACS, CARICOM Secretariat, the CTU, the

1. Senior representatives may include: Chair/Member of Parliamentary Committees on ICT/Digital Affairs/Security/Intelligence; Ministerial or High Level Policy Makers from Ministries of National Security, Digital Affairs and Attorney Generals

RSS, Grenada and Trinidad and Tobago. Additionally, two rotating CARICOM Member States will serve as non-permanent members. Observers will include the Dominican Republic and development partners.

CARICOM IMPACS will chair the committee, representing the collective CARICOM and serving as the body responsible for CCSCAP implementation. Trinidad and Tobago and Grenada hold permanent positions on the C3SC given their roles in the CARICOM quasi-cabinet overseeing Security and Science and Technology, including Information and Communications, respectively.

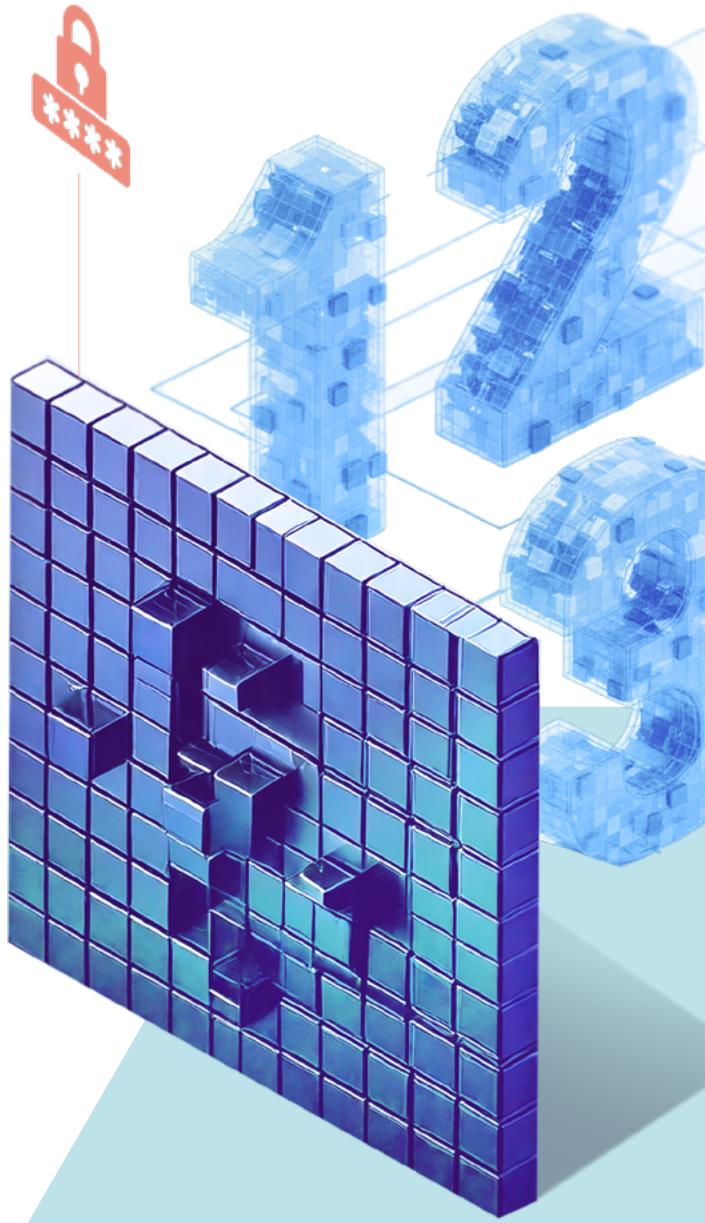
The C3SC does not implement operations directly; rather, it provides oversight and accountability over the CCSCAP, providing guidance to its operationalisation by the Regional Cyber Fusion Centre (RCFC).

The C3SC will convene biannually to review CCSCAP progress, consider M&E findings and adjust strategic direction in response to evolving cyber challenges. This review process will be grounded in data provided by the RCFC, which will track key performance indicators and analyse trends across member states.

Regional Cyber Fusion Centre (RCFC)

The RCFC will evolve from the Cyber Fusion Unit (CFU), which was established by CARICOM IMPACS in February 2024, significantly expanding its operations and mandate. It will serve as the central hub for CARICOM's cyber security cooperation efforts. This centre will work closely with national CSIRTs, law enforcement agencies and critical infrastructure operators, ensuring a cohesive, well-structured approach to managing cyber risks across the Region. It therefore will:

- Coordinate cyber threat intelligence and incident response across Member States.
- Support the delivery of technical training, awareness campaigns and simulation exercises.
- Provide operational oversight of National Cyber Points of Contact (NCPOCs), facilitating harmonised responses and streamlining communication channels between national and regional entities.
- Support law enforcement regional investigations, digital forensics and judicial processes.
- Collect and analyse regional cyber security data and incident trends to support evidence-based policy formulation and strategic planning.



- Assist Member States by offering support in conducting vulnerability assessments and building cyber resilience.
- Provide policy, legislative and compliance support to harmonise frameworks across the Region.
- Manage cross-cutting functions, including public–private partnerships, regional training and research and development.

The RCFC's mandate is focused on execution, coordination and technical delivery. It collects operational data, tracks key performance indicators (KPIs) and submits reports.

The organisational structure of the RCFC is designed to reflect and support its multifaceted mandate. In particular, the operational structure is foreseen to be organised into four main divisions:

- The Cybercrime Investigation Unit (CIU) handles cross-border investigations and coordinating international law enforcement operations, digital forensics, and capacity-building for law enforcement, led by a senior investigator.
- The Cybersecurity Unit (CSU), under the leadership of a national CERT specialist, supports CERT/CSIRT operations, conducts threat monitoring and vulnerability management, and disseminates alerts.
- The Cyber Defence Unit (CDU), coordinated by a defence strategist, assists intelligence and defence agencies in addressing cyberattacks that target State infrastructures, critical operators and public goods.
- Lastly, the Cyber Legislation, Policy & Strategy Unit (CLPSU), headed by a legal and policy expert, is responsible for drafting and harmonising cyber laws, strategic planning, and judicial engagement.

Supporting these core divisions are four cross-cutting enablers including a Regional Cyber Training and Education Centre, a Public–Private Partnership (PPP) Facilitation Hub, a Research & Development Department and a Monitoring, Evaluation & Impact Unit.

Guided by the C3SC and in close coordination with the NCPOCs, the RCFC will provide regular reports on performance indicators, incident data and risk assessments, supporting informed decision-making. As the main contact for international cyber security organisations, the RCFC will cultivate partnerships with global entities, enhancing CARICOM's access to resources, threat intelligence and technical support.

The RCFC will ensure alignment with international best practices and foster partnerships with regional and global cyber security organisations. It will serve as the main liaison to regional and international partners.

Monitoring and Evaluation (M&E)

To guarantee independence and credibility, final M&E functions are housed within CARICOM IMPACS. The RCFC contributes through structured logs, tracer studies, dashboards and KPI tracking, while compliance reviews, evaluations, and performance assessments are conducted at the CARICOM IMPACS. CARICOM IMPACS will submit biannual independent assessments and recommendations to the C3SC.

Key M&E functions will include:

- Developing a unified performance and impact framework
- Leading assessments, tracer studies and programme audits
- Harmonising regional indicators with national focal points
- Producing annual reports on the effectiveness of the RCFC

Examples of M&E indicators - aligned with Organisation for Economic Co-operation and Development's (OECD) Development Assistance Committee (DAC) and Results Based Management (RBM) methodologies - will range from impact metrics (e.g., reduction in successful cross-border cyberattacks), to operational outputs (e.g., number of regional threat alerts), to learning outcomes (e.g., percentage of interventions improved via M&E feedback). To support this framework, diverse data collection methods will be used, including structured logs, scorecards, user surveys, live dashboards and tracer studies.

A sustainable funding and resource allocation mechanism might be considered as integral to the RCFC, to support Member States with the financial and technical resources needed to implement CCSCAP effectively. To this extent, CARICOM may consider establishing a Cyber Security Fund, supported by contributions from Member States, international grants and partnerships with the private sector. This fund will cover the RCFC's operational costs, support training programs, incident response and capacity-building initiatives. Allocation of these resources will prioritise Member States with limited resources, high-risk critical infrastructure, or significant capability gaps, with day-to-day financial management handled by the RCFC. To reinforce sustainability, the RCFC will pursue partnerships with international organisations, development agencies and technology firms that can contribute to the Region's cyber security resilience.

To ensure compliance with CCSCAP's guidelines, standards, and protocols, the RCFC will also implement a policy and compliance oversight mechanism in collaboration with National Cyber Security Officers (NCOs). Annual compliance assessments will analyse each Member State's adherence to cyber security standards, incident reporting protocols and risk management practices. Compliance reports will be submitted to the C3SC, outlining achievements, gaps and recommendations.

Member States will receive customised guidance to address compliance issues. This oversight mechanism will reinforce CARICOM's commitment to a unified cyber security stance, where each member state plays its role in protecting the Region.

Public accountability and transparency are essential for building trust in CARICOM's cyber security initiatives. The RCFC's governance structure shall include provisions for public reporting on CCSCAP progress through annual reports that highlight achievements, challenges and future goals. These reports will be publicly accessible, allowing citizens, businesses and civil society organisations to understand CARICOM's efforts to secure digital infrastructure and personal data. Additionally, the RCFC will host public forums, webinars and stakeholder consultations each year to gather feedback from diverse groups, ensuring that the CCSCAP aligns with community needs and expectations. This engagement will foster a culture of cyber awareness and public involvement in cyber security efforts.

In the event of significant cyber incidents, the RCFC's crisis management and emergency response coordination function will be activated to address large-scale incidents, such as ransomware attacks on critical infrastructure or cross-border data breaches.

Working alongside national CSIRTs and NCOs, the RCFC will coordinate response actions, deploy resources and maintain communication with the public and international partners to ensure a swift, effective response. This crisis management function includes a clear escalation protocol, designated emergency contacts within each Member State, and pre-established communication channels with key international allies, such as the International Criminal Police Organization (INTERPOL), the OAS, and global cyber security providers.

The RCFC will conduct annual crisis simulation exercises to ensure that all stakeholders are prepared to act collaboratively and follow established response protocols, strengthening the Region's resilience to cyber incidents.

National Cybersecurity Offices (NCOs)

Each CARICOM Member State will establish a National Cybersecurity Office (NCO) – or designate an existing body to serve this function – responsible for implementing CCSCAP activities at the national level and coordinating with the RCFC. Given resource constraints, this may be realized as a small, dedicated cyber security desk or unit within an appropriate agency, rather than a large stand-alone office. The NCO (or designated entity) will act as the main liaison between the national government and the RCFC, coordinating activities such as incident response, public awareness campaigns, training and capacity building related actions, and legal framework development within its jurisdiction.

The primary function of NCOs is to act as the focal point for coordinating national cyber security policy and strategic planning, serving as the interface between national stakeholders and regional mechanisms. NCOs are also tasked with supporting incident response efforts and ensuring the effective operation of national CSIRTs, contributing to a timely and coordinated handling of cyber threats. Furthermore, NCOs are responsible for leading public awareness and education campaigns, aiming to enhance cyber security literacy across society and foster a culture of digital safety. Another core function includes facilitating the collection of national cyber security data, which feeds into regional monitoring efforts led by the RCFC. NCOs will also facilitate the conduction of cyber capacity building in the country, providing a channel between the interested national entities and the organisation/ donor responsible for such activities. Lastly, NCOs are charged with ensuring compliance with the obligations set out in the CCSCAP, aligning national activities with regional goals and standards. To strengthen this coordination, each NCO is required to designate two NCPOCs), who serve as the country's official liaisons with the RCFC.

National Cyber Points of Contact (NCPOCs)

The National Cyber Points of Contact (NCPOCs) are senior officials nominated by each Member State to maintain direct communication with the RCFC and ensure coordination between national and regional cyber security structures. Each Member State should designate a primary and a secondary NCPOC. Their responsibilities include providing real-time threat intelligence and incident reporting to the RCFC, as well as coordinating cross-sector cyber security initiatives at the national level. In addition, NCPOCs are expected to facilitate national participation in regional training and simulation exercises and to support the compliance review and reporting framework of the CCSCAP. Importantly, they also play a key role in establishing and leading a national community of cyber security professionals, fostering collaboration across public and private sectors. NCPOCs must map and share key information to provide status updates on national and international cyber projects and initiatives, collect data on incidents, relevant criminal cases, and lessons learned, and identify national resources and technical expertise to support both national and regional cyber security efforts. Through these combined functions, NCPOCs ensure a cohesive, informed, and responsive cybersecurity governance environment that is aligned with regional objectives.

STRATEGIC OBJECTIVES AND PRIORITY AREAS

In response to the increasing complexities of cyber threats, CARICOM has outlined six strategic priority areas within the CCSCAP to guide member states in developing a unified and resilient cybersecurity approach as follows:

1. Public Awareness, Education and Advocacy
2. Policy, institutional and regulatory frameworks
3. Capability development and capacity building
4. Technology and standards for resilient digital infrastructures and services
5. Incident Management
6. Regional and International cooperation

These areas address the fundamental aspects of a comprehensive cyber security strategy. Each priority area is designed to strengthen CARICOM's cyber security posture through tailored initiatives that meet the diverse needs of its Member States, from establishing a culture of cyber awareness to enhancing the Region's capacity to manage, respond to and recover from cyber incidents.

By focusing on these strategic objectives, CARICOM aims to build a robust cyber security ecosystem that enables a safe digital environment for economic growth, public safety and regional stability.

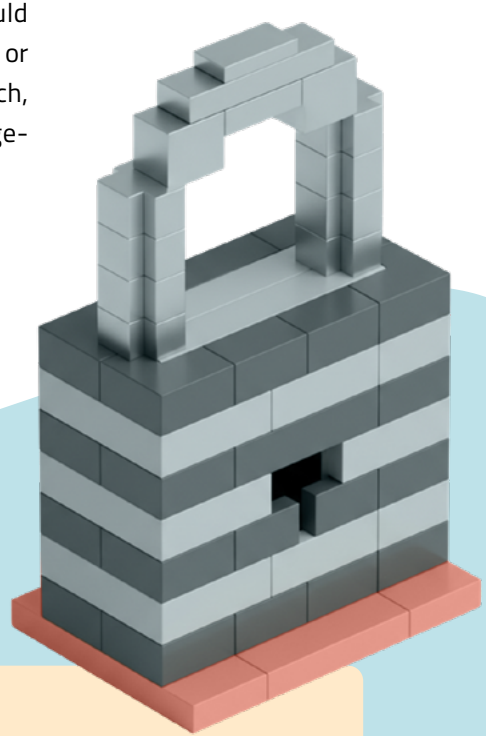
The CCSCAP's priority areas are interlinked, promoting not only the development of individual capacities within Member States but also fostering cooperation across borders. This collaborative approach is essential for CARICOM to effectively address emerging cyber threats, mitigate risks and ensure a secure, digitally empowered Caribbean.

Public Awareness, Education and Advocacy

An effective cyber security strategy relies on a well-informed and vigilant public, capable of identifying risks, practicing safe online behaviours and responding to cyber threats appropriately. Within CARICOM,

varying levels of digital literacy and awareness of cyber security best practices have left individuals, businesses and institutions vulnerable to cyber threats such as phishing, social engineering and ransomware. This disparity is particularly pronounced in rural areas and among smaller businesses, which often lack the resources and expertise to implement adequate cyber security measures.

Consequently, the CCSCAP prioritises Public Awareness, Education, and Advocacy as cornerstones of its comprehensive approach, targeting diverse audience groups and promoting a sustained culture of cyber awareness across the Caribbean. Implementation will emphasise inclusivity, recognising that within the heterogeneous regional population, there are homogenous sub-groups with intrinsically higher levels of risk, as identified through available data. At the same time, safeguards are needed to protect citizens from potential biases in data collection that could result in policies or programmes that lack flexibility or inadvertently disadvantage specific groups. As such, all CCSCAP actions will be gender-responsive, age-sensitive, and accessible. Implementers will:



- Collect sex, age, disability and location-disaggregated data across awareness, training and incident reporting
- Set participation targets in training and scholarships (e.g., ≥40% women and ≥20% youth as a minimum where feasible)
- Ensure accessible materials (plain language, captions, screen-reader friendly)
- Integrate safety-by-design content (e.g., online GBV/ technology-facilitated abuse prevention and referral pathways)
- Align national initiatives with international workforce and gender programmes and regional trainings to expand reach and consistency.

Strategic Objectives

The primary objective of the Public Awareness, Education and Advocacy pillar is to create a resilient cyber ecosystem by fostering a region-wide understanding of cyber security practices and the risks posed by the digital environment. This effort seeks to achieve two key outcomes:

A digitally literate population capable of recognising and mitigating common cyber threats; and

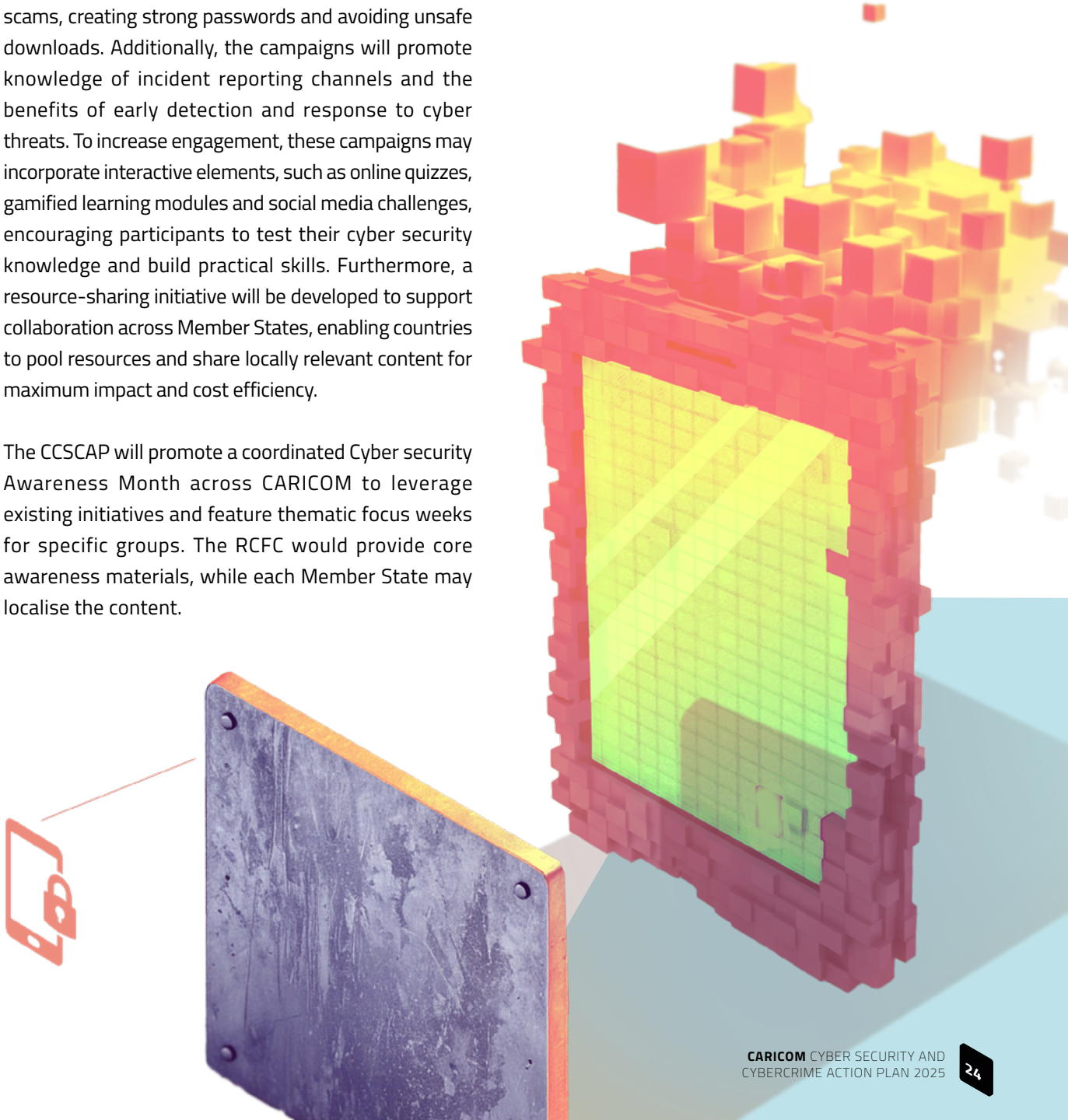
A supportive culture that encourages safe online practices and proactive reporting of cyber incidents.

Public Awareness Campaigns

Building on previous sensitisation campaigns undertaken by CARICOM IMPACS with the support of the Caribbean Basin Security Initiative (CBSI) programme with parliamentarians, high level government officials, law enforcement and the public and training, Member States should establish a series of public awareness campaigns that target different demographic groups, including youth, elderly, and small and medium-sized enterprises (SMEs). Development of tailored public awareness campaigns that are co-produced with national stakeholders could be considered, allowing for country-specific cultural adaptation.

These campaigns will utilise multiple media platforms, from traditional channels like radio and television to social media and mobile applications, to maximise reach and engagement. Messaging will focus on basic cyber security practices, such as recognising phishing scams, creating strong passwords and avoiding unsafe downloads. Additionally, the campaigns will promote knowledge of incident reporting channels and the benefits of early detection and response to cyber threats. To increase engagement, these campaigns may incorporate interactive elements, such as online quizzes, gamified learning modules and social media challenges, encouraging participants to test their cyber security knowledge and build practical skills. Furthermore, a resource-sharing initiative will be developed to support collaboration across Member States, enabling countries to pool resources and share locally relevant content for maximum impact and cost efficiency.

The CCSCAP will promote a coordinated Cyber security Awareness Month across CARICOM to leverage existing initiatives and feature thematic focus weeks for specific groups. The RCFC would provide core awareness materials, while each Member State may localise the content.



Educational iInitiatives in schools and universities

Embedding cyber security education within the formal education system is critical to building a future-ready workforce that prioritises security from an early age. The CCSCAP proposes the introduction of cyber security modules into school curricula, targeting students at both primary and secondary levels. These modules will be designed to teach safe online behaviour, including recognising cyberbullying, protecting personal information and securing devices used for schoolwork. Teaching materials will be made available in both print and digital formats, ensuring accessibility for schools with varying technological capabilities.

At the tertiary level, universities and colleges across CARICOM will establish cyber security-focused courses and degree programmes. To support the rapid development of these programmes, partnerships should be formed with established institutions offering cyber security education, providing curriculum support, access to guest lectures, and guidance on accreditation standards.

Additionally, scholarship schemes and internships in cyber security will be developed, incentivising students to pursue careers in field and contribute to the Region's growing need for cyber expertise. To this end, RCFC and NCOs should be encouraged to actively promote partnerships between academia and industry leaders, to leverage existing expertise and accelerate the development of local capacity, also through the establishment of cyber security degree programmes, research initiatives, and internships fostering an environment of innovation and knowledge sharing. These programmes will include both theoretical and practical components, ensuring graduates are well-equipped to tackle real-world cyber security challenges. Additionally, partnerships with technology companies, especially those in cyber security, can lead to opportunities for on-the-job training and exposure to cutting-edge technologies. Industry partnerships will also be instrumental in delivering up-to-date training on emerging threats, such as artificial intelligence-based attacks and advanced persistent threats (APTs). Leveraging these partnerships will allow CARICOM to stay at the forefront of global cyber security developments and continuously refine its capacity-building efforts in line with new threats and technological advancements.

Workshops and training for SMEs and vulnerable sectors

Small businesses and vulnerable sectors, such as healthcare and finance, are increasingly targeted by cybercriminals due to gaps in security practices. The CCSCAP proposes that these vulnerabilities be addressed by **offering cyber security workshops tailored specifically for SMEs and sectors handling sensitive information.** These workshops will focus on practical, easily implementable measures, such as securing online transactions, protecting customer data and establishing incident response protocols.

Recognising that time and cost constraints may hinder participation, the CCSCAP considers the exploration of partnerships with chambers of commerce, industry associations, and local authorities within Member States to facilitate convenient, affordable training options. For remote or underserved areas, **online training sessions** and recorded webinars will be made available to ensure accessibility.

A **certification programme** will also be developed, allowing businesses to showcase their participation and commitment to cyber security, thus also providing a competitive leverage in markets that increasingly value data privacy.

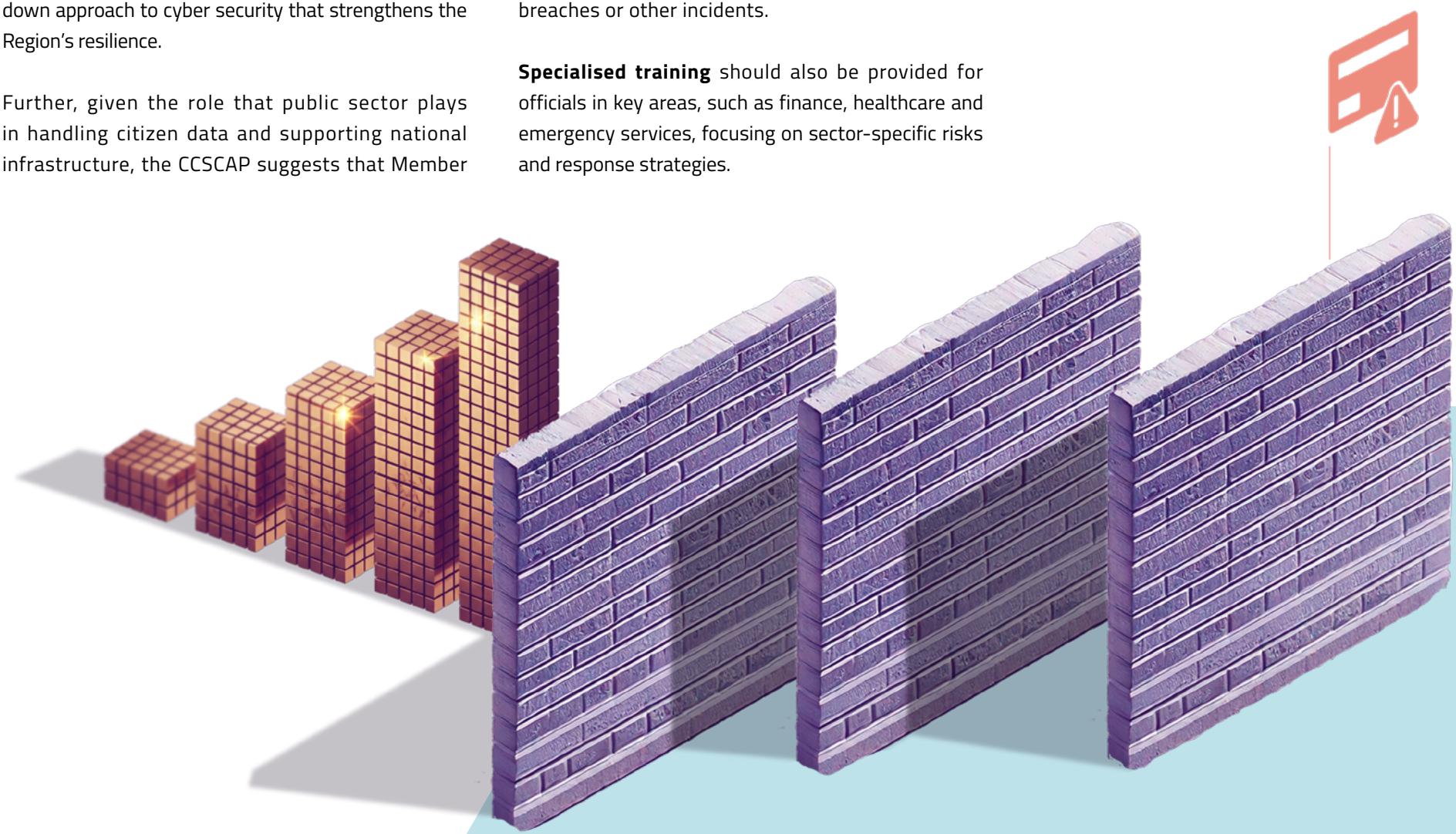
Cyber security awareness for public sector and decision makers

Recognising that effective cyber security is driven by informed decision-making, a dedicated initiative for **cyber security awareness training for senior government officials, policy-makers, and executives within both public and private sectors** is recommended. This training will provide decision-makers with a foundational understanding of cyber security principles, emerging threats, and risk management strategies, ensuring they can make informed policy and investment decisions to support national cyber security objectives.

These training sessions will cover high-level topics, including cyber security governance, data protection regulations and the impact of emerging technologies on cyber risk. By enhancing the cyber security literacy of those at the helm of policy and resource allocation, CARICOM Member States can drive a strategic, top-down approach to cyber security that strengthens the Region's resilience.

Further, given the role that public sector plays in handling citizen data and supporting national infrastructure, the CCSCAP suggests that Member States mandate that all public sector employees, from administrative staff to executives, undergo **mandatory cyber hygiene training.** This training, which should be periodically updated, will cover the fundamentals of securing government devices, recognise suspicious activity and respond to data breaches or other incidents.

Specialised training should also be provided for officials in key areas, such as finance, healthcare and emergency services, focusing on sector-specific risks and response strategies.



Summary of proposed actions in the domain of Public Awareness, Education and Advocacy and Key Performance Indicators

Objectives	Activities	Performance Indicators	1-2 years	2-3 years	3- 5 years
1.Public awareness planning as a component of the National Cyber Strategy with differentiated population groups based on age, gender, profession, risks and type of crime.	1.1. Development, publication and dissemination of a public awareness strategic plan.	1.1.1.Publication of a strategic plan on public awareness	X		
	1.2. Dissemination of public awareness campaign.	1.2.1. To develop at least, two public campaigns on cyber issues annually	X		
2-Awareness raising amongst senior officials, ministers, parliamentarians and policy makers on the issues of cyber security and cybercrime and the importance of policy and legislation.	2.1. Conduct regional awareness raising sessions targeting senior officials, ministers, parliamentarians and policy makers.	2.1.1. Delivery of at least one activity per year for every group.	X	X	X
3.Awareness raising and good practices in ICT usage among schoolchildren.	3.1. Promote agreements with local institutions for the creation and dissemination of public awareness campaigns in primary and secondary schools to encourage good practices in ICT usage.	3.1.1. Development of at least one program to be delivered at schools.	X		
		3.1.2. At least, two agreements with local institutions to include good practice on ICT usage and cybercrime prevention.		X	
		3.1.3. Development of model curricula and revision of national education policies to incorporate cyber security.		X	
4. Comprehensive cybersecurity media campaign for all sectors of society.	4.1. Partnership with traditional and digital media to promote safe digital habits and cybercrime reporting.	4.1.1. Media campaigns launched in 90% of Member States; measurable increase in public cyber literacy.	X		
5. Reducing the cost of awareness campaigns	5.1. Developing a repository of campaigns to be shared among countries, in order to exploit economies of scale.	5.1.1. Establishment of a platform to be used as a central repository for cyber awareness campaigns.	X		
6. Establishment of a regional cybersecurity awareness month	6.1.1. Coordination of annual cyber security month with thematic activities (SMEs, students, public sector).	6.1.1. Regional Cybersecurity Awareness Month launched; 15+ national activities held annually.	X		

Capability Development and Capacity Building

To establish a resilient cyber security ecosystem across CARICOM, capability development and capacity building are essential components. The growing sophistication of cyber threats demands that Member States develop a skilled and capable workforce equipped to address a wide range of cyber incidents, from basic network intrusions to complex, multi-layered attacks on critical infrastructure, both from the technical and procedural sides and from the criminal justice action that is implied in the commission of illegal conducts.

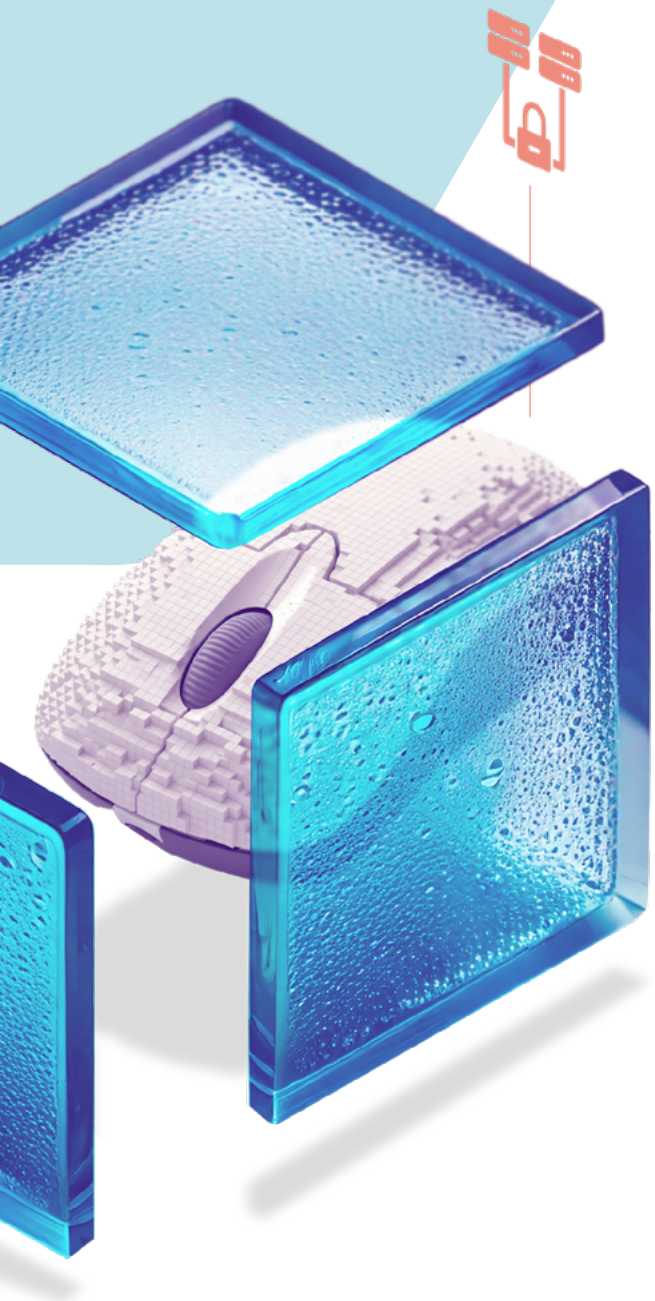
This sub-area of the CCSCAP is dedicated to enhancing technical skills, establishing standardised training frameworks and fostering a culture of continuous learning and knowledge sharing within the Region. By investing in cyber security capabilities, CARICOM aims to equip its workforce with the expertise required to detect, prevent, respond to, and recover from cyber threats, thereby strengthening the Region's overall cyber resilience.

Strategic Objectives

The primary objective of the capability development and capacity building initiative is to create a sustainable and adaptable cyber security and cybercrime workforce.

This workforce will be characterised by a high level of technical and legal proficiency, cross-sector knowledge and a robust understanding of international standards and frameworks. CARICOM's approach to capability building emphasises five core outcomes:

1. Ensuring the most effective implementation of international cyber security and cybercrime capacity building initiative in the Region
2. Establishing a regional cyber security and cybercrime talent pipeline
3. Standardising training programmes across member states
4. Fostering public-private partnerships to enhance local capacities, including with academia and private sector stakeholders
5. Promoting practical, hands-on experience for cyber security professionals and cybercrime practitioners



Effective implementation of international cyber security and cybercrime capacity buildinginitiative in the Region

The CCSCAP encourages the adoption of a regional approach to the implementation of international cyber capacity building initiatives in the Region by connecting the available resources and expertise to the needs identified at national level.

CARICOM could support this action by participating to the mapping and maintenance of a **repository of the cyber capacity projects implemented in the Region, and matching individual needs for cyber capacities to offers of support from the international community.** Such activity is expected to improve the efficiency of the cyber capacity building efforts by avoiding duplication and blind spots and it could further serve as a platform for high-level discussion of the cyber capacity building needs in the Region.

Regional cyber security and cybercrime expert pool

A central initiative under this sub-area is the **development of a regional cyber security and cybercrime expert pool,** composed of cross-sectoral specialists in fields such as network security, digital forensics, cyber intelligence, threat response, cybercrime legal framework, cyber security policies and governance and cyber risk management. This expert pool will serve as a shared on-demand resource for specialised skills and also play a key role in cataloguing and promoting regional talent. A maintained directory of Caribbean cyber security experts and their specialties will ensure visibility of local expertise and facilitate their deployment as trainers, consultants or mentors across the Region.

The use of this pool will also be feasible in the identification of **trainers and consultants.** To maintain a high standard, professionals within this pool will be subject to rigorous validation processes, with periodic updating of profiles to ensure their skills remain relevant and current. While Member States will be encouraged to contribute experts to this pool, with a commitment to continual training and professional development, a facility for voluntary enrolment by experts not affiliated with the public sector will be developed. Consideration should be given at a later stage whether to include in this pool also selected experts not coming from the Region.

The expert pool will also play a role in **knowledge transfer across CARICOM,** facilitating mentorship programmes where seasoned professionals may provide guidance to less experienced counterparts. This collaborative model will promote the sharing of best practices, enabling a consistent standard of cybersecurity expertise throughout the Region.

Standardised Cyber Security and Cybercrime Profiles, Training and Certification Programmes

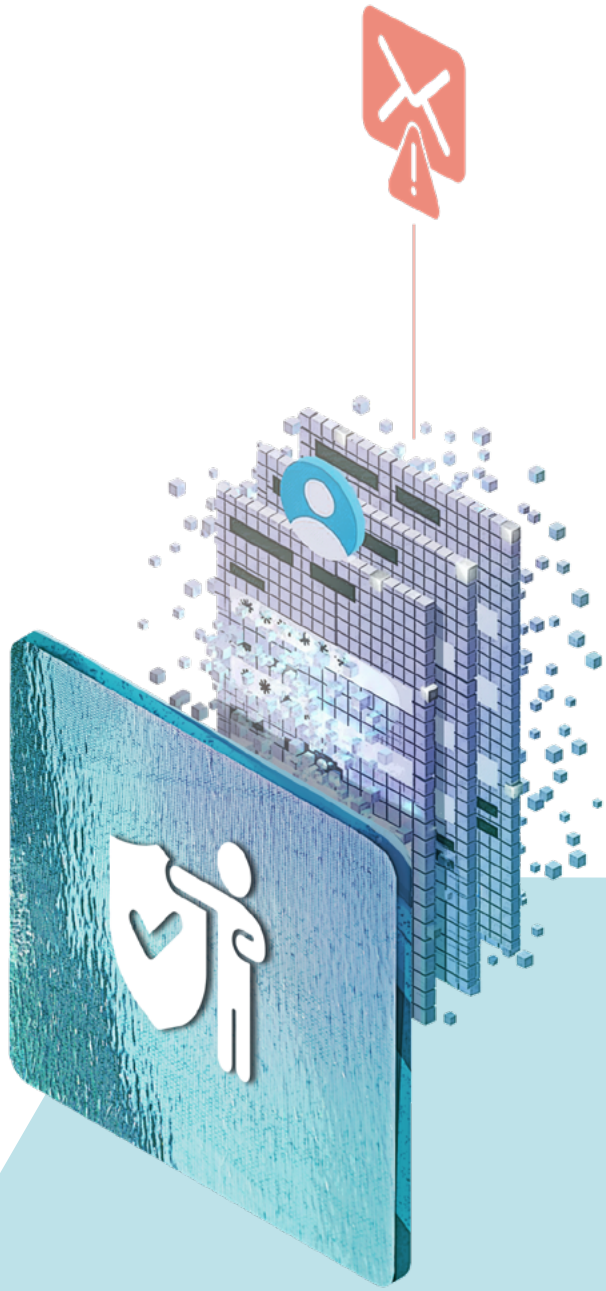
To ensure consistent skill levels across Member States, the CCSCAP proposes that the RCFC through the formation of a working group will establish a framework of **standardised profiles, training and certification programmes based on internationally recognised frameworks,** such as the European Cybersecurity Skills Framework (ECSF). These training programmes will be tailored to different levels of expertise, from foundational cyber security awareness for all employees to advanced technical training for cyber security specialists.

Also leveraging on the international capacity building initiatives developed in the Region, each Member State will be supported in developing training academies or working with accredited training centres to deliver these programmes. The curricula will cover critical topics, including incident response, digital forensics, criminal justice, international cooperation, handling electronic evidence in court, cyber threat intelligence and network defence.

In collaboration with international certification bodies and other accredited entities, CARICOM will verify the feasibility to introduce **regionally recognised certifications,** allowing cyber security and cybercrime professionals to achieve professional qualifications such as Certified Information Systems Security Professional (CISSP) or Certified Ethical Hacker (CEH). These certifications will provide a clear pathway for career progression and ensure that Member States have a qualified, competent cyber security workforce.

In addition, a "train-the-trainer" approach will be implemented, whereby **skilled professionals undergo training to become certified instructors.** This initiative will support the sustainable expansion of regional expertise, enabling CARICOM Member States to meet growing demands for cyber security education without solely relying on external trainers.

Last, a **mentorship scheme** should be established, pairing early-career cyber security professionals with experienced experts across CARICOM, also leveraging on structured rotations, guided research projects and fellowships linked to government and private sector placements.



Sector-specific cybercrime and cyber security capacity building

As an area of major concern and a sector directly involved in the capacity of a State to react to the ever increasing threats posed by cybercriminals, criminal justice authorities should prioritise **training of magistrates, prosecutors and law enforcement officials on cybercrime related issues,** including - but not limited to - national and international legal and policy frameworks, procedural provisions, conditions and safeguards in the exercise of investigative powers, digital forensics and cyber intelligence, handling of electronic evidence in court and international cooperation. Such training initiatives could benefit from the support provided in the framework of the related international cybercrime capacity building initiatives active in the Region, and should be organised in a sustainable manner, including through the implementation of a train-the-trainer mechanism.

Additionally, given the unique vulnerabilities in certain sectors, the CCSCAP encourages the prioritisation of **sector-specific cyber security capacity building,** focusing on areas such as finance, healthcare, energy, tourism, and government services. For instance, finance sector training will emphasise secure transaction protocols, fraud detection and compliance with data protection regulations. Healthcare sector training, on the other hand, will address the protection of sensitive patient information and the security of connected medical devices. Each sector-specific programme should include training on risk assessment, compliance with sector-specific regulations, and incident response tailored to that sector's unique needs.

Regional capacity building in infrastructure security

Training programmes will be developed at regional level for IT staff within public sector agencies, CII operators, and private sector partners, covering topics such as network security, secure configurations, and cloud security management. A **specialised module on securing critical infrastructure** shall also be developed, recognising that disruptions in these sectors can have far-reaching consequences for national security and public safety.

In addition to formal training, the CCSCAP will support **regular drills and tabletop exercises,** simulating cyber incidents that impact critical infrastructure. These exercises will enable public and private sector stakeholders to test their response protocols, identify areas for improvement and strengthen coordination mechanisms. CARICOM will also engage with international partners to access best practices and emerging technologies in infrastructure security, ensuring that member states benefit from global advancements in this field.

By **building local expertise in infrastructure security,** CARICOM aims to also reduce reliance on external providers, promoting greater autonomy and resilience across the Region.

Training will also include guidance on adhering to international standards such as ISO 27001:2022 for information security management, and internet related standards and IP numbering, ensuring consistency and alignment with global best practices.

Summary of proposed actions in the domain of capability development and capacity building and KPIs

Objectives	Activities	Performance Indicators	1-2 years	2-3 years	3- 5 years
1.Leverage investigation capabilities by promoting networking with other police organisations.	1.1. Establish agreement with organization to set up a curriculum of training activities in the area of digital forensics.	1.1.1. At least one agreement with organisation to set up a curriculum of training activities in the area of digital forensics.	X		
	1.2. Enhance regional capacity by providing standardized, hands-on training in digital forensics.	1.2.1.To design a programme related to hands-on training in digital forensics.		X	
	1.3. Facilitate train-the-trainer programs to build a self-sustaining pool of national instructors across Member States.	1.3.1. To design the document to involve grounds to facilitate future exchange trainers.		X	
2. Build specialised competencies in detecting, investigating and prosecuting cybercrimes.	2.1. Deliver modular training on topics such as online fraud, ransomware, CSAM, dark net investigations, and cryptocurrency tracking.	2.1.1. At least three per year. Deliver modular training on cyber topics such as online fraud, ransomware, CSAM, dark net investigations, and cryptocurrency tracking.	X		
	2.2. Provide learning experiences and strengthen ties through cybercrime peer exchange and secondment programme.	2.2.1. At least two per year peer exchanges.	X		
3. Enhance operational coordination and specialised investigations in cybercrimes issues.	3.1. Establishment of Cybercrime Task Forces in each Member State, with investigators in specific cybercrime areas for join investigations in international aspects in cybercrime (international organised crime)	3.1.1. To nominate one police officer in charge of the task force in each Member State.	X		
		3.1.2. To organise at least one joint investigation in cybercrime, using nominated task force.		X	
		3.1.3. Elaborating task force management protocols.	X		

Objectives	Activities	Performance Indicators	1-2 years	2-3 years	3- 5 years
4.Facilitate knowledge transfer and experience sharing among regional agencies.	4.1.Creation of a Cybercrime Knowledge Portal and Case Repository.	4.1.1. To design and the development of a Cybercrime Knowledge Portal and Case Repository.		X	
		4.1.2. To deliver completed set up platform of Cybercrime Knowledge Portal.			X
5. Institutional agreements with universities and third-party institutions.	5.1. Establishing collaborations, such as agreements with the University of the West Indies and third-party institutions, to provide specialised training and development programmes.	5.1.1. At least one agreement with universities or third-party institutions.			X
		5.1.2. At least one agreement with universities or third-party institutions.			X
6. Establish a repository of cyber security capacity building initiatives across the Region.	6.1 Design and launch an online regional repository for tracking training offers, requests, and support mechanisms.	6.1.1 Repository platform fully operational and accessible to all Member States.	X		
	6.2 Annual update and validation of repository content with national stakeholders.	6.2.1 Repository reviewed and updated annually with new offers and needs.		X	X
7. Create and maintain a regional pool of certified cyber security and cybercrime experts.	7.1 Establish certification criteria and selection process for regional experts.	7.1.1 Certification framework approved and published.	X		
	7.2 Operationalise a regional roster of certified experts available for cross-border support.	7.2.1 At least 50 experts registered by 2026 and available for deployment.		X	
8. Deliver tailored cyber security training to sectors managing critical information infrastructure (CII).	8.1 Conduct training needs assessments in key sectors (health, finance, energy)	8.1.1 Sectoral training needs mapped in at least three sectors by 2026.	X		
	8.2 Develop and implement sector-specific training programs in collaboration with relevant authorities.	8.2.1 At least one program delivered per sector by 2027.		X	

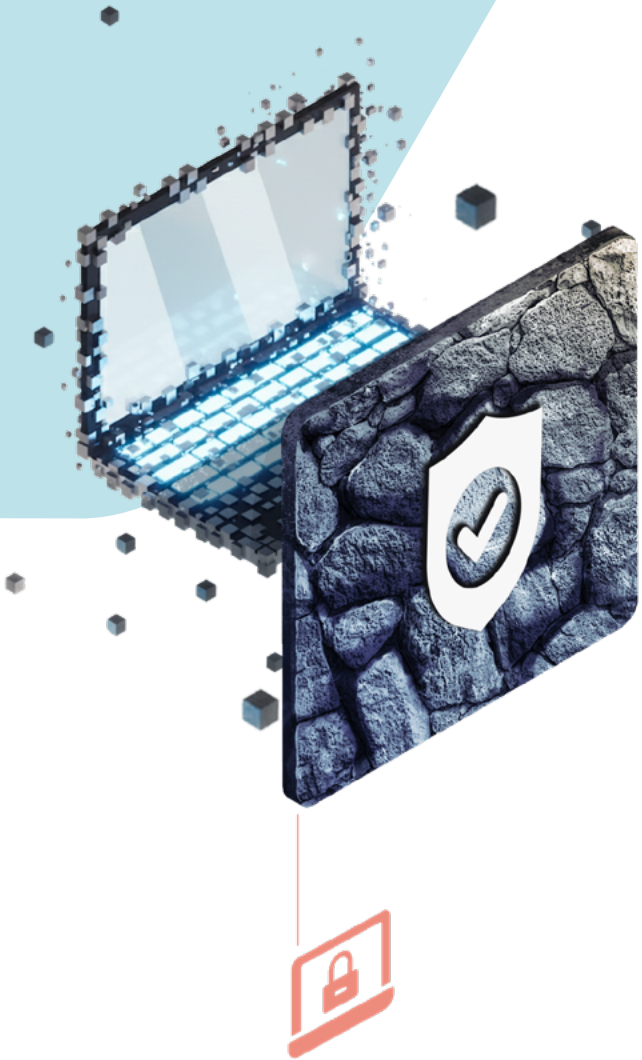
Technology and standards for resilient digital infrastructures and services

A robust cyber security framework requires clearly defined technical standards and resilient infrastructure to effectively defend against evolving cyber threats. Within CARICOM, varying levels of digital maturity and differing infrastructure capabilities among Member States have highlighted the need for harmonised technical standards and resilient infrastructure to promote a cohesive regional cyber security posture. This sub-area of the CCSCAP aims to standardise technical requirements, strengthen critical infrastructure protection and ensure interoperability across sectors and States, enhancing the Region's ability to prevent, detect and respond to cyber threats effectively.

Strategic Objectives

The primary objective of the Technology and Standards for Resilient Digital Infrastructure pillar is to create a unified framework that supports robust cyber security across CARICOM. This framework seeks to ensure that critical infrastructure within each Member State is adequately protected, while also promoting alignment with international standards to facilitate cross-border cooperation. To this aim, the strategic objectives are:

1. To establish a cybersecurity baseline for public and private entities.
2. To foster a programme aimed specifically at the protection of critical infrastructures.
3. To promote cyber security best practices for the supply chain.
4. To foster cybersecurity certification of products with digital components.



By defining technical requirements, establishing security protocols, and encouraging best practices, CARICOM will foster a secure digital environment that can withstand current and future cyber challenges.

Establishment of minimum technical standards

A cornerstone of this initiative is the **establishment of minimum technical measures for cyber security,** aligned with globally recognised frameworks such as, for instance, the NIST Cybersecurity Framework 2.0, ISO 27001:2022 for Information Security Management, and the IEC 62443 standards for critical infrastructure security. CSIRT Americas baseline to assess the maturity level of incident response teams will also be duly considered.

These minimum technical measures will include, among others, endpoint security, encryption protocols, authentication mechanisms and secure remote access and they should be updated biannually in consultation with national CSIRTs and RCFC. These standards will provide clear guidelines for securing networks, safeguarding data and managing cyber risks effectively. Member States will be encouraged to adopt these standards across both public and private sectors, ensuring a consistent approach to cyber security that transcends national boundaries.

To facilitate this, the CCSCAP provides for the regional governance structure to support the **development of national standards bodies** or committees within each Member State. These bodies will work in collaboration with CARICOM's central coordinating agency to adopt, adapt and enforce these standards at the national level. Standardisation will include protocols for access control, data encryption, network segmentation and secure software development practices, ensuring that security is embedded into digital infrastructure from the outset.

Protection of Critical National Infrastructure (CNI)

The protection of Critical National Infrastructure (CNI), with Critical Information Infrastructure (CII) now emerging as a central component of nearly all CNI sectors, is essential to ensure the continuity of vital services and safeguard public safety. CARICOM Member States rely on interconnected systems in sectors such as energy, telecommunications, healthcare and finance, which are increasingly targeted by cyber-attacks. The CCSCAP mandates **the identification and classification of CII assets within each Member State,** focusing on systems whose disruption would have severe national or regional consequences. To facilitate this task, a toolkit could be provided to identify, classify and assess the criticality of national infrastructure sectors and systems. The toolkit should include guidance on risk rating, resilience scoring and data dependency mapping. Priority will be given to developing regional guidelines that standardise how Member States identify and classify CII. This common framework will enable each country to build a national inventory of

critical infrastructure (CII/CNI) based on shared criteria for criticality, feeding into a consolidated regional catalogue of essential assets. Such standardisation will improve cross-border awareness and crisis coordination, bolstering regional cyber resilience in line with international best practices.

Once identified, these CII assets will be subject to **enhanced security protocols, including mandatory risk assessments, regular vulnerability testing and stringent incident response measures.**

Each Member State will be required to develop a **national strategy for CII protection,** which outlines the roles and responsibilities of relevant stakeholders, protocols for information sharing and minimum security requirements for CII operators. Furthermore, CII operators will be expected to maintain incident response and recovery plans, with regular training exercises to ensure preparedness for potential cyber incidents.

Vulnerability assessment and penetration testing

To ensure that Member States remain resilient against evolving cyber threats, the CCSCAP advocates for **periodic vulnerability assessments and regular penetration testing of critical infrastructure and government systems.** These assessments will identify weaknesses within digital assets, enabling timely remediation of vulnerabilities before they can be exploited by malicious actors. The CCSCAP recommends that vulnerability assessments are conducted at least quarterly for critical infrastructure, with more frequent assessments for high-risk sectors such as finance and healthcare. Penetration testing, simulating real-world cyber-attacks, will serve as a valuable tool for testing the efficacy of existing security measures and identifying potential points of failure. These tests will be performed by certified cyber security professionals following internationally recognised standards, such as those provided by the Penetration Testing Execution Standard (PTES) and the Open Web Application Security Project (OWASP). Member States will receive guidance and resources from CARICOM's central coordinating body to ensure that assessments are conducted effectively and consistently across the region.

Adoption of secure procurement and supply chain standards

The CCSCAP recognises that supply chain vulnerabilities represent a growing cyber security risk, as many Member States rely on third-party providers for critical ICT services and components. To mitigate these risks, the plan advocates for the **adoption of secure procurement standards across all CARICOM countries,** based on best practices such as the NIST Secure Software Development Framework (SSDF) and the European Union's (EU) Cybersecurity Act.

These standards will require vendors and contractors providing ICT services to CARICOM Member states to demonstrate **compliance with minimum security criteria,** including secure software development practices, regular vulnerability assessments and access control measures.

In addition, critical infrastructure operators will be encouraged to conduct thorough **risk assessments of their supply chains,** identifying and addressing potential security gaps that could be exploited by malicious actors. This will help ensure that third-party dependencies do not compromise the Region's cyber resilience.

Product certification

The implementation of cyber security certification for products with digital components circulating in the Caribbean Region might represent a step towards technological autonomy of the Tegion, and stronger consumer trust. Drawing inspiration from similar initiatives implemented in other regions of the world, such as the EU's Cyber Resilience Act, this initiative is expected to establish a **framework for addressing product vulnerabilities and ensuring compliance with international security standards,** thus also identifying criteria for providers' accreditation.

Summary of proposed actions in the domain of Technical Standards Compliance and Key Performance Indicators

Objectives	Activities	Performance Indicators	1-2 years	2-3 years	3- 5 years
1.Promote resource sharing and technological equity.	1.1. Develop a centralised procurement and loan framework for acquiring critical digital forensic and cybersecurity tools (e.g., RAM capture kits, forensic imaging stations.	1.1.1. Draft framework related to mentioned topics.	X		
2. Develop a basic standard for Digital Forensic Lab in order to facilitate evidence exchange.	2.1. Establish a uniform baseline for lab operations and e-evidence handling.	2.1.1. Form a technical working group with representatives from CARICOM IMPACS, national police forensic units, and legal experts.		X	
	2.2. Draft a standard aligned with international organisations' covering, among others, lab requirement criteria, and tool validation.	2.2.1. Distribute one practical implementation guidebook for national agencies related mentioned topics.		X	
	2.3 Draft a standard aligned with international organisations' covering, among others, standards operational procedures (SOPs), chain of custody, digital storage protocols.	2.3.1 .Distribute one practical implementation guidebook for national agencies related to mentioned topics.		X	

Objectives	Activities	Performance Indicators	1-2 years	2-3 years	3- 5 years
3. Harmonised criminal statistics.	3.1 Elaboration collaborated statistics templates with national cyber units, related to typologies of cybercrimes.	3.1.1. Creation a working-group to elaborate a draft of statistics templates.		X	
		3.1.2. Elaboration a draft of statistics templates.		X	
		3.1.3. Approve statistical models for national authorities.			X
	3.2. Creation collaborated statistics templates with Prosecutor´s officers, related criminal reports related cybercrime, cases prosecuted, convicted and acquittal cases.	3.2.1. Creation a working-group to elaborate a draft of statistics templates.		X	
	3.3. Creation systems to track and analyse data from law enforcement, police investigations, and judicial processes to inform decision-making.	3.3.1 To design of a system for a future software.			X
4.Cyberthreat intelligence platforms related typologies of cybercrime and cyber, criminal organisations APTs which operate in the Caribbean area	4.1. Elaboration collaborated threat intelligence platplatforms withional Cyber units, related to typologies of cybercrimes.	4.1.1. Creation a regular consolidated document of this topic.		X	
		4.1.2. Creation cyber threat intelligence platform.	X		
5.Cyber Fusion Unit will be expanded by improving its capacity to monitor cyber security and cybercrime	5.1. Strengthen the capabilities of the CFU members	5.1.1. Establishment of protocols and improvement of processes for the management of the Cyber Fusion Centre.	X		
		5.1.2. At least two training sessions for the unit members in the field of cybercrime.	X		
6. Establish CARICOM-wide minimum cyber security technical standards.	6.1. Convene a regional working group to draft minimum cyber security standards aligned with ISO/ IEC 27001:2022, NIST 2.0, and relevant frameworks.	6.1.1 .Minimum standards document finalised and adopted by 2026.	X	X	
	6.2. Disseminate and support implementation of minimum standards at national level.	6.2.1. Adoption in at least 10 Member States by 2027.		X	

Objectives	Activities	Performance Indicators	1-2 years	2-3 years	3- 5 years
7. Develop and implement national Critical Information Infrastructure (CII) protection frameworks.	7.1. Support Member States in developing national CII protection strategies covering key sectors (energy, finance, health, telecom).	7.1.1. National CII protection frameworks operational in at least 50% of Member States by 2027.	X	X	
	7.2 .Organise technical workshops and CII risk assessments.	7.2.1. At least five technical workshops held regionally by 2027.		X	
8. Promote vulnerability assessment and penetration testing (VAPT).	8.1. Develop a regional VAPT framework and operational guidelines.	8.1.1. Regional VAPT framework developed and validated by 2026.	X	X	
	8.2. Pilot vulnerability assessments in critical sectors in at least five Member States	8.2.1. Pilot Facilitate Member States Implementation VAPT reports delivered in five countries by 2027.		X	X
9. Develop secure supply chain cyber security standards.	9.1. Draft regional guidelines on secure procurement practices and supply chain risk management.	9.1.1. Guidelines finalised by 2027.		X	X
	9.2. Promote guideline adoption among public and private sector procurement units.	9.2.1 Dissemination to all Member States and uptake by at least eight by 2028.			X
10. Establish a voluntary certification scheme for cyber security products and service providers.	10.1 Develop a regional certification framework for cyber security tools and vendors.	10.1.1 Certification framework piloted by 2028.			X
	10.2 Partner with testing labs and regulators to validate and certify solutions.	10.2.1 At least three products/services certified by 2028.			X

Policy, Institutional and Regulatory Framework

A comprehensive and harmonised legal and regulatory framework is essential to enable consistent enforcement, cooperation across jurisdictions, and the protection of citizens and critical infrastructure from the growing threats posed by cybercrime. Given the disparities in digital development – and the diverging legal systems in the wider Caribbean – it is important to map out jurisdiction-specific regulatory gaps and capacity limitations to prioritise legal and institutional strengthening.

Within CARICOM, cyber security legal frameworks remain uneven, leading to challenges in cross-border cooperation and gaps in protection. Notably, while most CARICOM Member States share a common law heritage that facilitates harmonisation, the Region as a whole still contends with fragmented legal traditions (e.g. some jurisdictions following civil law or mixed systems), which has resulted in inconsistent definitions of cybercrime and procedural differences. Some States have advanced cybercrime laws aligned with international standards, but others lack comprehensive legislation, creating gaps that criminals exploit. This sub-area of the CCSCAP is therefore dedicated to establishing a robust, unified legal framework across Member States – aligned with instruments like the Budapest Convention and the new UN cybercrime treaty – to eliminate legal blind spots and enable swift cooperation.

Strategic Objectives

The Policy, Institutional and Regulatory Framework pillar aims to achieve the following core objectives:

1. To harmonise cybercrime legislation across CARICOM Member States, ensuring uniform definitions of offenses and legal procedures and alignment with international instruments. This harmonisation must also include shared enforcement mechanisms and judicial cooperation protocols.

2. To strengthen the Region's capacity to prosecute and deter cybercrime through updated legal instruments, streamlined extradition processes and effective investigative powers for law enforcement. These updates should incorporate safeguards such as judicial oversight and due process guarantees.

3. To foster the adoption of national cyber security policies, regulations, and guidelines – including data protection and privacy laws – that protect citizens and critical information infrastructure while upholding human rights.

4. To establish a consistent framework for identifying and managing cyber risks across all CARICOM Member States, enabling proactive risk assessment and mitigation strategies. The framework should be subject to regular audits and independent reviews to ensure continued relevance and effectiveness.

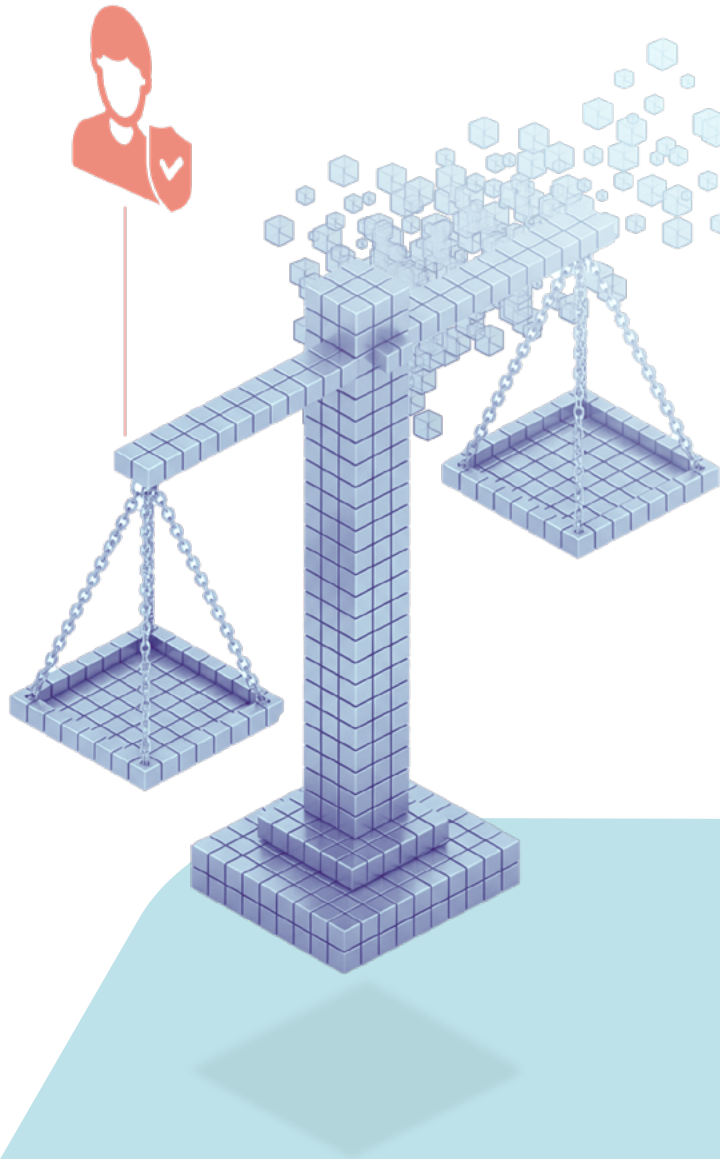
5. To institutionalise regional enforcement oversight mechanisms to monitor implementation and compliance with harmonised cyber security and cybercrime laws

To realise these objectives, CARICOM will support Member States by developing model legislation and policy guidelines in key areas of cyber law. These model laws (for example, in cybercrime, data protection and electronic evidence) will serve as templates that countries can adapt when updating their national legislation, ensuring reforms are guided by regionally harmonised principles and international best practices. Each Member State should be required to report on implementation progress against the model laws on an annual basis. By establishing a clear legal foundation for cyber security and cybercrime response, CARICOM seeks to eliminate legal gaps, promote mutual trust and enable swift cooperation both within the region and with international partners.

Harmonisation of cybercrime laws

Harmonisation of cybercrime legislation across CARICOM Member States is essential to facilitate cross-border collaboration and improve legal interoperability. The CCSCAP encourages countries to align their national cybercrime laws with international standards – notably the Council of Europe **Convention on Cybercrime** (Budapest Convention) and the newly adopted **UN Convention on Cybercrime** (UN Convention on Countering the Use of ICTs for Criminal Purposes). In pursuit of this alignment, CARICOM will prepare a model cybercrime law and accompanying guidelines that incorporate these international best practices, providing each Member State with a clear template for updating domestic statutes. To ensure effectiveness, implementation of the model law should be supported by monitoring mechanisms and legal technical assistance where gaps are identified. Member States are expected to adapt their definitions of cyber offenses, procedural powers and investigative tools in line with these conventions, which several CARICOM countries have already adopted.

A harmonised legal framework will also establish minimum sentencing guidelines and penalty structures for cyber offences, creating a credible deterrent against cybercriminal activity in the Region. By standardising legal definitions, investigatory procedures and judicial processes, CARICOM can remove barriers to cooperation and foster a cohesive regional response to cyber threats. Consistent laws will ensure that a cybercriminal cannot exploit legislative disparities between Member States to evade justice. The model law should also include clauses on expedited preservation and disclosure of data and establish procedures for cross-border execution of orders. CARICOM shall establish a Cybercrime Legislative Observatory to monitor and report on the status of harmonisation efforts and legislative implementation.



Development of E-Evidence and Digital Forensics Legislation

The increasing reliance on digital evidence in cybercrime investigations requires robust legal provisions to support the collection, preservation, and admissibility of electronic evidence. To this end, the CCSCAP proposes – and CARICOM will support – the introduction of a comprehensive **electronic evidence (e-evidence) framework** across the Region. This includes establishing uniform protocols for the handling and preservation of digital evidence so that it meets standards of admissibility in court proceedings in all CARICOM Member States. The framework will outline guidelines for collecting evidence from digital devices, cloud services, and internet service providers, ensuring that evidence gathered in one Member State can be lawfully recognised in another without procedural conflict. Where appropriate, model protocols or legislative provisions for e-evidence handling will be developed to guide national adoption of these standards while respecting fundamental rights and the chain of custody.

In parallel, specialised training programmes will be implemented to enhance regional capabilities in digital forensics. Law enforcement officers, prosecutors and judges will receive training on the proper handling and interpretation of digital evidence. These programmes will cover critical topics such as maintaining chain of custody for electronic evidence, handling encrypted data, and using advanced forensic tools and techniques. Training programmes should be delivered with follow-up certification and peer-review opportunities to reinforce professional standards. By building competence in digital forensics and having consistent e-evidence legislation, CARICOM Member States can increase the success rate of cybercrime prosecutions and strengthen public trust in the judicial process.

Enactment of Data Protection and Privacy Laws

Data protection and privacy are foundational elements of cyber security, as they safeguard individual rights and build trust in digital services. The CCSCAP advocates for each CARICOM Member State to enact or strengthen **national data protection legislation** that aligns with internationally accepted standards such as the EU's General Data Protection Regulation (GDPR), the Council of Europe's Convention 108+, and CARICOM's own data protection guidelines. Member States should also take into account new developments in global data privacy standards (for instance, the EU's forthcoming e-Privacy regulation) to keep their laws up-to-date. These laws should ensure that individuals' personal data is handled responsibly, transparently, and securely, defining the rights of data subjects and the obligations of organisations that collect or process personal information. Each law should include mandatory Data Protection Impact Assessments (DPIAs) for high-risk processing activities and define clear rules for cross-border data transfers. CARICOM, through its agencies, will consider developing a **model data protection act** to provide a blueprint balancing public safety with privacy rights, which Member States can adapt to their legal systems.

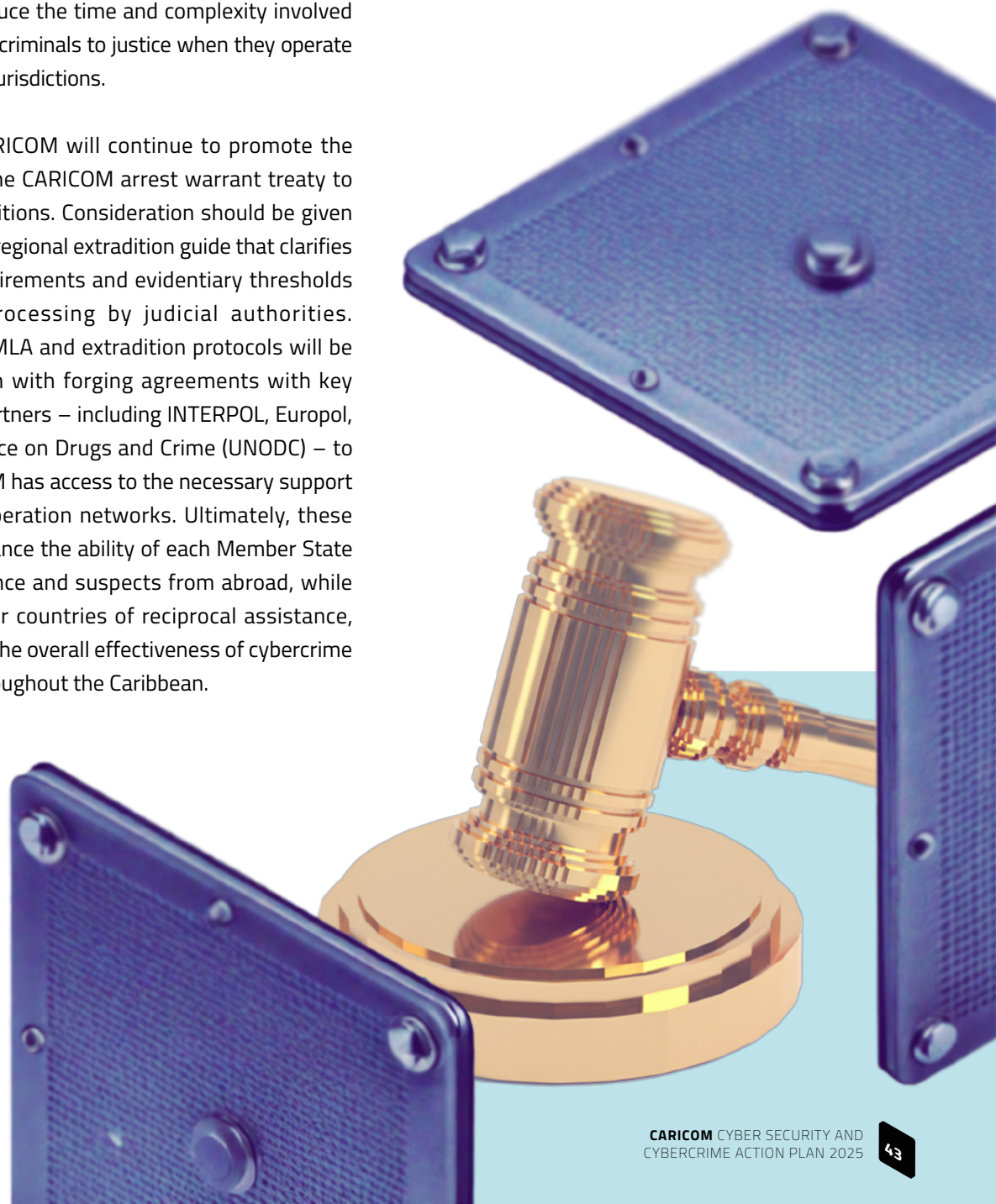
Under the recommended regional data protection framework, all entities handling personal data will be required to implement appropriate security measures to prevent unauthorised access, theft, or breaches of that data. Additionally, national laws will mandate timely breach reporting – organisations must report significant data breaches to their national Data Protection Authority within a specified timeframe and notify affected individuals when their personal data is compromised. Through the governance structures proposed in the CCSCAP, CARICOM will also support Member States in establishing independent Data Protection Authorities. These authorities must be adequately resourced and guaranteed operational independence from executive influence. These authorities will be responsible for enforcing compliance with privacy laws, investigating data breaches, and educating the public on their data privacy rights. By instituting strong and uniform data protection regimes, the region not only protects its citizens' privacy but also creates an environment of trust conducive to digital innovation and e-commerce.

Mutual legal assistance and promoting extradition protocols

To effectively combat transnational cybercrime, CARICOM must have robust mechanisms for mutual legal assistance (MLA) and extradition. The CCSCAP calls for the development of a standardised **regional MLA framework** based on the principles of the Budapest Convention, enabling seamless cooperation among Member States in investigating and prosecuting cybercriminals. This framework will detail clear procedures for cross-border evidence sharing (for example, handling requests for data from service providers in another jurisdiction), conducting joint investigations, and expediting extradition for cyber offences. The framework should also define timelines for response to MLA requests and designate national contact points responsible for coordinating MLA and extradition matters.

By streamlining these processes and basing them on established international conventions, the region can significantly reduce the time and complexity involved in bringing cybercriminals to justice when they operate across multiple jurisdictions.

In addition, CARICOM will continue to promote the ratification of the CARICOM arrest warrant treaty to facilitate extraditions. Consideration should be given to developing a regional extradition guide that clarifies procedural requirements and evidentiary thresholds to expedite processing by judicial authorities. Strengthening MLA and extradition protocols will be done in tandem with forging agreements with key international partners – including INTERPOL, Europol, and the UN Office on Drugs and Crime (UNODC) – to ensure CARICOM has access to the necessary support and global cooperation networks. Ultimately, these efforts will enhance the ability of each Member State to obtain evidence and suspects from abroad, while assuring partner countries of reciprocal assistance, thus improving the overall effectiveness of cybercrime prosecution throughout the Caribbean.



Law enforcement capacity building on handling to prevent re-victimization

Victims of cybercrime – whether individuals, businesses, or public institutions – often face significant financial, psychological, and reputational harm. Accordingly, the CCSCAP advocates for incorporating victim protection and support provisions into national cybercrime response frameworks. Each Member State should establish dedicated support mechanisms such as national cybercrime victim helplines or helpdesks to assist the public in reporting incidents and seeking guidance. Additionally, support services (potentially coordinated by law enforcement or civil society organisations) should offer counselling, legal advice, and technical assistance to victims, helping them recover lost data or funds and cope with the aftermath of incidents like identity theft or online fraud. It is also recommended that victim services be integrated into national emergency response plans and digital safety education initiatives.

The CCSCAP also encourages the inclusion of victim protection clauses in cybercrime legislation. For example, laws and protocols should mandate law enforcement agencies to inform victims of available support and, where possible, assist them in securing evidence and pursuing legal recourse. To support implementation, Member States should be encouraged to adopt minimum service delivery standards for victim support centres and to regularly publish statistics on victim assistance outcomes. Public awareness campaigns – as outlined in the Public Awareness, Education and Advocacy pillar (section 5.1) – will integrate messaging on victim rights and resources, so that individuals and businesses know how to respond if they fall victim to cybercrime. Moreover, CARICOM will promote the exploration of cyber insurance schemes and compensation mechanisms across Member States to help mitigate the financial impact on victims. These may include government-backed insurance schemes or public-private co-financing models tailored to small businesses and vulnerable groups.

By institutionalising victim support and protection measures, CARICOM aims to bolster public confidence in the digital economy and ensure that the human impact of cybercrime is not overlooked.

Cyber Risk Management Framework

Effective risk assessment and management are essential to a resilient cyber security posture, enabling organisations and governments to identify and mitigate threats proactively. Given the diverse digital maturity levels across CARICOM, a harmonised approach to cyber risk management is needed – one that can be adapted to each State's unique infrastructure and threat landscape while maintaining regional consistency. The CCSCAP therefore supports the development of a **standardised methodology** for conducting cyber risk assessments in every Member State, aligning with established frameworks such as ISO 31000 (Risk Management) and the NIST Cybersecurity Framework 2.0. This common methodology will guide countries through identifying and categorising critical assets, evaluating potential threat vectors, and assessing the likelihood and impact of various cyber incidents. It will also promote **sector-specific risk assessments,** ensuring that sectors like finance, energy, health, and government each evaluate and address the particular cyber risks they face on a regular basis. Member States should institutionalise risk assessments within regulatory regimes for critical sectors and report findings to a regional cybersecurity coordination body.

Based on these assessments, CARICOM will implement a **unified regional cyber risk management framework** to address both current and emerging threats. This framework will set out standard protocols and best practices for risk mitigation across critical sectors and government services. Key focus areas will include vulnerability management (e.g., timely patching of systems), network segregation and secure configuration baselines, access control policies and third-party risk management, among others. To support implementation, the CCSCAP will facilitate the creation of regional cyber security audit and compliance toolkits, providing Member States with tools to measure adherence to the agreed risk management standards and identify gaps. Special protocols will be developed to safeguard essential services and critical infrastructure operators – for example, ensuring redundancy and backup systems, incident response plans for high-impact scenarios, and integration of physical security measures with

cyber security. By adopting this comprehensive risk management approach, CARICOM countries will be better prepared to prevent incidents and ensure continuity of operations even under cyber-attack.

Adopting robust cybersecurity national policy and national strategy

As cyber threats grow in scale and sophistication, it is imperative that every CARICOM nation has a well-defined and actionable **national cyber security policy or strategy.** In recent years, several Member States have drafted or adopted national cyber security strategies, laying the foundation for cyber resilience through improved risk management, coordinated incident response, and protection of critical infrastructure. The CCSCAP seeks to ensure all Member States without a current strategy develop one, and that existing strategies are kept up to date and effectively implemented. Without coherent national frameworks to guide cyber security actions, countries remain vulnerable to disruption, data breaches and threats to national security. Therefore, **the prioritisation of well-designed, inclusive, and enforceable cyber security strategies** is placed at the core of the regional agenda. A specific attention will be dedicated to include a gender perspective in the national cyber security strategies, also taking into consideration examples coming from countries in neighbouring regions, such as Costa Rica (adopted in 2022) and Colombia (2025). This effort will continue to benefit from the support of the OAS-CICTE.

CARICOM will facilitate coordination – for example, by identifying and sharing best practices from those countries at the forefront of strategy development, and by providing a forum for alignment so that national policies complement regional objectives. Member States will be encouraged to address common elements in their strategies, such as public-private cooperation, critical infrastructure protection, capacity building, and legal measures (in harmony with the other parts of the CCSCAP). Additionally, it is recommended that each country institutionalise regular capacity assessments and strategy reviews (e.g. on an annual or biennial basis). Such reviews will enable governments to measure progress on their strategy's implementation and to adjust their policies in response to the evolving threat landscape and technological change.

By the end of the plan period, all CARICOM Member States should have a comprehensive cyber security strategy in place, and a routine process to update it – thereby ensuring sustained commitment to cybersecurity at the highest levels of government.

AI regulation and related policies

The rising adoption of Artificial Intelligence (AI) tools and services in both public and private organisations poses unique challenges and opportunities, both globally and at regional level, especially with respect to the security of sensitive data, the reliability of the produced outcomes and the potentially malicious use that can be made of them. Governance of artificial intelligence has become a compelling issue, making the drafting of a regional AI model law both timely and necessary. Such legislation would not only provide a harmonised framework for ethical AI adoption, but also strengthen regional digital resilience by addressing risks such as algorithmic bias, misuse of automated decision-making and cross-border data governance issues.

Importantly, the development of an AI model law is deeply interlinked with the cyber security domain as AI systems increasingly underpin critical infrastructure, finance, and e-government services, robust cyber security protections are essential to safeguard them from malicious attacks, data breaches and manipulation. Conversely, AI technologies can enhance cyber security by enabling advanced threat detection, real-time monitoring, and predictive defence systems. By aligning AI governance with cyber security strategies, Caribbean countries can foster trust in digital transformation, ensure data sovereignty, and build a secure foundation for innovation and economic growth across the Region.

Summary of proposed actions in the domain of Policy, Institutional and Regulatory Frameworks and Key Performance Indicators

Objectives	Activities	Performance Indicators	1–2 years	2–3 years	3–5 years
1. Cybercrime Model Act	1.1 Draft legislation conforming to Budapest Convention, UN Treaty, and investigative powers (e.g., remote access, record)	1.1.1 Model act available for Member States by 2026	X		
	1.2 Support national alignment of cybercrime laws with model act	1.2.1 Draft national laws Member States by 2027		X	X
	1.3 Develop and disseminate sentencing guidelines for cyber offences	1.3.1 Guidelines finalized and shared with Member States by 2026	X	X	
2. Digital Data Protection Model Act	2.1 Draft legislation balancing public safety, privacy, and alignment with GDPR and Convention 108+	2.1.1 Model data protection act published by 2026		X	
	2.2 Include mandatory breach notification and establishment of national DPAs in model framework	2.2.1 Updated draft shared with provisions included in at least 8 countries by 2027		X	X
3. E-Evidence Legal Framework	3.1 Draft and distribute regional model act for handling electronic evidence	3.1.1 Model law completed and shared with Member States	X		
	3.2 Provide digital forensics and e-evidence training for law enforcement and judiciary	3.2.1 At least 5 regional workshops completed by 2028		X	X
4. E-Evidence Protocols and Cyber Risk Tools	4.1 Draft national protocols for e-evidence chain of custody and management	4.1.1 Protocol distributed to all Member States by 2026	X		
	4.2 Draft protocol on CSIRT–LEA collaboration and cyberattack reporting deadlines	4.2.1 Protocol drafted and validated by 2027	X		
	4.3 Develop template protocol for cyber risk assessment methods (aligned with ISO 31000/NIS 2)	4.3.1 Template adopted regionally by 2026		X	

Objectives	Activities	Performance Indicators	1–2 years	2–3 years	3–5 years
5. Virtual Assets and VASPs Regulation	5.1 Draft regional model act for regulation of virtual assets and service providers	5.1.1 Model act published by 2027		X	
	5.2 Support national adaptation of virtual asset regulation aligned with model act	5.2.1 National-level legislation passed in at least 5 countries by 2028			X
6. AI Readiness Assessment in cybersecurity and cybercrime	6.1 Develop and administer national surveys to assess AI governance preparedness	6.1.1 Survey results available for at least 10 Member States by 2026	X		
7. Model AI Legislation	7.1 Draft regional model act for ethical and responsible AI use	7.1.1 Model act finalized and circulated to Member States		X	
8. Mutual Legal Assistance and Extradition for Cybercrime	8.1 Develop standardised CARICOM MLA provisions for cybercrime and align with Budapest mechanisms	8.1.1 MLA framework approved and used by at least 5 countries by 2028	X	X	X
	8.2Promoting CARICOM arrest warrant system	8.2.1 Promoting CARICOM arrest warrant	X	X	X
9. Cybercrime Victim Support and Restitution	9.1 Establish national cybercrime victim helpdesks or hotlines	9.1.1 At least 10 Member States with operational support systems by 2027	X	X	
	9.2 Integrate victim protection clauses in national cybercrime laws	9.2.1 Legal amendments adopted in at least 8 countries by 2028		X	X
10. National Cybersecurity Strategy Development and Alignment	10.1 Support all Member States in developing or updating national cybersecurity strategies	10.1.1 All Member States with up-to-date national strategies by 2028	X	X	
	10.2 Facilitate biennial review and alignment of national strategies with CCSCAP priorities	10.2.1 Biennial regional policy forum and scorecard established by 2026			X

Incident Management

In the face of an increasingly sophisticated cyber threat landscape, effective incident response is essential for protecting critical infrastructure, maintaining public confidence, and ensuring the continuity of essential services across CARICOM. A swift and well-coordinated incident response minimises damage, facilitates rapid recovery, and strengthens resilience against future attacks. Within CARICOM, incident response capabilities vary significantly across member states, creating challenges for regional coordination and timely intervention in the event of cyber incidents that span national borders. This sub-area of the CCSCAP is dedicated to building a cohesive, scalable, and adaptive incident response framework, empowering CARICOM to address cyber threats through proactive readiness, collaborative response, and efficient recovery mechanisms.

Strategic Objectives

The primary objectives of the Incident Response pillar are:

1. Strengthen national cyber incident response capacity through the establishment or enhancement of CSIRTs
2. Promote regional coordination of incident reporting, threat intelligence sharing and response activities.
3. Develop a trusted network of NCPOCs to facilitate rapid, secure communication between States and regional institutions.
4. Establish simulation exercises and training regimes to prepare stakeholders for cyber emergencies
5. Develop and implement a Vulnerability Disclosure Program (VDP) to enable individuals and organisations to responsibly report vulnerabilities identified in critical systems.
6. Foster a culture of proactive risk mitigation and coordinated crisis response across CARICOM.

By developing a robust incident response system, CARICOM aims to create a security posture that can anticipate, withstand, and recover from a broad spectrum of cyber threats.

National and Regional CSIRTs

At the heart of the incident response strategy is the **establishment and enhancement of CSIRTs at both national and regional levels.** Each member state will be encouraged to set up a national CSIRT that acts as the primary contact point for all cyber security incidents within the country. These teams will be responsible for receiving incident reports, conducting initial assessments, coordinating response efforts, and facilitating information sharing with the regional body and other national CSIRTs.

A **regional CSIRT will serve as the coordinating entity, connecting national CSIRTs across CARICOM** to ensure a harmonised approach to incident response and cross-border collaboration. This team will manage regional threat intelligence, provide guidance on emerging threats and act as a liaison with international cyber security organisations such as the OAS, INTERPOL, and the Global Forum of Incident Response and Security Teams (FIRST). The regional CSIRT will also oversee joint response efforts in the event of large-scale cyber incidents impacting multiple CARICOM States, providing a unified and coordinated response framework.

Incident response framework at regional and national levels

To create a seamless incident response process across CARICOM, the CCSCAP advocates for the **introduction of a unified Incident Response Framework** (IRF) that outlines standard protocols, roles, and responsibilities for incident detection, response, recovery, and post-incident analysis. This framework will be based on established international standards, including the NIST Computer Security Incident Handling Guide and ISO/IEC 27035, adapting these guidelines to the unique needs and capacities of CARICOM Member States.

The IRF will define the stages of incident management, from preparation and detection to containment, eradication, recovery and post-incident review. Each stage will include detailed actions, documentation requirements, and protocols for communication, both within and between national CSIRTs. This framework will enable CARICOM to respond to incidents consistently and efficiently, regardless of the specific Member State affected. A clear chain of command and communication will be established to ensure that each stage of the response process is managed effectively, minimising confusion and delays during critical incidents.

A **protocol for conducting thorough post-incident analyses** following each significant cyber event should also be established. This analysis will include a review of the incident's cause, the effectiveness of response actions, and the performance of the communication and coordination processes. Post-incident findings will be documented and shared across CARICOM Member States, providing valuable insights into common vulnerabilities, response challenges and best practices.

The **continuous improvement process** will involve updating incident response procedures, refining training programmes, and revising the incident response framework as new threats and technologies emerge. This adaptive approach will ensure that CARICOM's incident response capabilities evolve alongside the cyber threat landscape, maintaining an agile and prepared stance in the face of emerging risks.

Development of a Vulnerability Disclosure Program (VDP)

The CCSCAP will establish a formal mechanism through which individuals, ethical hackers, and organisations can responsibly report security vulnerabilities discovered in critical systems. The VDP will define clear procedures for submission, validation and remediation of reported vulnerabilities, ensuring coordinated communication between reporters and competent authorities. By fostering transparency and collaboration, the programme will enhance early detection of weaknesses, reduce exploitation risks and strengthen the overall resilience of critical infrastructure across CARICOM.

Standardised incident reporting

For CARICOM to effectively monitor and manage cyberattacks and cyber security incidents, Member States should consider adopting a **common regional framework for incident reporting**. The CCSCAP suggests that a working group be formed to develop a standardised incident reporting protocol that mandates prompt notification of cyber incidents, allowing for timely response and data-driven decision-making. This protocol will be applicable to all entities operating within critical sectors, ensuring comprehensive monitoring of the Region's cyber security landscape.

The CCSCAP advocates for Member States to use standardised incident reporting and notification protocols that require all critical infrastructure operators, government agencies and major private sector entities to report cyber incidents promptly to their respective national CSIRT. Reports will include essential information such as the nature of the incident, affected systems, suspected attack vectors, and any immediate actions taken. In this respect, the development of a **cyber-incident reporting and escalation playbook** could be considered, including standard operating procedures for threat identification, escalation tiers, cross-agency coordination, and breach notification. The playbook should be translated into French, Spanish and Dutch to ensure multilingual applicability.

To encourage transparency, the framework should establish **confidential reporting channels** for organisations that may be concerned about reputational damage. These channels will allow anonymous or semi-anonymous reporting, ensuring that incident data is collected and utilised without dissuading organisations from reporting. National CSIRTs will be responsible for notifying the regional CSIRT of significant incidents that may have cross-border implications or impact regional stability, allowing for rapid coordination and information sharing across CARICOM.

Threat intelligence sharing and coordination mechanisms

CARICOM will establish a **centralised threat intelligence platform,** accessible to all Member States, their CSIRTs, law enforcement agencies, and operators of critical infrastructure, who will contribute by sharing anonymised data on incidents, vulnerabilities and detected threats. The platform will be managed by the regional CSIRT and will provide Member States with access to up-to-date threat intelligence, indicators of compromise (IOCs), attack patterns and vulnerability information, thus enhancing CARICOM's situational awareness and ability to anticipate emerging threats.

This data-sharing initiative will promote a proactive security posture, allowing Member States to prepare for and mitigate threats before they impact critical systems. The platform will support integration with international threat intelligence feeds and databases, ensuring that CARICOM has access to global insights on emerging cyber threats. The platform will also facilitate collaboration during active incidents, enabling national CSIRTs to coordinate responses, share technical expertise and access resources from other Member States.

Incident response training and simulation exercises

Building and maintaining effective incident response capabilities requires regular training and simulation exercises for all relevant stakeholders, including CSIRT personnel, critical infrastructure operators, government agencies and private sector partners. The CCSCAP through its pillar on Capability Development and Capacity Building will establish a structured training programme that includes both **foundational and advanced incident response training**, covering topics such as malware analysis, network forensics, containment strategies and incident escalation.

To reinforce these skills, the RCFC will coordinate **annual regional cyber incident simulations** that mimic real-world scenarios, such as ransomware attacks on healthcare systems, denial-of-service attacks on financial institutions, or data breaches in government networks. Regional cyber drills shall include not only government and technical teams, but also participation from utility companies, telecom providers, financial institutions, and media representatives. These exercises will test the readiness of national and regional CSIRTs, assess coordination between agencies, and identify areas for improvement in existing protocols.

Following each simulation, a post-exercise review will be conducted to capture lessons learned, inform future training, and refine the incident response framework.

Establishment of a Regional Incident Response Support Fund

To ensure that financial constraints do not hinder effective incident response, the CCSCAP advocates for the creation of a **Regional Incident Response Support Fund.** This fund will provide emergency financial assistance to member states experiencing significant cyber incidents that require resources beyond their current capacity. The fund can be used to support immediate response needs, such as hiring additional incident response personnel, accessing third-party expertise, or procuring necessary tools and infrastructure.

Member States will be able to apply for support through a streamlined application process, with approval contingent on the severity and impact of the incident. This financial safety net will help CARICOM Member States manage the costs associated with incident response, recovery, and remediation, reducing the economic and operational impact of cyber incidents on national and regional stability.

Summary of the actions in the domain of Incident Management and KPIs

Objectives	Activities	Performance Indicators	1–2 years	2–3 years	3–5 years
1. Strengthen national incident response capabilities	1.1 Support the establishment or enhancement of CSIRTs with clear mandates, staffing, and technical capacity	1.1.1 Functional national CSIRTs operational in at least 12 Member States by 2028	X	X	X
2. Operationalise regional coordination of incident reporting and threat intelligence	2.1 Establish RCFC as a regional hub for cybersecurity information sharing and incident coordination	2.1.1 RCFC fully operational by 2026; regional threat reporting network established	X	X	
3. Increase National Cyber Point of Contacts (NCPOCs)	3.1 Require Member States to appoint two NCPOCs for real-time cyber communication and coordination	3.1.1 Two NCPOCs appointed in each Member State by end 2026	X		
4. Develop and implement a standardised incident reporting protocol	4.1 Implement the Simplified Draft Standardised Incident Reporting Protocol for consistent cyber incident submissions	4.1.1 Incident reporting protocol adopted and used by 80% of Member States by 2027		X	
5. Test and evaluate incident response capacity through simulation exercises	5.1 Conduct annual regional cyber incident simulations and crisis management exercises	5.1.1 At least two major regional cyber drills completed by 2028		X	X
6. Develop a Vulnerability Disclosure Program	6.1 Establish a formal mechanism through which individuals, ethical hackers, and organizations can responsibly report security vulnerabilities discovered in critical systems	6.1.1. Define a Vulnerability Disclosure methodology to be adopted by the Caribbean countries	X		
		6.1.2. Create a centralized database of cybersecurity vulnerabilities affecting ICT products and services in the region		X	

Regional and international cooperation

In today's interconnected digital landscape, effective cyber security requires strong, coordinated efforts that extend beyond national borders. For CARICOM, regional and international cooperation is essential to tackle the scale and sophistication of cyber threats that threaten economic stability, public safety, and digital sovereignty. This sub-area of the CCSCAP is dedicated to fostering strategic partnerships, enhancing cross-border collaboration, and aligning cybersecurity practices with international standards. Through these efforts, CARICOM aims to build a cohesive, resilient cyber security ecosystem that leverages the collective strength of Member States and aligns with global best practices, ensuring a robust defence against cybercrime and other digital threats.

Strategic Objectives

The primary objectives of the Regional and International Cooperation pillar are:

1. To facilitate cross-border collaboration and information sharing within CARICOM
2. To establish strategic alliances with international organisations, law enforcement agencies, cyber security partners and partners and donors focusing also on funded projects provisioning.
3. To strengthen existing international partnerships.
4. To harmonise CARICOM's cyber security policies and practices with international standards.

These objectives are designed to enhance CARICOM's collective cyber security posture, promote interoperability, and enable rapid, coordinated responses to cyber incidents with regional or global impact.

Information sharing and intelligence exchange

Timely information sharing is essential for identifying and mitigating cyber threats before they cause widespread harm. As such, **protocols will be established for real-time intelligence exchange**, enabling Member States to share threat indicators, vulnerability information and attack signatures through a secure, centralised Digital Forensic Management Platform managed by the RCFC. This platform will connect CARICOM Member States with key international partners, including the (OAS, EU, and INTERPOL, providing access to global threat intelligence that enhances CARICOM's situational awareness.

To ensure the effectiveness of information sharing, there is a need for a **framework for classifying and handling sensitive data,** ensuring that intelligence is disseminated securely and in compliance with privacy regulations. Member States will be encouraged to contribute anonymised data on incidents and vulnerabilities, fostering a culture of mutual support and collaboration. **Regular intelligence briefings and updates** will also be provided to all CARICOM stakeholders, promoting proactive threat identification and mitigation across the Region.

Joint cyber security exercises and capacity building initiatives

Regional and international cooperation is strengthened through joint cyber security exercises that test response capabilities, refine incident management protocols and enhance coordination between stakeholders. The CCSCAP proposes the introduction of a**nnual joint cyber security exercises across CARICOM**, simulating real-world scenarios such as ransomware attacks on critical infrastructure, coordinated phishing campaigns and cross-border data breaches. These exercises will involve national CSIRTs, law enforcement agencies, public sector entities and private sector partners, providing a realistic and comprehensive evaluation of the Region's cyber security readiness.

In addition to regional exercises, the RCFC will collaborate with international partners to organise multilateral cyber drills and workshops. These initiatives will enable CARICOM Member States to learn from global best practices, exchange knowledge with international experts and benchmark their capabilities against international standards.

International capacity building programmes will also be implemented in partnership with organisations such as the Global Forum on Cyber Expertise (GFCE) and the Latin America and Caribbean Cyber Competence Center (LAC4), focusing on developing technical skills, incident response expertise, and legal knowledge within CARICOM. These programmes will ensure that member states have the resources and skills necessary to participate effectively in global cybersecurity efforts.

Regional and international public-private partnerships (PPPs) in cyber security

The role of the private sector is critical in maintaining a secure digital environment, as private companies own and operate a substantial portion of critical infrastructure and digital assets. The CCSCAP promotes the development of public-private partnerships (PPPs) across CARICOM and internationally, encouraging collaboration between governments, private sector entities, and industry associations, possibly to be formalized through the establishment of a regional ISAC (information sharing and analysis centre) in areas such as incident response and threat intelligence.

Through these partnerships, CARICOM Member States will work with technology providers,

telecommunications companies, financial institutions and cyber security firms to strengthen overall regional resilience. The RCFC will facilitate fora and working groups that bring together public and private sector stakeholders to discuss cyber security challenges, share best practices, and develop joint solutions for emerging threats.

In addition, PPPs will provide access to resources, training, and technology for Member States, bridging capacity gaps and enabling smaller countries to leverage private sector expertise in their cybersecurity efforts.

Harmonisation with international cyber security standards

Adopting and aligning with international cyber security and data protection standards is essential for ensuring interoperability, fostering trust, and facilitating cross-border collaboration. The CCSCAP will advocate for the adoption of standards such as the ISO/IEC 27001 for Information Security Management, the NIST Cybersecurity Framework 2.0. These standards provide a unified approach to security practices, legal frameworks and incident management, making it easier for CARICOM to integrate with global cyber security initiatives.

CARICOM Member States will be encouraged to harmonise their cyber security policies, legislation, and technical standards with international frameworks, ensuring consistency in security practices and enhancing the Region's credibility as a secure and compliant digital environment.

The RCFC will provide guidance and resources for member states in implementing these standards, supporting the establishment of regulatory frameworks that align with global norms and promote cyber security resilience across CARICOM.

Mutual legal assistance and international law enforcement collaboration

To effectively combat transnational cybercrime, CARICOM must engage in mutual legal assistance (MLA) and collaborate closely with international law enforcement agencies. The CCSCAP will **establish MLA protocols that facilitate the sharing of digital evidence, enable joint investigations, and expedite extradition requests for cybercriminals**. These protocols will align with international agreements, including the Budapest Convention and the UN Treaty on Cybercrime, ensuring that CARICOM's legal framework supports seamless cooperation with foreign jurisdictions.

In addition to MLA protocols, CARICOM will formalise/further develop relationships with INTERPOL, Europol, and other law enforcement bodies, participating in **joint task forces that target cybercrime networks operating across borders.** These collaborations will enhance CARICOM's investigative capabilities, providing access to resources, intelligence, and specialised expertise from international partners. By building strong relationships with global law enforcement agencies, CARICOM will strengthen its ability to prevent, investigate, and prosecute cybercrime at both regional and international levels.

Cyber diplomacy and international representation

As cyber threats increasingly influence global security and economic stability, CARICOM must **engage actively in international dialogues on cyber security policy, governance and norms, international cooperation on cybercrime**. The CCSCAP promotes cyber diplomacy as a key component of CARICOM's cyber security strategy, encouraging member states to participate in forums such as the United Nations Open-Ended Working Group (OEWG) on Cyber security, the International Telecommunication Union (ITU), and the Global Forum on Cyber Expertise (GFCE). CARICOM will also engage through regional initiatives like the **OAS Working Group on Cooperation and Confidence-Building Measures in Cyberspace (Cyber CBMs)**, in which 13 CARICOM Member States participate to foster transparency and norms of responsible state behaviour online. By speaking with a united voice in such forums and investing in cyber-diplomacy (including dedicated training for Caribbean diplomats in cybersecurity matters), CARICOM can punch above its weight in shaping global cyber governance – ensuring that its regional interests are represented and that its commitments align with hemispheric confidence-building efforts. Through these engagements, CARICOM will have a platform to advocate for its cyber security interests, share regional perspectives, and contribute to the development of global norms for responsible state behaviour in cyberspace.

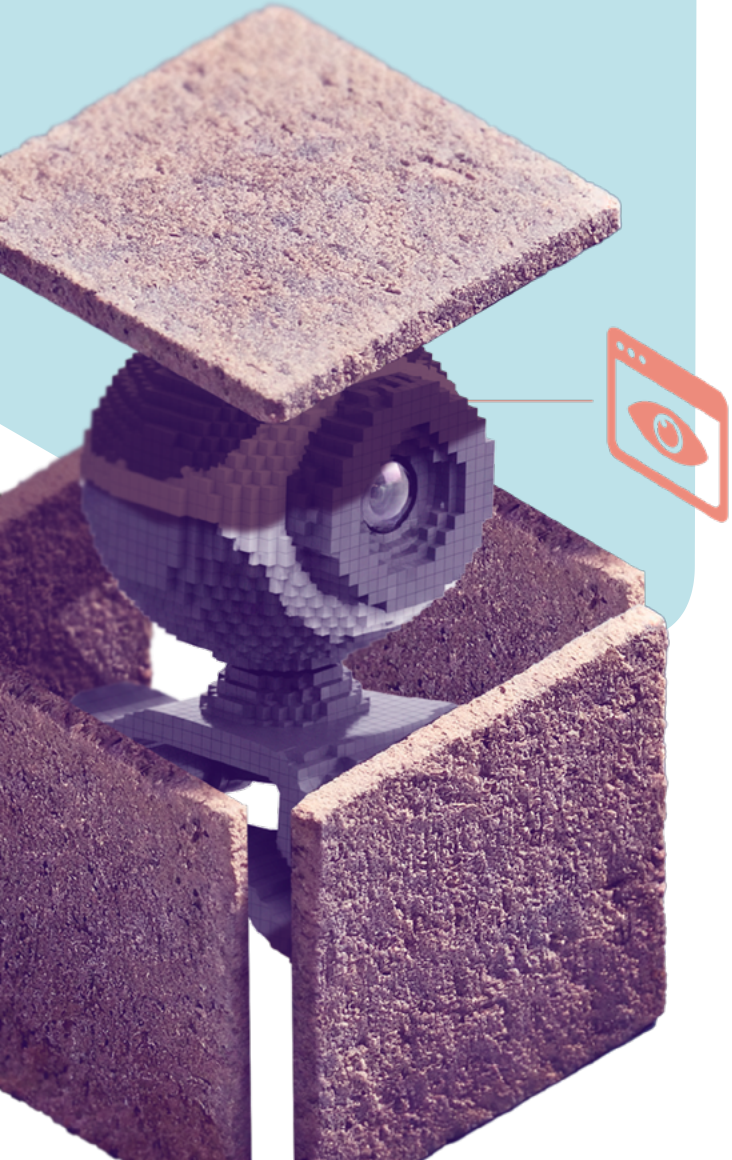
The CCSCAP advocates for the **development of regional positions on emerging issues, such as the application of international law in cyberspace, responsible state behaviour, and norms for the use of artificial intelligence in cyber security.** By establishing a united voice on these issues, CARICOM can play an influential role in advancing a secure and open cyberspace, while ensuring that regional interests are represented on the global stage.

A specific focus should be dedicated to **education and training of the diplomatic bodies of the Caribbean countries**, based on the successful implementation of such initiatives by LAC4 in countries from neighbouring regions, so as to equip officials with sufficient knowledge for an informed participation in the global debates developed in this area.

Summary of the actions in the domain of regional and international cooperation and KPIs

Objectives	Activities	Performance Indicators	1-2 years	2-3 years	3- 5 years
1.Improve regional and international cooperation	1.1.Promoting international agreements, promoting partnerships with international organizations related Cybercrime	1.1.1.At least 2 meetings promoting international agreements		X	
		1.1.2.Signature of, at least, one agreement with a partner institution promoting information sharing			X
		1.1.3. Signature of 1 agreement with a partner institution promoting cybercrime related training delivery			X
2.Development a Cybercrime operational network	2.1.Developing informal operational network for cybercrime investigation and law enforcement.	2.1.1.Establishment of guidelines to facilitate operational international networking	X		
3. Collaboration Public-Private Sector in working group	3.1.Sharing experiences and techniques to enhance the approach to tackling cybercrime	3.1.1. At least 2 per year meetings promoting working groups with private sector stakeholders	X		
		3.1.2. At least, constitution of one working group for best practice sharing		X	
4. Strengthen strategic regional cybersecurity coordination	4.1 Convene an annual CARICOM cybersecurity policy and coordination meeting hosted by RCFC	4.1.1 Annual coordination meeting held and documented (starting 2025)	X	X	X
5. Facilitate Member State participation in global cyber governance processes	5.1 Provide logistical, financial, and diplomatic support to Member States to attend international forums	5.1.1 All Member States represented at least once a year in 3 major forums (starting 2026)		X	X
6. Operationalise regional cyber threat intelligence sharing protocols	6.1 Develop formal regional protocols for threat intelligence sharing, integrated with CSIRTs and global platforms (e.g., FIRST, ITU)	6.1.1 Protocols adopted by 80% of Member States and alerts issued quarterly by 2027	X	X	

MONITORING AND EVALUATION



The success of the CCSCAP depends on a rigorous Monitoring and Evaluation (M&E) framework that measures progress, identifies areas for improvement and ensures alignment with strategic objectives. Given the diverse capabilities, infrastructure and needs of CARICOM Member States, an effective M&E framework is essential to provide data-driven insights that support adaptive management and continuous improvement. This M&E section of the CCSCAP outlines the structure, processes, and tools needed to evaluate the plan's effectiveness, enhance transparency and ensure accountability across all initiatives.

Strategic Objectives

The M&E framework aims to achieve three primary objectives: (1) to establish clear metrics and KPIs that measure the impact and effectiveness of CCSCAP initiatives; (2) to provide a structured approach for assessing implementation progress and identifying gaps across Member States and (3) to support data-driven decision-making by generating actionable insights that inform future revisions of the action plan. By prioritising these objectives, CARICOM will ensure that the CCSCAP remains responsive to emerging threats and evolving regional needs, maximising the plan's long-term impact.

M&E Governance and Roles

The responsibility for monitoring and evaluating the CCSCAP's implementation lies with the RCFC. This unit will operate under the guidance of the C3SC, reporting annually on progress, challenges and recommendations. Each NCO within Member States will appoint a point of contact who liaises with the RCFC to ensure consistent data collection, compliance with reporting standards, and timely submission of performance metrics.

Data Collection and Reporting Mechanisms

To support the M&E framework, the RCFC will implement a centralised data collection platform that aggregates data from member states and provides real-time access to progress metrics. This platform will enable automated data collection where possible, reducing the administrative burden on NCOs and improving data accuracy. NCO points of contact will be responsible for inputting national-level data.

Half yearly reports from each NCO will be compiled into annual progress reports by the RCFC, which will be presented to the CCSC. These reports will include an analysis of KPI trends, a summary of major achievements, and recommendations for addressing any challenges. In addition, an annual public report will be published, providing transparency on the CCSCAP's progress and enhancing accountability to CARICOM's citizens and stakeholders.

Independent Evaluations and Peer Reviews

To ensure objectivity and strengthen accountability, the M&E framework will incorporate independent evaluations and peer reviews. Every three years, CARICOM will conduct an independent evaluation of the CCSCAP, assessing the plan's effectiveness, relevance, and impact on regional cybersecurity resilience. These evaluations will be conducted by external experts in cybersecurity, M&E, and regional policy, providing impartial assessments and recommendations for improvement.

Continuous Improvement Process

The M&E framework is designed to support a continuous improvement process, ensuring that the CCSCAP remains responsive to new challenges and opportunities. Based on the insights generated through M&E activities, the RCFC will implement an adaptive management approach that allows for real-time adjustments to strategies, resource allocation, and action plan objectives. This process includes:

1. Annual KPI Review and Adjustment: KPIs will be reviewed and, if necessary, revised annually to align with evolving cybersecurity goals, emerging threats, and changes in CARICOM's digital landscape.
2. Mid-Cycle Adjustments: In response to significant shifts in the cybersecurity environment, the RCFC will conduct mid-cycle reviews and recommend adjustments to CCSCAP initiatives, resource allocation, or specific action items. This adaptability ensures that CARICOM remains proactive and resilient against emerging threats.
3. Feedback Loops with Stakeholders: Regular feedback loops will be established with NCOs, the Advisory Council on Cybersecurity and Cybercrime (ACCC) – if established, and other stakeholders to gather input on M&E findings. This feedback will inform adjustments to the CCSCAP, ensuring that member states' needs and challenges are addressed effectively.

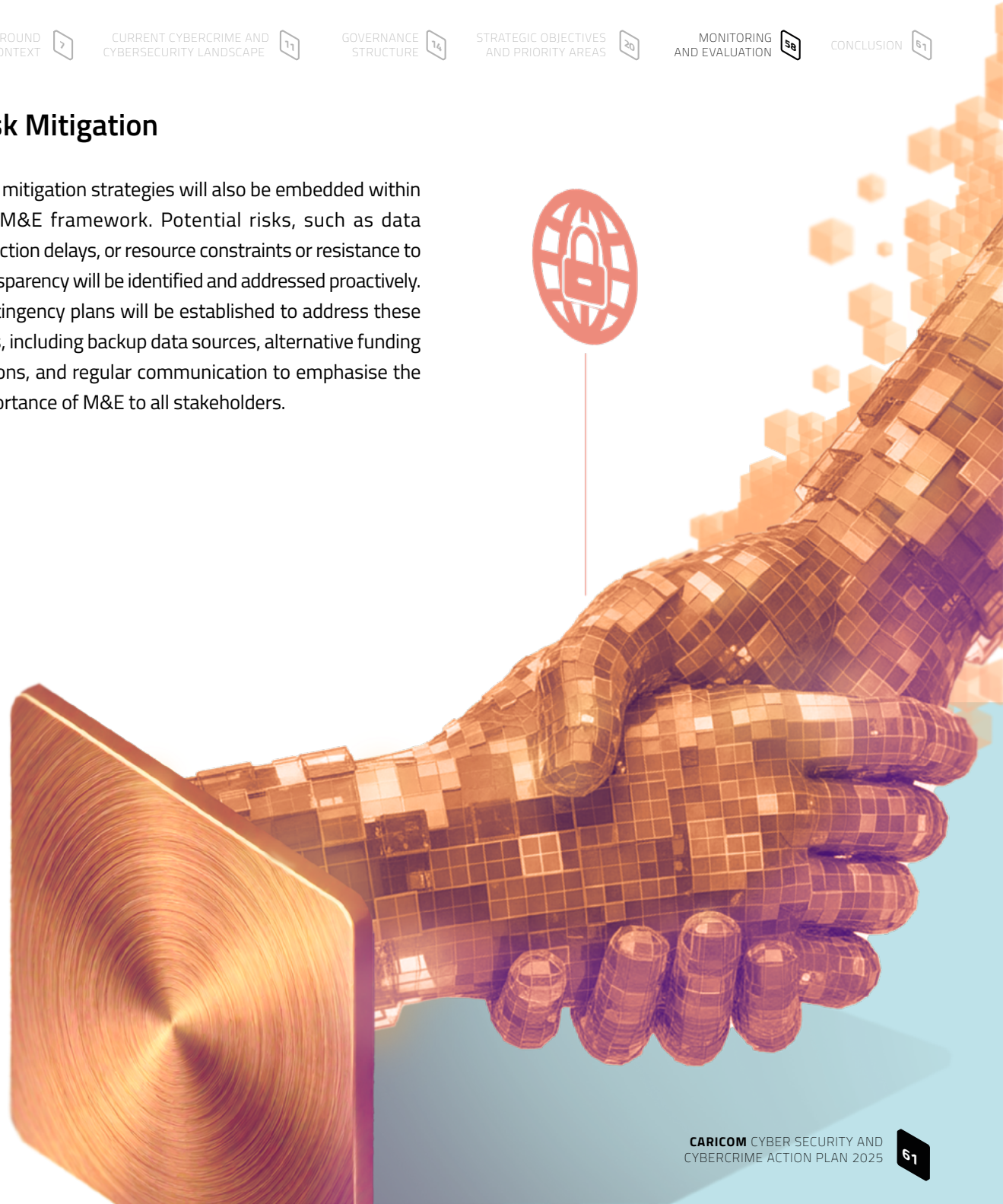
Public Transparency and Stakeholder Engagement

Transparency is a core principle of the M&E framework, ensuring that CARICOM's citizens, partners, and stakeholders have visibility into the CCSCAP's progress and impact. Annual public reports will be issued to summarise key achievements, performance against KPIs, and areas for improvement. These reports will be accessible through CARICOM's website and will include infographics, success stories, and regional data on cybersecurity trends. Notably, the content of publicly disseminated material will have to be vetted to ensure that critical information is not shared with threat actors in the process of informing citizens.

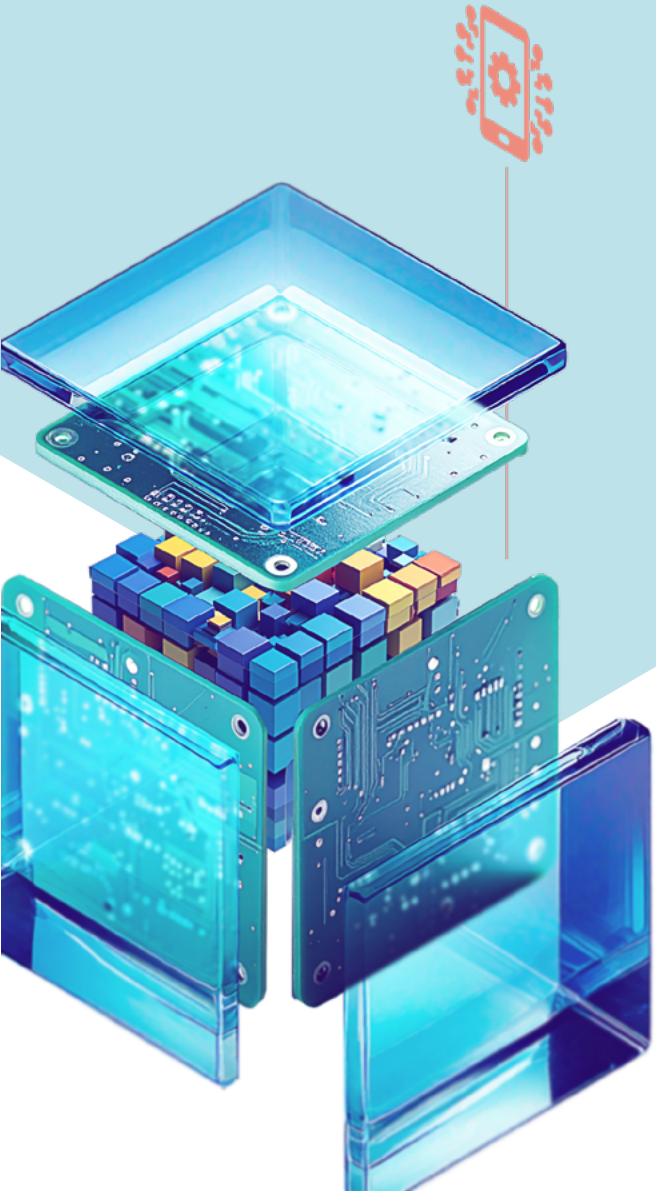
Stakeholder engagement will be maintained through public forums and workshops that invite feedback, share updates, and provide education on cybersecurity initiatives. By actively engaging with the public and stakeholders, CARICOM will foster trust, promote awareness, and encourage community involvement in its cybersecurity efforts.

Risk Mitigation

Risk mitigation strategies will also be embedded within the M&E framework. Potential risks, such as data collection delays, or resource constraints or resistance to transparency will be identified and addressed proactively. Contingency plans will be established to address these risks, including backup data sources, alternative funding options, and regular communication to emphasise the importance of M&E to all stakeholders.



CONCLUSION



The CCSCAP establishes a comprehensive framework to secure the Region's digital landscape, safeguard critical infrastructure, and strengthen cyber resilience across CARICOM Member States. By prioritising a structured approach with clearly defined goals, timelines and collaborative frameworks, the CCSCAP addresses both current cyber security needs and emerging challenges posed by increasingly sophisticated cyber threats.

This action plan lays out strategic initiatives in public awareness, incident response, legal harmonisation, risk management, capability building, technical standards and regional and international cooperation. Each priority area is supported by specific goals and measurable indicators, ensuring that progress can be tracked, evaluated, and continuously improved. The establishment of the RCFC, NCOs, developing informal operational network for cybercrime investigation and law enforcement, and a robust Monitoring and Evaluation (M&E) framework will provide CARICOM with the operational infrastructure needed to coordinate, implement, and refine cybersecurity efforts effectively.

In implementing the CCSCAP, CARICOM recognises the importance of fostering a collaborative environment that brings together national governments, regional entities, the private sector, academia and international partners. This CCSCAP emphasises the value of partnerships, both within the Caribbean and with global stakeholders, as vital to achieving a secure digital ecosystem. By aligning with international standards and participating actively in global cyber security forums and best practices against cybercrime, CARICOM Member States not only enhance regional security but also contribute to a more secure global cyberspace.

The CCSCAP's commitment to transparency and public engagement further reinforces its foundation. Annual public reporting, stakeholder consultations, and feedback mechanisms will ensure that CARICOM's cyber related issues (cyber security and cybercrime) efforts remain accountable, accessible and attuned to the needs of its citizens.

As CARICOM embarks on this five-year journey, the CCSCAP provides a roadmap for building a digitally resilient Caribbean, capable of withstanding cyber threats while fostering economic growth, innovation and public trust in digital systems. By adhering to the milestones, responsibilities, and standards outlined within this plan, CARICOM Member States will strengthen their collective cyber security and cybercrime posture, creating a safer, more prosperous future for the Region.