COMPUTER FORENSICS AND SECURITY INSTITUTE

[CFSI]

SERVICE CATALOGUE

2026

Cybersecurity • Risk Management • Digital Forensics • AI • Training

#EverythingCyber #EverythingIT #OnlyAtCFSI

www.CFSI.co | 868-684-0029 | info@CFSI.co

Contents

1 / SECTION

About CFSI

Established in 2011, the Computer Forensics and Security Institute (CFSI) is a Caribbean-headquartered cybersecurity firm with over 15 years of demonstrated experience serving small and medium businesses, large enterprises, banking and financial institutions, insurance companies, law firms, and government agencies across the Caribbean, Latin America, and North America.

We specialize in offensive and defensive cybersecurity disciplines including Vulnerability Assessments, Penetration Testing, Digital Forensics and Incident Response (DFIR), Dark Web and Threat Intelligence, Governance & Risk Consultancy, Network Infrastructure Engineering, and Advanced Cybersecurity Training. Our team operates as a full-spectrum Purple Team, blending Red Team offensive techniques with Blue Team defensive expertise to provide a complete view of your security posture.

CFSI's approach combines globally recognized methodologies with deep regional understanding. We are uniquely positioned as the only EC-Council Accredited Training Centre (ATC) in the Caribbean, the only firm in the region producing a dedicated annual CARICOM Ransomware Report, and home to the Caribbean's only Certified EC-Council Instructor (CEI). Our work has been trusted by central-bank-regulated financial institutions, regional insurance leaders, government ministries, and international firms operating in the Caribbean.

15+	60+	4	1st
YEARS IN MARKET	THREAT GROUPS MONITORED	PUBLISHED BOOKS	EC-COUNCIL ATC IN CARIBBEAN

02 / SECTION

Vision, Mission & Values

Our Vision

To be the Caribbean and Latin America's most trusted strategic partner in cybersecurity and digital forensics — evolving alongside our clients in a rapidly changing threat landscape, and setting the regional benchmark for technical excellence, ethical practice, and operational impact.

Our Mission

To raise the standard of cybersecurity services across the Caribbean by combining world-class technical capability with practical, business-aligned advisory. We don't just deliver assessments — we build security programs that protect what matters, demonstrate compliance, and create lasting resilience for our clients.

Our Core Values

INTEGRITY & CONFIDENTIALITY

Every engagement is grounded in strict confidentiality, ethical practice, and verifiable competence. We follow rigorous data-handling and chain-of-custody standards, and we never disclose client information beyond agreed contact points.

TAILORED SERVICE

No two organizations face the same risk profile. Every assessment, policy, and remediation plan we deliver is calibrated to the client's industry, regulatory context, technical maturity, and operational reality.

TECHNICAL EXCELLENCE

Our consultants hold globally recognized certifications across offensive, defensive, and governance disciplines. We invest continuously in methodology, tooling, and research to stay at the forefront of regional and international threats.

LONG-TERM PARTNERSHIP

We measure success not by individual reports delivered, but by the security maturity our clients build over time. Many of our relationships span multiple years and multiple engagement types, from penetration testing to vCISO advisory.

03 / SECTION

Why CFSI

What sets us apart from other cybersecurity providers in the region:

- **Only EC-Council Accredited Training Centre (ATC) in the Caribbean.** We are the sole authorized provider for the world's most recognized cybersecurity certification stack including CEH, CHFI, CCISO, CND, CTIA, CSA, and ECIH.
- **Only Certified EC-Council Instructor (CEI) in Trinidad & Tobago.** Our director and senior trainer is the only CEI in the country, qualified to deliver certification training across the entire EC-Council portfolio.
- **Published authority on Digital Forensics and Penetration Testing.** Our director has authored four (4) books with international tech publisher Packt Publishing, sold globally via Amazon and Packt with over £100,000 in cumulative sales.
- **The Caribbean's only annual Ransomware Threat Intelligence Report.** CFSI produces the only dedicated CARICOM Ransomware Report covering attacks on regional institutions — a publicly available resource trusted by IT leaders across the region.
- **Active monitoring of 60+ ransomware leak sites and dark web forums.** We maintain continuous visibility into the threat actor ecosystem most likely to target Caribbean organizations, providing early warning and exposure intelligence.
- **Demonstrated CBTT (Central Bank of Trinidad & Tobago) alignment experience.** We have helped multiple regulated financial institutions align with CBTT cybersecurity guidelines, including credit unions, insurance brokers, and banks.
- **Full Purple Team capability under one roof.** Red Team offensive testing, Blue Team defensive engineering, governance, training, and forensics — delivered by a single coordinated team rather than fragmented across vendors.
- **End-to-end assess-and-remediate capability.** From the first scoping conversation through technical assessment, governance documentation, and infrastructure remediation — we close the loop in a single coordinated engagement rather than handing you off between vendors.

04 / SECTION

Subject Matter Expertise

CFSI is led by Shiva V. N. Parasram, an Enterprise Risk and Cybersecurity Consultant with more than two decades of experience across financial services, energy, technology, and government sectors. He holds an MSc in Network Security with Distinction from Anglia Ruskin University (UK) and is the Caribbean's only Certified EC-Council Instructor.

Active Engagements & Affiliations

- **CIBC FCIB —** Enterprise Risk and InfoSec Consultant, responsible for project Threat Risk Assessments (TRA), Information Security Assessments (ISA), and Penetration Testing reports.
- **Springboard (California, USA) —** Cybersecurity Mentor, guiding mentees through industry-grade curriculum since 2021.
- **Packt Publishing —** Information Security Author and Technical Reviewer, contributing to titles on firewalls, networking, and penetration testing.
- **ITAC / Ministry of National Security (T&T) —** Curriculum developer and trainer for Critical Infrastructure Security under the Integrated Threat Assessment Centre, in partnership with UWI St. Augustine.

Published Works

Our director's publications have been distributed worldwide through Packt and Amazon, with cumulative sales exceeding £100,000:

- **Digital Forensics with Kali Linux — 3rd Edition** — ISBN *978-1837635153 (2023)*
- **Digital Forensics with Kali Linux — 2nd Edition** — ISBN *978-1838640804 (2020)*
- **Kali Linux 2: Assuring Security by Penetration Testing — 4th Edition** — ISBN *978-1838640804 (2018)*
- **Digital Forensics with Kali Linux — 1st Edition** — ISBN *978-1788625005 (2017)*

Selected Certifications

CCISO Certified Chief Information Security Officer (2026)	**CEI** Certified EC-Council Instructor (2026)	**CEH** Certified Ethical Hacker v13 (2026)
CHFI Computer Hacking Forensic Investigator v11 (2026)	**CRAGE** Certified Responsible AI Governance & Ethics (2026)	**CAIPM** Certified AI Program Manager (2026)
CTIA Certified Threat Intelligence Analyst	**CND** Certified Network Defender	**CSA** Certified SOC Analyst (2026)
ECIH EC-Council Certified Incident Handler (2026)	**ECES** EC-Council Certified Encryption Specialist (2026)	**ICS/SCADA** ICS/SCADA Cybersecurity (2026)
ECSA EC-Council Certified Security Analyst	**ACE** AccessData Certified Examiner	**ISC2 CC** Certified in Cybersecurity
CCNA Cisco Certified Network Associate	**MCSA** Microsoft Certified Systems Administrator	**CompTIA** Network+, Security+, A+, CTT+

05 / SECTION

Our Service Pillars

CFSI organizes its capability across seven integrated service pillars. Most engagements draw on multiple pillars — for example, a financial-sector client may engage us for penetration testing (Pillar 1), dark web monitoring (Pillar 2), CBTT-aligned governance support (Pillar 4), AI governance advisory (Pillar 7), and quarterly awareness training under a single coordinated relationship.

I

Cybersecurity Assessment & Testing

Vulnerability Assessments, Penetration Testing (Internal, External, Web App), Phishing Campaigns, Firewall Analysis, Network Audits.

II

Threat Intelligence & Monitoring

Dark Web Reconnaissance, Data Leak Monitoring, Threat Intelligence, Ransomware Tracking, Brand & Credential Exposure.

III

Incident Response & Digital Forensics

Cyber Triage, DFIR Investigations, Evidence Handling, Incident Response Planning, Data Recovery, Threat Hunting.

IV

Governance, Risk & Compliance

vCISO Services, Policy Development, CBTT Alignment, NIST/ISO/CIS Frameworks, Third-Party Risk, Risk Registers.

V

Network Infrastructure & Security Engineering

Firewall & WAF Deployment, Network Architecture, VLAN Segmentation, Structured Cabling, Wireless, QoS, Zero Trust.

VI

Specialized Services

TSCM (Surveillance Countermeasures), ICS/SCADA & Operational Technology (OT) Security, Encryption & Cryptographic Services.

VII

AI Governance, Ethics & Security

AI Risk Assessment, Responsible AI Frameworks, AI Program Management, Ethical AI Audits, AI Security Testing, AI Strategy Consultancy.

PILLAR I CYBERSECURITY ASSESSMENT & TESTING

Identify, validate, and prioritize the technical vulnerabilities that present the greatest business risk to your organization. Our assessments combine automated discovery with manual exploitation to give you actionable findings — not just scanner output.

- **Vulnerability Assessments —** Authenticated and unauthenticated scanning across internal and external assets, mapped to CVSS scoring, asset criticality, and exploit availability.
- **External Penetration Testing —** Controlled testing of internet-facing infrastructure including websites, portals, public IPs, and cloud instances, with safe exploit validation.
- **Internal Penetration Testing —** Lateral movement, privilege escalation, and segmentation testing from an insider-threat or post-compromise perspective.
- **Web Application Penetration Testing —** OWASP Top 10 / API Top 10 aligned testing, including authentication, session, access control, injection, and business logic flaws.
- **Non-Disruptive Guided Testing —** Specialized engagement type designed for legacy or sensitive infrastructure, validating exploitability without service interruption.
- **Phishing Campaigns —** Targeted social engineering simulations to measure user susceptibility and validate awareness training effectiveness.
- **Firewall Configuration Review —** Rule-base analysis, NAT/VPN review, management-plane hardening, and exposed-services validation against international best practices.
- **Network Infrastructure Audit —** Topology, segmentation, switch/router/wireless baseline review, and documentation of administrative access paths.
- **Threat Modelling —** Hypothetical-but-realistic attack-scenario development based on your discovered gaps, control weaknesses, and configuration drift.
- **Retesting Services —** Targeted re-validation of remediated findings to confirm risk reduction and close out critical and high-severity issues.

PILLAR II THREAT INTELLIGENCE & MONITORING

See your organization the way attackers see it. CFSI maintains active visibility into the criminal ecosystem most relevant to Caribbean and CARICOM organizations — including ransomware leak sites, credential markets, and dark web forums where company data is traded.

- **Dark Web Reconnaissance —** Active scanning of forums, ransomware leak pages, underground marketplaces, and information-selling portals for references to your domains, brands, executives, and assets.
- **Continuous Dark Web Monitoring —** Daily, weekly, or monthly monitoring against agreed scope, with verified-exposure alerting and recommended response actions.
- **Leaked Credential Monitoring —** Detection of exposed employee email/password combinations across breach databases and credential-stuffing lists.
- **Data Leak & Breach Detection —** Identification of leaked internal documents, payment-related data, customer records, and brand/identity misuse.
- **Ransomware Group Tracking —** Active monitoring of 60+ ransomware leak sites with regional impact analysis and early-warning intelligence on Caribbean-focused threat actors.
- **Threat Intelligence Reports —** Periodic threat awareness reports tailored to your industry, regulatory context, and threat landscape.
- **CARICOM Ransomware Report —** Clients receive direct access to our annual CARICOM Ransomware Report — the only Caribbean-focused ransomware threat publication of its kind.
- **Brand & Identity Monitoring —** Detection of typosquatting, domain impersonation, fake social profiles, and brand misuse targeting your customers and staff.
- **Verified Exposure Alerting —** We separate signal from noise: every alert delivered is validated by a CFSI analyst before reaching you, with response playbooks for confirmed exposures.

PILLAR III INCIDENT RESPONSE & DIGITAL FORENSICS (DFIR)

When a breach is suspected or confirmed, the first 72 hours determine outcomes. CFSI delivers rapid, evidence-based response that prioritizes containment, evidence preservation, and clear decision-making for executive teams.

- **Cyber Triage & Rapid Response —** Evidence-based assessment to determine whether active compromise is present, scoped to give decision-makers clarity within days, not weeks.
- **Digital Forensics Investigations —** Full forensic acquisition and analysis of endpoints, servers, mobile devices, and cloud workloads, with chain-of-custody documentation suitable for legal proceedings.
- **Incident Response Planning —** Development and tabletop testing of incident response plans, runbooks, and escalation procedures aligned to your operating model.
- **DFIR Framework Development —** Building of organizational DFIR capability including roles, tooling recommendations, evidence-handling procedures, and retention policies.
- **Containment Recommendations —** Immediate, prioritized actions for credential resets, isolation, blocking, and hardening — designed to minimize business disruption.
- **Indicator of Compromise (IOC) Analysis —** Identification of persistence mechanisms, lateral movement signals, and recommended detection rules for ongoing monitoring.
- **Data Recovery & Restoration Advisory —** Practitioner-led guidance through ransomware recovery, backup validation, and restoration sequencing.
- **Threat Hunting —** Proactive search across telemetry (firewall, AD, EDR, DNS) for high-risk indicators including suspicious admin activity, unusual outbound traffic, and failed-login spikes.
- **Post-Incident Review & Reporting —** Executive-grade reporting with technical evidence, root cause analysis, and a prioritized remediation roadmap.
- **Memory & Malware Analysis —** Quarterly sampling of critical infrastructure server RAM for ransomware detection and benchmark analysis (offered as part of vCISO retainers).

PILLAR IV GOVERNANCE, RISK & COMPLIANCE (GRC)

Sustainable security is built on policies that are understood, controls that are owned, and risks that are tracked. CFSI's GRC practice translates technical findings into governance structures, board-level reporting, and audit-ready documentation.

- **vCISO Services —** On-demand executive cybersecurity leadership combining the roles of CISO, Risk Manager, and Security Consultant — delivered by the Caribbean's only Certified CCISO Instructor.
- **Enterprise Cybersecurity Strategy —** Multi-year security roadmap aligned to your business objectives, regulatory environment, and risk appetite.
- **Information Security Policy Development —** Drafting, updating, and maintenance of policies, standards, and procedures based on international NIST frameworks.
- **CBTT Cybersecurity Guideline Implementation —** End-to-end alignment with Central Bank of Trinidad & Tobago cybersecurity guidelines for regulated financial institutions including governance, risk management, awareness, and BCDR.
- **Risk Register Development —** Building and operationalizing risk registers for compliance, patch management, and vulnerability programme oversight.
- **Third-Party / Vendor Risk Assessments —** Formal Information Security Assessment (ISA) processes for evaluating vendor security posture before procurement and on an ongoing basis.
- **Threat Risk Assessments (TRA) —** Project-level risk assessments aligned to organizational risk frameworks, including residual risk scoring and treatment recommendations.
- **PCI DSS Alignment —** Quarterly Internal (11.2.1) and unofficial External (11.2.2) PCI DSS scanning and gap-analysis advisory.
- **Business Continuity & Disaster Recovery —** Development of IT Systems Recovery Objectives (RTO/RPO), data backup strategies, and BCDR test plans.
- **Framework Alignment —** Practical, audit-ready alignment to NIST CSF 2.0, ISO/IEC 27001, CIS Critical Security Controls v8, COBIT, and PCI DSS.
- **Board & Executive Reporting —** Translation of technical findings into board-ready risk reporting, with KPIs, control maturity scoring, and remediation milestones.
- **Regulatory & Audit Readiness —** Preparation for cyber insurance underwriting reviews, regulator inquiries, and external audits.

PILLAR V NETWORK INFRASTRUCTURE & SECURITY ENGINEERING

Findings without remediation create risk registers — not security improvements. CFSI's engineering practice provides the design, implementation, and configuration capability to translate assessment outcomes into deployed controls.

- **Next-Generation Firewall (NGFW) Deployment —** Design, deployment, and tuning of enterprise firewalls (Sophos XGS, Fortinet FortiGate, and others) including IPS/IDS, AV, deep packet inspection, and TLS inspection.
- **Web Application Firewall (WAF) Implementation —** Reverse-proxy or appliance-based WAF deployment with OWASP Core Rule Set, virtual patching, rate limiting, bot mitigation, and DDoS protections.
- **Network Architecture Design —** Star-topology redesigns, core/aggregation/access tiering, server connectivity, and 10G/40G backbone deployment for performance-bound environments.
- **VLAN Segmentation & Zero Trust —** VLAN design, inter-VLAN routing, segmentation enforcement, and Zero Trust Architecture review including identity-based access controls.
- **WAN Load Balancing & High Availability —** Multi-ISP aggregation, WAN load balancing, automatic failover, and policy-based routing for business-critical services.
- **Structured Cabling & Certification —** TIA/EIA-aligned copper and fiber installation, link certification (NEXT/PSNEXT, attenuation, return loss, wiremap), and remediation reporting.
- **Inter-Building Fiber Backbone —** ADSS OS2 fiber installation, fiber cassette deployment, optical testing, certification, and patch-cable fabrication.
- **Wireless Design & Hardening —** WPA3-Enterprise/PSK design, RF tuning, captive portals for guest access, controller hardening, and rogue-AP detection.
- **Switching & Access Layer Configuration —** Switch baseline configuration (AAA, SNMP, NTP, STP), LAGs, 802.1X, and centralized management via UniFi Controller or equivalent.
- **QoS & Traffic Prioritization —** Quality of Service policies for VoIP, database, and critical-application traffic, with backend load management and congestion-point elimination.
- **Server & Endpoint Connectivity Optimization —** 10G NIC bonding (LACP), structured-cabling rewiring of bottlenecked endpoints, and access-layer redesign for performance-bound services.

- **Network Topology Documentation —** Top-down logical and physical network diagrams, IP addressing schemes, and as-built configuration documentation.
- **Post-Implementation Hypercare & Support —** Active monitoring during the first week post-rollout, fine-tuning of policies, warranty and support periods (typically 90 days to 6 months depending on engagement).
- **Managed Network Monitoring —** SNMP-based monitoring of firewalls, switches, and access points, with proactive alerts and quarterly health checks.

PILLAR VI SPECIALIZED SERVICES

CFSI delivers specialized capabilities that extend beyond traditional IT cybersecurity — including counter-surveillance, industrial control system protection, and cryptographic security. These services address the physical, operational, and data-protection dimensions that standard assessments often miss.

- **Technical Surveillance Countermeasures (TSCM) —** Professional sweeps to detect unauthorized technical surveillance risks in agreed areas, conducted with discretion and full chain-of-custody documentation.
- **Physical Inspection —** Controlled inspection of meeting rooms, executive offices, and sensitive operational areas for suspicious devices, tampering indicators, and concealed hardware.
- **RF Spectrum Analysis —** Detection of hidden transmitters, unauthorized wireless transmitters, and anomalous RF activity using professional spectrum-analysis equipment.
- **Executive Boardroom Sweeps —** Pre-meeting and routine sweeps of board-level meeting spaces, with confidential findings reporting and procedural mitigation.
- **ICS/SCADA & Operational Technology (OT) Security —** Security assessment of Industrial Control Systems and SCADA environments for critical infrastructure, energy, manufacturing, and utilities. Includes Purdue Model architecture review, IEC 62443 alignment, OT network segmentation analysis, and identification of IT/OT convergence risks.
- **OT Threat Landscape Assessment —** Evaluation of threat vectors specific to industrial environments including PLC/HMI vulnerabilities, legacy protocol weaknesses (Modbus, DNP3, OPC), remote access exposure, and supply-chain risks.
- **ICS Incident Readiness —** Development of OT-specific incident response plans, tabletop exercises, and recovery procedures that account for safety-instrumented systems and physical process risks.
- **Encryption & Cryptographic Security —** Review and advisory on implementation of encryption standards across data at rest, data in transit, and data in use. Includes PKI architecture assessment, certificate lifecycle management, cryptographic protocol evaluation (TLS, IPsec, S/MIME), and compliance with data protection requirements.
- **Cryptographic Risk Assessment —** Identification of weak or deprecated cipher suites, insecure key management practices, and preparation for post-quantum cryptographic migration.

PILLAR VII AI GOVERNANCE, ETHICS & SECURITY

As organizations adopt artificial intelligence across decision-making, customer service, risk management, and operations, the governance, ethical, and security implications demand specialist attention. CFSI's AI practice — led by professionals holding the CRAGE (Certified Responsible AI Governance & Ethics) and CAIPM (Certified AI Program Manager) certifications — provides the structured advisory, assessment, and implementation services that boards, regulators, and stakeholders expect.

- **AI Governance Framework Development —** Design and implementation of organizational AI governance structures aligned to international standards including the NIST AI Risk Management Framework (AI RMF), ISO/IEC 42001 (AI Management Systems), and the EU AI Act classification methodology. Covers roles, oversight committees, decision rights, and escalation protocols.
- **Responsible AI Risk Assessment —** Systematic identification and evaluation of AI-specific risks across your deployed and planned AI systems, including bias and fairness risks, explainability gaps, data quality issues, model drift, adversarial vulnerabilities, and unintended outcomes.
- **Ethical AI Audits —** Independent assessment of AI systems against ethical principles, regulatory expectations, and organizational values. Includes bias detection and fairness testing across protected characteristics, transparency and explainability reviews, accountability mapping, and documentation of AI decision-making processes.
- **AI Security Testing —** Adversarial testing of AI/ML systems to identify vulnerabilities including prompt injection, data poisoning, model extraction, evasion attacks, and privacy leakage. Covers both internally developed models and third-party AI tools adopted by the organization.
- **AI Program Strategy & Roadmap —** Strategic advisory for organizations planning or scaling AI initiatives, including use-case prioritization, build-vs-buy analysis, vendor assessment frameworks, ROI modelling, and phased implementation planning with governance gates.
- **AI Vendor & Third-Party Risk Assessment —** Evaluation of AI vendors, SaaS-embedded AI features, and third-party AI tools for security posture, data handling practices, model transparency, bias disclosures, and contractual risk allocation. Includes supply-chain risk analysis for AI components.
- **AI Policy & Standards Development —** Creation of organizational AI usage policies, acceptable-use standards, data governance standards for AI training data, model lifecycle management procedures, and AI incident response protocols.

- **AI Regulatory Compliance Advisory —** Guidance on alignment with emerging AI regulations and frameworks including the EU AI Act risk classification, NIST AI RMF functions (Govern, Map, Measure, Manage), sector-specific AI guidance from financial and data protection regulators, and privacy considerations under GDPR/CCPA as they apply to AI systems.
- **AI Awareness & Training —** Executive, board, and staff training on responsible AI use, AI risk awareness, prompt security, deepfake detection, and organizational AI policies. Includes role-based training for developers, procurement, legal, and business-unit leaders.
- **AI Incident Response —** Preparation and advisory for AI-specific incidents including model failures, bias incidents, data contamination, adversarial exploitation, and regulatory inquiries related to AI decision-making.

06 / SECTION

Advanced Cybersecurity & AI Training

CFSI is the only EC-Council Accredited Training Centre (ATC) in the Caribbean, delivered by the only Certified EC-Council Instructor (CEI) in Trinidad. We deliver internationally accredited certification training to corporate, government, and individual learners, both as scheduled cohorts and as customized in-house programs. In 2026, we expanded our portfolio to include AI governance, ICS/SCADA, and advanced encryption certifications.

Internationally Accredited Certifications

CEH v13 Certified Ethical Hacker (2026)	**CCISO** Certified Chief Information Security Officer (2026)	**CHFI v11** Computer Hacking Forensic Investigator (2026)
CRAGE Cert. Responsible AI Governance & Ethics (2026)	**CAIPM** Certified AI Program Manager (2026)	**CND** Certified Network Defender
CSA Certified SOC Analyst (2026)	**CTIA** Certified Threat Intelligence Analyst	**ECIH** EC-Council Certified Incident Handler (2026)
ECES EC-Council Certified Encryption Specialist (2026)	**ICS/SCADA** ICS/SCADA Cybersecurity (2026)	**NSE** Fortinet Network Security Engineer
CCNA Cisco Certified Network Associate	**Net+** CompTIA Network+	**Sec+** CompTIA Security+
Pen+ CompTIA Pentest+		

Corporate Awareness & Role-Based Training

- **Enterprise Cybersecurity Awareness Training —** Tailored training programs for staff, managers, and executives covering phishing, social engineering, password hygiene, and incident reporting.
- **AI Risk & Responsible Use Training —** Executive, board, and staff training on responsible AI adoption, AI risk awareness, prompt security, deepfake detection, and organizational AI governance policies. Tailored for developers, procurement, legal, and business-unit leaders.
- **ICS/SCADA Security Awareness —** Specialized training for operators, engineers, and IT staff working in industrial, energy, or critical infrastructure environments — covering OT-specific threats, safety implications, and incident reporting.
- **Role-Based Information Security Training —** Targeted curriculum for IT staff, finance, customer service, and other risk-relevant roles, delivered virtually or on-site.
- **Quarterly Awareness Programs —** Recurring awareness training delivered as part of vCISO retainers, with completion certificates and reporting.
- **Executive & Board-Level Briefings —** Targeted briefings for senior leadership on threat landscape, AI governance, regulatory expectations, and cyber risk governance.
- **Custom Curriculum Development —** Curriculum design for cybersecurity and AI academies, postgraduate programs, and vendor training initiatives — with proven track record at COSTAATT, UWI, and the Ministry of National Security (ITAC).
- **CFSI CyberFence Initiative —** Free public webinars and workshops with completion certificates, supporting cybersecurity literacy across the Caribbean. Recordings available on the CFSI YouTube channel.

07 / SECTION

CBTT Cybersecurity Guideline Implementation

Regulated financial institutions in Trinidad and Tobago — including credit unions, insurance companies, brokers, and licensed financial entities — are required to align with the Central Bank of Trinidad and Tobago (CBTT) Cybersecurity Best Practice Guidelines. CFSI has supported multiple regulated entities through this alignment, combining technical assessments with governance documentation.

A. Governance

- **Formal Cybersecurity Strategy Development —** Identification, protection, detection, response, and recovery program design, with policies, procedures, and standards aligned to CBTT expectations.
- **Strategy Implementation & Oversight —** Ongoing oversight of cybersecurity strategy execution, with measurable outcomes and reporting cadences appropriate to board and regulator expectations.

B. Risk Management

- **Risk & Incident Management Frameworks —** Building of formal risk and incident management frameworks to identify cybersecurity threats and vulnerabilities across all IT aspects of the organization.
- **Risk Register & Treatment Plans —** Operational risk registers with treatment plans, owners, and timelines that satisfy regulatory documentation expectations.

C. Awareness and Training

- **Tailored Awareness Programs —** Awareness training tailored to managers, IT staff, and front-line employees, with role-specific content and completion tracking.
- **Customer Education —** Materials and programs to educate customers on safe use of online services, privacy protections, and reporting suspicious activity.

D. Business Continuity & Disaster Recovery

- **IT Systems Recovery Objectives —** Development and validation of Recovery Time Objectives (RTO), Recovery Point Objectives (RPO), and data backup strategies aligned to business criticality.
- **Regular Vulnerability Assessment —** Recurring assessment of IT assets for security vulnerabilities and exploits, supporting CBTT's expectation of ongoing technical risk visibility.

08 / SECTION

Frameworks & Standards Alignment

Every CFSI engagement is grounded in internationally recognized methodologies and standards. We do not invent frameworks — we apply, adapt, and document the ones that matter to your auditors, regulators, and insurers.

NIST CSF 2.0	PCI DSS	ISO/IEC 27001
CIS Controls v8	OWASP Top 10	NIST 800-115
COBIT	OSSTMM v3	TIA/EIA
NIST AI RMF	ISO/IEC 42001	EU AI Act
IEC 62443	NERC CIP	Purdue Model

How We Apply These

- **PCI DSS —** Aligned to requirements 11.2.1 (internal penetration testing) and 11.2.2 (external penetration testing) for clients handling payment card data.
- **NIST 800-115 —** The foundation of our information security testing methodology, covering planning, discovery, attack, and reporting phases.
- **NIST Cybersecurity Framework (CSF) —** Used for governance engagements, vCISO advisory, and broader risk management programs across industries.
- **CIS Critical Security Controls v8 —** Applied for posture-questionnaire engagements, control-maturity scoring, and prioritized remediation roadmaps.
- **OWASP Top 20 / API Top 10 —** The reference for all web application and API penetration testing engagements.
- **COBIT —** Used in IT governance and audit-readiness engagements where alignment of IT processes with organizational goals is required.
- **OSSTMM v3 —** Provides the scientific foundation for operational security testing where measurable, repeatable methodology is essential.

- **ISO/IEC 27001 —** Applied when developing Information Security Management System (ISMS) controls, policies, and Statements of Applicability.
- **NIST AI RMF —** The Govern, Map, Measure, and Manage functions applied across AI governance engagements, ethical AI audits, and AI risk assessments.
- **ISO/IEC 42001 —** The emerging standard for AI Management Systems, applied when building organizational AI governance structures and documentation.
- **EU AI Act Classification —** Risk-tier classification methodology used when helping clients categorize AI systems and determine proportionate governance obligations.
- **IEC 62443 / NERC CIP —** Industrial control system security standards applied for ICS/SCADA assessments, OT network segmentation, and critical infrastructure protection engagements.

09 / SECTION

Selected Client Listing

CFSI is trusted by multi-million-dollar organizations across the financial, insurance, government, technology, energy, legal, and education sectors. Due to confidentiality obligations under our Non-Disclosure Agreements, only the clients explicitly approved for reference are listed below — engagement details are not disclosed for any client.

TRUSTED BY LEADING ORGANIZATIONS		
▪ Government of Barbados (MIST)	▪ CIBC (Barbados & Canada)	▪ iGov Trinidad (T&T Government)
▪ NPICTT (National Payment & Innovation Company of T&T)	▪ NIS Grenada	▪ British Virgin Islands (BVI) Airport Authority/ Digicel
▪ NAGICO Insurance Limited	▪ Maritime Financial Group	▪ Fujitsu Caribbean (T&T and Jamaica)
▪ Sheppard Securities Limited	▪ Unipet	▪ New India Assurance (NIATT)
▪ I UWI (St. Augustine)	▪ Pollonais, Blanc de la Bastide & Jacelon	▪ Tranquility Credit Union
▪ PTRMS (Canada)	▪ T&T Insurance Institute (TTII)	▪ Cannings Employee Credit Union
▪ Joint Secretariat Corp. (ATTIC)	▪ Pure-ICT (Curaçao)	▪ Insurance Brokers Assoc. of T&T
▪ eTecK	▪ WiPay Ltd	▪ Charlett & Gatcliffe Insurance Brokers
▪ Genesis Insurance Brokers	▪ Trinidad Dataforms Limited	▪ CARICOM — AgriCarib
▪ NPCITT	▪ Bacon Woodrow & de Souza Limited	▪ PTRMS (Canada)

Industries served include: Financial Services & Banking, Insurance, Credit Unions, Government & Public Sector, Critical Infrastructure, Legal Services, Education, Energy, Technology Services, Aviation and Telecommunications.

10 / SECTION

Our Engagement Approach

Every CFSI engagement follows a structured lifecycle that prioritizes safety, evidence quality, and clear communication. The model below applies to assessment, governance, and engineering work — adjusted in scope and intensity based on the engagement type.

1

Scoping & Rules of Engagement

Discovery interviews with technical and executive stakeholders, finalization of in-scope assets and boundaries, agreement on rules of engagement, change control, and escalation paths.

2

Discovery & Baseline

Asset and configuration inventory, reconnaissance, and baseline establishment. Includes dark web reconnaissance and open-source intelligence where relevant.

3

Detection & Validation

Active testing using a combination of proprietary, public domain, and commercial tools — sequenced to minimize disruption to production services.

4

Exploitation & Threat Modelling

Manual exploitation of validated vulnerabilities (where authorized), construction of realistic attack scenarios, and assessment of business-impact pathways.

5

Analysis & Reporting

Executive summary for leadership and a technical report with reproduction steps, evidence, prioritized remediation guidance, and risk ratings aligned to CVSS and asset criticality.

6

Briefing & Knowledge Transfer

Post-assessment briefing with stakeholders and technical staff, with question-and-answer dialogue, remediation workshops, and optional retesting.

Project Management Commitments

- **Client Communication —** Weekly progress updates, informal communication as needed, and constant accessibility by email and phone for the duration of the engagement.
- **Progress Monitoring —** Weekly or daily review meetings as requested, with proactive identification of potential delays and corrective action.
- **Quality Control —** Quality reviews performed for every deliverable to ensure consistent, high-quality output across reports, policies, and configurations.
- **Confidentiality —** All findings handled under strict NDA, with secure communication channels, evidence destruction within 30 days of final report delivery, and no third-party disclosure.

READY TO START?

Let's Talk About Your

Cybersecurity Posture

Computer Forensics and Security Institute

Chaguanas, Trinidad, West Indies

www.CFSI.co

info@CFSI.co

868-684-0029

The Caribbean's Trusted Cybersecurity Partner Since 2011