

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 61

SEPTEMBER 2026

Cybersecurity Compliance in the Caribbean: Are You Meeting Regulatory Expectations?

INTRODUCTION



Dr. Ronald Walcott
Managing Director

Cybersecurity is no longer only a technical responsibility. For organizations operating across the Caribbean, protecting information and managing cyber risk are increasingly connected to legal, regulatory, contractual, and governance obligations.

Businesses collect and process significant amounts of personal and sensitive information, including customer records, employee information, financial data, and identification documents. As digital services expand, regulators are placing greater emphasis on how organizations collect, protect, retain, and re-

spond to incidents involving this information.

Compliance, however, should not be viewed simply as completing paperwork before an audit. Effective compliance provides organizations with a framework for understanding their risks, strengthening security controls, demonstrating accountability, and responding appropriately when incidents occur.

At Precision Cybertechnologies, we believe cybersecurity compliance should be approached as an ongoing process of risk management and continuous improvement. This month, we explore data protection, security audits, risk assessments, governance, and incident reporting obligations relevant to organizations across the Caribbean.

UNDERSTANDING CYBERSECURITY COMPLIANCE

Cybersecurity compliance refers to an organization's ability to meet applicable laws, regulations, standards, contractual requirements, and internal security policies.

The exact obligations vary depending on the organization's:

- Country of operation
- Industry
- Type of information processed
- Customers and business partners
- Regulatory environment
- Cross-border data activities

For example, Trinidad and Tobago has the Data Protection Act, 2011, which establishes a legal framework concerning the protection of personal information.

Other Caribbean jurisdictions have developed their own data protection frameworks. Jamaica's Data Protection Act, 2020, and Barba-

CONTINUED ON PAGE 2



IN THIS ISSUE:

CYBERSECURITY COMPLIANCE IN THE CARIBBEAN: ARE YOU MEETING REGULATORY EXPECTATIONS?

UPCOMING EVENTS



dos's Data Protection Act, 2019, contain specific requirements concerning personal data protection and security breaches.

For businesses operating across multiple Caribbean jurisdictions, understanding which laws apply is therefore critical.

DATA PROTECTION: KNOW WHAT YOU ARE PROTECTING

The first step toward compliance is understanding what information an organization possesses.

Organizations should identify:

- What personal data they collect
- Why they collect it
- Where it is stored
- Who can access it
- How long it is retained
- Which third parties receive it
- How it is protected
- What happens when it is no longer required

This process is sometimes referred to as data mapping.

An organization cannot effectively protect information that it does not know it possesses.

Data inventories should therefore be reviewed regularly, particularly when businesses introduce new applications, cloud services, customer portals, or third-party providers.

RISK ASSESSMENTS: COMPLIANCE STARTS WITH UNDERSTANDING RISK

Compliance and cybersecurity should be built around risk rather than assumptions.

A cybersecurity risk assessment helps organizations identify:

Assets — What systems and information are important?

Threats — What could compromise those assets?

Vulnerabilities — Where are the weaknesses?

Impact — What would happen if those weaknesses were exploited?

Likelihood — How probable is the event?

The resulting risk picture allows management to prioritize security investments.

For example, an organization may discover that its most significant risks involve compromised employee credentials, unsupported

systems, inadequate backups, or insufficient monitoring.

Instead of attempting to solve everything simultaneously, management can prioritize the risks that could have the greatest business impact.

SECURITY AUDITS: ARE YOUR CONTROLS ACTUALLY WORKING?

Having a security policy does not necessarily mean an organization is secure.

An audit provides an opportunity to determine whether policies and controls are actually implemented and operating effectively.

A cybersecurity audit may examine:

- Access controls
- Password and MFA policies
- Backup procedures
- Vulnerability management
- Endpoint security
- Network security
- Logging and monitoring
- Incident response procedures
- Third-party security
- Employee security awareness

Audits can identify gaps before regulators, customers, or cybercriminals do.

Organizations should also retain evidence demonstrating that security controls are being maintained. Examples include access reviews, vulnerability reports, training records, incident logs, backup tests, and security monitoring reports.

If you cannot demonstrate that a control exists and operates effectively, it becomes difficult to demonstrate compliance.

INCIDENT REPORTING: KNOW YOUR CLOCK BEFORE AN INCIDENT HAPPENS

One of the most important aspects of compliance is understanding what happens after a security incident.

Organizations should know who must be notified, what must be reported, and how quickly reporting must occur.

REQUIREMENTS DIFFER ACROSS JURISDICTIONS.

For example, Jamaica's Data Protection Act requires data controllers to report security breaches affecting or potentially affecting personal data to the Information Commissioner within 72 hours of becoming aware of the breach, with specified information included in the report.

Barbados's Data Protection Act, 2019 similarly provides for notification of qualifying personal-data breaches to the Data Protection Commissioner without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach.

These examples demonstrate why organizations should not wait until an incident occurs to determine their reporting obligations.

A mature incident response plan should identify:

1. Who declares an incident?
2. Who investigates it?
3. Who contacts legal counsel?
4. Who communicates with regulators?
5. Who communicates with affected customers?
6. Who manages public communications?
7. What evidence must be preserved?

Important: Regulatory obligations vary by jurisdiction and circumstances. Organizations should obtain appropriate legal or regulatory advice rather than assuming that one Caribbean country's requirements apply everywhere.

GOVERNANCE: CYBERSECURITY STARTS AT THE TOP

Cybersecurity governance establishes who is responsible for managing cyber risk.

Senior management and boards should understand:

- The organization's major cyber risks
- Critical systems and data
- Regulatory obligations
- Security investment requirements
- Incident response capabilities
- Third-party risks

Cybersecurity should not exist solely within the IT department.

A serious cyber incident can affect revenue, operations, customers, reputation, regulatory standing, and business continuity. Consequently, cybersecurity decisions should form part of broader enterprise risk management.

THE ROLE OF AN MSSP IN COMPLIANCE AND RISK MANAGEMENT

Maintaining compliance can be challenging for organizations without dedicated cybersecurity and compliance teams.

An MSSP such as Precision Cyber-technologies can support organizations by providing capabilities including:

- 24/7 security monitoring
- Managed Detection and Response (MDR)
- Vulnerability management
- Security assessments
- Log management
- Incident response support
- Security reporting
- Threat detection and investigation

Continuous monitoring also creates valuable evidence for governance and audit activities.

Security reports can help demonstrate that an organization is actively monitoring its environment, investigating suspicious activity, and addressing identified risks.

However, an MSSP does not transfer the organization's legal responsibility.



UPCOMING EVENTS

CYBERSECURITY AND COMPLIANCE CONFERENCES - 2026

Industry events throughout the year continue to address data protection, governance, regulatory compliance, and cyber risk management.

SANS CYBERSECURITY TRAINING - 2026

Professional courses covering incident response, security operations, risk management, and defensive cybersecurity.

ISACA TRAINING AND EVENTS - 2026

Programs focused on IT governance, risk, audit, compliance, and cybersecurity management.

CARIBBEAN CYBERSECURITY AND DIGITAL RESILIENCE INITIATIVES - 2026

Regional programs supporting cybersecurity awareness, capacity building, data protection, and organizational resilience.

ities. Management remains accountable for understanding its obligations and ensuring appropriate governance.

BUILDING A COMPLIANCE-READY ORGANIZATION

Caribbean organizations can take several practical steps toward improving their compliance posture:

1. Identify Applicable Requirements

Determine which laws, regulations, contracts, and industry requirements apply.

2. Inventory Sensitive Data

Understand what personal and confidential information is collected and where it resides.

3. Conduct Regular Risk Assessments

Identify vulnerabilities and prioritize risks based on likelihood and impact.

4. Test Security Controls

Do not assume that policies and technologies work—validate them.

5. Prepare an Incident Response Plan

Document regulatory contacts, responsibilities, escalation procedures, and reporting requirements.

6. Monitor Continuously

Use SOC, SIEM, EDR, and MDR capabilities to detect threats.

7. Review and Improve

Compliance is not a once-a-year activity. Security controls and risks should be reviewed continuously.



Frequently Asked Questions:

IS CYBERSECURITY COMPLIANCE ONLY RELEVANT TO LARGE ORGANIZATIONS?

No. Any organization that processes personal information or operates in a regulated industry may have legal or contractual obligations. SMBs should understand the requirements applicable to their specific operations.

HOW OFTEN SHOULD A CYBERSECURITY RISK ASSESSMENT BE CONDUCTED?

Organizations should conduct assessments regularly and whenever there are significant changes to systems, business operations, regulations, suppliers, or the threat environment.

WHAT SHOULD AN ORGANIZATION DO IMMEDIATELY AFTER DISCOVERING A DATA BREACH?

Activate the incident response process, contain the threat, preserve evidence, determine what information may have been affected, involve appropriate legal and cybersecurity personnel, and assess applicable notification requirements.

DOES PASSING AN AUDIT MEAN AN ORGANIZATION IS COMPLETELY SECURE?

No. An audit provides evidence about compliance and control effectiveness at a particular point in time. Cybersecurity risks continually change, so organizations need ongoing monitoring and improvement.



868-610-7237



info@precision-cyber.com



www.precision-cyber.com



Ground Floor, Brair Place, 10-12 Sweet Road
St. Clair, Port of Spain, Trinidad