CDML Computer Services

Empowering Business Growth through Innovation with Secure, Sustainable Solutions.

53-43 198TH Street Fresh Meadows New York 11365
Tel. (718) 393-5343 Fax (646) 837-0860 Email sales@cdml.com
Toll Free:800-CDML-123 Website: http://www.cdml.com

CDML 360° Compliance & Cybersecurity Program

CDML Computer Services is proud to offer our 360° Compliance & Cybersecurity Subscription Program - an all-in-one service designed to help small and medium-sized organizations in New York and beyond meet the complex requirements of state and federal cybersecurity regulations. This monthly subscription includes proactive services tailored to align with NYDFS, NYDOH, HIPAA, PCI DSS, NIST (SP 800-53 and 800-171), GLBA (including WISP), and the NY S.H.I.E.L.D. Act.

Covered Frameworks & Regulations

- **NYDFS 23 NYCRR 500:** NY Department of Financial Services Cybersecurity Regulation: requires risk assessments, incident reporting, and a cybersecurity program.
- **HIPAA & NYDOH/NJDOH:** Health Insurance Portability and Accountability Act: mandates protection of electronic protected health information (ePHI).
- **NIST CSF:** Cybersecurity Framework (v2.0): standards based on Identify, Protect, Detect, Respond, & Recover.
- **NIST SP 800-53:** Defines baseline security and privacy controls for information systems.
- **NIST SP 800-171:** Focuses on protecting Controlled Unclassified Information (CUI) in nonfederal systems.
- **PCI DSS:** Applies to any organization that processes, stores, or transmits credit card data; requires secure network architecture, access controls, monitoring, and regular testing to protect cardholder data.
- **GLBA:** Gramm-Leach-Bliley Act: requires financial institutions to safeguard consumer data and implement a Written Information Security Program (WISP).
- **NY S.H.I.E.L.D. Act:** Stop Hacks and Improve Electronic Data Security: mandates reasonable safeguards for personal information of NY residents.

What Are DR, BC, and IR Plans and Why Do You Need Them?

Cyber incidents are a matter of when, not if, making proactive planning essential to protect your operations and ensure rapid recovery.

Disaster Recovery (DR) Plan

Outlines how your IT systems and data will be restored after a disruption such as a cyberattack, fire, flood, or hardware failure.
Why it matters: It minimizes downtime and ensures your business can bounce back quickly and securely.

Business Continuity (BC) Plan

Focuses on maintaining essential business functions during and after an unexpected event. It includes communications, staffing, and access to systems.
Why it matters: Your clients and partners expect uninterrupted service. A BC plan keeps your business running even when things go wrong.

Incident Response (IR) Plan

Details how your business will detect, contain, and recover from cybersecurity incidents like data breaches or ransomware.
Why it matters: Regulators like NYDFS and HIPAA require it. A tested IR plan helps reduce damage and ensures compliance with breach notification rules.

Written Information Security Program (WISP)

A formal document outlining your company's policies and procedures for protecting sensitive customer data, as required under GLBA and the NY S.H.I.E.L.D. Act.
Why it matters: A WISP demonstrates due diligence and is a core requirement for legal compliance and cybersecurity insurance coverage.

Achieving Cybersecurity Certification Requires

CDML serves as your compliance partner, handling the implementation, monitoring, and ongoing management of the following requirements so your organization can focus on operations while maintaining a strong security and compliance posture.

- **Network Security & Perimeter Protection**
  Protect the organization's network from unauthorized access and external threats.
  - Next-generation firewall management, secure configuration, and network segmentation
  - Continuous vulnerability monitoring, firmware updates, and unauthorized device detection
  - Secure remote access to the organization's network
- **Endpoint Protection & Threat Detection**
  Ensure all devices are protected against malware, ransomware, and advanced threats.
  - Endpoint Detection & Response (EDR) with real-time monitoring, alerting, and response
  - Patch management for operating systems and third-party applications
  - Detection of unauthorized software, accounts, and peripheral devices
  - Device health monitoring, security posture tracking, and lifecycle management (warranty, EOL)
- **Identity, Access, and Email Security Protection**
  Protect user identities, control access, and defend against phishing, social engineering, and credential-based attacks.
  - Identity and access management, including provisioning, privilege control, and least-privilege enforcement
  - MFA, conditional access, and secure identity integration
  - Identity Threat Detection & Response (ITDR) for suspicious logins and anomalous behavior
  - Email security, encryption, and phishing awareness training
- **Data Protection, Backup & Recovery**
  Ensure business-critical data is protected, recoverable, and handled securely.
  - Secure, immutable cloud backups with integrity testing and reporting
  - Data retention, archival policies, and disaster recovery readiness
- **Governance, Risk, Incident Management & Compliance**
  Establish and maintain a complete cybersecurity and compliance program aligned with regulatory standards.
  - Risk assessments, WISP development, and policy/governance alignment
  - Vendor risk management and third-party oversight
  - Incident response, business continuity, and disaster recovery planning
  - Regulatory incident reporting support (NYDFS, NYDOH, HIPAA, PCI DSS)
  - Ongoing compliance reporting, audit preparation, and certification tracking

Earn Your Compliance Certification with CDML

Organizations today are not just expected to implement cybersecurity controls, they are expected to prove compliance. CDML's 360° SMB Compliance Program includes a structured certification path to demonstrate your organization's commitment to security, privacy, and regulatory alignment. Compliance Certification Levels are structured to reflect your organization's security maturity:

- **Foundational Certification (Silver Level)**
  - Establish the essential building blocks of cybersecurity and data protection.
  - Ideal for organizations beginning their compliance journey.
  - Includes baseline safeguards, policy creation, risk assessment, and employee training.
- **Advanced Certification (Gold Level)**
  - Strengthen your security posture with enhanced controls, monitoring, and documentation.
  - Designed for organizations handling sensitive data or operating in regulated industries.
  - Includes ongoing risk management, incident response readiness, and regulatory reporting support.
- **Comprehensive Certification (Platinum Level)**
  - Achieve a fully mature, audit-ready compliance posture aligned with major regulatory frameworks.
  - Best suited for organizations requiring the highest level of assurance and accountability.
  - Continuous monitoring, full documentation, executive reporting, audit readiness and audit support.
  - Support for cyber insurance requirements.

Demonstrate trust. Reduce risk. Stay compliant.

Contact CDML Computer Services

Phone: 718-393-5343 | Website: https://cdml.com | Email: sales@cdml.com

Blog: https://cdml.com/blog-2 | YouTube: https://www.youtube.com/@CDMLComputerServices