Fractional CISO

www.FractionalCISO.com

New York State Department of Financial Services Cybersecurity Regulation Compliance Packages for Registered Investment Advisors (RIAs) Provided by Fractional CISO

The State of New York is the first state in the country to issue regulations that require cybersecurity policies, procedures, controls and personnel for financial firms. The regulations affect organizations regulated by the New York State Department of Financial Services (DFS), including those registered under the Banking Law, Insurance Law or the Financial Services Law.

Fractional CISO offers service packages to improve the cybersecurity of its RIA customers and keep them compliant with the DFS regulations, Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500.

The cybersecurity regulations broadly address a variety of needs for Advisors to materially improve and maintain their cybersecurity posture. Requirements for 2017 include:

- The **Cybersecurity Program** should be "designed to protect the confidentiality, integrity and availability" of Information Systems.
- Organizations must designate a **Chief Information Security Officer (CISO)** who is responsible for overseeing and implementing the cybersecurity program and enforcing its cybersecurity policy. The CISO may be employed by the organization or by a third-party service provider such as **Fractional CISO**.
- **Cybersecurity Personnel** need to be well qualified with expertise in cybersecurity. They need the latest information covering the changing cybersecurity threats and countermeasures. All personnel need regular cybersecurity awareness **Training**.
- Every organization is required to implement and maintain a written **Cybersecurity Policy**.
- **Access Privileges** to systems must be reviewed on a periodic basis.
- A written **Incident Response Plan** designed to respond to and recover from a cybersecurity event such as a breach is required for all organizations.
- **Notices to Superintendent** of DFS must be filed within 72 hours of a cybersecurity event.

Additional requirements will take effect in 2018, many of which have significant technical control requirements, including:

- **Penetration Testing & Vulnerability Assessments** to evaluate and attempt to circumvent technical controls.
- **Audit Trail** designed to reconstruct material financial transactions and assist in managing Cybersecurity Events.
- Establishment of **Application Security** procedures, guidelines and standards for those organizations that develop in-house applications.
- Periodic **Risk Assessments** to identify risk and threats to the organization.
- **Multi-Factor Authentication** to protect against unauthorized access to nonpublic information or information systems.
- Creation of policies and procedures for **Limitations on Data Retention**.
- **Encryption of Nonpublic Information** for data being stored or transmitted to external networks.

Fractional CISO offers service packages to New York State RIAs to materially improve their cybersecurity posture and comply with the new regulations.

The **Bronze** package will start your compliance effort, meet many of the regulatory requirements and place your organization on a path to full regulatory compliance.

The **Silver** package meets the needs of most Advisors in New York that are not exempt from the regulations. It includes everything you need to comply with the regulations and will improve your cybersecurity, protecting your clients and their assets.

The **Gold** package is for organizations that develop their own software or have more sophisticated cybersecurity needs. Gold takes you beyond the regulatory requirements allowing your organization to minimize cyber-attack risk and placing your organization in position to promote its advanced cybersecurity protection to its clients.

Smaller firms such as those with fewer than ten employees or less than five million dollars in annual revenue are eligible for exemptions from some but not all parts of the regulations. Contact Fractional CISO for a package option to meet these requirements.

New York State DFS Cybersecurity Compliance Packages

Function	Regulation Citation	Bronze CISO[1]	Silver CISO[2]	Gold CISO
Included With All Packages				
Cybersecurity Program	500.02	✓	✓	✓
CISO title, email, business card (if desired)	500.04	✓	✓	✓
Annual Training	500.10, 500.14	✓	✓	✓
New Employee Training	500.10, 500.14	✓	✓	✓
Vulnerability Assessments	500.05	✓	✓	✓
Access Privileges	500.07	✓	✓	✓
Notices to Superintendent	500.17	✓	✓	✓
All other aspects of regulations not explicitly mentioned below	500.01, 500.18, 500.19, 500.20, 500.21, 500.22, 500.23	✓	✓	✓
Written Policies				
Cybersecurity Policy	500.03		✓	✓
Third-Party Service Provider Security Policy	500.11		✓	✓
Limitations on Data Retention (Policy)	500.13		✓	✓
Technical Controls & Monitoring				
Cybersecurity Event	500.02, 500.04, 500.06, 500.11, 500.16, 500.17		✓	✓
Penetration Testing Prep & Management	500.05		✓	✓
Basic Penetration Testing Implementation	500.05		✓	✓
Audit Trail[3]	500.06		✓	✓
Risk Assessment	500.09		✓	✓
Multi-Factor Authentication[3]	500.12		✓	✓
Encryption of Nonpublic Information[3]	500.15		✓	✓
Additional Capabilities				
Continuous Monitoring[3]	500.05			✓
Application Security	500.08			✓
Two additional cybersecurity projects annually				✓
Annual commitment required[4]			✓	✓

1: Bronze package will require additional services or others to perform the service to fully comply

2: Silver package will cover most RIAs. If you develop your own software or want a higher level of security then Gold is recommended.

3: Software and services are not included. These will typically be supplied by a third-party vendor such as one that makes multi-factor authentication software.

4: A three-month commitment is required for Bronze CISO.

Fractional CISO is available to help your organization improve its security posture. Please call us at 617.658.3276 or email us at info@fractionalciso.com for a no cost initial consultation.