New York Cybersecurity Regulation

23 NYCRR Part 500 Compliance Services

The New York State Department of Financial Services (DFS) has enacted new regulations or New York-based financial services companies and other regulated entities. The 23 New York Codes, Rules, and Regulations Part 500 Regulation (NYCRR) was developed to ensure that companies and individuals dealing with sensitive financial information maintain a minimum set of technical and administrative security controls, and an information security program sufficient for protecting sensitive financial data and systems. Entities that do not comply and file with the DFS are subject to penalties, and an entity that suffers a breach of data could be fined from $2,500 – $75,000 per day of non-compliance under current New York banking laws.

The NYCRR went into effect in March of 2017, and applies to all Covered Entities (defined as "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law"). If you are a Covered Entity, such as a Bank, Mortgage Lender, Insurance Company, HMO, or Retirement Community incorporated in New York then the Regulation likely applies to you.

The requirements for meeting compliance with the NYCRR can seem daunting: there are many variables and exemptions that need to be considered that can greatly impact the scope of your compliance program. Additionally, the Regulation is not overly prescriptive, requiring things like a Risk Assessment that is "sufficient to inform the design of the cybersecurity program as required by this Part". That's where we come in.

We have assisted companies across a variety of financial services industries with understanding and complying with the NYCRR requirements, providing a comprehensive suite of services and expert advice to help organizations meet all facets of the NYCRR. Our approach is tailored to each organization's unique environment and requirements, and we're there every step of the way to help you reach your compliance goals.

How we do it.

BSI's Cybersecurity and Information Resilience (CSIR) consultants follow a progression of phases for NYCRR engagement, intended to help your organization meet full compliance with the Regulation:

Phase 1: Assess

We start with an analysis of your status, filing requirements, and scope. As applicable requirements will vary depending on your organization's size, revenue, and types of data being collected and processed, we'll make sure your program is designed appropriately. After the scope and requirements have been determined, we perform an analysis of current controls that can be leveraged to meet compliance with the Regulation, and then perform an in-depth gap analysis of applicable controls against the Regulation. The result is a detailed assessment report, containing actionable remediation recommendations and strategies based on the findings.

bsi.

...making excellence a habit.™

Phase 2: Plan and Remediate

During this phase, BSI consultants work with the organization's stakeholders to build a comprehensive project plan and remediation roadmap to address noncompliant findings. BSI will assist in performing required activities for compliance, which can include:

- Development of a Cybersecurity Program, designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. (Section 500.02)
- Development or enhancement of existing security policies and procedures in accordance with NYCRR requirements (Section 500.03)
- Performing Penetration Testing, intended to uncover technical vulnerabilities present in the organization's environment (Section 500.05)
- Assessment and enhancement of your organization's application security policies and practices to ensure that code is developed securely (Section 500.08)
- Performing a comprehensive IT Risk Assessment, customized to the applicable scope and requirements of the organization (Section 500.09)
- Development or enhancement of Third-Party Service Provider Security Policies (Section 500.11)
- Providing online security awareness training to ensure staff are aware of their information security responsibilities (Section 500.14)
- Development of an Incident Response Plan, designed to help the organization respond and recover from a security incident (Section 500.16)

Additionally, BSI will assess your organization's compliance with all other facets of the Regulation, and provide actionable advice and the tools you need to comply. These areas include:

- Analysis of your organization's requirements for a Chief Information Security Officer (Section 500.04)
- Requirements related to Cybersecurity Personnel and Intelligence (Section 500.10)
- Review of policies and procedures related to Limitations on Data Retention (Section 500.13)
- Review of policies and procedures related to Review of Encryption of Nonpublic Information (Section 500.15)
- Review of policies and procedures related to breach notification to Superintendent (Section 500.17)

Phase 3: NYCRR Program Maintenance

BSI will work closely with your security and compliance teams to make sure that your organization has the processes and knowledge in place to maintain and continuously improve your NYCRR and broader cybersecurity program. Although the Regulation is a single framework, the outcome of building a NYCRRcompliant program is an improved overall cybersecurity and compliance posture and increased security awareness throughout your organization.

bsi.

BSI Group America
12950 Worldgate Drive, Suite 800
Herndon VA 20170
USA

To find out more
Call: +1 800 862 4977
Email: Cyber.us@bsigroup.com
Visit: bsigroup.com/cyber-us