SOLUTION GUIDE

7 NYDFS Cybersecurity Requirements You Can Tackle with Rapid7 Consulting Services

RAPID7

On March 1, 2017, the New York State Department of Financial Services' (DFS) mandatory cybersecurity requirements for financial services entities became effective, with implementation to occur within 180 days (August 28, 2017).

The purpose of the regulation is to require organizations to establish and maintain a "risk-based, holistic, and robust security program" that is designed to protect consumers' private data.

The requirements are widespread and range from more general guidelines, such as maintaining a cybersecurity program, to specifics like maintaining an audit trail. Luckily, you don't need to enlist a different security vendor to help you with each requirement. Rapid7 products and services can help, and we have expert consultants standing by to help you put a compliance plan in place.

Who's Affected?

Broadly, the requirements cover any organization operating under or required to "operate under DFS licensure, registration, or charter, or which are otherwise DFS-regulated, as well as, by extension, unregulated third-party service providers to regulated entities."

This includes:

- State-chartered banks
- Licensed lenders
- Private bankers
- Service contract providers
- Trust companies
- Mortgage companies
- Foreign banks licensed to operate in New York
- Insurance companies doing business in New York

It does EXEMPT companies with fewer than 10 employees, less than $5 million in gross annual revenue for three years, or less than $10 million in year-end total assets.

RAPID7

IMPORTANT DATES

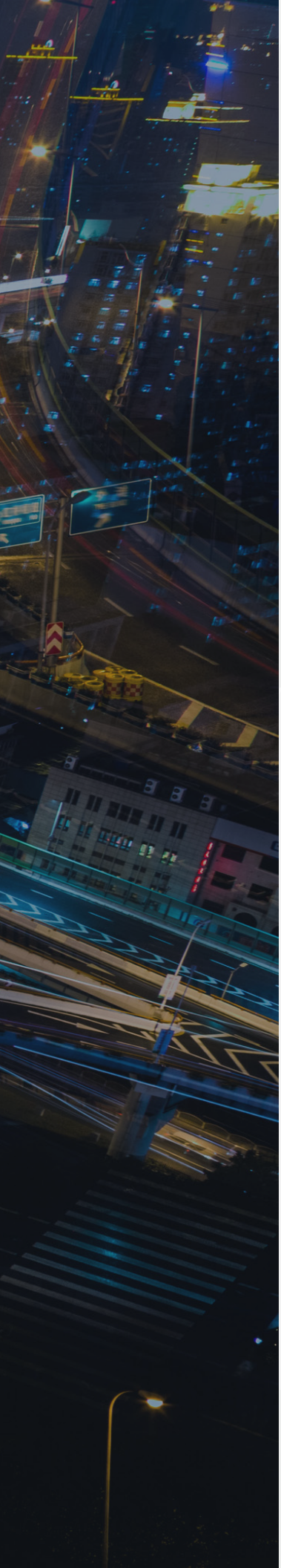
March 1, 2017
New requirements became effective

August 28, 2017
New requirements to be implemented

February 15, 2018
Required annual Certifications of Compliance begin

What You Need to Do
(And How Rapid7 Can Help)

This regulation requires covered entities to file an annual certification of compliance with the regulation. These Certifications of Compliance will commence February 15, 2018.



In order to comply with New York's cybersecurity regulation, organizations must satisfy several security guidelines. With so many aspects and approaches to consider, it can be difficult to know where to start. Many organizations opt to kick things off with a NYDFS Maturity Assessment to identify their strengths and weaknesses, and to establish strategic and tactical goals.

Rapid7's NYDFS Maturity Assessment service is designed to help you understand your cybersecurity program's alignment with the new regulation. Our team of experts evaluates your security controls across the 14 DFS regulations and identifies strategic and tactical goals to achieve compliance. At the conclusion of this engagement, you are armed with a prioritized roadmap of what to focus on to maximize impact, minimize risk, and be prepared for the Certification of Compliance deadline.

Rapid7 Consulting also offers a variety of services to assist with 23 NYCRR 500, specifically targeted at the following sections:

1. **Cybersecurity Program (Section 500.02)**
   Establish a cybersecurity program based on periodic risk assessments and designed to identify and assess risks; protect information systems and nonpublic information; detect, respond to, and recover from cyber events; and fulfill all reporting obligations.
   - Rapid7 Consulting offers a variety of **Program Development** services designed to help you build, maintain, and measure the core cybersecurity functions of your program. Program development offerings are available for vulnerability management, risk management, incident response, security policies, security program metrics, and more.

2. **Cybersecurity Policies (Section 500.03)**
   Create and maintain written policies and procedures for the protection of information systems and nonpublic information based on the company's risk assessment.
   - The security policy **Program Development** offering evaluates the comprehensiveness of your current set of cybersecurity policies and provides you with new or updated policy language that will set the standard for the implementation of security controls within your organization.

3. **Chief Information Security Officer (Section 500.04)**
   Designate a CISO to oversee and implement the cybersecurity program. The CISO may be employed by the regulated entity, an affiliate, or a third-party service provider.
   - Rapid7's **Virtual CISO** service provides your organization with trusted security advisors to help guide security efforts, strategy, and execution plans. The Virtual CISO works as an integral part of your security team and provides extensive experience in information security program assessment, development, and management.

4. **Penetration Testing and Vulnerability Management (Section 500.05)**
   The cybersecurity program must include continuous monitoring or annual penetration testing and bi-annual vulnerability assessments.
   - **Penetration Testing Services** from Rapid7 give you a real-world look at how attackers could exploit your vulnerabilities—and guidance on how to stop them. Our team performs +1,000 penetration tests yearly and is dedicated to ongoing security research, making them as close to real-world attackers as you can get.

5. **Risk Assessments (Section 500.09)**
   Conduct bi-annual risk assessments that consider threats, particular risks to the entity, and an examination of existing controls in the context of identified risk.
   - Rapid7's **Cyber Security Maturity Assessment** (CSMA) evaluates the effectiveness of your cybersecurity controls and provides you with a prioritized and risk-based security roadmap, as well as detailed recommendations that allow you to move your security program forward with confidence. CSMA engagements can align to various security frameworks and regulations such as CIS Critical Controls, NIST, ISO, PCI, and HIPAA.

6. **Cybersecurity Personnel and Intelligence (Section 500.10)**
   Utilize qualified cybersecurity personnel or "an Affiliate or a Third-Party Service Provider" sufficient to manage the organization's risks and to perform or oversee the performance of the core cybersecurity functions.
   - Rapid7 **Managed Detection and Response** (MDR) becomes your SOC, staffed by some of the industry's most regarded security analysts and a threat intelligence operation. Rapid7 MDR is powered by our InsightIDR solution that combines the power of user behavior analytics, endpoint detection and response (EDR), and log analysis to unify security data in order to detect, investigate, and remediate incidents.
   - Rapid7's **Breach Readiness Assessment** connects you with Rapid7's Incident Response team to assess the current state of your organization's environment and identify any potential risks or gaps if a breach were to occur in your environment.

7. **Incident Response Plan (Section 500.16)**
   Establish a written incident response plan for responding to and recovering from cybersecurity events.
   - The **Incident Response Program Development** offering evaluates your environment to rate your response capability and provides relevant, business-based recommendations to help you design and meet your IR program goals.
   - Rapid7 Consulting provides **Incident Response Services** to help in the event of a breach. Our team is ready to collaborate closely with your in-house team to detect threats, document findings, and recommend the right remediation activities to help ensure attackers are out—and that they can't find their way back in.

Not quite sure where to start? We can help with that too. Contact us today to speak with a consultant about how Rapid7 can get you on the fast path to NYDFS compliance.

www.rapid7.com/contact

RAPID7