

Compliance

New York DFS Cybersecurity Regulation



In today's evolving threat landscape, protecting digital information is a priority – and in some cases, a requirement. Complying with industry and government security regulations, though, can be complicated. You need a partner that understands your security obligations, and can help you fulfill them.

Tevora IS that partner. Our consultants have the extensive security knowledge and experience needed to **assess** your compliance readiness; **implement** the appropriate security controls, policies, and processes; **attest** to your adherence to the defined requirements; and **transform** your compliance requirements into a competitive advantage. ▲



The independent examination and evaluation of a company's in-place security program and controls are necessary to ensure compliance with New York State's Department of Financial Services (DFS) Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations. In today's highly regulated business environment, banking, insurance and financial services organizations operating in the State of New York must prove compliance with this state regulation.

How Tevora Helps You Comply With New York DFS Cybersecurity Regulation

- Assess existing controls against DFS Cybersecurity Regulation 23 NYCRR 500
- Analyze and measure risk using Tevora's five-factor HydraRisk decision framework
- Recommend treatment for all identified risks, large and small
- Comprehensive supporting services to address all required controls
- Experienced local staff in New York City, NY

Our Purpose

To protect the world from cyberthreats.

Insightful Advice
Expert Resource
Confident Delivery

About Us

Founded in 2003, Tevora is a specialized management consultancy focused on cybersecurity, risk, and compliance services. Based in Lake Forest, CA, our experienced consultants are devoted to supporting the CISO in protecting their organization's digital assets. We make it our responsibility to ensure the CISO has the tools and guidance they need to build their departments, so they can prevent and respond to daily threats.

Our expert advisors take the time to learn about each organization's unique pressures and challenges, so we can help identify and execute the best solutions for each case. We take a hands-on approach to each new partnership, and –year after year –apply our cumulative learnings to continually strengthen the company's digital defenses.

Go forward.
We've got your back.

We work directly with your key stakeholders to document evidence of compliance, identify control gaps, plan out remediation solutions and deploy gap closing solutions to help your organization meet the New York DFS Cybersecurity Regulation.

Our specialized risk management team begins by helping your management define and categorize assets throughout the enterprise environment. Existing controls are assessed against industry standards and best practices. Process risks are identified and evaluated based on emerging trends and industry standards. Based on the measurable assessment results, our team recommends treatment plans for all identified risks, including activities to monitor your critical risks. From updating policies and procedures to deploying needed technology, Tevora has all of the solutions your organization needs to meet its compliance requirements.

Need a different kind of Assessment?

Please refer to our datasheets for other Assessment and Compliance products:

- Enterprise Risk Assessment
- GDPR
- HIPAA
- HITRUST
- ISO 27001 Risk
- PCI DSS
- SOC 1 / SOC 2
- Vendor Risk Management

