

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.

How Tevora Helps You Comply With New York DFS Cybersecurity

- 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

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.

AUTHORIZED ASSESSOR:



ACHIEVED ACCREDITATIONS:



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

TEVORA™ Compromise Elsewhere.

Tevora is a global leader in enterprise cybersecurity, risk, and compliance services. Founded in 2003, Tevora's team of expert consultants is devoted to supporting the CISO in protecting their organizations from digital threats, creating more secure and compliant business operations. With 20 years of consistent growth, Tevora has accumulated numerous awards and recognitions for growth and industry leadership. Most notably, Tevora has been recognized as one of Inc 5000's fastest growing companies for 9 years since 2014. Today, Tevora boasts over 1000 enterprise clients and robust practices around compliance, risk, threat management, and cyber solution integration.

Go forward. **We've got your back.**