



23 NYCRR Part 500: Your Roadmap to Better Cybersecurity and DFS Compliance

Are You Ready for 23 NYCRR Part 500?

CompCiti Can Help Get You in Full Compliance

COMPCITI.COM

Three Key Messages You Need to Know about 23 NYCRR Part 500

The heart of the financial system in New York is, in many ways, the heart of the financial system in the world. It's fitting then that the State of New York's Department of Financial Services (DFS) be the first in the nation to create a specific set of regulations to protect the cybersecurity of our financial institutions.

23 NYCRR Part 500 (the "Regulation") outlines what you need to do to protect client data. However, the Regulation itself can be bewildering in detail. That's why many seek the help of a professional cybersecurity consultant. Here are the three main takeaways you need to know to get you started:

1

You need to create a Cybersecurity Program. This program will be "designed to protect the confidentiality, integrity and availability of the Covered Entity's (i.e. your) Information Systems." The plan is needs to include several core functions such as identifying cybersecurity risks and reporting serious cyber attacks to the DFS

2

You need to designate a Chief Information Security Officer (CISO). Despite the name, this isn't necessarily a C-level position. In fact, this position could be held by a third-party entity such as CompCiti (see the next point, below). The CISO is responsible for developing and overseeing the company's Cybersecurity Program.

3

You don't need to do it alone. The DFS allows – and in some case, encourages – using third-party providers such as CompCiti who have the technical expertise to meet all the requirements outlined in the Regulation. This provider could act as your CISO or provide any of the services required under the Regulation.



CompCiti Offers Cybersecurity Services Tailored to Your Needs

CompCiti Business Solutions provides cybersecurity strategies tailored to your needs. We offer CISA-certified cybersecurity services from an initial Risk Assessment to full Chief Information Security Officer (CISO) services.

Plus, with our decades of experience in business networking, cloud services, managed IT services, and more, we can ensure your systems are secure AND running efficiently.

Call CompCiti today for a free needs assessment: (212) 594-4374



Business Solutions Inc.

Read the full Regulation here: <http://www.dfs.ny.gov/about/cybersecurity.htm>

What is an IT Audit?

An IT audit is similar to a financial audit in that it helps ensure your company is following best cybersecurity practices. An IT audit includes a Risk Assessment for cyber threats (as required by 23 NYCRR Part 500), but it also is designed to find holes in your cybersecurity, review software update policies, and more to ensure your client data is secure. Most importantly, a comprehensive IT audit gives you the full picture of your current cybersecurity preparedness, allowing you to develop a more effective Cybersecurity Program and Cybersecurity Policy than you could with a Risk Assessment alone.

CompCiti provides its clients with CISA-certified IT auditing services. We offer a range of services from IT auditing to helping you address any cybersecurity issues identified during the audit. CompCiti can also act as your Chief Information Security Officer (CISO), taking care of all the details to ensure compliance.

Contact CompCiti today for a free needs assessment. We'll explain to you what you need to meet full DFS compliance and how we can help you every step of the way.



REGULATION SECTION & DESCRIPTION	STAND-ALONE SERVICE	AS CISO
500.02 Cybersecurity Program	✓	✓
500.03 Cybersecurity Policy	✓	✓
500.04 CISO		✓
500.05 Penetration Testing and Vulnerability Assessments	✓	✓
500.06 Audit Trail	✓*	✓
500.07 Access Priviledges	✓*	✓
500.08 Application Security	✓	✓
500.09 Risk Assessment (CompCiti Recommends a Full IT Audit)	✓	✓
500.10 Cybersecurity Personnel and Intelligence	✓	✓
500.11 Third-Party Service Provider	✓	✓
500.12 Multi-Factor Authentication	✓	✓
500.13 Limitations on Data Retention	✓	✓
500.14 Training and Monitoring	✓	✓
500.15 Encrytion of Non-Public Information	✓	✓
500.16 Incident Response Plan	✓	✓
500.17 Notification to Superintendent (Yearly Reporting)	✓*	✓

*Some tasks inherently need to be completed or overseen by the CISO, especially if ongoing. However, CompCiti can provide assistance such as setting up systems (for example, in the case of Audit Trail) and consulting on compliance requirements.



CompCiti Business Solutions Inc.
 261 West 35th Street, Suite 603
 New York, NY 10001
 Phone: (212) 594-4374
 Fax: (212) 594-6714
 CompCiti.com