GRC+ SERVICE SHEET · NOVEMBER 2026

NYDFS Part 500 Cybersecurity Audit

Part 500 requires covered entities to maintain a cybersecurity program, report to the board, and certify compliance to the Department every 15 April; Class A companies must also have independent audits of their program. We audit your program against Part 500 as amended in 2023, and give you the evidence your certification and your board need.

SERVICE
Advisory service

What It Is

An independent audit of your cybersecurity program against 23 NYCRR Part 500, including the independent audit Class A companies need and support for the 15 April certification.

WHY IT MATTERS
Certifying without evidence is a risk
The 2023 amendment added requirements in phases up to November 2025, and the certification must reflect all of them.
- Universal multi-factor authentication since 1 November 2025
- Independent audits required for Class A companies
- Penalties and consent orders for false certifications

THE OUTCOME
A certification you can sign
Management and the board sign the certification knowing it is backed by an independent audit.
- Evidence for the 15 April certification
- A remediation plan where you fall short
- Input for the CISO's board report

What We Audit

Governance	Your CISO, the yearly report to the board, policies, risk assessment and the board's oversight.
Technical controls	Multi-factor authentication, asset inventory, access privileges, vulnerability management, monitoring and encryption.
Resilience and third parties	Incident response and business continuity plans, notification within 72 hours, and third-party service provider policy.
Each finding with a recommendation	Every gap comes with its risk, the section concerned and a practical recommendation.

What You Receive

The audit report PDF	Scope, method and a conclusion for each section, with the evidence behind it.
Findings and recommendations Excel finding list	Each gap with its risk, the section concerned and a practical recommendation.
A certification evidence pack Evidence index	The evidence that supports your 15 April certification, section by section.
A briefing for the board Presentation and a closing call	The result and the decisions needed.

From Scoping to Audit Report

1	**Scoping** Entities, systems and the sections of Part 500 in scope.
2	**Documents** Policies, risk assessment, inventories, plans and the CISO's reports.
3	**Interviews and testing** Sessions with control owners and tests of the controls on evidence.
4	**Draft findings** You see every conclusion before it is final and can add evidence.
5	**Audit report** The report for management, the board and your certification.

A guide, not a fixed promise: the length of each phase depends on your scope and on how quickly evidence and people are available.

Regulations That Ask for It

NYDFS Part 500 (United States)	An independent audit of your cybersecurity program against 23 NYCRR Part 500, including the independent audit Class A companies need and support for the 15 April certification.

Why Financial Companies Choose GRC+ for Part 500

Independent audit expertise	Audits are led by an auditor who holds CISA, CISSP and CRISC.
Every amendment covered	We test the requirements phased in up to November 2025, not only the 2017 requirements.
Ready for your certification	The evidence pack follows the sections of Part 500, so the certification has a clear basis.
One audit, more frameworks	Our mappings link Part 500 to the NIST CSF and ISO 27001, so the evidence serves those audits too.

Questions Buyers Ask

Are we a Class A company?

A Class A company has at least USD 20 million in gross annual revenue in each of the last two fiscal years from business in New York (its own and its affiliates'), and either more than 2,000 employees or more than USD 1 billion in gross annual revenue worldwide, counting its affiliates. We confirm your status at scoping.

Does the independent audit have to be external?

Part 500 defines an independent audit as one by auditors free to make their decisions without influence from the entity being audited or its owners, managers or employees. External auditors such as GRC+ meet that test.

Talk to Us

Tell us your entity type, the areas in scope and when your certification is due. We send a written proposal with scope, dates and a fixed fee.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/nydfs-cybersecurity-audit