

NYDFS CYBERSECURITY REGULATION.



New York’s cybersecurity rule ties compliance directly to a named executive’s signature — **the CISO and highest-ranking officer personally certify the program each year**, turning a paperwork exercise into individual accountability.

- CISO PERSONAL CERTIFICATION
- MANDATORY MULTI-FACTOR AUTH
- 72-HOUR BREACH NOTIFICATION
- CLASS A ENHANCED CONTROLS

01 THE MECHANISM

Covered Entity Scope via NY Licensing

Any company holding a license, charter, or registration under NY Banking, Insurance, or Financial Services Law is a “Covered Entity” — **this pulls in banks and insurers alike through the same licensing hook**, not just depository institutions.

Personal Certification Accountability

The CISO and highest-ranking executive must jointly certify compliance each year, or file a written acknowledgment of material noncompliance instead — **a false certification is itself a violation**, closing the option to attest and hope for the best.

Class A Enhanced Controls

Large “Class A” companies face heavier obligations — independent audits, privileged access management, and endpoint detection and response. **Size and complexity, not just sector, determine how strict the program must be.**

02 THE FLOW

The Certified, Tiered Program

CONTAINED

1

The covered entity scopes its program to actual size and risk, applying Class A enhanced controls only where the revenue and employee thresholds require them.

2

The CISO and senior executive jointly certify compliance annually based on a real, documented program, **or file a noncompliance acknowledgment instead of a false certification.**

3

MFA is enforced on all remote access, privileged accounts, and third-party connections, so **a stolen password alone can't reach nonpublic information.**

The Self-Attested, Unenforced Program

EXPOSED

1

A generic policy binder is treated as the cybersecurity program regardless of the entity's actual size, complexity, or risk profile.

2

Compliance is certified based on assumption rather than a documented program, **exposing the CISO and executive to personal liability** once an incident surfaces the gap.

3

MFA is applied inconsistently or only where convenient, so **a single compromised credential can reach privileged systems and nonpublic information** directly.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
CISO Governance & Board Oversight	Requires a designated CISO reporting in writing to the board or equivalent body at least annually, with the board expected to understand and oversee cybersecurity risk directly.
Mandatory Multi-Factor Authentication	Requires MFA for all remote network access, third-party access, and any access to privileged accounts or nonpublic information, closing discretion earlier versions of the rule allowed.
72-Hour / 24-Hour Incident Notification	Requires notifying NYDFS within 72 hours of a qualifying cybersecurity event, and within 24 hours of any extortion payment made in connection with one.
Data Minimization & Encryption	Requires limiting retention of nonpublic information to what's necessary and encrypting it in transit and at rest, with documented compensating controls where encryption isn't feasible.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Generic Compliance Policy, Not Tiered to Size	No	Applies the same controls whether an entity is a small NY mortgage broker or a Class A financial conglomerate, over- or under-shooting actual risk.
Annual Certification Without a Documented Program	No	A signed certification isn't a safe harbor if the underlying cybersecurity program doesn't actually exist or meet the regulation's requirements.
Risk-Based, Optional MFA	No	The 2023 amendments removed most of the discretion that let entities skip MFA for accounts they judged lower-risk.
Ad Hoc Breach Notification	No	Missing the 72-hour, or 24-hour extortion-payment, notification window is itself a separate compliance failure regardless of how the incident is handled.
Tiered Program + CISO Certification + Mandatory MFA + Timely Notification	Yes	Matches program intensity to entity size, backs it with personal accountability, and keeps the regulator informed on the required clock.

NYDFS CYBERSECURITY REGULATION.

CERTIFY · ENFORCE · NOTIFY

05 PROGRAM OPERATIONS

23 NYCRR 500 was one of the first prescriptive U.S. state cybersecurity rules for financial services. Its Class A tiering and certification model has since shaped later rules, including the NAIC Insurance Data Security Model Law.

The 2023 amendments closed the “certify anyway” loophole. A knowingly false certification is now a distinct violation, not just evidence used after the fact if a breach occurs.

Nonpublic information is defined broadly. It covers business information whose exposure would cause material harm, not just the personal and health data most breach laws focus on.

Small covered entities get limited exemptions, not a full pass. Reduced employee, revenue, and asset thresholds trim some obligations but leave core requirements, like MFA and notification, in place.

06 CONTROL MAPPING

23 NYCRR PART 500

The core NYDFS regulation, covering any entity licensed under NY Banking, Insurance, or Financial Services Law.

2023 AMENDMENTS (CLASS A TIER)

Enhanced requirements for large covered entities — independent audits, privileged access management, and endpoint detection and response.

NAIC INSURANCE DATA SECURITY MODEL LAW

A closely related state insurance law modeled directly on 23 NYCRR 500's structure and requirements.

NYDFS ENFORCEMENT ACTIONS

A track record of fines and consent orders against covered entities for program gaps, giving the regulation real enforcement weight beyond its text.

07 WHAT THIS DOES NOT SOLVE

Federal Regulatory Overlap

Complying with 23 NYCRR 500 doesn't by itself satisfy **separate federal obligations**, like GLBA Safeguards Rule requirements or SEC disclosure rules, that may also apply.

Out-of-State Risk

The regulation binds entities licensed in New York, but doesn't extend NYDFS's authority over **a group's operations or subsidiaries outside that licensing scope**.

Non-Cyber Operational Risk

A compliant cybersecurity program doesn't address **traditional operational, credit, or market risk** a financial or insurance entity carries.

Physical Security & Insider Threat

Technical and governance controls under the rule don't replace a **dedicated physical security or insider-threat program** for the same entity.

08 MYTHS VS. REALITY

MYTH

“23 NYCRR 500 only applies to banks.”

REALITY

Any entity licensed under NY **Banking, Insurance, or Financial Services Law** is a covered entity — this pulls in insurers, money transmitters, and mortgage brokers, not just depository banks.

MYTH

“A signed annual certification is a safe harbor from enforcement.”

REALITY

A **knowingly false certification is itself a violation** under the 2023 amendments — the certification only helps if the underlying program actually meets the rule's requirements.

MYTH

“MFA is only required for customer-facing logins.”

REALITY

MFA is required for **all remote network access, third-party access, and privileged or nonpublic-information access** — internal and administrative access included.

MYTH

“Small companies are exempt from the regulation entirely.”

REALITY

Limited exemptions reduce some obligations for small covered entities, but **core requirements like MFA and incident notification still apply**.

MYTH

“This is just a New York problem for New York-based firms.”

REALITY

Because the trigger is a **NY license or registration**, out-of-state and even foreign financial and insurance companies doing licensed business in New York are covered too.

09 SPEAK THE PROGRAM — KEY TERMS

COVERED ENTITY

Any organization operating under a **license, charter, registration, or similar authorization** under NY Banking, Insurance, or Financial Services Law.

NONPUBLIC INFORMATION (NPI)

Broadly defined business, personal, and health information whose **exposure would cause material harm** to the covered entity or an individual.

CLASS A COMPANY

A large covered entity, defined by **revenue and employee thresholds**, subject to enhanced controls like independent audits and privileged access management.

CISO CERTIFICATION

The annual requirement for the **CISO and highest-ranking executive to jointly certify compliance**, or file a written acknowledgment of material noncompliance instead.

72-HOUR NOTIFICATION RULE

The requirement to notify NYDFS within **72 hours of determining a qualifying cybersecurity event occurred**, separate from any federal or other state breach law.

LIMITED EXEMPTION

Reduced obligations available to **small covered entities** meeting defined employee, revenue, or asset thresholds — a partial, not full, carve-out.