NYDFS PART 500 / RISK ASSESSMENT

What NYDFS examiners look for in your risk assessment.

The September 10, 2026 industry letter in plain language: five common gaps examiners find, and five questions for your team.

INSIDE THIS BRIEF

01-05 Five common gaps

ACTION Five questions for your team

Dan Didier

Co-founder & Principal, CyberRisk One

THE SHORT VERSION

No new rules.
Clearer expectations.

- **No new obligations.** NYDFS says so directly. The letter explains existing requirements and adds recommended practices.
- **What examiners look for.** NYDFS reviews risk assessments during examinations and investigations.

THE CORE RULE

> Your risk assessment must be sufficient to **inform the design of your cybersecurity program**, and the program must be based on it.

It must be documented, under written criteria that include how risks are mitigated or accepted.

23 NYCRR 500.9(a), 500.9(b), 500.2(b)

The letter lists **five common gaps examiners find.** The following pages take them one at a time.

GAP 1 / ASSET SCOPE AND VISIBILITY

It starts with knowing what you have.

WHAT NYDFS EXPECTS

- **Broad coverage.** Hardware, software, infrastructure, people, processes and data.
- **A complete, accurate, documented inventory.** The foundation includes owner, location, sensitivity, support end date and recovery objectives. 500.13(a)
- **Visibility into nonpublic information.** Where it lives, how it flows, who can reach it and how it is protected.

WHAT EXAMINERS FIND

Outdated inventories, unmapped data, and missing critical processes, service providers, cloud environments and other outside dependencies.

An incomplete inventory can **undermine every rating built on it.**

GAP 2 / METHODOLOGY

One method, applied consistently.

WHAT NYDFS EXPECTS

- **Repeatable criteria.** A consistent method for likelihood and impact, so results compare over time.
- **Many inputs.** Threat intelligence, incidents, scans, penetration tests and audit findings.
- **Business impact.** Financial loss, disruption, legal and regulatory exposure, and reputation.

WHAT EXAMINERS FIND

Risks rated inconsistently, control effectiveness not adequately evaluated, and no line between inherent and residual risk.

Inherent risk

The risk before your controls.

Residual risk

What is left after your controls.

No method is mandated; NIST CSF 2.0 and ISO/IEC 27005 are among the examples NYDFS names.

GAP 3 / EVOLVING AND CONNECTED RISKS

Look past your own walls.

WHAT NYDFS EXPECTS

- **Critical providers.** Rate third parties by how critical the service is, how sensitive the data is, how connected they are, and the operational impact.

  Include cloud, managed security, software, payment providers and affiliates.

- **Shared dependencies.** Consider single points of failure: one event that takes down several systems at once.

- **Emerging risks.** AI adoption, quantum computing's potential effect on encryption, software supply chain attacks, evolving ransomware and geopolitical conflict.

WHAT EXAMINERS FIND

Assessments that miss new technology, a changing threat landscape, concentration risk and single points of failure.

GAP 4 / GOVERNANCE AND RISK TREATMENT

Every risk needs an owner and a decision.

WHAT NYDFS EXPECTS

01 **Name the owner**

A named owner for each risk, and each risk linked to the controls that address it.

02 **Document acceptance**

Risk acceptance documented, with the justification and the residual risk.

03 **Track treatment**

A risk register, or a comparable tracking process, for remediation and changes over time.

WHAT EXAMINERS FIND

No owners, undocumented decisions, results kept apart from enterprise governance, and no update after changes that moved cyber risk.

Review and update timing is covered on the next page.

GAP 4 / REVIEW AND UPDATE TIMING

Keep the assessment current.

Review and update it as reasonably necessary, **at least once a year**, and whenever a business or technology change materially changes cyber risk.

01 **At least once a year**

Review and update as reasonably necessary.

02 **When material changes occur**

A business or technology change that materially changes cyber risk calls for an update.

CHANGES THAT MAY QUALIFY

Migrations, mergers, major outsourcing and new technology, including frontier AI models.

Reference: 23 NYCRR 500.9(a)

GAP 5 / INFORMING THE PROGRAM

Show the line from risk to spending.

This gap ties the other four together. If you can't show how assessed risks drive your policies, controls and resource decisions, the assessment isn't doing its job.

1	2	3	4	5
Risk	→ Owner	→ Decision	→ Control or acceptance	→ Evidence

WHAT NYDFS EXPECTS

- **Decisions based on risk.** Results that drive policies, procedures, controls, testing and resource decisions.
- **Traceable records.** Records traceable enough that internal audit and testing can focus where the risk is.

WHAT EXAMINERS FIND

Policies, controls and resource decisions not demonstrably based on identified risks.

BEFORE YOUR NEXT EXAM

Five questions for your team.

1

INVENTORY

Is our inventory complete enough to support our ratings, including providers, cloud and where our data flows?

2

METHODOLOGY

Do we rate likelihood and impact on consistent criteria, and separate inherent from residual risk?

3

DEPENDENCIES

Have we mapped our single points of failure and our most critical providers?

4

OWNERSHIP

Does every major risk have an owner and a documented decision?

5

DECISIONS

Can we show how our major risks drive our controls and spending?

Bring these questions to your next security team meeting.

SOURCES AND NEXT STEPS

Make the assessment useful to the business.

CyberRisk One builds risk methodologies and assessments that leadership, examiners and boards can follow.

Visit cyberriskone.com →

SOURCE MATERIAL

NYDFS industry letter

September 10, 2026

NYDFS website: dfs.ny.gov

23 NYCRR Part 500

References carried through this briefing:
500.9(a) and 500.9(b): risk assessment
500.2(b): cybersecurity program
500.13(a): asset inventory
500.19: exemptions

A summary of public guidance in our own words, not legal or compliance advice. Some obligations differ for exempt entities (500.19).
