Key Risk Assessment Gaps To Note From NY Cyber Guidance

By **Justin Herring and Kathryn Allen** (October 27, 2026)



Justin Herring



Kathryn Allen

On Sept. 10, the New York State Department of Financial Services published guidance on conducting and using risk assessments required by the department's cybersecurity regulation.[1]

The guidance outlines the department's expectations around risk assessments and their critical role in covered entities' cybersecurity programs. The department underscores that a risk assessment is not merely a compliance exercise, but also a foundational element of a cybersecurity program.

The guidance represents the latest in a series of cybersecurity guidance updates from the department, following the May industry letters addressing the heightened cyber threat environment and the risks posed by frontier artificial intelligence models.[2]

While the guidance states that it does not create new legal obligations, it details the NYDFS' regulatory expectations, identifies common problems and highlights best practices. Regulated entities should expect this guidance to inform NYDFS supervision and enforcement going forward.

The Risk Assessment and Common Compliance Gaps

The guidance begins by reiterating and summarizing the cybersecurity regulation's risk assessment requirement. The New York Codes, Rules and Regulations, Title 23, Part 500, requires each covered entity to conduct a periodic risk assessment of its information systems sufficient to inform the design of its cybersecurity program.[3]

Covered entities must review and update their risk assessment at least annually, and whenever a change in the business or technology causes a material change to covered entities' cyber risk.[4]

The guidance then identifies five categories of common deficiencies that the NYDFS has observed during examinations and investigations of covered entities' risk assessment practices.

Covered entities should pay particular attention here, as the NYDFS stated that these common gaps have contributed to "deficient cybersecurity programs":

- "Incomplete asset scope and visibility, including outdated or incomplete asset inventories; failing to identify where NPI resides or flows; and omitting critical business processes, Third-Party Service Providers, cloud environments, or other external dependencies";

- "Weak or inconsistent methodologies, including failing to consistently identify, analyze, prioritize, and document cybersecurity risks; evaluate the effectiveness of existing controls; or distinguish between inherent and residual risk";

- "Failure to account for evolving and interconnected risks, including emerging technologies, changes in the threat landscape, interdependencies, concentration risk, and single points of failure that could materially affect the Covered Entity's operations";

- "Insufficient governance and risk treatment, including failing to assign ownership, document risk response decisions, integrate Risk Assessment results into enterprise governance, or update Risk Assessments following material changes to the business, technology, or threat environment"; and

- "Failure to account for or inform the cybersecurity program, resulting in policies, controls, and resource decisions that are not demonstrably based on the Covered Entity's identified cyber risks."

Key Elements of the Guidance

The guidance is organized into five substantive sections, each addressing a critical aspect of the risk assessment process. Key elements of each section are discussed below.

Governance and Oversight

The guidance emphasizes the importance of enterprisewide engagement in the risk assessment process and findings.

While risk assessment is usually overseen by a chief information security officer, it should be informed by input "from relevant business units, operations, compliance, legal, and other key stakeholders." The department states that cross-functional involvement is needed to ensure a "more comprehensive and risk-informed assessment."

The guidance also strongly encourages reporting to senior management and the senior governing body.

While Part 500 has certain reporting and oversight obligations for management and the senior governing body, the guidance notably goes beyond that to encourage leadership and management to use the risk assessment to help "make informed decisions regarding resource allocation, cybersecurity investments, control selection, and risk acceptance."

Defined and Repeatable Methodology

Covered entities should adopt a clear, repeatable and well-documented methodology for conducting risk assessments. The methodology should estimate both the likelihood and the potential impact of identified risks and should apply consistent rating criteria.

In order to produce a more accurate assessment of risk severity and prioritization, risk assessments should consider, evaluate and include a number of factors, to the extent applicable:

- Threat intelligence feeds and reporting;

- Incident trend analysis;

- Vulnerability scans and penetration testing results;

- Internal and external audit findings or prior risk assessments;
- "[E]xternal and internal threats, such as malicious actors, system misconfigurations, insider misuse, and process failures";
- "[W]eaknesses in administrative controls, natural disasters, human factors, and third-party dependencies that could be exploited by threat actors or otherwise cause cyber risk";
- "[P]otential malicious actions and user errors, as well as natural disasters that could cause power outages, disrupt data centers, and impair system availability"; and
- "The potential loss of [nonpublic information], financial loss, operational disruptions, legal or regulatory exposure, reputational damage, and replacement costs."

The guidance notes that mature programs apply consistent risk criteria across relevant categories, including "those for third-party ... risk management, IT operations, and business continuity or disaster recovery planning."

Scope and Coverage

Risk assessments should consider all factors that could materially affect a covered entity's cybersecurity risk profile, and they should be appropriate to its size, complexity and technological environment. The guidance addresses four subareas of scope, discussed below.

All Assets

Risk assessments should cover all categories of assets that could affect the confidentiality, integrity or availability of information systems, including hardware, software, infrastructure, human capital, processes, and data (including nonpublic information) and data flows.

Emerging Risks

Risk assessments must account for emerging and evolving threats, including those arising from AI, quantum computing, supply chain attacks, evolving ransomware techniques and geopolitical tensions.

Third-Party and Supply Chain Risk

Covered entities should evaluate third-party and supply chain risks based on the criticality, sensitivity, connectivity and operational impact of each relationship, including cloud service providers, managed security service providers, software vendors, payment processors and affiliates.

Cyber Interdependencies and Concentration Risk

The guidance instructs covered entities to understand points of failures and evaluate whether technologies that present limited risk individually may collectively create significant risk when viewed in the aggregate.

Documentation and Traceability

Covered entities should maintain thorough documentation of the entire risk assessment process and methodology. "Effective programs" document methodology, data considered, management decisions and rationales, the link between each risk and controls that mitigate that risk, and risk acceptance.

The department encourages such documentation management and other stakeholders to prioritize, track and manage risk mitigation over time. This routine also strengthens audit function, independent testing and supervisory review.

The guidance places particular emphasis on traceability, meaning that each identified risk should be linked to specific cybersecurity controls or compensating measures. Traceability will allow covered entities to more efficiently validate that the controls identified are configured correctly and operating as intended.

To support the risk assessment process, covered entities should also maintain a risk register or comparable tracking mechanism that records each identified risk and its disposition in order to provide visibility and allocate resources appropriately.

Integration and Updates

The guidance reinforces that risk assessments must be integrated into the broader cybersecurity program, and dynamic and responsive to material changes in the covered entity's threat environment, technology and business operations.

The department emphasizes that risk assessments should not be treated as stand-alone, episodic exercises.

Section 500.2 of Part 500 requires each covered entity's cybersecurity program to be "based on" its risk assessment, meaning that the program's policies, controls and resource decisions should demonstrably derive from the risk assessment's findings.[5]

The guidance notes that covered entities that maintain continuous or regularly refreshed risk assessment processes demonstrate greater adaptability and resilience.

Part 500 requires that risk assessments are reviewed and updated at least annually and whenever a material change in business or technology warrants reassessment.

To highlight the requirement to update risk assessments for material changes, the guidance provides specific examples of events that may trigger an update, including:

- Major system migrations or technology platform changes;
- Mergers, acquisitions or significant corporate restructurings;
- Significant outsourcing arrangements;
- Adoption of or exposure to frontier AI model developments;
- Changes in threat actor capabilities or techniques;
- Adoption of emerging technologies;
- Exploitation of critical vulnerabilities; and
- Geopolitical events affecting the cyber threat landscape

Practical Implications for Covered Entities

The guidance signals the NYDFS' continued and intensifying focus on cybersecurity. Covered entities are encouraged to proactively review and, where necessary, enhance their risk assessment processes and documentation in light of the department's stated expectations.

Given the NYDFS' track record of issuing increasingly specific supervisory guidance on cybersecurity — and leveraging that guidance in enforcement actions — entities should not treat the guidance as merely aspirational.

For next steps, covered entities should consider assessing whether their current risk assessments and processes address each of the recommendations set forth in the guidance. Covered entities should pay particular attention to the following.

Scope

Confirm that risk assessments cover all applicable categories — including third-party and supply chain relationships, emerging technology risks and concentration risk — as gaps in scope are among the most common deficiencies cited by the NYDFS.

Asset Inventory

Confirm that the risk assessment is tied to comprehensive asset inventories. In particular, while Part 500 does not require a data and data flow inventory, the guidance emphasizes that this is needed for an effective risk assessment. This is consistent with the department's increasing focus on data governance and data retention.

Governance and Reporting

Evaluate whether governance structures provide for cross-functional input — including from legal, compliance and business units — and ensure risk assessment results are reported to the senior governing body and senior management.

Documentation

In addition to documenting the risk assessment process itself, assess whether the entity's cybersecurity policies, controls and resource allocation decisions are demonstrably derived from risk assessment findings.

Update

Maintain processes to review and update risk assessments at least annually and to reassess them following any material change in business operations, technology or the threat environment. Lastly, document the update process to show meaningful consideration of the relevant factors, cross-functional input and senior management reporting.

Justin Herring is a partner and Kathryn Allen is an associate at Mayer Brown.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and

should not be taken as legal advice.

[1] N.Y. Comp. Codes R. & Regs. tit. 23, § 500.1(p). https://www.dfs.ny.gov/industry_guidance/industry_letters/il20260910-cyber-risk-assessment.

[2] See NYDFS, Industry Letter Re: Cybersecurity Risks Arising from Artificial Intelligence (Oct. 16, 2024); NYDFS, Industry Letter Re: Heightened Cybersecurity Threat Guidance and Industry Letter Re: Frontier AI Model Guidance (May 2026); NYDFS, Industry Letter Re: Managing Risks Related to Third-Party Service Providers (Oct. 2025). https://www.mayerbrown.com/en/insights/publications/2026/05/nydfs-issues-two-industry-letters-on-responding-to-a-heightened-cybersecurity-threat-environment-including-frontier-ai-models.

[3] N.Y. Comp. Codes R. & Regs. tit. 23, § 500.9(a).

[4] The Second Amendment to Part 500 was adopted on November 1, 2023, with phased compliance deadlines. The updated Risk Assessment requirements under Section 500.9 became effective on April 29, 2024.

[5] N.Y. Comp. Codes R. & Regs. tit. 23, § 500.2.