VISION by protiviti®

In Focus

November, 05
2025

How NYDFS's 2025 Guidance Elevates Third-Party Service Provider Oversight and Cybersecurity Standards

By Paul Kooney

Managing Director, Technology Risk & Resilience

On October 21, 2025, the New York State Department of Financial Services (NYDFS) released updated guidance that significantly clarifies and elevates expectations for how regulated financial entities manage cybersecurity risks tied to third-party service providers (TPSPs). Building on Section 500.11 of the NYDFS Cybersecurity Regulation (Part 500), this guidance outlines a comprehensive, lifecycle-based approach to third-party risk — spanning initial due diligence, contractual safeguards, ongoing oversight, and secure termination protocols.

While the guidance does not introduce new regulatory obligations, it signals a heightened supervisory posture. NYDFS emphasizes that covered entities must embed TPSP governance into their broader risk management and resilience frameworks, with active oversight from senior governing bodies. The agency also warns against outsourcing critical compliance responsibilities without robust internal verification, underscoring that accountability cannot be delegated.

Why it matters

NYDFS is sending a clear message to financial institutions: outsourcing services does not mean outsourcing responsibility. As cybersecurity threats grow more sophisticated and as firms increasingly rely on cloud-based and third-party solutions, the new guidance from NYDFS is reinforcing that regulated entities remain fully accountable for the security and oversight of their vendors.

This matters because the guidance, while not introducing new rules, sharpens expectations around governance, due diligence, and verification across the entire third-party lifecycle. Businesses must now demonstrate that their risk management frameworks actively integrate third-party oversight, from onboarding to termination. In practice, this means stronger internal controls, clearer accountability, and more rigorous monitoring of vendor relationships.

For organizations operating in New York or under NYDFS jurisdiction, this guidance is a wake-up call to reassess how third-party risks are managed — not just on paper, but in daily operations. Those that fail to align with these heightened expectations may face increased scrutiny, reputational risk, and regulatory consequences.

NYDFS expects covered entities to implement a comprehensive and risk-based third-party management framework that spans the entire lifecycle:

- Governance and Oversight – The board and senior management must approve policies, establish risk appetite, and ensure integration of third-party oversight into the enterprise risk management framework.
- Risk Assessment – Entities must classify third parties by criticality and inherent risk, incorporating factors such as access to nonpublic information (NPI), system access, location of service, and operational dependency.
- Due Diligence – Firms should assess financial condition, cybersecurity posture, data handling practices, and subcontractor management prior to engagement.
- Contract Management – Contracts must include enforceable provisions for audit rights, incident notification, data ownership, confidentiality, and NYDFS supervisory access.
- Ongoing Monitoring – Entities must continuously evaluate performance, control environment, and compliance with contractual obligations, using risk-based frequency and metrics.
- Termination and Exit Planning – Entities must have exit strategies to ensure business continuity and data protection if a provider fails or service is discontinued.

The guidance highlights several high-risk domains warranting additional oversight:

- Cloud and Concentration Risk – Institutions must evaluate multi-cloud and vendor concentration exposures, including systemic implications of large-scale service disruptions. Avoid over-reliance on one hyperscaler or region (e.g., AWS US-EAST-1 outage). Maintain multi-region or alternative processing capability. The October 20, 2025, disruption cascaded across thousands of services (banking apps, payments, consumer platforms). Outage duration and recovery varied by customer architecture. This incident exposed the risks of systemic reliance on large-scale cloud providers for critical internet infrastructure.
- Subcontractors and Fourth Parties – Covered entities remain accountable for the actions of all subcontractors in the service chain. Oversight mechanisms must extend beyond direct vendors.
- Data Security and Incident Notification – Providers must adhere to encryption, access control, and breach notification requirements consistent with Part 500.

- Business Continuity and Resilience – Firms must test contingency plans, validate recovery objectives, and ensure third-party participation in joint exercises.

The NYDFS guidance raises expectations for structured governance and thorough documentation in third-party oversight. It urges risk and compliance leaders to align oversight practices with cybersecurity and operational resilience standards, embedding controls across key functions. Additionally, it calls for regular board-level reporting on third-party risk exposure and concentration trends.

What they say

Kaitlin Asrow, Acting Superintendent of NYDFS

"While third-party service providers have driven innovation and enabled significant efficiencies in our financial system, regulated entities are still ultimately accountable for protecting consumers and managing risk."

"Entities must establish and maintain appropriate internal risk management controls when using third-party service providers."

Bob Maley, Chief Information Security Officer at Black Kite

"They've added language about AI and AI use and they're recommending clauses to put into contracts around how your vendors are training their models and how AI should be treated at third parties. This is kind of like walking the edge of a sword."

"The AI guidance is an amazing thing but also potentially problematic for service providers."

What we say

The latest NYDFS guidance signals an urgent need for formalized governance and thorough documentation of third-party oversight. Risk and compliance leaders must act swiftly to align with heightened regulatory expectations, integrating key controls across Information Security, Procurement, Legal, and Business Continuity. Board-level reporting on third-party risk posture and concentration trends is now essential to demonstrate resilience and regulatory readiness.

The bottom line

NYDFS's 2025 guidance reinforces that third-party risk management is a core element of an entity's cybersecurity program. To demonstrate readiness and compliance with the NYDFS Guidance, covered entities should consider the following actions:

- Conduct a gap assessment against each Guidance component, mapping to existing third party risk management and cybersecurity controls.
- Update third-party risk policy and standards to explicitly cover subcontractors, concentration risk, and incident response.

- Enhance due diligence questionnaires and contract templates to include NYDFS-required provisions.
- Establish a risk taxonomy aligned with criticality, inherent risk, and service type (e.g., cloud, IT, operations).
- Implement risk-based ongoing monitoring leveraging both internal metrics and third-party assurance reports (SOC, ISO, etc.).
- Establish formalized Business Continuity Plan (BCP) testing procedures that verify the organization's ability to retrieve data and restore systems within defined recovery parameters. Covered entities must also ensure that third-party service providers actively participate in joint recovery exercises and demonstrate compliance with established Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- Develop management and board-level reporting to monitor residual risk and compliance progress.

Organizations must adopt a proactive and documented approach — linking governance, technology, and regulatory compliance — to ensure an effective strategy in managing third parties in an evolving risk landscape.

Anil Chacko, Director, Technology Risk & Resilience, contributed to this report.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk, and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2025 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, and with government agencies. Protiviti is a CMMCAB RPO organization and has been supporting companies with CMMC services for seven years. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About VISION by Protiviti

VISION by Protiviti is a global content resource exploring big, transformational topics that will alter business in the future. Written for the C-suite and boardroom executives worldwide, *VISION by Protiviti* examines the impacts of disruptive forces shaping the world today and in the future. Through a variety of voices and a diversity of thought, *VISION by Protiviti* provides perspectives on what business will look like in a decade and beyond.

protiviti®