WHITE PAPER

The NYDFS Part 500 cybersecurity audit requirement

Turning compliance into value

protiviti®
Global Business Consulting

Executive summary

As cyber threats grow ever more sophisticated and relentless, New York's financial institutions face heightened regulatory expectations under NYDFS Part 500—anchored by a rigorous cybersecurity audit requirement for large entities. This mandate is not just about compliance; it's an opportunity to strengthen resilience and build lasting trust in an increasingly digital financial ecosystem. NYDFS Part 500 is a requirement that was introduced in a 2023 amendment to the New York Department of Financial Services (NYDFS) 23 NYCRR Part 500 ("Part 500") regulation, originally enacted in 2017. The regulation was enacted in response to the increasing frequency and sophistication of cyber threats targeting the financial sector, and seeks to protect sensitive customer information and ensure the resilience of financial institutions. A critical element of this regulatory framework is the annual cybersecurity audit requirement.

From regulation to transformation: NYDFS Part 500's audit requirement is more than compliance—it's an opportunity to strengthen trust and competitive edge.

This guide explores leading practices for planning, conducting and reporting on these audits, emphasizing the importance of aligning them with financial institutions' overall cybersecurity risk management strategies. Beyond compliance, this is a regulatory requirement that presents an opportunity for organizations to enhance their cybersecurity posture, ensuring they are better equipped to defend against evolving cyber threats.

Introduction

In an age where cyber threats are increasingly sophisticated and prevalent, the NYDFS seeks to be a trendsetter for other regulators with a first-of-its-kind cybersecurity regulation. Part 500 was introduced in March 2017 in response to the growing need for enhanced cybersecurity measures within the financial services industry. Recognizing the evolving nature of cybersecurity threats, the rule is designed to be applied largely based on an organization's unique view of cyber risk, and the NYDFS continues to adapt the requirement to address the evolving cybersecurity landscape. In 2023 the regulation was amended with several new and revised requirements, including a new requirement that Class A companies[1] conduct independent annual audits of their cybersecurity programs.

Cybersecurity audits serve as a critical tool for organizations to identify vulnerabilities and drive the implementation of controls to manage their cybersecurity risks. The regulation does not provide specific guidance on the audit requirement, other than it being independent and based on the risk assessment, leaving organizations with the challenge of knowing where to start. Should audits focus on the effectiveness of the cybersecurity tools and technology, the cybersecurity governance and organizational structure, an assessment of compliance with the regulation or all of the above? Should organizations conduct one comprehensive audit of the cybersecurity program, or a series of audits targeted at key risks? Understanding the answers to these questions — which we will strive to do here — and the impact of those decisions have been challenging for financial institutions operating in New York.

Ultimately, viewing cybersecurity auditing as merely a compliance requirement is a missed opportunity to provide management assurance of the effectiveness of the organization's cybersecurity program and, often, to gain support for necessary investment in the program. Conducting thorough and effective audits involves careful planning, clear scope definition and a structured methodology. It also requires proactive issue management and comprehensive reporting to ensure transparency and accountability within the organization.

[1] Defined as more than $20 million in revenue from the covered entity itself and more than 2,000 employees or more than $1 billion in gross revenue in aggregate including all affiliates.

What is NYDFS Part 500?

The core mandate of the regulation is to protect the financial assets of New York customers and counterparties from cyber threats by setting a framework of foundational cybersecurity control requirements. This can provide a base for covered institutions[2] to implement cybersecurity programs that are risk-based and adaptive. Key components of the regulation include:

- **Risk assessments:** Regular risk assessments are required to be performed by the security organization to inform the design of the cybersecurity program. The regulation explicitly ties many requirements to the results of these assessments, making the risk assessment foundational to compliance with the rule and ensuring a focus on the most pertinent threats and vulnerabilities to the covered entity's systems and data.
- **Cybersecurity program & policies:** Each organization must maintain a cybersecurity program based on an annual risk assessment. The program should be designed to include a baseline of cybersecurity controls that protect its systems and the non-public information stored on those systems. Each Class A company must conduct independent audits of its cybersecurity program based on its risk assessment. Each covered entity is expected to implement policies and procedures that are approved by senior management; are based on the risk assessment; and address control areas such as data governance and privacy, asset management, access management, technical controls, network and system monitoring, and so on.
- **Chief information security officer:** A qualified individual must be appointed to oversee and enforce the cybersecurity program. The CISO must report at least annually to the board or senior officers on the program's status and material risks.

[2] Defined as "any entity that is chartered, licensed, or approved to operate in New York state by DFS under the NYS Banking, Insurance or Financial Services Laws." Source: Treasury.gov

- **Technical controls:** Part 500 sets expectations for controls like penetration testing and vulnerability assessments, audit trail retention, multi-factor authentication (MFA) and encryption of nonpublic data. For example, firms must conduct periodic pen tests and maintain audit logs for certain systems, implement MFA for remote access, encrypt sensitive data, and privileged accounts should be monitored and managed in a tool.
- **Third-party security:** Vendors and third-party service providers must be risk-assessed based on the risk they present to the entity and meet cybersecurity requirements that are contractually enforced, recognizing the supply-chain impact on the covered entity's security.
- **Incident response and notification:** Firms must have an incident response plan and are required to report significant cybersecurity events (e.g., those affecting the confidentiality or integrity of information systems) to NYDFS within 72 hours. Additionally, an annual certification of compliance must be submitted by a senior officer or Board annually, by April 15th, attesting that the firm meets Part 500's requirements.

The Part 500 regulations had an immediate effect from their inception in 2017, but the precise impact varied depending on the maturity and strategy of financial institutions' cybersecurity programs. Many organizations had to quickly uplift their cyber program governance, including hiring a CISO and implementing regular cybersecurity risk assessments, as well as implementing new technical controls and security operations processes. Boards and leaders of covered entities that chose to wait and see if the NYDFS would allow flexibility in the implementation were forced into action as the examinations of non-compliant entities resulted in fines and penalties. Part 500's reputation as a strong regulation grew through the issuance of consent orders and fines. Given the wide recognition, acceptance and adoption of the rule, NYDFS could have maintained the rule as it was, but recognized the need to adapt to meet the evolving nature of cybersecurity risks. In November 2023, a second amendment to the rule was implemented to further strengthen the requirements.

Turning the annual audit requirement into an opportunity for improvement

Recognizing the outsized impact of a cyber-attack on New York financial markets, in 2023 the revised rule introduced Class A companies, a new category of the largest covered entities. These Class A companies are subject to heightened requirements, the most notable of which is a mandate to conduct periodic independent audits of their cybersecurity programs. Initially proposed as an annual audit, the final regulation ties the frequency and scope of the audit to the company's risk assessment. In practice, risk assessments must be done at least annually, effectively ensuring regular (annual or risk-driven) audits for these larger Class A entities.

One potential pitfall is to treat the cybersecurity audit requirement as a standalone or check-the-box exercise — something done to appease regulators and then put aside. To truly reap the benefits, organizations should fully integrate their audit approach into a broader cybersecurity strategy and risk management program. This ensures that insights from the audit process continuously inform improvements and conversely, that strategic priorities shape the focus of the cyber audit program.

Why are independent audits required?

Originally, the Part 500 certification relied on the attestation of a senior officer of the covered entity. Over time, the NYDFS realized that additional assurance beyond management's attestation was required. Under the amended rule Part 500.2, Class A companies are required to perform independent audits of their cybersecurity program based on its risk assessments. The purpose of the independent audit requirement is to evaluate the design and effectiveness of the cybersecurity controls that comprise the basis of NYDFS compliance certification. This not only strengthens management's confidence in the annual compliance certification, but also provides assurance of the effectiveness of the cybersecurity program.

The ripple effect: How independent audits shape cybersecurity programs

The NYDFS sent a clear message when it issued Part 500, that managing cybersecurity risk is the responsibility of the entire organization. For Class A companies, failing to conduct independent cybersecurity audits could constitute non-compliance with Part 500. NYDFS can impose penalties for non-compliance and has cited lack of sufficient oversight or ineffective programs in past enforcement actions. A robust cybersecurity audit program will help reduce the likelihood of these types of regulatory actions.

Beyond the compliance benefits, when properly executed, audits will deliver insight into the effectiveness of an institution's security controls and processes. The audit process can serve as an annual report card on the cybersecurity program, highlighting what is working well and where improvements are needed. Organizations should reconsider their approach to board-level reporting to ensure the results of the audit are appropriately highlighted, maintaining alignment in messaging around risks, gaps and potential for improvement with the CISO and technology leadership.

Avoid getting it wrong: Three common mistakes

With the best of intentions, we have seen organizations address the cybersecurity audit requirement in a way that misses or misinterprets key elements of the rule. The following are three common pitfalls to avoid:

Mistake #1: Treating this as a compliance testing exercise

Some organizations approach this as an audit of their compliance with the NYDFS Part 500 rule, often building an audit testing program that ties closely to each component of the rule. While covering the rule is important in the context of the audit program, each organization's control environment will look different and those objectives will be achieved using different organizational structure, technologies and processes. A better approach is to define your cyber controls based on an established control framework, such as NIST CSF 2.0 or CIS, and identify the correlations between the control framework and the rule as part of your control documentation.

Mistake #2: Inadequate consideration of management's cybersecurity risk assessment when scoping the audit

The second is to minimize or overlook the importance of the risk assessment to scoping the audit. This can lead to incomplete coverage of cybersecurity risks in the audit and misalignment with management's cybersecurity program design which itself should be based on the same risk assessment. Audit teams can avoid this by reviewing the most recent cybersecurity risk assessment results during audit planning and scoping, and including the risk assessment itself in the scope of the audit. Effective cyber risk assessments should start with a threat-based assessment of IT assets to prioritize risks and identify associated controls. Auditors can use the risk assessment results to define the systems, applications, and data in scope for the audit. The audit team should develop a risk and control matrix (RCM) based on the risk assessment results, then map the RCM to the NYDFS

The cybersecurity risk assessment is not only core to complying with the rule, it should be central to how the organization approaches its cybersecurity auditing.

cybersecurity requirements to ensure the audit covers each requirement of the Part 500 regulation.

Mistake #3: Failure to articulate how "material compliance" is measured

The third common mistake is failure to take a considered, strategic approach to defining and measuring "material compliance," which is a critical concept in the rule that drives whether a particular control issue is reportable to the NYDFS as an area of non-compliance. There should be clear and agreed to criteria for evaluating whether audit findings are materially non-compliant with the regulation. Finding areas of material noncompliance that cannot be remediated by year end, and depending on the timing of the audit, may trigger reporting of noncompliance with part of the rule to the NYDFS as part of the annual certification process. Establish a consistent method of evaluating if evidence achieves the requirements of section 500.17(b)(1)(i)(b), including the term "based on data and documentation sufficient to accurately determine and demonstrate material compliance." All audit stakeholders should agree on this material compliance criteria before the audit begins.

In the remainder of this paper, we share our approach to planning and executing an audit that meets the Part 500 requirements and validates the strength of your cybersecurity program to effectively manage the landscape of evolving risks. Based on our experience advising NYDFS regulated clients, we will provide insights on how to plan, execute, and report effectively to meet the compliance requirements and improve the organization's confidence in their capabilities to protect against the various threats they face.

When to perform the audit: Align with the compliance certification process

NYDFS requires the annual compliance certification to be submitted by April 15th of each year (covering the prior calendar year). However, it does not require the audit program to be completed before making that certification. That said, to confidently sign that certification, management should consider having the results of the independent audit in hand by that date. Where possible, the audit findings and remediation actions should be addressed before the certification is due. In situations where this is not possible, at a

minimum ensure that remediation plans, owners, and target dates have been agreed upon and approved. In addition, when the audit process is completed prior to certification, management should have a well-defined process of evaluating audit findings to determine whether any constitute reportable areas of material non-compliance with a part of the rule. While not required, completing the audit process prior to certification will increase management's confidence in the accuracy of its certification.

Coordinate with cybersecurity risk assessments

Part 500 requires each covered entity supervised by NYDFS to conduct, at least annually, a cybersecurity risk assessment to inform the organization of the top risks its cybersecurity program needs to mitigate. The risk assessments should be updated as necessary to include changes in business or technology, the threat landscape, and other factors that could change the company's cybersecurity risk profile. The recommended approach is to perform the annual risk assessment first (e.g., mid-year), update the cybersecurity program as needed, and then conduct an independent audit process informed by the risk assessment. This sequencing ensures the audit evaluates the cybersecurity controls and processes in their current state and verifies that risk assessment results are being appropriately addressed.

The risk assessment should be updated as necessary to include changes in business or technology, the threat landscape, and other factors that could change the company's cybersecurity risk profile.

Cybersecurity implementation timeline for Class A companies

Q1

Ideal timing to conduct an independent audit of the prior year's cybersecurity program for Class A companies to validate control effectiveness and regulatory alignment.

April 15

Submit Certification of Compliance (or Acknowledgment of Noncompliance) to NYDFS for the prior calendar year.

Q2 - Q3

Remediate known gaps and audit findings; refresh the annual cybersecurity risk assessment and update the program based on results.

November 1

CISO delivers annual cybersecurity report to the senior governing body; governing body affirms oversight of the cybersecurity program.

Establish a baseline for evaluating compliance

The key to a successful audit is to establish a structured, risk-based approach that evaluates the effectiveness of cybersecurity controls and maturity of the environment as its primary objective while also considering compliance with Part 500 requirements. This starts with setting a framework that stands on three foundations, all of which should be agreed to by all parties before starting the audit.

1. Set a standard for evaluating whether the covered entity "materially complied with all parts of the regulation" per section 500.17(b)(1)(i)(a).
2. Establish criteria for determining if the evidence evaluated for each in scope control achieves the requirements of section 500.17(b)(1)(i)(b), including the term "based on data and documentation sufficient to accurately determine and demonstrate material compliance."
3. Develop a decision tree (see "NYDFS Materiality Decision Tree," right) to ensure gaps are evaluated consistently for whether they constitute material non-compliance with the rule, including alignment with the cybersecurity risk assessment, potential impairment to the protection of information systems and NPI, and consideration of compensating controls.

NYDFS Materiality Decision Tree

1. Identify NYDFS Requirement

Q: Is there an NYDFS requirement?

- **No:** Stop the assessment.
- **Yes:** Proceed to the next step.

2. Check for Existing Policies

Q: Is there a policy that exists?

- **No:** Move to Step 5 (policy gap noted, requires remediation).
- **Yes:** Proceed to the next step.

3. Evaluate Policy Sufficiency

Q: Does the policy specifically address NYDFS requirements sufficiently?

- **No:** Move to Step 5 (policy gap noted, requires remediation).
- **Yes:** Proceed to the next step.

4. Assess Compliance with Policy

Q: Are supporting processes performed in full accordance with policy and/or the regulation?

- **No:** Move to Step 5 (document noncompliance).
- **Yes:** Mark as in compliance.

5. Determine Impact of Noncompliance

Q: Did the policy or process gap/instance of noncompliance:
(i) meaningfully impact or pose a meaningful risk to confidentiality, integrity, or availability of information systems, or
(ii) persist for an extensive amount of time?

- **No:** Identify as immaterial noncompliance; requires documentation and remediation. Move to Step 6.
- **Yes:** Identify as material noncompliance; document, report, and remediate.

6. Identify Additional Instances of Noncompliance

Q: Were any additional instances of immaterial noncompliance identified?

- **No:** Move to Step 7.
- **Yes:** Document, report, and remediate potential material noncompliance based on aggregate considerations.

7. Review Corrective Action Plans

Q: Are there corrective action plans in place to address the risk?

- **No:** Document, report, and remediate potential material noncompliance.
- **Yes:** No further action required; document accordingly.

From compliance burden to strategic asset

Defining the audit scope with risk and regulatory clarity

Elevating the cybersecurity audit from a routine compliance exercise to a driver of strategic value begins with a deliberate approach to defining its scope. The scoping process should provide a lens that brings clarity to where regulatory demands and the organization's cybersecurity risk truly intersect. By thoughtfully determining which business units, information systems, and control areas to include, organizations not only satisfy the expectations of NYDFS Part 500, but position themselves to better understand their cybersecurity vulnerabilities, highlight operational strengths, and prioritize resources where they can be most impactful. When scope is crafted with both risk and regulatory insights in mind, the audit can begin to serve as a strategic driver of cyber resilience and informed decision-making, rather than being just another regulatory obligation.

- **Business unit coverage:** Consider the structure of the organization and its approach to managing cybersecurity. For companies with multiple subsidiaries or business lines, the audit should include all covered entities regulated by the NYDFS. The scope should reflect any differences in how each subsidiary implements the cybersecurity program, with an overarching goal of consistency across the enterprise wherever possible. Setting the foundation of common standards and criteria described above will ensure a consistent approach across the different subsidiaries.

Smart scoping starts with risk. Align your audit to NYDFS priorities and your risk profile—because compliance without context is just a checkbox.

- **Treat the control catalog as the backbone of the audit scope:** While achieving coverage of NYDFS Part 500 requirements is critical, ideally the regulation will not be your starting point for scoping controls. Design a cybersecurity control catalog that meets the needs of the organization, typically tied to a recognized framework such as the NIST CSF or CIS, then map it back to the regulation. This does more than confirm coverage: it surfaces gaps and redundancies, producing a focused, defensible scope that concentrates effort where risk — including regulatory compliance risk — is highest.
- **Risk-based control selection:** With the controls selected the decision must be made about what level of testing will be performed on each control. NYDFS expects the independent audit to be tied to the company's risk assessment results. Critically, beyond this, there is no regulatory requirement to drive specific scope or testing standards, giving each covered entity significant latitude. Management should take a risk-based approach to selection and depth of control testing. This means that areas identified as higher risk should receive more attention in the audit (more thorough testing), whereas low-risk areas can be reviewed at a higher level. Prioritize critical assets, high-risk processes and any controls that have known issues or past audit findings.

By thoughtfully defining scope, two key objectives are met — 1) ensuring the audit is aligned with and supports the entity's risk profile and cybersecurity objectives, and 2) covering the full breadth of Part 500's requirements giving a window into the state of compliance. A risk-informed scope yields an audit report that is balanced, provides reasonable assurance of compliance to management and the board, and detailed insights on the most critical security areas. NYDFS's own commentary suggests audits be flexible and risk-driven rather than a static annual checklist. Thus, scope planning should be an annual exercise, revisited each year to adjust to changes in the business, cybersecurity threats and regulatory requirements.

Beyond compliance

The accountability dividend of audit independence

In planning the Part 500 audit, it is crucial to establish and maintain independence in both fact and appearance. NYDFS defines an independent audit as one conducted by internal or external auditors who are free from influence by the company's management or employees. Let's consider ways organizations can ensure the audit is independent — in both fact and appearance.

Who performs the audit?

Since Internal Audit (IA) typically reports to the Audit Committee of the Board, it is a good practice for IA to perform the cybersecurity audit assuming it has, or can obtain, the appropriate skill sets to do so. In many firms, internal audit is already performing one or more annual cybersecurity-related audits and so in those cases there may only be incremental scope changes needed to align with Part 500 requirements. Alternatively, especially if the third line of defense lacks cybersecurity expertise or is too small, the company can engage an external firm to conduct the audit. Whichever route is chosen, clearly document that the auditors have their own, distinct reporting line — e.g., they report findings directly to the board or a committee, not to the CISO — to demonstrate organizational independence.

What other factors can support independence?

We recommend using clearly articulated, objective standards, evaluation criteria, and testing methodology for executing the audit. For example, the use of established frameworks (i.e., NIST CSF, CIS etc.) mapped to the Part 500 controls helps ensure the audit is based on authoritative standards rather than subjective opinions. The use of more traditional random selection and sampling procedures, where possible, helps in this regard as well.

A crucial, yet sometimes overlooked, element of audit independence lies in the mindset and governance that underpin the process. Mindset refers to the auditors' commitment to objectivity, skepticism, and ethical rigor—approaching each engagement determined to uncover the truth, free from undue influence or bias. Governance, meanwhile, encompasses the formal structures and policies that safeguard this independence: clear reporting lines, documented procedures, and oversight by an independent board or committee. Together, these factors establish an environment where audit results are credible and can be trusted by all stakeholders. This, in turn, translates into more actionable findings, stronger controls, and continual improvement in the organization's cybersecurity posture.

Whether it is your internal audit team or an external advisor, make sure they have the credibility, skills, and independence — in fact and appearance — to do a thorough job. Companies that demonstrate a truly independent audit process will not only comply with the letter of the law but also gain deeper trust in the findings, which leads to more effective risk mitigation.

Independence reveals truth. Risk defines focus. Together, they turn a cybersecurity audit into the sharpest instrument for strengthening your defenses.

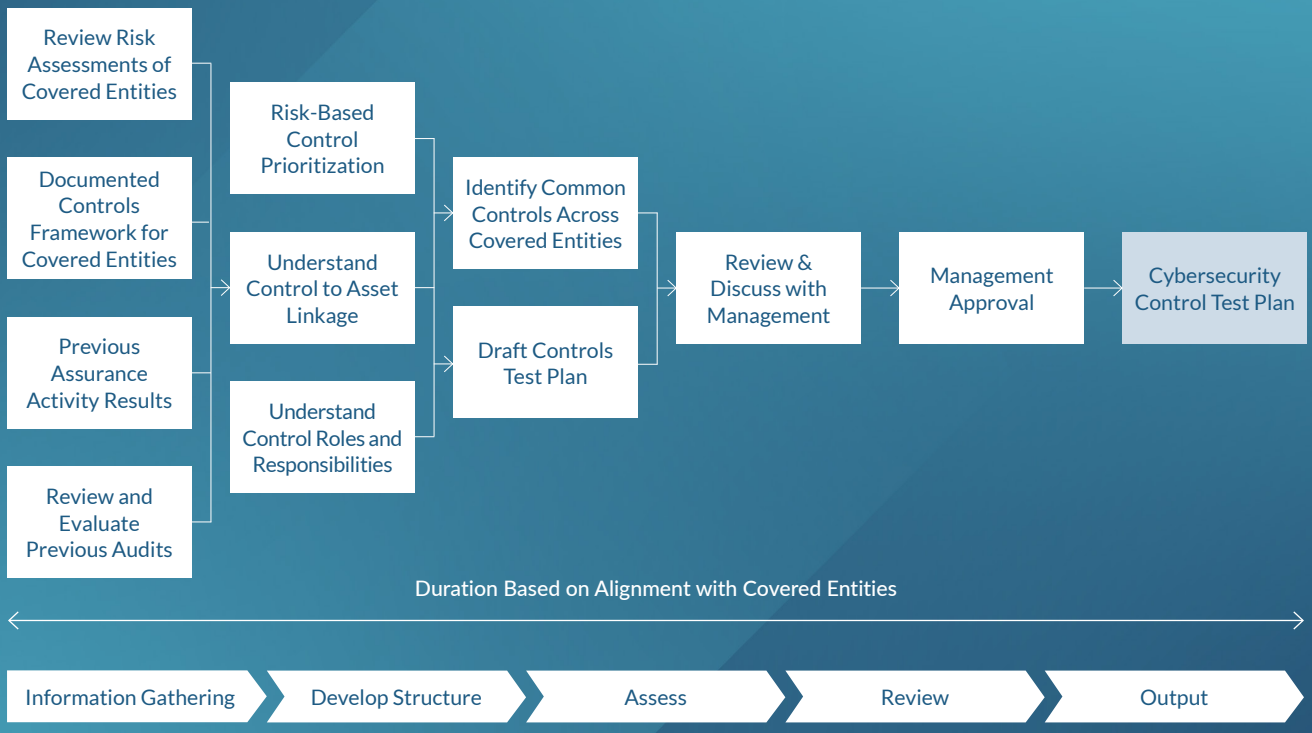
True independence builds confidence. When audits speak without bias, boards listen—and act.

Executing audits to achieve successful outcomes

Once a plan is in place, the approach and methodology are defined, and the scope is agreed to, the audit execution can begin. This involves assessing policies and procedures, testing controls, identifying issues and agreeing with stakeholders on remediations and target delivery dates. Efficient and effective audit execution can be achieved through technology enablement such as a Governance Risk and Compliance tool as well as supporting testing and evaluation tools. Executing the audit effectively requires technical expertise, diligence in evidence gathering and close collaboration with stakeholders to validate observations.

NYDFS Controls Scoping Process

This framework illustrates how Protiviti aligns NYDFS Part 500 control testing with each entity's risk profile, prior assurance activities, and regulatory submissions to deliver efficient, risk-focused coverage.



The strategic path for auditors: Technology enablement and AI

NYDFS Part 500 cybersecurity audits can benefit from technology enablement tools like GRC (governance, risk, compliance) software to automate the audit workflow. If the organization uses a tool like AuditBoard or Archer to track controls, the audit methodology can include extracting reports from those systems. Automated scanning tools can gather evidence via automated scripts, such as running a configuration compliance scan to verify that systems have up-to-date patches or encryption settings. The emergence of artificial intelligence (AI) has impacted many processes across all industries, and audit is no exception. Cybersecurity audits can benefit from the use of AI to drive efficiencies through automation and analytics. AI tools can be leveraged to transcribe walkthrough recordings into process flows and narratives. Control testing can be automated using large language models (LLMs) and robotic process automation (RPA) tools. Utilizing these tools can increase coverage, efficiency and accuracy. Their use and availability will depend heavily on the maturity of the audit program, skills of the auditors and specifics of the technology stack of the financial institution.

Cyber audit reporting: The results are in

The culmination of the audit process is the reporting phase—documenting findings and communicating them to stakeholders. An effective report serves as a decision-making tool for management, offering insights on compliance considerations and actionable recommendations. Clear communication ensures that all relevant parties understand the results and their implications. Consider providing benchmarking, implementation tier assessment (NIST CSF) or maturity rating evaluations for the process areas included in scope.

When presenting to the Audit Committee, it is critical to focus on key outcomes rather than overwhelming members with excessive detail. Given the breadth of many cybersecurity audits, over-reporting can dilute the message and obscure what truly matters. The discussion should emphasize areas of highest risk, significant control gaps, and—when the CISO or equivalent management is present to discuss it—where investment in the cybersecurity program is needed to strengthen resilience.

It is important to note that the audit report is not a formal compliance assessment and should not attempt to provide an overall opinion on compliance. Instead,

it evaluates the effectiveness of controls and highlights areas where compliance considerations may exist. This information enables the CISO and management to determine whether any reportable instances of "material" non-compliance exist for the year.

The cybersecurity audit report for Part 500 should include a similar structure and level of detail included in any high-quality audit report. Below are critical reporting elements unique to a Part 500-compliant cybersecurity audit:

- **Compliance impact of findings and recommendations:** This is the core of the report, often organized either by Part 500 section or by thematic area. For each area or control tested, state whether it was effective or if issues were found. If the control was ineffective, include an opinion as to whether this should be considered material noncompliance with any applicable Part 500 requirement. Each finding should be described in detail, as discussed in the issue management section. It's often helpful to number the findings (e.g., Finding #1: XYZ) for reference. After describing the finding and its implication, provide recommendations that are actionable and specific — for example, "Implement a formal process to periodically review user access rights. This should include quarterly reviews of all privileged accounts, with documentation of the review and revocation of any excessive access. This will help address the access control gaps noted and fulfill the requirement of section 500.7."
- **Compliance summary:** While not an overall or final compliance assessment, the report should be viewed as a tool for management's assessment of compliance. One way to report this is to include a table or appendix that explicitly lists each NYDFS Part 500 requirement and communicates whether compliance considerations exist for each section, possibly with a brief note or reference to a finding. For example: "500.11 Third-Party Security — Compliant (Third-Party Security Policy in place and risk assessments conducted)" or "500.13 Limitations on Data Retention — Partially Compliant (Data retention policy exists, but no process to securely dispose of certain data types; see Finding #5)." This is where the report delivers real value—helping management make informed decisions about compliance and identify any areas that may represent material non-compliance. To enhance clarity, many audit teams present these results in a scorecard format, using color-coding (green/yellow/red) to indicate the status of each major domain or requirement at a glance.

Conclusion

In today's increasingly inter-connected global economy, companies find themselves under an almost unrelenting assault from cyber criminals of various stripes. Financial institutions, which supply the infrastructure that allows this system to function, are often a primary target. For this reason, it is imperative that the financial sector optimize cybersecurity governance and control in light of each market participant's unique risk profile. The annual audit, as mandated by NYDFS Part 500, can be a cornerstone to these efforts. By following the strategies outlined in this guide and taking advantage of the latest technology enablement capabilities and AI, financial institutions can conduct audits that not only comply with regulatory demands, but also significantly bolster cybersecurity defenses against established and emerging threats. As such they can form a bedrock toward creating and maintaining critical cybersecurity controls.

Of course, an annual audit is just one part of the cybersecurity defense foundation. Financial institutions will also need to maintain vigilance with risk assessment, IT asset management controls and encryption efforts, to name just a few. Demands of regulators, not to mention business-specific risks, will also play a role. Ultimately, it is up to CISOs, compliance officers and others to be proactive, adaptable, and ready and willing to implement new policies and protocols to mitigate the various risks that are sure to arise.

In today's increasingly inter-connected global economy, companies — and particularly financial institutions — find themselves under an almost unrelenting assault from cyber criminals. For this reason, it is imperative that the financial sector gets cybersecurity right.

How Protiviti can help

We know cybersecurity controls testing, risk advisory and we know NYDFS Part 500. Protiviti has helped organizations design, build, and run NYDFS compliance programs since its first effective date in 2017 and have numerous in-flight engagements with clients seeking to address the new requirements and validate their compliance programs. We assist clients in aligning their cybersecurity assurance program with the amended rules and can provide perspectives on emerging approaches and standards as we help our clients plan and execute cybersecurity audits. We can assess the readiness to evaluate your current cybersecurity controls and process to comply with the Part 500 requirements. Protiviti can be your one-stop shop for planning and delivering your cybersecurity audit, reviewing all NYDFS Part 500 documentation including NYDFS certification compliance forms and supporting evidence, propose compensating controls where applicable, reviewing and validating all documentation required for the NYDFS Part 500 certification process. No matter what stage your cybersecurity program is at, we can deliver the requirements you need, as your trusted advisor and partner.

Footnotes:

1. Class A company means a covered entity with at least $20,000,000 in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and the business operations in this State of the covered entity's affiliates and:

    - over 2,000 employees averaged over the last two fiscal years, including employees of both the covered entity and all of its affiliates no matter where located; or

    - over $1,000,000,000 in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and all of its affiliates no matter where located.

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 its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the *Fortune* 100 Best Companies to Work For® list for the 11th consecutive year, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI).

Contacts

David Lehmann
Managing Director
david.lehman@protiviti.com

Tom Luick
Managing Director
thomas.luick@protiviti.com

Lonzo Jackson
Director
lonzo.jackson@protiviti.com

11,000+	90+	25+	$2 BN
Protiviti professionals*	office locations worldwide	countries	in revenue*

THE AMERICAS

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA*
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®