edgile

WHITE PAPER

CLOUD SECURITY

Five Pitfalls for Financial Organizations in Complying with the New York DFS Cybersecurity Regulation

Meeting the Demands of Cyber-security Regulation Requirements

> "It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark."
>
> — New York State Department of Financial Services
> 23 NYCRR 500 Introduction

Tougher rules from various regulatory bodies and governmental agencies are causing fundamental shifts in the way financial organizations establish and sustain IT risk management policies and practices. The new cybersecurity regulation from New York's Department of Financial Services (NYDFS) is a prime example.

The NYDFS Cybersecurity Regulation not only increases the stringency and rigor of cybersecurity for financial institutions, but also broadens the scope. The regulation language suggests that financial institutions can no longer restrict their data security policies to retail-facing consumer information. They must now also protect all non-public information, including commercial accounts.

Many financial institution executives have been hoping to see a walk-back of certain regulatory demands imposed on them in recent years as a result of the new administration in the White House. But no matter what happens in Washington, D.C., institutions will still have to comply with New York's DFS Cybersecurity Regulation requirements.

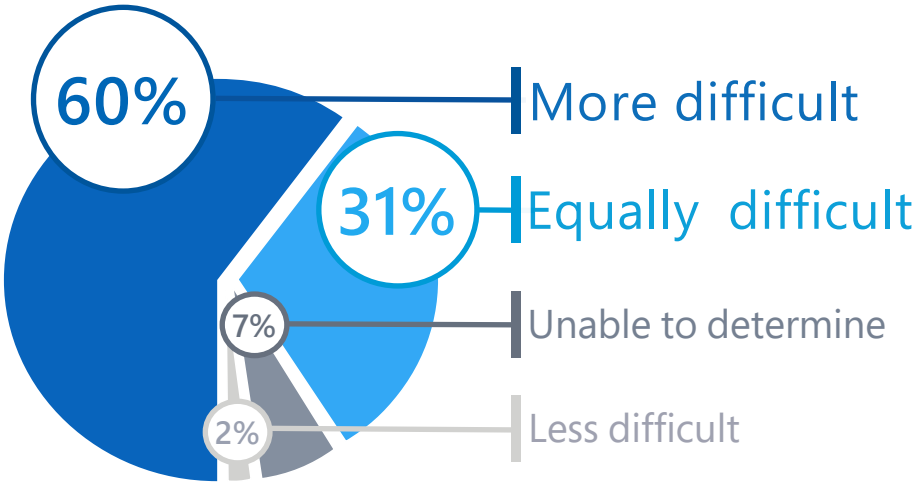
A Focused Risk Management Framework Is Required

There was a time when it was possible for organizations to run compliance programs in isolation for each set of regulatory demands. But the administrative overhead of this approach has grown increasingly difficult. NYDFS requirements go way beyond mandating that a simple checklist of technology capabilities and supporting processes be in place.

Banks, financial services institutions and other relevant organizations need a cybercompliance and IT risk management framework that can focus their priorities and programs, while maintaining the ability to trace everything back to the mandates required for supervisory check-ups.

How Difficult Are the NYDFS Cybersecurity Regulations to Implement?

According to a survey comparing GLBA, HIPAA, PCI DSS and SOX, respondents believe it will be:

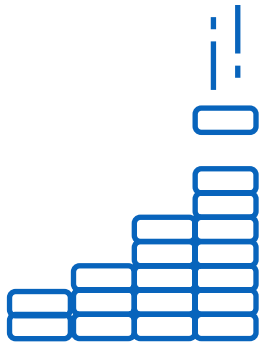


Source: Ponemon Institute, "Countdown to Compliance," 2017

"The approach must be practical, flexible and resilient, otherwise we threaten to undermine our security posture by distracting organizations with uncoordinated, ineffective 'check the box' security protocols that divert resources from more potent security operations and emphasize compliance over security. We, as a nation, cannot take that risk.

— Judith Germano, a senior fellow at the NYU Center for Cybersecurity."

Certification Requirements Raise the Stakes



Much of what's in the NYDFS Cybersecurity Regulation may not be new to a seasoned CISO. What is new is the requirement to certify that an organization is in full compliance with the regulation. This raises the stakes significantly for cybercompliance and risk management, and suggests that it is a very good time for organizations to reevaluate their IT security and risk readiness.

It's a challenge but also an opportunity. Here's a chance to harmonize compliance and risk management practices into a modern cybersecurity program that will reduce the overall risk exposure from both regulators and the bad guys.

Who's Affected?

This mandate points to the undisputable reality of today's security environment: Financial institutions need to adopt better internal hygiene around cybersecurity and data privacy. While this regulation is specifically aimed at organizations operating under or required to operate under NYDFS licensure, registration or charter, it is expected to act as a harbinger of what other states and municipalities are likely to adopt.

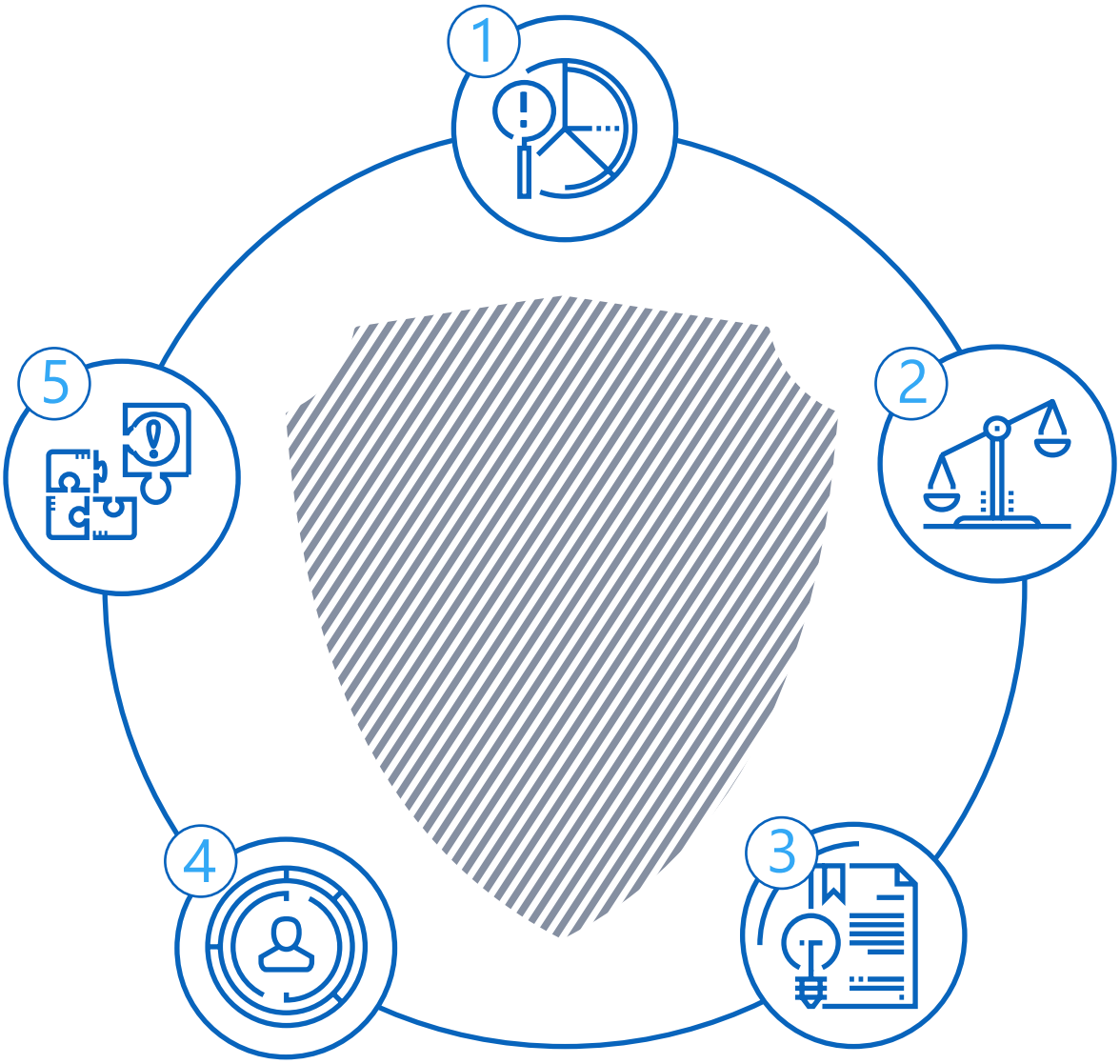
Covered entities include state-chartered banks, licensed lenders, private bankers, foreign banks licensed to operate in New York, mortgage companies, insurance companies and service providers. That final covered entity—service providers—is an important one to understand, given the highly interconnected nature of financial service organizations and their partners, which often are headquartered in different geographies. Those organizations with access to a regulated financial institution's non-public information or information systems, or providing services to New York-based institutions, are included under the mandate.

It's also worth noting that the regulation does exempt certain smaller organizations, such as those with less than $5 million in gross annual revenue derived from New York operations, or those employing fewer than 10 people.

Understanding the 5 Pitfalls

We've identified five pitfalls financial organizations face as they work toward complying with the NYDFS regulation.

1. Relying on Meager Risk Analysis
2. Promising Overly Ambitious Policies
3. Developing Procedures and Practices in a Bubble
4. Failing to Understand the Evolution in Personal Liability
5. Putting Faith in Incomplete Vendor Risk Management Check-Ups



1 Relying on Meager Risk Analysis

The overarching goal of the NYDFS Cybersecurity Regulation is for organizations to thoroughly understand their IT risks. Fundamental to realizing that goal is the ability to conduct thorough risk assessment and analysis and document risk posture against policies and practices over time. Unfortunately, many financial institutions fall short in this department because they fail to institute a comprehensive risk framework that can cover their assessment and analysis needs across all the different requirements from both internal and external sources.

> "To understand the full scope of risk, organizations require a comprehensive view across all business units and risk and compliance functions, as well as key business partners, suppliers and outsourced entities."
> — John Wheeler, research director at Gartner.

A lack of risk management visibility severely hampers an organization's capability of truly moving the needle on their cyber-risk exposure. Without the proper risk analysis, it is very difficult to make decisions on acquisitions, personnel and vendor management based on how those decisions may affect the risk posture. Additionally, a lack of risk analysis documentation makes it difficult to establish a system for stakeholders up and down the food chain to make decisions on mitigating or accepting risk.

Organizations will have trouble complying with the NYDFS Cybersecurity Regulation if they:

- ⊗ Don't have robust risk methodologies in place
- ⊗ Fail to institute risk processes or risk rating systems

Understanding the organization's size and complexity with respect to business practices, products and services is crucial to ensuring that risk evaluation and management is fundamentally sound.

2 Promising Overly Ambitious Policies

Risk-based compliance agencies like NYDFS tend to allow individual organizations to develop their own prescriptive policies. Regulators are less concerned about the technologies being used to mitigate risks and more focused on ensuring that the risks are identified and a reasonable plan of action is in place to address them incrementally over time.

This provides an added degree of flexibility to the compliance equation, but also a great deal of responsibility to figure out what a "reasonable plan" really is. It can be tempting for a financial organization to simply look at the regulations and then create an overly ambitious set of policies with the hope that this will be more likely to satisfy security auditors. That could be a big mistake.

Overpromising—both internally and externally—through unrealistic cybersecurity policies adds tremendous strain to a security program and ultimately increases an organization's risk exposure. Pie-in-the-sky policies that track the stringent requirements specified by NYDFS give external auditors justifiable cause to repeatedly flag an organization for violating its own policies.

Institutions are often better off not including aspirational policy language that could be used against them if litigation occurs.

By default, the regulator's role within an industry provides insight enabling comparisons on how firms adopt new requirements. Avoid overly aspirational commitments and your organizational credibility remains intact. This is too often undervalued as a competitive advantage.

3 Developing Procedures and Practices in a Bubble

Organizations that design procedures and practices without accounting for the costs and realities of implementing them are setting themselves up for failure.

The NYDFS Cybersecurity Regulation includes much more stringent rules around the scope and efficacy of non-public information encryption. **This might cause an organization to overreact with unfeasible data encryption plans.** For instance, recently a large multinational financial institution pledged to encrypt everything within its digital purview, but then had to backpedal when the implementation costs became unsupportable.

Another example is in the realm of access management accreditation. It's easy to promise regulators a quarterly attestation process, but it may be more costly from a process and culture perspective than first expected. This is a surefire way to raise red flags with auditors while simultaneously sabotaging the goal of reducing risk.

While best practices emphasize proof-of-concept-based approaches (i.e., fail fast and cheap), implementation deadlines often constrain decision-making processes. Where feasible, firms may fare better by obtaining benchmarks among peer groups to avoid overcommitting.

4 Failing to Understand the Evolution in Personal Liability

The NYDFS Cybersecurity Regulation significantly steps up the stakes for CISOs, board chairs and members, and other executives, as they're now required to certify compliance with the regulation. This could potentially require them to shoulder personal long-term liability.

If an organization is not compliant with its own policies and the board isn't empowering management and holding them accountable for implementing appropriate safeguards, then board members may face exposure.

This evolution in liability is illustrated by the increased security breaches at major organizations. Take, for instance, the Equifax breach scandal that monopolized national headlines in the fall of 2017. Detailed financial records of 145 million Americans were compromised due to poor patching practices at the credit scoring agency. Equifax's CEO, CIO and CISO all retired amid a firestorm of criticism from the victims, legislators, regulators and the press. NYDFS chimed in on this major incident and made it clear that the agency plans to regulate credit scoring companies alongside other financial institutions. The point here is that the hazards continue to grow for security and line-of-business leaders.

Do you need compliance counsel? With many of the industry experts expressing breach likelihood in terms of "when" rather than "if," CISOs are finding themselves troubled to reconcile the ramifications for certifying compliance against a new law where highly probable events may call their statements into question. Progressive firms are providing legal counsel to CISOs and senior management involved in the certification process to ensure they are comfortable providing the required assertions.

5 Putting Faith in Incomplete Vendor Risk Management Check-Ups

Many mature financial organizations do not perform on-site reviews of vendors. According to a recent Willis Towers Watson survey, only about 56% of U.S. organizations have completed any kind of review of the cyber-risk introduced by contractors or third-party suppliers. Often, organizations check off the vendor review box by simply sending out an overly simplified online questionnaire and calling it a day.

Source: Data Threat Report, "Financial Services Edition", 2017

That's a risky prospect no matter which vendor a financial institution is doing business with, but it is particularly scary when dealing with vendors that may not be familiar with the highly regulated financial sector. Some vendors may have a cultural DNA that does not include any kind of security consciousness.

NYDFS requires financial institutions to ensure that their vendors are in full compliance with the revamped regulation. Organizations that continue to do simple surveys of vendors may fall short of NYDFS standards.

Establishing proper oversight to ensure the compliance of third parties with the NYDFS regulation can and will be an overwhelming task for many of today's firms. While the deadline for full compliance extends to 2019, firms should be careful not to underestimate the lead time required to revise existing contracts enabling "right to audit" and take action to build the assurance capabilities now.

How Edgile Can Help You Avoid These Pitfalls

Edgile provides its clients with accelerators to speed compliance with NYDFS Cybersecurity Regulation requirements. Edgile's enablement approach helps financial institutions add brainpower and deep expertise where it is most needed. This includes services for:

- Developing integrated risk and compliance frameworks
- Establishing policies, standards, processes and procedures
- Identifying, assessing and treating risk
- Designing and implementing cybersecurity technologies and solutions (e.g., access control, access governance, encryption, logging and monitoring, and more)
- Reporting and documenting compliance readiness for audits across multiple mandates
- Edgile delivers technical expertise and a multidiscipline knowledge base across law, privacy, GRC, identity, cybersecurity and risk management. Edgile offers service delivery flexibility in managed services, professional services and staff augmentation models

For more on how Edgile can help organizations address the new NYDFS regulation, please visit www.edgile.com.

About Edgile

Edgile is the trusted cyber risk and compliance partner to the world's leading organizations, providing consulting, managed services, and harmonized regulatory content. Our strategy-first model optimizes IAM, GRC, and cybersecurity both on-premises and in the cloud. By transforming risk into opportunity, we secure the modern enterprise through solutions that increase business agility and create a competitive advantage for our clients.

For more information about Edgile, visit **www.edgile.com**.

TechTarget | Custom Media