GLOBAL CYBER RISK SERVICES

New York Department of Financial Services Cybersecurity Regulation

Foundational solutions that ensure regulatory compliance, mitigate cyber risks and safeguard capital reserves

THE REGULATION:

As part of Governor Cuomo's commitment to protecting consumer data, New York State's Department of Financial Services (NY DFS) has enacted the first-in-the-nation cybersecurity regulation to protect a state's financial services industry and consumers from the ever-growing threat of cyber-attacks.

Effective March 1, 2017, the law requires banks, insurance companies and other financial services institutions regulated by the NY DFS to establish and maintain a cybersecurity program to protect consumers' private data and manage cyber risk.

The new NY DFS regulation has come at a time when federal regulatory agencies are also considering enhanced cyber risk standards for the financial institutions they oversee. We believe the focus from the regulators will require entities to have more robust cyber operational risk management practices in areas such as cyber risk governance, cyber risk management and internal- and external- dependency risk management, as well as incident response and resilience.

THE REQUIREMENTS:

All organizations affected by the regulation must achieve certain milestones by established dates. Some elements of the cybersecurity and risk management program must be in place 180 days after the regulation takes effect. Additional regulatory controls are required to be in effect within the 12-month, 18-month, and 24-month periods. Below is a summary of when controls must be implemented by the covered organization.

Due September 1, 2017:

- The organization shall identify a qualified employee or contractor as Chief Information Security Officer (CISO), responsible for overseeing and implementing the cybersecurity program; and
- The organization shall initiate a cybersecurity program, starting with access control and required policies and procedures.

Due March 1, 2018:

- The appointed CISO shall report in writing annually to the board of directors on the topic of material risks;
- The organization shall implement a monitoring and testing program to assess the cybersecurity program; and
- The organization shall add regular cybersecurity training for personnel.

Due September 1, 2018:

- The organization's cybersecurity program will have written and approved procedures and policies regarding secure development practices for applications developed in-house;
- The organization shall securely manage the disposal of nonpublic information once it is deemed no longer necessary for business purposes; and
- The organization shall implement controls, including encryption, to protect nonpublic information held or transmitted by the organization, while in transit or at rest.

Due March 1, 2019:

- The organization shall have written policies and procedures governing third-party providers' systems that access or store nonpublic information.

While the regulation provides for limited exemptions in some cases, once the exemption no longer applies, an organization will have a very aggressive deadline of 180 days from fiscal year end to achieve compliance.

THE SOLUTION:

We believe the approach taken by the NY DFS is a step in the right direction. Organizations affected by this new regulation should already have some of these requirements in place. However, for those that do not have a mature cyber risk program and would like to move toward compliance, we offer our Cyber Operational Risk Management program.

Alvarez & Marsal's (A&M) Cyber Operational Risk Management program helps organizations understand their current cyber risk maturity level with respect to the new regulation and helps them develop a roadmap to ensure each control is successfully implemented by the required dates.

The A&M Cyber Risk team, in collaboration with your executive management and information security teams, will help address your organization's compliance with the NY DFS regulation through one or more of the following services:

- Aiding directly or through partnership with law firms to determine what aspects of the new regulation are applicable to your organization and what areas — if any — you are exempt from;
- Providing an experienced, qualified individual to act as the CISO responsible for overseeing and implementing the required cybersecurity program;
- Developing and providing some or all of the written policies and procedures as required by the NY DFS;
- Providing a gap analysis identifying what sections of the NY DFS regulation are currently in place, covered by other industry / government regulations, or not implemented;
- Providing a comprehensive risk assessment of information systems to enhance or develop the cybersecurity program;
- Aligning the cybersecurity program with your organization's approach to risk management; and
- Developing a cybersecurity roadmap that will provide an approach to meet the necessary NY DFS requirements for your organization within the timelines dictated by the NY DFS.

A&M'S CYBER AND OPERATIONAL RISK MANAGEMENT APPROACH

A&M brings a deep operational heritage and hands-on approach to delivering cybersecurity solutions that create sustainable operational, regulatory, and financial results. Our Cyber Risk team is comprised of senior professionals uniquely qualified with regulatory and industry experience to address the demands of organizations and to manage cyber and operational risks in a comprehensive manner. A&M's approach focuses on providing foundational solutions that mitigate risk and ensure appropriate levels of capital reserves while maximizing operational effectiveness. We provide an integrated strategy that addresses and manages the full spectrum of threats posed by the dynamic operational and cyber risk landscape.

CONTACT US

A&M Global Cyber Risk Services (GCRS)
Financial Industry Advisory Services
+1 212 763 1958
gcrs@alvarezandmarsal.com

Alvarez & Marsal's GCRS team has extensive experience in designing, developing and implementing effective and sustainable programs. Our seasoned cyber professionals have sat in your chair and possess the right blend of technical and business savvy. Our team has decades of government and private sector experience, which includes defending individuals, companies and nations against the most sophisticated cyber adversaries. We work as advisers, interim leaders and partners who not only tell you what you need to know, but will work side by side with you to achieve your objectives.

When action matters, find us at:
www.alvarezandmarsal.com

Follow us on:

ABOUT ALVAREZ & MARSAL

Companies, investors and government entities around the world turn to A&M when conventional approaches are not enough to activate change and achieve results.

Privately held since 1983, A&M is a leading global professional services firm that delivers performance improvement, turnaround management and business advisory services to organizations seeking to transform operations, catapult growth and accelerate results through decisive action. Our senior professionals are experienced operators, world-class consultants and industry veterans who draw upon the firm's restructuring heritage to help leaders turn change into a strategic business asset, manage risk and unlock value at every stage.

ALVAREZ & MARSAL