BDO KNOWS:
CYBERSECURITY

NEW YORK DEPARTMENT OF FINANCIAL SERVICES ISSUES FINAL CYBERSECURITY REGULATION

SUMMARY

On February 16, 2017, New York's Department of Financial Services (DFS) issued the "first-in-the-nation" cybersecurity regulation.

Effective March 1, 2017, the final regulation requires the thousands of covered financial institutions that do business in the State of New York to conduct a risk assessment and maintain a risk-based cybersecurity program. The regulation, which includes certain minimum regulatory standards, is designed to protect customers' private data and ensure the safety and soundness of New York's financial services industry.

"Covered Entities" under the new regulation include state-chartered financial institutions, licensed foreign banks and insurance companies that operate in New York State, even if they are domiciled outside of New York. To be clear, any covered entity with operations in the State of New York will be required to comply with these regulations.

DETAILS

At a high level, the regulation mandates that covered entities:

- **Conduct a documented risk assessment** upon which the entity's cybersecurity program and policies will be based.
- **Establish a risk-based cybersecurity program** that addresses the following core cybersecurity functions: identify cyber risks; use defensive infrastructure and implement policies and procedures to protect information systems and nonpublic data from unauthorized access; detect cybersecurity events; respond to identified cybersecurity incidents to mitigate any negative effects; recover and restore normal operations and services following an attack; and fulfill applicable regulatory reporting obligations.
- **Adopt a written cybersecurity policy** that addresses, to the extent applicable to the organization's operations: information security; data governance and classification; access inventory and identity management; business continuity and disaster recovery planning and resources; systems operations and availability concerns; systems and network security and monitoring; systems and application development and quality assurance; physical security and environmental controls; customer data privacy; vendor and third-party service provider management; risk assessment; and incident response.
- **Designate a qualified CISO** responsible for overseeing and implementing the organization's cybersecurity program and enforcing its cybersecurity policy. The CISO may be employed by an affiliate or a third-party service provider, but the organization maintains responsibility for compliance and must also designate senior personnel to direct and oversee

CONTACT:

JUDY SELBY
jselby@bdo.com

TIM MOHR
tmohr@bdo.com

KEITH MCGOWAN
kmcgowan@bdo.com

the third party. The CISO, whether employed by a third party or the covered entity, will be required to report to the board or a senior officer at least annually.

- **Implement written third-party cyber risk policies** that, based on the organization's risk assessment and to the extent applicable, 1) identify and assess the risk associated with third-party access to information systems or nonpublic information; 2) establish minimum cybersecurity requirements; 3) confirm strong due diligence processes are used to evaluate the adequacy of third parties' cybersecurity practices; and 4) periodically assess third parties based on the risk they present and the continued adequacy of their cyber practices.
- **Establish a written incident response plan** that outlines the internal and external processes for responding to a cyber event; assigns roles, responsibilities and levels of decision-making authority; identifies remedial measures; sets documentation and reporting requirements; and allows for revision, as necessary, following a cyber event.
- **Notify the superintendent of DFS of any cybersecurity events** that either 1) require notice to be provided to a supervisory entity or 2) have a reasonable likelihood of materially harming business operations, no later than 72 hours after a determination has been made.
- **Submit an annual certification of compliance**, signed by the board chairperson or senior officer(s), to the superintendent by February 15 of each year. This is a certification that the covered entity is in compliance with all the requirements of the regulation. All records, schedules and data supporting this certification must be maintained for five years.

Additional requirements outline rules for monitoring and testing, records retention and proper data disposal, employment and training of cybersecurity personnel, multi-factor authentication (or reasonably equivalent access controls), and encryption of nonpublic information held or transmitted (to the extent feasible).

INSIGHTS

The DFS regulation presents compliance and operational challenges for many organizations, particularly those that fall outside the 50 largest banks. The regulation is more stringent than what we've seen from other governing entities and sets forth a clear timeline for implementation. Many covered organizations have a lot of work ahead of them—and for some requirements, 180 days or less from the March 1 effective date to implement them.

It's easy to see how an entity with a less-mature cybersecurity program might feel daunted by the demands of the DFS regulation. However, the 180-day timeline doesn't apply to everything—for example, covered entities have two years from the effective date to comply with the third-party requirements. A gap analysis can help organizations quickly assess their current policies and operations against all the regulation's requirements, identify holes and prioritize their remediation initiatives to achieve timely compliance.

BDO works with insurers and financial institutions to develop a comprehensive approach to cybersecurity and compliance, taking a 360-degree view of information risk and opportunity. We are well-versed in the DFS regulation, and well-equipped to help clients quickly address any areas of noncompliance. Additionally, BDO's Cybersecurity Risk Assessment Portal, our proprietary state-of-the-art online tool, utilizes our risk scoring algorithm and provides a cost-effective assessment and an easy-to-understand scorecard and report, highlighting areas of strength and uncovering areas for improvement.

For more information about how your organization can get ahead of the NYDFS-proposed cybersecurity regulation, or to learn more about our cost-effective Cybersecurity Risk Assessment Portal, contact any of our NYDFS Cybersecurity team members, including Judy Selby at jselby@bdo.com, Tim Mohr at tmohr@bdo.com, or Keith McGowan at kmcgowan@bdo.com.

About BDO Consulting

BDO Consulting, a division of BDO USA, LLP, provides clients with Financial Advisory, Business Advisory and Technology Services in the U.S. and around the world, leveraging BDO's global network of more than 67,000 professionals. Having a depth of industry expertise, we provide rapid, strategic guidance in the most challenging of environments to achieve exceptional client service.

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 500 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 1,400 offices across 158 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm's individual needs.