CARLTON FIELDS

Regulators Demand Third-Party Risk Management

April 10, 2017

While third-party risk management has been a required component of an effective enterprise risk management program for many years, the topic is receiving elevated attention at insurance companies and related businesses. The recently effective New York State Department of Financial Services (NYDFS) cybersecurity standards for NYDFS licensed financial institutions and the current proposed draft of the NAIC Insurance Data Security Model Law require licensees to implement specific policies and procedures designed to protect the security of company information systems and nonpublic information (including personally identifiable information of customers and policyholders) that are accessible to, or held by, outside service providers as part of an overall cybersecurity program. The regulators recognize that an entity's cybersecurity program should start with, and be based on, the results of a risk assessment. The risk assessment should take into account factors specific to the entity, such as its size and complexity. However, regardless of specific regulatory mandates, every well-designed third-party risk management program should include the following:

- an analysis of the particular risks associated with the service organization and the services to be provided;
- baseline cybersecurity and other requirements to be eligible for hire;
- due diligence steps to be followed prior to contracting with a third-party;
- standard contractual provisions;
- mechanisms to monitor performance and compliance under the contract; and
- address termination and post-contractual procedures.

Implementing an appropriate third-party risk management program will require enterprise-wide engagement, including the participation of representatives from areas such as business units,

procurement, sourcing, IT, risk, compliance, internal audit, legal, privacy, and the individual designated to manage the program.

Related Practices

Cybersecurity and Privacy
Financial Services Regulatory

Related Industries

Life, Annuity, and Retirement Solutions