AN ALERT FROM THE BDO FINANCIAL SERVICES PRACTICE

ASSET MANAGEMENT INSIGHTS

SEC RISK ALERT: OCIE FOCUSES ON CYBER STANDARD COMPLIANCE

On August 7, 2017, the SEC published a Risk Alert (the "Alert") detailing the results of the Office of Compliance and Examinations' (OCIE) Cybersecurity 2 Initiative, which builds on the observations from its first round of cyber examinations announced in April 2014.

For the Cybersecurity 2 Initiative, OCIE examined 75 firms including broker-dealers, investment advisers and investment companies registered with the SEC to assess cybersecurity preparedness, with more emphasis on validation and testing of procedures and controls than had been performed in previous examinations. These most recent examinations focused on the written policies and procedures covering 1) Governance and Risk Assessment, 2) Access Rights, 3) Data Loss Prevention, 4) Vendor Management, 5) Training and 6) Incident Response. The Alert can be useful as a benchmark to use in evaluating your firm's cybersecurity program.

The Alert noted an overall improvement in firms' awareness of cyber-related risks since the previous examination initiative. Perhaps most significant were the number of firms which had adopted written policies and procedures addressing the protection of sensitive information. Additionally, the vast majority of firms examined by OCIE conducted periodic risk assessments to identify threats, vulnerabilities and the business consequences of a cyber incident.

While the industry showed overall improvement, the OCIE examinations identified one or more issues requiring attention in most of the firms reviewed. Some of the more common issues included:

- Written policies and procedures were not adequately tailored to the risk profile of the firm nor were they consistent with the actual practices the firm followed.
- The systems maintenance processes in place to make sure that systems were patched were not adequate.
- Risks identified through penetration testing were not addressed in a timely manner.
- Employee training was either inadequate or there was no process in place to ensure that training was completed.

Finally, the Alert identified certain best practices that firms should consider including in their program:

- Maintaining a complete inventory of data and information accessible by third-party vendors and service providers.
- Maintaining prescriptive schedules and processes for testing data integrity and vulnerabilities. This includes employing adequate penetration and vulnerability

For more information about how your organization's cybersecurity program stacks up, please contact

Mike Stiglianese
BDO National Technology & Cybersecurity – Financial Services Industry Lead
mstiglianese@bdo.com.

Read more ▶

testing along with adequate patch management procedures.
- Maintaining acceptable use policies along with other procedures for controlling the access to sensitive information and systems. This includes employing adequate controls to terminate access where appropriate.
- Maintaining adequate employee training and processes to make sure senior management is engaged in the cybersecurity program.

BDO INSIGHTS

It is clear the SEC considers cybersecurity one of the top compliance risks facing financial firms. OCIE will continue to scrutinize cyber preparedness in all compliance examinations, evolving the standard from check-the-box implementation to the satisfactory implementation of policies, procedures and controls. Firms should leverage the information in the Alert to make sure they address any identified issues from this round of examinations relevant to their organization and adopt the best practices to improve their existing cyber programs. In addition, all policies and procedures should be reviewed to make sure they reflect the firm's actual practices. As OCIE's focus moves to implementation effectiveness, the key to compliance will be not only instituting risk-based policies and procedures, but ensuring they are followed.

HOW DO I GET MORE INFORMATION?

IGNACIO GRIEGO
Assurance Partner
San Francisco
415-490-3182
igriego@bdo.com

KEITH MCGOWAN
Assurance Partner
New York
212-885-8037
kmcgowan@bdo.com

JONATHAN SCHMELTZ
Tax Partner
New York
212-885-8170
jschmeltz@bdo.com

SAMUEL SEAMAN
Tax Partner
San Francisco
415-490-3157
sseaman@bdo.com

BHARATH RAMACHANDRAN
Assurance Partner
Boston
617-239-4161
bramachandran@bdo.com

MATT DEMONG
Tax Partner
Boston
617-422-7575
mdemong@bdo.com

NICK MAROULES
Assurance Partner
Chicago
312-730-1332
nmaroules@bdo.com

JOE PACELLO
Tax Partner
New York
212-885-7375
jpacello@bdo.com

DARIN SCHINDLER
Tax Partner
Pittsburgh
412-281-7618
dschindler@bdo.com

People who know Asset Management, know BDO.

BDO'S FINANCIAL SERVICES PRACTICE

BDO's Financial Services Practice provides assurance, tax, and advisory services to asset management entities, primarily Hedge Funds, Private Equity Funds, Broker Dealers and Mutual Funds. The practice services over 600 advisors nationwide with funds ranging from start-up funds to those with billions under management.

ABOUT BDO USA

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory 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 550 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 67,700 people working out 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.