Best Practices for Registered Investment Adviser Business Continuity Plans

By David J. Baum and Brian Lawrence, Alston & Bird LLP*

Over the last several years, certain significant events, primarily weather-related disruptions such as Hurricane Katrina and Hurricane Sandy, severely tested the ability of registered investment advisers (RIAs) to continue their business operations and led to an increased focus by the Securities and Exchange Commission (SEC) on the effectiveness of RIA business continuity and disaster recovery plans (BCPs).

The SEC's increased focus on RIAs' BCPs culminated in June 2016, when it proposed new Rule 206(4)-4 under the Investment Advisers Act of 1940, as amended ("Advisers Act"). This rule would specifically require RIAs to adopt and implement written business continuity and transition plans "reasonably designed to address operational and other risks related to a significant disruption in the [RIA's] operations," and require these BCPs to address, at a minimum, certain specific issues.

While proposed Rule 206(4)-4 has not yet been adopted, RIAs should nonetheless review their BCPs and ensure that they address many of the issues identified in the proposal and incorporate certain best practices so that they are better positioned to respond to and recover from significant business disruption events.

David J. Baum, Partner, Alston & Bird LLP

Brian Lawrence, Associate, Alston & Bird LLP

Regulatory Background

Rule 206(4)-7

Rule 206(4)-7 under the Advisers Act requires RIAs to adopt and implement written compliance policies and procedures reasonably designed to prevent violations of the Advisers Act. In the 2003 adopting release for Rule 206(4)-7, the SEC stated that an RIA should address BCPs in its written compliance policies and procedures to the extent that they are relevant to the RIA. Neither Rule 206(4)-7 nor its adopting release, however, provided much, if any, guidance on the critical components of a BCP or addressed the specific issues, areas, or factors that an RIA should consider in developing and implementing its BCP. Accordingly, it is not surprising that the SEC found, as noted in the proposing release for Rule 206(4)-4, that BCPs among RIAs can be "uneven and, in some instances, may not be sufficiently robust to mitigate the potential adverse effects of a significant business disruption on clients."

National Exam Program Risk Alert

On August 27, 2013, the SEC's National Examination Program (NEP) issued a NEP Risk Alert, based on the NEP staff's review of the BCPs of approximately 40 RIAs in areas impacted by Hurricane Sandy the previous year. In the NEP Risk Alert, the NEP staff described its observations and lessons learned from the BCP review, which included: (1) the general BCP policies and practices of the RIAs it examined; (2) notable practices of RIAs that were able to perform critical business operations and maintain more consistent communications with clients and employees while operating under their BCPs; and (3) BCP weaknesses of RIAs that experienced more interruptions in their key business operations and inconsistently maintained communications with clients and employees. The NEP Risk Alert also addressed areas that RIAs should consider when reviewing their BCPs. The NEP Risk Alert provides substantial guidance for RIA BCPs and appears to have had a significant influence on proposed Rule 206(4)-4.

Continued on page 11

Proposed Rule 206(4)-4

On June 28, 2016, the SEC proposed new Rule 206(4)-4 under the Advisers Act, as well as amendments to certain current rules under the Advisers Act, which would require RIAs to adopt and implement written business continuity and transition plans. In the proposing release for Rule 206(4)-4, the SEC indicated that it was particularly concerned with those risks that may impact the ability of an RIA and its personnel to continue operations and provide services to clients and investors, including such operational risks as technological failures of systems and processes and the loss of RIA or client data, personnel, or access to the RIA's physical location(s) and facilities. Accordingly, under the proposed rule, an RIA would be required to assess and inventory the components of its business, including operational and other risk related to significant disruptions in its operations, and design and implement BCPs tailored for such specific risks. Specifically, an RIA's BCP would be required to address, among other things: (1) the maintenance of critical operations and systems and the protection, backup, and recovery of data; (2) pre-arranged alternative physical location(s) of the RIA's office(s) and/or employees; (3) communications with clients, employees, service providers, and regulators; and (4) identification and assessment of third-party services critical to the operation of the RIA.[1]

Best Practices

While proposed Rule 206(4)-4 has yet to be adopted, the proposal and NEP Risk Alert provide RIAs guidance on best practices that can be incorporated into BCPs. These best practices can help RIAs fulfill their fiduciary obligations to their clients, which, according to the SEC, requires an RIA to take steps to protect its clients from being placed at risk by the RIA's potential inability to continue to provide advisory services during a business disruption event.

RIAs should consider forming special committees to plan, develop, test, and if necessary, execute the RIA's BCP. These committees should be composed of business unit staff and senior management to ensure that the BCP fully reflects the RIA's business.

General Considerations

In preparing a written BCP, RIAs should ensure that the BCP addresses critical systems of the RIA and is specifically tailored to the RIA's business (*i.e.,* boilerplate BCPs are not sufficient). RIAs should also regularly update their BCPs to reflect new regulatory requirements.

RIAs should consider forming special committees to plan, develop, test, and if necessary, execute the RIA's BCP. These committees should be composed of business unit staff and senior management to ensure that the BCP fully reflects the RIA's business. Similarly, RIA compliance personnel should work collaboratively with various business lines in designing BCPs and should seek to achieve redundancy in key services and operations. RIA compliance personnel should work collaboratively with senior management and the RIA's various business units, including technology, information security, operations, human resources, communications, legal, compliance, and risk management. Working collaboratively across various business units should help RIAs create more robust and comprehensive BCPs that fully reflect the RIA's business, and creating redundancies in key services and operations should help RIAs continue operations if they have certain key service providers experience issues of their own.

Additionally, RIA BCPs should contemplate backing up the RIA's books and records (both physical and electronic). Finally, RIAs should require all business units to identify contingency scenarios that would affect operations and derive multiple solutions to help ensure that the RIA can continue operations should such scenarios take place.

Widespread Disruptions

BCPs should address and anticipate widespread disruptions, including possible interruptions in the key business operations and loss of key personnel for extended periods. RIAs should distribute their BCPs widely within their businesses and operations to ensure that their employees are familiar with both the contents of the BCP and their roles under the BCP. Additionally, RIAs should consider requiring employees to acknowledge receipt of BCPs annually. Finally, BCPs should consider continued facility and systems operations with widespread remote access by employees.

Alternative Locations

RIA BCPs should take into account the potential need for maintaining critical business functions at alternative/backup locations. RIAs could potentially accomplish this by establishing a remote, backup location with an unaffiliated RIA or using employees' homes, branch offices, data centers, or hotels as alternative locations. RIA BCPs should also account for the possibility of significant regional events, such as Hurricane Sandy, disrupting entire regions and power grids. While more local alternative/backup locations may be appropriate for certain disruptions, RIA BCPs should account for the potential for such locations being affected in the same manner as the RIA's principal location. Further, RIAs should evaluate how to operate when faced with the possibility of electrical failure and the loss of other utility services (*e.g.,* cable or phone).

If necessary, whenever possible, RIAs should switch to backup sites or systems in advance of trouble rather than waiting for shutdown or imminent threat to avoid prolonged business disruptions.

Continued on page 12

Continued from page 11

Vendor Relationships

As many RIAs are heavily dependent on outside service providers in running their advisory businesses, RIAs should evaluate the BCPs of their service providers regularly. In doing so, RIAs should maintain a list of vendors and contacts at each vendor for ease of access.

RIAs should consider reviewing the information technology infrastructure of service providers and may wish to consider whether, based on risk, it is necessary to have multiple backup servers. If an RIA is heavily dependent on a service provider, the RIA should consider how weather-related and other events could impact that service provider since disrupted operations at a key service provider could lead to unforeseen operational challenges for the RIA.

Telecommunications Services and Technology

RIAs should avoid relying on one telecommunications service provider and should consider contracting with multiple telecommunications carriers to provide a failover (*i.e.,* a method of protecting the RIA's computer system from failure by having standby equipment at a different carrier automatically take over during a system failure). RIAs should also implement technology to allow employees to work from remote sites (*e.g.,* from home). Potential examples of such technology include Citrix and virtual private network (VPN) or internet-based access portals. Additionally, RIAs could consider maintaining current portfolio data at multiple service providers and testing the connectivity to the providers to ensure that the data remains accessible from remote locations during periods of disruption.

An RIA should consider the following practices in its physical location:

- Having key power systems tied to the RIA's generators so electricity and air conditioning are available for the entire building (the NEP Risk Alert observed that this consideration was especially important in a multitenant building with no electricity backup).
- Adequately maintaining system capacity (physical and electronic) to accommodate staff who may be displaced and may need to work from home or an alternative location.
- Establishing and testing server internet connection via wireless cards for use if the primary connection becomes lost.
- Elevating electronic equipment to mitigate the risk of damage in case of flooding.

Further, RIAs should consider engaging service providers to ensure that backup servers function properly (the NEP Risk Alert observed that RIAs that relied solely on self-maintenance experienced more interruptions in their key business operations). Similarly, RIAs should consider having alternative internet providers available or obtain guaranteed redundancy from internet providers, and RIAs should explore the appropriateness of keeping backup files and systems separate from the RIA's primary office location (*e.g.,* via cloud computing).

Finally, RIAs should generally consider and address as relevant the operational and other risks related to cybersecurity, including having RIA BCPs contemplate monitoring incidents and communicating protocols of key service providers regarding cybersecurity.

Communications Plans

RIAs should include in their BCPs a plan for maintaining continuous communication with their employees during significant business disruptions. Such a plan should indicate which of the RIA's employees are responsible for executing and implementing the various aspects of the plan, and the RIA should plan for communicating with its employees regarding the status of the RIA's business, operations, and backup locations.

RIAs should also consider regularly communicating the status of their operations with their clients, such as through the RIA's website, a recorded message at the RIA's main number, etc. Additionally, RIAs should consider contacting clients directly, and/or via an email blast, before a foreseeable business disruption event such as a major storm to see if they have any transactions they will need executed if an extended outage occurs. Examples of such transactions include cash raised, funds transferred, and wire instructions executed.

Finally, an RIA's BCP should contemplate communication with regulators during significant business disruptions.

Review and Testing

RIAs should regularly (at least annually) conduct tests of their BCPs and should consider specifically testing their BCPs in anticipation of certain significant business disruptions (*e.g.,* before a major storm). RIAs should consider testing the operability of all critical systems under the BCP using various scenarios. Such testing may minimize disruptions to operations because critical weaknesses may be identified and resolved and personnel may become better acclimated to using key systems while in the BCP mode. Additionally, RIAs should consider testing generators frequently to ensure they are working properly (the NEP Risk Alert observed that some RIAs tested generators at least weekly). Finally, RIAs should avoid vendors that provide disincentives to BCP testing (*e.g.,* charging extra for tests).

Conclusion

While proposed Rule 206(4)-4 has yet to be adopted, RIAs should still review their BCPs and consider their overall effectiveness and relevance to the RIA's business operations now. By ensuring that their BCPs are tailored and incorporate a number of these best practices, RIAs are likely to be better positioned to respond to and recover from significant business disruption events and therefore meet their fiduciary obligations to their clients.

Continued on page 18

IACCP CERTIFICATION AND COMPLIANCE TRAINING

The Investment Adviser Certified Compliance Professional® (IACCP®) program is designed to advance investment adviser compliance as a profession. The program was established by National Regulatory Services in 2004 and is cosponsored by the IAA. Certification requirements include education, work experience, examination, ethics, and continuing education. Go to **www.investmentadviser.org >> Events >> IACCP Training** to view the full training schedule. To learn more about the IACCP certification program, contact IAA Special Counsel Paul Glenn at (202) 293-4222 or paul.glenn@investmentadviser.org.

ONLINE SESSIONS

Except as noted, online session times are 1:00 - 3:00 pm ET

January 12	Cybersecurity
January 19	Form ADV Part 1: Annual Updating Amendment and More
January 24	Form ADV Part 2: Identifying and Disclosing Conflicts
January 26	DOL New Fiduciary Rule – Part 1
January 31	Investment Adviser Performance and Advertising
February 2	Investment Adviser Codes of Ethics: The Rule Plus Implications of Gifts and Whistleblowers
February 7	Introduction to the Advisers Act
February 9	Trading Practices, Portfolio Compliance and Related Enforcement Cases
February 14	State-Registered Investment Advisers: A Compliance Tutorial for Working with State Regulators
February 23	Books and Records Requirements for Investment Advisers
February 28	Insider Trading and Advisory Contracts
March 2	IACCP Exam Study Session *1:00 - 4:00 pm ET*
March 7	Trading Compliance: Best Execution, Soft Dollars and Directed Brokerage
March 9	SEC Examination and Enforcement Update for Investment Advisers
March 14	Understanding Fiduciary Duties and a Sweep of Certain Anti-Fraud Provisions of the Advisers Act
March 16	FINRA Priorities 2017
March 21	DOL New Fiduciary Rule – Part 2
April 4	Advisers Act Anti-Fraud Rules: Custody, Political Contributions, Solicitors and Proxy Voting Requirements
April 6	Valuation and Trade Errors
April 13	Compliance Programs Rules and Strategies for Managing Your Annual Review
April 18	Anti-Money Laundering, ERISA and '34 Act Section 13 Reporting for Investment Advisers
May TBD	Critical Skills for High-Performance Compliance Professionals
May TBD	Ethical Decision-Making for Compliance Professionals *(approved for IACCP CE Ethics credit)*
May 16	Data Protection: Privacy, Identity Theft and Cybersecurity
May 23	Investment Adviser Regulatory Update

COMPLIANCE CORNER—*continued from page 12*

** David J. Baum is a partner in the Financial Services & Products Group of Alston & Bird LLP located in the Washington, DC office. David's practice includes counseling investment companies and investment advisers on a wide range of issues under the federal securities laws. He can be reached at (202) 239-3346 or david.baum@alston.com.*

Brian Lawrence is an associate in Alston & Bird's Financial Services & Products Group. He can be reached at (202) 239-3194 or brian.lawrence@alston.com.

[1] In addition to these BCP requirements, proposed Rule 206(4)-4 would also require RIAs to incorporate transition plans relating to certain transitions such as retirement or loss of key personnel, bankruptcy, acquisition, or the impact of financial stress at affiliated firms. While RIAs should also consider transition plans, this article focuses only on the BCP aspects of the proposed rule.