PRACTICE NOTE: Compliance checklist for operating during a pandemic

Published 24-Mar-2020 by Julie DiMauro, Regulatory Intelligence
Expert Analysis

As the global COVID-19 pandemic spreads, compliance and risk departments at financial services firms have been on high alert and working overtime as firms switched on business continuity plans, closed offices and sent employees home to work.

Establishing and maintaining continuity plans is a normal part of the compliance and risk function. Review of BCPs is also a standard part of exams by regulators. The fact that virtually every firm has now had to enact at least some parts of their BCP, it is logical that regulators will ask how things went in the next exam cycle.

Below, we provide a checklist for compliance and risk professionals regarding the altered work landscape for employees as a result of the pandemic. The list is broken into two parts: items that require attention at all firms, and a section with links of useful resources.

Checklist for businesses

— Business continuity strategies must be sufficiently flexible to address a wide range of possible scenarios, including pandemics – even long-duration, multi-national ones.

They should spell out remote access solutions, emergency procedures that outline how to recover data and equipment, reach employees and security specialists, protect the integrity of the physical workspaces the business owns. The back-up systems must be well-established and responsibilities over providing access must be clear. A point person should be routing inquiries and sending updates to top executives and the board of directors.

— Consider whether and how vendors can fulfill their obligations. Speak with counsel about how contract terms can be altered and emergency provisions triggered. Force majeure or unforeseeable circumstances clauses are not as straightforward as one might think, and there can be a high hurdle in meeting unique ones.

— Remind employees of the heightened cybersecurity risk of working remotely, specifically phishing and ransomware attacks. Remote workers must also be reminded of the necessity to safeguard customer records and privacy information. Consider prohibiting the printing of any business documents at home.

— Archiving communications between staff and clients is perhaps one of the most common work-from-home pitfalls. Reminding and training remote workers of this essential task along with other safeguard measures is vital.

— Firms should anticipate additional burdens on IT Help Desks as more individuals work remotely and experience technology problems. Firms should be sure all help desks are adequately trained and staffed to handle increased volumes.

— Compliance and risk departments should also coordinate a review and testing with technology departments. The compliance team and the tech department should test the company's remote VPN capacity and measure connection speeds.

— Firms should also redistribute all relevant company policies related to the use of personal computers, smartphones, tablets, and WiFi networks and remind staff that the policies still apply to those working from home, and security protocols will not be relaxed.

— Remote work requires training personnel to be able to spot fraudulent behavior and report it promptly; phishing scams can increase during emergency periods like pandemics.

— The creation of a pandemic task force or committee is valuable to coordinate information from various business lines, and departments including; IT, human resources, compliance, risk, operations, facilities, and communications.

— Compliance and HR departments should also be careful to protect personal medical information under applicable health privacy regulations such as Health Insurance Portability and Accountability Act (HIPPA) if employees become infected or ill. Despite a perceived need to share such information, it is imperative to maintain individual employee health privacy, and counsel should be consulted on when and how disclosures can be made.

— Compliance, risk, and senior management must take inventory of essential employees and determine how many and which personnel are needed onsite at various locations and consider backup personnel as well under various business disaster or disruption scenarios. Contact information for all personnel, especially key employees, should be updated.

— Regulatory filing deadline relief for disclosures and registrations can be made us of. Firms must summarize why the relief is needed. Impediments should be listed with specificity, like disruptions to transportation, limited access to facilities and support staff, etc. Include the virus as a source of uncertainty in any management discussion and analysis.

— If no-action relief is sought from the regulator, explain why the relief is needed as a commonsense or ethical solution, even if not technically permitted.

— For corporate board meetings, a change of meeting time, date and communication medium should be noted in the proxy statement, if there is still time.

— Protecting data at all costs is essential. Cybercriminals might use this pandemic as a means of scamming customers and compromising data. Keep clients, regulators and the workforce informed on cybersecurity solutions for computers, networks and your encrypted connectivity. Enforce policies regarding personal computers and phones and what data can be accessed by whom.

— Tell customers what is being done behind the scenes to be able to provide continuing service, and what delays they might experience

— Review the business's insurance coverage. Business interruption and supply-chain coverage, including contingent business interruption, will typically require a showing of property damage that gave rise to the loss. They typically offer very limited coverage for pandemic diseases, due to exclusions and sub-limited coverage.

— Ideally, members of the emergency response organization have received training on performing their duties and on testing the BCP's effectiveness with relevant courses and emergency exercises before a pandemic or other emergency strikes. But don't feel it's too late now: Start the training as soon as possible, and remember the responses to this pandemic need to change with it and with legal authorities' directives.

Industry professionals weigh in

"My business has a significant present in Puerto Rico, and dealing with Hurricane Maria really forced us to refine our business continuity and emergency preparedness," said John Vaccaro, CEO of MassMutual Financial Advisors in Springfield, MA. "Thanks to being battle-tested, we feel like we have the right processes in place to deal with the investments our clients worry about, and the right technology in place to contend with remote working."

Vaccaro advises other firms to use a variety of communication methods to make sure you reach those employees possessing different familiarity and comfort levels with a range of tech tools. He also encourages businesses to reach out to their federal and state regulators, as he has found them to be receptive and informative during this considerably uncertain time.

"My biggest concern is technology and trading, because as markets break down, volume spikes and liquidity shrinks and I want to be confident I can manage portfolios and positions without interruption," said Eric Sams, president at E&E Financial Services, Inc. in San Diego.

"And I want to ensure the financial viability of my broker-dealer/registered investment advisory firm, so I make sure we have sufficient capital to weather the storm. Finally, I must communicate with clients, keeping them informed and being transparent, but without causing them to panic," he said.

"At AFS, each of us has a mi-fi (mobile hotspot) device so we have a back-up internet connection if our main lines go down or if we need to spread the surge in bandwidth to additional

lines," added Daniel Nikci, founder and managing partner at Applied Fund Solutions, LLC in New York. "We also are a paperless firm, which is coming in handy as we all work remotely."

Additional resources

The Securities Industry and Financial Markets Association (SIFMA) trade group has a web page with links to an operational resiliency podcast, and numerous resources related to industry guidance, BCPs and COVID-19.

The SEC issued a coronavirus directive calling for transparency on the part of firms in disclosing material risks and operational concerns to investors, adding that it would ease regulatory burdens modestly and "consider additional relief from other regulatory requirements" if needed.

The bank regulators have a coronavirus disease 2019 portal of announcements and information for regulated businesses. "Regulators note that financial institutions should work constructively with borrowers and other customers in affected communities," said one statement. "Prudent efforts that are consistent with safe and sound lending practices should not be subject to examiner criticism."

The Financial Industry Regulatory Authority (FINRA) released a regulatory notice advising brokers to review their business continuity plans and consider their preparations for such pandemic situations.

FINRA has provided a Small Firm Business Continuity Plan Template as an optional tool to aid small firms. Another valuable resource can be found in items 16 and 18 in the FINRA Business Continuity Planning FAQs, which discuss a firm's preparation and testing efforts, particularly related to pandemics.

There is an annual requirement to review BCPs under FINRA Rule 4370, saying such plans should address the critical areas all noted above – from data backup and recovery, to communications with customers and regulators, to customer access to funds.

FINRA Regulatory Notice 09-59 was released in 2009 as a result of the outbreak of influenza A (H1N1) or swine flu, and it continues to help firms understand the risk-mitigating actions and appropriate measures to prepare for the effects of a pandemic.

NOTE: For a regularly updated list of U.S. regulations related to the COVID-19/novel coronavirus update, please click on this link to the Skopos Labs Coronavirus Policy Tracker: https://coronavirus.skoposlabs.com

(By Julie DiMauro and Todd Ehret, Thomson Reuters Regulatory Intelligence in New York.)