

Don't Let Unimplemented Changes Place Your Compliance Program at Risk

For financial organizations, data security is king. Given the amount of secure information that comes across the computers and desks of everyone from investment advisors to private equity firms, both clients and regulatory agencies expect financial professionals to handle the information wisely and securely.

When most of the business world shifted - nearly overnight - to remote work in the spring of 2020, those in the financial sector seemingly took all the sensitive information they process daily home with them, opening pandora's box.



This abrupt change created serious data privacy and security risks due to the lack of regular oversight, the inability to follow normal protocols, sloppy record-keeping and unintentional insecure data practices - driving up risk for the firm.

Updating Compliance Standards

In guidance issued last summer, the SEC put the industry on notice that enforcement and examinations will be stringent due to the new “operational, technological, commercial and other challenges and issues” faced by many SEC registrants, which it noted have created “important regulatory and compliance questions and considerations.”

The SEC Office of Compliance Inspections and Examinations recommended the following:

1. Implementing additional steps to validate the identity of the investor and the authenticity of disbursement instructions.
2. Remote oversight of trading, including reviews of affiliated, cross, and aberrational trading, particularly in high volume investments.
3. Modified or enhanced security and support for facilities and remote sites to secure communications or transactions occurring outside of the firms’ systems.

Many firms immediately worked to update their policies and procedures for remote employees, reevaluating their supervisory priorities and reporting requirements, but lacked the technological infrastructure and know-how to properly translate their in-office security measures to remote settings.

Benefits of Compliance Technology

Without the right technology in place, logins, financial data and more can potentially be exposed both in-office and during remote work, with a continual risk for fraud and conflicts of interest. The ever-evolving response to the pandemic has driven up the need for compliance technology as a vital partner in the task of staying compliant. As Tom C.W. Lin notes in *The Temple 10-Q*, “The key to addressing many of the challenges posed by adapting old practices and operating under new rules during this unprecedented pandemic lies in technology.”

It’s important for firms to take a step back and consider if technology can streamline their approach to dealing with shifting compliance priorities. This isn’t always easy to execute – one survey flags corporate governance as key to deploying compliance technology correctly. When evaluating firms should

consider:

- Budget limitations
- Existing IT infrastructure
- Buy-in by boards and risk and compliance functions

A Comprehensive Solution

The financial compliance management software offered by BasisCode Compliance enables firms to automate processes securely, dramatically reducing the risks inherent to complicated paper processes. The software was built specifically for those in the financial services sector, so the platform intuitively addresses the many risks unique to the field, like handling employee conflict of interest and Code of Ethics administration.

With an expert tech solution guiding risk and compliance, financial firms are on stronger footing to stay within protocol, satisfying both regulatory agencies and clients—and supporting ongoing growth.