Financial Services

Regulatory compliance for RIAs: the time to address IT is now

By Cynthia Doe and Daniel New

With new Dodd-Frank rules looming, registered investment advisors must act quickly – but diligently – to make certain that their information technology can support new compliance requirements.

As registered investment advisors (RIAs) tailor their operations to meet the requirements of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), some are finding that that their information technology group (IT) is not ready to support new compliance processes and requirements. Dodd-Frank, passed in July 2010, will require an expanded class of companies to register. After registering, these new RIAs, like existing RIAs, will be required to implement written compliance policies and procedures, perform annual compliance assessments and will be subject to SEC examination, among other changes.

To be successful, the compliance strategies that RIAs implement must be supported by robust processes and technologies. But because some companies fail to bring IT into the compliance planning process from the beginning, they find themselves stuck with processes that IT cannot support or that are not sustainable. And others have not performed adequate assessments of their IT capabilities to identify and remediate shortcomings.

In this article, we examine how current and future RIAs should work with IT to create and/or enhance policies and upgrade procedures and systems to support Dodd-Frank compliance initiatives. We also discuss specific areas – records management, email retention, oversight of third-party service providers and business continuity, among others – that should be the focus of successful compliance strategies.

Compliance with the new requirement mandates not only careful planning, training and implementation, but also a thorough capabilities assessment of the IT systems that make compliance possible. Through such an assessment, IT can identify gaps between the technology's capacity and existing processes and the specific demands of new compliance requirements, and make improvements as needed.

Ernst & Young
Quality In Everything We Do

The real key to success, however, is making IT a full partner — from the beginning — in crafting a compliance strategy. With adequate time and a full understanding of the technological needs of each stakeholder, IT can be a change enabler and catalyst. However, if planners treat technology considerations as an afterthought — as many do — compliance initiatives will inevitably face challenges that could you unable to stand up to the rigors of an SEC examination and expanded reporting.

Setting a baseline

An effective technology plan for registration as an RIA should begin with a baseline current-state assessment of IT policies, procedures, risks and control activities. The ultimate goal of this assessment is to identify and document necessary improvements in the key compliance technologies and related processes that your RIA compliance program. When reviewing IT's current capabilities and capacity, focus on the following areas:

Electronic records management

Successful regulatory compliance requires a sophisticated ability to archive, maintain, report on and recall relevant operational data. Of all the IT focus areas, records management will likely be the most complex and challenging. It entails capturing written and electronic records, historical data, data acquired through acquisitions and multiple copies of the same files that reside in different locations throughout the company. From the outset, compliance, operations and other stakeholders must work with IT to determine which systems contain the official books and records, a process that can be challenging. Beyond categorizing data, IT must also correlate it to software/application systems, associated servers and databases, network drives and other data repositories and create a current archival inventory. During this process, IT can identify gaps where archival tools and processes are missing or insufficient to meet the demands of the compliance plan and take remedial action.

Protection of investor data

Working with stakeholders throughout the company, IT should review its data protection and security and privacy policies to identify any gaps between existing security policies and SEC requirements. With this information, IT can create a risk-based remediation plan to address these gaps through technology enhancements and procedural adjustments, such as expanding entitlement reviews to cover additional systems and privileges. IT should track the progress of its remediation efforts closely to ensure that all procedural/technology gaps are closed. It is vital that IT keep all data protection tools, practices, policies and procedures current on an ongoing basis, and deploy these enhanced security measures in new systems and processes.

Email and IM retention

RIAs must be able to archive all email and instant message communications. Companies that do not have archival tools or third-party service providers in place should look to acquire these tools or contract with a specialty third-party service provider that can meet compliance's needs. These tools should work seamlessly with existing security and archival systems and provide monitoring of load status, data purges and changes to key logging and retention settings.

Business continuity

Companies typically create business continuity plans for moments of crisis or temporary technological interruption, and IT is usually the steward. As the organization changes systems and procedures to support SEC compliance, it must update its business continuity plans to ensure that these changes are addressed. Additionally, business continuity plans should be formally documented, reviewed and agreed upon by senior firm leadership, should include a process for periodic updates and should undergo routine testing.

A robust business continuity plan begins with the execution of a business impact analysis (BIA), updated periodically when changes to the business occur. The results of this BIA can be used to drive the development of the plan and to identify gaps in existing plans. IT can then work with the business to prioritize remediation efforts, assign ownership and track progress made toward closing the gaps.

General IT controls

IT should make certain that it has formal and evidenced control processes in place for change management, logical and physical security administration, job/process scheduling, operations management, backup and recovery. Working closely with members of the compliance team,

IT must also create mechanisms — such as internal audits or risk and control self-assessments — to periodically evaluate the design and operation of these controls in order to continually identify potential regulatory gaps and close them.

Oversight of third-party service providers
IT general controls, security, business continuity planning and records management assessments should, naturally, include an examination of those third-party service providers currently working with the company. Compliance officers and IT can approach this assessment by classifying and ranking by level of risk all outside services the firm utilizes. In conducting the IT controls assessment, the services provided by the vendor should dictate where you focus your evaluation efforts (e.g., governance, personnel controls, logical security, physical security, change management). After a thorough assessment of third-party service providers is completed, the results can be analyzed and integrated with the company's broader vendor-assessment effort. The frequency and depth of ongoing reviews of vendors can be determined using the factors noted above as well as considering the results from the first assessment.

Inclusion is the key

Four to six weeks is the expected timeline for baseline IT diagnostic completion — for companies who have included IT in compliance readiness discussions from the beginning. (This timing also, of course, depends on the availability of stakeholders to meet with IT and on the adequate allocation of resources to support the effort.) After completing these assessments, companies that have the basic IT structures in place needed to support Dodd-Frank compliance initiatives may be able to get by with relatively simple reconfigurations and adjustments. They can hold training and awareness sessions to introduce upgraded processes and address individual compliance issues as they arise.

However, companies that keep IT in the dark during the planning process face a more formidable set of challenges. Without adequate time to create baseline assessments of their systems capacities, IT will be forced to prioritize remediation efforts, leaving some components of a company's compliance plan incomplete, and possibly affecting key strategic projects. The sooner IT can identify the systems it will need to support compliance requirements, the better. A company that must develop or acquire new systems will need months or even a year to implement depending on the resources it can put behind the effort.

Finally, there are large companies with longstanding RIA credentials that may feel that Dodd-Frank's regulatory requirements apply only to companies that are currently unregistered. They may mistakenly feel that they already have their compliance house in order. They should remember that Congress is still writing some rules for major components of Dodd-Frank, and reporting requirements remain fluid. Even established RIAs should assess their compliance practices and perform thorough IT diagnostics.

It is time, right now, to become compliant and prepare for an SEC examination and expanded reporting. Companies new to RIA compliance and those getting a late start with the planning process can engage consultants with the knowledge to guide them. Ultimately, regulators want to see if RIAs possess the right governance model and the right practices to run the business and protect investors. RIAs should be able to demonstrate that they have plans to fix any processes and systems that are not compliant and be able to show their progress against their plans.

Baseline assessment questions your IT group should be asking

1. Are IT systems retaining the data required for proper regulatory reporting?
2. Are your books and records mapped to the production applications, network drives and other similar repositories (e.g., document management systems)? Is there a process to maintain this mapping?
3. How are you managing email and instant message communications?
4. An RIA has a fiduciary duty to protect its clients' interest, which includes protecting investor data. Do current IT systems adequately secure confidential data?
5. Does IT have effective and documented change management processes in place?
6. Is a documented and tested business recovery plan in place? Has it been reviewed and agreed upon by senior leadership?
7. Does IT have a formal program in place to periodically assess key vendors' IT controls and evidence results?
8. Is access to sensitive data limited to those who should be seeing and updating it?
9. Are any compliance-related systems redundant?

Cynthia Doe is a principal in the Financial Services Office of Ernst & Young LLP. Cynthia is based in New York City and can be reached at +1 212 773 1152 or cynthia.doe@ey.com.

Daniel New is an executive director in the Financial Services Office of Ernst & Young LLP. Daniel is based in Boston and can be reached at +1 617 585 0912 or daniel.new@ey.com.