

# *Integrating technology into your compliance program to improve effectiveness and efficiency*

2011



# Contents

- Why technology? ..... 1
- Five major areas where technology can help ..... 2
  - 1. Archival and surveillance of electronic communications ..... 2
  - 2. Firm trade surveillance..... 5
  - 3. Document management..... 7
  - 4. Code of ethics monitoring..... 8
  - 5. Compliance case management ..... 11
- Evaluating and selecting technology vendors..... 12
  - Key selection considerations ..... 14
  - Step 1: Requirements gathering ..... 14
  - Step 2: Vendor profile creation ..... 15
  - Step 3: RFI and vendor review process ..... 16
  - Step 4: Vendor selection and solution implementation..... 16
  - Implementation timeline.....17
- Today’s reality.....17
- How PwC can help.....17
- Additional information..... 18

As financial services firms prepare for increased regulation, scrutiny, and oversight, they are evaluating their compliance and control systems. With new regulatory requirements in the wake of the financial crisis and the Dodd-Frank Wall Street Reform and Consumer Protection Act, a fully functioning, comprehensive compliance program is more important than ever.

Although regulatory, investor, and management expectations of compliance programs have never been higher, resources to perform compliance functions have not increased commensurately. Compliance programs must meet demands — to perform better, dig deeper, provide broader coverage, faster — without significant additional resources. To do so, leading firms are embracing technology that can help them manage their day-to-day compliance functions and meet these new expectations.

### ***Why technology?***

New technological tools can make financial services' firms compliance programs both more effective and more efficient. Technology can help utilize existing resources and can extend the breadth and depth of coverage.

As chief compliance officers (CCOs) assess gaps in their compliance programs, plan improvements, and determine the associated costs, they quickly realize that technology is integral to the solution. The compliance department, like other firm functions, can leverage technology to automate manual processes and maintain audit trails while greatly improving efficiency, precision, and overall effectiveness.

More importantly, technology can play a key role in fulfilling requirements to test the adequacy of compliance policies and procedures. It allows compliance personnel to focus on analyzing results and identifying potential violations rather than performing labor-intensive, manual reviews.

Regulators and investors expect to see technology integrated into compliance programs, demonstrating a robust culture of compliance. As firms continue to adopt technology in their compliance programs, regulators' focus on whether and how firms are using technology will likely increase. And in the face of growing regulatory demands for information, technology can assist with timely production of key indicia of the operation of the compliance program.

In addition, senior managers, boards, and audit committees are demanding more assurance with respect to compliance as they are asked to certify, report on, or oversee the effectiveness of the compliance program. Technological tools can help provide a stronger foundation for these representations.

Unfortunately for many firms, they are not capitalizing on the robust compliance technology solutions available. Some firms maintain manual compliance processes, which are time consuming, costly, and prone to error. Others combine manual and automated processes, making it difficult to reconcile data and ensure accurate and

timely reporting. Many firms, including some that have grown rapidly, have done piecemeal compliance automation. This approach could lead to disparate, nonintegrated systems that are costly to maintain and do not provide a consolidated view of risks.

Organizations that do not leverage technology to modernize their compliance programs may find that they utilize valuable human resources on manual processes that could be directed to better use. They may put the firm and its employees at risk by not having as broad or as deep a focus on compliance risks as other firms and missing indications of noncompliance that would otherwise be revealed and addressed early. And, as the use of technology continues to grow, they will find that they are not meeting industry “best” practices or even industry “standard” practices.

### ***Top reasons to integrate technology into your compliance program***

- *Compliance officers can spend more time analyzing data rather than gathering information.*
- *Increased efficiency leads to cost reduction.*
- *It enables conflict management, a key area of any comprehensive compliance program.*
- *Data accuracy is enhanced, which reduces risks by limiting human error.*
- *It demonstrates a prudent, responsible compliance culture, providing confidence to regulators and investors.*
- *New infrastructure can scale quickly as the business grows, and it is resistant to staff turnover.*
- *It allows compliance staff to track issues uniformly, eliminating ad hoc records.*
- *It reduces the burden of inspections by automatically generating predesigned reports that can be downloaded at a regulator’s request.*

## ***Five major areas where technology can help***

Although technology solutions can be used in many areas of a firm’s compliance program, the five areas described as follows exemplify how technology can aid in compliance: archival and surveillance of electronic communications; firm trade surveillance; document management; code of ethics monitoring; and compliance case management. In each area, compliance technology vendors provide a multitude of capabilities to monitor, report, and manage and test.

### **1. Archival and surveillance of electronic communications**

Financial services firms are required to monitor, archive, and have the ability to search their electronic communications in accordance with federal regulations.<sup>1</sup> The records must be held for minimum time periods (e.g. three to six years, the first two of which in a readily accessible location). Further, surveillance of this electronic communication is critical, particularly in areas where employee communications are known to present risks (e.g. around information barriers, those firm employees with

<sup>1</sup> For example, investment companies and certain investment advisers are subject to Rule 31a-2 under the Investment Company Act. Investment advisers must also comply with Rule 204-2 under the Investment Advisers Act of 1940. Broker-dealers are subject to Rules 17a-3 and 17a-4 of the Securities Exchange Act as well as the following SRO rules: NASD 3110, NTM 98-11 (Amendments to Rules 3010 and 3110; FINRA Rule 2360 (b)(17)); and NYSE Rule 342.

confidential client information or intellectual property, those employees who communicate with clients and customers, and those who are “key” producers). Email surveillance and monitoring is now an expected aspect of a compliance program.

Regulators will become skeptical of the overall control environment if the firm is not able to demonstrate the archival and surveillance of email and other electronic communications, such as instant messaging and social media.

Email monitoring has been of interest to the SEC for many years, and now the SEC is expanding its purview to include social media usage. Regulators are performing examinations to discover how social media is being used by financial services firms and personnel for business purposes and how this use is being monitored.

As it stands, guidance by the Financial Industry Regulatory Authority (FINRA) (Notice 10-06) states that all postings made to a social media site or blog by the firm or its associated persons are subject to existing record retention and suitability rules. Firms are also reminded to “adopt policies and procedures reasonably designed to address communications that recommend specific investment products.”<sup>2</sup>

*So what does this all mean for a chief compliance officer?* Archiving and surveilling electronic communications are crucial parts of a healthy compliance program. The daily volume of communications continually increases as the methods expand beyond email to chat applications, blogs, and social networking sites such as Facebook, LinkedIn, and Twitter. Time spent by a CCO reviewing all communications has increased in recent years, and we expect the trend to continue.

In looking at the sheer volume of electronic communications transmitted by employees on a daily basis, a company using manual monitoring has to question whether its method to achieve effectiveness is impractical or even impossible. The review process is critical, so the cost of time spent to review communications must be considered in evaluating the role of technology as a strategic investment in a firm’s compliance infrastructure.

Some vendors allow CCOs to track all activity by individual employees, which can identify patterns among the various forms of communication and quickly identify any suspicious activity. Today’s solutions are much more sophisticated than the outdated, simplistic “keyword” searches that often produced a great number of false-positive search results.

Many technology vendors are working to stay ahead of the curve to provide email surveillance and archiving solutions to firms, reducing the burden of this task on CCOs. Most solutions offer the following benefits:

- ***Tracking and archiving of communications (e.g. corporate and external email, instant messaging, and social networks) by user or by device.*** Software tools’ core functionality is to integrate with your email and messaging services to preserve communication traffic. These tools should integrate with your corporate email, external email, mobile messaging, and Web-based mail and Web posting sites. Messages can be stored locally or offsite using a cloud-based model.

---

<sup>2</sup> FINRA Regulatory Notice 10-06: Social Media Web Sites — Guidance on Blogs and Social Networking Web Sites, January 2010.

- **Report generation.** The ease of use and flexibility of reporting vary by vendor. In case of an investigation, many providers will assist with data retrieval and provide a letter of attestation to confirm that no tampering with archived data has occurred.
- **Surveillance capabilities.** These software tools offer significant search and surveillance functionality. This functionality can be used to identify incoming or outgoing material nonpublic information (MNPI), customer data, proprietary intellectual property, and communications between employees and other parties that may present a potential conflict of interest, among other things. Specific surveillance functionality varies by vendor but should include the ability to search for keywords using wildcards and Boolean search parameters, search for files with specific “hash” values, and dynamically load and refresh search parameters.

#### ***Email management program leading practices***

- *Establish an enterprisewide protocol for retaining and retiring email. Adopt an enterprisewide policy reducing the retention of email backup tapes for only as long as is necessary for disaster recovery or system restore. Do not use backup tapes as an archive or preservation tool.*
- *Enable existing technology features (e.g. disable reply to all) to reduce email volume.*
- *Use clearly written, enforceable retention policies to meet technology solutions.*
- *Develop a coordinated governance structure for enterprise email management.*
- *Establish an effective date three to six months out when implementing new policies to provide business units with the time and support needed to become familiar with and adopt the necessary policies, processes, and supporting technologies to sustain compliance.*

When analyzing and comparing the tools’ features, you could ask questions about ease of use; monitoring capabilities of the technology; search capabilities; assistance with compliance with regulations set forth by the SEC, FINRA, etc.; and ongoing training and support.

You should also coordinate with your chief technology officer to address questions about data storage capacity, scalability, and the deployment model. Deployment may be with software as a service (SaaS), onsite hardware, or a hybrid model.

SaaS options typically cost less upfront and increase in cost based on the number of users. Most providers charge on a per-month basis for the life of the relationship. Many solutions are multitenant, which allows all users to receive upgrades simultaneously as they are rolled out by the vendor. This can be a benefit because there is no need to actively seek out upgrades, but it is important to understand the vendor’s future vision of the product and evaluate whether it is in line with your organization’s goals. Onsite hardware solutions cost more upfront and also may be more complicated to integrate, but the maintenance price tag will be lower.

While email monitoring and archiving technology costs vary, the overall cost of compliance technology pales in comparison with the damage of a publicly disclosed SEC investigation or the discovery of insider trading that might have otherwise been detected by an automated monitoring program. For example, most of the recent investigations of and charges against investment managers for trading on inside information have been proven using email evidence.

## 2. Firm trade surveillance

Monitoring and analyzing trading and investment activities are essential to detect possible violations and possible deviations from investment objectives, risk tolerances, or firm policies. Regulators, investors, senior managers, and others expect that firms will have an effective trade surveillance and monitoring program.

A robust trade surveillance and monitoring program will help provide confidence to senior managers, investors, boards, and regulators that the firm is operating with effective controls. In addition, a strong trade monitoring program will anticipate the types of regulatory requests most often made and will be able to generate reports showing compliance rates.

Firm trade surveillance software can provide a very effective and efficient solution to analyze firm activity for a wide range of regulatory and in-house requirements. This includes monitoring for:

- Insider trading — Does trading activity show a pattern surrounding important market events, announcements, or large moves in a security's price?
- Restricted list — Is there extensive activity just prior to a security being added to your restricted list?
- Investment guidelines — Is the trading activity within the investment guidelines for the portfolio?
- Window dressing — Is the portfolio's activity excessive and unusual just prior to the end of a statement period?
- Concentrations — Is the portfolio unusually or inappropriately concentrated in a specific region or sector?
- Market manipulation — Is a trader or asset manager intentionally trying to manipulate the price of a security?
- Allocations — Are trade allocations being done in accordance with policy guidelines? Is there any favoritism for certain clients or funds? Are certain portfolios getting an unusually large amount of profitable trades?
- Valuation alerts — Are your valuations accurate and in line with market activity? Is a trade price unusually different from your mark-to-market?
- Cross trades — Does activity represent cross trades, and are they being done pursuant to firm guidelines?
- Hot issues — Are your portfolio managers buying them, and is the activity within firm guidelines?
- Best execution — Have you analyzed your portfolio activity to test for price competitiveness and favoritism toward specific counterparties?

Firm trading surveillance can occur before or after a trade. Order management systems typically contain controls to enforce certain pre-trade compliance policies, such as restricted list, investment guidelines, credit limits, concentration, and allocations. These systems can be configured to stop trades that potentially violate a compliance policy or simply to alert the trader and/or compliance function of such activity. The system should have an alerting capability that includes email alerts and an intuitive work flow that allows for alerts to be quickly and effectively reviewed.

Although these pre-trade controls are important, it is equally important to consider post-trade surveillance, which serves to:

- Test the existing pre-trade controls — Post-trade surveillance can be used to identify trades that potentially violate trading guidelines in order to test the design or effectiveness of pre-trade controls.
- Address risks not being addressed by pre-trade controls — Certain trading guidelines and policies cannot be readily tested with pre-trade controls because necessary surveillance information is not available at the time of the trade. An example would be misuse of MNPI where a compliance officer may wish to examine trades where an unusually large risk was taken ahead of an earnings release. Also, pre-trade controls cannot test for price accuracy because third-party pricing may not be available on a real-time basis.
- Act as a preventative control — If portfolio managers and traders are aware of such monitoring, they may be less likely to attempt trades that violate guidelines.

Efficiently documenting, tracking, and escalating activity violations are also key benefits of any comprehensive trade surveillance technology. After being alerted to a violation, a user can efficiently document action taken or escalate via email. Records are archived, providing an audit trail that is easily retrievable.

The task of manually monitoring firm trading activity can be extremely complicated, require extensive human resources, and be prone to errors. Of equal importance is the potential failure to identify issues because of the lack of interconnectivity between different departments within a firm. A software solution takes raw trading activity and efficiently analyzes it, providing compliance officers, risk managers, and portfolio managers with an effective tool to monitor for violations and demonstrate to regulators that a robust monitoring process is in place.

A number of technology solutions can be applied to facilitate firm trade surveillance including:

- Order management systems — The major order management systems have pre-trade controls, which enforce certain trading compliance rules, and post-trade monitors. For multistrategy funds and multiproduct trading desks with multiple order management systems, trade surveillance performed by a single order management system may not be sufficient as it may not consider all products.
- Code of ethics monitoring system — Some code of ethics monitoring systems are offered with add-on capabilities that can be used to analyze firm trading activity in addition to personal trading. This may be a good option for a compliance officer who wants to consolidate compliance testing into a single package.
- Broker-dealer trade surveillance system — Several major trade surveillance platforms have been developed for and used by the broker-dealer community for years. These systems were originally developed to detect broker-dealer compliance risks such as front running. In recent years, the systems have evolved to address buy-side risks and may be a reasonable option for larger multistrategy funds as well.
- “Home-grown” system — Firms can also develop their own post-trade surveillance platforms using an SQL-based database management system. This option provides maximum flexibility but typically requires additional development time.
- Existing system — CCOs may be able to leverage tools currently used by the risk management function of their firm that have overlapping capabilities.

### 3. Document management

Financial services firms are required to maintain a tremendous volume of information relating to their business. This obligation is often one of the most difficult for a CCO to monitor because it requires the cooperation of all employees of the firm. Attempting to control the activities of all employees and ensure the maintenance of a large volume of required records without considering a technological solution or upgrade greatly increases the compliance burden over time and the likelihood of the destruction of required records — and noncompliance with applicable regulations.

#### ***Typical considerations for choosing a document management vendor***

*Answering these questions upfront can help you hone in on the right solution for your organization:*

- *Do you intend to use the solution as a platform to enable collaboration within your teams for creating new documents?*
- *How will existing physical documents be entered into this system?*
- *Will you be using the system to streamline business processes around document management and approval? If so, are your approval processes simple (few steps) or complex (multiple steps with branches and decision points)?*
- *Do you intend to enforce document retention policies through this system?*
- *Does your organization need to adhere to additional record retention standards beyond those of the Advisers Act and the Securities Exchange Act?*
- *Do you need a tight integration with other software?*
- *Will you be integrating this system with other document management systems or internal applications?*

Examples of the records that must be maintained include accounting records, operational records, legal contracts, trade information including original trade instructions, trade tickets and trade confirmations, communications with potential and current investors, and all documents necessary to demonstrate the controls in place across all lines of a firm's business. The full list of necessary documents will differ among firms based on their specific processes, but firms will have one thing in common: The documents will be onerous and burdensome to effectively capture.

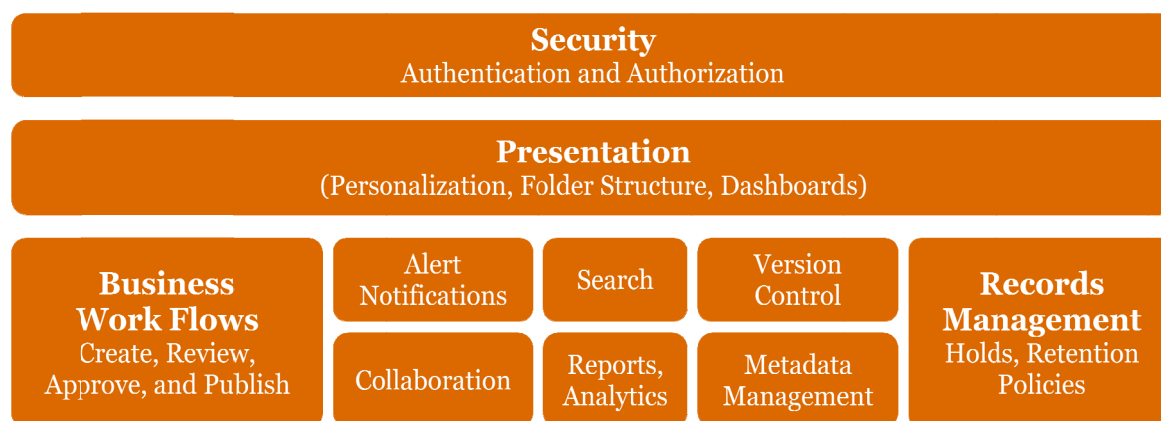
In addition to the requirement to initially capture and retain such records, firms also must subject such records to safeguards that have been reasonably designed to ensure the maintenance, version control, physical and electronic safety, backup, and destruction of all documents in definitive periods. A firm is expected to know the location, restriction of access, and proper safety around thousands of individual documents that span a time period, in some cases as long as the history of the firm. Failure to maintain proper records can result in regulatory and private legal actions, as well as a loss of investor confidence in a firm's ability to properly control its business.

Many of these records will be inherently captured and retained through various front-office systems, accounting systems, and email archiving systems. But a firm must be aware that there are countless other documents that aren't as conveniently captured through existing systems and therefore must be carefully mapped out and stored through manual processes. However, numerous enterprise content management (ECM) solutions are available to a financial services firm, and they are designed to ease the monitoring, storage, retrieval, and overall management of these documents.

An effective ECM solution can help a CCO ensure that documents and their corresponding versions or copies are stored in a centralized repository with appropriate access controls for employees. Additional compliance features of such a solution include audit of the activities performed on documents (tracking all editing, copying, or deleting of documents), a full-text search to help retrieve documents quickly, and facilitation of business work flows to pass documents across groups for approvals in a streamlined manner.

Utilizing the features of an ECM, a CCO can help ensure that the organization stores documents properly and uses appropriate safeguards, thereby promoting leading practices and compliance with legal and regulatory requirements.

The accompanying diagram represents the typical features of an ECM system.



Traditionally, enterprise content management involved large, cumbersome systems that were centrally installed and tightly controlled. Such huge systems can be difficult to maintain and tough to adapt as the industry's needs change. Over the last decade, significant improvements have been made in the ECM industry. Current ECM systems are more user friendly and agile and come in various sizes and prices, so an organization can choose the technology that fits technically as well as culturally.

However, the wide range of ECM systems also makes it harder for the buyer to select the right solution. Even though most solutions have the common set of features, each also tends to vary in specific features to differentiate itself from competitors. As a result, the buyer should first identify the most important objectives to accomplish with an ECM solution, and then weigh the vendors against these objectives to obtain the right fit.

#### 4. Code of ethics monitoring

Pre-trade approval of personal trades and a firm's code of ethics include provisions that require the reporting and monitoring of employee personal securities transactions and employee acknowledgement of the code.

Firms are required to adopt and implement written policies and procedures designed to prevent violations and must review the adequacy and effectiveness of these established policies and procedures at least annually.

### **Key code of ethics technology capabilities**

- *Feeds from any source, including brokers, trading systems, portfolio systems, watch lists, human resources systems, or custom feeds.*
- *Can translate code of ethics and trading policies into discrete rules that can be monitored and managed.*
- *Option to show specific policy statement or reason for denial or approval of a trade.*
- *Built-in reminder checklist.*
- *Work flow, such as trade approval notification emails, certifications, reminder notifications, and tracking of alert disposition.*
- *Document management capabilities.*

A byproduct of the rules is that they create the need for CCOs to maintain a paper trail evidencing the ongoing employee reporting of transactions and certifications, the ongoing compliance reviews performed, the issues identified, the resolution of these issues, and testing.

A well-organized employee reporting and compliance testing procedure that is supported with a transparent, documented trail of evidence will send a favorable message to a regulator and emphasize a culture of compliance. For this reason, CCOs need to consider a technology solution that addresses general compliance work stream responsibilities using case management or document management capabilities.

Such a program will allow CCOs to remain well-organized as they focus on identifying the most important issues, rather than overseeing mundane manual tasks or documenting issues already identified. Most code of ethics compliance monitoring software programs can automate several important but otherwise time-consuming areas of a compliance program including personal trading, affirmations and annual disclosures, gifts and entertainment reporting, and political contribution reporting.

**Personal trading** — Personal trading by employees is a major concern for regulators. Regulations provide specific requirements for firms to collect quarterly and annual reports from employees regarding their personal securities transactions and to review such employee personal security trading activity. The SEC staff has strongly recommended that the review of employee trading “incorporate automated or computerized analyses of trading patterns.”<sup>3</sup>

In light of the increasing complexity of trading systems, financial products, and trader sophistication, a technological solution is necessary if the CCO wants to capture and analyze the full range of employee trading activity. Software solutions available in the marketplace are able to monitor, to varying degrees, employee trading by automating the pre-clearance of trading, subjecting each requested trade to the set of rule parameters mandated by firm policy including looking at holding periods, restricted lists, and blackout windows; checking pre-cleared trades against an employee’s brokerage account; and conducting post-trade surveillance to screen for potential misuse of MNPI as well as front running.

<sup>3</sup> Thomas Lemke and Gerald Lins, “Regulation of Investment Advisers 2010 Edition,” Thompson Reuters 2010, 305 (citing Lori Richards, “Remarks at Investment Counsel Association/IA Week Investment Adviser Compliance Summit,” April 28, 2003).

*Pre-clearance of trades* — The pre-clearance of employee trade activity is a staple of compliance programs and can now be automated through compliance software. Available software provides a portal where an employee logs into the system, then enters the security's ticker symbol or CUSIP number, the number of shares or notes to be transacted, and the type of transaction. Most software products have connectivity to a wide range of global security directories and a feature that allows ticker symbol searches.

The system automatically screens the request against the firm's restricted list, trading activity, and any other specific rules, including holding periods and blackout windows, that may affect an employee's ability to trade. Depending on the software product and the configuration, the system generates an automated response to the request; otherwise, a compliance officer may have to do a manual review. The software provides a central repository for all reported trading activity of a company's employees that can be easily searched and sorted.

*Electronic brokerage feeds* — Most compliance software vendors have established protocols with a wide range of brokers to obtain electronic feeds of brokerage activity. In some cases, this data is provided through a third party that obtains feeds from multiple brokers. Written consent from the employee is required in either case. Some also have systems for scanning or entering trades from paper statements. The electronic reception and aggregation of employee trade data serve as a powerful deterrent for employees because they know the firm is monitoring their trading regularly.

*Restricted trading list* — An automated list of restricted securities provides employees with a real-time ability to seek clearance to effect personal securities transactions. The software can be tailored to allow the compliance officer or any other authorized individual to add a security to the restricted list as soon as it is determined that the firm may be in possession of MNPI, a confidentiality agreement is executed, or any other criteria that the firm predetermines is met. An automated restricted list creates an electronic record of restricted securities and denotes when they were placed on the restricted list and for what reason.

When employees use the software to obtain trade pre-clearance, any request to trade in securities on the restricted list will automatically be denied.

**Affirmations and annual disclosures** — Many financial services firms are required to, or undertake to, provide employees with their firm's code of ethics and to obtain an acknowledgement from each employee in writing that the employee has received and reviewed it.<sup>4</sup> Firms undertake an annual exercise to accumulate from all employees (or a category of employees) a certification stating that they have read, understood, and complied with the elements of the code of ethics. In addition to this simple certification, annual certifications typically include specifics around employee personal trading activity, personal and outside business relationships and affiliations, other policy acknowledgements, and legal and other disciplinary disclosures.

---

<sup>4</sup> Rule 204A-1(a) of the Advisers Act requires advisers to "maintain and enforce a written code of ethics that, at a minimum, includes ... provisions requiring you to provide each of your supervised persons with a copy of your code of ethics and any amendments, and requiring your supervised persons to provide you with a written acknowledgment of their receipt of the code and any amendments."

The process of distributing and receiving completed certifications without an automated solution can be an unnecessarily burdensome administrative task. Automated solutions also can offer standardized templates that will break certifications down into easy-to-follow tabular formats that can be tailored quickly and routed to other employees. Once received via email, these certifications can be completed and routed back to the compliance officer with a few simple keystrokes. The software will automatically log and store responses and produce reports to monitor for missing responses. The compliance officer has the option to manually follow up with delinquent employees and access persons or to simply send an automatic reminder out to all delinquent respondents.

**Gifts and entertainment reporting/political contribution reporting** — Most financial services firms have a gift and entertainment policy. Policies vary from requiring the reporting of any gift and entertainment given or received to requiring only the reporting of items over a threshold amount. Political contribution disclosure requirements also vary from firm to firm. From a technology perspective, software provides functionality for employees to enter and request approval for expenses with an automated and/or work flow-oriented approval process.

A key feature of technology used to address this risk area is an easy-to-access, easy-to-use interface for reporting such activity. This is especially important for gift and entertainment and political contribution disclosures because they rely on self-reporting by employees. Automated solutions in this area afford employees with easy-to-navigate reporting interfaces. The reported information is then viewable by designated supervisors.

Automated solutions have powerful reports that can assist the CCO in reviewing gift and entertainment activity by employee, vendor, or counterparty or on a firmwide basis. Additionally, political contribution monitoring reports are available that can easily monitor for pay-to-play and Foreign Corrupt Practices Act issues. This type of analysis cannot be performed nearly as effectively without an automated solution.

## 5. Compliance case management

To satisfy the requirement to review the adequacy and effectiveness of their policies and procedures, firms need to perform ongoing monitoring of their compliance program. But it is not enough just to perform the monitoring and testing procedures. Firms must be able to demonstrate the procedures performed and the results obtained. For this reason, maintaining logs of tests and documenting potential issues identified are essential parts of a compliance program.

Using compliance technology, a compliance officer can document activities and issues within standardized templates that will be logged and maintained as a book and record. These standardized templates can be further routed through email to designated supervisors for formal review and sign-off, evidence of which will be captured as part of a documented case.

Cases can also be created for future events and viewed, along with outstanding sign-offs required, as well as ongoing cases within a calendar format. When used properly, this type of compliance calendar will allow a CCO to see a snapshot of all activity that requires attention in a given day, week, or month. Among the numerous reasons to create a case is that through such an automated solution, each case can be routed, tracked, and monitored in an organized manner.

Only through automated solutions can CCOs effectively focus on the high-risk issues while meeting their regulatory requirements, staying organized, and not allowing the documentation requirements of a compliance program to get in the way.

## ***Evaluating and selecting technology vendors***

Effective compliance programs reach beyond the compliance department into the entire organization. Technology can help embed a compliance culture into the daily routine and mind-set of every employee. Technology solutions should be evaluated with your entire firm in mind, not just the needs of a single department.

Although firms recognize the need for a technology-enabled compliance infrastructure, many find that they do not have the internal resources to provide guidance about the myriad laws, rules, and regulations applicable to them, the reasons these requirements apply, and the particular business controls needed to make compliance an operational reality. Furthermore, financial services firms may not have insight into the types of technology providers in the market today and the capabilities and relative effectiveness of their software solutions.

In some cases, a single provider can offer most or all of the capabilities a firm needs, although customization is usually required. More often, the best solution is a combination of software packages from multiple vendors. In such cases, a third party with knowledge of the vendors involved can help with a successful customization and integration across platforms.

PwC has developed a methodology for helping our clients evaluate compliance technology providers and implement customized solutions based on our experience in assisting investment management clients, broker-dealers, and other financial services organizations. Our approach has proven effective for organizations that are transitioning from manual to automated compliance systems, as well as those that need to upgrade or enhance their technology.

Our methodology consists of four steps, shown in the accompanying chart and described as follows:

- Requirements gathering.
- Vendor profile creation.
- Request for information (RFI) and vendor review process.
- Vendor selection and solution implementation.

|                             | <b>Step 1</b>  | <b>Step 2</b>  | <b>Step 3</b>   | <b>Step 4</b>   |
|-----------------------------|--|--|---|---|
|                             | <b>Requirements gathering</b>  | <b>Vendor profile creation</b>   | <b>RFI and vendor review process</b>  | <b>Vendor selection and solution implementation</b>   |
| <b>Activities performed</b> | <p>Interview a cross-section of groups/stakeholders to gather business and technical requirements.</p> <p>Incorporate specific requirements into a scoring matrix.</p> <p>Assign a weighting to each requirement, based on need.</p> | <p>Create vendor profiles using data gathered through interviews, market research, vendor websites, and (if applicable) firsthand knowledge.</p>         | <p>Develop a request for information for vendors, using requirements gathered during the discovery phase.</p> <p>Issue RFI to vendors, and obtain and score responses using the scoring matrix.</p> <p>Interview three reference companies in your industry that currently use the top-scoring solutions.</p> | <p>Facilitate vendor selection and develop implementation plan using information gathered from the organization's groups, external interviews, vendor profiles, and RFI analysis.</p> <p>Convert data and systems, and perform systems integration and testing.</p> <p>Train employees.</p> <p>Develop user guides and system technical documentation and security plans.</p> |
| <b>Milestones achieved</b>  | <p>Explain project to all affected groups, and conduct preliminary interviews with the business units that are in scope.</p>   | <p>Vendor profiles are developed from data gathered from market research, subject matter professionals, interviews with users, and company websites.</p> | <p>RFI is issued to all vendors.</p> <p>Responses are obtained from vendors.</p> <p>Vendor responses are qualitatively and quantitatively analyzed and scored against one another.</p> <p>Based on references provided by each vendor, feedback from users is gathered through phone interviews.</p>          | <p>Recommendations and plan/strategy are defined.</p> <p>User acceptance, system acceptance, and integration/interface testing are completed.</p> <p>Initial employee training is completed.</p> <p>User and technical documentation is developed.</p>  |

## Key selection considerations

- Beware of vendors that say they are “adaptable” to the client’s critical requirements. Many times, this equates with customizations of existing tools or custom-built applications that can significantly increase the solution’s cost.
- Vendors will often show the strengths of their product, not necessarily how the package fits with your business requirements and data environment. Individual user evaluation criteria and test plans should be developed to challenge the vendors to show the specific impact of their software solution.
- During the step of vendor tool procurement, consider interacting with at least two vendors. The purpose is to provide competition for price, service, and timeliness. Also, it provides a backup in case negotiations with the top choice fall through.

## Step 1: Requirements gathering

Before considering specific vendors, your firm must gain a thorough understanding of its business and technical requirements for a compliance technology solution. The organization’s existing systems and tools should be analyzed to understand if they might be leveraged to produce a more cost-effective solution. Without a clear understanding of its requirements, the organization might procure an inappropriate or inadequate vendor solution, overspend, and increase compliance and business risks.

In many cases, a single department (either IT or compliance) drives initiatives to procure compliance software. In the process, business or technology requirements may be overlooked or minimized; this can lead to ineffective solutions that require costly revisions down the line or do not integrate with the existing technology. It is important to address the requirements of the business and IT so that the eventual solution meets the needs of both groups.

In our experience, requirements gathering is best conducted through interviews with a cross-section of employee stakeholders, including key business managers and representatives of the IT department. The goal is to identify the business needs that compliance technology must meet, as well as the technical requirements for a successful implementation, and to reconcile any identified differences. The interviews should focus on current and projected future requirements to help ensure a long-term, sustainable solution. At a minimum, the following employee groups should participate in the interviews: compliance personnel, operations managers, traders, portfolio managers, risk managers, and any other employees involved in the trading cycle, including accounting personnel.

Technology needs vary depending on the size of your firm, your existing systems, the complexity of your firm’s trades, and your budget and staffing. Whether you build it yourself or buy it from an outside vendor, several considerations help you make up your wish list.

### **Additional vendor selection considerations**

- *Do you have the expertise to manage the selection and integration process yourself? How much time and attention will it require? Should you bring in an outside consultant to manage the project?*
- *Make sure your outsourced technology does what you want it to do out of the box without you having to write a lot of customized rules.*
- *Regarding flexibility, how easy is it to modify rules or create new ones?*
- *Can it accommodate any international compliance issues?*
- *How does the vendor plan to adapt its technology to the changing regulatory environment?*
- *Does the software automate and centralize your routine compliance functions?*
- *Is the vendor sustainable as a going concern? Review the most recent audited financial statements, most recent credit rating received (if applicable), and sales and net income for the past five years.*
- *Where will the technology be deployed, onsite or hosted?*
- *Is it compatible with your existing systems?*
- *Can your IT people support it?*
- *Is the system scalable? What happens if your firm grows?*
- *How do you take an existing policy and convert it to specific rules that a computer will test for?*
- *How much will it cost? Does the vendor charge by user, assets under management, or enterprise?*

As business and IT requirements are gathered, they are incorporated into a scoring matrix you can use to rate vendors on factors critical to your sound selection decision. The factors can range from cost and quality to product support, how long the company has been in business, how widely the software is used in the industry, and the level of customer satisfaction.

You may assign more weight to certain attributes. For instance, when we conduct vendor evaluations, we may suggest assigning greater weight to a vendor that has high customer satisfaction scores and whose solution has been widely adopted in the marketplace than to a new market entrant.

Although cost typically is a major factor in selecting compliance technology solutions, it should not be the overarching consideration. A low-cost option that does not satisfy an organization's business and IT requirements could result in even greater expense over the long term, in the form of performance problems and/or compliance violations that could increase risks to the business.

A third party with detailed knowledge of vendors and the technology they provide can help identify the solution that best balances cost with the needs of your firm.

## **Step 2: Vendor profile creation**

After gathering business and IT requirements, the next step is to create profiles of potential vendors and their compliance software offerings so the requirements can be mapped against the offerings. This process allows you to determine which vendors will be sent a request for information (RFI). Profiles can be created using information gathered through interviews, market research, vendor websites, and firsthand knowledge of the experience of customers that are using various vendors' products.

The following questions should be posed to targeted vendors of compliance technology to ensure they can meet your business and IT requirements:

- Does the vendor have the ability to translate business requirements (such as policies, procedures, and testing driven by regulatory requirements) into technical capabilities?
- Does the product meet critical technical requirements (for example, database and operating system requirements and end-to-end transaction monitoring)?
- Can the vendor meet the scheduled expectations of business managers and the IT department?
- Does the vendor have internal development and configuration standards that it enforces on projects? If so, do these standards meet the expectations of IT?
- What are the challenges of prioritizing multiple demands from the business and IT? In PwC's experience, firms generally have limited IT resources and a large pipeline of requests to satisfy.

### **Step 3: RFI and vendor review process**

After the vendor profiles have been created, RFIs are issued to selected vendors, with a clear deadline for receiving responses. Once vendor responses are received, they are scored using the scoring matrix. In reviewing RFI responses, it is important to focus on quality rather than quantity. After vendors have been ranked using the scoring matrix, interviews should be conducted with various reference firms that currently use the top-ranked identified vendors.

Such interviews can be a valuable step in the process of selecting the right vendor. Sometimes an interview makes it clear that there is a gap between vendor claims and customers' perceptions and experience. For instance, the vendor might exaggerate the resources it devotes to staffing an implementation project, or it might paint an overly optimistic picture of implementation challenges and time frames.

### **Step 4: Vendor selection and solution implementation**

With RFI responses analyzed and reference interviews completed, the final step is to select a vendor or vendors and develop and execute an implementation plan. Implementation often involves the following steps:

- Customization.
- Data and system conversion.
- Training.
- Conversion of user policies into specific rules.
- Development of user guides and system technical documentation.
- System security planning.

A key challenge in the implementation phase is coordinating and integrating with the firm's existing systems and tools. The integration process can require significant time and effort to complete.

Testing the solution for accuracy and performance is another critical element of implementation. Generally, this step includes user acceptance testing (UAT), system

acceptance testing (SAT), and integration/interface testing. It may be helpful to continue to run current processes in parallel with the compliance technology solution after implementation for a period. Results can then be compared to ensure the accuracy of data and reports generated by the new system.

## **Implementation timeline**

The length of the implementation process depends on a number of factors, such as the size, needs, and complexity of the firm; the budget for the initiative; the time sensitivity of implementation; and the human resources committed to the project (e.g. support of senior management, from the CEO to compliance, business, and IT staff).

## ***Today's reality***

With technology a staple in any business, regulators expect firms to leverage it to ensure effective, accurate, and documented compliance processes. Financial services firms that do not use technology to manage and control risks run the risk of falling behind their peers in sophistication and ability to meet regulator and investor expectations for a robust, dynamic compliance program.

PwC routinely advises clients on these compliance issues. We are familiar with the technology solutions in the marketplace and the unique compliance challenges that financial services firms face. You may be dealing with similar compliance program issues, and our experience gives us an informed, grounded perspective on how to incorporate technology as you solve ongoing problems.

## ***How PwC can help***

Clients can receive tailored services from PwC including the following:

- Benchmarking assessment of use of compliance technology, including regarding the pre-clearance of trades, surveillance and monitoring of portfolio trading, personal trading, and electronic communications surveillance
- Assessment of technology controls related to information barriers and data security
- Development of requirements and matching of company risks with the rules for surveillance/monitoring that software packages use
- Advice on the selection and implementation of software solutions
- Requirements gathering and analysis
- Assistance with vendor selection
- Implementation facilitation
- Data and system integration
- System testing and tuning for efficiency and effectiveness
- Development of policies and procedures

## ***Additional information***

### ***PwC's Financial Services Regulatory Practice Leaders***

**Dan Ryan**

FS Regulatory Practice  
Chairman  
646 471 8488  
daniel.ryan@us.pwc.com

**Gary Meltzer**

FS Regulatory Practice  
Managing Partner  
646 471 8763  
gary.c.meltzer@us.pwc.com

**John Garvey**

FS Advisory Practice  
Leader  
646 471 2422  
john.garvey@us.pwc.com

### ***For more information, please contact:***

**Thomas Biolsi**

646 471 2056  
thomas.biolsi@us.pwc.com

**Emanuel Bulone**

646 471 5131  
emanuel.bulone@us.pwc.com

**Peter Horowitz**

201 463 1030  
peter.a.horowitz@us.pwc.com

**Timothy Mueller**

646 471 5516  
timothy.mueller@us.pwc.com

**Lori Richards**

703 610 7513  
lori.richards@us.pwc.com

**David Sapin**

646 471 8481  
david.sapin@us.pwc.com

**Anthony Conte**

646 471 2898  
anthony.conte@us.pwc.com

**Robert Nisi**

415 498 7169  
robert.nisi@us.pwc.com

**Tom Anguilla**

646 471 7767  
thomas.anguilla@us.pwc.com

**Brian Castelli**

646 471 2563  
brian.castelli@us.pwc.com

**Rosalind Conway**

551 482 2830  
rosalind.d.conway@us.pwc.com

**Duer Meehan**

703 918 6191  
a.duer.meehan@us.pwc.com

**Matthew Nullet**

617 530 7057  
matthew.nullet@us.pwc.com

**Nathan Chao**

646 471 4905  
nathan.l.chao@us.pwc.com

### ***Acknowledgements***

The following people  
contributed to this  
article:

Lori Richards

Tom Anguilla

Brian Castelli

Rosalind Conway

Aarthi Artham

Nathan Chao

Jason Golieb

David Harpest

Matthew Nullet

Nick Shah

Sathyanarayanan  
Srinivasan

## ***www.pwcregulatory.com***

© 2011 PwC. All rights reserved. "PwC" and "PwC US" refers to PricewaterhouseCoopers LLP, a Delaware limited liability partnership, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity. This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

PricewaterhouseCoopers has taken all reasonable steps to ensure that information contained herein has been obtained from reliable sources and that this publication is accurate and authoritative in all respects. However, it is not intended to give legal, tax, accounting or other professional advice. If such advice or other expert assistance is required, the services of a competent professional should be sought.