

Strengthening internal control through forensic testing*

July 2007

Dear Clients and Friends,

Forensic testing is a topic of growing interest—and not just to those who enjoy watching investigative tales unfold on “CSI.” Increasingly, the U.S. investment management industry is embracing the subject, in response to compliance program rules adopted by the U.S. Securities and Exchange Commission (SEC) in 2003. As a result of these rules, registered investment companies and investment advisers can expect the SEC, during its inspections and examinations, to inquire about whether they have incorporated forensic testing into their annual compliance review processes.

How did this focus on forensic testing emerge? What are the SEC’s expectations of registered investment companies and investment advisers in this regard? And how can these firms and their service providers strengthen their internal control by incorporating forensic testing in their compliance programs?

This document addresses these questions and related matters in the hope that readers will benefit from the concepts and other information presented. The document is intended primarily for use by chief compliance officers of registered investment companies and investment advisers as well as other compliance professionals, risk managers, internal auditors, and supervisors of these personnel. While the SEC rules are applicable only to compliance programs of registered investment companies and investment advisers, the information in this publication also should be useful to compliance professionals of unregistered funds and advisers.

I hope you find the accompanying information helpful as you work continuously to strengthen the internal control of your fund’s or adviser’s operations. If you have any questions about the material covered in this publication, please contact me, or your local PricewaterhouseCoopers partner.



Barry P. Benjamin
Leader, U.S. Investment Management Practice
PricewaterhouseCoopers LLP
phone: 410-783-7623
email: barry.p.benjamin@us.pwc.com

Table of contents

1. Foreword	5
2. Setting the context for forensic testing	7
3. Focusing on the future	10
4. Incorporating forensic tests in compliance programs –ten considerations	16
Appendix: Illustrative forensic tests	24
Endnotes	34

1. Foreword

In December 2003, the SEC adopted new rules under the Investment Company Act of 1940 and the Investment Advisers Act of 1940. Among other provisions, these rules require each investment company and investment adviser registered with the SEC (fund and adviser, respectively) to do the following:

- adopt and implement written policies and procedures that are reasonably designed to prevent violation of federal securities laws specified in the rules applicable to them (including policies and procedures that provide for the oversight of compliance by specified fund service providers);
- review those policies and procedures at least annually for their accuracy and the effectiveness of their implementation; and
- designate a chief compliance officer (CCO) to be responsible for administering the policies and procedures.

These SEC rules are designed to protect investors by ensuring that funds and advisers have internal programs to enhance compliance with federal securities laws and regulations. The rules are commonly referred to as “38a-1” for funds and “206(4)-7” for advisers.

In recognition of the significant differences among funds and advisers in the U.S. investment management industry (in terms of size, business models, operational structures, investment products, investor profiles, systems, and risks), the SEC did not impose a single standard or framework for conducting annual reviews of compliance programs. And indeed, funds and advisers have developed customized policies, procedures, and approaches to annual compliance reviews that are suited to their particular circumstances. However, one common response to the new rules has been the significant resources devoted by many funds and advisers to the design, development and implementation of compliance testing programs used in conducting such annual reviews.

“...We have also given as much attention to forensic testing in [our] examination program, as we have urged upon you. It has seemed clear to me that we can’t ever be certain that we are effective in our work unless it is somehow tested. So, as we have been talking to you about testing your compliance programs by using forensic tests, we have also been doing the same thing in our program. For your programs and ours, the rationale is the same—to be good, to stay good, you must always strive to be better...”

*Lori Richards,
Director, SEC Office of
Compliance Inspections
and Examinations,
Remarks before the
National Society of
Compliance Professionals
National Membership
Meeting, Washington, DC,
October 25, 2005*

The term “forensic testing,” while not incorporated explicitly in the rules’ language, has its roots in the rules and in related SEC staff guidance. For instance, a footnote in the SEC Adopting Release to the rules is commonly viewed as referring to forensic testing. The footnote states:

“Where appropriate, advisers’ policies and procedures should employ, among other methods of detection, compliance tests that analyze information over time in order to identify unusual patterns, including, for example, an analysis of the quality of brokerage executions (for the purpose of evaluating the adviser’s fulfillment of its duty of best execution), or an analysis of the portfolio turnover rate (to determine whether portfolio managers are overtrading securities), or an analysis of the comparative performance of similarly managed accounts (to detect favoritism, misallocation of investment opportunities, or other breaches of fiduciary responsibilities).”¹

Equally important, since the adoption of the new rules, SEC staff have sent clear signals that they are taking the issue of forensic testing seriously. In that regard, in a keynote speech at an industry conference, Andrew Donahue, Director of the SEC Division of Investment Management, encouraged the implementation of forensic testing and referred to it as “another important tool” which “can enable CCOs to identify patterns or problems that spot-checking may not find.”²

Given this focus on forensic testing, funds and advisers can expect that SEC examiners will ask whether their compliance testing undertaken in connection with their annual compliance reviews includes the use of such tests. They can also expect the SEC to apply forensic tests as part of its inspections and examinations of fund and adviser activities.

It’s likely that a number of CCOs were using forensic tests to some degree well before the adoption of the new SEC rules, albeit under a different label. And since 2003, many others have begun to incorporate forensic tests in their compliance testing programs. Yet there remain core questions about forensic tests, among them: What do forensic tests intend to achieve? How does one best go about developing and implementing them? And, what are some types of forensic tests?

The remaining sections of this publication address these questions.

2. Setting the context for forensic testing

Several contextual points about forensic tests can be helpful to keep in mind when designing and implementing them.

Look beyond the conventional use of forensic tests

Initially, people often associate forensic tests with forensic accounting investigations. Such investigations usually are undertaken following an incidence of fraud or upon suspicion of fraud. Forensic accounting investigations may also be undertaken in connection with litigation—for instance, to establish or confirm damage amounts in claim proceedings.

This investigatory slant, however, is not the main lens through which funds and advisers should customarily view forensic tests. While forensic tests could produce information which ultimately leads to or compels a forensic investigation, their use should be to help management of funds and advisers maintain effective compliance programs and, more broadly, the funds' and advisers' internal control over compliance with federal securities laws and regulations.

Inquisitiveness matters more than testing particulars

The guidance provided so far by SEC staff and other industry participants related to forensic testing is useful. It paints a general picture that forensic tests often examine existing data in new ways and over longer periods of time. It suggests that the tests are inherently detective in nature—designed to spot unusual, unexpected, or potentially problematic patterns or trends in transactions processed or other information produced; unintentional errors or violations; exceptions indicative of internal control deficiencies; and intentionally hidden schemes or arrangements, including those involving fraud.

Yet, despite such guidance, there remains uncertainty and, at times, even a quiet angst within the investment management industry about whether a particular testing activity “qualifies” as a forensic test. Much of this concern seems unnecessary. Those responsible for designing and implementing forensic tests need not adopt the view that every test must incorporate the same objectives or analyze information or data in a similar manner over a similar period. In the end, forensic tests are less about definitions and

“A good forensic test has three characteristics. First, it provides a real test. In other words, it does more than simply repeat things you already do. Second, it helps you answer the question: what am I missing? In other words, it covers new material to test and validate the material you usually work with. Third, it adds current value. You can use it in your everyday program.”

*Lori Richards,
Director, SEC Office of
Compliance Inspections
and Examinations,
Remarks before the
National Society of
Compliance Professionals
National Membership
Meeting, Washington, DC,
October 25, 2005*

rigid characteristics and more a means to challenge the ‘status quo’—i.e., information about the state of compliance produced by a fund or adviser *without performing forensic tests*. In a sense, it’s about trying to disprove “the positive” or “current assessment” by:

- gaining additional insight from data or other information or evidence evaluated in new ways from current information sources, and in additional ways from new information sources;
- determining whether currently undiscovered circumstances are, in fact, present;
- exploring uncertainties; and
- acting on one’s instincts and with skepticism, as in asking questions of “what if,” “what about,” or “how do we know.”

Many of these underlying characteristics or attributes of forensic tests are incorporated in the illustrative forensic tests presented in the Appendix.

Forensic testing is part of internal control

When speaking about controls, many people focus on transaction-level processing controls. In the context of compliance, such controls generally aim to ensure that transactions are authorized, processed accurately and completely, and that their nature is consistent with applicable laws and regulations, corresponding compliance policies, as well as any relevant contractual terms or provisions of other agreements. These manual or computer-based controls can be either preventive (designed to prevent processing of an unauthorized, inaccurate, incomplete, or noncompliant transaction) or detective (designed to identify such transactions on a timely basis after they’ve been processed).

Internal control, however, is a broader concept. One commonly accepted internal control framework, COSO,³ includes five components:

- control environment
- risk assessment
- control activities
- monitoring
- information/communication

Forensic testing is not a new appendage to this framework, nor does it broaden COSO's boundaries. Rather, when used, forensic testing fits within it—most commonly as part of the monitoring component. Further, its particular classification within one or more components of internal control is not as important as how it often enhances an entity's internal control, such as strengthening a fund's or adviser's compliance program and, more broadly, the fund's or adviser's internal control over compliance with federal securities laws and regulations.

When used as a monitoring activity, forensic testing constitutes a part of the assessment of a fund's or adviser's design and operation of controls directed at compliance with federal securities laws and regulations. Forensic testing can provide information about current compliance policies and procedures and identify real or potential compliance issues that were not discovered through performing day-to-day transaction-level processing and other controls.

3. Focusing on the future

The roots of today's forensic tests often are found in the risk assessment phase of compliance programs. Risk assessments typically focus on identifying the higher compliance risks of the fund or adviser, after taking into account factors such as the following:

- the inherent risks of the investment management industry;
- the nature of the fund's or adviser's business activities and potential conflicts of interest present;
- the types of operations and systems that comprise the fund's or adviser's business processes;
- fraud risk conditions present; and
- the relative effectiveness of the fund's or adviser's controls in managing compliance risks.

The higher compliance risks identified through the risk assessment process typically are the main focus of the annual compliance review. These risks should similarly be the focus of forensic tests.

Consider trends reshaping the industry

When designing forensic tests, funds and advisors should consider not only current compliance risks but the forces that are likely to reshape the investment management industry over the next 3-5 years, and the new and/or greater risks some will present. Four of these forces, and the relevancy of forensic testing to these forces, are discussed below.

Increasing convergence

Signs of convergence within the U.S. investment management industry are already well in view. Increasingly, single strategy advisers are adopting additional strategies to remain competitive. Sponsors of mutual funds are adopting hedge fund-like strategies. More than a few hedge funds have moved toward multistrategy investment products, including private investments, commodities, and real estate. In turn, in the private investment arena, historical lines are converging and blurring. Structured products are being used both for funds' investment and financing purposes. On Wall Street,

it's hard not to notice the expanding labyrinth of business roles, beyond investment adviser, in which many financial firms serve their clients. And, of course, there's the growth of proprietary trading as firms who manage funds on behalf of third-party investors seek also to boost their own earnings.

These forces of convergence rightly put the spotlight on protection of confidential information as well as fiduciary duties owed each client, trade fairness among client and proprietary accounts, and management of risks arising from uneven incentives embedded in these account relationships. And while the investment management industry has measures in place designed to manage them, the increasing regulatory and other liability risks arising from unmanaged potential conflicts of interest may call for more oversight, applied through a different lens.

Forensic tests may well help in addressing such conflicts. For example, as regulatory bodies have done, advisers might develop forensic tests aimed at assessing the nature and extent of their trading in securities immediately preceding significant investment-related announcements, such as earnings releases, a merger or acquisition, a company's recapitalization, or a new securities issuance. Using forensic tests, unexpected or suspicious trading patterns around the time of the event's announcement potentially could be more easily identifiable. This retrospective, event-focused technique might be informative to advisers as they seek to ensure equitable trading across applicable accounts using only public or broadly available market information. In addition, thanks to newer technologies, forensic testing might be capable of uncovering unexpected or troubling patterns of electronic communications among investment professionals, by identifying anomalous patterns in customary communications, new parties to customary communication chains, or unusual subjects of communications, given the roles and responsibilities of the parties sharing such communications.

Rise in outsourcing

The investment management industry has long applied the outsourcing business model, through its use of third-party service providers such as subadvisers, distributors, prime brokers, administrators, custodians, and shareholder service agents. Looking ahead, use of third-party service arrangements can be expected to increase. In a spring 2007

PricewaterhouseCoopers survey of more than 150 finance executives from sponsors of U.S. mutual funds and hedge funds and other asset-management firms, approximately 31% reported plans to increase their outsourcing arrangements over the next few years.⁴

Two trends, at least in part, are likely influencing investment managers to increasingly engage in outsourcing key asset-servicing functions, particularly in the more rapidly growing alternative investments sector. The first trend is the continuing evolution of sophisticated investment strategies and instruments, often involving a global trading platform. The second is the industry's growing dependency on technologically advanced, cost-efficient and functionally capable middle- and back-office servicing organizations.

While operations, information, and data increasingly move to third parties, important legal and fiduciary responsibilities remain with funds and advisers. In this environment, how should funds and advisers manage or oversee forensic tests? Should they expect these tests to be performed by third-party service providers? Should the tests be incorporated in service level agreements? In off-shoring arrangements, could any local privacy laws or regulations preclude the fund or adviser from getting access to information or data? In consultation with their counsel, investment management firms should consider these and other relevant questions to ensure that outsourcing does not compromise their ability to fulfill their legal and regulatory obligations.

Growing expectations for sound privacy and confidentiality practices

Looking ahead, we can expect the SEC, shareholders and other stakeholders to pay increasing attention to whether funds and advisers are taking sufficient precautions to safeguard investor information and determine if any breaches

of privacy or confidentiality have occurred. At the same time, according to the *Global State of Information Security Survey, 2006*, conducted by PricewaterhouseCoopers and CIO Magazine, 36% of financial services firms responding had not measured and reviewed the effectiveness of their information security policies in the past year.⁵

This gap in awareness is noteworthy. When asked about security-related attacks, more than three in ten survey respondents from the financial services industry were either unaware or uncertain about critical factors affecting their organization's security environment. Specifically:

- 30% couldn't estimate the number of security attacks in the past 12 months;
- 32% didn't know the type of attack; and
- 32% weren't sure about which class of vulnerabilities had been exploited.

The expanse of digital networks and electronic records is an appealing territory for sophisticated intruders seeking to gain valuable currency—namely, information about investors, including account numbers, dates of birth, and Social Security numbers—the single most valuable piece of consumer information to identity thieves. Risks to the privacy and security of investor data come not just from hacking attacks on firms' computer networks. They also arise from activities of knowledgeable insiders who exploit vulnerabilities in controls and abuse their access to confidential information; sophisticated schemes to bypass authentication controls in shareholder service call centers; and accidental loss of back-up tapes or companies' unencrypted laptops.

The increase in outsourcing, noted previously, also points to one of the hottest areas of regulatory attention around privacy and data security compliance. With outsourcing on the rise, regulators are seeking to affix/clarify responsibility and accountability among the parties involved for safeguarding the sensitive data of fund and adviser shareholder records and other information shared with third-party providers.

Issues in regulatory examinations around compliance with privacy and confidentiality rules can be expected to grow in coming years, reflecting trends throughout the financial services industry. Those trends include heightened enforcement actions at both state and federal levels.

In this environment, funds and advisers will be looking to do more work in this area, particularly in regard to detecting electronic-based security lapses. Forensic tests oftentimes can be a part of this effort; and one piece of an integrated information risk management and regulatory compliance program that combines administrative, technical and physical safeguards to protect sensitive customer information.

New opportunities arising from new uses of technology

The use of forensic tests need not be limited to examining data in existing automated accounting application systems. Emerging or newer technologies support efficient transcriptions or analyses of voice and text communications, further pushing the application of forensic tests to information beyond structured data.

“...Interactive data will transform static figures into dynamic databases that can readily be searched, analyzed, and compared. There is no more important place for application of this tool than mutual funds, where millions of Americans engage in comparison shopping each day...”

*Christopher Cox, Chairman,
U. S. Securities and
Exchange Commission,
Press Statement,
January 4, 2007*

Further, the SEC is moving ahead rapidly in developing and implementing its interactive data filing and disclosure platform. When fully implemented, the platform’s underlying international standard—eXtensible Business Reporting Language (XBRL)—will allow users to access and view information filed with the SEC independently from the reports themselves, and to use that information interactively in spreadsheets or other analytical applications. Recently, as part of its interactive data voluntary filing program, the SEC announced it will permit mutual funds to voluntarily furnish information in the risk/return summary of their prospectuses using XBRL.

Again, when fully implemented and used by funds, it is envisioned this new interactive platform will provide greater accessibility to fund industry and peer fund data, making it possible to undertake analyses not easily performed today. The platform will allow investors to comparison shop and enable funds to compare financial information, ratios, holdings, investment performance, fees and expenses, and other data of similar funds across the U.S. mutual fund industry. In this manner, the interactive platform will facilitate a fund’s process to confirm expected similarities in information and identify unexpected dissimilarities in information that can be further investigated, if necessary.

Such detailed comparisons to third-party information can be viewed as extending forensic testing beyond its historical paradigm of examining in-house information. Viewed differently, the SEC’s interactive platform can also represent a new means to identify matters for which additional conventional forensic tests could be undertaken. Either way, chief compliance officers may wish to begin considering the potential forensic testing opportunities embedded in this electronic language.

4. Incorporating forensic tests in compliance programs – ten considerations

As conveyed in Section 2, CCOs continue to face uncertainties about designing, implementing and expanding their use of forensic testing in their compliance programs. The information presented below is intended to assist CCOs and other compliance, risk management, and internal audit professionals in navigating some of the gray areas.

1. Use forensic tests for multiple purposes.

Forensic tests can be designed for one or, more desirably, multiple purposes, such as:

- identifying deficiencies in current compliance policies and procedures;
- identifying unintentional errors;
- providing information that is useful in enhancing or strengthening a fund's or an adviser's existing compliance programs and, more broadly, its internal control over compliance with laws and regulations;
- identifying unusual or unexpected trends or patterns over a period of time; and
- detecting hidden schemes or arrangements, including fraud.

The nature, extent, and timing of forensic tests should be influenced by the specific test objective(s) established and the business area(s) and related circumstance(s) in which the tests are to be applied.

2. Incorporate more, rather than fewer, perspectives when developing tests.

In determining how best to implement forensic testing, a broad group of fund or adviser management should be involved, to ensure that all relevant perspectives are discussed. Beyond the CCO, that group should include other compliance, risk management, internal audit, finance and accounting professionals as well as senior legal staff. Those charged with governance, such as the board of directors or its audit/compliance committee(s) might also participate; at a minimum, the decisions made in this phase should be presented and discussed with them.

3. Focus on all aspects of operations, including the activities of third-party service providers.

When determining the nature and extent of compliance testing to be performed, including forensic tests, CCOs must consider the activities of any affiliated or third-party service providers, such as subadvisers, transfer agents, administrators, underwriters, and custodians, in addition to activities conducted directly by the fund or adviser. In cases where a higher compliance risk has been identified in third-party service provider activities, CCOs and/or other responsible parties will need to work with the service provider to develop an agreed-upon course of action that achieves this objective.

4. Take a fresh look at existing capabilities and skills, and supplement them if needed.

The effective application of forensic tests requires both general and specialized competencies and skills. Many funds and advisers employ or have access to individuals with considerable skills and experiences in audits of financial statements, compliance reviews, operations assessments, and evaluations of computer operations, application systems and other technologies. These individuals have important knowledge of, and experience with, corresponding test methodologies.

All of these competencies, skills and experiences provide a necessary foundation for effective use of forensic tests. However, in many environments, more may be needed. The widening business interests within many financial services companies (e.g., side-by-side investment management activities and firm trading); growing complexities in fund and adviser operations; the continued presence of potential conflicts of interest; and increasingly sophisticated technologies all can contribute to an increase in fraud risk conditions or inadvertent errors. Because of this, in addition to the competencies described above, forensic testing may need often to draw upon stronger and deeper technical and data analysis skills, investigatory mindsets, and communication capabilities, as well as newer automated tools, such as those being used in voice and text analysis. Funds and advisers should assess the availability of these specialized skills and tools within their organizations to ensure that appropriate resources are in place to support an effective forensic testing environment. They should supplement their internal resources, if needed, with third-party “testers” having competencies in this area.

5. Evaluate current information technology systems and functionality, to ensure they can support forensic testing.

Management of funds and advisers should evaluate their firms' information technology systems to determine their sufficiency to support the forensic testing plan. This evaluation should include:

- inventorying source systems to determine what relevant data may be available;
- identifying means to capture and gather relevant data from systems, including external systems when appropriate;
- assessing the current state of data quality for its reliability and compatibility with data extraction and formatting routines;
- determining the availability and frequency of updating of information, housed in data marts, which is stored and accessed for analysis; and
- identifying which data analysis programs exist and which additional programs may require development.

6. Use forensic tests in conjunction with other compliance program testing activities.

The implementation of compliance programs for funds and advisers takes many forms, reflecting the diverse nature of the investment management industry. Yet there is one common planning element of each annual compliance review: the process of aligning higher compliance risks to the measures in place to manage those risks. The means used to identify

such measures vary among funds and advisers, but generally begin with a consideration of the following factors:

- the overall internal control structure in place;
- compliance policies and procedures adopted and implemented;
- the features of application systems used; and
- the nature and extent of any testing of internal controls over compliance undertaken by business unit personnel and by internal audit and compliance staff.

Chief compliance officers should keep all of these considerations (and recent corresponding test results) in mind when determining the nature, extent, and timing of compliance testing procedures. Forensic testing is one of many testing means available to CCOs in this regard. In determining the extent of forensic tests to be performed, CCOs should take into account whether this type of testing in selected areas can be performed with reasonable efficiency and effectiveness, or whether an alternative testing approach can address similar testing objectives at less cost. Further, in some circumstances, the implementation of forensic tests may allow a fund or adviser to alter the nature, timing, and extent of other compliance tests performed.

7. Establish an appropriate review structure.

By its nature, forensic testing often produces results that are less familiar than the results of more conventional tests of internal control. This can present additional challenges for funds and advisers. For example, they must consider the following:

- Are the purposes of these forensic tests fully understood by people in supervisory and oversight roles?
- What constitutes a “problematic” finding?

- Are the activities or behaviors observed in test results reasonable and recurring, or suspicious in nature?
- Has forensic testing uncovered information or trends which point to a possible violation of a law or regulation?
- Should expectations be set before the testing begins so that any data falling outside those expectations are more critically reviewed?
- Are there other potential compliance vulnerabilities that are not covered by the forensic analyses?
- What other analyses should be performed?

To address these questions, fund and adviser management may wish to supplement normal supervisory reviews with the input or perspectives of other parties with forensic testing expertise, so that their experience-based judgment can be looked to, at least by those in their early steps of this type of testing.

8. Consider forensic test results in connection with other embedded reporting responsibilities.

Practically speaking, the recent impetus behind forensic testing in the investment management industry is the SEC compliance program rules adopted in December 2003. In this regard, forensic testing can provide important information to CCOs about their fund's or adviser's compliance programs in the context of 38a-1 and 206(4)-7 and, more broadly, such entities' internal control over compliance with laws and regulations.

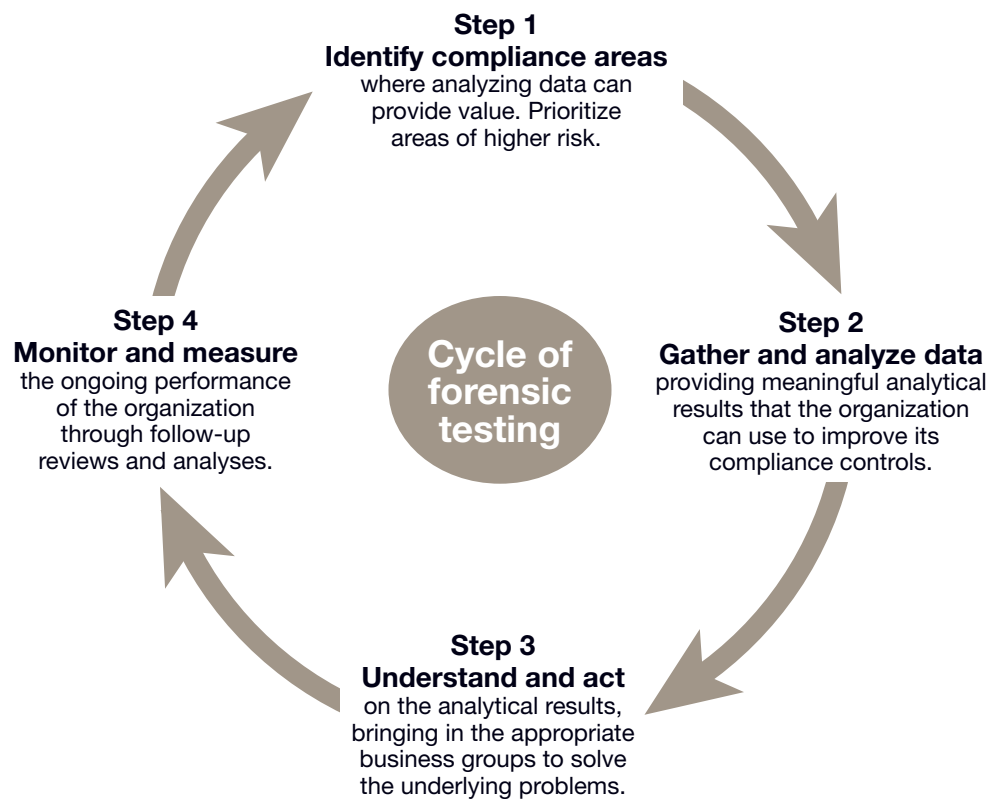
However, the results of these new testing activities should also be considered in the context of other embedded reporting responsibilities. They can also support broader compliance and financial reporting objectives. Forensic tests can provide information (and, sometimes, supporting evidence) that should be considered in preparing fund officer certifications related to the Sarbanes-Oxley Act of 2002 (specifically, Section No. 302-3 regarding disclosure controls and procedures and internal control over financial reporting and Section No. 906 regarding corporate responsibility for financial reports). Similarly, as appropriate, results of forensic tests undertaken by an adviser entity with reporting obligations under Section 404 of the Act should be considered in connection with management’s evaluation of internal control over financial reporting.

9. Use forensic test results to enhance internal control.

Similar to other forms of testing, the results of forensic tests can be used to enhance a fund’s or an adviser’s compliance program and, more broadly, its internal control over compliance with laws and regulations. For example, forensic test results can provide insights into the following:

- how existing compliance policies and procedures should be clarified or changed;
- the ways in which front-end application or processing systems could be modified to incorporate additional “preventive” and “detective” controls to prevent and spot earlier noncompliant transactions, respectively; and
- where control activities may be enhanced to reduce the number of exceptions or violations occurring.

The diagram below illustrates the cycle of forensic testing, findings and remediation, which serves to enhance a fund's or an adviser's compliance program and its internal control over compliance with laws and regulations.



10. Communicate test plans and results to all relevant parties.

The effective development, implementation, and ongoing use of forensic testing by funds and advisers require robust and clear communications among a number of parties. In their annual compliance review plans, fund and adviser CCOs should document the details and expected use of forensic tests and discuss these with those who are responsible for governance. The results of forensic tests should be discussed with the same parties on an annual basis, at a minimum, or more frequently, as circumstances dictate. Relevant information about forensic test plans and results also should be communicated to others with oversight responsibilities for funds and advisers, such as internal auditors, risk managers, fund treasurers, and counsel.

Appendix: Illustrative forensic tests

CCOs and other compliance professionals face significant challenges in designing and conducting forensic tests because these tests differ from customary compliance activities in several ways: Often, forensic tests require a retrospective examination of large volumes of data. Detection routines must be embedded in test parameters that can ferret out sometimes-sophisticated schemes or subtle historical patterns. Certain patterns may be known, but the testing process must be sufficiently flexible to identify and adapt to new emerging patterns. Also, forensic tests may encompass both structured data, such as trading blotters, and unstructured data, such as personal trade statements, email messages and attachments and, in some cases, voice-related communications.

To assist CCOs and other compliance professionals, this Appendix presents examples of forensic tests that might be applied in areas of higher compliance risk and in other selected areas of a fund's or adviser's operations. These examples are not intended to compose a complete list of possible forensic tests that could be performed in these areas, nor do the areas shown necessarily represent all areas of higher compliance risk to funds or advisers. Specific business circumstances may require the use of forensic tests different than those presented in this Appendix. In addition, the period over which and the frequency with which forensic tests should be applied vary among the different tests and the funds or advisers executing them.

Further, funds and advisers may have different expectations when conducting forensic tests. Some may be confident that the tests will affirm expected results—namely, that they will not produce any new information about the status of compliance with laws and regulations beyond that previously produced by applying other components of internal control. Others may be less certain about the results of forensic tests and their implications. Regardless of these varying expectations, certainly all funds and advisers will wish to identify any unintentional errors or unexplained or unusual trends or patterns. It is also expected that appropriate follow-up or remediation of any such matters will take place and will be reported to relevant parties. Of course, funds and advisers also should prepare and retain documentation pertaining to forensic tests and any corresponding follow-up and/or remediation taken.

Forensic tests: Brokerage arrangements and related portfolio activities

Brokerage arrangements and related portfolio activities constitute one of the more fertile areas of operations for which the application of forensic tests can be efficient and effective. The high volume of data, velocity of transactions, susceptibility to processing errors, potential conflicts of interest, and opportunities for abusive trading and other arrangements combine to provide an environment in which additional checking—performed through a detective lens—can well serve funds, advisers, and investors.

Broker-dealer selection and use

1. Summarize trades with and commission dollars paid to broker-dealers. This will aid in understanding which broker-dealers are used, the types of trading arrangements used (e.g., soft dollar, directed brokerage, electronic communication networks (ECNs) or similar trading platforms, and traditional or full service brokerage), the level of business directed to each (see also **Commission arrangements**, below), and the investment-related purpose of each relationship. Identify any broker-dealers who appear to be strongly favored in terms of level of business, and determine if there may be undisclosed potential conflicts of interest, such as soft dollar or client referral arrangements, favorable IPO allocations, favorable personal trade arrangements, or the existence of other corporate or personal financial relationships.
2. Determine whether any familial relationships or other potential conflicts of interest exist between or among investment professionals who can direct or influence the selection and use of broker-dealers and the broker-dealers' senior management and trading personnel. Examine business and allocation arrangements with these specific broker-dealers. Understand how the potential for abusive practices or arrangements in this area is identified and managed.
3. Compare research and execution commission budgets to actual broker-dealer allocations.

Best (comparative) execution by broker-dealer

Compare execution prices achieved through and commission rates paid to each broker-dealer who traded the same security on the same day in the same direction. Examine results of these comparisons, taking into account relevant factors such as the liquidity of the holding, size of trade, and intraday price movements, to identify trends in broker-dealer trade execution. Understand results for broker-dealers with potential conflicts of interest or trading activities involving special arrangements.

Nonapproved broker-dealer transactions

Identify trades executed through broker-dealers (including affiliated broker-dealers) who were not approved for use at the time of the transaction.

Commission arrangements

1. For each fund/account, summarize commission dollars paid to each broker-dealer, by relevant type, for execution, clearance and settlement of each security type. Include the corresponding total number of trades made and shares transacted, and the average commission per share. For any "outliers," understand the investment purpose underlying the use of, or value derived from, the corresponding broker-dealer relationship(s) and the potential for undisclosed arrangements.

2. Compare the total dollar volume of sales of fund shares and the total number of client referrals by broker-dealers to commission information for all broker-dealers (as described in the previous test). Identify unusual or unexpected trends or relationships which may indicate the potential misuse of fund or client assets.
3. Compare commission rates to approved or contractual terms. Examine overrides of established or approved commission arrangements or terms to identify potential problems or unusual patterns. Identify and understand any changes in commission rates by broker-dealers that result in an increase in such rates.
4. Confirm with broker-dealers whether any brokerage reallowances, rebates, or other payment arrangements, established as part of trade commission arrangements, are in place between or among the broker-dealer, the fund/client, adviser, or any other parties.
5. Identify potential principal trades executed through any affiliated broker-dealers.
6. Compare commission rates paid to affiliated broker-dealers to approved terms and to rates paid to unaffiliated broker-dealers.
7. Identify any unusual or unexpected positive values (excluding special fees, taxes, or other routine assessments levied on securities trades) in data fields in trade records, apart from the brokerage commission data field. Understand the nature and investment purpose of the cost or fee borne by the fund/account.
8. Identify any negative values in commission data fields in trade records, which may indicate unintentional processing errors or adjustments for one-time or recurring arrangement(s) between the adviser and the broker-dealer(s).
9. Identify spikes in trading or "outlier" commissions to soft-dollar brokers near year-end.
10. Compare fund/account portfolio turnover rates to disclosures made to shareholders/clients and, for unexpected or unusual higher rates, understand any salient correlations able to be drawn with specific broker-dealers, to identify potential instances of 'portfolio churning.'
11. Compare securities transactions made shortly before the end of a reporting period and those made shortly after the end of such period to identify potential 'window dressing' arrangements.

Best (comparative) execution by fund/account

1. Compare execution prices and commission rates paid by each fund/account that traded the same security on the same day in the same direction. Examine these comparisons, taking into account relevant factors such as the trade aggregation policy, liquidity of the holding, size of trade, and intraday price movements, to identify potential preferential treatment afforded individual funds/accounts. Understand results, particularly in cases in which there are potential conflicts or higher risks, such as when the adviser manages both affiliated and nonaffiliated funds/accounts.
2. For each fund/account, compare execution prices and commission rates on securities trades made through broker-dealers who sell fund shares or make client referrals with similar information for other broker-dealers who traded the same security on the same day in the same direction.

Trade allocations

1. Compare the investment performance of all accounts, including proprietary/personal accounts, which have similar investment objectives. Compare also to external benchmarks (and/or peer groups, if available). Understand explanations for any outliers.
2. If feasible, based on the allocation policy and data available, examine security allocations across each

fund/account. Determine fairness and compliance with the adviser's trade allocation policy, and scan for any patterns of noncompliance by individual portfolio managers/traders.

3. Identify and determine the fairness of trades allocated among proprietary accounts; accounts receiving performance-based fees; and accounts with no performance-based fee component.
4. Identify any system-embedded adjustments made to automated trade allocations produced by the order-entry/trading system (which should be programmed to comply with firm policies for trade allocation). Identify any other management overrides of established trade allocation policies and practices.
5. Identify trades generating the largest profits. Determine if such trades are allocated fairly to each fund/account. Examine allocations (among funds/clients and proprietary accounts) of new issues, initial public offerings (IPOs), and secondary public offerings for compliance with established trade allocation policies and practices. Determine if any 'access person' accounts were allocated any of these issues.
6. Scan securities purchased and sold during the month for a particular investment strategy. Identify funds/accounts within the investment strategy that did not purchase or sell such securities to determine if any unintentional or intentional misallocations were made.

Cross trades

1. Examine opposite direction trading in the same security on the same day to identify cross trades. Using established policies for transactions of this nature, determine whether any cross trades identified were (i) allocated to eligible funds/accounts in a manner consistent with such policies; and (ii) made for only funds/accounts for which consent for such trading had been provided.
2. Scan buy/sell trade prices for cross trades for consistency with established policies and the provisions of any applicable SEC exemptive order and for reasonableness in light of intraday prices available in the market.

Trade errors

1. Examine error reports for securities descriptions, affected funds/accounts (including proprietary accounts), error types, financial impact, root causes, responsible personnel, and remediation/resolution steps taken, to identify any unusual patterns or trends. If possible, aggregate trade error information over time to determine the overall error rate, and error rates for each fund/account.
2. Compare cancel/rebook transactions in trading/accounting systems to management reporting (error reports) for completeness and accuracy.
3. Identify accounts with patterns of numerous short-term trades resulting in losses to the fund/

account. Examine these transactions for potential hidden trade errors.

4. Inspect fund/account/adviser cash journals to identify any nonrecurring or special payments to/from broker-dealers.

Trade aggregation

Based on the adviser's policy for combining funds/accounts in the same trade and the corresponding execution of these block trades, identify situations in which funds/accounts were improperly excluded from a block trade. Examine the overall patterns of accounts excluded from block trades to determine if these exclusions appear to have impacted funds/accounts favorably or unfavorably. Determine if price and commission arrangements used in block trades (e.g., average) are consistent with the adviser's policy.

Restricted securities/investments

Scan transaction data for trading of securities on the adviser's restricted securities list during the prohibited time window.

Private investments in public equities

If the adviser participates in private placements of securities for publicly traded entities, gather or compile a list of private placements, and determine the transaction volume, patterns and gains/losses

from purchasing or selling shares of the publicly traded equity on and near the date of the private placement issuance. Also compare the list of private placements with the list of restricted securities.

Holding limits

For adviser-wide and individual funds/accounts, sweep all relevant portfolio holdings files and aggregate values of individual securities holdings and other relevant classifications (e.g., industries/sectors, emerging markets, and counterparties) to identify any instances in which such holdings exceed permissible limits.

Forensic tests: Personal trading

Strict regulations exist in the area of personal trading because of the significant potential for abusive practices that can materially harm fund shareholders/clients. Funds and advisers monitor the personal trading activity of portfolio managers (and other “access persons”) to ensure they do not gain any trading or investing advantage over the funds/accounts they manage, such as using their knowledge about security transactions in fund/client accounts for the benefit of their own personal portfolios. Among other possible circumstances, portfolio managers, traders, and analysts often are in a position to be able to ‘time’ their personal trades in securities to benefit from price movements that may be attributable to larger transactions in the same securities associated with fund/client accounts.

The potential for harmful or adverse consequences to a fund’s or adviser’s reputation arising from a breach of laws, regulations, rules, or the fund’s or adviser’s policies in this area makes it essential that controls aimed at achieving compliance with codes of ethics and regulations pertaining to personal trading be well designed and rigorously tested. Among others, forensic tests can be an efficient and effective means to accomplish this.

1. Examine areas of higher risk to detect any sign of unfair trading advantage over funds/accounts (e.g., front running; short-term trading; investments in restricted securities, IPOs, and public entities associated with a private placement; and same-day trading as funds/clients).
2. Identify personal trading activity in securities on the adviser’s restricted or watch list, or in securities of issuers that have announced material news.
3. Inspect personal transactions and holdings in reports provided by brokerage firms to identify any potential trading or investment violations. Determine whether preclearance for any securities transactions was obtained when required.
4. Determine whether any personal trading activities in proprietary or sponsored funds, including through employee benefit plans, could be construed as ‘excessive trading.’
5. Scan personal trading activities for potential violations of minimum holding and trading “blackout” period requirements.

Forensic tests: Gifts and entertainment

Inappropriate or excessive gratuities shared between or among parties having fiduciary duties to funds/clients can be a source of harm to such funds/clients and/or the adviser's business reputation. Forensic testing can help to identify inappropriate gifts or entertainment.

1. Correlate information about gifts and entertainment provided to third parties or received by employees of the adviser to business activities conducted, such as:
 - the level of securities trades directed to broker-dealers;
 - commission rates and execution prices obtained from broker-dealers who participate in gift and entertainment activities and others who don't, for securities traded on the same day in the same direction;
 - products or services (research-related) paid for with fund/account assets;
 - client referrals or procurement of "platform" or "shelf space" for fund distribution.
2. Scan expenses of employees in corporate accounting records or corporate travel service provider records. Identify expenses that represent the sponsorship or underwriting of another third-party person's activities or consumption (e.g., sporting event tickets, other entertainment, and transportation and lodging), including those incurred in connection with events or conferences hosted by the adviser.

3. Review employee expense reports periodically to identify any unusual or unexpected patterns of gifts or entertainment.

4. Confirm understanding of gifts and entertainment information directly with third parties.

Forensic tests: Fund accounting

Fund accounting books and records provide another rich source of information or data to which forensic tests may be applied.

Securities reference or master files

Often a securities reference or master file is maintained by the adviser and another file is maintained by the fund accounting agent. In these cases, compare all relevant data fields in one file to the other file for consistency of information such as CUSIP number, security description, interest rate, maturity date, and call features.

Books and records

Sweep general ledger posting entries and identify any nonstandard automated or manual entries made. Determine that sufficient support and authorization exists for such journal entries and appropriate documentation has been prepared and retained (numbered, dated, including preparer/reviewer information and journal entry description, etc.).

“Dummy identifiers”

Compare the trend in the number of “dummy identifiers” held in the security reference file(s) to the trend in the volume of securities that would reasonably be traded. Inspect “dummy identifiers” to uncover instances in which security set-up parameters are potentially being circumvented.

Anomalous securities data

Sweep relevant securities holdings files to identify unpriced securities; securities whose prices/quotations are not being second-sourced; and rates on variable rate securities that have not been reset in during a period of time.

Expense processing

Use trend analyses on expense adjustments to identify situations in which under/overaccruals of expenses are not being “trued up” in appropriate periods.

Forensic tests: Valuation

Valuation is an area comparable to **Brokerage arrangements and related portfolio activities** (see page 24) in its breadth of potential unfavorable consequences to investors arising from activities that violate laws, regulations or policies. Among other considerations, valuations have an impact on investment

performance, fees paid to advisers; compensation of portfolio managers; the buy-in or redemption price for shares or units of the fund or account; and consideration paid or received for allowable securities trades among affiliated entities. Each of these considerations involves the potential for unfair gain by one interested party over another party or investor.

1. Identify all funds/accounts whose circumstances create higher incentives to manipulate securities pricing routines or to “game” the valuation system (e.g., the existence of performance fees or other compensation arrangements tied to growing the assets in the fund/account). Array and analyze relevant securities pricing over periods of time to identify any unusual or unexplained trends, stale prices, or unusual changes to such prices (related to the timing of the change, such as near a quarter or year’s end, or to the degree of the change). Scan securities trading records for period-end ‘minor’ purchases which may have been executed to ‘push up’ reported securities prices.
2. Compare selling prices for fair valued or hard-to-price securities (e.g., restricted and illiquid securities) to their prior day’s fair values to determine the reasonableness of their pricing.
3. For advisers managing multiple investment products across multiple system platforms, identify any commonly-held securities for which the established valuations/prices differ. Determine whether such differences are supportable in the circumstances.

4. Identify and review securities pricing overrides made by advisers, subadvisers, general partners, managing members, or boards of directors.
5. Back-test third-party vendor fair values for securities versus next market opening price.

Forensic tests: Anti money laundering

While the number of known incidences of money laundering appears to be higher in banking and other financial institutions than in the mutual fund industry, money laundering provisions of the U.S.A. Patriot Act of 2001 extend to mutual funds. As a result, the fund industry has expended significant resources over the last several years in policies, systems and controls to help detect suspicious activities which may constitute money laundering. Among other references, funds have looked to guidance (in the form of Frequently Asked Questions) provided in October 2006 by the Financial Crimes Enforcement Network when considering the type of circumstances for which a Suspicious Activity Report should be filed. Forensic testing also can be used to detect suspicious activities that could be indicative of money laundering.

Conduct retrospective analyses to identify unusual transactions and behaviors. To detect potentially unlawful

activities, when available, use money laundering risk ratings of shareholders by type of account; pattern analyses (e.g., quick turnarounds in funds received and redeemed); and behavioral analyses of actual activity (e.g., identify transactions that deviate from expected patterns built through statistical modeling).

Forensic tests: Transfer agent

Transfer agent activities generally are subject to numerous, detailed guidelines or provisions contained in fund prospectuses and statements of additional information. Processing errors, noncompliant transactions, and schemes to gain unfair advantage over other shareholders can sometimes be discovered through forensic tests. Also, forensic testing can be a helpful means to uncover incidences of market timing.

1. Sweep the shareholder master file to identify negative value accounts.
2. Scan shareholder transaction history file in dormant accounts to identify questionable or unexpected activity.
3. Sweep the shareholder transaction history file to identify unusually high frequency of adjustments in individual accounts.

4. Sweep the shareholder transaction history file to identify noncompliant shareholder transactions (e.g., not meeting purchase minimums, making excessive exchanges between or among funds, or Class B share purchases in excess of prescribed dollar limit).
5. Sweep the shareholder master file to identify accounts in amounts below the minimum balance required, as described in the fund prospectus.
6. Map provisions (contained in fund prospectuses and statements of additional information) covering the rights of purchasing and redeeming shareholders to share in the fund's capital gains and investment income to actual fund-level money flow practices. Determine that crediting practices at the shareholder level are aligned, as desired, with the availability of such monies at the fund level for investment purposes.
7. Compare level of shareholder purchase and sale activities to corresponding fund size and investment objective to identify unusual or unexpected patterns or levels of activity.
8. Identify account holders whose trading patterns appear to be excessive or in violation of specific trading restrictions.
9. Scan significant transactions in omnibus accounts to identify potential market timing transactions.

Forensic tests: Books and records—email

Funds and advisers maintain email pursuant to their policies and procedures as well as SEC books and records rules. This information must be readily available for review by SEC staff upon request. Forensic testing can be used to review emails as part of a fund's or an adviser's monitoring activities.

Developing effective forensic tests for email requires an investment in requisite tools and data stores to facilitate comprehensive searches. In addition, it requires the development of keywords that target communications that might be relevant to the issue at hand. Also, for a forensic test to be effective, the population of emails captured for review needs to be manageable. Techniques that may be used to focus a forensic review of email include the following:

- defining a specific time period under review;
- focusing the analysis on specific individuals as opposed to a wider group;
- utilizing Boolean terms (AND, NOT, etc.) to link keywords;
- reviewing communications that only involve one or two individuals as opposed to emails that are copied to larger groups; and
- developing a key word list that incorporates slang terms as well as precise technical terms.

Endnotes

- ¹ *Final Rule: Compliance Programs of Investment Companies and Investment Advisers, Investment Advisers Act Release No. 2204* (December 13, 2003).
- ² Andrew J. Donahue, Director, SEC Division of Investment Management, *Keynote Address before IA Week's 6th Annual Fall Compliance Conference*, New York, NY, September 25, 2006.
- ³ Developed by The Committee of Sponsoring Organizations of the Treadway Commission.
- ⁴ Survey of more than 150 finance executives from mutual funds, hedge funds and other asset management firms, who attended PricewaterhouseCoopers' Investment Management forums in May 2007.
- ⁵ The survey was based on 7,791 responses from IT and security professional in 50 countries. Approximately 10% of respondents to the survey were from companies in the financial services industry.

Incorporating forensic tests in compliance programs— 10 considerations:

1. Use forensic tests for multiple purposes.
2. Incorporate more, rather than fewer, perspectives when developing tests.
3. Focus on all aspects of operations, including the activities of third-party service providers.
4. Take a fresh look at existing capabilities and skills, and supplement them if needed.
5. Evaluate current information technology systems and functionality, to ensure they can support forensic testing.
6. Use forensic tests in conjunction with other compliance testing program activities.
7. Establish an appropriate review structure.
8. Consider forensic test results in connection with other embedded reporting responsibilities.
9. Use forensic test results to enhance internal control.
10. Communicate test plans and results to all relevant parties.

pwc.com

© 2007 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP (a Delaware limited liability partnership) or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate and independent legal entity. *connectedthinking is trademark of PricewaterhouseCoopers LLP (US). MC-NY-07-1166-A