TOP 10 OPERATIONAL RISKS
A Survival Guide for Investment Management Firms

seic.com/ims
Introduction

In 2010, then-consultants Holly Miller and Philip Lawton authored the book, *The Top Ten Operational Risks: A Survival Guide for Investment Management Firms*. Growing from a presentation and discussion at an industry roundtable, the book was motivated by recognition of a simple fact: when investment management firms stumble or fail, their clients suffer.

Having since joined SEI’s Investment Manager Services division in mid-2011 as Managing Director of Middle Office Outsourcing, Holly works with organizations that understand that coming to grips with operational risk is becoming ever more critical for investment managers who want to survive, let alone thrive. Indeed, she champions the view that investment organizations need to tackle the issue with the same intensity they bring to battling market volatility and economic crises.

Accordingly, we at SEI are pleased to issue an on-line summary version of the book with abridged content and a redesigned format. Our goal is consistent with Miller and Lawton’s original objective: to make key concepts easily accessible and actionable without becoming mired in esoteric issues or technical terms. Besides updating each chapter with proactive risk management steps, we have added a concluding chapter on developing an action plan to strengthen operational risk controls.

Like the book from which they are based, these summaries are designed as a resource for investment managers—traditional and alternative alike—who seriously want to understand and reduce their exposures to operational risks. They have every reason to do so. The operational realm is one in which a minor oversight or a single misstep in daily routines can have potentially major consequences. In worst-case scenarios, a single incident can result in significant direct costs and, worse still, devastating reputational damage from which it may take years to recover. This is why operational risk is such a grave concern not only to investment management firms, but also to their clients, investors, regulators and trading partners.

Operational risk can stem from many sources. The Basel Committee on Banking Supervision defines operational risk as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.” The definition considers the full range of material operational risks and lists examples ranging from fraud and data entry errors to hardware failures and floods.

Further complicating risk management efforts, organizations may differ widely in their exposure to operational risk, depending, for instance, upon their investment strategies, the markets in which they operate and the instruments they employ. As with investment risk, firms also have varying tolerance levels for operational risk. Consequently, there is no generic checklist for identifying operational risk, nor is there a single, universally applicable set of mitigation measures. Still, we believe virtually every investment management firm can benefit from taking a fresh look at common areas of risk, and considering the variety of relatively straightforward risk management measures that can readily be deployed by large and small organizations alike. This guide is offered in that spirit.
Our “Top Ten” list summarizes the areas of risk that are frequently encountered by those who work in or around investment operations (though not in order of severity or potential loss). The list includes issues that keep arising in operational reviews even though they have received significant attention in industry media over the years. The first three chapters take up personnel issues, including supervision and training. Chapters four through seven address organizational and support issues, including the role of technology, which can be both a solution and a source of risk in itself. Chapters eight through ten focus on common areas of weakness in reconciliation, legal review and planning.

While there can be no “one size fits all” approach to operational risk management, each chapter provides best-practice suggestions for identifying whether a given risk exists within your organization, as well as potential steps for mitigating it. We hope that this guide will help many organizations to rethink and reduce their exposure to operational risks.

It has been observed that operational risk offers no upside; to use Castle Hall Alternatives’ phrase, it is risk without reward. But we at SEI have a different perspective. We think in terms of operational excellence as a way to create investment value by reducing costs, increasing client satisfaction and reinforcing sound business relationships with trading partners.

To our way of thinking, effective risk management is the foundation of operational excellence. With this guide, we offer investment managers one more resource for pursuing that goal.


Complacency might be summed up as a mindset that fails to ask, “What if...?” It’s a passive laid-back attitude that says, “So far, so good. We have policies in place. Nothing terrible has happened. Everything’s under control, no need to worry...”

Is This Your Firm?

Firms with a culture of complacency take a passive approach toward operational risk rather than adopting a proactive one. This way of thinking may be evidenced by:

› Reacting to headline risks, such as the September 11th attacks or the Madoff scandal, rather than factoring operational risks into day-to-day planning.
› Risk-planning exercises that focus on the rearview mirror rather than considering what might happen next.
› Sketchy business continuity plans. (Has anyone considered the potential loss of staff in a worst-case scenario?)
› Poor recordkeeping. (Is there a chronic backlog of documents waiting to be scanned?)
› Deficient insurance coverage. (Are there adequate policies in force for errors and omissions as well as general liability and directors’ and officers’ coverage?)
› Short-changing of operational and IT investments for several years running. (How many releases behind are critical investment applications?)
› Launching new investment strategies without conducting a cross-functional product launch review.

Avoiding Common Pitfalls

Inexperienced or underqualified staff
Hiring insufficiently skilled staff introduces significant operational risk to an organization, and neglecting to train new employees compounds the error. This is a needless risk, especially in the current market environment, when so many good people are available.
One reason firms may fail to hire qualified staff is that they underestimate the complexity of the products they offer or the financial instruments they trade. For example, firms that manage fixed-income securities generally require more advanced skills and systems than those focused solely on equity instruments. Likewise, investing outside one’s own country requires substantially more data elements and operational effort. Emerging markets, derivatives or illiquid securities can introduce even more variables.

To be proactive:

› Recognize the importance of aligning staff skills with operational complexity and hire or train appropriately.

Ignoring input from middle- and back-office staff

These staff members may be the best equipped to see ways of reducing the probability of errors within their own functional areas. Beyond that, they often see risks that originate elsewhere in the organization. For instance, they may notice consistently incorrect or late trade entries by a particular trader, or see sales and marketing teams change presentation materials following a compliance review.

To be proactive:

› Invite and listen to the feedback offered by support teams as well as by service providers, making sure senior management takes immediate action to resolve any critical issues raised.

› Maintain and regularly review error logs that capture both errors and near misses; the instructional value they offer should not be squandered.

› Establish a formal new product committee that includes not only investment and sales/marketing staff, but also compliance, operations and IT.

› Keep staff informed, introducing a new counterparty or unfamiliar security type without a heads-up to operations, compliance and IT may significantly increase the risk of failed trades, a problem that can be avoided without any additional expense to the firm.

Lack of robust electronic document management

Have crucial documents such as investment management agreements, guidelines and objectives, client correspondence and other contracts been scanned and backed up? Or are they sitting in locked file cabinets, vulnerable to anything from plumbing issues on the floor above to a forced relocation after a disaster? (For a real-life illustration of such perils, read the SEC’s July 2000 response to Jennison Associates’ request for a no-action letter.1 In a warehouse fire, Jennison lost records that supported the firm’s performance track record—arguably any investment manager’s single most valuable non-tangible asset. As for plumbing problems, ask JP Morgan about the pipe that burst on the firm’s London trading floor in September 2010.)

1 sec.gov/divisions/investment/noaction/2000/jennison070600.pdf
To be proactive:

› Ensure that critical documents are always effectively backed up. In today’s environment of inexpensive document scanners and cloud computing, this is a measure that even the smallest investment manager can afford.

Blind trust of operational teams

Many investment managers operate with the philosophy that they should simply hire good people, and then get out of the way so they can do their jobs. While this may seem laudable, it is actually a disservice to leave team members with no effective oversight. With no checks on whether an account was reconciled properly, performance-based fees were calculated correctly or a compliance rule was interpreted and coded appropriately, staff members are put in the position of being solely responsible for the accuracy of their work. They are also left vulnerable to suspicion should things go wrong or evidence of improprieties comes to light.

To be proactive:

› Develop procedures that provide appropriate checks and balances for operational staff. Just as even the best writer needs an editor, staff members deserve to work with effective oversight. The same point applies when it comes to managing service providers. (At SEI, we consider an effective oversight program to be the hallmark of a good client.) Rather than indicating a lack of trust, proper oversight demonstrates a firm’s commitment to risk management on behalf of clients and staff alike.

In sum, take a minute to consider what could “bite” your firm. Ask your staff the same question. Think about whether you reward, punish or ignore news of a risk. And then work on some ways to keep potential problems from ever happening.
Supervision is a major area of operational risk because breakdowns occur so often and in so many different forms. It is one thing to manage our own tasks. Directing the decisions and activities of others is a much greater challenge—and the larger the firm, the more difficult that job. Another set of risks is encountered when investment managers outsource critical support services to specialists, a measure that, ironically, is often intended to reduce operational risks.

Avoiding Common Pitfalls

Managers unfamiliar with operational functions
This problem is not confined to small firms that cannot yet afford to hire specialists in domains such as operations and systems, human resources and accounting. As organizations grow, they eventually reach the point where managers can no longer be hands-on supervisors with the time and knowledge to perform any job in their purview. Instead, they become executives who must rely on the experience and expertise of their direct reports. Problems also occur when, in a well-intentioned effort to promote from within, firms select team leaders who are insufficiently versed in operations and quickly find themselves in over their heads.

Top-level managers are often even more removed from operational functions. Within most buy-side firms, the chief executive typically comes from the investment or distribution side of the organization; operations, compliance and information technology (IT) are typically not seen as incubators for CEO positions. As a result, few senior executives have a solid understanding of increasingly complex middle- and back-office functions, much less a firm grasp of the details involved in identifying and managing operational risk.

This leaves many executives at a loss when it comes to evaluating the performance of operational teams or the recommendations of their direct reports—not to mention assessing operational risk. They may end up falling back upon their instincts, or heeding the advice of their most persuasive team members rather than the most knowledgeable ones; indeed, they may not even realize which team members are the most expert. This is not to say that executives in the areas of business management, investment, or marketing must become operational experts. They should, however, be equipped to ask the right questions about risks to which the firm and its stakeholders might be exposed.
To be proactive:

› Offer a management training program in which recruits or employees with leadership potential are rotated through the various functional areas of the organization. Often used in the military and by firms such as Vanguard, such programs can help ensure that tomorrow’s leaders have a strong grasp of key functions and activities. Ensure the time spent in each area is sufficient to obtain a strong grasp of its functions.

› Use process mapping and workflow documentation to help managers understand middle- and back-office functions. For example, show what happens when a new account is opened or a portfolio manager initiates an order. Graphical representations of the systems architecture and various workflows can be a great help here. By memorializing processes, procedures and accountabilities, such documentation not only assists in daily functioning, but also facilitates effective training. (This is not a panacea however—see Risk Area #6, “Playbooks,” for a discussion of potential issues with workflow documentation.)

› Provide for external assessments such as mock regulatory examinations, peer benchmarking and operational due diligence reviews, all conducted under strict nondisclosure agreements. Such reviews may not only identify improvement opportunities, but also tell CEOs whether they should continue to rely upon their direct reports.

› Create or strengthen internal audit departments for recurrent monitoring. This could complement or substitute for external assessments.

Delegating responsibility to managers unqualified for the tasks

This is another frequent consequence of executives’ failure to appreciate operational complexity. For example, CEOs commonly assign all responsibility for operational risk to a compliance team composed entirely of attorneys and paralegals. To suggest that a law degree or a regulatory background qualifies someone to identify and mitigate technological or operational risk is as misguided as calling upon an IT or operations expert to prepare the offering documents for a fund. It also raises a question of corporate governance: Who oversees compliance?

To be proactive:

› External operational reviews can help pinpoint areas of organizational risk within a firm.

› Develop more comprehensive job descriptions that spell out essential skills and competencies in detail, and update them regularly. This can assist in hiring and promotion decisions while also illuminating employee training and development needs.

› Develop and maintain robust training and cross-training programs to preserve institutional history and knowledge.

› Implement succession planning for all key positions, noting that even very junior positions may be vital.
Understaffing for the volume of activity

During the 2007-2009 downturn, many buy-side firms made significant cutbacks in staffing. Support teams were often affected and, in some cases, bore the brunt of those cost-cutting measures. Yet the number of securities transactions did not decline during this period—on the contrary, the volume of trades on the New York Stock Exchange rose throughout the crisis—and today we often see firms stretched to the limit. As the job market continues to improve, beleaguered managers and employees are more likely to seek greener pastures, leaving firms with too few experienced staff to get the job done adequately, let alone well.

Insufficient managerial bandwidth is another aspect of the problem. Some managers have such a wide span of managerial responsibility that they cannot possibly keep track of all their direct reports’ activities. Others have been placed in the dual role of managing some tasks while executing others, undercutting their focus and effectiveness in both realms.

To be proactive:

- A long-term plan for improved automation or outsourcing of back- or middle-office functions may offer solutions for investment managers who want to maintain a lean headcount while they grow. (That being said, automation isn’t a cure-all; we’ll have more to say on this topic in the chapter on Risk Area #5, “Naïve Reliance on Technology”).

Outsourcing with insufficient due diligence

A lack of experience in operations and IT can lead CEOs to assume that outsourcing will help them manage their risks as well as their operations. Indeed, there are many sound reasons to outsource, such as wanting to focus on core competencies, securing access to better technology or expertise, or taking advantage of labor and/or time arbitrage opportunities, to name a few.

Yet, without careful management of the process, outsourcing may actually increase a firm’s operational risk profile rather than reducing it. A perfect illustration of this point is the remarks made after the BP oil spill by then-CEO Tony Hayward: “This was not our drilling rig, it was not our equipment, it was not our people, our systems or our processes... We are taking our responsibility to deal with it very, very seriously.”

Key service providers such as accountants, custodians, prime brokers, fund administrators, software vendors and middle-office outsourcing providers introduce operational risk, but many investment management firms—even those that have been placed under the microscope by prospective clients—don’t seem to put concerted effort into the due diligence they perform themselves. Additionally, many investment managers pay scant attention to the risks introduced by hand-offs to or from these service providers (for more on that topic, see Risk Area #4, “Dropped Batons”). Effective risk management in this domain calls for more than simply hiring a big global custodial bank and/or moving to a multi-prime broker service model.

1NYSE Group Share and Dollar Volume in NYSE Listed, 2009.
To be proactive:

- Adhere to best practices in due diligence, which call for managers to issue RFPs, obtain financial statements, perform initial and ongoing annual on-site visits and read all the fine print (see Risk Area #9). SEI’s own experience indicates that proactive investment managers are substantially increasing the depth of their due diligence, asking for more visits and issuing more detailed questionnaires than ever before.

Rogue activity

No discussion of operational risk would be complete without a mention of rogue activity—that is, the conscious departure from sanctioned operating policies and procedures. To be clear, rogue activity is not always due to malign intent. While firms may worry about the rogue who is actively seeking ways to cheat or embezzle, the more common problem is employees who may sincerely want to do a good job, but take shortcuts or triage their responsibilities when they are overstretched. Often they push tasks aside with the intent of catching up later—for example, reviewing past reconciliations at some unspecified future date. Another type of rogue activity is the senior staff member who routinely ignores policies and procedures, a situation to which smaller firms may be especially prone.

To be proactive:

- Maintain an operational risk log that documents operational mishaps and near misses. Requiring violators to recount and present the issue may help educate them, if not shame them into compliance.
- Review and beef up mechanisms for enforcement of existing policies.
- Consider the need for tougher new policies, particularly if offenses are chronic. For example, employees who fail to file personal trading forms can be fined, or firms can withhold a portion of their pay until the problem is remediated.

When senior executives and managers lack a solid understanding of middle- and back-office workings, the repercussions can be far-reaching. At worst, they can spiral out of control. The first step toward wisdom is to recognize that we don’t know what we don’t know.
While we have already mentioned staff training as an essential tool for mitigating investment managers’ operational risk, the lack of adequate training and cross-training is so ubiquitous within operational departments that it deserves to be called out as an area of risk.

Avoiding Common Pitfalls

One facet of the issue is key-person risk, which is not limited to an organization’s senior staff, but can also be spotted in low-ranking yet vital positions. Other problems stem from poor organizational design, a lack of consideration for business continuity planning, and the notion that ad hoc on-the-job training constitutes a coherent program. Today, many firms are operating at historically low staffing levels, further increasing the importance of proper training and cross-training.

Highly specialized operational teams

Many firms build small teams to focus on a specific asset class, investment strategy, client or fund; some have dedicated teams for each large fund. This approach has obvious appeal: management can put their best people in a particularly challenging area, clients like having a team dedicated to their accounts or funds, and staff may be less distracted by other tasks.

Many investment managers create these specialized teams in an effort to lower their operational risk profiles; yet, ironically, all too often the result is more risk rather than less. A small, specialized team’s intellectual capital and institutional knowledge may be severely depleted by the loss of a single member, whether such absences are short-term (vacations), over a longer period (sabbatical or maternity leave) or permanent (leaving the firm or being promoted). Such brain drains may occur abruptly when an illness, family emergency or resignation is involved, leaving organizations scrambling to cope. Worse still, in keeping with Murphy’s Law, these unexpected gaps in staffing often seem to come at the worst possible times—e.g., during a period of peak transaction volume, while other key staff members are on holiday, or when a product or system launch is imminent—not only disrupting operations, but producing enough stress and chaos to discourage or drive away some of those who remain on the job.
A proliferation of processes and procedures
Because the specialized-team approach fosters isolation, it often leads teams to develop idiosyncratic processes and procedures rather than adapting a master set of workflows. We will delve into this issue more thoroughly in the chapter on workflows (Risk Area #6, “Playbooks”), but it should be kept in mind when considering how to organize support teams.

Failure to grasp the bigger picture
We touched on problems stemming from the lack of training for managers in chapter 2, “The Blind Leading the Blind.” The same kinds of issues are encountered at lower organizational levels where the work actually gets done. When consultants conduct operational reviews, they often find junior staff members who operate in a kind of bubble—that is, they cannot explain how their jobs fit into the functions of the department as a whole. Indeed, even among those who are adept at what they were hired to do, many cannot articulate what their firm actually does.

Without understanding how their individual roles fit into the larger organization, staff members cannot fully appreciate the urgency of information, the importance of accuracy, or how much even minor improvements would benefit the business. For example, every reconciliation clerk should understand the potential effect a position break could have on the investment team and the trading desk. Yet, all too often one side of the organization has no idea what happens on the other side. How many traders understand the downstream effects—and costs—of an erroneous trade ticket?

Lack of exposure to industry advances
Employees with a narrow view of their own workplace are unlikely to know how other organizations tackle operational challenges. This kind of tunnel vision is particularly common among firms where many staff members have been there for years and do not regularly attend conferences or make a point of networking with their peers. Such organizations often stick with processes and procedures that might once have been leading-edge, but have fallen behind industry practice and technological change. No firm or department can be sure it has the best approach without considering solutions that other organizations have devised. Firms that encourage lifelong learning may have a lasting competitive advantage because their employees are engaged and their solutions are up-to-date.

“Soloists” with exclusive ownership of functions or relationships
Soloists are employees who perform functions that no one else knows how to do—or, perhaps, wants to do. In some cases, no one else has sufficient access rights to systems to perform a function. There is no doubt that security master maintenance can be tedious and the list of people with access to payroll should be limited. A soloist may also be someone who views client relationships as personal property. Some relationship managers (RMs) seem to lose sight of the fact that client relationships belong to the firm, not to RMs. Feeling that their contacts are just that—their contacts—such RMs may never get around to updating client relationship management (CRM) systems. Too often, supervisors fail to step in for fear of rocking the boat or undercutting results. Such problems are not limited to small organizations, however. Many large sales or client service teams harbor soloists who overtly balk at letting anyone else perform tasks or service relationships they claim as their own. The point is that even well trained, high-performing soloists may stand in the way of firm-wide efforts to mitigate operational risks through cross-training.
To be proactive:

Identifying training and cross-training challenges generally is not difficult. Start by looking at your organizational chart to identify small teams. (Ideally, teams should never be smaller than three fully cross-trained people.) The good news is that effective training can be accomplished in a variety of ways, but also can be designed to address multiple problems. Among possible measures:

- A well conceived set of do-it-yourself training measures can be effective. Quiz staff on what they should have read in the firm’s compliance manual or code of ethics. Review system access capabilities. Spot-check CRM updates. Ask people to describe what they do—and really listen to their answers.

- A series of internal “lunch-and-learn” sessions can be an effective approach to cross-training; more often than not the participants also discover opportunities for operational improvements. Those staff members who lead training sessions also stand to benefit from the experience.

- A professional credentialing program in investment operations does not yet exist, but the Certificate in Investment Performance Measurement (CIPM®) offered by CFA Institute ensures that performance practitioners have the requisite skills in their specialized fields. Many classes and short courses, both live and online, are available across a wide range of topics.

- Customized on-site training is also an option. This can be provided by internal experts and/or external specialists who can tailor training to the firm’s methods and requirements.

- Job rotation, job shadowing and job swaps can help ensure that cross-training takes place, especially if these measures are accompanied by presentations on the system’s architecture and workflows.

- Ask teams to document or review their workflows as a group and share each team’s workflows with other teams.

- Attending webinars, industry conferences and networking events can be helpful to many employees, particularly those who are knowledgeable in their jobs but would benefit from more exposure to other organizations.

- Ensure that all clients are assigned a primary and a back-up RM, and that both are in regular contact with them.

Murphy’s Law frequently comes into play and exposes poor organizational design when firms can least deal with it. Identify training and cross-training challenges when they aren’t needed so that you can start mitigating operational risk in the calm before the storm, not in the eye of the hurricane.
Competitive runners know that in a 4x100 meter relay, significant time, or even the race itself, can be lost if someone bobbles or, worse still, drops the baton while it is passed from one sprinter to the next. Investment managers face similar risks when passing information between the people, departments, organizations and systems involved in complex sequential activities. Hand-offs are fraught with communication and timing challenges. Luckily, some simple tools can go a long way toward remedying the problem.

**Avoiding Common Pitfalls**

**Failing to identify where hand-offs occur**
A great way to think about hand-offs is to revisit the old practice of using paper trade tickets (a method that is still in use by some firms, and can be workable for firms with limited transaction volumes). Tickets could get lost because someone mislaid them, a data entry clerk forgot to input them, or they simply fell behind a file cabinet. In firms using industry best practices, the number of tickets written in the course of a day would be compared with the number of trades entered into the firm’s investment accounting system. If the totals didn’t match, an inquiry would be initiated. This approach wasn’t fail-safe—if one ticket was missing and another trade had been entered twice, then the counts would appear to be correct—but it did help reduce problems. Duplicate trade entries could be avoided by marking tickets as they were entered into the system, and the lost-behind-the-file-cabinet problem could be ameliorated by keeping tickets in designated wire baskets.

These days, of course, investment managers operate with less paper, fewer wire baskets, and more automation. But firms today also have far higher transaction volumes and, typically, more moving parts to their processes, both within the firm and in dealings with trading partners, custodians, prime brokers, administrators, middle-office outsourcing providers, exchanges and settlement facilities. While every information hand-off creates the possibility for error, many firms have failed to systematically map where these interchanges occur.

**Poorly designed or documented system interfaces**
Hand-offs from one electronic system to another are common trouble spots. The problem may stem from poor planning or insufficient foresight in the original system design (e.g., built for equities but not fixed income because “we’ll never need that”). Systems may also be poorly written, inadequately supported by vendors, or insufficiently documented (if documented at all). Firms also run into problems when one system gets upgraded and another one doesn’t, or when a legacy system has been in place for so long that no one still in the firm’s employment knows exactly how they function.
Timing can also be a challenge. In many instances, information is only sent from one application to another on a nightly batch basis. Yet as settlement cycles shorten, such a batch-based approach may not be sufficiently frequent for communicating critical information between systems. Other timing challenges arise when interfaces fail to consider the impacts of backdated activity. Global investment managers are often plagued with timing issues because there is never an end to the day. Information must be handed off seamlessly from one office—and application—to another in an endless cycle, leaving no time for the traditional “overnight cycle.”

Many interfaces suffer from more than one of these problems, and operational risk increases geometrically as more interfaces are involved. Indeed, the inadequacy of system interfaces is often a key driver in the decision to consider outsourcing. Many investment management firms choose outsourcing because it is more cost-effective and less complex than addressing all the known and unknown issues with their internal systems.

To be proactive:

› Develop a thorough system diagram that includes every application in use and identifies the interfaces between them.

› Diagram workflow to determine where hand-offs occur. A “swim-lane” diagram that depicts each system in its own lane can be particularly helpful in identifying where information hand-offs occur. Such a diagram can also capture hand-offs between people and systems (again, think of entering data from paper tickets), as well as those between teams or departments, between one firm and another (such as receiving execution details from a counterparty and sending back trade allocation information), between two or more systems, and between the investment manager and its clients (such as client reports or subscription and redemption activity).
Examine each identified hand-off in detail. Once an exchange has been captured, consider how often the hand-off occurs, the kind of information transferred, the timing around the hand-off, and what might go wrong with it. We find it helpful to look at available metrics, procedural documentation, data requirements, and error logs to evaluate the scope, nature and repercussions of potential operational mishaps.

Develop a comprehensive inventory of trouble spots. For example, if we again think in terms of the old paper-ticket systems, a ticket could be lost or entered twice. It might be illegible, or contain bad information in one or more fields, or have been submitted after the data entry team has gone home for the night. It is also possible that the security—or the counterparty, the currency, or even the portfolio—has not yet been set up, or set up incorrectly, in the investment accounting system. With an inventory of what might go wrong, firms can assess each one, estimating the likelihood that problems will occur and the damage they might cause.

Build workflows, processes and escalation protocols to mitigate the risks. In some cases, a quick fix may be sufficient to solve the issue. If, for example, a security or currency has not been properly set up, some firms may be able to fix that on the spot. In other organizations, however, the problem and its solution may not be so simple. For example, if trade entry clerks are not authorized or trained in new security or counterparty set-up, a further hand-off is required between trade entry and the security/counterparty maintenance group. This new hand-off needs its own examination of risks and how to mitigate them.

Examine hand-offs to and from outsourcing providers, and expect that those providers have done the same thing. Firms such as SEI use automated workflow tools where possible to ensure better tracking, increased consistency, and faster exception processing. Where appropriate, each hand-off should be covered by a service-level agreement with deadlines, quality expectations and metrics that provide benchmarks for evaluating the performance of both the provider and the investment manager.

Don’t forget to consider information provided by clients. Even the most sophisticated institutional clients sometimes fail to notify managers of contributions or withdrawals in separate accounts, for example. Such failures create needless reconciliation work for harried operations staff and can lead to distorted or misattributed returns. A portfolio manager is more likely to forgive the client than the operations group when his/her performance is affected because the client neglected to inform the firm of a cash flow.

Once investment managers have a complete inventory of where their operational processes might go wrong, they can take systematic steps to reduce or eliminate their risks.
Let’s be clear from the start: automation is a powerful tool for mitigating operational risk. Properly selected, programmed and managed, computers can perform repetitive tasks with accuracy and lightning speed. They never grow bored or inattentive. And they’re willing to work 24/7 without once stopping for a break. Yet computers also have the capacity to spew out mistakes at superhuman speed.

Moreover, computers are fundamentally obtuse. They will do only what we tell them to do, and then, like a surly adolescent, they will do exactly what we say. They won’t demonstrate initiative; for example, computers will not perform a reasonability check unless we specifically instruct them to do so and define “reasonable” in unambiguous, syntactically correct terms.

A case in point: In June 2010, Deutsche Bank’s algorithmic trading system acted on bad pricing inputs by placing 7,468 orders to sell Nikkei 225 futures contracts on the Osaka Stock Exchange. The total value was more than $182 billion. Any trader would have questioned the size of the transaction, but the system’s developers hadn’t taught the system to make such evaluations, and approximately $546 million of the orders were executed before the error was caught. Ultimately the bank was reprimanded by the exchange, shut down the proprietary trading unit in question and received a great deal of unfavorable publicity.

Firms that want to reduce their exposure to operational risks must recognize that automation is a double-edged sword. While helping to reduce many risks, it may also pose a host of new ones.

Avoiding Common Pitfalls

**Insufficient knowledge of the manual tasks being automated**

The U.S. Army Rangers would never be allowed to use GPS systems to navigate in the field without knowing how to use a compass. Yet in our industry, automation has taken over some activities to the point that few people remember how to do them manually, if they ever knew.

Is it any wonder that the finer points of accrued interest calculations may be elusive to a younger generation accustomed to using calculators for every computation? Can we really expect them to determine whether a fixed-income system is applying the correct day-count convention to U.S. corporate bonds (generally 30/360) as opposed to U.S. Treasury bonds (actual/actual)?
To be proactive:

› Make sure that automation project teams include staff members who thoroughly understand how to manually perform the activities being automated. Without bringing such fundamental understanding to bear, it is impossible to consider the necessary steps in a process—or those that might not be necessary in an automated environment—and to make certain that vital, consequential functions are not skipped, missed or ignored. Staff who know how something is done will also know how mistakes are made and whether results generated by an application are correct.

Poorly designed, implemented or documented technology solutions

Problems may arise for a variety of reasons, including:

› Using a system for portfolios and instruments it wasn’t built to handle. For instance, an investment manager may be trying to support a handful of multi-currency portfolios using a single-currency investment accounting system, or trading fixed-income securities on a system originally designed only to handle equities. In other cases, the manager may be relying on spreadsheets or databases in lieu of an application that has been tested and locked down to protect against ad hoc changes.

› Poorly designed interfaces between two systems (see chapter 4, “Dropped Batons”). Interfaces are particularly suspect if they were originally built in a phased implementation process—for example, one that was initially implemented to support equities only and then extended to support fixed-income and derivatives instruments. Too often, the early project phases were poorly documented and subsequent phases are delayed, leaving IT and operations departments unsure how an interface will perform when confronted with a new set of inputs. (We know the interface works with common stocks; will it cope with preferreds?)

› Shoe-horning information and transactions into earlier system designs or makeshift applications developed into “skunkworks” projects. This leaves investment management firms even more exposed to the risks in chapter 3 (“Novices, Soloists and Apprentices”). Anyone who has ever tried to decipher the inner workings of someone else’s spreadsheet knows how challenging that can be, even when dealing with a standalone spreadsheet, let alone one linked to scores of other spreadsheets. Likewise, if multi-currency portfolios are managed on a single-currency platform, figuring out the workarounds created to record foreign exchange transactions and to reflect that information in client reports can be maddeningly complex. Some database applications are notorious for their lack of documentation.

› Inadequate audit trails. This problem is often encountered with older vendor systems as well as with many of the less robust newer applications. It is ubiquitous among electronic spreadsheets and relational databases created without corporate oversight by business units that cannot wait for IT resources to become available. However, it may prove important to know who changed a price or cancelled a trade or set up a security, on what date, and at what time of day. A reliable audit trail will not only help during regulatory exams but will also assist in unwinding errors, designing process controls and identifying additional training needs.

› Neglected or out-of-date systems access controls. Many well-designed buy-side applications allow an investment manager to control access at the function level. For example, traders could be authorized to enter trades but prohibited from setting up securities, and portfolio managers might be able to view information and run reports but not change any data. Some firms neglect to implement these built-in system controls; others establish the controls but fail to update them as workflows are altered, systems capabilities are upgraded and people change jobs. Jérôme Kerviel’s €4.9 billion fraud at Société Générale was facilitated, in part, by a failure to keep systems access privileges up-to-date.
To be proactive:

› **Develop detailed written specifications as a guide for any system or software development project.**
  These specifications should be developed with thorough input and reviewed by staff members who understand the operational context for the functions being automated.

› **Diagram systems and workflows to identify all systems in use, including spreadsheets and proprietary databases.** Properly executed, this step will not only make it much easier to identify key interfaces and system access rights, it will also help bring potential audit trail issues to light.

› **Whenever a new system is implemented, review all workflows around that application for possible re-engineering.** The same holds true when a new third-party service provider such as an administrator, prime broker or middle-office outsourcing provider is engaged. While ideally, some activities will be eliminated thanks to automation or outsourcing, new activities may be required to oversee processing and ensure data accuracy.

### Inadequate testing of new systems and software

Failing to thoroughly test systems, including upgrades, reports and, for that matter, workflows, is another source of unforeseen risks. Insufficient testing often results from a sketchy understanding of the functions being automated. If staff members do not know how to perform a task manually, how can they properly test any automation? Another underlying cause is a lack of clear functional specifications for system development. Organizations may be tempted to shortcut this step by basing software development on informal user requests, rather than fully documented functional specifications.

And, of course, many end users are simply unaware of the critical need for regression testing—unaware, that is, until an upgrade unexpectedly “breaks” another component of the application. Unfortunately, however, many are too easily lulled back into complacency, especially in the face of mounting deadlines and too few resources.

To be proactive:

› **Refer back to written system specifications.** Testing new software is obviously more difficult when there is a lack of clarity on precisely what it should do.

› **Make sure that new systems and features are evaluated and tested by staff who understand the manual processes being automated.** Those who know how something is done will be better equipped to know how mistakes can be made, and to assess whether the application is producing correct results.

### Allowing potentially disruptive ad hoc changes

Investment managers have invested significant time and money to implement pre-trade compliance systems intended to flag or block transactions which, if executed, would result in breaching an account’s investment guidelines. Yet, we see the same firms enabling traders to set up skeleton securities on the fly. If the firm were purchasing, say, Exxon Mobil for the first time, the trader could set up a common stock skeleton security with the security name, ticker and currency so that trading can proceed apace, leaving other details (e.g., Exxon Mobil’s primary exchange, indicated annual dividend or sector and industry classifications) to be filled in later by someone else. While this procedure certainly accelerates the trading process, the investment management firm has impaired its state-of-the-art pre-trade compliance system. How can the system evaluate the percentage held in energy stocks if it does not know that Exxon Mobil should be classified within energy?
To be proactive:

› *Think through workflows and system access controls to prevent expedient, but potentially troublesome changes.* Periodic team-wide, and even cross-team, reviews of workflows and access controls often highlight the “downstream” effect that some changes can have. Likewise, review system access when people join and leave individual teams and not just the firm. All system access should additionally be reviewed on a regular and periodic basis.

**Failure to implement and test system updates in a timely manner**

Investment managers may engage teams of consultants to assist with a new system implementation, but give relatively little thought to the resources needed later for installing and testing new system releases (let alone the changes to workflows, interfaces and business continuity plans that such upgrades should trigger). Ignoring software updates is perilous: new releases may contain critical bug fixes and vendor contracts often limit support to recent releases. Some managers implement new software releases but curtail or skip testing due to the press of time, thus taking on risks that would make their clients shudder.

To be proactive:

› *Develop, and adhere to, work processes and timelines for maintaining and updating your firm’s systems infrastructure, however costly and time-consuming those activities may be.* In some cases, outsourcing might be an attractive alternative since it can limit that number of applications for which the investment manager is directly responsible for maintaining, updating and testing new releases.

**Relying on consultants whose knowledge is too narrow or too general**

Knowledgeable consultants can help dramatically mitigate operational risk by conducting well-directed operational reviews, evaluating systems or outsourcing vendors, and guiding technology selection and implementation projects. But consultants are no panacea; they may even inflate operational risk if they don’t have the specialized knowledge an assignment requires.

To be proactive:

› *Make sure that consultants understand the investment management business, not just financial services in general.* The buy-side does do things differently. This advice is especially important when it comes to implementation projects, which often involve vendor specialists. While vendor-supplied consultants do provide knowledge of the latest releases and bug fixes, as well as priority access to the vendor’s support team in the event an issue arises, those who lack solid experience with buy-side firms may be unaware of best-practice workflows or the upstream and downstream impacts of key activities or errors.
When staffing technology evaluation/selection projects, make sure that any consultant being considered is independent or has fully disclosed any compensation arrangements with vendors.

When it comes to a large-scale system or outsourcing implementation, more than one kind of expertise may be necessary. It is often advisable to engage specialized consultants as well as the vendor consultants to ensure your firm’s priorities and objectives are kept in sharp focus.

If you don’t want to be working with consultants indefinitely, confirm that they have a plan for transferring their knowledge to your staff during the project.

Competitive rather than cooperative relationships
Over the years, the balance of power between operations and IT departments has shifted in many investment firms. In the past, IT departments commonly dictated which systems would be used to support operations. More recently the pendulum has swung back in favor of operations calling the shots. But it is impossible to build or maintain an effective environment for operational risk management if the departments involved see each other as competitors rather than partners. Similarly, risk management is compromised if investment managers and third-party service providers operate in a siloed fashion.

To be proactive:

Manage project plans and communications with an eye to developing well-aligned, collaborative working relationships. We believe strongly that IT and operations staff must work hand-in-glove to create a smoothly operating, risk-managed infrastructure. That means that IT needs to support operations rather than mandate solutions; at the same time, operations must be sensitive to IT’s perspective on the costs and requirements of some potential solutions.

Likewise, outsourcing works best when investment managers and their third-party service providers establish strong lines of communication with some degree of give and take. At SEI, we encourage an open exchange of ideas and information on a scheduled and ad hoc basis, from strategic planning to day-to-day operational activity. In our observation, those clients who treat their relationship with us as a true partnership are the ones who realize the most value from it.

In sum, firms that want to reduce their operational risks need to factor that goal into every aspect of their ongoing automation effort.
Documenting processes and procedures is such a fundamental and obvious requirement for effective operations management that one might question the need to call it out. Yet, non-existent, obsolete or incomplete documentation is implicated in so many operational snafus that it deserves to be singled out as a risk area in its own right.

An operations department without workflows is like a traveler without a set of maps or a community without a zoning plan. Even if your firm’s documentation is useful, comprehensive, up-to-date and readily accessible in an emergency, you may still find the topic worth revisiting. If, on the other hand, the state of your documentation is less than adequate or even worrisome, you may wish to use this chapter as the basis for dialogue and planning within your firm or department.

Not only will well-documented workflows help you avoid mistakes and miscommunication, they make it much easier to train new employees. Reviewing workflows is a perfect way for new hires to occupy themselves during idle periods when no one is available to train them. As an added benefit, you will get helpful feedback on the clarity and effectiveness of your documentation.

Avoiding Common Pitfalls

**A total lack of formal workflows**

Extreme as this may be, having no formal set of workflows is unfortunately the case at some organizations, especially but not only, at emerging firms. In such situations, teams are managed on what might be called the “whack-a-mole model,” with predictable consequences for the quality of work life. When the entire firm lacks a playbook, the resulting chaos often resembles a game of soccer as played by a team of unruly six-year-olds who race after the ball with little concern for their assigned positions or even the goalposts. (Some parents call this “swarm ball.”)

Without established workflows, it is impossible to ensure that operational controls are in place, staff are performing all necessary tasks, and all systems involved—especially mission-critical spreadsheets—have been identified. When there is a total absence of workflow diagrams or documentation, operational due-diligence reviews may be over before they have even started.
To be proactive:

➢ *Develop a plan and timeline for developing and documenting workflows.* Don’t try to tackle every process at once, or you will be overwhelmed. Start with the simplest and most basic functions, and build from there. The swim-lane and system diagrams discussed in chapter 4 (“Dropped Batons”) can be invaluable in this effort.

As you embark on any documentation project, remember that workflows necessarily go hand-in-hand with policies and procedures. In fact, it’s impossible to properly develop and document workflows and controls without a thorough knowledge of the policies and procedures in place. Make sure to consider all potentially relevant items—from compliance policies and expense report procedures to information security policies, escalation procedures and business continuity plans.

**Workflows that are out of date**

Firms should revisit their workflows with the occurrence of any meaningful change—e.g., reorganizations, systems implementations, product launches, new reporting requirements, changes to system access levels and new instrument types. Yet many operational teams seem to lack the time, expertise, or motivation to do so.

To be proactive:

➢ *Establish and enforce a regular schedule for reviewing and updating workflows.* Even when firms are well-established and relatively unchanging, managers should take a fresh look at their workflows at least annually.

**Documentation that is either too vague or too detailed**

Neither type is as useful as it should be. Overly vague documentation leaves staff members to flounder in a crisis. On the other hand, excessively detailed documentation generally has such a short shelf life that the material loses its value by the time it is critically needed. While those with disciplined, analytical minds may insist on exhaustive, step-by-step documentation, complete with screen shots and keystrokes for every task, oftentimes such perfectionism is rarely worth the considerable effort and expense it entails to create and maintain.

To be proactive:

➢ *Get feedback from managers and employees to help identify the right level of detail.* The appropriate level of documentation is a matter of individual judgment, taking into account the firm’s and the department’s operational risk appetite, training requirements, and overall preparedness for disaster recovery. Firms can often achieve a good balance by developing reasonably informative, but not exhaustive, documentation and supplementing it with extensive cross-training.
No escalation procedures
Escalation procedures are worthy of special mention. When things go wrong, as they sometimes will, it is important to have established the criteria and protocols for elevating an issue to a higher level of management. Heads of operations, for example, needn’t be informed about every individual reconciliation break or failed trade as it occurs. (They do need to see error logs on a regular basis.) If managers in larger firms were notified of every single issue, they would be so inundated by small, manageable items that they would be unable to identify whether a major problem is lurking in their inboxes.

To be proactive:
- **Define which incidents should go up the chain of command, and when.** The most effective escalation procedures use both size/impact and time as decision criteria. For example, a small failed sell transaction may not initially merit escalation due to its inconsequential size, but it should get escalated well before the counterparty issues a buy-in notice. On the other hand, a similar trade that is very large might be escalated immediately based on its size alone, especially if it is material in relation to the overall portfolio.

Staff that ignore or are unaware of documented workflows
Regardless of the state of a firm’s documentation, workflows do no good if staff do not follow whatever workflows, policies and procedures have been memorialized.

To be proactive:
- **Take steps to ensure that staff have not only received copies of workflows, and have them at hand, but have also actually read and understood them.** Confirming receipt is only the first step. Managers should also consider having periodic meetings to review and explain policies, procedures and workflows. (Note that this applies to all the policies, procedures and workflows across the firm, not just those that are compliance-related.) When it comes to determining whether workflows are actually followed, job swapping, operational reviews and audits can help.

Multiple undocumented variations on the same basic workflow
This problem often occurs when firms develop small teams that are specialized by product, instrument type, investment strategy or client. Often these small teams will start out with a single set of workflows used by similar teams across the organization, but then they customize their processes and procedures over time, perhaps without documenting these refinements. The result may be a firm with multiple sets of workflows for the same basic function, such as trade settlement or reconciliation. When encountered and questioned about such situations, teams may protest, “but we’re different!” It’s true that one size doesn’t fit all, but if a firm’s workflows can only handle one product or one client or one strategy, then it is time for them to re-think their processes.
To be proactive:

- **Consolidate and focus workflows as much as possible.** As an analogy, consider the simple workflows for pouring and serving coffee. Whether we have one team or four, we’re dealing with four workflows: black, with sugar only, with milk only or with milk and sugar. However, even if we organize four teams to serve coffee, they can all follow one central workflow with optional steps depending on customers’ stated preferences.

  This approach makes sense for several reasons. First, only one set of workflows has to be maintained. Secondly, all staff will be familiar with the overall workflow, even if their team performs some of the optional steps and not others (e.g., adding sugar but not milk). Finally, a single workflow with options is easier to review, update, and explain during audits and operational due diligence meetings.

  Ideally, workflows define a single, logical set of activities in manageable pieces. In our example of serving coffee, the workflow would intentionally exclude the steps required to make the coffee, secure the ingredients or select a cup. Likewise, it leaves off before covering coffee consumption or cleanup activities. By documenting in bite-sized chunks, investment managers get immediate benefit from each function that is documented. When managers start a new documentation effort by focusing on relatively simple functions, they can build on the resulting feedback and experience as they add more complex functions later in the process. For example, a trade settlement workflow might be updated to consider trade cancellations, trade corrections or situations when trades are first posted after trade date (or worse still, after settlement date).

  Individual workflows can then be linked to other workflows to cover longer, more intricate processes. In addition, users can coordinate with outside service providers to ensure hand-off scenarios are adequately covered.

Workflows that are inaccessible when needed most

In a sudden evacuation, you may not have time to collect those reassuringly substantial three-ring binders from your office bookshelf and take them to an offsite location. Likewise, when systems are down and internet access is unavailable, having access to hard copies may be critical.

To be proactive:

- **Make sure that updated workflows are available both online and in hard copy.** During a business continuity or disaster recovery event, investment managers often must call upon staff to discharge functions they are unaccustomed to performing on a daily basis. It is in exactly these situations that clear, concise, well-documented workflows can be a life-saver.

A lack of time, insufficient expertise and an undersupply of motivation are all reasons why workflow documentation is so often pushed to the back burner. But investing the effort it takes to do the job will pay off in expedited and consistent training, more effective controls, improved efficiency and a lower rate of errors every single business day.
Given the number of moving parts in the investment process, it’s no surprise that the roles and responsibilities of those involved are not always appropriately delineated. The issue goes beyond opening the door to fraud and embezzlement. The failure to clearly and properly assign duties can create conflicts of interest, throw up barriers to accountability, and complicate matters of compliance and administration.

Such problems afflict traditional and alternative managers alike, as well as some of their key service providers. Moreover, these problems have become more common since the financial crisis and the ensuing downsizing of operational and IT staff across the industry. Reductions in the workforce leave fewer people in place to handle the same workload initially and, as the market continues to recover, a growing volume of portfolios and transactions. Not only does this mean that operational staff may become chronically overextended and more prone to errors, it leads to situations where employees must wear multiple hats, sometimes stretching or crossing the boundaries of good segregation controls. It is not uncommon for firms that once had appropriate controls in place to no longer be able to support those controls after a workforce reduction. Clearly smaller firms, especially start-ups, are challenged from the outset by having a relatively small number of employees available to handle multiple functions.

Avoiding Common Pitfalls

Confusing assets of funds with the assets of firms
This issue is a particular concern to firms managing pooled vehicles, including traditional firms that manage mutual funds and alternative firms that manage hedge funds, private equity funds or funds of hedge funds. It often involves recordkeeping staff, but may affect others as well.

Consider the hypothetical example of Opaque Asset Management (OAM), which manages the Opaque Fund. For purposes of this discussion, the type of fund and strategy are irrelevant. What is important is that the Opaque Fund is a client of Opaque Asset Management—perhaps even its largest client—and is distinct from the firm. That point, while critically important, may escape staff at all organizational levels; they may either forget the distinction between manager and fund or never grasp it in the first place. Indeed, many clients and due diligence firms also fail to pick up on the distinction when reviewing fund procedures. The common practice of giving funds names similar to those of their managing firms only increases the confusion.
If you are tempted to think that muddling firms and funds doesn’t really matter, let’s consider some of the issues that can arise in practice—for example, who should be approving wire transfers? Clearly, best practice calls for having two approvals before a transfer is released. But who should those approving parties be? In many organizations, portfolio managers believe that they should approve all wires. But because portfolio managers actually oversee the fund’s trading activities, proper segregation of duties would generally dictate that they should have no control over the movement of fund (i.e., client) assets. The exception might be those cases where portfolio managers are principals of the investment management firm and feel strongly they should approve wire transfers for the firm’s money (e.g., payroll, taxes or other major firm expenses).

To be proactive:

› **Consider an operational review to identify potential issues and remedial actions.** Outsourcing may be a remedy to explore, particularly in cases where firm resources are stretched or segregation of duties is inadequate.

› **Be clear on where the lines between functional activities should be drawn.** For instance, recalling the notorious examples of Nick Leeson at Barings Bank and Jérôme Kerviel at Société Générale, under no circumstances should portfolio managers or traders price their own portfolios; nor should they be involved in trade settlement or reconciliation. Likewise, trade support staff should not perform the duties of reconciliation staff and vice-versa. And performance measurement teams—at least, those responsible for generating performance data used in marketing and possibly in incentive compensation calculations—should not report to the investment team or the sales/marketing area.

› **Manage information flows to minimize the potential for manipulation of data.** Trade confirmations are sometimes sent by counterparties to the trading desk which, in turn, passes the confirmations on to investment operations. This sets up a situation in which a rogue trader could alter a confirmation. A better approach is to have counterparty confirmations sent directly “to investment operations. Traders may certainly be copied on confirmations, if desired, but they should not serve as the primary conduit or as an intermediary in the delivery process.

› **Make sure clients are in control when their assets are moved.** The question of who should have the authority to wire money has a simple answer: that authority always rests with the client (or the fund). For separate accounts, best practice dictates that the investment manager should never be given authority to wire funds. Indeed, when the manager has such authority, it is considered constructive custody, which needs to be disclosed on the investment manager’s Form ADV.

In the case of funds, where the investment manager wears two hats, this responsibility should be assigned with special care. The authority to transfer funds should not rest with the investment team or anyone involved in reconciliation. Ideally, wire transfers are handled by a combination of an internal operations team and the external fund administrator. In all cases, a wire transfer should be approved by at least two people. Moreover, checks should be put in place to ensure that the amounts drawn and accounts involved are correct. Limiting the specific accounts to which funds can be wired is a sound practice (and, of course, a different group should manage that set-up). For example, individual staff at the investment manager might only be authorized to wire from the custodian to the administrator while the administrator’s staff might only be able to wire from the administrator accounts to either investors or to the custodian—and then based only on written instructions from the investment manager’s operations team.
One last caution concerns network authentication system security tokens, those little devices that banks or prime brokers provide to issue updated codes for initiating wires or authenticating users. Don’t leave them in a desk drawer! First, they could easily be found and are subject to misuse by someone else. Second, if they’re in your drawer, they won’t be very helpful in the event you need to invoke your business continuity plan. Inconvenient as it may be, put them on your keychain so they will be with you at all times.

Failing to separate fund records from those of the firm

This problem involves custodians, prime brokers, fund administrators and auditors. Every fund will have one or more agents that serve as the fund’s custodian(s) for the safekeeping of assets. (Hedge funds generally utilize prime brokers who function not only as asset safekeepers/custodians, but also as execution counterparties and lenders.) Likewise, the fund will have an auditor, as well as a fund accountant or fund administrator, the latter of which is increasingly an independent third-party service provider such as SEI.

The custodian, auditor and fund administrator are hired by the fund—not by the investment management firm. Moreover, the books and records maintained by these parties are those of the fund (read: client), not the investment management firm. So what happens when the regulators walk in for a periodic examination of the firm? Should Opaque Asset Management (OAM) rely on client records? The answer is clearly ‘no.’

The management of separate accounts brings the books-and-records issue into sharper relief, in that separate account clients do not require a fund administrator. Thus, the only book of record would be that of the custodian or prime broker as the safekeeper of assets. Once again, it is problematic if OAM, the investment management firm, is subject to a regulatory exam and can rely only upon the books and records produced by agents of its separate account clients.

True, failure to maintain separate firm and fund records certainly streamlines operations because everyone refers to a single record. On the other hand, with that approach, the term “STP” can take on new meaning—not “straight-through-processing,” but “straight-through-problems.” If, for example, a manager downloads trade confirmations and uploads them to the manager’s investment accounting system, rather than inputting transactions manually or loading them from the manager’s trading system, there is no way to catch mistakes should the counterparty’s confirmation be incorrect—an all too common occurrence.

To be proactive:

Consider some level of shadow portfolio accounting. Investment management firms that practice shadow accounting maintain their own independent sets of books and records (generally through the use of an investment or portfolio accounting system). The intent is to enable managers to spot mistakes or improprieties by periodically reconciling their records with those of safekeepers and fund administrators.

Shadow portfolio accounting is commonly used in the traditional investment arena. And with many hedge funds, especially those with Level 3, hard-to-value or illiquid assets, it is often considered to be a necessary double-check, rather than a luxury. Still, it is the subject of some debate, especially within the alternative side of the industry. Some consider maintenance of manager records—as opposed to simply maintenance of fund records—to be best practice, yet the discussion is particularly critical in two scenarios: first, when the fund’s custodian also performs the middle-office portfolio accounting function for the investment manager; and second, when the fund relies on one or more prime brokers for trade instructions, eschewing a robust, independent trade matching process.
When evaluating the need for shadow portfolio accounting, careful review of the sources of data for critical operational functions and recordkeeping is of paramount importance. While fund accounting calculations can leverage middle-office portfolio accounting data, to do so properly, care must be taken to ensure portfolio accounting information is appropriately sourced. For example, all trading information should be fed to the portfolio accounting application directly from the investment manager’s order management system or paper tickets and not from broker confirmations or, worse still, feeds provided from the prime broker or custodian. This is even more important when the prime broker acts as the counterparty on the trade or the custodian also functions as the fund administrator and/or middle-office recordkeeper.

Some managers determine that, since responsibility ultimately rests with the investment management firm, they will duplicate 100% of what the administrator does. Said one European hedge fund manager quoted in Ernst & Young’s Coming of Age, its 2011 survey of the hedge fund industry, “We have to have our own records. We can’t rely on third parties. As a regulated firm, we have to have them and can’t outsource that to an administrator. But having an outside administrator is a form of back-up and insurance. We see it as our responsibility to have our own records.” In these instances, often managers will shadow portfolio accounting records to track what a given fund owns, but do not shadow partnership accounting records, which identify who owns the fund. And shadowing of portfolio accounting data has critical benefits when managers employ a multi-prime and/or multi-administrator model.

While the debate continues, SEI suggests that each investment manager should consider where on the spectrum of partial to complete shadow accounting they wish to be, given the firm’s specific situation. We further work with firms to carefully track information flows, however, to ensure that source data, such as trades, that feeds portfolio accounting systems is independent from source data supplying safekeeping systems employed by custodians and prime brokers. The investment manager should be the source for all trade information and we recommend that all investment managers match trades to counterparty confirms 100% of the time, regardless of whether the manager (or its third-party middle-office provider) serves as the affirming party.

On a final note, it’s important to remember that issues relating to segregation of duties are fluid and can crop up as a consequence of hiring or management decisions that seem relatively innocuous. In light of this, investment management clients and firms evaluating outsourcing providers should recognize that due diligence is not a one-time occurrence, but a critical point of control that should be repeated on a regularly scheduled basis.

Even when exhaustive RFP and due diligence processes are performed prior to engaging outsourcing providers, and on an ongoing basis, investment managers should ensure appropriate processes and procedures are in place for effective oversight of third-party providers. This might include identification of exception items for additional review and spot-checking information on a periodic basis, as well as design and review of summary reports with a particular focus on high-risk areas or new processing by the outsourcing partner. These high-level checks should be examined periodically to ensure they are appropriate and, if warranted, adjusted from time to time.
Everyone knows that keeping track of clients’ assets is a fundamental responsibility of investment managers. Everyone also knows that reconciliation—the process of comparing records, identifying and researching discrepancies and, importantly, seeing to it that material errors are corrected—is a critical step in satisfying this obligation. It’s as simple and obvious as locking the dead bolt on the front door at night.

Investment managers employ time-consuming, expensive reconciliation processes and systems to ensure that their books and records are accurate, and many readers may be thinking, “We’ve got it covered. We’re in good shape.” Yet there are considerations that may not be quite so apparent. Even in the best-managed firms, there may be reconciliation issues that leave managers more exposed to risks than they realize. In other words, they may be locking the front door... but are they also locking the one in back?

Avoiding Common Pitfalls

Less-than-comprehensive reconciliation procedures

At a minimum, we expect on the buy side to see reconciliation between the investment manager’s records (or, if investment operations are outsourced, the third-party provider’s investment accounting records) and the records of the safekeepers (e.g., the custodian or prime broker). But, depending on the investment vehicle and the structure of operations, this may not be sufficient to catch all mistakes and red-flag potential problems.

To be proactive:

＞Develop procedures that provide for a full set of checks. For commingled vehicles such as mutual funds and hedge funds, where a fund administrator is required, there should additionally be a reconciliation between the administrator’s records and those of the safekeeper. At SEI, we recommend what is commonly called a “three-way reconciliation,” but is more accurately described as three separate reconciliations: the investment manager’s records vs. the safekeeper’s; the safekeeper’s vs. the administrator’s; and the administrator’s vs. the manager’s.
Remember that performance analysts are not portfolio accountants. At firms that manage institutional money held in separate account portfolios, performance analysts are typically responsible for investigating out-of-tolerance variances between the rates of return calculated by the manager, the custodian and/or the client’s investment consultant. While this process may provide a final check on the accuracy of data inputs to the return calculations, this does not constitute a full reconciliation.

Assign reconciliation duties to appropriate staff. Trade support staff should not be in the reconciliation business, nor should portfolio managers or traders. In assigning these responsibilities, firms need to guard against the potential for fraudulent activity while also recognizing that it is generally difficult to catch one’s own typos.

Assuming the accuracy of electronic or consolidated records
A fundamental question is what really constitutes the safekeeper’s official records. While transaction files, for instance, are important sources of information, many safekeepers will not stand by these back-up reports or electronic representations of an account, considering the paper statement to be the only “official” record. Reconciliation risks crop up when reports other than “official” records are relied upon.

Another related, but thornier, problem occurs when hedge fund managers utilize multiple prime brokers to support a given fund, receive consolidated (or “hearsay”) reporting from one of those prime brokers showing assets across all the primes servicing the account. This approach has advantages for the hedge fund manager, in that the main prime broker shoulders all the operational complexity associated with a multi-prime model and provides aggregated reports to the manager. However, prime brokers are generally quite clear in stating that in these instances, they are not responsible for accuracy of the information they obtain electronically from other service providers.

To be proactive:

- Always obtain detailed, account-level statements and reports directly from the individual safekeepers. While consolidated reporting saves time and is certainly more convenient for managers, only by double-checking summary reports against the individual underlying safekeeper reports can a manager confirm that the assets actually exist and can properly reconcile accounts.

- Ensure final safekeeper records are obtained and stored. While the cost/benefit ratio for manual reconciliation of these statements may be unattractive, periodic sampling can pay significant benefits by identifying situations where the safekeeper’s final, official report can differ from data provided electronically.

Reconciliations that are too limited in scope
Too often, position reconciliations are limited to a review of the quantity held on each set of books. Such a procedure is neither complete nor effective.
To be proactive:

- **Reconciliations should examine the cost basis and market value of all positions in local currency terms.** Although tolerances are generally established on these items, we recommend zero tolerance on position quantity, along with a careful examination of fractional shares (especially for funds of hedge funds). In addition, when reconciling the quantity on mortgage-backed securities, we suggest reconciling the original face amount, particularly since securities trade on that basis.

Neglecting the security identifier for each position

There are few things worse than believing that you own class B shares, but discovering that you actually own class A shares, or vice versa.

To be proactive:

- **Only by comparing the security identifier can you be certain you are reviewing the same issue.** Where possible, compare the CUSIP for U.S. and Canadian issues and the SEDOL for non North American securities. (The acronym CUSIP comes from the Committee on Uniform Security Identification Procedures circa 1964; SEDOL stands for the London Stock Exchange Daily Official List.)

Many managers are unaware that an ISIN (International Securities Identifying Number) does not distinguish the market in which a given security was purchased and is held. While it is possible to purchase a security in one market and then sell it in another market, possibly receiving proceeds in a different currency, shareholders must take additional steps to convert the shares. So it is important to confirm the security’s market denomination. While a given issue will have the same ISIN across markets, the SEDOL number will establish the distinction.

Excluding local-currency cash balances

Even the most careful reconciliation of a portfolio’s holdings is incomplete without concurrently reconciling the portfolio’s cash positions (as opposed to transactions). A cash balance that does not reconcile is a potentially important sign of other trouble in the portfolio.

To be proactive:

- **Include local-currency cash balances in any position reconciliation.** If examining trade-date positions, then trade-date cash balances should be used; settlement-date balances should be validated only when reconciling settlement-date positions.

Lack of timeliness

An overly long time span between the “as of” date and the date of reconciliation is a common but critical problem area. Performing a reconciliation as of September 30 on October 1—and promptly taking appropriate action to correct errors—is far more effective than, say, performing that same September month-end reconciliation on October 25. If position breaks remain undiscovered in the interim, managers may be basing investment decisions and compliance monitoring upon incorrect portfolio weights. In addition, managers have increased risk of inadvertently selling short if they hold smaller positions than they suppose.
(Obviously, managers could also fail to sell or purchase as many shares as they intend if they hold larger positions than they think. But erroneously selling short is of particular concern because it exposes the portfolio and manager to unlimited potential losses.)

While reconciliation timeframes often are dictated by custodian/prime broker timetables for delivery of reports, automation of the process minimizes delays. If an investment manager’s reconciliations are consistently behind schedule, it signals the lack of adequate staffing, or insufficient automation, or both.

To be proactive:

➤ *Provide the staff and IT resources needed to ensure that reconciliations are conducted on a timely basis, if not daily.* Position reconciliation (including cash as a position) on a timely basis is most critical. The need for more costly daily reconciliation of transactions generally depends on several factors, including portfolio turnover, instruments traded and the normal level of cash available. Daily transaction reconciliations do have their drawbacks. Most obviously, they are expensive and time-consuming. Second, reconciliation teams often find themselves hunting down what we call “known ghosts” that will disappear of their own accord, such as dividends that the manager credits to cash on the pay date while the custodian or prime broker credits them one business day later. In this case, a reconciliation of sorts occurs when the manager matches 100% of trade tickets to counterparty confirmations. Although it is not the classic manager-to-safekeeper transaction reconciliation typically envisioned, confirmation matching coupled with careful oversight of external cash flows generally results in an excellent early-warning system for most portfolio activity (and is an approach that alerts managers far sooner than if they wait for the custodian to update systems).

To determine whether more formal daily transaction reconciliations are needed, managers should diligently review all position breaks to identify whether they resulted from errors on the part of a counterparty, a custodian/prime broker, or the managers themselves. If the manager’s records are correct most of the time, the need for daily transaction reconciliation diminishes.

Using the wrong statements for margin and collateral
Managers that trade derivative instruments, or have assets held as collateral or margin for some other reason, should ensure they are receiving statements from the party holding the margin or collateral—and that these statements are the ones used for reconciliation. Some managers assume they know who is in possession of collateral without actually hunting down statements. Yet in the event of a prime broker failure, a crucial step in claiming collateral that may have been hypothecated (i.e., pledged) and re-hypothecated is establishing ownership on the basis of accurate accounting records.

To be proactive:

➤ *Review and, if needed, revamp reconciliation workflows and systems to make sure that reconciliations are properly and fully accounting for margin and collateral.* The process should include review of statements showing that the agent has actually received collateral and that those assets are still in the agent’s possession.
Lack of management review
A common reconciliation gap is the absence of a management review confirming that each portfolio was reconciled. Yet such a check is imperative from both a management and regulatory point of view. Staff may have noted breaks, but failed to flag or escalate the issue. New accounts may have been established, but not assigned to a staff member. And there may be those times—rarely, one hopes—when reconciliation staff simply fail to do their jobs. When regulators come to visit, they will seek some sort of proof that a review has been conducted.

To be proactive:

- **Establish consistent reconciliation review procedures and documentation.** This can be as simple as having the manager who conducted the review initial and date a reconciliation “worksheet or checklist of accounts, specifying the date each account was reviewed. When investment managers outsource their middle offices to a third-party firm, that service provider should perform the management-level check of reconciliation. Nonetheless, at SEI we recommend that clients use a “belt-and-suspenders” approach, reviewing summary break reports daily (or, at a minimum, on a monthly basis). Our workflow system is designed to date- and time-stamp both our reviews and those of the investment manager. The system also records who performed the review and which documents were examined. (Regulators love it.)

Commissions also belong to the investment manager’s clients, as is spelled out in the CFA Institute Asset Manager Code of Professional Conduct. There are additional recordkeeping requirements when they are used under commission-sharing arrangements (CSAs) as “soft-dollar” payments for research or other products and services supporting the investment decision-making process. Managers who use multiple executing brokers and decision-support providers need to keep track of numerous cash flows to ensure that soft dollars are being paid as intended.

To be proactive:

- **Take steps to ensure that soft-dollar payments are properly made and recorded.** Soft-dollar payments are not normally included in a firm’s accounting-based reconciliation process but should nonetheless be periodically reviewed somewhere in the organization, for example, by the accounts payable team. Demonstrably sound recordkeeping practices are particularly important in jurisdictions, such as the U.S. and the U.K., where regulations specifically address potential conflicts of interest arising from CSAs. Industry best practices can be found in the CFA Institute Soft Dollar Standards.

As much as investment managers may feel that they devote ample resources to reconciliation processes and systems, hidden gaps and problems are all too common. In our view, it’s worth another look to make sure that all accounts are in fact reconciled and secure.
Why do operational disasters occur? Many are linked by a common thread: pressured by the sheer volume and complexity of work in a high-velocity business, investment managers and their attorneys don’t always take the time to get things right. They don’t always consider all the players involved in a series of transactions. They don’t always think through their own processes and controls. And they don’t always read all the fine print in key documents and agreements.

Yet we’re in an industry where minor oversights can have huge repercussions. A relatively little-known Midwestern investment manager fires up an algorithmic trading program, and markets around the world drop like a stone, inspiring the now well-known phrase, “flash crash.” A major bulge bracket investment bank collapses and more than 140,000 trades fail, leaving many hedge funds unable to find or retrieve their collateral. Mortgage lenders and servicers disregard the time-consuming legal niceties, property foreclosures grind to a halt, and as a result, bank stocks lose billions of dollars in value.

Most people who work in investment operations aren’t lawyers; we’re business people who are more or less expert in a specialized domain of systems and operations. But our lack of training in the law does not exempt us from reading and understanding legal documents—especially contracts—before we sign or approve them.

**Avoiding Common Pitfalls**

**Depending solely on attorneys for review of business documents**

Documents such as ISDA, prime brokerage, custodial and administrative agreements should not be left solely to the lawyers; nor should they allow us to shirk our responsibilities. Attorneys know securities law, but those of us on the business side know investment operations, technology and client behavior. It takes both groups—lawyers and business people alike—to properly review any agreement.

Significant business issues are often buried within legal documentation. For example, Bear Stearns used a standard Limited Liability Authority Certificate and Trading Authorization agreement for brokerage accounts. The last full paragraph on the first page laid out what the authorized signatories could do, including trading, receiving confirmations, entering into agreements, wiring funds and even deputizing others to be so authorized. Moreover, each signatory could individually and unilaterally take all these actions.
What’s wrong with that? Signing that document essentially would eliminate, as far as Bear Stearns was concerned, any segregation of duties that the manager might have established between trading and settling securities. There would be nothing in place with Bear Stearns to prevent the breach of a manager’s internal policy prohibiting a single individual from performing all the listed activities. Yet we have seen managers sign similar documents without blinking—and then reassure investors in due diligence meetings that proper segregation of duties was in place.

Both Nick Leeson and Jérôme Kerviel would have liked Bear Stearns’ standard agreement. While their own firms’ policies might have prohibited certain actions, the trading agreement allowed abundant opportunities for fraud while ensuring that Bear’s interests as counterparty and safekeeper were protected.

**Signing documents without a careful reading**

Senior managers who execute documents as authorized signatories often simply follow the “sign here” stickers, on the assumption that their subordinates have scrutinized the details or the agreement is the same as the last one they signed. Then the document is duly placed in a file cabinet, readily available in case the regulators ask to see it, without a careful review by the very people who are responsible for managing the operational risks the agreement may entail.

Of course, this bad habit is not limited to operational areas; many portfolio managers and financial analysts may similarly fail to read prospectuses assiduously before purchasing securities (although they likely do not fail to include them in their research files for the regulators’ benefit). Likewise, simply filing ISAE 3402 or SSAE 16 (formerly SAS 70) reports without having critically examined them, let alone learned from them, defeats the purpose.

This is how many firms found themselves in trouble during and after the Lehman Brothers bankruptcy, an event that gave new meaning to the phrase “collateral damage.” In some cases, rather than entering into an agreement with Lehman Brothers, Inc. (LBI), investment managers contracted with Lehman Brothers (International) Europe (LBIE), a U.K. limited liability company. This placed the assets of the investment managers and their clients outside the protections of U.S. bankruptcy courts. In other instances, clients of LBI signed agreements permitting assets to be transferred to LBIE in order to circumvent U.S. re-hypothecation limits. (For an examination of the often convoluted relationship between prime brokers and their clients, as well as a summary of the tortuous search for collateral after the Lehman Brothers failure, read J.S. Aikman’s 2010 book, *When Prime Brokers Fail: The Unheeded Risk to Hedge Funds, Banks, and the Financial Industry.*)

Similarly, during the Bear Stearns crisis many managers discovered that while they enjoyed the legal safeguards created through the use of Bear Stearns Securities Corp. (which insulated prime brokerage assets from a default by Bear Stearns & Co.), they had signed cash-sweep agreements that moved excess cash into accounts that ultimately made their fund a general creditor to Bear Stearns & Co. In many instances, portfolio managers had signed such standard sweep agreements without legal review.

Worse still, some investment managers have policies that permit operations staff to select sweep vehicles (and sign corresponding legal documents) without benefit of either legal or investment review, thus enabling operations staff to make investment decisions.

Although inadequate review of documents may leave the door open to fraud, calamities can and do arise in the absence of malign intent. The parties involved haven’t necessarily set out to obfuscate the terms or conceal the risks. But disasters may still occur, simply because too few qualified and knowledgeable people have read the fine print in agreements.
To be proactive:

- **Develop procedures that provide for a full set of checks.** Ensure that agreements are reviewed by both legal and operational departments. It is crucial that documents be examined from both a legal and a business perspective.

- **Scan contracts with key service providers and make them available to staff throughout the organization.** This is a simple step that can help firms raise awareness and share information concerning entities, contractual terms and obligations.

- **Use workflow tools to help ensure that documents are reviewed by appropriate individuals.** The concept of transparency isn’t limited simply to investors’ understanding their hedge fund and private equity holdings, but applies to communication within a manager’s firm as well.

- **Beyond identifying which legal entities are counterparties, be sure to know the regulators to which that entity is subject.** When assessing counterparty risk, firms should also continuously monitor counterparties’ net exposure as well as their creditworthiness.

Admittedly, poring over and deciphering byzantine legal documents is neither easy nor enjoyable. Ensuring adequate review takes state-of-the-art data management, know-how and time. But in a period when investors and regulators are focusing on operational controls and counterparty risks—not to mention calling for improved corporate governance—the burden lies with each of us, in our respective roles, to take responsibility for getting it right.
Neglecting to plan ahead is a fairly obvious source of business risk. So why do we mention it in our series on operational risk? Because organizations that fail to anticipate future conditions in the marketplace could suddenly find themselves out of business, stranding clients, dislocating employees and damaging shareholders. And because a lack of advance planning can throw operational teams into a frenzied, hurry-up mode in which mistakes multiply.

Existing stakeholders deserve better. Moreover, no matter how consistently a firm might outperform the market and its peers, prospective clients and investors will not knowingly allocate assets to organizations whose long-term business prospects are dim or whose ability to keep pace with rapid change is doubtful.

Avoiding Common Pitfalls

Underestimating the momentous environmental shifts taking place

The investment management industry is in a state of metamorphosis. Buy-side firms continue to be pressured by clients and competitors to offer new investment products that generate what has been called “true alpha.” Meanwhile, clients and regulators are pushing the industry to increase transparency, provide timelier reporting and information, adopt key industry standards and reduce investment and operational risk. And clients want it all done for lower fees—even as legislators overhaul the financial services framework and regulators formulate new layers of requirements.

To be proactive:

- **Place a high priority on effective long-term business planning.** Now more than ever, managers need to focus on their own balance sheets and attend to their long-term profitability and survival. In practical terms, that means earnestly considering what may lie ahead and mobilizing the resources needed to manage change at both the firm and industry level. To put it in the simplest terms, managers need to think of their organizations not just as asset managers, but as dynamic, ongoing business enterprises.
Delaying or avoiding a concerted effort to manage change

Undertaking strategic and operational planning on this scale is daunting, to be sure. Human nature being what it is, we’re naturally inclined to focus on the many urgent and relatively well-defined issues that are already on our plates, pushing off the long-term challenges and threats until another day. This tendency is so natural and widespread that respected philosophers, psychologists and economists have created an interdisciplinary field of academic research known as “procrastination studies.” But investment managers who want to survive and thrive in the years ahead cannot ignore the changes taking place in their industry.

To be proactive:

- **Use the many resources available to help firms begin the task.** Investment managers and their consultants aren’t starting at square one. They can’t run their firms without knowing the business, reading the news, attending conferences and generally keeping abreast of what’s happening in the industry and the world at large. Management teams can also call upon well-established techniques for surveying, evaluating and addressing business risks, including brainstorming, mind-mapping and forecast calibration. Giving clear definition to the issues and problems ahead makes them more manageable (or at least less intractable). Simply taking that first step can be enough to help management teams break the logjam and move on toward an effective business planning initiative.

Failing to project cost structures

Even after several years of political and market pressure to reduce Wall Street compensation, staffing still represents the largest single expense category in most buy-side organizations. Yet the failure to anticipate staffing costs and manage them proactively is commonplace, especially in intermediate- and long-term business plans. To a large extent this breakdown arises from the disconnect between the key driver for increased revenues—assets under management (AUM)—and the key driver for increased costs—the number of accounts or portfolios managed. Too many business projections focus solely on AUM growth without regard to the underlying account growth that impels increases in staffing as well as systems and, of course, operational risk.

To be proactive:

- **Use operational benchmarking to help analyze cost structures.** Benchmarking can also help firms quantify the financial impact of changes in key drivers.

Neglecting to anticipate needs for organizational expansion

Rather than investing to upgrade staffing or infrastructure in advance of growth, many organizations hold off until key indicators of service quality, such as the timeliness and accuracy of client reporting, begin to slip in the wake of significant business expansion. In some cases, this lack of planning results in band-aid solutions that are intended to be temporary measures but, due to the unending stream of burning issues to resolve, become permanent fixtures over time. When that happens, workarounds become standard operating procedure. Staff get overstretched. And operational risk soars.
To be proactive:

- Utilize metrics and factor operational staffing and systems needs into planning for new product and sales initiatives. Additionally, each budget cycle should include consideration of the resources needed to match expected AUM or product growth.

Waiting too long to loop operations into the product launch process

Inaugurating a new investment strategy or fund requires significant planning and conscientious communication. Whether in the interests of secrecy or the rush to bring offerings to market, firms often wait until the last minute to notify operations or technology staff of strategic decisions. But it takes time—and, again, careful planning—to put in place the workflows, procedures and systems needed to support a new initiative. Problems are particularly likely to arise when new products involve markets or instruments in which the firm has not invested before. Such initiatives may demand unforeseen systems changes; extra set-up with the affected custodians, prime brokers and administrators; additional valuation policies and pricing sources; and new client and regulatory reporting.

To be proactive:

- Notify operations staff of new products early in the product launch process. As a general rule, the greater the advance notice provided, the fewer the operational problems encountered. Best-practice firms have new product committees that meet regularly to discuss, review and approve all new product launches, including the utilization of new types of investment vehicles (separate accounts, hedge funds, etc.). They also invite compliance, operations and IT staff to be active participants from the outset, rather than receiving a memo or e-mail late in the game—or, worse still, learning about new operational requirements only after the fact.

Ignoring external factors that lie beyond management teams’ control

The need for business continuity and disaster recovery planning is self-evident. Less obvious, but no less critical, is planning for emerging developments in the market and regulatory environment—and there we see a tsunami of change on the horizon.

Of course, while the Dodd-Frank Act has passed in the U.S., and the Alternative Investment Fund Managers Directive (AIFMD) has entered into force in Europe, and it is reasonably clear which agencies and regulators will implement their provisions, many of the details have yet to be revealed. Still, forward-looking investment firms will read the handwriting on the wall and assess the general directions in which regulation is going.
To be proactive:

➤ *Take the time to absorb and discuss industry group analyses of Dodd-Frank, AIFMD and their effects.*

In Europe, the Alternative Investment Management Association (AIMA) and the Irish Funds Industry Association (IFIA) are among groups that have analyzed the implications of AIFMD. In the U.S., the CFA Institute, the Council of Institutional Investors, and other organizations have all studied aspects of Dodd-Frank’s sweeping legislation. Their findings point to a number of likely impacts on buy-side firms, for example:

- Many more alternatives managers, including firms that are not domiciled within the U.S., now have to register with the Securities and Exchange Commission (SEC). For many managers, this will require implementing and documenting a host of new policies and procedures. (Some managers will also have to contend with state-level regulatory requirements, as insurance companies have done for many years.)

- To comply with the voluminous reporting requirements imposed by clients and regulators, investment managers will need to harness their data to satisfy new demands for transparency. Robust data aggregation, normalization and governance become even more important than ever before.

- Fulfilling all these additional regulatory requirements will cost money. This is likely to result in an acceleration of merger-and-acquisition activity and outsourcing across the industry, as firms that are already under margin pressure try to leverage their infrastructure by achieving greater scale—that is, expansion of AUM—without a proportionate increase in staffing. Many of the smaller firms that are not acquired will likely struggle to survive, though the rise of middle-office outsourcing will help some to stay afloat.

- Institutional investors will relentlessly hammer their investment managers for higher returns and lower fees, as they themselves are pressed to deal with their unfunded liabilities.

**Failing to prepare for rising operational performance and due diligence standards**

When selecting external managers today, institutional investors and their consultants require traditional firms (but not hedge funds) to comply with the Global Investment Performance Standards (GIPS®). They also subject hedge funds (but not traditional managers) to intensive operational due diligence (ODD). Convergence of these two standards is all but inevitable as M&A activity accelerates and the line between traditional and alternative managers continues to blur.

To be proactive:

➤ *Start getting ready now for the new requirements.* Hedge fund managers may wish to implement the GIPS® standards before they are widely demanded and traditional managers should prepare for ODD. Many organizations with forward-thinking leadership are already taking steps toward meeting the new standards, including performing operational reviews, documenting their workflows, developing IT roadmaps and reviewing their approach to outsourcing and managing external service providers.
Let’s end this discussion with some encouraging scenarios. Rising client expectations and heightened regulatory oversight will likely prompt senior management to place greater emphasis on operational excellence through best-practice processes, improved data management, more effective controls and appropriate investment in staff and infrastructure.

As the market improves and growth resumes, investment managers’ firms will be strongly motivated to re-examine their organizational structures and develop forward-looking staffing and technology plans. At the same time, margin pressure will drive further technological improvements and outsourcing to increase scalability, improve quality and control costs. Rapid industry change has its upside, and firms that want to manage and reduce their operational risk will make the most of it.
At times, managing buy-side investment operations can seem like a thankless job. In many organizations, senior management is blithely unaware of just how much it takes to design, implement, maintain and upgrade the systems and workflows that support the business—from account set-up through client reporting across a range of investment strategies, markets and instruments.

Middle- and back-office supervisors and employees may feel, justifiably, that they are noticed only when things go wrong. And if their department is understaffed, they may despair of ever getting ahead of the relentless flow of transactions long enough to make improvements, despite their desires to streamline processes, reduce error rates and mitigate the firm’s liabilities and reputational risks.

Take heart! We offer this series as a source of hope, inspiration, and practical guidance for those who aspire to break through the logjam. And we sincerely hope the issues and ideas raised will encourage you to embark on a formal or informal process of assessing risks and considering action steps to address them. That need not entail some massive, hugely time-consuming effort. This guide’s structure, which breaks risks down into ten discrete categories, may actually facilitate a piecemeal, iterative approach which, with perseverance, may be just as effective as a “big bang” effort.

To briefly recap the areas of risk we have highlighted:

1. **Complacency** – These types of risks crop up in flawed business continuity plans, poor recordkeeping and deficient insurance coverage. Other practices that place organizations at risk include hiring inexperienced or under-qualified staff, neglecting to train new employees, disregarding feedback from middle- and back-office staff, operating without an electronic document management system and failing to check employees’ work. To tackle these issues, consider better training, tightening up internal procedures and improving communication.

2. **The Blind Leading the Blind** – Mid-level and senior managers who are unfamiliar with investment operations may rely upon subordinates who are also unqualified for the task at hand. (Outsourcing has benefits, but it is not a panacea, and doesn’t relieve an organization of responsibility. It also brings its own due diligence demands.) External operational reviews can help illuminate these risks. To address them, consider ways to improve hiring, promotion and coaching practices as well as strengthening due diligence frameworks.

3. **Novices, Apprentices and Soloists** – Problem areas here include small, specialized teams that work in isolation, and individuals who assume sole responsibility for a function or relationship, often zealously guarding their “turf.” Thoughtful attention to organizational design, training and cross-training can promote teamwork and reduce key-person risk at all levels. Firms can take advantage of an array of training resources and formats including conferences, live and online classes, short courses, and internal “lunch-and-learn” sessions.
4. **Dropped Batons** – Information handoffs between people, departments, organizations and systems are fraught with communication and timing challenges. The most useful tools for identifying potential trouble spots are system diagrams that identify all applications and their interfaces, and workflow diagrams that display hand-offs between teams or departments and between the firm and external counterparties, service providers and clients.

5. **Naïve Reliance on Technology** – While automation is a powerful tool for mitigating operational risk, it can create new hazards if systems are not carefully designed and implemented. To reduce those risks, make sure that staff and consultants who deal with operational systems know how to perform automated functions manually and, furthermore, understand their operational context, including system and workflow linkages. Keeping system access permissions up to date, maintaining system infrastructure, and building in thorough audit trails are all high priorities. The importance of written functional specifications and detailed testing cannot be overemphasized.

6. **Playbooks** – Nonexistent, obsolete or incomplete process-and-procedure documentation is frequently a factor in operational breakdowns. The remedy is workflow diagrams that are kept up-to-date and readily available. Not only are such workflows important in the effort to lower day-to-day risks, they are also useful in new-hire training, system- and process-improvement initiatives and disaster recovery. Firms should also have well-defined issue escalation protocols that take into account both the magnitude and timing of potential impacts.

7. **Amalgamated Assignments** – When designing organizational structures, policies and procedures for the segregation of duties, it is vitally important to maintain the distinction between the firm and the fund(s) it manages. Operational reviews can help flag potential conflicts of interest as well as opportunities for theft or fraud. Firms may want to consider whether it is appropriate to institute some degree of shadow accounting, whereby investment managers maintain their own sets of books and records for comparison with those of custodians, auditors and independent third-party fund administrators.

8. **Reconciliation Gaps** – Less than comprehensive procedures can leave investment managers unknowingly exposed to risks. To reduce that exposure, firms should conduct full reconciliations between their records and those of the custodians and administrators, with provisions for supervisory review and accountability. Full reconciliations include comparisons of cost basis and market value (in local currency terms), security identifiers, and local-currency cash balances; they also entail reconciliation of margin or collateral positions using statements from the party holding the assets. While performance analysts who investigate out-of-tolerance variances in rates of return do provide a final check on the accuracy of input data, that is no substitute for a full reconciliation.

9. **Reading the Fine Print** – Legal documents should be reviewed in detail not only by the firm’s attorneys, but also by knowledgeable operational managers. When assessing counterparty risk, firms need to identify exactly which legal entity is their counterparty, determine who has regulatory jurisdiction, and continuously monitor net exposures as well as the counterparty’s creditworthiness.

10. **Poor Planning and Slow Response Times** – Investment management organizations that fail to plan ahead may sustain huge business and operational impacts as a result of the sweeping regulatory, marketplace and competitive changes that are transforming the industry. Against a backdrop of expanding regulatory requirements, clients and investors are pressing firms to increase transparency, accelerate reporting, and reduce risks—all while lowering advisory fees. Operational benchmarking can assist firms in analyzing cost structures and the financial impacts of changes in key business drivers. As the line between traditional and alternative managers continues to blur, the former are encouraged to prepare for operational due diligence and the latter, to implement the GIPS® standards.
At SEI, we work with clients on fund administration and middle-office outsourcing solutions. Identifying and reducing operational risks is one of our primary objectives. Indeed, risk management is one of the major reasons why investment management firms consider outsourcing in the first place. In light of the complexities and constant change in our industry, virtually every firm has the opportunity to take risk management to the next level.

Thus, this guide is intended not only for operations managers who seek to update and elevate their risk management practices, but also for senior business executives. In our experience, the firms best equipped to keep the machinery of investment management running smoothly are those where senior management is engaged with that effort. Operations departments function best when senior managers understand how things are done, provide the resources needed to mitigate risk, recognize that some events are beyond reasonable control, and reward operations staff for their successful efforts. If this guide contributes, however modestly, to a culture of excellence and ongoing innovation in the operations of investment management firms, it will have fulfilled its purpose.

Visit [www.seic.com/OpRisks](http://www.seic.com/OpRisks) to download each chapter or the entire book.

This information is provided for educational purposes only and is not intended to provide legal or investment advice. SEI does not claim responsibility for the accuracy or reliability of the data provided.

Information provided in the U.S. by SEI Global Services, Inc. Beyond the U.S., this material is provided by SEI Investments - Global Fund Services Limited (Reg. in Dublin No. 242309), SEI Investments Trustee & Custodial Services (Ireland) Limited (Reg. in Dublin No. 315393), and their affiliates, which are all wholly owned subsidiaries of SEI Investments Company. SEI Investments - Global Fund Services Limited and SEI Investments Trustee & Custodial Services (Ireland) Limited (Styne House, Upper Hatch Street, Dublin 2, Ireland) are authorised by the Central Bank of Ireland under the Investment Intermediaries Act 1995. This material is not directed to any persons where (by reason of that person’s nationality, residence or otherwise) the publication or availability of this material is prohibited. Persons in respect of whom such prohibitions apply must not rely on this information in any respect whatsoever.
SEI (NASDAQ:SEIC) is a leading global provider of investment processing, fund processing, and investment management business outsourcing solutions that help corporations, financial institutions, financial advisors, and ultra-high-net-worth families create and manage wealth. As of June 30, 2012, through its subsidiaries and partnerships in which the company has a significant interest, SEI manages or administers $424 billion in mutual fund and pooled or separately managed assets, including $182 billion in assets under management and $242 billion in client assets under administration.

SEI's Investment Manager Services division provides comprehensive operational outsourcing solutions to support investment managers globally across a range of registered and unregistered fund structures, diverse investment strategies and jurisdictions. With expertise covering traditional and alternative investment vehicles, the division applies customized operating services, industry-leading technologies, and practical business and regulatory insights to each client’s business objectives. SEI's resources enable clients to meet the demands of the marketplace and sharpen business strategies by focusing on their core competencies. The division has been recently recognized by Buy-Side Technology as “Best Fund Administrator,” by Hedge Funds World Middle East as “Best Service Provider,” by Global Investor as “Hedge Fund Administrator of the Year,” and by HFMWeek as “Best Single Manager Hedge Fund Administrator (Over $30B AUA)” in the U.S. and “Best Administrator – Technology Provider” in Europe.

SEI Knowledge Partnership
Insights for Investment Managers

The SEI Knowledge Partnership is an ongoing source of action-oriented business intelligence and guidance for SEI's investment manager clients. It helps clients understand the issues that will shape future business conditions, keep abreast of changing best practices, and develop more competitive business strategies. The Partnership is an initiative of SEI's Investment Manager Services division.

Find us on LinkedIn and Twitter:
LinkedIn: SEI Knowledge Partnership
Twitter: SEI_KP