



ENABLING AND MAINTAINING THE CULTURE OF COMPLIANCE IN FINANCIAL SERVICES:

*The Importance of
Appropriate Tools for
Compliance Risk Reduction*

EXECUTIVE SUMMARY

In October 2005, the Security Industries Association (SIA) Compliance and Legal Division (known today as the Compliance and Legal Division of the Securities Industry and Financial Markets; SIFMA/CL) released a white paper titled, *White Paper on the Role of Compliance*, which offered practical and concise recommendations to the financial industry for differentiating the responsibilities of compliance personnel from those of business personnel who are acting in a supervisory capacity. Included within the text of the paper is a section that emphasizes the important role that compliance personnel play in promoting a culture of compliance. Such a culture has largely become successfully entrenched throughout the financial services industry—leading some regulators to generally commend the activity of firms to this end.

Many industry experts would agree that a culture of compliance has been established, and that this culture extends beyond the boardroom to permeate sales and trading desks, operations areas, and the broader employee workforce. In fact, the National Association of Securities Dealers (NASD) recently noted in its annual report that the number of non-compliance cases the organization brought against member firms dropped in 2006 to 1,147—almost 200 fewer than in 2005—and the total amount of levied fines was halved. As such, it would appear that compliance responsibility has been distributed appropriately and effectively to business supervisors—with compliance personnel maintaining effective roles in establishing supervisory policies and procedures and monitoring subsequent supervisory activities.

But whereas most firms have rigorously documented policies and procedures, many are still struggling to implement adequate mechanisms that enable supervisors to execute their compliance responsibilities efficiently (or even at all). While responsibilities have been placed squarely on the shoulders of business supervisors and risk managers through comprehensive and written instructions, regulators note that enterprises have not done a good job of demonstrating that they are actually doing all the things *they say* they are doing in their written policies and procedures. At the 2007 SIFMA/CL seminar, Lori Richards of the NASD Office of Examinations called this the “bad news” in the industry.

Many organizations have failed to introduce tools and technology that avails all the necessary information to all stakeholders in the compliance process and that allows them to review their business areas effectively, highlight problems in a timely fashion, and document supervisory activity/response in a manner that stands up to regulatory muster. By better equipping all the stakeholders in the compliance process, firms will be able to state confidently that they are satisfying the requirements of their own internal policies and, thus, entrenching a culture of compliance. So while they have taken reasonable steps that introduce a culture of compliance across their organizations, enabling and maintaining a culture of compliance looms as the next challenge. Institutions will heed the clear message that regulators are sending that there is much more to do at firms of all sizes.

Simultaneously, the global regulatory landscape is quickly being clouded with discussions of movement from a prescriptive, controls-based compliance requirements model that dictates rules and actions to firms about how they should operate their businesses to a principles-based approach. Such a philosophical shift would serve to accelerate the need for enterprises to implement tools, technologies, and practices that help managers to apply a compliance mentality that is driven by identifiable and measurable risk.

TABLE OF CONTENTS

- 3 History of the Culture of Compliance
- 4 The Culture of Compliance Today
- 7 The Future of the Culture of Compliance
- 11 Conclusion
- 12 How SunGard Can Help
- 13 About SunGard

The Story Behind Principles-based Compliance

In the UK, the Financial Services Authority (FSA) has led much of the movement toward principles-based regulation. In recent years, the FSA has applied an approach that recognizes the risks inherent in financial markets and applied an evidence-based model to new policy wherein market failure and potential costs and benefits of regulatory intervention are considered prior to introduction of such policy. While the FSA does not claim to have achieved a full principles-based model, it has—over the past year—increasingly taken such an approach in its activities. In the US, regulators have demonstrated a willingness to initiate discussion of a similar shift away from a prescriptive approach to an “outcome focused” philosophy that applies high-level rules as a way to achieve regulatory objectives. While perhaps the perceived decline in the “competitiveness” of the US financial markets is an instigator of such discussion, it is also clear that regulators are very aware of the importance of applying a similar approach to regulation in an environment of rapid globalization, which is characteristic of the financial services industry.

At the Federal Reserve Bank of Atlanta’s 2007 Financial Markets Conference on May 15, 2007, Federal Reserve Bank Chairman Ben Bernanke endorsed principles-based supervision, stating that “Central banks and other regulators should resist the temptation to devise ad-hoc rules for each new type of financial instrument or institution.” He indicated his preference, instead, for developing principles-based policy responses to meet clearly defined public policy objectives and stressed the importance of applying such principles consistently across the financial sector. Chairman Bernanke also noted specifically that the FSA’s activities in the UK are influencing the US regulatory approach.

This executive brief highlights the need to help business supervisors achieve and preserve a culture of compliance throughout their respective organizations by:

- Demonstrating the requirement for tools that drive efficiencies in compliance activities throughout their organizations (downstream)
- Developing the process for sharing best practices, enabling information access and flow amongst employees, and educating supervisory and risk management staff in the business activities that are being performed and monitored (upstream)

It is through the delicate balance of both downstream and upstream needs that financial services organizations will satisfy internal requirements for marrying business- and compliance-side responsibilities and do it in a way that delivers on the true promise of *creating, enabling, and sustaining* a culture of compliance.

HISTORY OF THE CULTURE OF COMPLIANCE

Compliance Departments have established themselves as a stand-alone resource for supervision, advice, monitoring, and training in support of business units and management. And as noted in the SIA white paper, “firms prioritize a culture of compliance at every level of their organization as a critical facet of their self-regulatory efforts.” This is especially important to note because it shows that most financial institutions recognize that such an environment provides the first line of defense for the identification of potential problems, deterrence of misconduct, and possible reduction of fines when inappropriate activities occur.

In the advisory role today, Compliance provides proactive and reactive education and is often physically located within or adjacent to business units. Compliance usually assists management in the development of policies, procedures, and guidelines designed to facilitate adherence to applicable laws and regulations. And with regard to education and training, Compliance is expected to keep all personnel apprised of policies and procedures, as well as regulatory events. Compliance also performs critical ongoing monitoring and surveillance of the business units and proactively reviews business activities for potential regulatory, compliance, and reputational risks.

However, the SIA white paper clearly states that “The management function in a securities firm, not the Compliance Department function, has the responsibility to supervise business units and to direct firm and employee activities to achieve compliance with applicable laws.” That means that while the Compliance Department is essential to support a firm’s overall compliance system and promote the underlying organizational culture necessary to sustain it, supervisory authority rests firmly on the management level and in the business units themselves. *It also means that many firms may be at serious risk for noncompliance by virtue of their failure to provide supervisors with the tools to accomplish the supervisory activity specified within their policies and procedures.*

“An important role of the Compliance Department is to assist senior management and business unit managers in promoting a culture of compliance at the firm. Senior management must put in place the people and systems necessary to achieve compliance. This includes allocating sufficient resources to build effective compliance systems (including technology), creating incentive structures that reward compliant behavior (and penalizing behavior that sacrifices compliance principles), and giving Compliance personnel regular and unfettered access to senior management. If business personnel view compliance as a crucial institutional value, they will value the Compliance Department’s role and work with Compliance Department officials to achieve business goals within the constraints of the applicable regulatory framework.”

– *White Paper on the Role of Compliance*, October 2005, Securities Industry Association

THE CULTURE OF COMPLIANCE TODAY

Pressures on Business Supervisors

Today, ensuring and enforcing a culture of compliance has also become the responsibility of business supervisors, often without the appropriate tools and resources necessary to successfully balance their traditional responsibilities, as they relate to the business, with these new compliance obligations.

Consider that business supervisors must:

- Continue to manage their primary responsibilities in the areas of revenue generation and customer service
- Manage staff
- Respond to often redundant requests from the Compliance, Internal Audit, External Audit, and Risk Departments to describe their business activities
- Monitor their businesses and employees in accordance with extensive written supervisory procedures and evidence their supervisory activities

Thus, such responsibility can greatly constrain the business supervisor from his/her “primary” objective of generating profits within the business unit and through efficient customer service and product innovation. This is not to say that supervisory responsibilities are excessive; the current environment appropriately aligns compliance responsibilities (and personal liabilities) with those highly compensated leaders of organizations and business units. But in the worst cases, some supervisors may be “signing off” on completed compliance checks—often on non-timely bases and without the adequate information to do so. As such, they may be “betting” their very careers on their intuition and gut feel that nothing untoward has occurred. Firms must provide the necessary information and tools to enable these supervisors to perform their jobs properly and reduce the stress that they experience over possible allegations of “failure to supervise.”

Business Supervisors are under tremendous pressure to:

- ✓ Generate revenue
- ✓ Collaborate with operational risk professionals
- ✓ Respond to internal and external auditors
- ✓ Collaborate with compliance personnel on new items
- ✓ Assume compliance responsibility and promote a culture of compliance throughout their staff and the larger organization

Failure to Supervise

Supervision failure represents a very real threat to individuals' careers—and their livelihoods and reputations—not to mention associated criminal liability. And even those enterprises that *do* have policies and procedures that are expected to be executed by business supervisors, often *do not* have adequate technology to enable such supervision.

Many global investment banking and securities trading and brokerage firms have been cited by the Securities and Exchange Commission (SEC) over allegations that they have inadequately supervised salespeople with regard to customer e-mail and fax communications. The citations are for specific violations of The Securities and Exchange Acts of 1933 and 1934 and in recognition of firms' failure to reasonably supervise their employees via effective pre-approval and post-transmission policies for review of electronic communications.

Challenges, Obstacles, and Requirements

Various time drains, coupled with an obvious concern regarding personal liability for "failure to supervise," are already initiating an unintended response in order to accommodate the demands placed on business supervisors.

For example, some firms are now taking advantage of an "Admin 24" distinction and certifying their administrative talent through the NASD Series 24 General Securities Principal examination process to manage the day-to-day tasks of "supervising" complex business activities. As the Admin 24, support staff are focused on completing the many checklists associated with an institution's supervisory procedures. Such an approach may achieve the narrow objective of addressing the letter of the prescribed activity, but it arguably falls short of the spirit of that charge, which is the ability to quickly isolate problems within the institution. If the Business Supervisors and Admin 24s were equipped with enabling technologies that generated alerts applying sophisticated rules, they could work together to identify real problems while also expediting supervisory tasks and making the existing "checklists" themselves more meaningful and helpful.

The Dawn of the “Admin 24”

The Admin 24 is an individual who has passed the NASD Series 24 General Securities Principal exam and is dedicated to satisfying the monitoring and initialing of checklists highlighted and referenced throughout a firm’s supervisory procedures. While in many cases, the Admin 24 possesses the requisite experience to perform these supervisory tasks, organizations often entrust this important role to administrative talent that has passed the exam but may not understand the underlying business activity with the proficiency expected of a supervisor. Moreover, people in this role may not fully understand the responsibility (*and personal exposure*) associated with adequately protecting the firm and its customers from liability.

There also exists an excessive use of “sampling,” where institutions elect to make spot checks of emails and trades or other events in order to determine inadequacies in their processes against regulatory requirements. But such an approach does not provide adequate supervision in today’s high volume environment. Technology can eliminate the need for “sample-driven” compliance. Firms can—and should—be looking at every trade, transaction, deal, and communication from a variety of different angles, including a “pattern-based” perspective to achieve appropriate supervision. After all, a single transaction can be easily dismissed as a one-time aberration when, in fact, it may be part of an intentional set of activities that is not in accordance with the firm’s policies or standards. Appropriate tools provide the ability to identify certain types of behavior but only report them as an “alert” when they have occurred a specified number of times, demonstrating a pattern. And, this threshold should be able to be set independently by each company or department.

In an effort to quickly and effectively address their specific regulatory drivers, many financial institutions have built their own compliance solutions as opposed to buying third-party vendor products. In some cases, the “build” approach is necessary to satisfy unique organizational requirements or fill a demand where externally developed solutions are inadequate. However, an internally developed technology model may limit a firm from benefiting from best practices in rules and surveillance techniques that are embedded in mature, third-party software. (Thus, they may miss a “peer-driven,” best-practices-based approach to certain types of compliance activities.)

Even more unfortunate is the inadvertent minimization of institutions' written policies via the literal inundation of supervisors with reviews of procedural language. Because they are typically required to read and comment on numerous draft versions or revisions to written supervisory procedures (WSPs), these activities are often completed in a cursory manner. Business supervisors may become overwhelmed by the seemingly endless and iterative review cycles of for their firms' compliance policies and procedures and resort to simply accepting words and rules because they are too tired or distracted to do anything else. This leads to a failure to ensure that the language in the WSPs—which is often crafted by Compliance or Legal personnel—is acceptable before the document is published. However, technology-driven tools can help supervisors (and all employees) review, respond to, and access compliance documentation and also provide mechanisms for easy and direct communication of important changes with the stakeholders.

At the other end of the spectrum, are firms that are consistently engaging in "verbal" approval for activity that is an exception to stated policy and procedure. There are many cases where it is appropriate for such exceptions to be granted, but a company that routinely does so without capturing the rationales risks regulatory consequences—and worse. After all, supervisors cannot possibly be expected to remember the details of every such exception, and few are diligent enough to prepare an acceptable diary of all of their overrides in a way that these decisions are accessible and understandable to an internal or external examination or audit. But, technology can help here, as well—and via functionality for "on the fly" exception recording and reporting.

THE FUTURE OF THE CULTURE OF COMPLIANCE

Business supervisors are seasoned at establishing and maintaining best practices for managing risk, being held accountable for business unit P&L, and protecting the value of the brand. But, these same business unit supervisors are less comfortable with the more recent addition of compliance in their job descriptions.

More than ever, there is a tightening of interests between operational risk activity and compliance-side responsibility. A report in the March 9, 2007 issue of the *Compliance Reporter* found that while operational risk is becoming more central to regulators because it is integral to larger risk mitigation initiatives and culture, the responsibilities associated with proving performance can be confusing, tedious, and time-consuming—and bring an unprecedented level of personal exposure to supervisors. But, most of today's business unit heads who must place their signatures on, say, a trade blotter each day, do so without the advantage of insight that senior compliance officers have via access to aggregated system data and dashboards.

The Convergence of Risk and Compliance

The Basel committee defines operational risk as “the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. The definition includes legal risk, which is the risk of loss resulting from failure to comply with laws, as well as prudent ethical standards and contractual obligations. Finally, operational risk also includes the exposure to litigation from all aspects of an institution’s activities.”

Thus, many regulators view compliance risk as an integral part of a firm’s overall risk management program. Moreover, the internal expectation is that Compliance must understand risk issues and bring them to the attention of management, then assist management in any necessary remediation.

So it is no surprise that many financial companies have merged their Compliance and Operational Risk Departments in order to integrate their efforts and results—and ensure that compliance activity is viewed through the operational risk lens.

Case in point: The December 1, 2006 issue of the *Compliance Reporter* stated that Lloyds TSB recently combined its Compliance and Operational Risk Oversight Departments because of the increasing overlap between them.

While deemed at the forefront of a trend, the strategy is sound because of the influence risk plays in the compliance function and the particular pressures financial institutions face in this area.

The executive board and key stakeholders are demanding that business units be accountable not only for what they are accomplishing in terms of both financial and non-financial performance, but also for increased transparency into how they are working toward and meeting their goals. And increasingly, examiners are spending more time in face-to-face discussions with business supervisors looking specifically to evaluate their abilities to accomplish the tasks itemized in written procedures and demonstrate access to information that enables supervisors to accomplish their compliance responsibility in an informed, rigorous manner. This growing relationship between business supervisor and regulator will undoubtedly be furthered by a principles-driven environment.

The primary sources of pain experienced by individuals with compliance responsibility are associated with limited access to data and/or poor quality data—but this pain is often higher with business supervisors than with compliance officers who have been buying and building systems specifically tailored for their monitoring and surveillance needs. Worse, some of the data required for compliance and risk monitoring activities often resides in systems that are not accessible by all of those charged with ensuring compliance and/or are not even designed to support “compliance purposes” in the first place. Hence, these tools need to evolve to satisfy the requirements of business constituents across the organization by delivering information *to those who need it, when and how they need it*. That said, they must also evolve to ensure the proper checks and balances occur.

Necessary Supervisory Functionality

Thus, as organizations drive the responsibilities of compliance and risk education further down their management layers to the lines of business, they must also deliver the tools to enable these managers to meet compliance requirements with greater efficiency. Today's buyers of technology products require embedded or readily accessible add-on functionality that addresses compliance issues, and in doing so, mitigates their individual risk of having "failed to supervise." For example, the implementation of real-time (at time of trade), near real-time, and T+1 systems provide business supervisors and compliance personnel with access to information required to monitor, record, and report on compliance performance, including:

- Supervisory view into trade monitoring solutions to see unusual trades before signing off on the daily blotter
- Supervisory connections to employee trading activity to pre-approve trades as part of an electronic workflow process
- T+1 reports identifying patterns of specific behaviors
- Running trend analyses on individual alerts generated through monitoring systems to identify personnel or system behaviors that demonstrate anomalies
- Automated access to case management and document management systems to record actions, decisions, and resolutions

"Today's buyers of financial technology products require embedded or readily accessible add-on functionality that addresses compliance issues, and in doing so, mitigates the individuals' and firms' risk of having 'failed to supervise.'"

Building a compliance framework that satisfies the needs of a broader audience requires, at a minimum, that compliance monitoring system outputs also feed into broader operational risk monitoring solutions. To do that, reporting requirements must be infused throughout the application architecture to consider all touch points that can be affected both positively and negatively by access (or lack thereof) to aggregated data.

Supervisory rules applicable to broker/dealers, for example, are creating the need for "compliance-like" applications for business supervisors and access to data and reports that enable them to complete their daily managerial responsibilities in an efficient and timely manner. Similarly, compliance personnel are expected to comprehensively monitor business activities—and that requires deeper, yet minimally disruptive, access into business data. At the heart of today's challenge in satisfying these goals, however, is the lack of consistency in management processes, multiple siloed and ad-hoc performance monitoring systems, and limited data integration.

Beyond Technology—Compliance and Risk Management Educational Requirements

According to a survey in the *Compliance Reporter*, March 2007, only half of Europe's top publicly listed companies claim to have the necessary corporate governance policies in place to protect against ethics and compliance failures. The study revealed that although 99% of respondents said they had a corporate governance code of conduct, a mere 50% ensure that all company employees actually read it.

Financial services firms that are committed to developing best practices in how they treat the provisioning of information throughout their organizations realize that to be successful, risk and compliance efforts must be integrated into business processes. That integration starts with dialogue and information exchange between business supervisors and compliance and risk officers to ensure:

- Compliance and risk officers learn more about the firm's actual business operations and methodologies in order to equip them with a clear understanding as to which activities need to be monitored toward ensuring comprehensive compliance
- Business managers learn more about their roles and responsibilities as they relate to compliance monitoring and management

In this way, firms can further develop their cultures of compliance by adopting a disciplined approach to imparting pertinent information throughout their organizations.

Holistic risk and compliance initiatives that consider the data collection, analysis, and reporting needs of its many stakeholders can be leveraged throughout the organization to satisfy a broader array of requirements. Consider the benefits of having "at your fingertips" data that included:

- Market data replays against actual firm trade performance
- Trade blotters that can drill into "alerts" generated on a trade for easy supervisor review and approval
- Trade data that is integrated with a case management system, so that investigation results could be preserved and retrieved efficiently
- Real-time access to pricing and position data in order to provide context for trade and portfolio valuation reviews by compliance analysts and risk managers

Further, by centralizing data from across the enterprise, key stakeholders can gain visibility into data that would not otherwise be aggregated or represented. Such information could be leveraged to benefit a broader array of corporate requirements to deliver additional benefits beyond compliance management—and into true business advantage. For example, a broker surveillance application designed to identify areas of concern to a compliance analyst (e.g. a retail customer account that suddenly demonstrates an unusually high-level of trading activity) may also serve to provide CRM-like indicators to sales personnel who can generate additional revenues (e.g. that retail customer account may be a candidate for more sophisticated financial products and services). In this scenario, related compliance and sales "alerts" would be derived from a common data source and delivered to the appropriate users.

CONCLUSION

As financial services firms become increasingly aware of the interdependencies of governance, risk, and compliance, they must build and apply solution frameworks that fully integrate data and deliver it in a way that serves the needs of their many constituents, including risk managers, business supervisors, and compliance officers. That goes beyond simply preparing a corporate code of conduct or a set of written supervisory procedures and expecting employees to read it. It means fully instituting and enforcing a culture of compliance by allocating budgets and building technology-driven systems that enable people to supervise in accordance with policies and procedures, and then monitoring and measuring adherence over time, with particular attention paid to continuous improvement. Using appropriate tools is the most effective way to reach the integrated business, risk, and compliance objectives of mitigating reputational and regulatory risk for the firm and its employees.

Firms must do a better job of recognizing the pressures on today's business supervisors and help them avoid "short cuts" to completing compliance supervisory needs that may appear to meet regulatory requirements (e.g., checking the box), but do not provide an educated review of the process and the resulting risks. Ultimately, failure to equip personnel with the appropriate tools to supervise may lead to formal "failure to supervise" allegations that can threaten the reputation of the firm and its employees, and can lead directly to revenue loss.

The right tools simplify the task of identifying compliance risk, because they can automate time-consuming processes and translate overwhelming amounts of data into information that:

1. Provide insight into business activities that typically cannot be "observed" in the normal course of business by supervisors
2. Allow people to react and respond in an appropriate and timely manner

Technology also enables the "right" information to be exposed based on a user's need to know—a particularly important consideration with regard to compliance applications.

HOW SUNGARD CAN HELP

SunGard offers technology-driven solutions that support the compliance requirements of compliance officers and business supervisors across the financial services industry. These solutions present results in a manner that helps managers to quickly and efficiently identify and correct issues.

Within SunGard, we are leveraging a Common Services Architecture (CSA) to help ensure that we bring solutions to our customers that reuse and/or enhance proven components in order to accelerate delivery time and provide ready integration with other products. Through CSA, SunGard offers a broad array of financial services software components aimed at addressing end-to-end compliance needs. These products reflect SunGard's unique breadth and depth of experience at the supervisory level, span the buy- and sell-sides and are designed to equip organizational personnel to institute, enable, and sustain a culture of compliance.

SunGard offers several tools aimed at streamlining the process of compliance with such specific features as:

- Automated monitoring of trades and transactions
- Policy and document management
- Automated reporting of information to regulators
- Compliance and risk dashboards and management reports
- Operational risk analytics
- Case management and investigations
- Governance via a streamlined compliance and performance-improvement environment

These toolsets comprise an efficient and cost-effective framework of solutions that financial services firms can apply to help meet the complex requirements of regulatory compliance in a risk-based manner while helping drive performance gains across the organization via automatic procedures for monitoring and controls, case management, data retention, documentation, and reporting.

About SunGard

With annual revenue exceeding \$4 billion, SunGard is a global leader in software and processing solutions for financial services, higher education, and the public sector. SunGard also helps information-dependent enterprises of all types to ensure the continuity of their business. SunGard serves more than 25,000 customers in more than 50 countries, including the world's 50 largest financial services companies. **Visit SunGard at www.sungard.com for more information.**

Author

Bill Nosal, managing director, compliance products
e-mail: bill.nosal@sungard.com

Managing Editor

Pat McAnally, vice president marketing, enterprise solutions
email: pat.mcanally@sungard.com

www.sungard.com

For more information:
1-800-825-2518
getinfo@sungard.com

© 2007 SunGard.

Trademark Information: SunGard and the SunGard logo are trademarks or registered trademarks of SunGard Data Systems Inc. or its subsidiaries in the U.S. and other countries. All other trade names are trademarks or registered trademarks of their respective holders.