

Compliance Risk Management

EXECUTIVE SUMMARY

The financial services industry is experiencing tremendous growth, diversification and innovation. Derivatives, globalization, product innovation, dynamic markets, and new methods of taking on and managing financial risk are key catalysts to profit growth and evolution. Wide-scale adoption of high-performance computing like that powered by AMD Opteron™ processors has further accelerated this financial services transformation.

Proactive Enterprise Risk Management ("ERM") has become critical in managing the many activities and various risks that a modern financial firm is exposed to. When determining the soundness of an institution, financial regulators are increasingly assessing both the quantity of the firm's ERM initiatives and the quality of its ERM programs and infrastructure. Compliance risk management is an integral component of ERM. Its goal is to minimize the effects of violation of or non-conformance with the many rules that govern how financial service business activities are properly supposed to be conducted.

Throughout this ever-changing environment, each and every financial firm is expected to remain compliant with all applicable international, national and local laws, regulations and rules. There already were many regulations. Recent years have witnessed even yet more rules. The critical importance of compliance risk management at the enterprise level has been reemphasized. The passage of new laws on protection of the homeland, accurate financial reporting, and various policy initiatives like customer privacy and anti-money laundering specified stiff penalties and fines for both individual violators and their managers and financial organizations.

External initiatives have created other regulations. Basel II, rules of evidence for Federal courts, business continuity standards and the European Data Protection Directive have all added to the multiplicity of policies and procedures for financial firms that exist today. Yet others like the Regulation National Market System in the United States and the European Markets in Financial Instruments Directive ("MiFID") are still in the process of being fully implemented. And yet more compliance requirements are being contemplated.

The financial markets are, by nature, a sea of dynamic uncertainty with constantly shifting values, risks and opportunities.

This paper highlights some of the practices financial firms need to implement for a strong and effective, near real-time compliance risk management program. Technology is one key element as modern financial operations are becoming increasingly complex. The reader should come away with a basic understanding of key issues, a desire to learn more, and the tools to upgrade key technologies to address compliance risk challenges in their organizations.

BACKGROUND

The financial markets are, by nature, a sea of dynamic uncertainty with constantly shifting values, risks and opportunities. Leading financial firms have evolved with product innovations, service enhancements and new methods of satisfying their customers' needs. As these institutions have grown, often they have expanded into new financial market sectors, and refined new methods of taking on and managing financial risk. Throughout this evolution, each financial firm has been expected to adjust its internal policies and procedures so that its processes, people and systems remain compliant with all applicable laws, rules and regulations.

In this dynamic environment, occasionally senior management and business activity leaders do not devote sufficient attention to compliance issues. Instead, attention is often focused on customer development, product enhancement, increasing revenues with the next transaction, or minimizing expenses. As a result, compliance matters can receive lesser focus. Some financial firms may then violate compliance rules or otherwise become in non-conformance. Significant fines and other penalties often result when these compliance violations or non-conformities are discovered by regulators or external parties.

Expenses from compliance loss events can be quite substantial. In the past decade, the

financial markets have witnessed hundreds of millions in fines and legal costs associated with NASD market-making practices, the independence of securities research from investment banking, and the allocation of IPO shares to favored clients. More recently, numerous investment firms, mutual fund managers, Wall Street dealers and even administrative firms have been penalized and fined for their activities around market-timing or late-trading in mutual funds and annuity products. Several leading NYSE market makers have been fined for putting their own interests in front of getting "best execution" for customer orders. In the insurance sector, various organizations have had to pay substantial fines regarding policy premium rebates and the improper use of finite reinsurance products.

These all are examples of wide-scale internal control breakdowns. Such compliance failures have also been the cause for renewed regulatory scrutiny across the financial services spectrum. The breadth and cost of these compliance loss events has been quite sobering. External events have also contributed to the much enhanced compliance environment. Lessons learned from the September 11th terrorism attacks and the various corporate America scandals such as Enron and WorldCom have fueled numerous new rules. The USA Patriot Act alone has added diverse regulations about the financing of terrorism, business continuity planning, terrorism insurance, information security, privacy, and enhanced anti-money laundering requirements.

The Sarbanes-Oxley Act was enacted to protect investors by improving the accuracy and reliability of financial statements and other corporate disclosures. To be compliant, companies must identify key business processes, the financial reporting risks arising from those processes, the controls in place to minimize those risks, and the strengths and possible deficiencies of those controls. The controversial Section 404 further requires that such controls must also be tied to specific financial accounts that they were designed to protect and an assessment must be regularly

made on the reliability of the financial statements. Finally, both the CEO and CFO are required to sign the resulting statements and for the first time, they may be held criminally liable for any material inaccuracies therein.

Other regulatory initiatives have also recently been promulgated. There are new financial service regulations and directives intended to ensure capital adequacy; to protect confidential customer data; to address structural market changes; to ensure fair-dealing requirements; to "know thy customer"; and to improve market transparency. In short, there is a multiplicity of regulations and standards that may be applicable to many business activities of the modern financial institution.

The financial sector's increasing reliance on risk-transfer strategies, the dizzying array of new products being offered to customers, and its increasingly global nature ensure that compliance challenges will continue. Policies and procedures at each financial firm will need to persistently evolve in response to both the changing composition of business activities and the many regulations that govern its conduct.

COMPLIANCE RISK MANAGEMENT

Enterprise Risk Management is a proactive activity ideally performed in near real-time whereby financial organizations use risk-management policies, procedures, processes, and technologies to properly conduct the three M's of ERM -- to measure, monitor and manage (control) their various risk exposures. These exposures might be related to credit, interest rate, liquidity, price, equity, foreign exchange, commodity, transaction, compliance, strategic, or reputation risk. Stress tests and scenario analyses that encompass potential, but plausible, variations produce estimates of potential aggregate loss exposures that may cause economic loss.

Compliance risk management is an integral component of Enterprise Risk Management. Its goal is to mitigate the current or potential compliance risk in the conduct of business

activities that exposes a financial institution to fines, civil money penalties, payment of damages, and the voiding of contracts. More egregious violations can also lead to diminished reputation, reduced franchise value, limited business opportunities, reduced expansion potential, or an inability to enforce contracts. Extreme compliance violations can result in suspension of license, being barred from certain business lines or even an institutional "death" sentence.

Compliance risk often overlaps with other types of risk exposures and as a result, its precise definition varies. Conceptually, though, compliance risk can be thought of as the risk of legal or regulatory sanctions, financial loss, or damage to reputation and franchise value that arises when a financial institution fails to comply with laws, directives, rules, regulations, prescribed practices, internal policies and procedures, or the standards or codes of conduct of self-regulatory organizations applicable to all of that institution's varied business activities and functions. Compliance risk also arises in situations where the laws or rules governing certain financial products or activities of the firm's clients may be ambiguous or untested.

FINANCIAL REGULATORS AND ENTERPRISE-WIDE COMPLIANCE RISK MANAGEMENT

Financial institutions worldwide have long been required to have written policies and procedures to ensure compliance with various rules and regulations. More recently, though, regulators have begun to use a framework to assess both the quantity of compliance initiatives and quality of the expected enterprise-wide compliance risk management programs and infrastructures. They have specified that such a compliance framework needs to be commensurate with the nature and level of the firm's risk profile, business strategies and compliance risk management objectives.

Financial regulators emphasize certain elements are essential for any sound and effective

Governance, Risk and Compliance ("GRC") framework like compliance risk management. These elements include:

- Establishment of an appropriate compliance risk management environment including active Board of Directors and senior management support and oversight.
- Regular identification and assessment of the compliance risk exposures inherent in all new and existing "material" products, activities, processes and systems.
- Creation of specific policies, procedures, and processes to control and/or mitigate compliance risk.
- Appropriate resource and technology allocations to perform ongoing measurement, monitoring and management of compliance risk.
- Construction of internal controls that enable comprehensive review and audit trail of the compliance risk management function by adequately trained and component internal audit staff.

Financial regulators recognize that the way these elements are integrated into a specific compliance risk management program will vary depending upon the inherent risk profile of the individual organization; however, they insist that they must be integrated somehow. Henceforth, regulatory examiners are likely to appraise how the Board of Directors reviews and approves key elements of the compliance program.

For instance, examiners will likely assess the risk assessment process that identifies current compliance risk throughout and across the many legal entities of a financial organization. They will review the process for reporting material compliance risk events up to and including the Board. The Board is expected to provide oversight of senior management. In turn, senior management is expected to carry out the Board's objectives by implementing a compliance program that is written, outlines roles and responsibilities, is appropriately resourced, and is disseminated to appropriate personnel throughout the financial firm.

Financial regulators expect specific compliance risk programs and infrastructure to evolve together with the ever-changing product lines and business activities of any growth-oriented financial firm. Also, as new compliance rules and regulations are promulgated, the firm's existing business activities will need to be re-assessed. Possible changes will then need to be incorporated into both the ongoing processes, procedures and systems as well as those of the compliance risk management function.

COMPLIANCE RISK EVENT EXPOSURES

Estimating a financial firm's aggregate compliance risk exposure is no simple task. Consider the many sources of compliance risk exposure, their probability of occurrence and the potential severity that might result from any of the following events. Examples of compliance risk events include:

- An employee might pass "insider" information about a corporate action to some third-party.
- A "rogue" trader might hide potential or realized losses at a trading firm.
- The firm may be able to locate only some back-up tapes memorializing electronic communication retention.
- A quantitative model used for electronic trading or valuations might produce inaccurate results.
- A superior might sexually harass or discriminate against someone he or she supervises.
- The firm might lose its branch license in some country or product line.
- A commercial banker might approve a financial transaction that violates fair-lending standards.
- Some type of third-party fraud might be uncovered.
- "Aggressive" market valuations might be submitted by an asset manager or private banker.
- A branch manager at a broker might sell unsuitable investments to a retail customer.

→ Some confidential customer information might somehow be lost or even stolen.

At a minimum, compliance risk can expose the financial institution to fines, civil money penalties, payment of damages, and/or possible voiding of contracts. Examples exist in each of the above categories where the compliance loss expenses exceeded one million dollars.

COMPLIANCE RISK MANAGEMENT SOLUTIONS

Particularly in the post-September 11th environment, leading financial market participants are focusing on a new compliance ERM intelligence model that leverages technology and is updated in real-time. Continually, these systems update as inquiries are made, events occur, transactions are conducted, valuations change, and financial funds are received and disbursed. The associated intense focus on monitoring and measuring various compliance risk exposures is sharply increasing compliance risk awareness. A key goal is to identify more actionable opportunities that allow potential compliance risk exposures to be nipped in the bud before they grow into bigger potential (or even worse, realized) losses. When coupled with a disciplined risk culture, risk transparency and intelligent risk-taking that appropriately balances risk and return, such financial firms are enabling higher profits for a given level of risk tolerance.

To monitor and better provide actionable compliance ERM intelligence, latencies need to be reduced at every step to mitigate the effects of stale data, stale calculations and ultimately, stale knowledge. Clearly, the biggest challenge for enterprise-wide compliance risk management solutions surrounds the issue of data. Can the compliance technology solution proactively access data throughout the many "silos" of a modern financial firm, including all product, distribution, operational and support areas? And assuming that it is able to do so, can the solution "rationalize" the various ways

that key data elements might be differently defined in each silo?

Consider, for instance, the broad area of sub-prime loans. Investment products exist in the residential mortgage, consumer credit cards and corporate loans sectors. Since each of these three silos has seemingly unique and different data requirements, often specialized technology subsystems are built in-house or acquired to meet specific needs in the origination, analysis, evaluation, trading, research and/or support areas. Each of these sub-systems collects, stores and manipulates data elements such as "loan balance." However, one sub-system might define this loan balance data element as the loan balance at time of origination, another might mean the balance as of the last payment date, and the third might refer to the last payment balance plus accrued interest through some evaluation date. All might be correct for the requirements of that particular silo. However, it does make it rather difficult to get an aggregate loan balance across the three example silos for a particular borrower credit quality!

This data integrity problem is compounded many times over when applied to compliance ERM systems. As noted above, there are a tremendous number of types of compliance risk exposure. Each type in turn requires many different data elements for its risk exposure evaluation. Hence, enterprise-wide compliance risk management systems have added to the pressure for improved data standards throughout the financial organization and across the information lifecycle. Data integrity in this context refers to the consistency, accuracy and appropriateness of the information in the database and model, as well as to the processes that produce and use that information. The concept of a "golden copy" is being emphasized — the integrated, trusted, timely and comprehensive single-source set of reference data for all aspects of a business and its related IT applications.

Which software vendor is appropriate for a compliance ERM solution is highly dependent on

Clearly, the biggest challenge for enterprise-wide compliance risk management solutions surrounds the issue of data.

the particular financial firm and what other technology commitments already exist. At the more custom-build end of the spectrum, Microsoft, IBM and Oracle all have robust enterprise database products that allow for the efficient manipulation of vast sets of data. These also have effective methods in which compliance rules can initially be coded and later modified as appropriate. Finally, advanced tools exist for these major database systems that allow building custom compliance solutions that include advanced statistical calculations, specialized reporting possibilities and various methods of displaying results in a graphical manner. Other more specialized compliance risk management systems exist and generally focus on some sub-set of overall compliance risk management.

THE AMD OPTERON™ PROCESSOR ADVANTAGE

Leading financial firms continue to evolve to a new risk intelligence standard based on accurate and actionable data, calculations and knowledge that are updated in near real-time as events occur. This involves considerable organizational change as shifts are made from data being gathered, aggregated and analyzed solely as part of periodic, batch-driven, core IT system processes. Utilizing reliable, cost-efficient, high-performance computing power, newer risk applications operate almost continually, assessing current operations and delivering risk intelligence as needed with minimal latencies.

To support these newer risk applications, financial institutions often select systems based on the 64-bit AMD Opteron™ processor. With native multi-core computing where two or more processing cores are on a single piece of silicon versus being packaged together, these systems are designed from the ground up for fast, efficient performance. They also help IT managers respond to today's key technology drivers: virtualization, security and enhanced manageability.

AMD's Direct Connect Architecture is inherent in all AMD64 processors and is key to the delivery of exceptional performance for compute-intensive applications. This design provides a high-bandwidth interconnect between computing cores, and directly connects memory, I/O, other processors in the system and third-party coprocessors through the use of HyperTransport™ technology. Direct Connect Architecture separates the I/O address and memory paths to help reduce bus contention and memory latency. The net result is that AMD Opteron processors can help reduce the amount of time it takes to move information from memory into a processor's cache to actually perform a mathematical calculation.

While such actions only take nanoseconds, improvements in this process when repeated billions of times can lead to significant time savings. Complex quantitative risk calculations, such as Monte Carlo simulations and Extreme Value Theory models, repeatedly invoke advanced mathematical instructions like random number generation and statistical functions. In designing the AMD Opteron processor, particular focus was given to the computational efficiency and accuracy of basic math calculations like log, sine and cosine.

All AMD64 processors feature low power consumption and heat generation. The performance-per-watt focus can help firms pack larger numbers of AMD Opteron processor-based systems into smaller areas. This can allow for higher compute density, better performance and potentially lower cost of ownership due to reduced power and cooling expenses.

The AMD Opteron processor natively supports both 32-bit and 64-bit applications and operating systems. It can run both at the same time without emulation, and while maintaining outstanding performance for either type of application, providing high-performance simultaneous 32- and 64-bit computing. This capability enables an enormous amount of flexibility, helping organizations to protect

investments in 32-bit applications, while easing the migration path to newer 64-bit applications.

The 64-bit architecture supports multiple terabytes of random access memory (RAM), compared to the 4 gigabyte limit of older 32-bit systems. This allows larger amounts of data to be stored in memory. The 64-bit AMD Opteron™ processor allows large amounts of data to be stored in memory, so larger time-frame and enterprise risk calculations can run faster.

The adoption of new levels of high-performance computing power as delivered by the AMD Opteron processor enables even more near real-time analytics. Sophisticated scenario analyses and in-depth stress-testing can be performed alongside the monitoring of compliance with various rules. The estimated losses from compliance risk exposures may be able to be calculated intraday together with key parameter risk sensitivities. Operational issues like where to focus management and compliance personnel attention next can be tackled on a frequent basis, leading to improved business performance. Indeed, as data obstacles are resolved, continuous, near real-time, enterprise-wide, operational risk management is becoming a possibility in global financial firms.

■



Advanced Micro Devices
One AMD Place
P.O. Box 3453
Sunnyvale, CA 94088-3453

www.amd.com