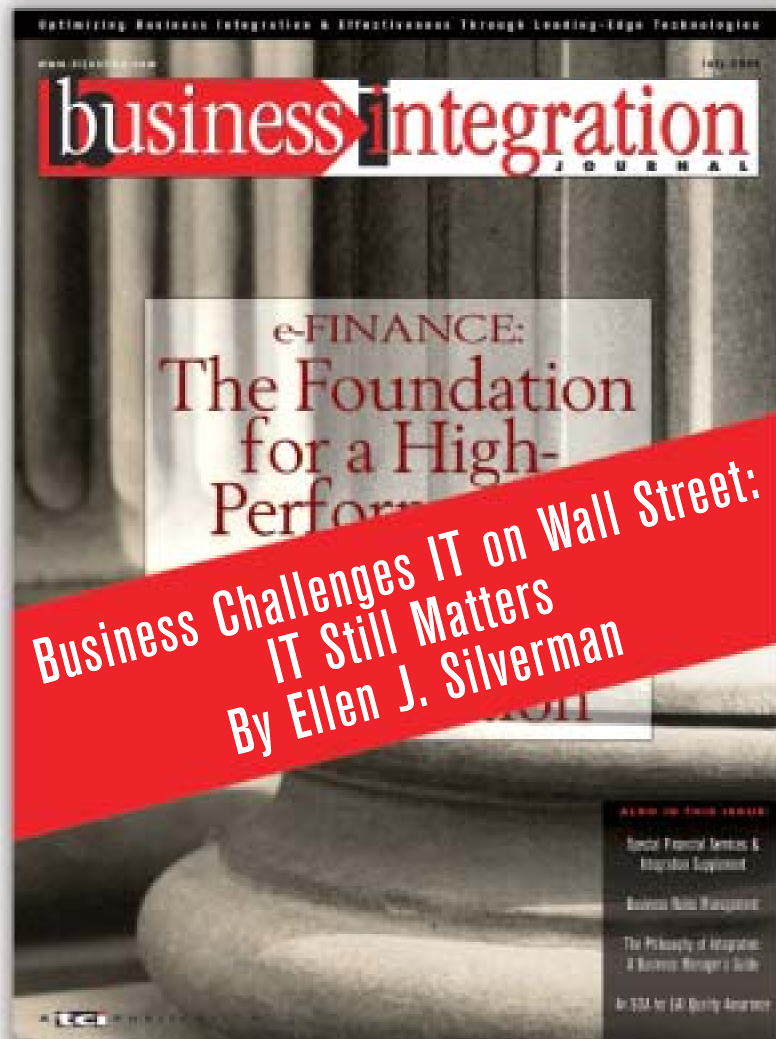
This article appeared in the
July 2004 issue of

business integration JOURNAL



Subscribe instantly at
www.bijonline.com

- Free in the U.S.
- $18 per year in Canada and Mexico
- $96 per year everywhere else

Business Challenges IT on

IT Still Matters

By Ellen J. Silverman

The main challenge facing IT managers in financial institutions today is learning how to integrate innovative technology that adheres to the ever-increasing and demanding compliance and risk management regulations. According to a recent presentation at a Securities Industry Association Technology Management Conference, it's estimated that close to 65 percent of IT on Wall Street is now devoted to complying with regulatory requirements such as Sarbanes-Oxley, Basel II, and the Patriot Act.

These new restrictions require firms to expand risk controls and electronic records management. Along with written records and e-mail, corporate policies and evidence of their enforcement must be retained, organized and submitted for audit under specific guidelines. The cost of market rule violations, as well as compliance, continues to climb while the requirements of modern risk management continue to grow in complexity. The cumulative dollar value of operational risk management failures is estimated to be nearly $25 billion through the end of 2003. That includes losses from rogue trading, business interruption, fraud, and failures in execution, delivery, and process management. While such failures obviously can have large financial consequences, they can also lead to even greater costs—such as the loss of investor confidence in a company, its products and services, or its leadership. Ineffective risk management can destroy a company, and in the process inflict tremendous damage on the world's financial markets.

Technology infrastructure and applications are essential partners to any robust risk management process. Without a culture that emphasizes the value of comprehensive risk analysis in making strategic business decisions, the best tools that technology has to offer are bound to fall short of the goal of successful risk management. Corporations need to recognize that risk management directly affects the ability of a financial institution to prosper and benefit its clients.

SARBANES-OXLEY COMPLIANCE

The Sarbanes-Oxley Act of 2002 is the most significant audit and corporate governance reform in recent history. With the Act's requirement of certification, auditability and disclosure, information security will have to be more attentive to the new requirements that audit departments require.

The goal of Sarbanes-Oxley is to restore investor confidence in the financial reporting of public companies and to hold an organization's officers personally responsible for any misrepresentations. The focus is management accountability for financial statement accuracy and associated controls, but some sections have great relevance to IT. Internal controls with respect to IT that produce financial statements are enforced primarily by information security tools and techniques. When the CEO and CFO sign off on the organization's annual report, they are implicitly stating that the organization's financial systems have appropriate controls and security to assure them that the resulting financial statements are reliable. Non-compliance, a missed deadline, or a material weakness reported in internal controls will certainly and significantly harm a company's shareholder value, executives' careers, and business relationships.

INCREASED COMPLEXITY OF RISK MANAGEMENT RESULTS IN SHARP GROWTH OF IT EXPENDITURES

While overall IT spending in the financial industry is expected to increase 5 percent in 2005 to $23.6 billion from 2004, Financial Insights, a consulting firm, is forecasting 9 percent annual growth in risk management IT investments in North America between 2004 and 2009, representing nearly double the rate of growth for overall IT expenditures. ›

Factors Affecting Risk Management Complexity

Ernst & Young surveyed IT managers in 2001 and found the lack of an organizationwide consistency in risk-assessment methodology to be the greatest barrier to effective risk management. Other obstacles included:

- The lack of an early warning system linking financial and risk data
- Unclear definitions of risk tolerance and limits
- Inadequate integration of risk management into core business processes
- Little process to ensure corrective action
- Poor communication channels
- Insufficient risk-monitoring mechanisms.

The discipline, tools, and methodology of risk management will continue to evolve as a result of globalization, client demands, marketplace improvements, regulatory reforms, and political realities, according to Richard E. Thornburgh, chief risk officer of Credit Suisse Group. Thomburgh feels that the task of managing risks is becoming increasingly complex for several reasons. The first reason is the increasing number of interrelationships among capital markets around the world, as 14 percent of the equities held by U.S. investors are in foreign markets with the total holdings of U.S. securities by foreign investors at almost $5.1 trillion. Moreover, in 2003, the value of U.S. investors' net transactions in foreign securities was nearly $44.6 billion; for foreign investors dealing in U.S. securities, it was $745 billion. There's a need for sophisticated financial instruments that take into account foreign currency fluctuations, interest-rate differentials, and compliance with different tax codes and regulatory regimes.

A second reason why risk management is growing in complexity is financial engineering. Today, some of the most creative people in the world spend their working hours designing new strategies to help financial institutions separate, distribute, and hedge risks. As their solutions become more complex, approaches to controlling risk require greater sophistication.

A third factor affecting risk management is the changing nature of regulatory requirements. The BASEL II capital accord is having a major impact on global financial institutions. Its purpose is to better align regulatory capital with the economic risk profile of internationally active financial organizations. To provide these dealers and banks with incentives to better measure and manage their risks, BASEL II introduces a meaningful recalculation of regulatory capital. The expectation is that BASEL II will result in a higher level of transparency and more sound risk management practices and techniques.

Finally, terrorism is a political reality that has changed the scope of operational risk assessment. Firms are meeting the risk challenges posed by terrorist threats with more elaborate business continuity planning.

e-Mail Compliance Is a Primary Focus

The emphasis on e-mail compliance is escalating for several reasons. To begin with, virtually all enterprises view e-mail as their primary corporate application. In addition, an increasing proportion of "records" are contained in the e-mail system. It has been estimated that close to 80 percent of enterprises use e-mail for closing orders and conducting other business. Message stores are growing 24 percent annually, and the typical messaging user sends and receives nearly 25,000 e-mails on an annual basis. As far as compliance is concerned, electronic documents are just as valid as paper documents. During discovery, all documents are subject to review and an enterprise must prove that every document or record is retained for the correct period.

The e-mail archival field has lately been characterized by much misinformation, mostly due to rapidly changing regulations and the corresponding state-of-the-art technologies emerging to address the dramatic escalation in the scope and depth of e-mail archival. For the evaluation of any archival solution, there are as many as 30 important parameters to consider. Some key parameters, if not addressed adequately, can result in the broker-dealer doing an inadequate job of meeting compliance requirements. Key parameters include the ability to capture e-mail emanating from systems other than the main e-mail servers or ability of the archival system to pre-review and block objectionable e-mails. Archiving information is the smartest course of action for any organization, as improper archiving can potentially cost heavy fines or adverse judgments. In December 2002, five Wall Street brokerages were fined more than $8 million for improper archiving.

A structured framework for weighting the evaluation to determine the "best-fit" solution is now mandatory for IT managers. This starts with leveraging the best practices for compliance risk and deploying process management. Identifying where e-mail is an integral component of knowledge and content management processes, implementing content filtering and archiving as well as developing an integrated electronic communications and content management strategy are additional steps required.

Effective Risk Management Helps a Firm Stay Competitive

By carefully assessing market conditions, the firm's capital, and the potential value of financial instruments, a firm can maximize its investment returns. By controlling risks, institutions don't just limit their losses, they also gain greater productivity and improve the quality of their services. By doing this consistently on a daily basis, risk management can bolster the investing public's trust and confidence in the capital markets.

High-performing management teams understand and embrace the fact that risk management enhances effectiveness. By determining where the potential opportunities and risks lie under varied market conditions, a firm is ultimately protecting its bottom line. In addition, it plays an important role in optimizing shareholder value, defining competitiveness in the marketplace by guiding pricing, and strengthening investor trust and confidence.

In summary, while effective technology is an indispensable tool of risk management, it is insufficient by itself. Companies must also have a robust risk culture. That means embedding the risk-management function into their core business processes. It means that risk managers must be partners in risk-return discussions. And it means that companies must place a high value on both the ability to operate sophisticated IT systems and the business judgment needed for sound business practices. **bij**

About the Author

Ellen J. Silverman is founder and principal of The Silver Word, a consulting firm that provides financial and technology research, analysis and marketing communication services to *Fortune 500* companies, financial institutions and technology firms. She is also senior editorial manager for Urban Bear Marketing, a New York-based marketing, design and branding firm. Prior to working in the technology sector, she spent several years on Wall Street working as an equity research analyst for Salomon Smith Barney and Deutsche Bank. Ellen received her bachelor's degree in Mathematics from Carnegie-Mellon University and holds a master's degree.
e-Mail: ellen@thesilverword.com