Industry Advisory Council

Transition Study Group

Building a Modernized Financial Regulatory System

January 30, 2009

Industry Advisory Council

Industry Advisory Council

The Industry Advisory Council (IAC) is a non-profit, non-partisan organization dedicated to fostering improved communications and understanding between government and industry. Through its affiliation with the American Council for Technology (ACT), the Industry Advisory Council provides a forum for industry to collaborate with and advise government executives on IT issues.

The Industry Advisory Council in cooperation with ACT is a unique, public-private partnership dedicated to helping government use technology to serve the public. The purposes of the organization are to communicate, educate, inform and collaborate. ACT-IAC also works to promote the profession of public IT management. ACT and IAC offer a wide range of programs to accomplish these purposes.

ACT and IAC welcome the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of information technology. For membership and other information, visit the ACT-IAC website at **www.actgov.org**.

Disclaimer

This document has been prepared to provide information regarding a specific issue. This document does not – nor is it intended to – take a position on any specific course of action or proposal. This document does not – and is not intended to – endorse or recommend any specific technology, product or vendor. The views expressed in this document do not necessarily represent the official views of the individuals and organizations who participated in its development. Every effort has been made to present accurate and reliable information in this report. However, ACT-IAC assumes no responsibility for consequences resulting from the use of the information herein.

Copyright

Further Information

For further information, contact the Industry Advisory Council at (703) 208-4800 or www.actgov.org.

3040 Williams Drive, Suite 610, Fairfax, VA 22031
www.actgov.org ● (p) (703) 208.4800 (f) ● (703) 208.4505

Government and Industry IT: one vision, one community

Executive Summary: Building a Modernized Financial Regulatory System

The headlines have been shocking and have come one after the other in rapid succession.

Federal regulators seize Washington Mutual in the biggest U.S. bank failure in history. Blue-chip investment firm Lehman Brothers collapses, a faltering Merrill Lynch is acquired by Bank of America and the Federal Reserve rescues insurance giant American Insurance Group. Congress passes a $700 billion bail-out to save the financial system. Investment guru to the rich, Bernie Madoff, is arrested in a $50 billion Ponzi scheme.

There are many reasons for the meltdown of the nation's financial system and for what are likely to be additional headlines recounting financial misdeeds: the housing bubble fed by super low interest rates, greed, lax government enforcement and regulation, and inadequate laws.

But one should not overlook a potentially important factor in the government's failure to sound early alarm bells to the crisis - the inability to use information technology effectively to gather data across markets, financial sectors and regulatory agencies to properly assess risks and glean troublesome trends.

As its stands now, multiple financial regulatory agencies have fallen behind the rapid growth of the global financial industry, relying on fragmented information technology systems that do not connect or overlap, and which have had the unintended consequence of keeping federal authorities in the dark.

We believe that there is an urgent need for a common technology strategy for financial industry regulation that could enhance governance and oversight of financial institutions.

Federal regulators have divided responsibilities, and individually and collectively cannot monitor systemic risk in the financial services industry. Each regulatory agency communicates with the private sector through entirely separate systems.

Financial institutions operate as distinct entities from an IT perspective, and use their own proprietary models, systems and risk and valuation methods. The result is that communications and data transfers across agencies and between the government and private sector are encumbered by limited and inefficient exchanges.

In short, the fractured information technology system has impeded transparency and cloaked the true health of our financial systems.

We need reform, which means streamlined processes, open interfaces, common data architecture, data standardization, effective information sharing and collaboration. We also need a solid risk management and analytics platform.

To achieve these goals, we recommend:

- Development of a National Financial Risk Management Strategy that will drive a unified understanding of systemic risks in the system and common objectives to mitigate those risks.
- Creation of a Financial Institutions Regulatory Enterprise Architecture to identify redundant capabilities and opportunities for synergy across the regulatory environment. This will provide regulators the ability to develop common processes and manage information systems holistically through common services, shared and consistent data, and joint collaboration and decision-making capabilities.
- Establishment of a Service Oriented Architecture (SOA) for agency optimal effectiveness that can rapidly respond to the affected agencies' changing information or application requirements. Rather than requiring all data and logic reside within single applications on single platforms, the service-oriented regulatory model could facilitate the leveraging of information and IT resources across or even outside the regulatory agencies.
- Creation of common data architecture to help ensure that data can be accessed, communicated, and utilized by the community of financial regulatory agencies in a timely manner.
- Use of common systems and tools across the regulatory environment to help integrate agencies towards a more unified regulatory environment.
- Development of cross-regulatory architecture security standards and encryption methods.

These changes and others recommended in this report will take time, money and perseverance, but the health of the financial sector and the American economy depend on both a vigilant government and one that has the information it needs.

This will take collaboration by government regulators, the private financial sector and IT industry leaders. It will also require strong presidential leadership to ensure that regulators and the American people get the kind of information and data they need and deserve to help promote greater financial stability.

Building a Modernized Financial Regulatory System

The federal Financial Regulatory structure was established 80 years ago. The banking and financial services sector has undergone much change during that time, and information technology advances continue to be tightly coupled with such change. While there were changes in the regulatory environment as a result of the Savings and Loan crisis in the 1980s and Gramm-Leach-Bliliey Act in the 1990s, the basic approach to Information Technology used by regulatory agencies has remained fragmented. A variety of government agencies implement regulations and communicate with the private sector through separate systems, websites and documents. By their very nature as private business entities, financial institutions – including banks, insurance companies, GSEs, dealers and hedge funds – operate as distinct entities from an IT perspective, developing proprietary models, systems, risk and valuation methods. Communications and data transfer across agencies and between the government and private sector are encumbered by limited and inefficient interfaces. Present IT systems do not adequately meet the needs of regulatory agencies to effectively regulate financial institutions. As the recent economic crisis has grown, the current fragmented approach has been unable to provide effective and timely insights needed for the government to prevent serious risk to the U.S. economy.

Additionally, regulatory agencies have limited insight into the risk exposure, standards and asset valuations of the private sector. This is in large part because the IT systems at financial regulatory agencies and private financial institutions are characterized by disparate, opaque, and closed information systems and technologies with minimal data sharing. To more effectively regulate financial institutions, there must be a common strategy that will integrate use of regulatory data and technology, regardless of whether agencies are consolidated or not.

We believe that a common technology strategy for financial industry regulation will enhance governance and oversight of financial institutions and enable efficient implementation of new regulations as well as effective application of existing regulations. Furthering that goal, streamlined processes, open interfaces, common data architecture, and data standardization are important features in promoting transparency and collaboration between agencies and private institutions. In addition, a solid risk management and analytics platform is necessary for risk assessment and mitigation. Such a next generation approach to using technology that is built on fundamental concepts of regulation, oversight and risk management is paramount to executing a unified approach to the new and evolving financial regulatory functions and fostering collaboration between all financial entities.

CURRENT STATE OF THE REGULATORY PROOCESS

The United States has several federal and state agencies that regulate banking institutions. These include: the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corp. (FDIC), the Office of Thrift Supervision (OTS), the Federal Reserve, the

National Credit Union Administration (NCUA) and state banking authorities. The OCC charters, regulates and supervises nationally chartered banks. The FDIC, the Federal Reserve and state banking authorities regulate state-chartered banks. The OTS examines federal and many state-chartered thrift institutions, which include savings banks and savings and loan associations. The Federal Reserve is responsible for bank holding companies and foreign branches of U.S. banks. NCUA is responsible for credit unions. The Federal Reserve Bank of New York has documented (http://www.newyorkfed.org/banking/regrept/BIATR.pdf) the matrix of responsibilities of the various regulatory agencies. The structure creates redundant and overlapping responsibilities for regulatory agencies chartering, licensing, insuring, supervising and examining banks subject to their oversight.

Similarly, state, federal, and industry regulators all carry out securities regulation in the United States. States have limited regulations on securities transactions which are superseded by federal regulations. The Securities and Exchange Commission (SEC) is the primary overseer and regulator of the U.S. securities markets. Industry regulators (e.g. stock exchanges, credit agencies) provide additional oversight and regulations. This system creates inconsistent regulations among market participants dependent upon the specific requirements of the state, federal, and industry regulators.

Individual states are the primary regulators of insurance entities. Regulations vary widely state to state. The National Association of Insurance Commissioners (NAIC) coordinates insurance regulations across the states and develops uniform policy where appropriate. The NAIC has made progress in making solvency regulation more uniform; however, achieving uniformity in other state regulatory functions, such as in the areas of consumer protection or market regulation, has proven more difficult.

While regulatory authority is shared among many organizations, the data and IT architecture is not. The IT architectures of regulating organizations do not address the following:

- Shared collection of information
- Common data and information architecture
- Common risk assessment methodology / rating system
- Systemic risk profiling
- Coordination, communication, and collaboration / data exchange between primary regulators
- Governance, transparence and collaboration
- Integrated information sharing
- Dissemination of timely and actionable information

KEY ISSUES DRIVING THE NEED FOR REFORM

The key issues driving the need for financial regulatory reform stem from industry evolution, an outdated regulatory structure, and an inefficient use of technology to provide transparency and insight into the health of the financial system.

The financial services industry has undergone a significant transformation in the short time since the Thrift Crisis in the 1980s. Financial products have expanded to include new forms of securities and derivatives. The differences between commercial banks, investment banks, insurance companies and brokerages have blurred as have the distinction between the securities markets and the commodities markets. Markets for financial products have grown in volume and expanded geographically. Financial services have become increasingly interconnected and have changed the way in which they impact world economies.

The financial industry regulatory structure in the United States has not changed significantly since the 1930s. Our current regulatory institutions, the Office of the Comptroller of the Currency, Office of Thrift Supervision, Federal Deposit Insurance Corporation, Federal Reserve, Securities and Exchange Commission, and many state regulatory institutions, were created to oversee a specific type of financial service as a single entity, but these services are no longer separate and distinct. Consequently, our regulatory institutions represent a fractured regulatory regime with divided responsibilities without a mechanism to see the big picture. As a result the regulatory institutions, individually or collectively, cannot monitor systemic risk in the financial services industry and are not in a position to prevent or mitigate negative impacts of financial crises on the economy.

Similarly, information technology for regulatory agencies has been designed around their stated regulatory responsibilities. Generally, each regulatory organization collects its own data and maintains its own technology platforms necessary to perform their regulatory function. Effective information sharing would provide the transparency and analysis necessary to effectively monitor the systemic risk in the financial system.

These disparate IT systems have created obstacles as financial services have evolved:

- Disparate and proprietary systems cannot be formed into a enterprise architecture to support a global, holistic regulatory framework
- Lack of standards for information management prevent agencies from effectively exchanging and utilizing other agencies' regulatory information
- Common tools and applications for processing and managing information across agencies are not available or effectively utilized
- Lack of security and data protection standards threaten the exchange and utilization of information across agencies

- Lack of flexible and open platforms slows innovation and broadening of knowledge, based on many years of regulatory reform and experience

Until these issues are addressed, information technology will inhibit rather than support a modern, unified and collaborative financial regulatory environment.

OPTIONS FOR IMPROVING FINANCIAL REGULATORY IT SYSTEMS

The options presented below can drive improvements in the financial regulatory environment.

Financial Industry Regulatory Model. *A Financial Industry Regulatory Model* must begin with underlying improvements in the governance structure for overseeing financial institutions. We believe there are three basic structural approaches that should be evaluated and considered.

1. Establishment of a Coordinating Office. This entity would oversee and coordinate implementation of the financial regulatory program across the multitude of agencies with current regulatory authority. This entity would also be responsible for identifying opportunities for organizational, process and technology improvements.
2. Consolidation of Federal Financial Institution Regulatory Agencies. This approach would consolidate existing organizations under a single roof. The leadership of this new agency would have responsibility for setting policy, directing implementation of the financial regulatory program and establishing holistic processes and systems.
3. Restructure Existing Regulatory Agencies along functional Lines. This approach would consolidate existing organizations under single reporting structures, where the leadership would be responsible for overseeing and directing programs along functional lines, such as safety and soundness; capital markets oversight, and market stability.

Additionally, a Financial Institutions Regulatory Enterprise Architecture is necessary to identify redundant capabilities and opportunities for synergy across the regulatory environment. It would provide regulators the ability to develop common processes and manage information systems holistically through common services, shared /consistent data, and joint collaboration and decision-making capabilities. Options include:

- Establish a new governance framework
- Develop regulatory enterprise target architecture
- Implement service oriented architecture into technology components
- Establish common interfaces and linking ability

The establishment of an Enterprise Architecture would allow for a more complete framework of the financial regulatory technologies. This would help support efforts performed across the entire regulatory environment, such as a comprehensive risk assessment of the financial services industry. It is imperative this model adhere to industry agreed upon standards,

guidance, tools, and technologies for developing service-oriented infrastructures and applications.

Establish a Service Oriented Architecture (SOA) for Agency Optimal Effectiveness. SOA is a technology approach that can rapidly respond to the affected agencies' changing information or application requirements. Rather than requiring that all data and logic reside within single applications on single platforms, the service-oriented regulatory model facilitates the leveraging of information and IT resources across (or even outside) the regulatory agencies. An automated regulatory function (such as receiving a bank call report) is a type of "service" in this model. Since services are designed to be independent and autonomous, they can be readily recombined into applications that aggregate data or enable decision processes which evolve according to an agency's changing needs. These composite or dynamic applications would allow agencies to orchestrate business processes in compliance with evolving policies, regulations, and legislation. The net result is that agencies adopting a service orientation gain agility. The Agencies can quickly update applications, change the way applications function, or deploy new capabilities as their circumstances and requirements evolve. Adhering to this type of framework and standards compliance will promote:

- **More productive applications.** A service-oriented approach will enable existing IT assets, including legacy systems and applications, to be more accessible, more productive, and more valuable to the organization.
- **Faster, more productive development.** Standards-based design will allow Agencies to create a repository of reusable services that can be quickly composed into applications. This lowers the cost of development and testing, reduces redundancy, and speeds time-to-deployment.
- **More manageable and secure applications.** Service-oriented solutions provide a common infrastructure (and documentation) for developing secure, monitored, and predictable applications. SOA makes it possible to map in new capabilities without disrupting operations. A SOA approach also enhances overall security for two important reasons. First, strong authentication and authorization are built into all services. Second, SOA services exist independently of one another which provides a resilient type of defense-in-depth between the components of a dynamic application.

Even if it were practical (or affordable), a "rip-and-replace" approach would be sub-optimal. It would eliminate technology improvements that inevitably come over time. Even today's "best-of-breed" solutions will become obsolete in the future. Locking into what's available now limits flexibility. Additionally, considerable business value remains in legacy systems and applications in the form of embedded domain knowledge. Eliminating those systems will erase decades of intellectual capital. For these and the evident reasons of cost and risk, SOA implementations must encompass legacy platforms.

Another factor that makes heterogeneity fundamental to SOA is that few service-oriented implementations are exclusively internal. An important reason for taking a SOA approach is to avoid redundancy and to leverage the investments others are making. Most SOA implementations will make use of externally hosted services, if only to access endpoints operated by vendors or other agencies.

Finally, SOA enables agencies to mix the software and development capabilities that give them the most mission value, with little or no penalty for integration. Certainly, some IT departments might want to limit the number of vendors and solutions in their portfolio but this should not be the sole force driving their architectural decisions. The vision of SOA is that mission requirements should drive portfolios, applications, systems, and infrastructure—not the other way around. In such an environment, the agencies *must* take advantage of best-in-class solutions (and providers) whenever it makes good technical and business sense. Therefore, encouraging and intelligently governing heterogeneity must be one overall goal of any SOA implementation.

Create a Data Architecture that is enhanced with unstructured financial data. Establishing a common data architecture will help ensure that that data can be accessed, communicated, and utilized by the community of financial regulatory agencies in a timely manner. Potential IT options include:

- Establishment of standard data elements to collect across the enterprise
- Develop a standardized ontology and taxonomy
- Create an enterprise / regulatory data warehouse
- Establish migration capability to migrate legacy data
- Establish a standard data language, e.g. XBRL
- Create a common vision for data stewardship and maintenance
- Create common operating platforms and data exchange standards
- Create an enterprise disaster recovery and data backup methods

Policy groups at the Treasury and Federal Reserve assess market conditions using statistical reports based on company reporting to economic survey (e.g. census survey) that are up to 12 months out of date. Data used to assess financial institution health must shift to more current unstructured financial data provided by banks.

Improving the data architecture of regulatory agencies will help ensure that regulators can effectively utilize the most current data available to oversee the financial industry, ensure compliance with evolving regulations, perform analyses to support the development of new regulations, and monitor the evolution of financial markets. These data could also be shared with the public and academic institution for greater transparency of the financial system.

Establish common systems and tools. Establishing common systems and tools across the regulatory environment will help integrate agencies towards a more unified regulatory environment. Options include:

- Create an automated workflow capability through COTS products (via a target architecture)
- Create real time collaboration and data sharing capabilities
- Develop integrated analytics
- Develop standard reporting mechanisms and leverage automated work flow and collaboration capabilities
- Create capability for ad hoc analytics and reporting by leveraging common data warehouse
- Implement a Federated approach utilizing a common business model and shared information staging areas as an iterative approach to quickly move toward aggregated data

The development of common systems and tools can help streamline processes and workflow as well as enable greater collaboration and analysis and reporting across the regulatory environment. For example, as banks are downgraded, the OCC could readily share the exam report with the FDIC to allow for early resolution strategy planning.

Security Architecture. As technologies are developed across the regulatory environment, the security around those technologies will need to be addressed. Threats and vulnerabilities will need to be assessed. A potential IT solution is to develop cross-regulatory architecture security standards and encryption methods. This will allow all agencies involved with the regulatory functions to streamline to one security platform, enabling interoperability while reducing the number of threats and vulnerabilities.

ROADMAP TO REFORM

In addition to exploring the options for improving IT systems addressed above, we recommend the following actions:

Provide Leadership in Development of a National Financial Risk Management Strategy
Through a collaborative process that includes the key constituencies – Government regulators, private sector finance, and IT industry leaders – a comprehensive "enterprise" risk assessment of the financial services industry should be performed to facilitate the development of a National Financial Risk Management Strategy. Such a strategy would drive a unified understanding of systemic risks in the system and common objectives to mitigate those risks.

The strategy should address IT innovation to level the playing field between the high level of IT sophistication in the financial markets and the low level of IT sophistication within the 1930's based regulatory environment, still somewhat pervasive in the current regulatory systems.

Visible presidential support will be critical to focus attention and to bring together key stakeholders. Presidential commitment can be best demonstrated by assigning the responsibility to a senior finance leader (e.g., Treasury) and senior IT leader (e.g, Government CIO) within the Executive Branch, with access to the President. These senior leaders must have the authority to work proactively with industry and influence regulators spending, and the ability to compel regulators to coordinate to achieve economic stability through sound regulation.

Enhance the tools and skills of the government regulators

The role of government regulators to ensure economic stability through sound regulation calls for expert technical, management and collaboration tools and skills. The government's National Financial Risk Management Strategy must specify the critical tools and skills needed to successfully implement this national strategy, and then offer the means to develop these tools and skills with urgency. The strategy should identify needed IT enabled tools to facilitate common analytical methods applicable across the financial services spectrum. This will help facilitate a uniform understanding of identifying and evaluating systemic risks, and as a result will lead to more effective regulation.

Drive change through inclusion and extend transparency to communities

The populace is a ripe source for ideas for improvement and innovation and can be an effective voice in contributing to the monitoring of financial markets. An IT enabled method for periodic sharing of accurate, relevant and standard data not only between financial organizations and their government regulators but also the general public could help foster an understanding of and adherence to certain fundamentals of basic financial management and logic. Policymakers and regulators should consider the possibilities of increasing open access to information for the public good.

ACKNOWLEDGEMENTS

Writing Team
Brien Lorenze, Deloitte
Olympia, Nguyen, Pragmatics
Paul Craig, CGI Federal
Tim Comello, KPMG
Shannon Fitzgerald, Booz Allen Hamilton
Ken Knueven, Microsoft
Joe Inqui, Pragmatics

Transition Study Group Leadership
Mark Forman (Chair), KPMG LLP
Roger Baker (Vice Chair)
Mary Ellen Condon, Booz Allen Hamilton
Judy Douglas, EDS, an HP Company
Dee Lee, Compusearch
Brien Lorenze, Deloitte
Leslie Steele, InterImage

ACT-IAC Staff
Kenneth Allen
Sarah Lindenau