Information Sharing and Financial Market Regulation: Understanding the Capability Gap

Djoko Sigit Sayogo
Center for Technology in Government
187 Wolf road, Suite 301
Albany, New York
dsayogo@ctg.albany.edu

Theresa A. Pardo
Center for Technology in Government
187 Wolf road, Suite 301
Albany, New York
tpardo@ctg.albany.edu

Peter Bloniarz
College of Computing & Information
University at Albany
Albany, New York
pbloniarz@albany.edu

ABSTRACT
In testimony on April of 2012 before the House Financial Services Committee, U.S. Securities and Exchange Commission (SEC) Chairman, Mary Schapiro, stated that effective information sharing between financial market actors and their regulatory bodies is critical to fulfilling the regulatory obligations of the SEC. The 2008 financial crisis is recognized as a show case for the risks to the stability of the markets that ineffective information sharing among supervisory authorities represents. This paper constitutes a preliminary exploration of the challenges facing financial regulators building on prior research in the computing and information science community (CIS). Current literature as well as data from a recent study of financial market regulation is used to identify key actors in financial market regulation information sharing relationships and to begin to outline the challenges faced in this unique context and the resulting risk if those challenges go unaddressed. A recently developed theoretical framework for cross-boundary information sharing (Garcia et al 2007) is used to present insights about challenges and risks from the literature and the field.

Categories and Subject Descriptors
K.4.1 [**Public Policy Issues**]: Information sharing for regulators.

General Terms
Management, Human Factors, Theory.

Keywords
Financial market regulators, systematic information sharing, challenges and risks assessment.

1. INTRODUCTION
Non-systematic and ad-hoc information sharing practices among financial market regulatory agencies are regarded as key contributors to the 2008 financial crisis. The economic crisis of 2008 is a case in point for how ineffective information sharing has hindered supervisory authorities from detecting vulnerabilities in global financial markets [24]. Unfortunately, the impact of constrained and ineffective information sharing on market regulation was well-known long before 2008. In a 2004 report the U.S. Government Accountability Office (GAO) called for the creation of routine and systematic fashion of information sharing across financial regulators [16] citing the vulnerabilities introduced as a consequence of gaps in these areas. Challenges at that time were recognized to include lack of authority, multiple overlapping jurisdictions, security and sensitivity of information, and protection of turf [16, 17, 30]. Since then researchers and practitioners alike have worked to understand and mitigate the challenges to routine and systematic information sharing in financial market regulation.

The criticality of effective information sharing to the monitoring of financial markets and the consequences of gaps in capability for effective information sharing is increasingly recognized by a range of national and international organizations. Each of these organizations is calling for specific and significant investments in the capability necessary to close the gaps in information available to and held by regulatory agencies. A statement from The Financial Stability Board to G-20 Finance Ministers and Central Bank Governors specifically addressed the need for a future focus on "information exchange standards in the financial regulatory and supervisory area" [15]. Testimony from the International Monetary Fund (IMF) in 2009 indicated the need for more information disclosure at a high level of granularity to cover the gap of information among supervisory regulators [24]. Cross-border cooperation and information sharing was among the ten recommendations of cross-border bank resolution of the Basel Committee on Banking Supervision reported by the Bank for International Settlements [1]. In her testimony on the Lehman Brothers Examiner's Report before House Financial Services Committee in April 2010, Chairman of the US Securities and Exchange Commission, Mary Schapiro called particular attention to the critical role of information sharing in meeting public expectations, "Effective information sharing by regulators is critical to fulfilling our regulatory obligations, and it is something that the American public has every right to expect. Cooperation and coordination with other financial institution regulators is essential [38]" Information exchange standards, more sharing of more detailed data, cross-border cooperation and information sharing are clearly recognized as necessary to ensure financial regulators meet public expectations.

Previous studies, such as Pardo et al [30] identify various challenges for financial market regulation. On the other hand, they did not specify the impact of the challenges to the different actors

ICEGOV2012, October 22–25, 2012, Albany, NY, United States, NY, USA, Copyright 2012 ACM 978-1-4503-1200-4/12/10…$15.00

of financial market regulation. Davenport and Prusak [5] define information sharing as "the voluntary act of making information available to others" [5]. Information sharing involves an exchange between an information holder and requester in the initial stage and information sender and receiver in the transfer stage. As a consequence of the above assertion, to understand information sharing, we need to identify those involved the sharing relationship, their role in the sharing process, and the challenges and risks faced by each actor.

This paper will draw on current literature on information sharing and integration as well as data about information sharing collected in interviws with inidividuals with a role in financial market regulation. Using this literature and data we identify a set of challenges facing systematic information sharing in financial market regulation. We map current actors in financial market regulation, specify their relationships to each other, and identify challenges and risks for each actor in financial market regulation information and knowledge sharing. Finally this paper lays out a foundation for future research in this area.

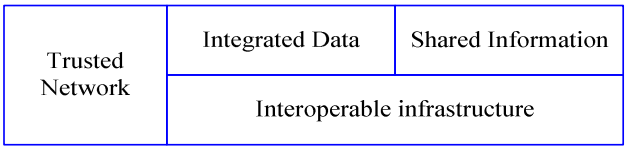
The paper begins by briefly describing inter-agency information integration and sharing and introducing the framework proposed by Gil-Garcia et al [20] as a lens to focus the discussion of the challenges. Section three describes the method used in this paper Followed by an introducing to the primary actors in financial market regulation information sharing. Section four focuses on the challenges facing financial market regulators in their efforts to share information. The paper concludes in section five a with discussion on financial market regulation challenges, actors and risks and epitomes a set of future directions for research on information sharing in FMR.

2. INFORMATION SHARING AND INTEGRATION

This paper uses the framework proposed by Gil-Garcia et al **[20]** to examine information sharing in FMR. This interagency information integration framework is useful for characterizing sharing activities and for focusing discussions of challenges to that sharing. Building from a close examination of interagency information sharing Gil-Garcia et al **[20]** conceptualize an integrative framework for constituting interorganizational information integration **[20]**. They argue for four components of interorganizational information sharing, namely: a) interoperable technical infrastructure, b) integrated data, c) shared information, and d) trusted social network.

Interoperability, as the first component, is regarded as the most critical element for systematic sharing or integration of information across different agencies [33]. Gil-Garcia et al [20] identified the importance of technical aspects of interoperability for both hardware and software. They argue that despite the technical difficulties in developing interoperability, an interoperable system will make sharing information easier and provide accurate, protected, and usable information [20].

Figure 1. Four Components Interagency Information Integration



Source: Gil-Garcia et al, 2010

As the second component, integrated data is critical for sharing information with multiple organizations particularly when it is required sharing of information in multiple formats [20]. Common data elements will significantly improve sharing and integrating of information across organizational boundaries [20].

The third component, shared information, is recognized as essential to supporting effective information sharing. Information sharing systems should be designed around an understanding of the shared information needed [20]. Sharing of information is regarded as an initial step toward integrated data [20]. The fourth component of interorganizational information integration is trusted social networks. Trust among sharing partners is considered a prerequisite to successful sharing [33]. A network of trusted actors significantly influences the effectiveness of communication and reduces resistance to sharing information [20]. The level of trust is important to reducing turf barriers and concern over information misuse.

3. APPROACH

The mapping of the literature on information sharing and integration draws on three sources; 1) Literature in interagency information sharing and integration 2).Professional reports on information sharing challenges in financial markets and 3) Article on the challenges facing 21st century financial market regulators detailing the result of interviews with a set of financial market regulation professionals published in E-Gov conference [30].

4. ACTORS AND CHALLENGES

4.1 Key Actors in Financial Market Regulation

Financial market regulation in the U.S. is fragmented with multiple actors responsible for regulating various segments of the financial industry [28, 30]. In some cases regulatory responsibility is overlapping resulting in a web of interconnections and intricate relationships which is then further complicated by informal and ad-hoc information sharing practices [28]. To begin to understand this actors and unpack the unique and overlapping regulatory responsibilities it is necessary to identify the key actors in the financial market regulation environment. We identify five actors, each with different roles and responsibilities and each is with important and unique relationships with other key actors and other stakeholders. These five key actors identified are federal agencies, state governments, SROs (self-regulatory organizations), financial industry entities (firms, investors, rating agencies), and the public.

Federal and state government agencies share responsibility for setting regulatory policy, enforcing compliance, supervising, and monitoring specific sectors of financial market activity. Federal

agencies act as primary regulating agencies for most financial products (securities, commodities, futures, and others) except insurance. State governments act as the supplementary regulating actor for the previously mentioned financial products. The State governments acts as the primary regulators for insurance [28] with each state have different regulations for insurance.

The US financial market regulation system is based on a combination of mandatory regulation sanctioned by government agencies and voluntary regulation, which in the case of financial markets, is sanctioned by the SROs (Self-Regulatory Agencies). SROs are self-regulating agencies that exercise some degree of regulatory authority over the financial market indistury and professionals One example of an SRO in the U.S. is FINRA (Financial Industry Regulatory Authority). FINRA is an independent regulator for securities firms listed and doing business in the U.S with the mission to protect America's investors [13]. To a certain extent, SROs are allowed to generate supplementary rules and policies [22]. For instance, FINRA is allowed to generate policies and rules for broker-dealer and trading markets. SROs serve to supplement the government regulation or fill the vacuum of an absence of government oversight and regulation.

Financial industry actors in this paper are those organizations conducting transactions in the financial market such as firms, investors, and rating agencies, among others. The interest of financial industry actors lies in the requirement for compliance with the regulatory framework. These organization need to comply and trade within the regulation imposed by the Federal, State and to certain extent the SROs. The public refers to the general public who have interest on the conduct of financial market regulations.

4.2 Challenges to FMR Information Sharing

The need for information sharing capability is not unique to the context of financial market regulation. Public health, human services, and public safety are just three of the many policy domains that require effective information sharing across boundaries of organizations and jurisdictions and across levels of government. And in each of these areas various communities of practitioners and academics work to more fully understand information sharing and the challenges facing those communities as they seek to effectively share information in the interest of program execution and policy development. Creating capability for routine and systematic information sharing has long been a priority for the U.S. Justice community, in particular. One of the most recent products of this focus is the National Information Exchange Model (NIEM), a national program supported by the federal government. NIEM represents an ongoing collaborative partnership of agencies and organizations across all levels of government (federal, state, tribal, and local) and with private industry for the purpose of effectively and efficiently sharing information at key decision points [26]. In recent years, NIEM has expanded to include other federal and state agencies such as the Office of the Director of National Intelligence, Federal Bureau of Investigation, Texas, Florida, New York, Pennsylvania, and others [26]. In addition to such nationally led efforts, many efforts at the state level are resulting in the creation of multi-agency, multi-jurisdictional information sharing capability. For example, in 2003 a New York State Criminal Justice Information Technology Group representing 13 different Justice agencies was tasked with developing a framework for a new approach to state-wide information sharing among criminal justice agencies [20]. Insights from these efforts and others are increasingly available in both the practitioner and academic literature as resources to inform and guide information sharing efforts in other domains. Likewise, this section identifies and integrates challenges from financial market regulation and interagency information sharing literature.

4.2.1 Interoperability as the Key

The application and implementation of any information technology is nested within a particular organizational, sociological, ideological and political context [7]. Successful cross-boundary information sharing requires understanding of the different and diverse business processes and practices within the actors' organizations and in the broader context within which they operate [7]. As argued by Pardo et al [35] interoperability not only depends on the ability of systems to communicate with one another, employing shared terminology and definitions, but also requires management and policy interoperability. An examination of information sharing in the criminal justice arena indicated that differences in agency culture is a significant barrier to inter-agency information sharing [33], and requires the identification, understanding and accommodation of existing organizational cultures within each agency [to enable successful sharing. In this context, interoperable management and policy is seen as necessary for each agency to reduce resistance to sharing information. An understanding of the critical role of interoperability in cross-boundary information sharing highlights the need to understand the social processes required to develop a shared understanding of terms, concepts and information used and available within each agency [7], particularly considering that information is not objective, neutral or readily available within each agency [36].

For organizations to work together to build interoperable systems to share information, organization leaders must first understand the information sharing capability found in each sharing partner. Information sharing capabilities are dynamic, varied, complementary and multi-dimensional in nature. Leaders must assess the capabilities held collectively by the network to ensure the relevancy and appropriateness of capability to become interoperable [29]. Within a broader view, these dimensions of capability can be classified into two closely related but distinct components [29, 34], namely capability to create effective collaboration and capability to develop new systems and procedures.

Capability to create effective collaboration includes five dimensions, namely: business model and architecture readiness, strategic planning, collaborative readiness, organization compatibility, and project management. Building capability along these dimensions is necessary to develop mutual understanding and to reduce resistance in information sharing and integration. Strategic planning is important for clarifying roles and responsibility among participants [32] and to alleviate resistance to change and incompatibility of technology [11]. Assessment of business models is necessary to describe service and operational components of the organization, their interrelationship, and the technology used for implementation [25]. Assessment of strategic planning, business model, and collaborative readiness will generate information to inform understanding of the extent to which potential sharing partners are incompatible. It also will inform and ideally, alleviate resistance and interorganizational

conflict around information sharing. Each organization must understand each other's missions, strategic planning and needs. To have this level of understanding, the agencies often engage in several types of collaborative activities, such as coordinated planning and training [34].

Capability to develop new systems and procedure is comprised of six dimensions, including: data assets and requirements, information policies, resource and project management, and technology readiness. Data assets and requirements and information policies assessment refers to assessments of the ability to provide and encourage sharing through wide-ranging, clear, and precise information policies and management [31]. This requirement includes data governance and policies; developing policies for data stewardship and use [8, 10]. This capability also relates to the management of resources owned by different agencies. Appropriate resource allocation and procurement strategies to support the interoperable system. The technology readiness consists of three elements, namely: technology acceptance, knowledge and compatibility. Technology acceptance refers to the attitudes of actors toward changes bring forth by technology, reflecting the comfort of actors in accepting a new technology or initiative, the degree of trust in the new technology, and the beliefs on the usability and success of technology or initiative [31]. Technology compatibility refers to the presence of agreed-upon standards, interconnectivity among those seeking to share information, and experience of staff with sharing activities [4].

4.2.2 Integrated Data

Two interrelated issues in the development of integrated data, namely: developing linked data and ensuring data integrity and quality, were identified through the literature review and field study.

a. Ensuring Data Quality and Integrity

Data has a central role in financial markets. Regulators as well as firms need data for a variety of reasons; not the least of which is to protect consumers. Consumer protection, like other uses regulators and firms make of the data available to them, requires data to be of high quality and integrity.

The process of ensuring that data from trading, surveillance and compliance activities is of sufficient quality for the specific or intended use can be a daunting task. Financial market data come from many organizations; broker-dealers, banks, and other sources, with many different data management cultures. Ensuring a high quality, integrated data infrastructure, including sophisticated data management strategies, represents a significant cost [30]. Monitoring the markets in the new environment of trading; with ever increasing transaction speeds and the production of vast amounts of data requires whole new classes of technology and a new approach to data management.

b. Developing Linked Data

Developing shared terminology and common definitions is one element of creating an interoperable system [27]. Daniel Tarullo's statement [40] in front of US Senate points at two important issues for better oversight mechanism in financial market 1) access to high-quality and timely data that are organized and standardized for supervisory agencies, and 2) the availability of data in appropriate usable form to other government agencies. His assertion implies data sharing will occur through standardization and linked data [40]. The November 2009 NRC (National Research Council) workshop describes the need for standard language development to enable data aggregation, interpretation, and analysis to support for controlling systematic risks [12]. Technically, the development of common language and schema through ontology will enable a linkage of different systems which would support more systematic and routine sharing. The ontology will enables the creation of "shared and common understanding of a domain that can be communicated between people and application systems [6]", and served as a language to support data translation and queries from different system design [23]. The development of common language facilitates automatic reasoning about financial systems and proposed regulations, sharing a common understanding of financial structures, and facilitating the analysis of interrelationship in financial domains. Effort toward developing linked data for financial market is already being invested in. For instance, O'Riain et al [27] proposing a linked data driven information systems for integrating financial data from multiple web sources. They further outline the challenges and issues in addressing data integration in financial market regulation, namely: a) an increase in data inter-dependencies, b) data quality and c) three different types of mismatch: text/data, schema, and abstraction level mismatch [27]. Despite growing research on ontologies for the financial domain, there is still a great need for a stronger and more focused connection between regulatory and systematic risk.

4.2.3 Challenges to Sharing Information

As argued by Gil-Garcia et al [20], sophisticated systems do not necessarily provide effective platforms for information sharing. Integrating and sharing information across different agencies is a difficult endeavor to undertake. For example, Agencies sometimes act defensively in protecting what they see as their own "turf"; which in this case is their data [21]. The challenges confronting agencies as they work to share their information with other entities range from political and managerial to technical. This section introduces some of these importance challenges.

a. Collaborative governance structure and sharing strategies

Agency resistance to sharing information is typically driven by a variety of reasons, such as to avoid additional costs related to changes, to control risks, to protect autonomy and adversarial position [21], and to shun "reputation risk", that is a risk of being relevant to the market and losing power over the market [30]. As a result, agencies need to enact strategies to reduce the risks of information sharing.

One of the strategies proposed by Pardo, Gil-Garcia and Burke [33] is through the development of an effective collaborative governance structure organized around the expectation that agencies will be sharing information. They further outline six determinants of an effective collaborative governance structure: 1) knowledge of information needs, 2) knowledge of the environment, 3) willingness to accommodate to the diversity of participating organizations and their goals, 4) knowledge about participating organizations, 5) existing legislation, and 6) executive involvement [33].

Developing information sharing and integration capability also requires leadership and legislative support [21]. To achieve interoperability across the boundaries of agencies, levels of

government, and even across national boundaries, requires leadership and authority from the most top levels of government. Because only the highest level of authority will enable the formation of secure strategic partnership, build comprehensive planning, secure necessary resources, and handle conflicting interests across different agencies to sustain the governance of multi-agencies network [34].

b. Lack of authority

Lack of legal authority to access information was a challenge faced by many state insurance regulators [16]. For instance, state insurance regulators do not have the authority to access the FBI's nationwide criminal history record. As a consequence, state insurance regulators have limited ability to prevent individuals with serious criminal records from entering the insurance business in their states. Inter-state migrations complicate the issue when individuals with serious criminal histories move around [16].

The lack of authority for access is magnified by fragmented regulatory structures which often overlap. Financial industry actors and insurance companies find themselves regulated by different institutions with different approaches to regulation. The fragmented structure creates two prominent challenges, a) duplication and overlap of regulation and b) competition among regulators to be the first to protect consumers and to appeal to the public [30, 37]. The overlap and competitiveness leads to redundancy and causes higher costs for firms and regulatory agencies. It also creates confusion for firms as they must choose which regulators to comply with. This situation also challenges regulators themselves as they work to understand how firms are operating within the multiple fragmented and overlapping systems of regulation [30, 37].

A proliferation of complex hybrid financial products increases complexity of authority questions and hinders the ability of regulators and consumers alike to identify and mitigate potential risks. The multiple jurisdictions governing the markets is recognized as not only obstructing the oversight of hybrid financial products, but also confusing consumers [16]. For instance, consumers might lodge a complaint about a hybrid product with wrong regulator and as a consequences the complaint is not properly resolved by the appropriate regulator. To complicate the matter, the lack of a central body facilitating information sharing or negotiating agreements about what information could and should be shared means that the appropriate regulator is often left in the dark [19]. The result is that regulators are left with limited views of issues in the financial market that impede their ability to deduce potential problems in the market.

c. Lack of enforcement action from the current sharing mechanism

The Memorandum of Understanding (MOU) is the primary mechanism used to establish information sharing agreements. However, the MOU has been criticized for a lack of enforceable actions which challenges the extent of sharing. The MOU was criticized for a high reliance on the "soft power of persuasion" and willingness to cooperate, instead of taking a coercive approach [3]. The effectiveness of an MOU largely depends on the "goodwill" of the counterparties signing the MOU. In addition, compliance with an MOU also depends on the underlying legal authority and jurisdictions of each party [14]. In a similar manner, multilateral arrangements across nations, as a form of MOU, were also criticized for the high information asymmetries resulting from differences in legal systems, supervisory arrangements, social and moral habit, and competition among financial centers for securities transactions [3, 14].

d. Legacy information systems impede the access

Different regulators maintain different and separate information systems and these different systems can significantly complicate routine information sharing. The integration of different legacy systems or the creation of interoperable system out of existing legacy systems becomes a major hurdle [30]. Different legacy systems result in systems that "don't talk to each other" and create various "gold copies" of data [30]. Gold copies refer to the different data captured at different levels, organizations, and formats. These gold copies pose challenges to data accuracy due to the different formats and metadata and affect the level of understanding about the data [30]. Considering that information is constructed from data, the problem with data accuracy could distort the resulting information and create major barriers for routine information sharing.

e. Protection of sensitive data and information

Financial regulators expressed their concern over the protection of sensitive data and information In particular, they expressed concerns about the need to balance inclinations to share and the need to protect different types of regulatory information with varying degree of sensitivity [16]. The legal structure previously installed to protect financial market consumers, such as the Bank Secrecy Acts, sometime prohibit the disclosure of certain information [19].

This concern is not a unique problem to financial market. Information security and protection are still major concerns in information sharing across different federal agencies. Looking at the case of sharing terrorism related information, shows a variety of weaknesses in the control of information security in federal agencies [17]. Based on the 2008 GAO report1, almost all 24 major federal agencies continue to have problems with access control and security management and about 20 federal agencies have issues with configuration management for information protection [17, 18]. Pardo et al [30] also pointed at the challenge of data protection in the financial market. To share information with various different agencies necessitate sufficient data protection. With much information that flows around, regulators need to ensure adequate protection of privacy and proprietary information. Systems to protect the data and information against intrusions exist but the problem lies on the protection of data and information privacy [30].

The development of information policies for information sharing and integration can be challenged by two factors, 1) the conflicting interest of multiple agencies and 2) the tension among security, privacy and sharing needs [30]. Each financial regulator governs particular financial segments based on their mission; these regulators intend to protect their autonomy and adversarial position that can sometimes conflict with other regulators. As previously discussed, information sharing requirements are sometimes hindered by the need to protect sensitive data and privacy rights. There is a conflicting issue between the need to use shared information with the need to protect the same information

[1] http://www.gao.gov/new.items/d09546.pdf

for being misused [9]. Dawes [9, 10] provides a useful framework for understanding information policies supporting information-based transparency initiative. Dawes proposed a balancing of two complimentary requirements in the framework, namely: information stewardship and information usefulness [8, 10]. Stewardship "conveys the idea that all public officials and government organizations are responsible for handling information with care and integrity, regardless of its original purpose or source [9, 380]". Using this lens, regulators must handle any information with care regardless of who the initiator or owner of the information is. This principle requires agencies to forgo their differences and could alleviate the concern of misuse. Information usefulness, on the other hand, refers to the principle that the information is beneficial. Making the information more accessible provides a wide variety of public and private uses [8, 10]. This framework of stewardship and usefulness provides useful guidance for financial regulators in developing policy management to support inter-regulators information sharing and integration. Policy management refers to the "way to express, analyze, and realize desired sharing system behavior [39].

4.2.4 Trusted Social Network

Systematic inter-organizational information sharing requires the creation of networks consisting of various different agencies and at different levels. A network might consist of organizations with overlapping business processes and non-standardized but similar information [35]. It might be populated by officials from various different agencies, each having different cultures, practices and rules to follows. The diversity of actors in this network could generate a range of potential conflicts of interest. Pardo et al [30] argued that managing conflict of interests among different regulatory agencies might be regarded at one of the primary challenges for 21st century financial market regulators.

There exists high competitiveness among different regulatory agencies, each strives to become or maintain their functional relevance to the market [30, 37]. Considering the high potential for conflict and power negotiation among different agencies involved in regulating financial markets, enacting trusted relationships becomes key element to ensuring systematic sharing. Trust within the network could change the way people work, communicate and share information hence trust becomes the "catalyst for information sharing [20]". Regardless, it seems, of the sophistication of system, communications and sharing still benefit from strong interpersonal capabilities.

5. CONNECTING FINANCIAL ACTORS, CHALLENGES, AND RISKS

Drawing on the analysis in the previous sections, we identify eight challenges to information sharing in financial market regulation resulting from fragmented regulatory structures in US financial markets (table 1). These include: 1) lack of authority for cross-jurisdictional products, 2) conflicting organizational cultures, 3) challenges due to data interdependency and legacy systems, and 4) the need for collaborative governance. In addition, four other challenges emerge as side effects of institutional responses to this fragmented structure, namely, a need 5) to develop linked data and a common language, 6) to protect sensitive data and information, 7) to develop necessary capabilities for existing information sharing and 8) to create more robust sharing mechanisms and policies.

The financial market regulatory structure in the U.S. is fragmented with different actors regulating different products. Considering the diversity of financial market stakeholders and their role and interest in the market, the identified challenges will affect different actors in the financial market differently. For each of these actors, the different impacts of these challenges represent the risks that need to be addressed by them. In this section, we correlate the identified challenges with the primary actors in financial market regulation and identify the risks associated with the challenges for each actor (table 1).

The risks that government (federal and state) and SROs face are comparable and include 1) having a limited ability to see built-up vulnerabilities in the market [21], 2) having resistance to change in order to maintain "turf" [16, 35], 3) hindering interoperability due to differences in metadata and data formats [25], and 4) competitiveness and conflicting interests among regulators [30]. The regulators might also need to invest in ensuring data quality, developing linked data, and assessing gaps in capabilities.

Although the risks faced by Federal and State regulators and the SROs are comparable, the magnitude of impact is oftentimes different. For instance, having limited ability to see built-up vulnerabilities could create a larger impact for Federal agencies compared to the SROs. The resulting risks could also affect the effectiveness of relationships among these regulators, especially considering that the sharing practices among most federal and state agencies are primarily informal and ad hoc [28]. For instance, federal agencies and state government could share trading information and be involved in joint enforcement coordination.

The risk of resistance to change in order to maintain turf and the risk of competing and conflicting interests could undermine their joint efforts to share. As example, the report by the GAO indicated how sharing between state and federal agencies, as illustrated by the case of state insurance regulators and the FBI, are sometimes not fruitful due to the lack of authority and jurisdictions. The state insurance regulators could not access the criminal record of an insurer in the FBI database and were thus unable to assess and prevent potential fraud [16].

For the actors in the financial market industry (trading firms, broker-dealer, rating agencies, investors, etc), these challenges also induce risks. The authority barriers and inadequate sharing mechanisms could create confusion for market actors in filing complaints or in identifying relevant information. The report by the GAO illustrates how difficult it is for consumers to lodge complaints on hybrid products due to the level of complexities and the intersectional and multilayered nature of financial markets [16]. The lack of coercive power on the current sharing mechanism among the regulatory agencies could also create an opportunity for irresponsible actors to gain advantage by manipulating the system [14].

As the previous GAO report indicates [16], an insurer who has a criminal record could manipulate the system by moving to other states and create a similar fraud because the state insurance agencies could not access the criminal record in the FBI databases. The barrier due to lack of authority and legacy systems could complicate the effort by the public to identify and access relevant information.

Table 1. Actors, Challenges and Risks

Challenges	Government	SROs	Fin. Industry Actors	Public
Mitigating authority barriers - Lack of authority and cross jurisdictions	Limited ability to identify built-up vulnerabilities [24]	Limited ability to identify built-up vulnerabilities [24]	Confusion in filing complaints	Confusion in identifying relevant information [18]
Accommodating different organizational cultures	Resistance to change brought forth by new systems [9, 35]	Resistance to change brought forth by new systems [9, 35]		
Legacy systems and data interdependency impede access	Different metadata and formats inhibit integration and interoperability. [27]	Different metadata and formats inhibit integration and interoperability [27]	Different reporting formats increase cost [30]	Multiple points of access [16]
Developing collaborative governance culture – involvement of high-level officials and political leaders	Conflicting interests among regulatory agencies – the competitiveness and risks of being relevant to the market [30]	Conflicting interests among regulatory agencies – the competitiveness and risks of being relevant to the market [30]		
Developing linked data and a common language - Ensuring data quality and integrity	Investment to ensure data quality in large datasets [30]	Investment to ensure data quality in large datasets [30]	Investment to ensure data quality for compliance [30]	Distortion due to low quality data.
Protection of sensitive data and information, balancing usefulness and stewardship	Liabilities of privacy and proprietary data and information [30]	Liabilities of privacy and proprietary data and information [30]	Liabilities of privacy and proprietary data and information [30]	Security of personal data
Lack of enforceable action for the current information sharing mechanism	Dependence on the "goodwill" of counterparties [3, 14]	Dependence on the "goodwill" of counterparties [3, 14]	Opportunities to manipulate the system	Higher vulnerability to fraud and exposures
Developing capabilities for collaboration and developing new procedures	Gaps in capabilities that hamper collaboration [34, 35]	Gaps in capabilities that hamper collaboration [34, 35]		

*) *Intersection of challenges and actors represents the risk*

The relationship between regulators and the public is maintained through two primary activities: 1) public access to information, and 2) requests for comments on new regulatory proposals [2]. Legacy systems and differing jurisdictions could result in the risk of multiple points of access [16], because the public has various points to access information. On the one hand, multiple points of access provide a wider range of information for the public to compare and contrast. On the other hand, multiple points of access could create confusion as to which information is most relevant for them. As result, despite the notable transparency effort by regulators to open up access to information and enhance the public consultative process, this condition will make the public, especially individual investors, more vulnerable to fraud and more exposed to losses. Their inability to identify relevant information could distort decisions that ordinary investors make regarding their investment.

The challenge of protecting sensitive data and ensuring data quality and integrity also creates significant risks for the financial industry and the public. The challenges of protecting sensitive data significantly correlate with the firm's investment in ensuring data quality, compliance and privacy protection. This condition creates a risk of protecting the security of the personal data and information for the general public. For public, this challenge correlates with the risk of breach in personal data and security of personal data. For financial industry, the challenge correlates to the risk of liabilities related to privacy and proprietary data. The financial industry might have to invest heavily to reduce the risk of liabilities due to personal data breach.

6. FUTURE DIRECTIONS

Through the review on literature in the interagency information sharing and integration, this paper provides an initial framework for understanding the challenges relating to inter-agency information sharing for financial market regulators, focusing primarily on the information flows between the different agents playing significant roles in the regulation of financial markets.

There are a number of other areas in which computer and information science research can help support this information and knowledge sharing, through analyses of the types of information and knowledge that should be shared between the actors. For example, better analytic tools could build on a formal specification of trading data and financial actors' behavior. High level languages for identifying patterns of interest (e.g., fraud signatures) in financial data streams should enable highly scalable, real-time analysis of data streams to support decision making. As another example, data mining approaches will be essential to detect patterns of activity that produce anomalous market behavior, such as the May 2010 "flash crash," or identify the possibility of manipulative or fraudulent practice that warrants further investigation. Predictive data mining could be useful for identifying impending market destabilization or manipulation and developing better "circuit breakers." Social network analysis could be used in combination with structured data to provide evidence of individuals or organizations engaged in inappropriate activities. Financial market professionals can get the information they need to support their high-stakes decision making. The ensuing research should lead to new models of computing, system design, and data analysis that can improve practices in this important and challenging domain.

7. REFERENCES

[1] BIS 2010. Good Practice Principles on Supervisory Colleges: Basel Committee on Banking Supervision.

[2] Bradley, C.M. 2011. Transparency Is the New Opacity: Constructing Financial Regulation After the Crisis. *American University Business Law Review*. 1, (2011), 7.

[3] Brummer, C. 2010. Post-American Securities Regulation. *California Law Review*. 98, (2010), 327–383.

[4] Cresswell, A. et al. 2008. A Multi-dimensional Approach to Digital Government Capability Assessment.

[5] Davenport, T.H. and Prusak, L. 1997. *Information ecology: Mastering the information and knowledge environment*. Oxford University Press, USA.

[6] Davies, J. et al. 2003. *Towards the Semantic Web: Ontology-driven Knowledge Management*. Wiley Online Library.

[7] Dawes, S.S. et al. 2009. From "Need to Know" to "Need to Share": Tangled Problems, Information Boundaries, and the Building of Public Sector Knowledge Networks. *Public Administration Review*. 69, 3 (May. 2009), 392–402.

[8] Dawes, S.S. 2010. Information policy meta-principles: stewardship and usefulness. (2010), 1–10.

[9] Dawes, S.S. 1996. Interagency information sharing: Expected benefits, manageable risks. *Journal of Policy Analysis and Management*. 15, 3 (1996), 377–394.

[10] Dawes, S.S. 2010. Stewardship and usefulness: Policy principles for information-based transparency. *Government Information Quarterly*. 27, 4 (2010), 377–383.

[11] Ding, W.W. et al. 2010. The impact of information technology on academic scientists' productivity and collaboration patterns. *Management Science*. 56, 9 (2010), 1439.

[12] Engle, R.F. and Weidman, S.T. 2010. *Technical Capabilities Necessary for Systemic Risk Regulation:Summary of a Workshop*. The National Academies Press.

[13] FINRA - About FINRA: *http://www.finra.org/AboutFINRA/*.

[14] Friedman, F.B. et al. 2003. Taking stock of information sharing in securities matters. *Journal of financial crime*. 10, 1 (2003), 37–53.

[15] FSB 2011. Global Adherence to Regulatory and Supervisory Standards on International Cooperation and Information Exchange.

[16] GAO 2004. *Better Information Sharing Among Financial Services Regulators Could Improve Protections for Consumers*. Technical Report #GAO-04-882R. Government Accountability Office (GAO).

[17] GAO 2009. *Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses*. Technical Report #GAO-09-546. Government Accountability Office (GAO).

[18] GAO 2012. *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements*. Technical Report #GAO-12-137. Government Accountability Office (GAO).

[19] GAO 1992. *Securities and Futures Markets: Cross-Border Information Sharing Is Improving, but Obstacles Remain*. Technical Report #GGD-92-110. Government Accountability Office (GAO).

[20] Gil-Garcia, J. et al. 2010. Conceptualizing Information Integration in Government. *E-Government: Information, Technology, and Transformation*. H.. Scholl, ed. M.E. Sharpe.

[21] Gil-Garcia, J. et al. 2005. Interorganizational Information Integration in the Criminal Justice Enterprise: Preliminary Lessons from State and County Initiatives. (Jan. 2005), 118c– 118c.

[22] Jasanoff, S. 2006. Transparency in Public Science: Purposes, Reasons, Limits. *Law and Contemporary Problems*. 69, (2006), 21–45.

[23] Lumsden, J. et al. 2011. Ontology Definition and Construction, and Epistemological Adequacy for Systems Interoperability: A Practitioner Analysis. *Journal of Information Science*. 37, 3 (Jun. 2011), 246–253.

[24] Manual on Fiscal Transparency, 2007 Revised Edition: *http://www.imf.org/external/np/fad/trans/manual.htm*. Accessed: 2012-04-22.

[25] Mayer, R.C. et al. 1995. An integrative model of organizational trust. *Academy of management review*. (1995), 709–734.

[26] National Information Exchange Model (NIEM): *https://www.niem.gov/Pages/default.aspx*.

[27] O'Riain, S. et al. 2012. Linked Data Driven Information Systems as an Enabler for Integrating Financial Data. *Information Systems for Global Financial Markets: Emerging Developments and Effects*. A.Y. Yap, ed. IGI Global. 239–269.

[28] Pan, E.J. 2009. Structural Reform of Financial Regulation.

[29] Pardo, T. et al. 2008. Collaborative governance and cross-boundary information sharing: Envisioning a networked and IT-enabled public administration. (2008), 5–7.

[30] Pardo, T. et al. 2011. Computing and information technology challenges for 21st century financial market regulators. (Delft, Netherland, 2011), 198–209.

[31] Pardo, T. et al. 2012. E-Government Interoperability Interaction of Policy, Management, and Technology Dimensions. *Social Science Computer Review*. 30, 1 (Feb. 2012), 7–23.

[32] Pardo, T. et al. 2004. Modelling the Social and Technical Processes of Interorganizational Information Integration. (Hawaii, 2004), 10.

[33] Pardo, T. et al. 2008. Sustainable Cross-Boundary Information Sharing. *Digital Government: E-Government Research, Case Studies, and Implementation*. H. Chen et al., eds. SpringerLink. 421–438.

[34] Pardo, T. and Burke, B. 2008. Government Worth Having: A Briefing on Interoperability for Government Leaders.

[35] Pardo, T. and Burke, B. 2008. Improving Government Interoperability: A Capability Framework for Government Managers.

[36] Radin, B. 2006. *Challenging the performance movement: Accountability, complexity, and democratic values*. Georgetown Univ Press.

[37] Sayogo, D.S. et al. 2011. Understanding the impact of computing and information technology on critical challenges facing 21st century financial market regulators. (Maryland, 2011), 345–346.

[38] Schapiro, M.L. 2010. Testimony Concerning the Lehman Brothers Examiner's Report Before the House Financial Services Committee.

[39] Smith, K. et al. 2008. Everybody share: The challenge of data-sharing systems. *Computer*. 41, 9 (2008), 54–61.

[40] Tarullo, D.K. 2010. Equipping financial regulators with the tools necessary to monitor systemic risk.