Managing Governance, Risk and Compliance for Post-Crisis Regulatory Change: A Model of IS Capabilities for Financial Organizations

Daniel Gozman
Henley Business School
daniel.gozman@gmail.com

Wendy Currie
Audencia Nantes
wendycurrie1@gmail.com

Abstract

The 2008-2009 financial crisis and related organizational and economic failures have meant that financial organizations are faced with a ‘tsunami’ of new regulatory obligations. This environment provides new managerial challenges as organizations are forced to engage in complex and costly remediation projects with short deadlines. Drawing from a longitudinal study conducted with nine financial institutions over twelve years, this paper identifies nine IS capabilities which underpin activities for managing regulatory themed governance, risk and compliance efforts. The research shows that many firms are now focused on meeting the Regulators’ deadlines at the expense of developing a strategic, enterprise-wide connected approach to compliance. Consequently, executives are in danger of implementing siloed compliance solutions within business functions. By evaluating the maturity of their IS capabilities which underpin regulatory adherence, managers have an opportunity to develop robust operational architectures and so are better positioned to face the challenges derived from shifting regulatory landscapes.

1. Introduction

The financial services industry is currently facing a ‘tsunami’ of regulations [1]. The financial crisis revealed that the failure of financial organizations, such as Lehman Brothers, creates significant systemic risk to our economy. In 2009, the G20 met in Pittsburgh and defined new measures aimed at preventing another financial crisis. Through legislation, both the USA and EU’s regulators aimed to meet the G20 commitment to strengthen regulatory systems. The EU’s response to the 2007 crisis and G20 agreements has been fragmented into several European Directives1. In contrast, the USA has opted to develop a single sweeping piece of legislation known as the Dodd-Frank Wall Street Reform and Consumer Protection Act, passed in 2010. The resultant organizational projects derived from these institutional changes are often referred to as Governance, Risk and Compliance (GRC) initiatives. This paper seeks to assist practitioners faced with large scale regulatory change to understand, identify and monitor key IS capabilities which underpin GRC activities, particularly within financial services. The rationale for the study is derived from the perspective that in the post-crisis environment regulators increasingly perceive robust IS as essential for adherence to increasingly complex regulatory environments underpinned by the timely provision of risk/compliance related information. Consequently, our study addresses the following research question: What are the IS capabilities which support regulatory focused post-crisis GRC activities in financial services organizations? Gartner describes GRC as, “neither a project nor a technology, but a corporate objective for improving governance through more effective compliance and a better understanding of the impact of risk on business performance.” [2 p.1]. However, the phrase is often used an as umbrella term to cover a plethora of issues ranging from business continuity to audit management in a diverse set of industries and contexts. Within the context of this paper the term is used to bring together complimentary objectives which collectively assist organizations to manage and meet regulatory obligations. A key role of the corporate governance function is to oversee the compliance and risk management departments and to ensure they are effective. Ultimately, meeting regulatory obligations is the responsibility of the board. The policies set by the organizations’ board and senior management will influence ‘the tone at the top’ and so influence the culture within the organization, which may contribute to regulatory outcomes. The term ‘risk’ within this

context refers to the management of four types of risk: liquidity risk, market risk, credit risk, and operational risk. These four categories are reflected in the Basel Committee on Banking Supervision’s global regulatory standards on capital adequacy and liquidity, and have been endorsed by the G20 leaders [3]. These standards, termed the Basel accords, have been implemented within the EU by the Capital Adequacy Directives [4]. Liquidity Risk focuses on the risk of loss through being unable to trade in a market or a product when required. Market Risk is the loss of earnings or capital which occur as a result in change in the value of financial products. Credit Risk is the loss caused by counterparties within financial transactions when they fail to pay financial obligations. Operational Risk is, “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.”[5 p.144]. This last category includes the subset of risks resulting from an organization’s inability to develop appropriate systems and practices for supporting GRC. The Securities Institute [6 p.5] advises that, “operational risk exists throughout the IS process, from strategic decisions about IS, to design implementation and maintenance” and that responsibilities of the firm’s IS function includes, “highlighting and managing deficiencies in the design or operation of all systems that support the firm’s activities [Including GRC]” Correspondingly, Mills [7 p.18] provides a useful definition of the compliance function. “In a financial services’ firm, Compliance is the function of identifying relevant legislative, regulatory and best practice requirements and implementing the necessary arrangements, systems and controls so as to facilitate adherence to these obligations.” A key responsibility of compliance functions is to encourage a culture which promotes ethical standards and the perspective that compliance behaviors are consistent with organizational success [7-9]. IS capabilities within an organization can be calibrated on a scale. The study draws from the theoretical basis outlined by The Software Engineering Institute’s (SEI) Capability Maturity Model (CMM) which focuses on defining five states of maturity for processes underpinned by software, as well as previous studies which have explored IS capabilities. Our study utilizes a contemporary definition of IS capabilities. They are a, “distinctive set of human-based skills, orientations, attitudes, motivations and behaviors that, when applied, can transform resources into specific business activities. Collections of capabilities, in turn, create high-level strategic competencies that positively influence business performance.” [10 p.178]. Examples of studies which have addressed the use of IS capabilities within specific business contexts include the outsourcing of financial organization’s back office functions [11], mergers and acquisitions, the impact on firm performance [12], competitive positioning [13] However, the literature lacks studies which address the capabilities underpinning those technologies facilitating post-crisis regulatory compliance. Our study not only seeks to identify the IS capabilities which underpin GRC activities but also to provide a high-level overview of each capabilities’ five levels of maturity. The SEI’s CMM defines maturity as, “the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective.”[14 p.4]. At one end of the scale of IS capabilities for GRC are a set of fragmented or loosely interconnected activities and technologies focused on risk, regulation and policy. At the other end of the scale, they may be conceptualized as an enterprise wide approach with the potential to improve governance through developing an in-depth understanding of risk and compliance on business performance. Building on SEI’s CMM model we define five states of maturity [14]. Table 1 outlines each of the IS capabilities identified in the study and a summary of the five maturity states for each capability.

<table>
<thead>
<tr>
<th>IS Capabilities</th>
<th>Initial</th>
<th>Controlled</th>
<th>Managed</th>
<th>Optimized</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>All-fac. automation</td>
<td>IS-oc. controls</td>
<td>Collaboration via business to automate controls</td>
<td>Variable automated controls</td>
<td>Level of control across multiple business units</td>
</tr>
<tr>
<td>Understanding ethical practice</td>
<td>The organization has little focus on ethics</td>
<td>IS systems provide training on ethical issues</td>
<td>Governance policies require behavior that reflects obligations</td>
<td>It supports the development and implementation of policies on ethics</td>
<td>IS activities are measured to ensure that standards are met and legally compliant</td>
</tr>
<tr>
<td>Monitoring and reporting GRC outcomes</td>
<td>Measuring, monitoring and reporting is done on an ad-hoc basis</td>
<td>Measuring, monitoring and reporting is done as a regular activity</td>
<td>The organization has clear understanding of compliance activities to be measured, monitored and reported</td>
<td>Measurement, monitoring and reporting of compliance activities is a part of regular business planning</td>
<td>The organization is able to offer data-dashboards</td>
</tr>
<tr>
<td>Data aggregation and management</td>
<td>Poor data quality creates unnecessary processes</td>
<td>Data availability and formatting does not hinder compliance</td>
<td>Data for compliance is managed centrally with Compliance and Governance oversight</td>
<td>Data sourcing is considered in the design of data systems</td>
<td>The organization is able to offer data-dashboards</td>
</tr>
<tr>
<td>Accessing GRC functionality</td>
<td>No roadmap</td>
<td>Gap identification</td>
<td>Develop key vendor relationships</td>
<td>Rigorous roadmap defined</td>
<td>Actively advise any vendors</td>
</tr>
<tr>
<td>Managing service providers</td>
<td>GRC is not considered when defining SLA and contracts with 3rd Parties</td>
<td>SLA are defined with a focus on meeting regulatory requirements with results being operationally measured</td>
<td>Outcomes relating to critical business activities that result in regulatory requirements being met and satisfied</td>
<td>Contracts and SLA agreements consider regulatory requirements, policies and compliance</td>
<td>Long-term third-party contracts are detailed and flexible enough to allow for changes to regulatory requirements</td>
</tr>
<tr>
<td>Determining basic practice</td>
<td>Organizations understand basic IS and do not collaborate to share best practices</td>
<td>Formalization of GRC standards and best practices become accepted</td>
<td>Organizations understand IS and GRC standards and best practices which are the best fit</td>
<td>The firm has developed, in-house validated standards and awareness of relevant standards</td>
<td>The organization collaborates with IS and GRC vendors and services and builds custom solutions organizations to deliver best practice</td>
</tr>
</tbody>
</table>
The booking structure relied saw a million of the eight capabilities categories assigned which allowed the identification interest. Common themes were identified and reviewed to determine points of importance and analysis, primary and secondary data were closely and then abstraction [15]. During the process of data identification of patterns, first through categorization was conducted through long established interpretive twelve year period from 2001-2013. Data analysis and seventy eight interviews were conducted over a managers, compliance managers, IS Managers, depth interviews were carried out with traders, risk regulatory compliance within financial institutions. Using a semi-structured interviewing technique, in-structure processes and workflows accordingly and to assign levels of authority to separate individuals conducting specific areas of business. Technology plays a pivotal role in preventing opportunities for market abuse by assuring that individuals do not have inappropriate access to processes and systems through which they may commit unauthorized transactions or sign off breaches. Specifically, organizations are required to segregate duties and apply controls to ensure that trades and compliance breaches are managed by appropriate personnel. Controls are needed to ensure clients’ trades are executed appropriately and to calculate asset exposures, risk levels and collateral values. IS allow the ability to audit controls and their outcomes and report compliant and non-compliant trades to regulators. A key decision to be made is where to automate and where to apply manual controls. We found that potential investors are becoming increasingly focused on the automated systems and processes used to achieve compliance to establish whether financial organizations have robust GRC practices. Automation ensures their investments will be compliant but are also maximized within the limits that regulatory rules stipulate. Thus, an automated process, less prone to human error, provides greater comfort. Manual controls are often applied through the use of spreadsheets. Regulatory bodies have applied hefty fines where manual controls have led to failures. In 2006, the UK Regulator fined Credit Suisse £5.6 million for ‘systems and controls failings’ stating, “The booking structure relied upon... was complex and overly reliant on large spreadsheets with multiple entries. This resulted in a lack of transparency and inhibited the effective supervision, risk management and control.” [16]. Thus, using spreadsheets exposes financial organizations to considerable risk. A senior compliance executive commented, ‘I saw a million pound breach at my old firm... it cost a million

Table 1. Maturity of IS capabilities for GRC

| 1. Initial – Capability is unrefined, chaotic and ad-hoc, performance varies and focuses on ‘firefighting’. Knowledge is unshared. |
| 2. Controlled – Capability is more coordinated and performance is becoming predictable. Inconsistencies in design exist. Evolution is reactive and problem driven. Knowledge silos are present. |
| 3. Managed – The capability is developed to the point where it is effective and easily managed, performance is predictable. Standards and best practice are adopted. Processes are consistent and knowledge sharing and collaboration occurs at the organization level. |
| 4. Optimized – The capability is efficient and is aligned with other capabilities and functions within the enterprise. There is a focus on proactiveness, continuous improvement and service delivery. Where appropriate, organizations share knowledge between one another. |
| 5. Innovative – The capability is innovated to create further value. The organization is seen as an exemplar of best practice within this area and is involved with developing new standards. Knowledge sharing and collaboration occur at the industry level. The capability may be sold as a service to other organizations. The following sections discuss the IS capabilities identified and each of its respective states of maturity. |

Each of the capabilities were derived from a study conducted with eight financial organizations and one IS vendor with results condensed into a maturity model for measuring and aligning IS capabilities for regulatory compliance within financial institutions. Using a semi-structured interviewing technique, in-depth interviews were carried out with traders, risk managers, compliance managers, IS Managers, CIO’s, CFO’s and consultants. In total one hundred and seventy eight interviews were conducted over a twelve year period from 2001-2013. Data analysis was conducted through long established interpretive techniques for analyzing data through the recursive identification of patterns, first through categorization and then abstraction [15]. During the process of data analysis, primary and secondary data were closely reviewed to determine points of importance and interest. Common themes were identified and categories assigned which allowed the identification of the eight capabilities considered. Each capability was further validated through further discussions with practitioners. This approach allowed us to identify key decision points and challenges that IS and GRC executives face in ensuring readiness for managing regulatory change within financial organizations.

2. Administering automated controls

Capital markets’ regulations require systems to impose structured controls on financial organizations’ activities to ensure that risk tolerances are adhered to and that regulatory obligations are met. Controls are essential, not only to set limits on volumes and concentrations of financial positions, but also to structure processes and workflows accordingly and to assign levels of authority to separate individuals conducting specific areas of business. Technology plays a pivotal role in preventing opportunities for market abuse by assuring that individuals do not have inappropriate access to processes and systems through which they may commit unauthorized transactions or sign off breaches. Specifically, organizations are required to segregate duties and apply controls to ensure that trades and compliance breaches are managed by appropriate personnel. Controls are needed to ensure clients’ trades are executed appropriately and to calculate asset exposures, risk levels and collateral values. IS allow the ability to audit controls and their outcomes and report compliant and non-compliant trades to regulators. A key decision to be made is where to automate and where to apply manual controls. We found that potential investors are becoming increasingly focused on the automated systems and processes used to achieve compliance to establish whether financial organizations have robust GRC practices. Automation ensures their investments will be compliant but are also maximized within the limits that regulatory rules stipulate. Thus, an automated process, less prone to human error, provides greater comfort. Manual controls are often applied through the use of spreadsheets. Regulatory bodies have applied hefty fines where manual controls have led to failures. In 2006, the UK Regulator fined Credit Suisse £5.6 million for ‘systems and controls failings’ stating, “The booking structure relied upon... was complex and overly reliant on large spreadsheets with multiple entries. This resulted in a lack of transparency and inhibited the effective supervision, risk management and control.” [16]. Thus, using spreadsheets exposes financial organizations to considerable risk. A senior compliance executive commented, ‘I saw a million pound breach at my old firm... it cost a million
pounds, because a spreadsheet was being used to monitor for compliance and it had a wrong formula in a cell.’ However, while ideally all controls would be automated to remove human error, changes in regulations may create gaps in systems and processes which, in the short term, need to be plugged by manual processes. Short deadlines for remediation of new regulatory obligations mean that systems’ vendors are often unable to provide updates to existing systems to incorporate necessary changes and so firms are forced to rely on manual processes until systems can be appropriately updated. This reliance on manual processes increases the likelihood of human error and regulatory breaches, with possible financial and reputational penalties. This is potentially a major issue given the scale of regulatory change in the wind. Furthermore, manual controls still play an important role. As the outputs of controls may change over time, there should exist an element of validation to check results through running manual and automated controls in parallel and comparing results.

2.1 States of maturity for administering controls

At the Initial state, control automation occurs on an ad-hoc basis depending on the systems’ owner and the business function where the control resides. As the firm moves towards a Controlled state, effort is made to decommission critical manual controls. Governance policies require the automation of critical controls, necessary to meet regulatory obligations and maintain risk tolerances. At the Managed state, IS and GRC professionals collaborate across the business to develop controls, which are structured in a consistent manner. Best practice for internal control, such as COSO² is observed. Controls are mapped to key policies and regulations. Systems are in place to monitor related outcomes. At the Optimized state greater emphasis is placed on monitoring manual controls focused on covering functional gaps, ensuring they become automated in later systems. Automated controls are validated with manual checks. At the Innovative state, organizations can demonstrate such a high level of control and an absence of breaches that the firm’s control structure becomes a sales or marketing tool to demonstrate robust compliance to potential clients.

3. Underpinning ethical practice

During the post-crisis period, regulators have become more vocal on the importance of ethical and cultural factors to ensure stable financial markets. Prior to the crisis, the UK Regulator has recognized that a fundamental disconnect existed between the values which financial organizations ascribed to in ethical codes of practices and the alignment of such values with employee actions. Despite acknowledging that firms often did not, “practice what they preach”, the Regulator refrained from specifying the type of culture a firm should have or the measures and metrics appropriate for assessing culture. Instead, the Regulator announced that it would focus on the outcomes that the culture delivers and whether the firm can demonstrate that it has a framework for assessing and maintaining cultural aspects [17]. Correspondingly, COSO’s Internal Control Framework suggests firms foster a Control Environment and that an ethical culture is the foundation for implementing effective internal controls. The Securities Institute also emphasizes the importance of culture in managing risk. They define a risk culture as one where the firm’s employee’s, “possess an understanding of and awareness of what risk is, where it occurs and how it can be managed.” [6 p.1]. Yet, the development of a compliance and risk focused culture may occur at the expense of innovation. Over time financial organizations may build up considerable capabilities to innovate at the product, service and technological levels, not least as a reaction to changeable markets and evolving regulatory environments. Prior to the crisis, managers may have fostered a culture which allowed departments to adapt as required. However, the recent focus on policy and compliance may dominate thinking and consequently repress innovation. If institutions lose the ability to take risks, because of an overt focus on governance and compliance, the firm’s ability to innovate may diminish. Furthermore, the costs of dealing with the current regulatory tsunami coupled with reduced profitability across the industry may mean that fewer funds are available for innovation. One GRC executive advised that an important aspect of fostering a balanced culture was the need for employees to be given recognition for acting ethically. However, the often championed ‘learning culture’, where blame is not applied to individuals, is in contrast with the essence of compliance which is to, “hold people responsible for their actions and behaviors”. A compliance executive noted that, in his opinion, organizations, “need to accept that compliance is quality” so that the attitude within sales for example is that, “a sale is
not a good sale unless it is a compliant sale”. However, if GRC is misunderstood there is a danger of a culture of overt control developing which may stifle innovation. Yet a GRC professional suggested that compliance could act as an aide to innovation by helping to, “find alternatives if problems exist” and that good compliance was about, “business protection not business prevention” and that, “if compliance is acting as a barrier, it is not performing its role properly.” One risk manager commented that a risk culture could have a positive effect on innovation by helping to, “identify new opportunities” and situations, “where risks were worth taking”.

3.1. States of maturity for underpinning ethical practice

At the Initial state, the organization has little focus on culture beyond focusing on the need to adhere to legal requirements. As it moves towards a Controlled state, IS systems facilitate training on ethical issues. Risk tolerances are communicated where appropriate by individual departments. At the Managed state, Governance policies require behaviors that reflect the organization’s risk tolerances and legal requirements. At the Optimized state, IS supports the development of regular training programs on ethics as well as regularly communicating expectations regarding risk and legal compliance. Confidential help-lines are provided for those with ethical dilemmas. At the Innovative state, a culture is developed where individuals are aware of the expectations placed on them with respect to ethics, risk and legal regulations. However, this culture is balanced by a culture which simultaneously supports innovation. GRC activities are welcomed and viewed as ensuring that new ideas are risk appropriate and legally compliant.

4. Monitoring and reporting GRC outcomes

The final IS capability relates to the need to measure and report GRC activities across the organization and also to report to markets and regulators. GRC visualization technologies allow the measurement, management and reporting of controls and risk tolerances associated with transactions. These are benchmarked against internal policies and regulatory requirements, as well as industry best practice and standards. Senior management, including the board, are required to monitor compliance and risk and so it is important that GRC tools are able to present data in a form which is understandable. A GRC consultant noted, “I think [GRC Reporting] is about looking at the data in appropriate ways, pulling out what are their key issues, articulating that in a way that’s appropriate for [senior management].” Examples of relevant approaches and tools include key performance indicators, frameworks and standards which define how to measure the efficiency of controls, approaches derived from communities of best practice and the adoption of systems, which report GRC outcomes. Ultimately, the measurement, monitoring and reporting of GRC activities enhances understanding of risk and so enables strategic thinking at both the business and IS levels. The corresponding role of IS, in enabling monitoring and reporting, is to draw from various systems to provide the necessary data and to collate it and present it in an appropriate format.

4.1. States of maturity for monitoring and reporting GRC outcomes

At the Initial state, measuring, monitoring and reporting is done on an ad-hoc basis by each individual business silo. Duplicate channels of communication exist. At the Controlled state, measuring, monitoring and reporting are instigated by specific problems or regulatory requirements. Reporting is coordinated but inconsistent in format and content. At the Managed state, the organization has a clear understanding of what compliance activities need to be measured, monitored and reported to which stakeholders. Consistent formatting and content is achieved for reports. At the Optimized state, channels of communication are streamlined. Measurement, monitoring and reporting of compliance activities enable strategic thinking at both the business and IS levels. Finally, at the Innovative state the firm collaborates with other organizations to determine industry standards for defining compliance metrics, monitoring processes and reporting structures.

5. Data aggregation and management

Following the financial crisis, the Regulator has been perceived as increasingly focusing on the robustness of systems and practices which support GRC activities. The management and aggregation of data underpins GRC efforts and has become an increasing issue. A senior compliance executive commented, “Now in the old days, pre-2008, when compliance didn’t really matter, when compliance
wasn’t an issue, people didn’t focus effort on data. Now... compliance is a prime driver of many of the things you do and is a prime constraint... So, the big push around compliance has meant there’s a big push around data quality.” The UK Regulator’s handbook requires that organizations must ensure that data is relevant, reliable and timely. An IS executive commented on the issues caused by poor data. “At every level data is a problem. Let’s give you a few examples. Number one, from the front office perspective, they may only care about fields A, B, C and D being required. But from a risk or compliance perspective, maybe you also care about fields E, F and G. So, initially, when the front office implements their systems, if they’re thinking on a Silo departmental basis, they don’t include that stuff or they don’t put the same rigor around ensuring its accuracy. I mean another point, maybe risk and compliance take their data cuts based on different time points, or they take their data based on slightly different data extraction queries, different SQL statements.” Often GRC activities require data sourced from external parties. Data such as market prices (snap shot and real-time), reference data (ratings and classifications), security issuer details and indexes and benchmarks may be provided by third parties. An increasing challenge for financial services companies is to be able to manage this data. An IS executive commented, “So you want all your data to line up and one of the ways of doing that is making sure that all the departments in the bank use the same source with a single version of the truth. So you want that for your external ratings data from the ratings agencies. You want that for instrument data. You want that for counterparty data. You want that for your pricing or market data. You want it for basically any grouping of reference data. Making your data line up makes it so much easier when you’re trying to meet cross-departmental regulatory requirements.” As a result, vendors of GRC systems have begun offering additional services to provide a single ‘scrubbed’ source of data aggregated from third party data vendors. In addition to data being aggregated from external sources, often internally derived data regarding the positions held by firms may need to be aggregated for compliance purposes in order to provide a holistic view across different trading desks in different offices. This presents similar challenges to those previously outlined, with the added complexity of integrating disparate systems often developed within separate department’s utilizing disparate technologies. This problem is likely to be amplified while organizations continue to adopt a siloed approach to GRC.

5.1. States of maturity for data aggregation and management

At the Initial state, no analysis of data availability or formatting is considered before designing GRC processes and controls. Lack of data awareness diminishes compliance activities and creates unnecessary manual processes. As the firm moves towards a Controlled state, data availability and formatting does not hinder compliance. Data is often sourced from numerous external providers with different formats. At the Managed state, data for compliance activities is managed centrally with clear IS Governance policies relating to external data providers and formats. Data sourcing and management underpins the design and implementation of effective and efficient controls. At the Optimized state data sourcing and formatting is considered at the design stage of GRC systems. Adopters of the same systems may compare approaches to data sourcing and management for remediation with particular regulatory requirements. At the Innovative state, data sourcing and management enables the design of more advanced controls which enable the business and enhances its risk management capabilities and so reduce regulatory capital. The organization is able to offer data feeds and consulting to organizations requiring similar types of data.

6. Sourcing GRC functionality

This capability refers to the need for IS and GRC professionals to source the functionality required to meet regulatory changes, by purchasing the necessary functionality from a vendor or by developing internal systems. Firms must develop a clear understanding of where new controls are needed and assess whether existing systems are sufficiently robust to ensure compliance. Each business area must be able to ensure risk tolerances and associated controls are defined and observed. Systems supporting GRC activities may need to be continually developed to keep pace with the organization’s changing regulatory exposure and dynamic business environment. The launch of new financial products and services may expose the organization to new regulatory obligations and correspondingly new controls and systems. In addition to utilizing systems which implement risk and compliance controls, organizations must also seek functionality which will monitor and report on GRC activities through the use of visualization tools such as dashboards.
Tight deadlines for adhering to new regulations are causing some organizations to procure systems instead of developing in-house solutions. A senior compliance executive noted, “If we develop in-house, we have the internal IS cost and all the rest of it, head count, that we need to bring in to do that. So we have to balance the cost of doing that and having the people on board and the on-going maintenance with paying a license fee and putting a package in place.” However, firms which have developed bespoke GRC systems may be able to leverage the use of such systems to provide an additional source of income. One compliance executive observed how this was the case within his firm, “I mean, sorry to say, in most investment management firms [compliance] is a cost center but here actually those compliance services can be sold to other entities that might want to use your compliance platform. So it can be sold, so it can be a profit center.” As GRC requirements change faster than systems, organizations may have to embrace bespoke development even on vendor supplied systems. Bespoke changes, however, may create difficulties when applying the vendor’s upgrades which were designed for ‘Vanilla’ implementations. Here, strong IS Leadership is required to lobby vendors for required changes in future updates. The study also revealed that the configuration of bespoke work flows is a complex and costly process which has led to companies adopting vendors’ pre-configured workflows. An IS consultant described an implementation he worked on, “There are some companies that have spent three years rolling out the software... Because they wanted their existing workflow to be mapped into [the system] and it cost them huge amounts of money Other big companies are now saying, ‘We now want [the Vendor] to tell us what is the best way of doing this particular trade.”

### 6.1. States of maturity for sourcing GRC functionality

In the Initial state, no compliance systems’ roadmap exists. Decisions are made by business silos on an ad-hoc basis. Many controls are manual. As the firms move towards a Controlled state an understanding is developed of what compliance related functionality is available and where gaps in functionality and opportunities to automate exist. This analysis feeds decision making for obtaining functionality. In a Managed state, the organization has knowledge of different vendor offerings and has built key relationships. Heavily regulated industries, such as financial services, consider compliance implications when evaluating new requirements and during the development cycle. At the Optimized state, a clear compliance systems’ roadmap is developed which is in alignment with the organization’s policies, appetite for risk, upcoming regulatory requirements and IS and business strategies. IS and GRC practices are integrated. At the Innovative state, organizations actively advise key vendors on opportunities for improvement and work with them to automate new requirements. GRC personnel are integrated with IS development teams. Compliance systems may be sold as a service.

### 7. Managing service providers

Firms are required to report all critical outsourcing arrangements to the regulator and to assess and manage risks associated with such arrangements. The post-crisis ‘tsunami’ of regulation has driven firms towards outsourcing to reduce costs and gain quick access to functionality. As a result, ‘captive’ outsourcing is becoming increasingly costly and so firms are beginning to move towards software as a service (SaaS) for the preferred model. Currently, regulators are perceived as increasingly focusing on how firms are managing third party service providers to ensure they are meeting regulatory obligations. When using third party suppliers, firms must ensure that they manage the risks associated with those firms appropriately, as ultimately responsibility to meet regulatory commitments is retained by the regulated organization. PwC notes, “Outsourcing has increased considerably in scale and complexity since 2007 when the UK Regulators’ rules for such activities first became mandatory for UK banks under SYSC [Senior Management Arrangements, Systems and Controls section in the Regulators’ handbook]. Although these rules remain unchanged, the implications for Recovery and Resolution Planning (RRP), resilient client service provision and reliable market operations ensure these developments have become an increasing concern for [UK Regulators] and their interpretation and enforcement of SYSC requirements has hardened.” [18 p.1]. Key issues include ensuring that outsourcing /offshoring contracts reflect the level of service required for supporting GRC activities and that the firm retains enough knowledge in-house to be able to determine if the service provider is meeting requirements. Contracts should address support, maintenance and customer service, timeframes, the ability to subcontract services, statements of disclosure to regulators and the financial organizations’ clients and crucially, compliance with laws and regulations. A key issue is being able to
maintain the confidentiality and security of information. For example, UK data protection laws prohibit personal data being moved outside of the EU. However, if confidential client information is provided to a third party service provider, perhaps through the cloud, the service provider and financial organization must be able to demonstrate that the information has not left the EU. E-discovery tools which audit enterprises’ structured and unstructured data to monitor data movement and the effectiveness of associate controls may be invaluable in this regard and firms may stipulate the frequent use of such tools to audit service providers, within outsourcing contracts.

7.1. States of maturity for managing service providers

At the Initial state, GRC is not considered when defining SLA and contracts with 3rd Parties. SLA and contracts may fulfill regulatory requirements but are not monitored on that basis. At the Controlled state, contracts are drafted with a view to meeting regulatory requirements with results being periodically monitored. Basic outsourcing and offshoring policies are defined. At the Managed state, outcomes relating to critical processes and regulatory requirements are regularly monitored and validated. Risk management informs offshoring and outsourcing decisions. At the Optimized state, contracts and SLA agreements consider regulatory requirements, policies and risk tolerances and are aligned with business and IS strategy. GRC systems enable SLA/contact definition and monitor the performance of related controls. Finally, at the Innovative state, long term third party contracts are detailed and flexible enough to allow for changes to the organization’s regulatory exposure and risk appetite.

8. Determining best practice

We found that organizations who engaged in sharing GRC practices through forums and communities of practice were better placed to manage complex areas of regulatory change. The study suggests that informal networks are especially useful for sharing approaches for dealing with new regulatory requirements. High performers with in-depth knowledge of a specific regulation or facet of risk may also contribute at the industry level, through associations with high-level bodies and may assist with the development of systems. Yet, many of the practitioners we interviewed revealed that they were increasingly confused by the plethora of frameworks and standards which touch on IS capabilities and GRC activities. A complete review of all the relevant frameworks and standards is beyond the remit of this paper. However, Figure 1 highlights some of the more well-known frameworks and contrasts their direct relevance to technology and GRC. For example, Prince 2 provides a useful framework for project management which may be utilized to manage complex remediation projects but has little direct orientation towards GRC or technology management. It is a generalist framework, parts of which may constitute useful best practice for GRC projects. COSO is a highly abstract conceptual framework focused on internal controls and does not specifically address IS. Consequently, organizations often look to supplement COSO with COBIT. COBIT provides organizations with reasonable assurance of their IS control structure and maps to the COSO framework. However, it lacks a specific focus on GRC for meeting wider regulatory obligations. While there is no silver bullet for GRC and IS management, all of these frameworks give organizations a running start and prevent them from reinventing the wheel. They all provide structure, incorporate best practice and facilitate knowledge sharing. Crucially, they are auditible and are well recognized by stakeholders, including shareholders and clients. Each organization’s individual GRC requirements will differ due to nuances in their business environment, product portfolio, resources, strategy and regulatory obligations. No single framework or standard provides an all-encompassing technology orientated, yet GRC focused solution. Thus, organizations may wish to review available standards and frameworks and then plan an approach that blends the best practices of each along with the needs of the organization. Early effort may be directed towards the standard or framework that is the best initial fit or where the firm lacks knowledge.

8.1. States of maturity for determining best practice

At the Initial state, organizations utilize few best practices standards and do not collaborate or interact with competitors to share best practice. At the Controlled state, firms borrow aspects of IS and GRC standards but do not become accredited. Different departmental silos may adopt different standards. At the Managed state, organizations understand the usefulness of established standards and select the ones which are the initial best fit with an aim to becoming accredited where appropriate. At the Optimized state, the firm has detailed understanding
of the strengths and weaknesses of relevant standards for best practice and cherry picks accordingly. Organizations collaborate on solving GRC issues with peers. At the Innovative state, organizations collaborate with GRC systems vendors and standards organizations to define best practice.

9. IS leadership

GRC projects are best steered by upper-middle management reporting into a high-level forum, whereby departmental heads could share ‘GRC stories’ and senior leadership may be updated on current progress and outstanding issues relating to implementing new regulatory requirements. GRC projects may involve staff with different expertise, as appropriate. A consultant commented, “The committee consists of our own compliance staff from across the business and we invite people from other areas as necessary... systems, risk, finance, front office.” As IS underpins GRC activities at every level, it is important that IS management is included in GRC forums and committees. IS management can contribute to GRC projects by clearly articulating the limitations and possibilities provided by existing systems, architectures, and data structures. Due to tight timeframes for remediation, IS management may be able to assist with managing GRC projects and ensuring that project deliverables and milestones are communicated and managed. IS leadership may contribute to evaluating the advantages and disadvantages of adopting different GRC standards and practices and provide insight into underlying and hidden IS costs. Strong CIO leadership is necessary to communicate with vendors and steer them towards developing their systems in alignment with the firm’s shifting regulatory obligations. Furthermore, financial organizations are increasingly required to demonstrate robust GRC practices to attract and retain clients. IS leadership may provide reassurance by demonstrating the robustness of cross-enterprise GRC systems and so assist sales and marketing activities.

9.1. States of maturity for IS leadership

At the Initial state, IS is rarely consulted during the planning of compliance efforts. Typically, IS is only consulted after breaches occur. At the Controlled state IS becomes involved in GRC activities after requirements have been defined. At the Managed state IS middle management works with other subject matter experts across the organization, to enable policy setting and risk management activities and remediation with regulatory requirements. IS governance policies for automated controls are defined. At the Optimized state, IS is represented on senior forums defining GRC strategies and committees formed to discuss related issues at the business function level. IS Strategy and GRC are aligned. The firm’s IS Governance competencies are highlighted by sales and marketing. At the Innovative state, the relationship between IS and GRC leadership is bi-lateral with compliance, risk and IS working together to develop strategic solutions for internal customers and to facilitate new products and services for external clients.

10. Prioritization and transitioning

The IS capabilities identified are felt to be mutually reinforcing and so collectively provide a basis by which financial organizations can benchmark and improve GRC activities. A firms’ ability to transition through the various maturity stages will depend on the resources available, as well as the competencies of related personal and the support of senior management. Broadly speaking, organizations will have to deploy resources for: training individuals, systems and data management, process definition and documentation as well as restructuring organizational forms.

Firms which find they have weak states of maturity (Initial or merely Controlled) for the ‘Administering automated controls’, ‘Monitoring and reporting GRC outcomes’ and ‘Underpinning ethical practice’ capabilities may wish to prioritize efforts to bring these capabilities to at least a ‘Managed’ state as these capabilities provide the foundations of strong regulatory compliance through facilitating controls, reporting and an appropriate culture. Without these elements organizations may well find themselves...
non-compliant. As a second tier of prioritization firms are recommended to address their data and how GRC functionality is sourced either internally or through third parties. Data and sourcing activities ultimately support the control, reporting and monitoring capabilities which act as the bedrock of GRC. Finally, the ‘IS leadership’ and ‘Selecting best practice’ capabilities support the other capabilities and have the potential ensure smoother deployment and greater efficiencies.

11. Concluding Comments

Technological developments have allowed regulators to make demands on organizations which previously were unrealistic. As technology has developed, more regular and accurate reporting of information has been made possible. Increased automation of controls provides further assurance that regulations are being adhered to and human errors diminished. A key lesson learnt is that organizations may increase the confidence of key stakeholders, not just regulators but also clients and shareholders, by defining policies and demonstrating robust risk and compliance management and a commitment to ethical standards. The post-crisis regulatory environment creates a paradox because short timeframes are forcing firms to focus on creating non-strategic compliance and risk solutions which meet deadlines but are less robust in the long term. At a time when budgets are being squeezed and trading across the industry is reduced, organizations are being required to pour resources into large scale change management programs driven by regulatory change. Pressures on resources are compounded by tight deadlines for implementation set by regulators and the resultant need to begin working on implementing the regulations before final drafts have been agreed. Uncertainty is creating an additional drain on organizations’ resources and so many organizations are focused on meeting compliance deadlines and not on developing a strategic, enterprise-wide approach to compliance. Consequently, managers are in danger of implementing siloed compliance solutions within business functions. By evaluating the maturity of underpinning IS capabilities and how GRC activities are assigned across the enterprise managers have an opportunity to develop sound GRC architectures which are robust and able to cope with ongoing complex change caused by evermore dynamic regulatory environments.

12. References