Crocodiles in the Regulatory Swamp: Navigating the Dangers of Outsourcing, SaaS and Shadow IT

Completed Research Paper

Daniel Gozman
Henley Business School
Whiteknights, Reading, UK
daniel.gozman@gmail.com

Leslie Willcocks
London School of Economics
Houghton Street, London, UK
l.p.willcocks@lse.ac.uk

Abstract

Corporates are entering the brave new world of the internet and digitization without much regard for the fine print of a growing regulation regime. More traditional outsourcing arrangements are already falling foul of the regulators as rules and supervision intensifies. Furthermore, ‘shadow IT’ is proliferating as the attractions of SaaS, mobile, cloud services, social media, and endless new ‘apps’ drive usage outside corporate IT. Initial cost-benefit analyses of the Cloud make such arrangements look immediately attractive but losing control of architecture, security, applications and deployment can have far reaching and damaging regulatory consequences. From research in financial services, this paper details the increasing body of regulations, their inherent risks for businesses and how the dangers can be pre-empted and managed. We then delineate a model for managing these risks specifically focused on investigating, strategizing and governing outsourcing arrangements and related regulatory obligations.

Keywords: Outsourcing, Cloud, IT Governance, SaaS, Security, Privacy, Regulation, Compliance, Financial Services, Shadow IT.
Introduction: Let the Corporates Beware

The extent to which organizations are impacted by regulations aimed at restricting, structuring and supervising outsourcing arrangements differs across countries and industries. Impacted sectors include financial services, insurance, telecoms, mining, trade unions and public services (Practical Law 2014). But almost all countries regulate financial services. The picture emerges of an increasingly unsympathetic set of regulators in the United States (USA), United Kingdom (UK) and European Union (EU) intensifying regulatory requirements and penalties, and much more willing to act. What are the regulators up to, what are the real risks, and how to handle them? Focusing on the Cloud and SaaS model as well as more traditional Information Technology Outsourcing (ITO) and Business Process Outsourcing (BPO) arrangements, we uncover multiple related risks embedded in shadow IT, financial and data privacy regulations and over-dependence on suppliers.

Currently, the financial sector is distinguished from other industries by the depth and breadth of regulatory changes being enacted globally as a result of the 2008 financial meltdown and resultant Great Recession (Fligstein and Habinek 2013; Ford 2010; Gillespie et al. 2012; Sants 2010; Simons 2009; Turner 2009). Subsequently, firms were faced with a ‘new normal’ of higher operational costs, derived from the need to meet a ‘tsunami’ of new regulatory rules whilst being subject to heightened levels of supervision, all at a time when margins were being greatly reduced (Ricketts 2013; The Economist 2012).

Financial Services, Outsourcing and Regulation

As a result many financial firms, particularly asset management houses, looked to outsourcing and offshoring models as a means to cut costs and make efficiencies (Currie and Gozman 2014; FCA 2012; FCA 2013a). As the industry came under pressure through evermore burdensome regulatory regimes, financial organizations increasingly relied on third parties and intra-group outsourcing arrangements to support operational activities deemed ‘critical’ by regulators. Increasingly, firms began adopting ITO and BPO and handing back office (custody and unit value accounting), middle (trade services, data management and record keeping) and even front office (client servicing and strategy formation) work to service providers in order to update underpinning technologies and reduce costs in an uncertain environment (Norton Rose Fulbright 2011). As a result of this increase in outsourcing activity, stemming partly from the desire to ease compliance and reduce related costs, regulatory bodies such as the OCC and FED (US) (FED 2013; SEC 2013) the BaFin (Germany) (Practical Law 2014) and the FCA and PRA (UK) (FCA 2014a; FCA 2014b; FCA 2015b) are focusing on the emergent risks resulting from this increasingly complex environment. They are intensifying their supervision of outsourcing arrangements, ironically creating further compliance headaches for financial organizations.

Currently, outsourcing arrangements are coming under increasing scrutiny with firms being required to fully account for these arrangements and ensure they are robustly managed (FCA 2012; FCA 2013a). Within the UK, the Regulator’s (FCA) handbook outlines both guidance and rules which regulated financial firms should adhere to. A subsection of their ‘High Level Standards’ focuses on Systems and Controls (SYSC 8) for outsourcing (FCA 2015b). Such rules require that firms have necessary oversight and governance of outsourcing arrangements and that proper risk assessments have been conducted. Firms are encouraged to keep regulators informed of changes in their outsourcing arrangements, so that regulatory authorities may also take a view of related risks and the appropriateness of the arrangement. The FCA handbook states, ‘when relying on a third party for the performance of operational functions which are critical for the performance of regulated activities, listed activities or ancillary services on a continuous and satisfactory basis, ensure that it takes reasonable steps to avoid undue additional operational risk.’ (FCA 2015b). The current UK and US rules prevent organizations from contracting out of their regulatory obligations. They ensure that where outsourcing takes place, the regulated financial organization ‘remains fully responsible for discharging all of its obligations under the regulatory system.’ (FCA 2015b). While these requirements are not new and have been in place since before the crisis, recent communications and enforcement actions from US and UK regulators point towards more stringent application of these rules (FCA 2013a; 2014; 2015b; FED 2013).

While the current FCA rules on outsourcing are being more strictly enforced, new regulations are also indirectly effecting outsourcing arrangements. For example, the upcoming EU Markets in Financial Instruments Directive and Regulation II (MiFID/R II) may create a further shift to outsourcing (EY...
A further example is the upcoming enhancements to EU data protection laws (which applies across all sectors) and which may impose much stricter limits on where and how personal data is stored. These changes are likely to further focus both regulators and practitioners, as fines may potentially increase from tens of thousands of pounds currently to up to 5% of a firm’s annual worldwide turnover, or €100m, with the possibility for individuals and associations also to bring claims for non-compliance (Long, 2013).

Cloud, SaaS and Shadow IT

More intensive regulatory supervision of outsourcing is occurring at a time when innovative technology solutions are more readily available through the Cloud and Software as a Service (SaaS) models. Our study shows that many financial firms are increasingly viewing traditional ITO arrangements as expensive and inefficient when compared to the cost of Cloud based infrastructures, platforms and applications. Yet regulatory hurdles may prevent financial organizations leveraging innovative cloud based solutions. The attraction of SaaS is the ease and speed by which applications can be deployed and the ease of access to these applications anywhere where an internet connection and browser is available. Low subscription and maintenance costs are also important advantages of this outsourcing model. However, it is these qualities which obscure a clear understanding of the scope of applications contributing to regulated practices. As SaaS applications are so quick, cheap and easy to deploy they may be adopted without adhering to IT governance best practice, thereby creating additional operational and regulatory risks. Individuals under pressure to increase productivity with less resources and to deliver results quickly to pressing deadlines, no longer need to wait for IT departments to complete cumbersome and bureaucratic IT procurement, provisioning, testing and security processes. Instead a solution for quickly sharing information and data can be found through a cheap and cheerful SaaS offering which is only a credit card, a browser and a few clicks away. Pressurized individuals are also more likely to ignore existing policies and procedures in their rush to meet deadlines and targets.

Financial services outsourcing regulatory requirements may, on the surface, seem relevant to more traditional process-driven outsourcing arrangements. But regulated firms may still face further difficulties if its service providers’ employees use SaaS applications which impact on its compliance obligations, service provision or breach data protection. The obligations to monitor outsourcing providers may create new data discovery challenges. For example, how can firms monitor and be assured that their outsourcing providers’ employees haven’t utilized SaaS applications and moved crucial elements of customer data outside the EAA (for example into India or China) where the app is hosted. Where individuals are using shadow SaaS apps and uploading personal data without the firm’s knowledge, serious breaches may occur. Yet those signing up for SaaS applications may have little knowledge or care as to where the application is hosted or if the location changes. Social media and marketing apps. are particularly high risk on potential data breaches. So, while SaaS is often touted as allowing organization to cease worrying about managing and maintaining IT infrastructures, organization must still understand their vendors’ technical architectures to ensure data privacy rules and regulations are adhered to. The evolving technological and regulatory landscape provides challenges for financial firms who must keep pace with innovative outsourcing arrangements and technologies. A perpetual challenge exists in understanding the implications of firms using third parties to reduce costs access latest technologies either through SaaS or ITO/BPO.

Do Existing Studies and Industry Guidance Help?

Despite these important shifts, scholarly work on outsourcing has largely neglected the impact of financial regulation. Reviews of outsourcing work providing an otherwise comprehensive perspective of future avenues of research omit the impact of regulation on such arrangements (Hätönen and Eriksson 2009; Lacity et al. 2010). Yet studies of outsourcing within financial services (Clark and Monk 2013; Currie et al. 2008; Jennings 1996; Qin et al. 2012) and insurance (Ben-Shahar and Logue 2012; Herz et al. 2012; Rezac and Rezac 2013) are more common, while related studies have focused on Cloud security (Jamil and Zaki 2011; Pearson and Yee 2012; Shaikh and Haider 2011) and privacy (Ion et al. 2011; Wang 2011). Studies addressing regulation of the Cloud are also scarce. Notable exceptions focus on regulation of trans-border health data (Seddon and Currie 2013) and telecoms regulation, (Cave et al. 2012).
In summary, the convergence of traditional and cloud based outsourcing arrangements and their relationship with financial services and privacy regulation has been largely neglected by the academic community. Conversely, the practitioner community, specifically consultancies, law firms, ‘Big Four’ accountants as well as regulatory agencies have been forthcoming in highlighting related issues in previous years (Accenture 2012; FCA 2012; FCA 2013a; FCA 2014a; FCA 2014b; FED 2013; KPMG 2009; Norton Rose Fulbright 2011; PwC 2014; SEC 2013). However, our studies also show that there is still widespread lack of practitioner knowledge of such regulation and sources. Therefore, one major motivation for this study is to inform practitioner stakeholders - lawyers, policy makers, regulated firms and vendors, as well as the academic community - about current regulations of outsourcing and IT activities in financial services.

This paper outlines how an assemblage of factors including increasing focus by regulators on outsourcing arrangements, the pervasiveness of mobile technologies, the Cloud and the corresponding spread of shadow IT arrangements are creating new risks and challenges. Those firms which can overcome these hurdles may harness considerable benefits through cost savings and access to robust technological infrastructures and disruptive new applications. Yet the adoption of these practices comes with considerable risk where such arrangements are not properly managed and aligned with the regulators’ expectations. Our aim is to understand and evaluate how financial organizations are responding to these new challenges and to distil the experiences and findings into a framework to enable organizations to manage this increasingly complex yet crucial area. Specifically, the study seeks to answer two interrelated questions:

- What are the contemporary challenges, risks and opportunities within the new post financial crisis regulatory environment?
- How can the identified risks be managed and mitigated and opportunities leveraged?

The paper firstly outlines the systematic approach we employed in collecting and analyzing our data. The following section outlines the challenges, risks and opportunities the study revealed. Drawing from this analysis and our findings, we delineate a framework for managing outsourcing regulations. Finally, we provide some concluding remarks and suggest avenues for future research.

**Research Method**

**Data Collection**

Our method for primary data collection involved interviewing a differentiated range of stakeholders including lawyers, technologists, compliance executives and outsourcing managers (Miles and Huberman 1994; Silverman 2001). To gain deep insights into the operational effects and processes of outsourcing regulations we carried out field-work across 14 organizations. Our objective was to elicit views and comments from interviewees engaged in the adoption and implementation of outsourcing practices deemed critical by the UK Regulator. Participant organizations included two SaaS and two BPO and two ITO vendors, two law firms focused on providing advice on outsourcing contracts and regulation, two ‘Big Four’ Auditing and Consulting Firms engaged in providing advisory services to firms impacted by outsourcing regulations and eight regulated financial institutions. In total, 39 interviews were conducted from 2013-2015. All interviews were transcribed and managed by NVivo software. Table 1 summarizes the data sources employed.

Semi-structured interviews were adopted, as such an approach has previously proved effective in providing the necessary depth and flexibility required to explore complex and dynamic regulatory phenomena (Gozman and Currie 2013; Gozman et al. 2014; Tsatsou et al. 2009). The semi-structured approach allowed us flexibility to pursue new topics as the discussion evolved and also as responses to shifts in the UK Regulator’s position emerged and became better defined (Kvale and Brinkmann 2009; Punch 2005). Yet emphasis remained on the interviewer to frame what was important in understanding the behaviors, events and patterns related to the research topic (Bryman 2008). A separate interview guide was designed for each organization and job role. While each of the question guides addressed the same high level topics, it was felt that the specifics of each question could be best tailored to the role of the individuals being interviewed. This approach allowed us to ensure we were directing questions appropriately to the interviewees’ domain of expertise. For example, we avoided
asking IT experts to comment on detailed legal/regulatory matters and lawyers to comment on the nuances of specific technologies and related practices. Furthermore, as the legal domains under consideration (outsourcing contracts and regulation) were also distinct areas we ensured that questions were tailored to the specific area of law the interviewee was practicing.

<table>
<thead>
<tr>
<th>Primary Data Collection (39 Interviews)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Law Firms</td>
</tr>
<tr>
<td>Regulation Lawyers</td>
</tr>
<tr>
<td>Outsourcing Contracts Lawyers</td>
</tr>
<tr>
<td>Departmental Heads</td>
</tr>
<tr>
<td>Process Owners</td>
</tr>
<tr>
<td>Compliance/Risk Executives</td>
</tr>
<tr>
<td>IT Professionals</td>
</tr>
<tr>
<td>Vendor Consultants</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secondary Data Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS/BPO Vendor Manuals</td>
</tr>
</tbody>
</table>

**Table 1. Data Sources**

At the end of each interview time was allocated to reflect on the answers and update the question guide. Updates to the guide were not based solely on interview responses but also on shifting environmental conditions, including emerging responses to outsourcing failures and regulations. The identification of such environmental factors was also derived through analysis of secondary data including regulations, press releases and white papers from regulatory bodies, as well as industry commentary by the business press, accounting and legal professions.

Understanding the complex regulatory landscape and related emerging challenges and risk was further developed though one author’s role as an ‘Academic Advisor’ to a London based law firm and management consultancy engaged in advising SaaS vendors, ITO/BPO vendors (sellers) and financial institutions (buyers) on regulatory and contractual matters specifically relating to outsourcing arrangements and practices. In this capacity, the researcher attended relevant meetings with the firms’ existing and potential clients as well as internal strategy meetings with consultants and lawyers to discuss the current environment and related responses and advisory offerings. Overall, the participant observation element of the research study enhanced the study by providing understanding of key underlying environmental constructs (Becker 1958; DeWalt and DeWalt 2010; Schwartz and Schwartz 1955). As part of the Academic Advisor role, detailed notes were taken after each meeting (Sanjek 1990). These were reviewed prior to subsequent meetings so that future interactions could bridge gaps in understanding and identify areas where data was incomplete. These notes were considered alongside relevant email exchanges between the researcher, the law firms’ consultants and lawyers and their clients (Sanjek 1990). However, we should acknowledge that records of meetings, observations and informal interviews and discussions are constructed by the researcher and so have an inherent and inevitable bias (DeWalt and DeWalt 2010). However, few anthropologists believe that their research is unbiased or that eliminating bias is possible or even desirable (DeWalt and DeWalt 2010; Drury and Stott 2001). A process of triangulation reduced the potential for misleading results as key constructs derived from field notes were considered against secondary data sources as well as interview transcription (Flick 1998; Seale 1999).
**Sampling Strategy**

The study adopts 'purposive sampling', which allows researchers to 'seek out groups, settings and individuals where... the processes being studied are most likely to occur.' (Denzin and Lincoln 2000 p.370). This sampling strategy required a search for information-rich cases which were illustrative of how outsourcing regulations were being interpreted and managed within the financial service industry (Patton 1990). The vendors were selected as being market leading providers of SaaS and ITO/BPO offerings, whose customer base included large global financial organizations. Sampling criteria for selecting financial institutions also focused on identifying firms impacted by the regulations. Those considered included organizations which had comparable outsourcing arrangements and so had a similar level of regulatory exposure. The legal consulting and auditing firms were selected on the basis that they explicitly advertised themselves as being focused on providing expertise within this space through webinars, roundtables and publication of white papers.

**Data Analysis**

Data analysis was conducted through long established interpretive techniques for analyzing data through the recursive identification of patterns, first through categorization and then abstraction (Gibbs 2007; Guest et al. 2012; Miles and Huberman 1994; Saldana 2009; Silverman 2001; Spiggle 1994; Symon and Cassell 2012). 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. Thus, long interviews were simplified through the adoption of simple categories (Punch 2005).

The analysis adopted a two cycle approach to coding. The first cycle adopted a ‘Descriptive Coding’ approach for summarizing segments of data. This method is appropriate for inductive studies utilizing semi-structured protocols (Saldana 2009). This approach requires the application of a content phrase to a segment of data representing a topic of inquiry and so related to the risks and challenges being faced and related mitigation practices. For example, ‘Tensions in Data Privacy Regulations’ or ‘Tensions in SaaS Adoption.’

The second cycle adopted a ‘Pattern Coding’ approach to identify major themes by searching for causes and explanations from the data. Such an approach builds on the first cycle of analysis and are, ‘explanatory or inferential codes, ones that identify an emergent theme, configuration or explanation. They pull together a lot of material into more meaningful and parsimonious unit of analysis’ (Miles & Huberman, 1994 p.69). As a result, these codes were orientated towards the outsourcing practices firms’ employed. Examples include, ‘Requiring Transparency’, ‘Reducing IT Overheads’ and ‘Conducting a Review.’ By coding against major themes in the first cycle and then against more granular explanatory patterns in the second, we were able to draw out not only high-level challenges and risks but also related operational practices aimed to mitigate them. Consequently, the coding approach we adopted enabled us to address the two research questions.

Typically, interviewees were re-contacted during transcription and analysis in order to provide clarification on key issues. Scope, depth and consistency were achieved by discussing key concepts, constructs and terminology with each of the informants and triangulating the findings across primary and secondary data sources (Flick 1998; Seale 1999). For example, interviewee references to particular areas of regulation were triangulated with the original regulations and industry commentary to ensure key points were fully understood and consistent across sources.
Entering The Swamp: Seven Challenges

In this section we relate sourcing trends in financial services to the risks they engender relative to the growing regulatory regime. We identify seven potential 'crocodiles' in the 'swamp' of trends, practices and regulations and employ this metaphor to illustrate how the challenges and issues we studied are creating hidden and unseen risks which potentially lie in wait for practitioners. The first is the pervasive spread of SaaS, mobile technologies and Bring Your Own Device (BYOD) that is changing the sourcing landscape, yet creating lack of visibility and control over the IT estate. This challenge is foundational and underpins the further challenges identified. The second streams from growing multi-regional data privacy requirements and SaaS architectures. The third relates to the reliability and likely longevity of SaaS suppliers. The fourth concerns the stringent requirements for monitoring and auditing general outsourcing arrangements. The fifth focuses on 'Intra-Group Outsourcing.' The sixth 'crocodile' laying in wait emerges from constantly shifting regulatory landscapes. The seventh sees disruptive new technologies possessing inherent regulatory risks for businesses. These challenges are interrelated and not mutually exclusive and so collectively may combine to form specific risk patterns with increasingly severe consequences for firms and individuals. For example, a SaaS vendor who ceases to operate suddenly (Challenge #3) may disrupt business critical processes while also creating difficulties in managing data security and privacy (Challenge #2), all of which may be even more problematic if the firm's compliance, IT department and regulator were unaware of the relationship (Challenge #1).

1. Lack of Visibility and Control of the IT Estate

The first challenge relates to ensuring that compliance and IT managers have a transparent and holistic view of the organization's outsourcing arrangements in order to be able to accurately control and report on such practices, both internally and to regulators. The Cloud has allowed quick access to applications on a flexible low-cost subscription basis which can be almost instantly deployed, while the popularity of Bring Your Own Device (BYOD) and the widespread adoption of mobile technologies have also underpinned the growth of SaaS arrangements. Consequently, this challenge is further complicated by the pervasive use of SaaS and mobile technologies. Following the financial crisis, organizations of all sizes have seen their margins cut and consequently been driven towards cost cutting exercises. As austerity measures bite, employees have been driven to 'do more with less'. Correspondingly, often the use of SaaS has developed through the 'freemium' model where the initial use of the application is free and users pay for additional capabilities. Such applications can easily be configured to import corporate data or integrate with other corporate applications and be done without the approval or even knowledge of the IT department or compliance teams. Through such shadow arrangements employees in highly regulated industries may unwittingly set up 'critical' outsourcing arrangements. Even where firms do have a complete picture of all SaaS arrangements, a breach occur the regulator may decide that SaaS applications that were not deemed as critical by the firm in fact were(!). For example, social media applications may be deemed critical, in retrospect, as they record, manage and evidence behaviors and actions which may be called into question at a later date.

As a case in point, if social media platforms are used to share personal data or important documents such applications may be seen as integral to the firm's operational environment. Marketing applications may be seen as critical where such applications are implicated in investigations of mis-selling and failure to treat customers fairly (see Stonebridge case study in Challenge #4). In fact, business productivity, file sharing and storage social media, marketing and data analytics applications (which naturally utilize customer and employee data and may impact operational effectiveness) account for a considerable proportion of shadow IT, according to an executive report sponsored by MacAfee in 2013 (Stratecast 2013).

Traditionally, firms’ IT departments have closely controlled the software and hardware which individuals use in their day-to-day work and so had clear visibility of related third party relationships. However, through the SaaS model, employees may easily circumvent corporate IT who may remain blissfully ignorant that arrangements have been set up. For example, individuals or departments may quickly create new SaaS arrangements and then use such software to deliver business critical processes and/or manage personal data. In doing so, they create a critical outsourcing arrangement which may be hidden from the firm's compliance department and regulators. As the firm is unaware of this new arrangement they may (a) not report it to the regulator, (b) not be aware of the IT and operational risks inherent to the arrangement (c) monitor it all of which may cause the firm to be in breach of the SYSC rules (FCA 2015b) and reduce their ability to consolidate license agreements and

Thirty Sixth International Conference on Information Systems, Fort Worth 2015
make related savings. For example, one of our participant CIOs only became aware of the extent to which his firm was exposed to a SaaS provider when he was sent an email suggesting he buy a corporate license due to the high number of colleagues using the product. Furthermore, once users upload data into SaaS applications they surrender control of how and where the data is stored and located and if and where it is moved to in the future. This may be particularly problematic where personal data is being uploaded. If the SaaS arrangement has caused personal data to be lost or held outside of the stipulated jurisdiction (e.g. the EU) then data privacy laws may also have been breached but without the knowledge of the firm. Recently, regulators have taken a dim view of organizations which have only identified and reported data breaches far down the line long after they occurred (FSA 2010).

A key finding is that lack of visibility and control over SaaS arrangements is at the center of the regulatory dangers created through 'shadow IT'. This first challenge may also increase the difficulty of dealing with other challenges and increase the severity of breaches. The example outlined above highlights how a lack of visibility and control may increase the challenge of managing privacy and data security (see Challenge #2). Furthermore, the need to document accurately and audit outsourcing arrangements (Challenge #4) is clearly confounded if the organization does not have clear visibility of such arrangements.

2. Understanding Privacy Obligations and SaaS Architectures

While our first challenge relates to a lack of visibility and control over the outsourcing arrangements being introduced, our second challenge relates to a lack of visibility and understanding of the vendor’s IT architecture. In 2014, the UK regulator stated that: ‘Technological developments continue to affect the way consumers engage with financial services and how products and services are distributed. Technology may create effective and cost-efficient distribution channels, increasing competitiveness, innovation and efficiency, but can also be limited by vulnerabilities in the design and management of systems and infrastructure.’ Our own study shows that larger financial institutional firms often do everything in-house and have ‘well locked down systems’, which may be largely effective in preventing data breaches and the adoption of SaaS. However, middle to lower tier banks, brokerages, hedge funds and asset management houses often outsource their IT. Yet IT staff are often the biggest perpetrators of shadow IT arrangements (Stratecast 2013). Ultimately, if the service provider does not have complete visibility of its IT arrangements, then neither the firm nor the regulator will have a comprehensive view of the operational risks inherent in the outsourcing arrangement.

When users adopt SaaS they effectively extend their firm’s IT infrastructure and handover control of key architectural elements such as the network, storage, server and operating systems that support the application being provided. A compliance officer commented: ‘The Cloud itself is a big thing to be worrying about, and as it’s developed behind the scenes by a number of companies over the last few years and it’s a scary technology from one point of view. As you don’t really know where anything is or how it works. A lot of the Cloud systems are proprietary. You have no real control over where your data is, how it’s backed up, how secure it is.’ Consequently, firms may have no idea how reliable the IT architecture of their vendors is or have clear details regarding where their data is stored. Yet data protection laws often specify where and how personal data can be held and for how long. Where firms use SaaS arrangements, it may be difficult to prove that data deletion has occurred on platforms held and managed by third parties, particularly where the outsourcing arrangement may have ceased and the vendor is based overseas. Furthermore, the FCA handbook (2015b) requires that, ‘the firm, its auditors, the appropriate regulator and any other relevant competent authority must have effective access to data related to the outsourced activities, as well as to the business premises of the service provider.’

Firms and individuals may be heavy fined where data breaches occur. Yet often individuals can easily move data outside the firm’s technological boundaries through memory sticks or by emailing data to themselves. For example, in 2011 a US regulator, the SEC, levied its first fine against individuals for failing to protect customers’ data and breaching its ‘Safeguard Rule’, which requires firms to safeguard their customers' nonpublic personal information and provide them the right to opt out of having their information shared with unaffiliated third parties. GunnAllen Financial, a broker-dealer, was in the process of winding down operations as it went into liquidation when its former president and former national sales manager violated customer privacy rules by improperly transferring customer records to another firm. The SEC suggested the president authorized the national sales manager to take
As data protection rules apply universally, so the related risks also apply across all industries and sectors. The UK Information Commissioner (IC) has the power to levy fines and require businesses to take steps to comply with the Data Protection act. Failure to do so is a criminal offence. Other criminal offences which can result in prosecutions against directors and officers of companies may occur where disclosing personal data without consent and selling or offering to sell such data has occurred. Transgressions may occur in the processing of both employee and client data. Transfer of such data across borders outside of the European Economic Area (EEA) must also be tightly controlled. Requirements may differ across countries even within the EEA. Germany has introduced enhanced restrictions for transferring data outside the Federation and later this year the EU is expected to release a new data protection regulation which will increase obligations. A senior data privacy lawyer provided an example of how outsourcing arrangements may be influenced by regional differences in such data protection regulations, ‘There are places with very strict laws, particularly Germany where moving data is much more problematic. In South African who have laws very similar to the UK around data privacy the requirements dovetail in an elegant way, which means that there are several large bulk legal documentation review firms there who exist entirely because of this coherence in regulation between the jurisdictions. Because the data privacy laws line up and fit together…. it means that your data can go there, be reviewed by their outsource teams, and you get the cost benefits of offshoring, while the data stays in an appropriate jurisdictional boundary. So there are huge benefits for firms in certain sectors…. so as far as I understand it, these firms exist in South Africa pretty much exclusively because of that legal situation.’

Data privacy regulations provide specific challenges for those adopting SaaS solutions with or without the knowledge of the IT function. Furthermore, as with the previous challenge, the pervasive nature of mobile devices and growth of BYOD increases risks. An IT risk auditor observed: ‘So Bring Your Own Device has got all kinds of problems for the companies that do it but they’ve got pressure from their employees, who don’t want to be carrying multiple phones. And the big worry is that they might leave the company and still have some key data on their phone. In the case of a regulatory breach or litigation, if it’s a personal device belonging to an individual, then the company has no right to access that device if something goes wrong unless there’s a court order…’

As data protection rules apply universally, so the related risks also apply across all industries and sectors. The UK Information Commissioner (IC) has the power to levy fines and require businesses to take steps to comply with the Data Protection act. Failure to do so is a criminal offence. Other criminal offences which can result in prosecutions against directors and officers of companies may occur where disclosing personal data without consent and selling or offering to sell such data has occurred. Transgressions may occur in the processing of both employee and client data. Transfer of such data across borders outside of the European Economic Area (EEA) must also be tightly controlled. Requirements may differ across countries even within the EEA. Germany has introduced enhanced restrictions for transferring data outside the Federation and later this year the EU is expected to release a new data protection regulation which will increase obligations. A senior data privacy lawyer provided an example of how outsourcing arrangements may be influenced by regional differences in such data protection regulations, ‘There are places with very strict laws, particularly Germany where moving data is much more problematic. In South African who have laws very similar to the UK around data privacy the requirements dovetail in an elegant way, which means that there are several large bulk legal documentation review firms there who exist entirely because of this coherence in regulation between the jurisdictions. Because the data privacy laws line up and fit together…. it means that your data can go there, be reviewed by their outsource teams, and you get the cost benefits of offshoring, while the data stays in an appropriate jurisdictional boundary. So there are huge benefits for firms in certain sectors…. so as far as I understand it, these firms exist in South Africa pretty much exclusively because of that legal situation.’

3. Evaluating SaaS Vendor Reliability and Longevity

The previous challenge highlights why it is important for firms to open the ‘black box’ of vendors’ SaaS technical architectures and maintain an internal knowledge base capable of doing so. The FCA handbook (2015b) states, ‘the firm must retain the necessary expertise to supervise the outsourced functions effectively and to manage the risks associated with the outsourcing, and must supervise those functions and manage those risks.’ Building on this finding, the third challenge addresses the need to evaluate the reliability and longevity of SaaS vendors. Firms must have a good understanding of their vendors’ architecture if they are to conduct a comprehensive risk assessment of the outsourcing arrangement as required by the regulator. Lack of understanding here may be problematic where firms are required to evaluate and manage IT and outsourcing risks appropriately, in order to prevent unacceptable disruptions in services for which the organization may be held accountable by the regulator. Furthermore, SaaS arrangements which have been casually set up yet contribute to business critical processes may cause severe regulatory breaches should the vendor cease to operate. The FCA (2015c) handbook, advises that, ‘A firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business... The nature and extent of the systems and controls which a firm will need to maintain... will depend upon a variety of factors including: (a) the nature, scale and complexity of its business; (b) the diversity of its operations, including geographical diversity; (c) the volume and size of its transactions; and (d) the degree of risk associated with each area of its operation. To enable it to comply with its obligation to maintain appropriate systems and controls, a firm should carry out a regular review of them.’
RISK also comes from not understanding how robust a SaaS supplier is and not having arrangements in place should they cease to operate. For example, when traditional application providers have gone 'bust' user organizations have been able to gain access to the source code through escrow arrangements and have the applications and data hosted on their own internal systems. This allows a managed migration to another vendor without loss of service or data. However, when a SaaS application provider ceases to operate the switch may be turned off and access to the application and data cease instantly. For example, one executive at a mid-tier bank recently commented, 'We could lose our banking license if access to cloud based systems holding key customer information suddenly ceased and related data became 'stranded' on outside systems.'

In December 2012, following a 'thematic review' into outsourcing arrangements, the FCA wrote a ‘Dear CEO’ letter to 125 asset managers The review concluded that many firms were not fully in compliance, and were not prepared for the failure of a service provider. The consensus following the financial crisis is that ‘too big to fail’ organizations should be allowed to fail in a controlled fashion. Moreover, other financial organizations which rely on services provided by these ‘big’ firms should no longer assume their eternal resilience and must have adequate contingencies in place were these firms to face financial turbulence or operational disruption. The regulator recommended that asset management houses assess the effectiveness of their existing outsourcing arrangements and ensure they maintain required expertise in-house. In contrast, while many providers of new innovative apps might not easily be described as 'too-big-to-fail', they are perhaps much more likely to suffer from financial difficulties and lapses in service provision which drove the Regulator’s concerns. This view tallies with recent anecdotal evidence suggesting that the newly formed FCA and PRA have adopted the perspectives of their predecessor, the FCA, and are taking a much more stringent approach in applying the existing rules than prior to the financial crisis.

While the large IaaS and PaaS (e.g. Google and Amazon) operators are less likely to cease operation suddenly, the SaaS providers who use these services are at greater risk of running into unexpected financial difficulties and ceasing to operate. Regulated data may become stranded on hosted systems when SaaS providers shut up shop. Even where firms can identify the platforms and infrastructure where the data is being held, organizations may not have access to encryption keys. Providers are sometimes willing to provide the data and encryption keys and even allow data sets to be mirrored on the user’s internal systems. However, suppliers are less willing to share data schemas as they are inherent to the applications’ intellectual property, so data is often supplied in the form of a flat file. Without access to the data schema, organizations may need to invest considerable time and resources before the data in the flat file is in a form where it can be easily queried and audited. Where firms are aware of SaaS arrangements and include provisions in their contract with SaaS vendors to ensure they are provided with the encryption key, the data schema and the data itself, further barriers may arise as the vendor may no longer retain the technical capabilities required to meet these obligations. Once a firm is no longer able to meet its financial obligations, costly IT staff with specific knowledge and understanding of the application and its data may be the first to be let go by the firm or its receivers.

In summary, one often touted advantage of the Cloud and SaaS is to remove the overheads of running applications onsite. Yet ‘light touch’ low maintenance and inexpensive SaaS applications may prove not to be as light touch as initially thought once regulatory agencies perceive such arrangements as critical. Where such ‘shadow’ systems retain data or support activities critical to meeting regulatory obligations, there is an underlying and unseen risk, not least should access to such systems and underpinning data cease or be interrupted without the firm’s prior knowledge or control.


The fourth challenge relates to the need to document and audit outsourcing risks, policies and practices. The FCA handbook (2015b) states, ‘the service provider must carry out the outsourced services effectively, and to this end the firm must establish methods for assessing the standard of performance of the service provider...[and] appropriate action must be taken if it appears that the service provider may not be carrying out the functions effectively and in compliance with applicable laws and regulatory requirements. Clearly, where firm’s central IT or compliance function remains unaware of SaaS relationships this becomes problematic (see Challenge #1). The UK regulators (the FCA and PRU) handbook rules states that when organizations rely on a third party for practices and services which are deemed critical to compliance, impact financial performance or underpin services and activities firms must take steps to avoid operational risk and regularly review related practices.
and systems. In the USA, the Office of the Comptroller of the Currency (OCC) has also laid out similar provisions. Furthermore, the US SEC (Securities and Exchange Commission) has enhanced its rules to allow firms to outsource more of their operations, whilst simultaneously increasing related obligations for documenting and auditing outsourcing arrangements.

The SEC Secretary-General stated: ‘The revised outsourcing rules will allow securities and derivatives business operators to outsource activities directly relevant to its core or non-core businesses to enhance flexibility and efficiency of their business operations. In principle, the business operators must have an apparent outsourcing policy, measure, guidelines, service provider supervision, risk management, and business continuity measures. However, outsourcing does not discharge business operators from responsibility in their outsourced activities’ (SEC 2013).

In 2014, Stonebridge Insurance was fined £8.4 million for targeting middle-to-low income consumers without degrees or professional qualifications in underwriting personal, accident, accidental death and accident cash plan policies. The regulator found that while sales, post-sales and customer service operations were outsourced to firms also authorized by the UK regulator, Stonebridge remained ultimately responsible for the outsourcing arrangement. The investigation found that Stonebridge had failed to treat its customers fairly and that management controls failed to prevent customers being put at an unacceptable risk of being mis-sold products (FCA 2014a). The UK Regulator’s final enforcement notice stated that: ‘Failings were made possible by Stonebridge’s poor systems and controls, and inadequate oversight of the Outsourcing companies... Stonebridge did not obtain adequate management information from the Outsourcing companies to enable it to identify measure and manage risks to the fair treatment of customers. The management information that Stonebridge obtained was unclear and incomplete, which meant that there was lack of effective monitoring of the Outsourcing companies... Stonebridge failed to ensure that sales calls and post-sales cancellation calls by the Sales outsourcing company and the Customer service outsourcing companies were subject to adequate quality assurance procedures. Furthermore, Stonebridge was unable properly to monitor its systems and controls in the European Offices because its Compliance department was inadequately resourced.’ (FCA 2014c).

In 2014, the FCA released a checklist for firms using ‘third-party technology banking solutions’ which requires firms to have documented a clear business case supporting the decision to outsource critical technology services and how related risks will be addressed, as well as how multiple service providers will work together, if necessary, to deliver a holistic service. The checklist also highlights how firms who use hosted services, such as SaaS, must take into account additional factors where their hosting firms use the same infrastructure to provide the same service to different firms (multi-tenancy) in order to provide cost benefits. These additional considerations include how the financial organization will ensure its data is segregated and secure and that performance will not be impaired by other tenants using the same infrastructure. Firms are also required to consider if many of its competitors are using the same service provider and so if an acceptable level of supplier concentration risk exists. An exit plan must also be defined which addresses how the firm will get its data back and how the data will be removed from the supplier’s systems. Of course, when the ‘exit’ is occurring because the supplier is no longer able to operate - this will present the challenges already outlined (see Challenge #3) (FCA 2014a).

5. Managing Intra-Group Outsourcing Arrangements

Our fifth challenge relates to firms who rely on intra-group outsourcing arrangements and reflects the UK regulators’ concerns, outlined in a review focused on the governance of unit-linked funds. This review highlighted how the regulator’s supervisory focus would not be limited to purely third party arrangements. The review found that, ‘Where operational functions were outsourced to other companies in the same group, there was an ‘informal’ reliance on group control functions (such as Group Internal Audit) to provide assurance on the effectiveness of controls in the outsource service provider. This approach generally relied on personal relationships as opposed to specific, clear engagement with the audit universe, audit plan and reporting arrangements. A firm should not assume that because an outsource service provider is an intra-group entity (or, more generally, a regulated firm) an outsourcing arrangement with that provider will, in itself, necessarily imply a reduction in operational risk.’ (FCA 2013b).

For example, in 2010, Zurich Insurance (UK) was fined £2.3 million for failures arising from intra-group outsourcing arrangements. At the time this represented the largest fine levied against a single
organization for data management failings despite the fact that there was no evidence the data had been misused or that losses had been incurred by customers. Personal details of 46,000 customers, including credit card and account information, were lost during a transfer to a data storage center in Zurich, South Africa. The loss was not identified until one year after the event, which, in the Regulator's mind, further demonstrated that Zurich did not have effective control and oversight over the arrangement.

The UK Regulator's Director of Enforcement commented that: ‘Zurich UK let its customers down badly. It failed to oversee the outsourcing arrangement effectively and did not have full control over the data being processed by Zurich SA. To make matters worse, Zurich UK was oblivious to the data loss incident until a year later. Firms across the financial sector would do well to look at the details of this case and learn from the mistakes that Zurich UK made’ (FSA 2010).

In summary, firms should not assume that outsourcing arrangements with an intra-group entity will naturally create a reduction in operational risk. The review also identified intra-group outsourcing arrangements as creating potential issues in relation to appropriate levels of oversight, which may be less formalized across the group and limited to the internal audit function. Ultimately, firms are required to apply the same levels of rigor in the documentation, management and accountability of intra-group arrangements as they should with third parties (Challenge #4). Where intra-group providers’ employees use SaaS applications without the provider or user firm’s knowledge, risks inherent to the arrangements will not be fully understood, documented or managed.

6. Emergent Challenges: Shifting Regulatory Landscapes

The final two challenges relate to risks emerging from recent upheaval within the financial services industry following the financial crisis. As result of the financial crisis, there is an increasingly complex and shifting regulatory environment. For example, the EU’s upcoming Markets in Financial Instruments Directive/Regulation (MiFID/R II), due in 2017, makes changes in how and where trades are executed and so may drive asset management firms and other financial intermediaries who may lack the scale of resources required to invest in necessary systems to seek out new outsourcing arrangements. The MiFID/R II regime will also create new obligations around information systems and data (EY 2015). These obligations will become clearer when the Level 3 implementing measures are decided upon and released.

Another case in point is the Alternative Investment Managers Fund Directive (AIFMD), implemented in response to the G20 commitment to strengthen regulatory regimes globally, which requires firms to justify objectively the reasons for adopting ‘entire delegation structures’ to regulators. AIFMD requires firms affected by the regulation to have a written agreement between the investment firm and the delegated organization, to include rights of information, inspection and access. In addition, the investment fund must establish a review process to assess performance and put in place a continuity program to bring activities in-house or to transfer them to another delegate. The investment firm must instruct its outsourcing provider how to monitor compliance. Providers are obliged to disclose any developments that may have a material impact on their ability to maintain the service. Crucially, the investment fund must provide its regulator with detailed explanations and evidence and so demonstrate a strong rationale for implementing the outsourcing arrangement. This rationale should consider potential optimization of processes, cost savings, expertise and access to cross-border trading capabilities.

Clearly, the assumption inherent in all these obligations is that firms have a comprehensive view of the management functions which have been outsourced and, equally, a complete picture of associated benefits and risks (see Challenges #1, #3 and #4). Where shadow SaaS arrangements have been introduced, this assumption may be undermined as the firms’ view of its exposure to SaaS outsourcing risks may be incomplete. Even if firms have full visibility of all engagements, shifts in the regulatory landscape may alter the criticality of existing arrangements. Furthermore, as new regulations fundamentally change the rules and reshape the playing field (e.g. AIFMD, MiFID II, Basel III/CAD IV, Dodd-Frank, etc.) outsourcing arrangements are likely to become increasingly attractive and necessary for some firms to operate specific business lines with new outsourcing offerings and models emerging. Correspondingly, regulators are increasingly seeking to understand and monitor the risks of such arrangements. However, where new technologies (e.g. Cloud, SaaS, smartphones/BYOD) are facilitating such arrangements, regulators and firms are challenged to understand resultant new emergent risks which may differ from those associated with more traditional BPO and ITO practices.
7. Emergent Challenges: Shifting Technical Landscapes

The last challenge has also emerged as a result of the financial crisis. Large scale redundancies led newly unemployed individuals to form disruptive technology focused startups, often termed ‘Fin Tech’. The rise of ‘Fin Tech’ hubs in London, New York, Frankfurt and Singapore, where start-ups and existing players are developing cloud based innovative new approaches for conducting financial business, are examples of the rise of disruptive technologies within the financial services industry. The UK Regulator’s 2014/15 Risk Outlook states: ‘Some firms in financial services rely on technological systems of firms that are emerging outside the perimeter. While unregulated entities – such as alternative payment platforms or digital currencies – sit outside our scope of responsibility, they can generate pro-competitive benefits. They can also pose risks to market integrity and consumer protection through technological interfaces with regulated activities. These activities may have the potential to create systemic and financial crime risks that would be outside our perimeter.’ (FCA 2014b).

The rise of disruptive SaaS applications in financial services raises challenges for firms wishing to adopt such technologies and benefit from these innovations. The existing regulatory rules on outsourcing arrangements are based on assumptions built around shared, large, stable, global IT infrastructures (e.g. SWIFT) and traditional business models universally shared and understood amongst industry participants. Often, only regulated firms may have access to such offerings. Technologies which circumvent these infrastructures and apply innovative new business models may create new risks not well understood by regulators, particularly where such firms fall outside the regulator’s jurisdiction. The UK Regulator recently commented: ‘Growing reliance on technology is increasing the exposure to the disruptive capabilities of technologies in ways that can prove costly to firms and consumers in the future. This makes the integrity of IT infrastructure increasingly important for firms’ operational stability and, given the interconnectivity between systems, for market integrity more broadly’ (FCA 2015a). Within the UK, the Regulator has responded to the growth of disruptive technologies in financial services by inviting vendors to become part of its ‘Project Innovate’. In doing so the Regulator has opened its doors and invited vendors to liaise with its officers to allow vendors, ‘to understand the regulatory framework and how it applies to them’ and for the regulator to, ‘understand more about the needs of innovator businesses and their products and services, and the possible benefits and risks to consumers.’ Our respondents felt that this offer from the Regulator was unusual in that normally the Regulator’s feedback is restricted to binary responses, compliant or not, with little feedback provided beyond the guidance outlined in its whiter papers and handbook (FCA 2015a,b).

Technological and business model innovation provides many opportunities for financial organizations whilst simultaneously creating significant compliance problems. For example, a CIO in a mid-tier bank suggested: ‘We know that we can’t look to IBM, Microsoft and Oracle for innovation but are wary of SaaS apps as they are black boxes and the current regulations are not friendly to them.’ Correspondingly, in a recent global study of CIOs by BT (2015) 71% viewed cloud technologies as having potential to unlock creativity, while correspondingly 76% reported the presence of shadow IT arrangements within their organizations. 76% also suggest that the IT department is losing control of the firm’s IT estate. Three quarters of the study’s participants also advised that shadow IT is causing concern regarding both the security of their entire organization’s data and IT infrastructure. Yet, Cloud and SaaS do provide important potential advantages to financial organizations which can appropriately harness them by agilely accessing potentially disruptive yet low cost technological capabilities through innovative new applications. However, the adoption of new technologies is not without increased operational risk. For example, financial organizations often have numerous legacy systems which require integration with SaaS and Cloud offerings if their full value is to be realized. The UK Regulator highlights the opportunity SaaS offers and warns of related risks: ‘By taking on technologies that increase efficiency and respond to changing demands, the competitive dynamics in some markets are changing. New entrants, potentially better able to set up systems that respond directly to consumer requirements, may have a competitive edge on firms that need to integrate technologies with (possibly already overloaded) existing systems. Another aspect of this is the use of inherently scalable cloud technologies that may raise compatibility or resilience issues where firms are tacking these on to less scalable legacy systems.’ (FCA 2014a)

Traditional outsourcing arrangements will continue to provide important advantages as firms struggle with increasingly burdensome regulatory regimes and turbulent economic environments. Such
arrangements allow mid and lower-tier firms access to cost savings and innovative up-to-date technologies, while simultaneously providing more robust technological architectures which would otherwise create disproportionate costs. Yet ITO/BPO also pose risks as highlighted by the UK Regulator’s 2014/15 Risk Outlook stating: ‘Where firms choose to outsource functions to benefit from technological advances that they are unable to adopt in their own systems, consumers could face detriment, if firms do not have sufficient oversight of outsourced functions or an understanding of how outsourced technologies interact with existing systems.’ (FCA 2014b).

In summary, while the lure of ‘light touch’ SaaS applications may be enticing in the short term, such arrangements have the potential to create serious regulatory problems which may in turn create considerable overheads to fix, as well as causing costly fines and reputational damage. Consequently, in the medium to longer term SaaS arrangements shadow or otherwise may prove to be anything but ‘light touch’ for CIOs, heads of regulated business units, compliance and risk managers. Where the regulators view outsourcing arrangements as being insufficiently robust, firms may be required to engage in long and expensive projects to develop and implement fresh outsourcing governance policies and practices even where no substantial failure has occurred. Many heavily regulated firms feel unable to engage with the SaaS model due to the risks outlined and so seek to ensure that their IT infrastructure is locked down. Even where they are successful, they lock out potential opportunities to leverage disruptive capabilities available through SaaS applications.

Ways Forward: Managing Outsourcing Regulatory Risk

These seven ‘crocodiles’ lying in wait for the unwary make clear that our ‘swamp’ metaphor was no idle invention. How can business managers bring order and control to bear on a highly complex, sometimes inconsistent and constantly changing set of regulations and practices? In a recent survey of compliance officers, Accenture (2015) concluded that the compliance department has the potential to be disruptive in a positive way. However, the survey provided little insight into how or why. We suggest that this potential can be realized through the compliance department helping a firm access potentially disruptive cloud and outsourcing capabilities without endangering the firm’s regulatory position. This may be achieved by the effective management of outsourcing-related regulatory risk. Our study has allowed us to synthesize emerging, disparate, useful practices into a more systematic response. Figure 1 outlines a framework for managing outsourcing regulations and is structured around three themes: Investigate, Strategize and Govern. The framework represents a conceptual presentation of the proposed management process.

Figure 1 Managing Outsourcing Arrangements for Regulatory Compliance

The model should not be interpreted as a literal, linear or waterfall model. The process depicted should be viewed as iterative. The same activities may be repeated many times to create an increasingly accurate and valuable set of results. Each of the five stages is interrelated and mutually dependent. If one stage is revisited the impact of the change should be reviewed for each of the other stages. It may also be necessary to cycle through earlier steps to define the approach being adopted as individuals obtain a better understanding of the data or the business context influencing the analysis. Different areas of expertise (e.g. law, IT, business domain, risk, compliance, front/middle/back office)
may facilitate discrete elements of the model individually or more likely through collective collaboration.

1. **Review Regulatory Exposure and New and Existing Outsourcing Arrangements.** The first element of our model requires firms to understand the levels of regulatory exposure in relation to outsourcing arrangements. Consequently, we recommend that IT should be represented on any committees which review new regulations and compliance practices. Compliance executives should also be consulted when new outsourcing arrangements are introduced or even considered. Firms should then consider new and potential arrangements against the outsourcing strategy, policies, controls and risk appetite outlined in parts 2 & 3 of the model and if the arrangement is likely to be deemed ‘critical’ by the regulator. This element of our model also requires firms to conduct a review of third party, SaaS and intra-group outsourcing arrangements and develop a detailed inventory of all critical and non-critical outsourced services. Firms may consider different strategies and technologies for understanding where existing IT policies have been breached and shadow IT arrangements put in place. One strategy is to call an amnesty for a limited time period and encourage firms’ employees and departments to ‘fess up’ with the promise of no further disciplinary action taken. Another approach is to employ one of a variety of software vendors who claim to be able to identify and review shadow IT arrangements. Forensic tools such as e-discovery systems may help firms trawl through the enterprise’s structured and unstructured data to identify where shadow IT arrangements have been put in place. However, our study revealed that where individuals take data outside of the organization’s technological architectural boundaries, such tools may be less effective.

2. **Evaluate Supplier Operational, Technical & Data Risks.** In order for firms to ensure the necessary outcomes of the outsourcing arrangement from a regulatory perspective, it is recommended that firms clearly evaluate and document risks. This element of our model requires firms to consider systemic risks inherent in collective arrangements and risks related to discrete arrangements with individual suppliers. Key to this is retaining individuals with appropriate technical knowledge and expertise who can identify IT and operational risks and ask vendors the ‘right questions’ to uncover related risks. Such experts may consider the provider’s security controls and robustness in regards to resilience and speed of architecture, security of data at rest and in-transit, segregation of data from other clients, physical location of data, back up, controls for the prevention of data leaks through vendor employees (e.g. through USB sticks). Other risks to be considered include the firm’s ability to provide appropriate oversight of the relationship and quality control of effected processes, the reliability and longevity of the services provider and the cost implications. Firms are recommended to map risks to specific outsourcing arrangements, internal policies and procedures and regulatory obligations, as well as elements of contracts aimed at mitigating such risks. Consequently, the risk identification and mapping exercise may involve general counsel, compliance and risk managers, business domain experts, process owners and IT analysts. An important element of this process will be assessing the stability and security of the vendor’s infrastructure and data management. Smaller and mid-tier firms may not have the expertise to do this in-house and so may have to engage yet another third party. In fact, regulators are often more sympathetic to outsourcing arrangements reviewed and evaluated through a credible third party. Third party consultants and auditors may also be better placed to judge the maturity and robustness of policies and practices.

3. **Define Outsourcing Strategy, Policies and Practices.** At the center of the model is the view that outsourcing arrangements must support the firm’s strategic business plan, i.e. it is essential to consider the outcomes the firm wishes to achieve through these arrangements - both internally within the firm, and on external stakeholders such as its clients and regulatory agencies. Through developing an understanding of how outsourcing arrangements align with the business strategy it will become easier to make judgments regarding their criticality and relevance. However, before engaging with vendors it is important to ensure that existing infrastructures, processes and controls are sufficiently mature. Moving ineffective or immature regulated practices outside of the organization is high risk because organizations remain ultimately responsible for such practices. This is especially true for Cloud arrangements. Senior management should formulate a written policy outlining what can and should not be outsourced and how such arrangements support the firm’s strategic plan. The policy should clearly state what constitutes ‘critical’ outsourcing in relation to the firm’s strategic direction, maintaining appropriate levels of services to clients, meeting regulatory obligations and maintaining auditable records. Policies should define risk
tolerances for outsourcing arrangements, including mitigation tactics. Managers should develop clear written procedures for the consistent implementation of the outsourcing policy document and document related controls. Having a solid perspective of arrangements and related risks allows firms to take a more strategic view of their outsourcing regulations. This means they can justify their approach to the regulator if required to do so. But more becomes possible. Understanding arrangements and risks enables firms to begin defining policies which can be distilled into controls, standards and metrics which may ultimately be built into the outsourcing agreement/contract.

4. Disseminate Internal Procedures and Controls. It is important that responsibilities of the organizations and specific individuals (who may be directly fined, see the GunnAllen case above) are well understood and that senior managers can articulate the reasons for the arrangement, the risks involved and its criticality in relation to regulatory obligations. Training should be structured at different levels within the organizations as appropriate. Consequently, it is important to ensure that responsibilities are understood at the level of the firm and the individual and that senior staff can demonstrate a firm understanding of existing arrangements, related risks and the firm’s policies and related regulatory obligations. Senior management should provide appropriate training and differentiate focus between operational staff and senior management as appropriate. For example, process owners and departmental heads should be educated regarding the regulatory and legal implications of setting up shadow IT arrangements, whilst senior managers and business domain heads should be able to articulate how outsourcing arrangements support the firm’s strategy. In order to do so, they must be educated regarding the related risks and so make an informed decision as to whether the arrangement has strategic fit and is within the firm’s appetite for operational risk.

5. Build Obligations and Transparency Into Contracts and Agreements. We advise firms to ensure contracts stipulate appropriate controls and measures for meeting regulatory obligations, for example data location and movement controls, rights of inspection, access and e-discovery and obligations in the event of the vendor ceasing to operate. Where deficiencies in existing outsourcing agreements/contracts are uncovered, (for example if no agreements are in place for intra-outsourcing arrangements) negotiate amendments to existing agreements with the help of appropriate legal counsel. As firms seek to ensure contracts and agreements are appropriate in light of the previous analysis, firms should demand high transparency from their vendors. This may require organizations to seek out or develop new expertise in outsourcing contracts as Cloud arrangements may differ considerably due to the risks previously outlined. Firms should consider if their usual legal representatives have the required legal and technical knowledge to tackle such challenges. Within agreements, auditing and access rights should also be well defined, not least as the regulator may require the firm to demonstrate how it is monitoring its vendors or request information directly from the vendor. Furthermore, the regulator may require the firm to provide specific documents as part of a regulatory investigation, thereby creating document/e-discovery obligations. Consequently, the firm should ensure that the vendor will be able to respond to such eventualities and have related responsibilities and roles built into the agreement. In addition, firms may wish to build in rights of access to the vendor’s premises to assess their data management and security and architectures. In addition, firms may wish to also explicitly require that vendor’s respond to regulators’ requests for information or also to visit their premises. Key contract provisions may consider cost and compensation, right to audit, establishing and monitoring performance standards, confidentiality and security of information, ownership and licensing, default and termination, dispute resolutions, limits on liability, insurance customer complaints handling, and business continuity and planning as well as subcontracting (FED 2013).

Conclusion

The risks of adopting Cloud and particularly SaaS applications create specific regulatory risks. Firstly, firms may lack visibility and control over the security and compliance processes. For relatively cheap subscription based applications vendors may provide no guarantees in terms of privacy and security. Non-IT savvy staff who subscribe to SaaS applications without the approval of the IT function may not be fully aware of the extent to which they are ceding control to a third party or parties and therefore may not be aware that they have unwittingly created a ‘critical’ outsourcing arrangement which comes under the purview of the regulator. Firms must also ensure that outsourcing arrangements do not
materially impact critical operations and controls, or impede monitoring by the regulator as per the SYSC rules (FSA 2015b). Crucially, firms must inform the regulator when it intends to rely on a third party or internal shared service centers for performing ‘critical’ operational functions. They must also ensure that recovery and resolution planning is not impacted by outsourcing arrangements in the event of an organizational crisis or total failure. A key element in ensuring organizational resilience through enhanced governance of outsourcing is to go beyond the first level of interaction between the firm and provider and also to consider where critical services have been further sub-contracted and how/where key data is stored. Understanding and controlling where personal data is located is also paramount to meeting data protection laws. The complexity of managing evermore complex outsourcing arrangements is further compounded as robust governance requires cross-disciplinary knowledge and cooperation across a wide range of business units including legal, operations, sourcing and technology. Regulators must strike a balance between the need to keep compliance costs proportionate and not act as a barrier for innovation and competitiveness with protecting investors and the integrity of markets by ensuring that systems and controls are appropriate and robust. This is particularly the case where third party suppliers fall outside the regulator’s jurisdiction.

A limitation of this study is that it is aimed at providing practitioners with a high-level perspective of outsourcing challenges based primarily on the FCA’s high level SYSC rules and guidance which apply to all regulated firms. However, the financial services environment is highly complex and differentiated covering a vast array of products relating to retail banking, insurance, equities, currency, corporate banking, derivatives, and commodities and bonds/fixed income to name a few areas. Thus, firms may have additional levels of regulatory exposure depending on the particular blend of products and business areas the firm chooses to engage with and its position on the supply chain. Consequently, the micro practices and criticality of outsourcing arrangements may differ significantly across firms. In addition, providing a comprehensive explanation of granular practices is not possible given the length of the relevant regulatory documents. Furthermore, it is not the intention of this paper to provide specific legal advice regarding outsourcing regulations and related compliance practices. Nor do we feel that such detailed analysis would hold our audience’s attention. Instead, we aimed to provide a high level approach which can be applied across varied financial services firms who can then further flesh out the details based on their own unique circumstances.

In conclusion, this study has focused specifically on financial regulation and the challenges and risks inherent in the sourcing practices adopted in the face of changing technologies and regulations. However, the challenges, opportunities, risks and ways of managing we have outlined will also be of considerable relevance to all regulated industries. The framework we have developed from our research findings provides practitioners with a structured approach for understanding how regulation impacts their outsourcing strategy and how related obligations and risks may be managed and mitigated regardless of the industry under review. The suggested approaches for managing data privacy regulations are relevant across industries. However, this is a very unexplored area of rising concern to practitioners across the globe. Future streams of research are needed to explore the relationship between regulation, outsourcing and emerging technologies across a range of industries, countries and regulatory jurisdictions.
References


Crocodiles in the Regulatory Swamp


Long, W. 2013. EU Data Protection Regulation: fines up to €100m proposed., Retrieved 8th June, 2015, from http://www.computerweekly.com/opinion/EU-Data-Protection-Regulation-fines-up-to-100m-proposed


