Journal of Business Research xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Journal of Business Research

journal homepage: www.elsevier.com/locate/jbusres

The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations

Daniel Gozman[a,b,*], Leslie Willcocks[c]

[a] University of Sydney, University of Sydney Business School, Sydney, Australia
[b] Henley Business School, University of Reading, UK
[c] London School of Economics and Political Science, Houghton Street, London, UK

ARTICLE INFO

Keywords:
Outsourcing
Cloud
IT governance
Fintech
Shadow IT
Data privacy

ABSTRACT

The pervasive adoption of outsourcing and Cloud technologies proceeds apace, but the challenges and risks inherent in Cloud arrangements are causing concern amongst regulators globally. How well prepared are financial services multinationals for regulatory compliance? Cloud based Fintech companies are disrupting traditional banking models, signaling that highly regulated firms must adopt Cloud technologies. The paper focuses on understanding specific risks in relation to Cloud adoption, and the regulations and penalties for non-compliance being put in place. From the findings, we theorize a framework for deciding when to engage strategically with, or avoid Cloud technologies. This helps executives balance the need to innovate with the need to manage compliance risk. We then detail emerging effective practices for managing Cloud based innovation on a sustainable basis. While we focus on global financial services, the analysis applies to all regulated industries, wherever Cloud based innovations impact materially on business-critical services.

1. Introduction

The great financial crisis and the misconduct and malfeasance of various financial organizations has created unparalleled fines and changes in financial regulation in order to reduce systemic risk to economics and enhance consumer protection. Correspondingly, there has been an increasing focus on the technology which underpins financial transactions and the risks they create (Currie, Gozman, & Seddon, 2017). In this paper, we address how risks inherent in Cloud based innovations[1] have crystalized and how synergies in outsourcing regulation, adopted by financial services regulators from around the world, provide further challenges and risks. Such risks apply to both incumbent financial organizations and new Fintechs,[2] operating internationally under numerous regulatory jurisdictions.

Business failure and related risks have formed a key topic of interest for scholars of strategy, organizations and international business (Amankwah-Amoah, 2016). Such research has often focused on the failure of existing regulatory structures, new technological innovations and increased competition across industries as well as inter-organizational factors such as poor technological procurement and administrative practices and general mismanagement (Amankwah-Amoah, Osabutey, & Egbetokun, 2018). Through new empirical analysis we uncover multiple risks inherent in transferring data across borders, Shadow IT[3] and legacy systems, amongst others, and theorize a framework for managing the identified risks. While we draw upon data from financial services, the framework can be applied to all highly regulated industries and wherever Cloud based innovations impinge on business-critical activities.

* Corresponding author at: University of Sydney, University of Sydney Business School, Sydney, Australia.
E-mail addresses: daniel.gozman@sydney.edu.au (D. Gozman), l.p.willcocks@lse.ac.uk (L. Willcocks).

[1] We define Cloud computing ('the Cloud') as, '…The convergence of the evolution of two distinct strands: technological innovation–based around data-centers, networks and virtualization–and a distinct service based perspective on computing.' (Willcocks, Venters, & Whitley, 2011). While the UK regulator considers the Cloud to encompass, "…a range of IT services provided, in various formats, over the internet. This includes for example, private, public or hybrid 'cloud' and Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)' (FCA, 2015b).

[2] Fintech is an umbrella term used to describe the post-financial crisis growth of disruptive technologies and transformative services operating within and across the financial services industry. The rise of 'Fintech' 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 (Federation Global Fintech Hubs, 2017; World Economic Forum, 2015).

[3] We define Shadow IT as, 'SaaS applications used by employees for business, which have not been approved by the IT department or obtained according to IT policies. The non-approved applications may be adopted by individual employees, or by an entire workgroup or department.' (Netskope, 2016).

https://doi.org/10.1016/j.jbusres.2018.06.006
Received 26 June 2017; Received in revised form 11 June 2018; Accepted 13 June 2018

The use of the Cloud is very relevant to transforming traditional financial services models and practices. While Fintech is often billed as a battle between incumbents and new entrants, a review of 402 Fintech firms shows that many Fintechs are seeking to offer new services to incumbents and collaborate rather than directly compete with them (Gozman, Liebenau, & Mangan, 2018).

While those firms which are consumer (b2c) focused often disintermediate existing banking practices to some degree e.g. 'peer2peer lending' or 'robo-financial-advisors' there are many whose aim is to complement and collaborate with incumbents by providing Cloud based services which enhance their own capabilities and offerings (b2b). For example, Monzo launched in 2015 (Venkatraman, 2016) as a mobile technology challenger bank, developed its core banking systems from scratch in the Cloud and became a fully licensed bank in August 2016. Also in 2016, another UK challenger bank OakNorth became the first bank in the UK to use a Fintech provider (Mambu) for its core banking systems, hosted on the public Cloud, (Amazon Web Services (AWS)) (Penn, 2016). In the same year, the UK Regulator fined insurance firm Aviva £8,246,800 for failings in its oversight of its outsourced providers (FCA, 2016a).

Globally, outsourcing arrangements are coming under scrutiny as new laws and regulations require firms to be increasingly accountable for their operational practices, and transparent regarding the personal data held, and how it is managed. Impacted sectors include energy, insurance, telecoms, mining, law and public services (Outsourcing Law, 2017). This phenomenon, however, is particularly prevalent in the financial services industry recently distinguished from other sectors by the depth and breadth of regulatory changes being enacted globally following the 2008 financial crisis and global Great Recession (Gillespie, Hurley, Dietz, & Bachmann, 2012).

Despite these important shifts, scholarly work on outsourcing and the Cloud has largely neglected the impact of regulation. Notable exceptions focus on regulation of trans-border health data (Seddon & Currie, 2013) and telecoms regulation (Cave, Robinson, Kobzar, & Schindler, 2012). Indeed, comprehensive reviews of outsourcing and Cloud practices omit or point to the need for more research on the impact of regulation (Lacity, Khan, & Yan, 2016; Lacity, Khan, Yan, & Willcocks, 2010; Schneider & Sunyaev, 2016; Venters & Whitley, 2012). Studies of outsourcing within financial services (Clark & Monk, 2013; Gozman & Currie, 2014a; Jennings, 1996; Qin, Wu, Zhang, & Li, 2012) and insurance (Ben-Shahar & Logue, 2012; Herz, Hamel, Uebernickel, & Brenner, 2012; Řezáč & Řezáč, 2013) are more common while other related work has explored how organizational control mechanisms (e.g., internal controls for compliance) when aligned with outsourcing strategies can improve financial and strategic performance in multinationals (Li, 2012).

Recent studies of Cloud computing have underlined the conceptualization of the Cloud as an outsourcing relationship (Schneider & Sunyaev, 2016) and addressed the financialization of Cloud through pricing and service delivery mechanisms (Kauffman, Ma, Shang, Huang, & Yang, 2014) and security (Jamil & Zaki, 2011; Pearson & Yee, 2012; Shaikh & Haider, 2011) and privacy (Ion, Sachdeva, Kumaraguru, & Čapkun, 2011). Other studies have focused on the relationship between innovation and Cloud adoption (Ratten, 2016) and the relationship between innovation outsourcing and profitability (Stanko & Olleros, 2013). The need to innovate is currently of particular importance for the financial services industry. Incumbent organizations are under increasing pressures from new entrants (Fintech firms) who are using new technologies and practices to challenge and disrupt long embedded business models (Economist, 2015).

Consequently, managers in incumbent global regulated firms are faced with a quandary: whether to play safe and lock out Cloud based technologies and correspondingly lock themselves out of related innovations, or to negotiate a rocky course, balancing the risks associated with these technologies and cross–border regulatory expectations. We term this dilemma the 'Cloud Dilemma'. Specifically, the study seeks to answer two interrelated questions:

- What are the challenges and risks of adopting Cloud based innovations within highly regulated environments?
- When and how should managers deploy Cloud based innovations, and manage the identified challenges and risks on a daily basis?

Our analysis applies to all highly institutionalized environments, for example legal services, utilities, but really, in any increasingly regulated business environment, wherever Cloud based innovations materially impact business critical services, however the examples which we draw upon in this paper are from global financial services.

The paper first outlines the benefits and drawbacks of adopting Cloud. We then outline the regulatory landscape for technological outsourcing in financial services. The next section shows the new ways whereby firms are accessing innovative Cloud based practices. We then detail the challenges, risks and opportunities the study revealed. Drawing from this analysis and our findings, we then delineate frameworks for addressing the 'Cloud Dilemma' and managing outsourcing regulations on an ongoing basis. Our concluding remarks focus on how our findings point to new opportunities for business.

2. Theoretical framing and background: the technological and institutional context

The existing regulatory rules on outsourcing arrangements in financial services are based on assumptions built around large, stable, global IT infrastructures (e.g. SWIFT) and traditional business models universally shared and understood amongst industry participants. 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. A major UK regulator (FCA) 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).

The 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). Beyond the high-level guidance from financial services regulators, our study investigates the assemblage of factors that can create barriers to adopting Cloud based innovations with a view to distilling the experiences and findings into a framework to enable organizations to manage this increasingly complex yet crucial area.

2.1. Cloud based commodification of IT services

One perspective on Cloud computing views the Cloud as facilitating the commodification of IT services (Carr, 2004). Organizations may now pay a subscription fee for access to technological infrastructures, platforms and business applications, all managed externally. Through this model firms may reduce investment in underpinning hardware, software and IT infrastructure (IaaS, PaaS, SaaS), which now become managed and maintained by Cloud providers. A key advantage is that firms can quickly scale up and down their IT capabilities in a cost-effective way. From an accounting perspective, in-house IT assets may be treated as capital expenditure with depreciation, while the purchase of

Cloud related services is treated as an operating expense. For CIOs, this means that IT capital expenditure can be moved to more flexible operating expenditure.

Another potential advantage of the Cloud is access (depending on the supplier) to the latest cutting-edge architectures, which may be more secure than firm's own less up-to-date systems. Often contracts operate through a monthly subscription basis and so firms can, in theory, move between providers more frequently than with traditional outsourcing or off-the-shelf software vendors. There is also often a wide range of suppliers to choose from, all aiming to compete by innovating and improving their offerings. As SaaS applications increasingly encapsulate specific business services, this commodification, through the Cloud, allows organizations to more easily implement changes.

To summarize, the potential benefits of Cloud are agility, access to innovation and up-to-date infrastructure as well as reduced costs. However, the Cloud is not without its drawbacks and risks especially for firms in regulated industries. Firms who use Cloud services may become increasingly reliant on such firms to provide and support business critical applications. They are also reliant on suppliers having adequate security provisions in place.

2.2. The global regulatory landscape for outsourcing in financial services

Pre and post the 2008 financial crisis, operational failures and related malpractices have increased demands for more transparency and regulatory scrutiny of management practices (Roberts, 2009). Firms were faced with a 'new normal' of higher operational costs, derived from the need to meet a 'tsunami' of new regulatory rules, with short deadlines for implementation, while being subject to heightened levels of supervision (Gozman & Currie, 2014a). Fines levied against financial organizations also increased dramatically since the financial crisis (FCA, 2014b). As a result, many financial firms, looked to technology-based outsourcing and offshoring models to cut costs and make efficiencies, and support operational activities, even those deemed 'critical' by regulators. Table 1 summarizes highlights from recent surveys on outsourcing in financial services.

Following the financial crisis firms began 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 (Fulbright, 2011). Fig. 1 is a timeline outlining outsourcing policy, risk warnings and guidance missives issued by key regulatory authorities in the USA and Europe since the financial crisis, and, most recently in 2017, by the European Banking Authority (EBA).

Regulators across the globe have responded to firms increased reliance on outsourcing vendors. This timeline reveals how regulatory authorities are becoming increasingly focused on monitoring outsourcing arrangements in the financial services industry. Table 2 provides illustrative examples of common global regulatory perspectives.

As Table 2 shows, a common rule across regulatory jurisdictions is that financial organizations cannot outsource their responsibilities to remain compliant. Such rules require that firms have necessary oversight and governance of outsourcing arrangements and that proper risk assessments have been conducted. Firms must keep regulators informed of changes in their outsourcing arrangements, so that authorities may also take a view of related risks and the appropriateness of the arrangement. For example, in 2014, Stonebridge Insurance was fined £8.4 million. 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, 2014d).

Recent missives from regulators (see Fig. 1) and responses from our interview participants signal how rules on outsourcing are being more strictly enforced, with heightened levels of supervision and monitoring being observed in accordance with general regulatory trends across the industry towards increased levels of surveillance and transparency (Gozman & Currie, 2014b).

2.3. Cross-border tensions in data privacy laws

Further regulatory challenges for organizations wishing to use technology providers emerge from differing and sometimes conflicting data privacy regulations. Within the EU, different approaches adopted by member states towards data privacy rights have emerged since the EU Data Protection Directive was introduced in 1995. Germany for instance will not permit personal data to be moved outside the German borders (Nolte & Werkmeister, 2017). Currently, the UK does allow personal data to travel across the EEA, and also to other states with similar legal regimes such as South Africa (GOV.UK, 2017). France, according to its 'Blocking Statute', will not permit data to be moved outside of France for the purposes of foreign litigation (Liard & Lyannaz, 2012). Nor does France, according to a Supreme Court ruling, allow firms to access an employee's emails, even if stored on the firm's own hard drives and sent through the firm's email address, if those emails are deemed personal or private (Freehills, 2001).

In order to ease regulatory conflicts within the EU, and so harmonize the different approaches adopted by its member states, the EU General Data Protection Regulation (GDPR) was agreed in April 2016 after three years of discussion and review (Freehills, 2001). The GDPR repeals the 1995 Data Protection Directive and includes the new right of individuals to be forgotten, and have their personal data erased without undue delay. Major developments include dramatically increasing the potential sanctions which can be applied, for breaches to 4% of annual worldwide turnover or a fine of up to 20 million EUR, whichever is higher.[4] In contrast, the UK Information Commissioner's

Table 1
Outsourcing research in financial services.

Post-crisis outsourcing surveys in financial services			
2015	2015	2015	2011
77% retail banks now outsource at least one significant part of their business.[a]	49% % of banks plan to increase their use of outsourcing with only 9% of banks stating that would reduce outsourcing.[b]	86% of respondents outsource to some degree. 20% banks outsourced their entire back office. 78% view outsourcing as a long term strategy to help them focus on core activities.[c]	87% of banks cited cost reduction as a key factor in deciding to outsource[d]

[a] Capgemini and EFMA World 'Retail Banking Report', retrieved 22nd March 2016 from, < < https://www.uk.capgemini.com/thought-leadership/world-retail-banking-report-2015 > > (2015).

[b] Flinders, K. 'Banks increase outsourcing but slash use of consultants', retrieved 22nd March 2016 from, < < http://www.computerweekly.com/news/2240241919/Banks-increase-outsourcing-but-slash-use-of-consultants > > (2016).

[c] You Gov and BNP Paribas, 'Global Risk Survey', retrieved 22nd March 2016 from, < < http://securities.bnpparibas.com/to-receive/bp2s-yougov/global-risk-survey-2015.html > > (2015).

[d] Hudson & Yorke, 'ICT outsourcing trends in the financial services sector', retrieved 22nd March 2016 from, < < http://securities.bnpparibas.com/to-receive/bp2s-yougov/global-risk-survey-2015.html > > (2011).

[4] The Information Commissioner's Office (ICO) has indicated that it intends to implement the GDPR in the UK despite the referendum to leave the European Union (Information Commissioner's Office, 2017).

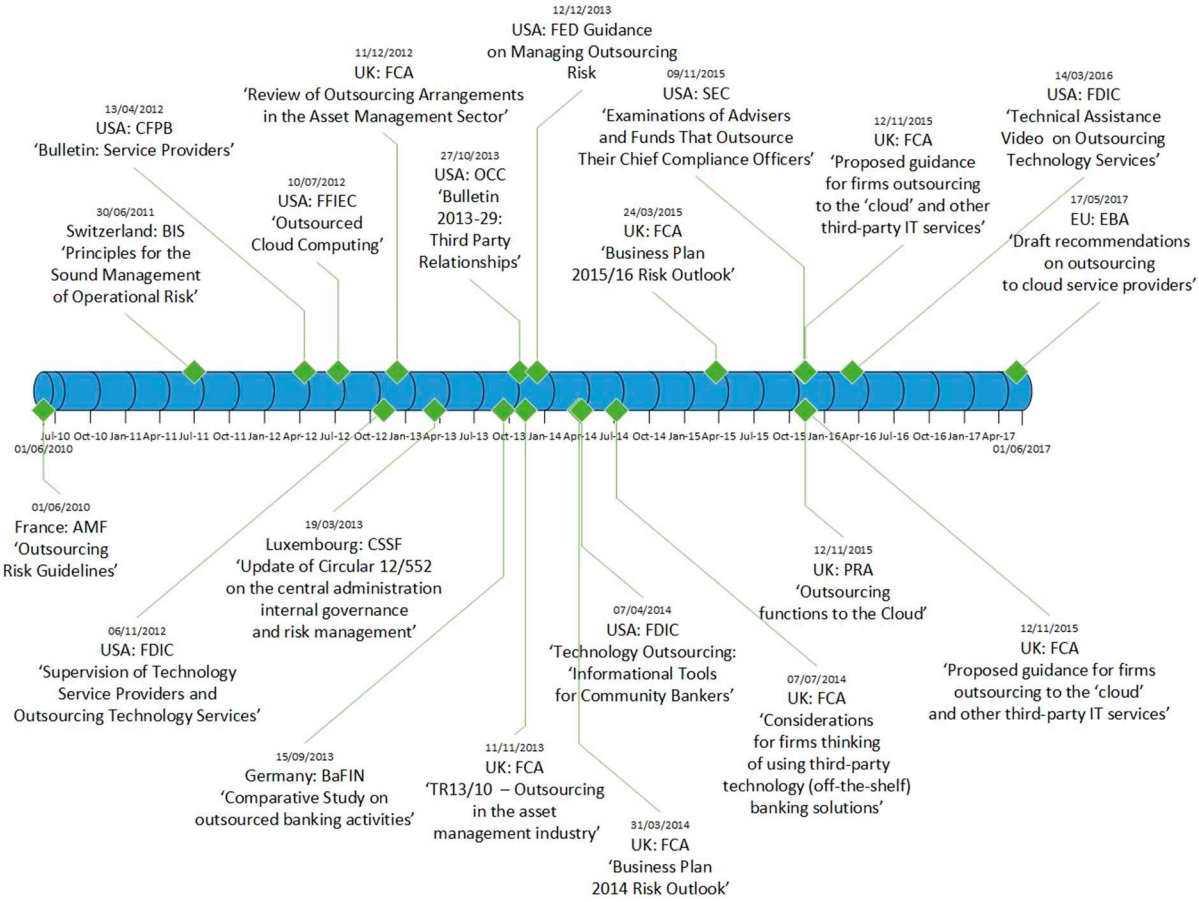

Fig. 1. Post-crisis timeline of financial services regulators' responses to outsourcing.
Source: Regulators' website.

Table 2
Common outsourcing obligations.
Source: Regulators' websites.

Common outsourcing regulatory obligations		
Regulator	Obligations	
	Firms cannot outsource regulatory and legal responsibilities	Firms must actively, monitor, document and manage outsourcing risks
OCC (USA)	*'A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.'*	*'A bank should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships.'* and *'A bank should ensure comprehensive risk management and oversight of third-party relationships involving critical activities.'*
BaFin (Germany)	*'The ultimate responsibility of the management board (or other persons appointed to represent the undertaking) for the outsourced function or insurance activity cannot be delegated but always remains within the undertaking.'*	*'The undertakings must adopt a written policy for the outsourced functions and insurance activities'* and *'If an undertaking also intends to outsource key tasks… it must designate an 'outsourcing officer' responsible for supervising the outsourcing process.'*
FCA (UK)	*'If a firm outsources critical or important operational functions or any relevant services and activities, it remains fully responsible for discharging all of its obligations under the regulatory system.'*	*'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.'*

Office (ICO) could previously only level fines of up to £500,000 for serious breaches and only £1000 if a service provider fails to notify the ICO of a security breach. Financial services regulators may also fine firms for data breaches.

Overall, the picture emerges of an increasingly unsympathetic set of regulators in the USA and Europe intensifying regulatory requirements and penalties, and much more willing to act. It is also worth highlighting that financial firms operating in the EU and USA, will often have to comply with regulatory obligations emanating from both areas simultaneously and across all their offices regardless of where they are actually physically located. Regulatory incongruities may emanate from firms and their technology providers operating across borders. These conditions contribute to the 'Cloud Dilemma' as regulations, often imposed before Cloud technologies were conceived (and so without

attention paid to underlying technological architectures), create significant barriers to firms wishing to benefit from the Cloud and related innovations.

2.4. Accessing innovation: shadow IT and Fintech

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 Cloud, employees may easily circumvent corporate IT who may remain blissfully ignorant that arrangements have been set up. Such arrangements are often termed, 'Shadow IT.' According to one study, on average, Shadow IT now accounts for a quarter of an organization's IT spend.' (BT, 2015).

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 are available. Low subscription and maintenance costs are also important advantages of this outsourcing model. However, these qualities 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 fewer resources, and to deliver results quickly to meet 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 what seems to be a 'cheap and cheerful' SaaS offering 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.

Shadow IT, however, may not have entirely negative implications. A recent global study of CIOs by BT (BT, 2015) 71% viewed Cloud technologies as having potential to unlock creativity and innovation, while correspondingly 76% reported the presence of Shadow IT arrangements within their organizations. A further 76% of respondents also suggested that the IT department is losing control of the firm's IT estate. Three quarters of the study's participants advised that Shadow IT is causing concern regarding both the security of their entire organization's data and the IT infrastructure.

To summarize, Cloud and SaaS do provide important potential advantages to financial organizations. But while '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 CEOs, CIOs, heads of regulated business units, and compliance and risk managers. Even where managers are successful in locking down the IT estate they also may lock out potential opportunities to leverage new innovations.

3. Research method

Our method for primary data collection involved interviewing 42 differentiated stakeholders including lawyers, technologists, compliance executives and outsourcing managers from 2013 to 2015 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 regulators across the globe. Our 'purposive' 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 (Denzin & Lincoln, 2000; Patton, 1980) The vendors were selected as being market leading providers of SaaS and ITO/BPO offerings. Sampling criteria for selecting financial institutions also focused on identifying firms impacted by the regulations. 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. All interviews were transcribed and managed by NVivo software. Table 3 summarizes the data sources employed.

A key source of secondary data was the missives issued by regulators from around the globe. A summary of outsourcing guidance issued by regulatory institutions in Europe and the USA is included in Appendix A. A summary of outsourcing risks identified by global regulators can be found in Appendix B. Both sets of analysis provided a fruitful point of departure for understanding common risks and related guidance issued by different regulatory bodies. This analysis defined the boundaries and scope of the study, which are analogous to the scope of global outsourcing regulations and the risks they aim to mitigate. Reviewing documentation from different regulators from around the globe (see Fig. 1) has allowed us to comprehensively identify the currently challenges faced by regulated firms. Correspondingly, an understanding of these issues helped us to define and structure our interview questions. We were further able to verify we had identified an exhaustive set of challenges through discussion with our interview participants, particularly those in the legal, auditing and consulting professions who has multiple experiences of such compliance challenges across many firms.

For our interviews, a semi-structured approach was adopted, as such methods have previously proved effective in providing the necessary depth and flexibility required to explore complex and dynamic technology related regulatory phenomena (Gozman & Currie, 2014a, 2014b; Tsatsou, Elaluf-Calderwood, & Liebenau, 2009). The semi-structured approach allowed us flexibility to pursue new topics as the discussion evolved and also as responses to shifts in the regulatory landscape emerged and new outsourcing obligations for the Cloud emerged (Kvale & Brinkmann, 2009). A process of triangulation reduced the potential for misleading results as key constructs derived from interviews were considered against secondary data sources (Flick, 1998).

Data analysis was conducted through long established interpretive techniques for analyzing data inductively through the recursive identification of patterns, first through categorization and then abstraction (Gibbs, 2007). Often qualitative studies create voluminous and varied data sets which are 'disordered' and difficult to systematize. We followed the 'Gioia Methodology' designed to enhance 'qualitative rigor' by deriving first-order, second-order and aggregate concepts. This method allowed us to systematically analyses our qualitative data and brought structure to the development and presentation of our findings and analysis. Fig. 2 outlines the data structure derived from this approach. The findings and analysis section of the paper is structured according to the inductively derived 'Aggregate Dimensions' outlined in Fig. 2.

4. Research findings and analysis: three emergent challenges

In this section, we relate sourcing trends in financial services to the risks our research points to relative to the growing regulatory regime. The three challenges the research highlights are: lack of transparency and impaired control over Cloud deployments; conflicting data rights and data architectures; and Cloud vendor resilience and longevity. These challenges are interrelated and so 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).

Table 3
Data sources.

Primary data collection (42 interviews)				
	2 Law firms	2 Auditing/consulting organizations	6 SaaS /ITO/BPO vendors	4 Outsourcing financial organizations
Regulation lawyers	3 Interviews	2 Interviews		3 Interviews
Outsourcing contracts lawyers	4 Interviews	2 Interviews		2 Interviews
Departmental heads				5 Interviews
Process owners				6 Interviews
Compliance/risk executives				4 Interviews
IT professionals		2 Interviews		3 Interviews
Vendor consultants			6 Interviews	

Secondary data sources					
Cloud vendor manuals	SaaS vendor website and marketing materials	Financial organizations' website and marketing materials	Commentary and white papers from legal, consulting and accounting firms	Legislative acts and directives, regulatory rules and guidance	Field notes derived from co-author's role as academic advisor to law firms

4.1. Challenge 1: lack of transparency and impaired control over Cloud deployments

Our interviews showed that technological and service innovation can create 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.*' Furthermore, reviewing the legislation, the UK Regulator's 2014/15 Risk Outlook (FCA, 2014c) 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.*'

Consequently, 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

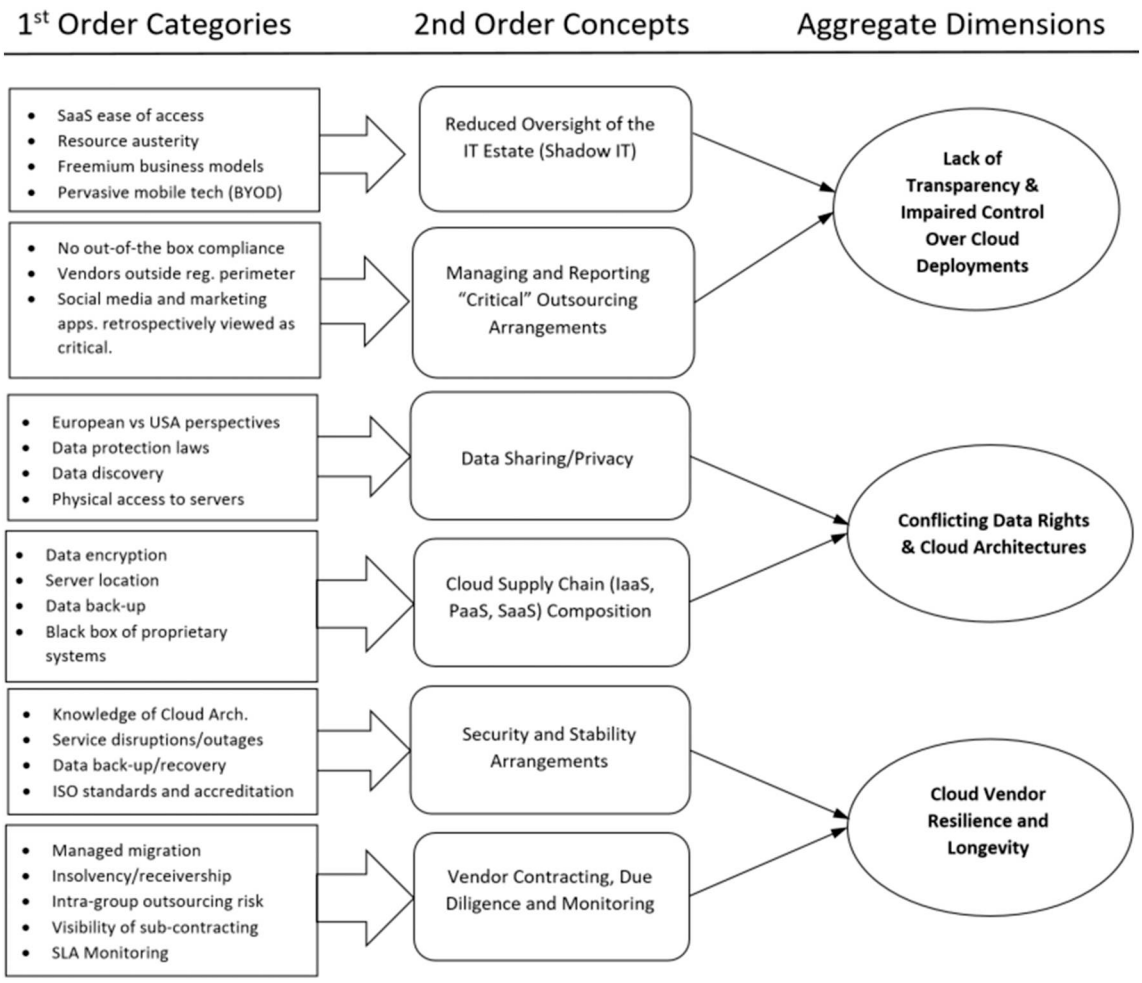

Fig. 2. Data structures.

and report on such practices, both internally and to regulators. One regulator states: '*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.*' and, '*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*' (FCA, 2014c). Clearly, where a firm's central IT or compliance function remains unaware of SaaS relationships this becomes problematic. Our respondents expressed concern over how easily individuals or departments may quickly create new Cloud arrangements and then use SaaS applications 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) not monitor it. Any of these may cause the firm to be in breach of regulatory rules (FCA, 2013b) and reduce the firm's ability to consolidate license agreements and make related savings.

For example, one of our interview 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. This challenge is further complicated by the pervasive use of SaaS and mobile technologies. Thus, a compliance officer interviewed stated: '*None of the Cloud vendors I know can provide a compliant solution straight out-of-the-box. The technology needs to be assessed for compliance and we need to be able to provide input, which we can't do if we don't know it's in play*.' Following the financial crisis, organizations of all sizes have seen their margins cut and have 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 these activities can 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.

Our interviewees suggested that even where firms do have a complete picture of all SaaS arrangements, should a breach occur the regulator may decide that SaaS applications 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 the firms' culture and individuals' conduct which may be questioned 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, while posts may be seen as evidence of the firm's culture of individual (mis)conduct. Marketing applications may be seen as critical where such applications are implicated in investigations of mis-selling and failure to treat customers fairly. 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 (Stratecast, 2013).

To summarize, 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. Moreover, the common obligation to document accurately and audit outsourcing arrangements is clearly confounded if the organization does not have clear visibility of such arrangements.

4.2. Challenge 2: conflicting data rights and Cloud architectures

According to our interviews and review of regulation and cases, regulatory tensions do emerge from different perspectives of data privacy rights. '*One lawyer commented: 'The European perspective emphasizes individuals' inalienable right to privacy and so is in stark contrast to the USA, where litigants have a broadly held right to discoverable, electronically stored data which may be used as evidence in court*'.[5] Thus our second challenge stems from a lack of visibility of vendor architectures and control over personal data storage in global organizations. In 2014, the UK financial services regulatory body 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.*' A 2016 study reviewed 22,000 Cloud applications and found that 75.4% were not ready for upcoming changes in data protection laws (NTT Communications, 2016). Key shortcomings included: lack of data encryption and security, lack of functionality for data export through download (in the event the customer ceases to use the application), failure to make audit logs available and contracts which omit clearly stating that the customer owns the data (Netskope, 2016).

Our research participants explained that obligations to monitor outsourcing providers may create new data discovery challenges. Transgressions may occur in the processing of both employee and client data. For example, how can firms monitor and be assured that their outsourcing providers' employees haven't utilized SaaS applications and moved crucial elements of personal data outside of regulatory jurisdictions (for example into Russia or China) where the application 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 applications are identified as particularly high risk for potential data breaches (Stratecast, 2013). As one IT manager noted: '*When users adopt SaaS they effectively extend their firm's IT infrastructure and hand over control of key architectural elements such as the network, storage, server and operating systems that support the application being provided.*' Our r4poisnetd highlighted a lack of visibility across the Cloud supply chain (SaaS, IaaS, PaaS) as a major risk. 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 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.*'

A further risk identified by out interviewees was that, firms may have no idea how reliable the IT architecture of their vendors is, and no clear details about where their data is stored. But 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. The UK regulator's handbook 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*[6] (FSA, 2010).'

Data privacy regulations provide specific challenges for those

[5] This conflict is not new the French Blocking Statue was introduced in 1968, in response to a USA antitrust investigation into French shipping companies.

[6] Related guidance clarified that 'business premises' may include head offices, operations centers, as well as data centers.

adopting SaaS solutions with or without the knowledge of the IT function. 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…*'

Firms and individuals can be heavily fined where data breaches occur. Yet, as one interviewee explained, often individuals can easily move data outside the firm's technological boundaries through memory sticks or by emailing data to themselves. As data protection rules apply universally, so the related risks also apply across all industries and sectors. Data breaches may result in criminal offences which can result in prosecutions against directors and officers of companies. This situation may occur where disclosing personal data without consent and/or selling or offering to sell such data has occurred. 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. The President and Sales Manager of Gunn Allen were each individually fined $20,000, while the Chief Compliance Officer was fined $15,000 (Schwartz, 2011).

Thus, while the Cloud is often touted as allowing organizations to cease worrying about managing and maintaining IT infrastructures, organizations must still understand their vendors' technical architectures to ensure data privacy rules and regulations are followed. 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. This emerged as 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 USA) 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, one example being the fine levied on Zurich Insurance (see below).

4.3. Challenge 3: Cloud vendor resilience and longevity

The UK regulator explicitly 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 (FCA, 2013b).' Building on this, our third challenge addresses the need to evaluate the reliability and longevity of Cloud vendors.

Many of our respondents highlighted the need for firms to have a good understanding of their vendors' architecture and supply chain 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.

A related risk observed by many of the interviewees was that, SaaS arrangements casually set up but underpinning business-critical processes may cause severe regulatory breaches should the vendor cease to operate. A regulator 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*' (FCA, 2013a).

Adopting Cloud - and particularly SaaS - applications creates specific regulatory risks around the supply chain of business-critical applications. Our respondents highlighted how firms may lack visibility and control over security arrangements across third party infrastructures, platforms, and applications. Subscription based applications may provide poor or no guarantees in terms of cybersecurity. Non-IT savvy staff subscribing to SaaS applications without the approval of the IT function may not be fully aware of the extent to which employees are ceding control to a third party or parties. Several of the lawyers we interviewed explained how under this scenario these employees may unwittingly create a 'critical' outsourcing arrangement. They advised that firms are required to ensure that outsourcing arrangements do not materially impact critical operations and controls, or impede monitoring by the regulator.

Crucially, firms must inform the regulator when they intend to rely on a third party or internal shared service centers for performing 'critical' operational functions (FCA, 2016b). CIOs explained how their firms 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 outsourcing governance 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. The complexity of managing ever more complex outsourcing arrangements is further compounded as robust governance requires cross-disciplinary knowledge and cooperation across a wide range of business units including legal teams, audit, compliance, technology and individual lines of business.

The research participants indicated that risk also comes poor contracting, due diligence and monitoring for example by not understanding how robust a SaaS supplier is and not having arrangements in place should they cease to operate. Prior to the introduction of Cloud technology, when traditional application providers have gone 'bust', user organizations have been able to gain access to the source code through escrow arrangements and often have the applications and data hosted on their own internal systems anyway. 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 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.*'

Our respondents felt that while the large IaaS and PaaS (e.g. Google and Amazon) operators are less likely to cease operation suddenly, the SaaS providers who sit upon 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 sub-contractors, 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. According to our interviewees, suppliers are often 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. 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.

A further challenge, highlighted through the recursive analysis of interviews and secondary data, relates to firms who rely on intra-group outsourcing arrangements.[7] The regulator's supervisory focus may not be limited to external third-party arrangements. A review by the UK regulator 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 outsourcing 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, 2013c).'

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. But 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.

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 summary, one often touted advantage of the Cloud is to remove the overheads of running applications onsite. Yet 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.

5. Discussion: managing the Cloud and regulatory risk

A key question this section addresses is: how can business managers bring order and control to bear on a highly complex, sometimes inconsistent and constantly changing set of regulations and practices? A survey of compliance officers, concluded that the compliance department has the potential to be disruptive in a positive way (Accenture, 2015). 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, yet useful practices into a more systematic response and builds from our primary data interviews as well as published guidance from global regulators including FCA, OCC, FED, FDIC, BIS, FMA. Fig. 3 outlines a framework for managing outsourcing regulations and is structured around three themes: Investigate, Strategize and Govern. While the focus of our study is predominately focused on Cloud deployments in financial services this framework may also be used to manage other outsourcing arrangements in other highly regulated industries.

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.

5.1. Addressing the Cloud Dilemma: to outsource or not to outsource…?

The state of affairs detailed above leaves executives, particularly those in highly regulated industries, with a difficult dilemma regarding when to adopt Cloud based technologies, how they should be managed, and what capabilities are required to underpin related governance and supervision. To assist managers in assessing the risks involved and correspondingly when to engage, we offer Fig. 4, which provides a matrix with two continuums. The first addresses the criticality of affected services to maintain compliance. The second addresses managers' ability to understand and control transparency and supervision over Cloud arrangements and draws upon the challenges and risks previously outlined.

5.2. Review regulatory exposure and new and existing outsourcing arrangements

The following sections outline each element of the management model outlined in Fig. 3. requires firms to understand the levels of regulatory exposure in outsourcing arrangements. 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/Cloud arrangements are considered. Firms should then consider potential arrangements against the outsourcing strategy, policies, controls and risk appetite outlined in parts 5.3 & 5.4 of the model; also where 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 comply with the promise of no further disciplinary action taken. Another approach is to employ a software vendor who offers the service of identifying and reviewing Shadow IT arrangements. Forensic tools such 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 interviewees revealed that where individuals take data outside of the organization's technological architectural boundaries, such tools may be less effective.

5.3. Evaluate supplier operational, technical & data risks

This element of our model requires firms to consider systemic risks inherent in collective arrangements and also risks related to discrete

[7] Intra-group outsourcing is an arrangement in which one company within a group of companies provides services for another company within the same group that could also be or usually have been provided in-house.

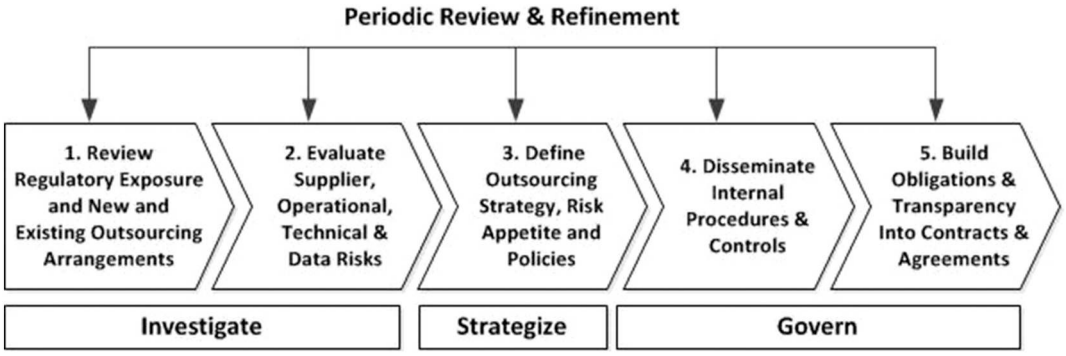

Fig. 3. Managing Cloud arrangements for regulatory compliance.

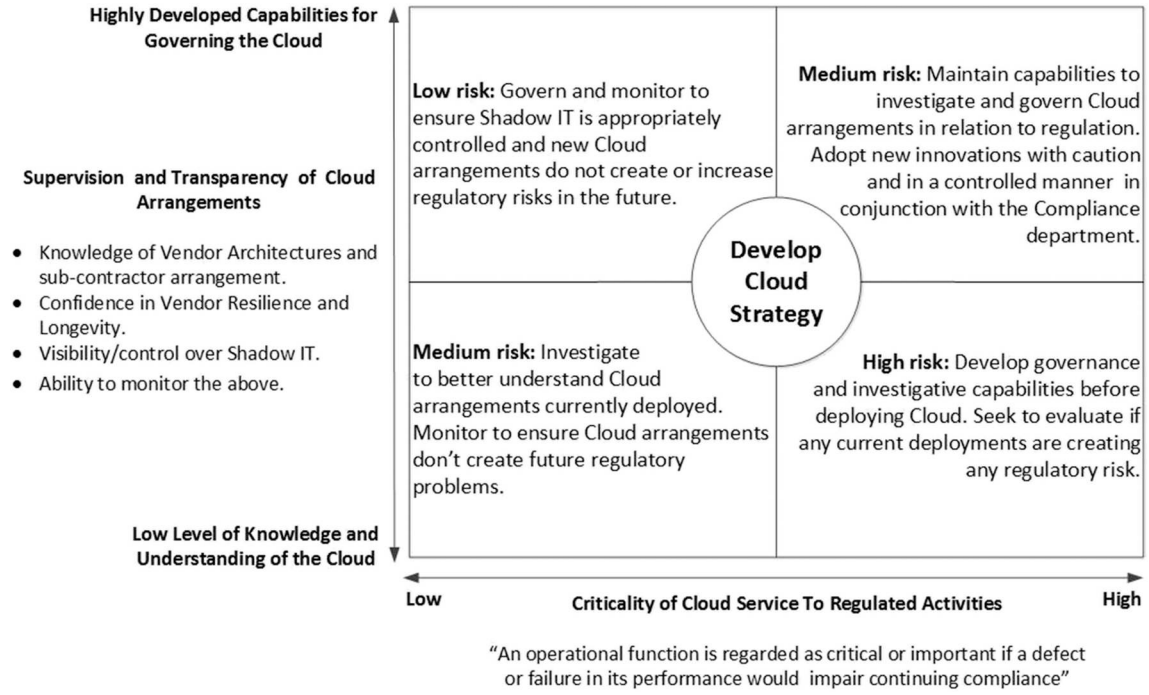

Fig. 4. Solving the Cloud Dilemma: What's the risk?

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, security of data at rest and in-transit, segregation of data from other clients, physical location of data, back up and 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/Cloud 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.

5.4. Define outsourcing strategy, risk appetite and practices

At the center of the management model (Fig. 3) 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 to outside the organization is high risk because organizations remain ultimately responsible for such practices.

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 on arrangements and related risks allows firms to take a more strategic view of their outsourcing regulations. This means firms 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 that can be distilled into controls, standards and metrics which may ultimately be built into the outsourcing agreement/contract.

5.5. Disseminate internal procedures and controls

It is important that responsibilities of the organizations and specific individuals 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, while 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.

5.6. 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 contractual 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. Firms need to build in rights of access to the vendor's premises to assess their data management and security and architectures. In addition, firms must explicitly require that vendors respond to regulators' requests to visit their premises and for information. 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.

6. Conclusions

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 worldwide. The challenges, risks and management practices outlined will also be of considerable relevance to other regulated industries. The frameworks we have developed, from our research findings, provide practitioners with a structured approach for addressing the right balance and understanding how regulation impacts their outsourcing strategy and how related obligations and risks may be managed and mitigated, regardless of the industry under review.

One emerging implication from our work is that with the commodification of IT through the Cloud and the increasing presence of Shadow IT, the role of the CIO would seem to be coming less relevant. If IT ‘comes through the wall’ (in the same way as electricity or gas) then there is, perhaps, a reduced need for a centralised IT group. Furthermore, if ‘coal-face’ staff are now able to select, source and deploy their own solutions the need for a centralised IT department is further eroded. Such departments are also expensive and employ costly staff.

Our work suggests, however, that this would be a very misguided assumption. In practice, Cloud, Shadow IT and growing regulation across industries and geographies collectively create a new and important role for the CIO beyond that of ‘gatekeeper’ or the department who merely keeps the IT services ‘switched on’. The emergent environment we detailed here creates an opportunity for the CIO to be creative, setting standards of governance that manage risk and ensure security while being a facilitator for new innovations, and correspondingly a source of competitive advantage. The challenge for organizations is to strike the right balance between innovation and control of technological arrangements, and the CIO is ideally placed to fulfil this role.

As a concluding comment, we identify outsourcing and regulation as an 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 (Big Data, Blockchain and Distributed Ledgers, Robotics and Artificial Intelligence, Internet of Things) across a range of industries, countries and regulatory jurisdictions, which are often both complementary and conflicting yet always highly complex.

Acknowledgements

We would like to acknowledge the excellent feedback provided by the special issue's editors Joseph Amankwah-Amoah and Xiaojun Wang and the anonymous reviewers. We would also like to acknowledge valuable feedback provided by Michelle Kaarst-Brown, Martin Mocker, Dorothy E. Leidner and Jeanne Ross during a presentation of an early draft of this paper. Any remaining errors are our own.

Appendix A. Global regulators' rules and guidance

Table 4
Outsourcing regulatory rules and guidance.
Source: Various USA and European Regulators.

European and USA Regulators' Outsourcing Guidance				
Date	Regulator	Country	Document	Key Comments and Findings
07/07/2016	**FCA**	**UK**	**FG16/5: Guidance for firms outsourcing to the 'cloud' and other third party IT services**	Our responses to the feedback we received on Guidance Consultation GC15/6 is set out in the annex of this finalised guidance. We do not consider that the feedback received requires substantial changes to our guidance and proposed approach as set out in GC15/6. However, in some areas we have amended the draft guidance, mostly to clarify our expectations. The main feedback issues were: • physical access to business premises, including data centers • the scope of firms' obligations relating to supply chain and sub-contracting arrangements • clarifying expectations around aspects of risk management, including concentration risk • points around the choice and control in relation to the jurisdictions where data is processed, stored and managed • the provisions to ensure firms have effective access to data • specific expectations around exit plans.
24/03/2015	**FCA**	**UK**	**Business Plan 2015/16 : Risk Outlook**	**Failure to invest and maintain** A significant amount of ongoing technological investment is required to enter or continue being present in a market. The complexity and cost of such systems encourages firms to modify existing systems to deliver new functionality rather than replace them. As a consequence, systems may become increasingly complex, less resilient and potentially less secure. This gives rise to a number of risks, for example, a failure in a firm's IT systems can significantly harm consumers. Outages can lead to consumers being unable to complete transactions, incurring fees on late payments and having a domino effect on transaction counterparties. The increased reliance on third parties in an outsourced, offshore model for the maintenance of key systems may also affect the speed of response to critical failures, leading to extended periods in which consumers suffer harm. Indeed, the perceived failure of a firm to provide an effective, secure and resilient systems environment can affect the reputation of the firm and lead consumers to withdraw their business. This could cause a market integrity issue.
31/03/2014	**FCA**	**UK**	**FCA 2014 Risk Outlook**	**Over-reliance on third parties** 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. Investment businesses that use third party administrators to handle and record the firms' client money need to be aware that their responsibilities are not discharged merely through a rigorous selection process and the receipt of reports on breaches of rules and service levels. The regulated firms retain responsibility for ensuring that the outsourced functions are compliant and should carry out active monitoring to discharge that responsibility. Some investment businesses may need to make significant changes to their businesses processes and systems and as a result of changes to the client asset rules which will be published in 2014. They will need to work closely with third party administrators to ensure that these changes are implemented effectively and on time. Where firms are using unregulated third party tools, for example, risk profiling tools, that have been developed by unregulated entities, they must ensure they have the appropriate knowledge and expertise to use these tools to ensure good outcomes for consumers. In addition, regulated firms have the responsibility to ensure the way in which risk profiling tools are used, and the way they use information, meets their requirements as regulated bodies.

(*continued on next page*)

Table 4 (*continued*)

European and USA Regulators' Outsourcing Guidance

Date	Regulator	Country	Document	Key Comments and Findings
30/10/2013	**OCC**	**USA**	**OCC Bulletin 2013-29: Third Party Relationships**	The OCC is concerned that the quality of risk management over third-party relationships may not be keeping pace with the level of risk and complexity of these relationships. The OCC has identified instances in which bank management has • failed to properly assess and understand the risks and direct and indirect costs involved in third-party relationships. • failed to perform adequate due diligence and ongoing monitoring of third-party relationships. • entered into contracts without assessing the adequacy of a third party's risk management practices. • entered into contracts that incentivize a third party to take risks that are detrimental to the bank or its customers, in order to maximize the third party's revenues. • engaged in informal third-party relationships without contracts in place.
05/12/2013	**FED**	**USA**	**Guidance on Managing Outsourcing Risk**	The Federal Reserve is issuing the attached *Guidance on Managing Outsourcing Risk* to assist financial institutions1 in understanding and managing the risks associated with outsourcing a bank activity to a service provider to perform that activity. This Federal Reserve guidance builds upon the *FFIEC Outsourcing Technology Services Booklet* (2004) that addresses outsourced information technology services and remains in effect.
30/06/2011	**BIS: Basel Committee on Banking Supervision**	**Switzerland**	**Principles for the Sound Management of Operational Risk**	Senior management should ensure that staff responsible for managing operational risk coordinate and communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those in the bank who are responsible for the procurement of external services such as insurance risk transfer and outsourcing arrangements. Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme The use of technology related products, activities, processes and delivery channels exposes a bank to strategic, operational, and reputational risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing technology risks.21 Sound technology risk management uses the same precepts as operational risk management and includes: (a) governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with and supportive of the bank's business objectives; (b) policies and procedures that facilitate identification and assessment of risk; (c) establishment of a risk appetite and tolerance statement as well as performance expectations to assist in controlling and managing risk; (d) implementation of an effective control environment and the use of risk transfer strategies that mitigate risk; and (e) monitoring processes that test for compliance with policy thresholds or limits. Outsourcing is the use of a third party – either an affiliate within a corporate group or an unaffiliated external entity – to perform activities on behalf of the bank. Outsourcing can involve transaction processing or business processes. While outsourcing can help manage costs, provide expertise, expand product offerings, and improve services, it also introduces risks that management should address. The board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities. Outsourcing policies and risk management activities should encompass: (a) procedures for determining whether and how activities can be outsourced; (b) processes for conducting due diligence in the selection of potential service providers; (c) sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights; (d) (d) programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider; (e) establishment of an effective control environment at the bank and the service provider; (f) development of viable contingency plans; and execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank. Internal audit coverage should be adequate to independently verify that the Framework has been implemented as intended and is functioning effectively.8 Where audit activities are outsourced, senior management should consider the effectiveness of the underlying arrangements and the suitability of relying on an outsourced audit function as the third line of defence

(*continued on next page*)

Table 4 (*continued*)

European and USA Regulators' Outsourcing Guidance

Date	Regulator	Country	Document	Key Comments and Findings
09/11/2015	**SEC**	**USA**	**Examinations of Advisers and Funds That Outsource Their Chief Compliance Officers**	OCIE staff (the 'staff') have noted a growing trend in the investment management industry: outsourcing compliance activities to third parties, such as consultants or law firms. Some investment advisers and funds have outsourced all compliance activities to unaffiliated third parties, including the role of their chief compliance officers ('CCOs'). Outsourced CCOs may perform key compliance responsibilities, such as updating firm policies and procedures, preparing regulatory filings, and conducting annual compliance reviews. The staff conducted nearly 20 examinations as part of an Outsourced CCO Initiative that focused on SEC-registered investment advisers and investment companies (collectively, 'registrants') that outsource their CCOs to unaffiliated third parties ('outsourced CCOs'). The purpose of this Risk Alert is to share the staff's observations from these examinations and raise awareness of the compliance issues observed by the staff
12/11/2015	**FCA**	**UK**	**Proposed guidance for firms outsourcing to the 'cloud' and other third-party IT services**	Innovation can be a driver of effective competition, so we want to support innovation and ensure that regulation unlocks these benefits, rather than blocks them. Stakeholders including firms and cloud service providers have told us that they are unsure about how we apply our rules relating to outsourcing to the cloud. Through roundtable discussions and other interactions with firms and cloud service providers; we understand that this uncertainty may be acting as a barrier to firms using the cloud.
11/12/2012	**FCA**	**UK**	**Dear CEO… Review of Outsourcing Arrangements in the Asset Management Sector**	The FSA is assessing the risk to our objectives arising from asset management firms outsourcing operational activities to external service providers. Our initial discussions and research have identified that the asset management industry outsources a growing number of activities, and that the small number of outsource providers are usually part of complex international banking groups. At group level, these organisations will have balance sheet exposure to activities other than the provision of outsourcing activities. Our concern is that if an outsource provider were to face financial distress or severe operational disruption, UK asset managers would not be able to perform critical and important regulated activities, thereby causing detriment to customers
11/11/2013	**FCA**	**UK**	**TR13/10 - Outsourcing in the asset management industry**	(1) Resilience risk Last year we found that asset managers were largely unprepared for the failure of a service provider undertaking critical activities, as firms' contingency plans had not considered how to maintain operations and service to their customers. So we wrote to CEOs in December 2012 setting out our expectations of asset managers that outsource critical activities. 1 An asset manager is engaged in outsourcing if it appoints a service provider to conduct an activity which the asset manager would otherwise complete itself whilst conducting its regulated business. 2 Managers of alternative investment funds will become subject to the delegation rules in Article 20 of AIFMD. In addition, the common platform requirements (including SYSC 8) continue to apply to an AIFM investment firm which is a full-scope UK AIFM in respect of its MiFID business. 3 Link to Outsourcing Dear CEO Letter We are pleased with the level of engagement from asset managers in response to our Dear CEO letter and during 2013 we have started to see improvements in asset managers' planning for the failure of a service provider. We are also encouraged by the industry-led work intended to help firms with contingency planning. This work is being driven forward by the Outsourcing Working Group (OWG) 4 whom are devising principles to guide the industry, with a key aim of improving portability between providers. In addition to helping mitigate the resilience risk, there could be wider benefits to the industry and their customers if asset managers were able to move service providers more readily. The detailed findings on Resilience risk are in Section 4 of this report. (2) Oversight risk We are reassured that all asset managers within the sample had oversight arrangements in place to oversee their service providers. The effectiveness of oversight arrangements varied from firm to firm, with only some asset managers able to demonstrate high standards of oversight consistently across all outsourced activities. Where oversight of an activity was lacking, we found the main cause was insufficient internal expertise to carry out the oversight. The detailed findings on Oversight risk are in Section 5 of this report.

(*continued on next page*)

Table 4 (*continued*)

European and USA Regulators' Outsourcing Guidance

Date	Regulator	Country	Document	Key Comments and Findings
12/11/2015	**FCA**	**UK**	**Proposed guidance for firms outsourcing to the 'cloud' and other third-party IT services**	1.3 Stakeholders including firms and cloud service providers have told us that they are unsure about how we apply our rules relating to outsourcing to the cloud. Through roundtable discussions and other interactions with firms and cloud service providers; we understand that this uncertainty may be acting as a barrier to firms using the cloud. 1.4 'Cloud' is a broad term, and stakeholders have interpreted it differently. The FCA sees the cloud as encompassing a range of IT services provided in various formats over the internet. This includes, for example, private, public or hybrid cloud, as well as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Cloud services are constantly evolving. Our aim is to avoid imposing inappropriate barriers to firms' ability to outsource to innovative and developing areas, while ensuring that risks are appropriately identified and managed. 1.5 There are particular risks associated with outsourcing to the cloud which differ from traditional outsourcing arrangements, and these risks primarily affect the degree of control exercised by the firm. a. Cloud customers may have less scope to tailor the service provided. b. Cloud customers may also have to accept that cloud service providers will move their data around; however, in some cases, cloud customers may be able to specify which overall geographic region in which their data is stored. c. Firms should also consider the risks associated with outsource service providers who may contract out part of their operation to other cloud providers. This may occur without the firm initially realising. 1.6 We are therefore setting out in more detail our approach to regulating firms who outsource to the cloud and other third-party IT services. We see no fundamental reason why cloud services (including public cloud services) cannot be implemented, with appropriate consideration, in a manner that complies with our rules. 1.7 Firms should also be aware of international developments taking place that are likely to have an impact on their decision-making process regarding the use of cloud services: notably, the new EU Digital Single Market strategy and reform of EU Data Protection legislation. These are evolving areas and the FCA is engaging in this work as proposals are developed. As such, firms and service providers should continue to monitor EU developments and the impact on their business. 1.8 We are required to consult on this guidance because it constitutes 'guidance on rules'. This guidance is not binding, however we expect firms to take note of the guidance and, where appropriate, use it to inform their systems and controls on outsourcing. 1.9 The guidance is not exhaustive, nor should it be read in isolation. Firms should consider this guidance in the context of their overarching obligations under the regulatory system. The FCA, based on its statutory objectives, is of the view that complying with this guidance will generally indicate compliance with the aspects of the FCA rule or other requirement to which the guidance relates, though it is not exhaustive. The PRA has different statutory objectives, and so firms that are subject to PRA regulation should confirm their approach with the PRA. FCA guidance on rules, the Act or other legislation represents the FCA's view, and does not bind the PRA or the courts.
12/11/2015	**PRA**	**UK**	**Outsourcing functions to the Cloud**	On 12 November 2015 the Financial Conduct Authority (FCA) published a consultation for firms seeking to outsource functions to the Cloud1 . The Prudential Regulation Authority (PRA) is working closely with the FCA on matters relating to the Cloud and other types of outsourcing. Dual-regulated firms seeking to outsource to the Cloud, or any similar arrangements, are reminded of the Fundamental Rules2 and requirements as set out in the relevant parts of the PRA Rulebook3 , under which they are obliged to notify the regulators of anything they would expect reasonable notice. With this in mind, dual-regulated firms considering outsourcing critical or important functions to a third-party IT provider, including to the Cloud, should liaise with their usual supervisory contact at the earliest opportunity. Dual-regulated firms may also want to refer to PRA publications such as Supervisory Statement 19/13 'Resolution planning', January 2015 and Consultation Paper 38/15 'Ensuring operational continuity in resolution', October 2015. In its consultation paper the FCA defines Cloud as 'The 'cloud' is a broad term, and stakeholders have interpreted it differently. The FCA sees the 'cloud' as encompassing a range of IT services provided, in various formats, over the internet. This includes for example, private, public or hybrid 'cloud' and Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Cloud services are evolving all the time.' 2 In particular Fundamental Rule 7. 3 The relevant requirements are set out in the Outsourcing Part of the PRA Rulebook for Capital Requirements Regulation (CRR) firms and in SYSC Chapter 8 (Outsourcing) for non-CRR firms. Until Solvency II is implemented, the equivalent provisions for insurers are SYSC 3.2.4G and 13.9.

(*continued on next page*)

Table 4 (*continued*)

European and USA Regulators' Outsourcing Guidance

Date	Regulator	Country	Document	Key Comments and Findings
07/07/2014	**FCA**	**UK**	**Considerations for firms thinking of using third-party technology (off-the-shelf) banking solutions**	In practical terms, we are looking for the following outcomes: At the time of authorisation, a firm's regulated activities must be supported by IT services which are effective, resilient and secure and have been appropriately designed to meet expected future as well as current business needs so as to avoid risks to our objectives. • The firm must have undertaken sufficient preparatory work to provide reasonable assurance that each OSP will deliver its services effectively, resiliently and securely. • The firm has established appropriate arrangements for the on-going oversight of its • OSPs and the management of any associated risks such that the firm meets all its regulatory requirements.
10/07/2012	**FFIECl**	**USA**	**Outsourced Cloud Computing**	The Federal Financial Institution Examination Council Agencies consider cloud computing to be another form of outsourcing with the same basic risk characteristics and risk management requirements as traditional forms of outsourcing. This paper addresses the key risks of outsourced cloud computing identified in existing guidance. Cloud computing is a relatively new term used to describe a variety of established business strategies, technologies, and processing methodologies. Although the term cloud computing is gaining in usage, there is no widely-accepted definition, 1 and numerous business strategies, technologies, and architectures are represented as cloud computing. In general, cloud computing is a migration from owned resources to shared resources in which client users receive information technology services, on demand, from third-party service providers via the Internet 'cloud.' Cloud computing has several service and deployment models. The service models include the provision of infrastructure, computing platforms, and software as a service. The deployment models relate to how the cloud service is provided. These models include: a private cloud, which is operated solely for an organization; a community cloud, which is shared by several organizations; a public cloud, which is available to any paying customer; and a hybrid cloud, which is a composition of two or more clouds (private, community, or public). Financial institutions that contemplate or use a cloud computing model in which all or part of the service is outsourced ('outsourced cloud computing') have to consider the fundamentals of risk and risk management defined in the FFIEC Information Technology Examination Handbook (IT Handbook), especially the Outsourcing Technology Services Booklet ('Outsourcing Booklet').
14/03/2016	**FDIC**	**USA**	**Technical Assistance Video on Outsourcing Technology Services**	Highlights: • As financial institutions become more involved in technology outsourcing, they must manage the risks associated with reliance on third-party service providers. Outsourcing has become more complex, with many banks using vendors for key business functions and relying on multiple providers. • The video on outsourcing technology services discusses the responsibilities of financial institutions' boards of directors and senior management in governing their institutions' vendor-management program. • A vendor-management program represents the policies and procedures established to select and monitor third-party relationships. • The video covers the main components of a vendor-management program, including the risk-assessment process, the service-provider selection program, contract negotiation and evaluation, and ongoing monitoring. • The video also discusses business continuity planning and testing, and resources available to assist institutions in establishing and maintaining a sound vendor-management program. • The video is available for viewing on the FDIC's website at https://www.fdic.gov/regulations/resources/director/virtual/vendor.html. • Alternatively, FDIC-insured institutions may download the video through FDICconnect by contacting their FDICconnect coordinator.
07/04/2014	**FDIC**	**USA**	**Technology Outsourcing: Informational Tools for Community Bankers**	Highlights: • The attached three documents, first issued on June 4, 2001, contain practical ideas for banks to consider when they engage in technology outsourcing. • These documents are intended to assist community bankers by providing information on: • Effective Practices for Selecting a Service Provider, • Tools to Manage Technology Providers' Performance Risk: Service Level Agreements, and • Techniques for Managing Multiple Service Providers. • The attached documents are for informational purposes only and are not considered to be official examination guidance. • Examination guidance and additional information on vendor management can be found in the FFIEC IT Examination Handbook, Outsourcing Technology Services. This guidance focuses on four key areas: risk assessment, service provider selection, contract terms, and oversight of outsourcing arrangements.

(*continued on next page*)

Table 4 (*continued*)

European and USA Regulators' Outsourcing Guidance				
Date	Regulator	Country	Document	Key Comments and Findings
06/11/2012	**FDIC**	**USA**	**Supervision of Technology Service Providers and Outsourcing Technology Services**	Highlights: • The FFIEC has issued a revised Information Technology (IT) Examination Booklet on the Supervision of Technology Service Providers (TSP Booklet), which addresses the supervision of third-party servicers that enter into contracts with regulated financial institutions and outlines the FFIEC's risk-based supervisory program related to the oversight of TSPs. • The revised TSP Booklet replaces the March 2003 edition and rescinds Supervisory Policy 1, 'Interagency EDP Examination, Scheduling and Distribution Policy,' September 1991 (Revised) and Supervisory Policy 11, 'Enhanced Supervision Program for Multidistrict Data Processing Servicers,' January 1995. • The Agencies have issued new Administrative Guidelines—Implementation of Interagency Programs for the Supervision of Technology Service Providers, which explain how the Agencies implement TSP supervisory programs. The Guidelines include examiner reporting templates. • The FFIEC has also updated the Outsourcing Technology Services Booklet, which details engagement criteria and examination procedures a financial institution should use when outsourcing the security management function to third parties (Managed Security Service Providers).
13/04/2012 reissued 31/10/16	**CFPB**	**USA**	**CFPB Bulletin: Service Providers**	The Consumer Financial Protection Bureau (CFPB) expects supervised banks and nonbanks to oversee their business relationships with service providers in a manner that ensures compliance with Federal consumer financial law, which is designed to protect the interests of consumers and avoid consumer harm. The CFPB's exercise of its supervisory and enforcement authority will closely reflect this orientation and emphasis. Title X authorizes the CFPB to examine and obtain reports from supervised banks and nonbanks for compliance with Federal consumer financial law and for other related purposes and also to exercise its enforcement authority when violations of the law are identified. Title X also grants the CFPB supervisory and enforcement authority over supervised service providers, which includes the authority to examine the operations of service providers on site.1 The CFPB will exercise the full extent of its supervision authority over supervised service providers, including its authority to examine for compliance with Title X's prohibition on unfair, deceptive, or abusive acts or practices. The CFPB will also exercise its enforcement authority against supervised service providers as appropriate. The CFPB expects supervised banks and nonbanks to have an effective process for managing the risks of service provider relationships. The CFPB will apply these expectations consistently, regardless of whether it is a supervised bank or nonbank that has the relationship with a service provider. The Bureau expects that the depth and formality of the entity's risk management program for service providers may vary depending upon the service being performed - its size, scope, complexity, importance and potential for consumer harm - and the performance of the service provider in carrying out its activities in compliance with Federal consumer financial laws and regulations. While due diligence does not provide a shield against liability for actions by the service provider, it could help reduce the risk that the service provider will commit violations for which the supervised bank or nonbank may be liable, as discussed above.
15/09/2013	**BaFIN**	**Germany**	**Outsourcing: BaFin compares outsourcing by institutions**	BaFin has analysed banks' outsourcing activities as part of a comparative study. This examined, among other things, the number of outsourcing activities, their geographical distribution, their integration into the business strategy, the risk analysis to be carried out by institutions prior to outsourcing, and monitoring and management of outsourcing by the institutions.
01/06/2010	**AMF**	**France**	**Outsourcing Risk Guideline**	This guideline sets out the AMF's expectations with respect to sound outsourcing risk management practices. Under the various sector-based laws it administers, the AMF has the authority1 to establish guidelines regarding sound and prudent management practices for financial institutions.
19/03/2013	**CSSF**	**Luxembourg**		

(*continued on next page*)

Table 4 (*continued*)

European and USA Regulators' Outsourcing Guidance				
Date	Regulator	Country	Document	Key Comments and Findings
			Update of Circular 12/552 on the central administration internal governance and risk management	The Circular CSSF 12/552 on Central Administration, Internal Governance and Risk Management The Circular CSSF 12/552 on Central Administration, Internal Governance and Risk Management gathers all (multiple) former circulars dealing with central administration, internal audit and control, compliance, risk (partially at this stage) and governance in one single circular. The circular also transposes a.o. the Guidelines on Internal Governance of the European Banking Authority (GL 44 of September 2011) and the guidelines from the Basel Committee on Banking Supervision on the Internal audit function in banks of June 2012. The purpose of this Circular is to ensure that entities in scope have a robust and formalised internal governance framework, allowing a sound and prudent management of risks. New requirements The requirements of this circular are numerous and huge. The Circular introduces a.o.: Significant changes in Board of Directors' composition and responsibilities New responsibilities for the authorised management, a.o. in its interaction with the three (Audit, Compliance and Risk) internal control functions, but also with the Board of Directors and with the CSSF A revision of the three internal control functions, including the new mandatory risk control function Requirements relating to the financial and accounting function and to the IT function with new requirements regarding the IT organisation including two mandatory functions: The IT officer and the Information Security Officer The implementation of a whistleblowing process allowing staff to notify any concern relating to governance, with adequate protection for the whistleblower

Appendix B. Outsourcing risks

Table 5
Types of outsourcing risk.
Source: Basel Committee on Banking Supervision 2005 'Outsourcing in Financial Services' Bank for International Settlements; Joint Forum & Board of Governors of the Federal Reserve System 2013 'Guidance on Managing Outsourcing Risk' Division of Banking Supervision and Regulation; Division of Consumer and Community Affairs and Federal Deposit Insurance Corporation 2004 'Appendix C—Outsourcing/Offshoring Risks' Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks, Federal Deposit Insurance Corporation 2004; Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks.

Outsourcing risks			
	Basel Committee on Banking Supervision (2005)	Federal Reserve System (2013)	Federal Deposit Insurance Corporation (2004)
Risk	Overview		
Strategic risk	• The third party may conduct activities on its own behalf which are inconsistent with the overall strategic goals of the regulated entity. • Failure to implement appropriate oversight of the outsource provider. • Inadequate expertise to oversee the service provider.		This is a risk to earnings or capital arising from adverse business decisions or improper implementation. The financial institution is also exposed to strategic risk when it uses a third party to perform banking functions or to offer products or services that do not help the financial institution achieve corporate strategic goals and provide an adequate return on investment. • Occurs when banking functions or products or services are offered that are not compatible with the bank's strategic goals. • Can occur when third-party relationships are used without fully performing due diligence reviews. • Can occur when risk management's scope or depth is not commensurate with the activity. • Can occur when the bank does not possess the adequate expertise to oversee the third party. • Financial institutions face the potential for loss of trade secrets if poor controls exist when a vendor performs work for competitors in the same outsource location.

(*continued on next page*)

Table 5 (*continued*)

Outsourcing risks			
	Basel Committee on Banking Supervision (2005)	Federal Reserve System (2013)	Federal Deposit Insurance Corporation (2004)
Risk	Overview		
Reputation risk	• Poor service from third party. • Customer interaction is not consistent with overall standards of the regulated entity. • Third party practices not in line with stated practices (ethical or otherwise) of regulated entity.	• Reputational risks arise when actions or poor performance of a service provider causes the public to form a negative opinion about a financial institution.	Risks to earnings or capital could arise from negative public opinion. • Arises from poor service, disruption of service, or violations of consumer law. • Occurs when third-party interaction with bank customers is not consistent with the bank's policies or standards. • Occurs when there is negative publicity about adverse events involving the bank
Compliance risk	• Privacy laws are not complied with. • Consumer and prudential laws not adequately complied with. • Outsource provider has inadequate compliance systems and controls.	• Compliance risks arise when the services, products, or activities of a service provider fail to comply with applicable U.S. laws and regulations	Risk to earnings or capital arises from violations of laws or regulations or nonconformance with internal policies or ethical standards. This risk exists when the activities of a third party are not consistent with law, policies, or ethical standards of the financial institution and the financial institution's country. This risk is exacerbated by an inadequate oversight and audit function. • Offshore vendors do not have the same privacy regulations as those that exist in the United States. • Can be due to improper review of products, services, or systems with respect to consumer law or other regulatory compliance matters. • Can occur if the bank's oversight program fails to include appropriate audit and control features. • Can occur if the vendor fails to adequately protect the privacy of nonpublic customer information.
Operational risk	• Technology failure. • Inadequate financial capacity to fulfil obligations and/or provide remedies. • Fraud or error. • Risk that firms find it difficult/costly to undertake inspections.	• Operational risks arise when a service provider exposes a financial institution to losses due to inadequate or failed internal processes or systems or from external events and human error.	Risks to earnings or capital arise from problems with service or product delivery. The lack of an effective business resumption plan and appropriate contingency plans increase transaction risk. • Occurs when products, services, delivery channels, and processes do not fit with the bank's systems, customer demands, or strategic objectives. • Weak control over technology used in the third-party arrangement may result in threats to security and the integrity of systems and resources. • Can be the result of fraud or error by the third party. • Arises from inadequate capacity, technology failure, or lack of effective business resumption and contingency planning by the third party. • Possible risks include liquidity, interest rate, price, and foreign currency transaction risk. • Loss of trade secrets is possible when an outsource company also does work with competitors.

(*continued on next page*)

Table 5 (*continued*)

Outsourcing risks			
	Basel Committee on Banking Supervision (2005)	Federal Reserve System (2013)	Federal Deposit Insurance Corporation (2004)
Risk	Overview		
Exit strategy risk	• The risk that appropriate exit strategies are not in place. • This could arise from over-reliance on one firm, the loss of relevant skills in the institution itself preventing it bringing the activity back in-house, and contracts which make a speedy exit prohibitively expensive. • Limited ability to return services to home country due to lack of staff or loss of intellectual history.		
Credit/ counter-party risk	• Inappropriate underwriting or credit assessments. • Quality of receivables may diminish.		This is a risk to earnings or capital that arise from the obligor's failure to meet the terms of any contract with the bank or to otherwise perform as agreed. The basic form of credit risk involves the financial condition of the third party itself. Appropriate monitoring of the activity of the third party is necessary to ensure that credit risk is understood and remains within board-approved limits. • Receivables quality declines as the third party performs inadequate account management, customer service, or collection activity. • Can occur when there is improper oversight of third parties who solicit and refer customers, conduct underwriting analysis, or set up other credit-related product programs. • Can occur when there is inadequate financial capacity by a third party to fulfil its contract with the bank.
Country risk	• Political, social and legal climate may create added risk. • Business continuity planning is more complex.	• Country risks arise when a financial institution engages a foreign-based service provider, exposing the institution to possible economic, social, and political conditions and events from the country where the provider is located.	• Assets might be confiscated by one or more governments. • Confiscatory tax rates or assessments could be imposed. • Employee risk-related issues. Background checks, etc.
Contractual risk	• Ability to enforce contract. • For offshoring, choice of law is important		
Access risk	• Outsourcing arrangement hinders ability of regulated entity to provide timely data and other information to regulators. • Additional layer of difficulty in regulator understanding activities of the outsource provider.		

(*continued on next page*)

Table 5 (*continued*)

Outsourcing risks			
	Basel Committee on Banking Supervision (2005)	Federal Reserve System (2013)	Federal Deposit Insurance Corporation (2004)
Risk	Overview		
Concentration and systemic risk	• Overall industry has significant exposure to outsource provider. This concentration risk has a number of facets, including: • Lack of control of individual firms over provider • Systemic risk to industry as a whole.	• Concentration risks arise when outsourced services or products are provided by a limited number of service providers or are concentrated in limited geographic locations.	
Legal risk		• Legal risks arise when a service provider exposes a financial institution to legal expenses and possible lawsuits.	
Event risk			(Source: Financial Services Technology Consortium 2004). • Disruption in Telecommunications • Severing of lines, destruction of infrastructure, failure of a telecommunications company, capacity problems in the grid, equipment or software failure, virus attack, human error, etc. • Disasters at a facility • Fire, building collapse, employee violence, hazardous material transportation accident, long-term water or electrical outage, etc. • Natural calamity • Hurricane, flood, tornado, earthquake, landslides, ice storms, heavy snowfall, extreme cold, etc. • Health Restrictions • Flu epidemic, SARS, Ebola, Aids, food poisoning, anthrax, biological weapons, plague, other infectious diseases. • Nuclear and chemical threats • Chemical spills and plant accidents, nuclear or chemical terrorism. • Visa restrictions • Government applies a quota or limit to visas that is lower than normal, processing time increases because of background checks, increased rejection of visa applications, etc. • Travel restrictions/aviation accidents

References

Accenture. 2015 compliance risk study: Be the disruptor, not the disrupted. (2015). http://www.accenture.com/us-en/Pages/insight-compliance-risk-study-2015-financial-services.aspx (Accessed 12th March 2016).

Amankwah-Amoah, J. (2016). An integrative process model of organisational failure. *Journal of Business Research, 69*(9), 3388–3397.

Amankwah-Amoah, J., Osabutey, E. L., & Egbetokun, A. (2018). Contemporary challenges and opportunities of doing business in Africa: The emerging roles and effects of technologies. *Technological Forecasting and Social Change, 131*, 171–174.

Ben-Shahar, O., & Logue, K. D. (2012). Outsourcing regulation: How insurance reduces moral hazard. *Michigan Law Review, 111*(2), 4–12.

BT. Research: Creativity and the modern CIO. (2015). http://www.globalservices.bt.com/uk/en/insights/creativity_and_modern_cio (Accessed 12th March 2016. Accessed 12th March 2016).

Carr, N. G. (2004). *Does IT matter. Information technology and the corrosion of competitive advantage.* Boston: Harvard Business School.

Cave, J., Robinson, N., Kobzar, S., & Schindler, H. R.. Regulating the cloud (March 30, 2012). (2012). http://ssrn.com/abstract=2031695 (Accessed 12th March 2016).

Clark, G. L., & Monk, A. H. B. (2013). The scope of financial institutions: In-sourcing, outsourcing and off-shoring. *Journal of Economic Geography, 13*(2), 279–298.

Currie, W. L., Gozman, D. P., & Seddon, J. J. (2017). Dialectic tensions in the financial markets: A longitudinal study of pre- and post-crisis regulatory technology. *Journal of Informtion Technology*. https://doi.org/10.1057/s41265-017-0047-5.

Denzin, N. K., & Lincoln, Y. S. (2000). *The Sage handbook of qualitative research.* London: Sage.

Economist, T. The fintech revolution. (2015). http://www.economist.com/news/leaders/21650546-wave-startups-changing-financefor-better-fintech-revolution (Accessed 25th March 2017).

FCA. SYSC 3.2 Areas covered by systems and controls. (2013). http://fshandbook.info/FS/html/FCA/SYSC/3/2 (Accessed 16th March 2017).

FCA. SYSC 8.1 General outsourcing requirements. (2013). http://fshandbook.info/FS/html/FCA/SYSC/8/1 (Accessed 16th March 2017).

FCA. Thematic review: The governance of unit-linked funds. (2013). https://www.fca.org.uk/publication/thematic-reviews/tr13-08.pdf (Accessed November 26th. 2017).

FCA. Considerations for firms thinking of using third-party technology (off-the-shelf) banking solutions. (2014). https://www.fca.org.uk/static/documents/barriers-to-entry-third-party-technology-considerations.pdf (Accessed November 26th).

FCA. FCA 2014 fines. (2014). https://www.fca.org.uk/news/news-stories/2014-fines (Accessed November 26th).

FCA. FCA risk outlook 2014. (2014). http://www.fca.org.uk/static/documents/corporate/risk-outlook-2014.pdf (Accessed November 26th).

FCA. Final notice - Stonebridge International Insurance Limited. (2014). http://www.fca.org.uk/your-fca/documents/final-notices/2014/stonebridge-international-insurance-limited (Accessed November 26th).

FCA. Innovator businesses: Project innovate. (2015). http://www.fca.org.uk/firms/firm-types/project-innovate (Accessed November 26th).

FCA. Proposed guidance for firms outsourcing to the "cloud" and other third-party IT services. (2015). https://www.fca.org.uk/publication/guidance-consultation/gc15-06.pdf (Accessed December 2nd 2017).

FCA. FCA fines Aviva Pension Trustees UK Limited and Aviva Wrap UK Limited £8.2m for client money and assets failings. (2016). https://www.fca.org.uk/news/press-releases/fca-fines-aviva-pension-trustees-uk-limited-and-aviva-wrap-uk-limited-8-2m

(Accessed December 2nd 2017).
FCA. FG16/5: Guidance for firms outsourcing to the "cloud" and other third party IT services. (2016). https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-"cloud"-and-other-third-party-it (Accessed December 2nd 2017).
Federation Global Fintech Hubs. A tale of 44 cities. Connecting Global FinTech: Interim hub review 2017. (2017). http://thegfhf.org/wp-content/uploads/2017/04/J11481-Global-Fintech-WEB.pdf?utm_source=gfhf_pdf&utm_medium=home&utm_campaign=Interim_Hub_Review_2017_pdf (Accessed December 2nd 2017).
Flick, U. (1998). *An introduction to qualitative research.* London: Sage.
Freehills, H. S.. Recent French supreme court decision on employer monitoring of employee's email. (2001). http://www.mondaq.com/x/14994/Ecommerce/Recent+French+Supreme+Court+Decision+on+Employer+Monitoring+of+Employees+Email (Accessed November 26th 2017).
FSA. SYSC 3.1 systems and controls. Financial services authority. (2010). http://fsahandbook.info/FSA/html/handbook/SYSC/3/1 (Accessed November 26th 2017).
Fulbright, N. R.. Outsourcing in the asset management industry. (2011). http://www.nortonrosefulbright.com/knowledge/publications/33753/outsourcing-in-the-asset-management-industry (Accessed November 26th 2017).
Gibbs, G. (2007). *Analysing qualititave data.* London: Sage.
Gillespie, N., Hurley, R., Dietz, G., & Bachmann, R. (2012). Restoring institutional trust after the global financial crisis. In R. Kramer, & L. Pittinsky (Eds.). *Restoring trust in organizations and leaders: Enduring challenges and emerging answers* (pp. 1–43). New York: Oxford University Press.
GOV.UK. Data protection. (2017). https://www.gov.uk/data-protection (Accessed November 26th 2017).
Gozman, D., & Currie, W. (2014a). The role of investment management systems in regulatory compliance: A post-financial crisis study of displacement mechanisms. *Journal of Information Technology, 29*(1), 44–58.
Gozman, D., & Currie, W. (2014b). The role of rules-based compliance systems in the new EU regulatory landscape: Perspectives of institutional change. *Journal of Enterprise Information Management, 27*(6), 817–829.
Gozman, D., Liebenau, J., & Mangan, J. (2018). The innovation mechanisms of Fintech start-ups: Insights from SWIFT's Innotribe competition. *Journal of Management Information Systems, 35*(1), 145–179.
Herz, T., Hamel, F., Uebernickel, F., & Brenner, W. (2012). Global IT multisourcing: objectives, challenges and requirements in multinational insurance companies. *PACIS 52 proceedings*.
Information Commissioner's Office. Guidance: what to expect and when. (2017). https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/guidance-what-to-expect-and-when/ (Accessed November 26th 2017).
Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011). Home is safer than the cloud!: Privacy concerns for consumer cloud storage. *Proceedings of the Seventh Symposium on Usable Privacy and Security*.
Jamil, D., & Zaki, H. (2011). Security issues in cloud computing and countermeasures. *International Journal of Engineering, Science and Technology, 3*(4), 2672–2676.
Jennings, D. (1996). Outsourcing opportunities for financial services. *Long Range Planning, 29*(3), 393–404.
Kauffman, R. J., Ma, D., Shang, R., Huang, J., & Yang, Y. (2014). On the financification of cloud computing: An agenda for pricing and service delivery mechanism design research. *International Journal of Cloud Computing, 2*(1).
Kvale, S., & Brinkmann, S. (2009). *Interviews learning the craft of qualitative research interviewing.* Thousand Oaks: Sage.
Lacity, M. C., Khan, S., Yan, A., & Willcocks, L. P. (2010). A review of the IT outsourcing empirical literature and future research directions. *Journal of Information Technology, 25*(4), 395–433.
Lacity, M. C., Khan, S. A., & Yan, A. (2016). Review of the empirical business services sourcing literature: An update and future directions. *Journal of Information Technology, 31*(3), 269–328.
Li, J. J. (2012). The alignment between organizational control mechanisms and outsourcing strategies: A commentary essay. *Journal of Business Research, 65*(9), 1384–1386.
Liard, B., & Lyannaz, C.. Discovery in the US involving French companies | White & Case LLP International Law Firm, global law practice. (2012). https://www.whitecase.com/publications/article/discovery-us-involving-french-companies (Accessed November 26th 2017).
Netskope. Netskope report reveals 75 percent of cloud apps not ready for EU general data protection regulation - Netskope. (2016). https://www.netskope.com/press-releases/netskope-report-reveals-75-percent-cloud-apps-not-ready-eu-general-data-protection-regulation/ (Accessed November 26th 2017).
Nolte, N., & Werkmeister, C.. Data protection in Germany: Overview. (2017). https://uk.practicallaw.thomsonreuters.com/3-502-4080?_lrTS=20171126163913279&transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 (Accessed November 26th 2017).
NTT Communications. Growing pains in the cloud II: The people vs. the ministry of no. (2016). http://www.eu.ntt.com/content/dam/nttcom/eu/img/LandingPages/ministryofno/NTT_Research_Report_Growing_Pains_in_the_Cloud_II.pdf (Accessed November 26th 2017).
Outsourcing Law. Industries. (2017). http://www.outsourcing-law.com/industries/ (Accessed November 26th 2017).
Patton, M. Q. (1980). *Qualitative evaluation models* (2nd ed.). Newbury Park: Sage.
Pearson, S., & Yee, G. (2012). *Privacy and security for cloud computing.* London: Springer Science & Business Media.
Penn, D.. OakNorth, the "first cloud-based bank in the UK," is powered by Mambu. (2016). http://findevr.com/oaknorth-first-cloud-based-bank-uk-powered-mambu/ (Accessed November 26th 2017).
Qin, L., Wu, H., Zhang, N., & Li, X. (2012). Risk identification and conduction model for financial institution IT outsourcing in China. *Information Technology and Management, 13*(4), 429–443.
Ratten, V. (2016). Continuance use intention of cloud computing: Innovativeness and creativity perspectives. *Journal of Business Research, 69*(5), 1737–1740.
Řezáč, F., & Řezáč, M. (2013). *Outsourcing in insurance. Proceedings of 10th International Scientific Conference European Financial Systems*.
Roberts, J. (2009). No one is perfect: The limits of transparency and an ethic for "intelligent" accountability. *Accounting, Organizations and Society, 34*(8), 957–970.
Schneider, S., & Sunyaev, A. (2016). Determinant factors of cloud-sourcing decisions: Reflecting on the IT outsourcing literature in the era of cloud computing. *Journal of Information Technology, 31*(1), 1–31.
Schwartz, M. J.. SEC fines former executives for client privacy breach. (2011). Retrieved from http://www.darkreading.com/risk-management/sec-fines-former-executives-for-client-privacy-breach-/d/d-id/1097104? (Accessed November 26th 2017).
Seddon, J. J. M., & Currie, W. L. (2013). Cloud computing and trans-border health data: Unpacking US and EU healthcare regulation and compliance. *Health Policy and Technology, 2*(4), 229–241.
Shaikh, F. B., & Haider, S. (2011). Security threats in cloud computing. *International conference for Internet technology and secured transactions*.
Stanko, M. A., & Olleros, X. (2013). Industry growth and the knowledge spillover regime: Does outsourcing harm innovativeness but help profit? *Journal of Business Research, 66*(10), 2007–2016.
Stratecast (2013). The hidden truth behind shadow IT. http://www.mcafee.com/uk/resources/reports/rp-six-trends-security.pdf.
Tsatsou, P., Elaluf-Calderwood, S., & Liebenau, J. (2009). Towards a taxonomy for regulatory issues in a digital business ecosystem in the EU. *Journal of Information Technology, 25*(3), 288–307.
Venkatraman, A.. Monzo: Building a mobile-first U.K. digital bank using cloud and microservices architectures. (2016). Retrieved April 12, 2017, from https://d0.awsstatic.com/analyst-reports/EMEA41642116Web.pdf (Accessed November 26th 2017).
Venters, W., & Whitley, E. A. (2012). A critical review of cloud computing: Researching desires and realities. *Journal of Information Technology, 27*(3), 179–197.
Willcocks, L., Venters, W., & Whitley, E.. Cloud and the future of business: From costs to innovation. (2011). http://eprints.lse.ac.uk/45211/ (Accessed November 26th 2017).
World Economic Forum. The future of FinTech: A paradigm shift in small business finance. (2015). http://www.weforum.org/reports/future-fintech-paradigm-shift-small-business-finance (Accessed December 2nd 2017).

Daniel Gozman is a Senior Lecturer at the University of Sydney (Australia) and an Honorary Fellow at Henley Business School at the University of Reading (UK). He is member of the LSE's Outsourcing Unit and a Research Fellow at UCL's Centre for Blockchain Technologies. Since 2009, he has focused on understanding how Governance, Risk and Compliance (GRC) activities are underpinned by technology with a specific focus on the intersection between regulatory change, information systems and operational resilience. He has published within respected peer reviewed journals including Journal of Management Information Systems, Journal of Information Technology and Journal of Small Business Economics. and been invited to present his work at international conferences. He has contributed to articles in the Sunday Times, and Computer Weekly. Prior to academia, Daniel worked for a global management consultancy and a big four accounting firm.

Leslie Willcocks is Professor in Technology Work and Globalization at the Department of Management at London School of Economics and Political Science. He heads the LSE's Outsourcing Unit research centre and is Editor-in-Chief of the Journal of Information Technology. Previously he taught at Oxford University for nine years. His doctorate is from University of Cambridge. Leslie has a global reputation for his work in robotic process automation, AI, cognitive automation and the future of work, outsourcing, global strategy, organizational change, and managing digital business. He is co-author of 54 books, and has published over 230 refereed papers in journals such as Harvard Business Review, Sloan Management Review, California Management Review, MIS Quarterly, Journal of Management Studies.