Bloomberg BNA

BNA's Banking Report™

CLOUD COMPUTING

Are Financial Institutions Ready for Cloud Computing?

By Charles M. Horn and Chris Ford

Charles Horn is a regulatory and transactional attorney whose practice focuses primarily on banking and financial services matters. Mr. Horn represents domestic and global financial services firms of all sizes on regulatory and transactional issues affecting their organization, structure, governance, management and operations. In addition, he provides regulatory counseling to banks and other financial services firms relative to federal and state financial regulation, supervision, and compliance matters affecting their corporate, institutional, wealth/asset management, and retail business activities.

Chris Ford is the Chair of Morrison & Foerster's firm wide Global Sourcing Group. His practice focuses on advising customers on the full life cycle of their complex information technology and business process outsourcing transactions. Mr. Ford also advises large clients on joint ventures, telecommunications, technology procurement and sophisticated licensing transactions, as well as Enterprise Resource Planning and other systems integration projects.

The rapid growth in the availability and sophistication of cloud computing services — on-demand, scalable information technology services provided over the internet — presents significant opportunities for cloud computing hosts and users alike. For potential users, cloud computing can offer a number of important benefits, including very significant cost savings and operational efficiencies, flexibility in deployment, ready access to systems, applications and data, better backup services, and faster and more responsive upgrade functionalities. Potential hosts such as major IT service providers correctly see significant business opportunities in cloud computing, whereas potential users of cloud services recognize the cost efficiencies and technological and business flexibility offered by potential cloud solutions. As a result, the interest in, and demand for, cloud computing services has increased dramatically over the past several years. IT industry surveys point to the likelihood of a continuing significant migration away from ''hard'' IT platforms towards internet based services as a solution for hardware, infrastructure and software needs alike.[1]

Financial services firms (e.g., banks, securities firms, asset managers and insurance companies) are among the business organizations that see significant potential benefits in cloud-based systems. Many banking and other financial services firms are closely examining cloud-based IT solutions, and several major technology services providers (TSPs) are creating cloud computing systems that are aimed at financial services firms.[2] For regulated firms such as banks, investment banks and money managers who may be tempted to move all or part of their IT infrastructure into the cloud, however, there are significant legal and regulatory challenges that they must consider and resolve before they do so.

[1] *See,* Pew Research Center, *The Future of Cloud Computing* (June 2010), *available athttp://pewinternet.org/Reports/2010/The-future-of-cloud-computing.aspx*.

[2] *See, e.g., http://www.ibm.com/cloud-computing/us/en/assets/Cloud_Computing_on_a_Smarter_Planet.pdf* (IBM ''Smarter Planet/Smarter Banking'' sublink'').

 ISSN 0891-0634

In turn, the issue that financial firms face today is whether the state of cloud computing has developed to a point where these challenges can be cost-efficiently and successfully addressed.

Cloud computing is an IT delivery model that covers a number of business/IT processes and activities, and the issues that financial firms may encounter will be affected by the nature and scope of cloud computing activities that are being contemplated. Through cloud computing services, users, including financial institutions, can effectively outsource all or part of their IT hardware architecture (infrastructure as a service, or IaaS), operating systems and platforms (platform as a service, or PaaS), or software applications (software as a service, or SaaS) as they individually choose. Further, financial institutions may choose from various methods in which these services may be delivered: Public clouds, where the IT services are delivered in a pure utility style to multiple customers using completely non-customized materials, methods and processes; private clouds, where such services are highly customized for one or a small number of customers using selected materials, methods and processes; and hybrid clouds, which is a combination of the two.

Because the choices are so individualized, the challenges and solutions that financial institutions face will vary significantly across the range of financial institutions. Thus, a small U.S. community bank that is thinking about outsourcing its IT infrastructure, systems and applications to a third-party web services host that offers multi-tenant cloud computing services will encounter challenges that can in many significant ways be quite different than those faced by a global financial services firm that is thinking about loading core customer or financial management systems into a private cloud.

Financial Services Legal, Regulatory Landscape

Regulated financial firms that have spent any substantial time thinking about cloud computing implementation issues have quickly recognized several key concerns that must be addressed before cloud computing becomes a viable solution, including data privacy, data and systems security, business continuity and contingency planning, and liability/risk management concerns. Adding concerns over regulatory oversight of cloud computing activities to the list of issues makes ''going into the cloud'' a complex undertaking.

Authoritative financial regulatory guidance on cloud computing activities for regulated financial firms is still somewhat sparse but is developing. In general, there is substantial regulatory guidance on financial firm third-party technology outsourcing activities, [3] and the financial regulatory agencies have indicated that they will apply to cloud computing activities the same regulatory requirements and standards that apply to IT outsourcing activities in general. To this end, earlier this summer the Federal Financial Institutions Examination Council (FFIEC) issued a joint interagency statement (Cloud Statement) on the use by financial institutions of outsourced cloud computing services, and the key risks associated with such services.[4] The Cloud Statement, the substance of which is also being incorporated into the FFIEC's IT Handbook,[5] is the first formal federal financial agency statement on the matter of cloud computing.

The Federal banking agencies — the Office of the Comptroller of the Currency (OCC); the Federal Reserve Board; and the Federal Deposit Insurance Corporation (FDIC) — have been explicit about their expectations when a regulated banking organization chooses to outsource technology services to a third-party TSP. Federal securities regulators and self-regulators for the most part also have issued guidance for regulated securities firms that is substantively similar, albeit less detailed, than the guidance provided by the banking regulars, although securities regulators have limited the authority of securities firms to outsource functions and services that would require registration or qualification of the TSP under the Federal securities laws.[6] Because the banking agencies' guidance on TSP outsourcing activities is most specific, however, a summary of banking agency expectations is instructive.

In general, the banking agencies' major expectations on IT outsourcing activities include the following core elements:

■ ***Effective oversight and risk management of IT outsourcing arrangements.*** The board of directors and executive management of a financial institution are expected to establish and approve, and assure compliance with, risk-based policies that govern the IT outsourcing process. These policies must recognize the risks to the financial institution of its outsourcing relationships and be appropriate for the size and complexity of the financial institution. This expectation is fully consistent with general financial regulatory agency expectations that

[3] *See*, Federal Financial Institutions Examination Council (FFIEC), IT Examination Handbook (IT Handbook), *Outsourcing Technology Services* (June 2004); *Supervision of Technology Service Providers* (March 2003)*; Audit* (Aug. 2003)*;* and *Information Security* (July 2006). All of these publications are available at http://ithandbook.ffiec.gov/it-booklets.aspx.

[4] FFIEC, Information Technology Subcommittee, Statement on Outsourced Cloud Computing (July 10, 2012). *See also* Morrison & Foerster's client alert discussing the Cloud Statement and its implications, *available athttp://www.mofo.com/files/Uploads/Images/120711-Federal-Financial-Agencies-Issue-Cautionary-Statement.pdf*.

[5] *See,* IT Handbook, *Outsourcing Technology Services*, Appendix A, ''Examination Procedures'' and Appendix D, ''Managed Security Service Providers.''

[6] Specifically, federal securities regulators and self-regulatory have provided guidance and the duties and responsibilities of regulated securities firms that seek to outsource key business processing and data maintenance functions. *See, e.g.,* National Association of Securities Dealers (NASD), Notice to Members 05-48 (July 2005), ''Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers''; Financial Industry Regulatory Authority (FINRA, the self-regulatory organization successor to the NASD) Rule 1230(b)(6), a relatively new rule which will require the registration *and supervision* of FINRA member firm ''operations professionals'' who supervise a member firm's covered functions, including functions involving customer funds, accounts, data processing and transactions, regardless of where these functions are performed, *available at http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=10203*. In addition, FINRA is considering the imposition of direct regulatory obligations for member clearing firms that outsource key IT, customer account, compliance and risk management, or financial reporting functions to TSPs. FINRA Proposed Rule 3190, published in FINRA Regulatory Notice 11-14 (March 2011), *available at* http://www.finra.org/Industry/Regulation/Notices/2011/P123399.

  BBR ISSN 0891-0634

the board of directors and senior management of a financial institution have ultimate legal responsibility for the condition and operations of the financial institution.

■ ***Risk assessment and requirements.*** The financial institution, under the oversight of management, is expected to assess the risks from outsourcing, reduce this assessment to suitable written policies, and use these written policies to govern the outsourcing process. Risk identification includes identifying the nature and quantity of relevant risks, taking into account the functions and activities to be outsourced, and from there developing definitions of business requirements that will govern the selection of a TSP, the outsourcing standards and requirements of the financial institution, and the controls that will be needed to manage the risks in question.

■ ***Service provider selection.*** A financial institution must evaluate TSP proposals in light of the institution's needs, and conduct a suitable due diligence on prospective TSPs.[7]

■ ***Contract issues.*** A financial institution's outsourcing arrangements must be memorialized in a written agreement that, among other things, (i) defines the parties' rights and responsibilities, (ii) contains adequate and measurable service level agreements (SLAs), (iii) is properly priced, taking into account the financial institution's needs, (iv) does not contain inappropriate or unsafe inducements for the financial institution, and (v) is reviewed by competent legal counsel.

■ ***Ongoing monitoring.*** Financial institution management is expected to monitor the performance of the service provider during the life of the contract, taking into account changes in the financial institution's needs that may occur during the contract period. Proper monitoring will include (i) key SLAs, (ii) the vendor's financial condition and capacity to perform its obligations, (iii) verification through appropriate audit reports and other internal control reviews, of the vendor's control environment, and (iv) the financial institution's and vendor's ability to address and respond to changes in the external environment affecting the outsourcing arrangements.[8]

The basic principles underlying these standards and requirements are relatively straightforward, and stem from the fundamental proposition that the management of a regulated financial institution is *risk-based*, as is the regulatory agencies' regulation and supervision of financial institutions under their regulatory jurisdictions. Accordingly, the risk management principles and expectations of the financial regulators that apply to the activities and supervision of regulated financial institutions in general will apply equally to technology based-activities and services, and their regulatory oversight, whether they are cloud-based or not.

. . . the regulatory literature that applies to technology outsourcing activities tends to focus most specifically on operational and compliance risk

From the regulatory perspective, the risks associated with technology outsourcing arrangements fall into the following principal categories:

■ ***Operational (or transaction) risk,*** or the risk to earnings or capital arising from problems with service or product delivery.

■ ***Legal/compliance risk,*** or the risk to earnings or capital arising from violations of laws, rules, or regulations, or from nonconformance with internal policies and procedures or ethical standards.

■ ***Strategic risk***, or the risk to earnings or capital arising from adverse business decisions or improper implementation of those decisions.

■ ***Reputation risk,*** or the risk to earnings or capital arising from negative public opinion of a financial institution.

■ ***Credit risk, or*** the risk to earnings or capital arising from an obligor's failure to meet the terms of any contract with the bank or otherwise to perform as agreed.[9]

Of the categories of risk summarized above, the regulatory literature that applies to technology outsourcing activities tends to focus most specifically on operational and compliance risk. In the case of operational risk, regulators tend to focus on operational risks arising from (i) the nature and scope (criticality of service, sensitivity of data, volume of transactions outsourced) of the financial institution functions and services that are outsourced, (ii) the service provider (technological platforms used, financial condition and stability, experience with services being outsourced, reporting and MIS capabilities, business continuity capabilities, etc.) and

[7] Additional considerations apply in the case of affiliated or foreign TSPs.

[8] The banking agencies each have articulated these principles in slightly different ways. For example, the OCC describes the general management of the third party relationships, including technology relationships, as follows:

The OCC expects the boards of directors and management of national banks to properly oversee and manage third-party relationships. National banks should adopt a risk management process that includes:

■ A risk assessment to identify the bank's needs and requirements;

■ Proper due diligence to identify and select a third-party provider;

■ Written contracts that outline duties, obligations, and responsibilities of the parties involved; and

■ Ongoing oversight of the third parties and third-party activities.

OCC, *Banking Bulletin 2001-47* (Nov. 2001), *available at http://www.occ.treas.gov/news-issuances/bulletins/2001/bulletin-2001-47.html*.

[9] In some cases, third-party technology relationships may also subject the financial institution to liquidity, interest rate, price, and foreign currency translation risk, or country risk in the case of a foreign-based technology service provider. (Country risk is the risk that economic, social, and political conditions and events in a foreign country will adversely affect the financial institution's financial interests.)

(iii) the type of technology used in performing the services (reliability, scalability, security). By the same token, compliance risk tends to center around data security, privacy and integrity issues, as well as the TSP's ability and/or willingness to comply, and assist the financial institution in complying, with legal and regulatory standards applicable to the financial institution. In this regard, compliance with financial privacy and data protection requirements under the Federal banking laws[10] ranks very high on the list of financial regulators' compliance risk concerns. In addition, Federal regulators place substantial emphasis on their legal right under the Bank Service Company Act to examine or inspect a TSP's activities performed on behalf of the financial institution,[11] and the TSP's willingness to accommodate this regulatory oversight.[12] Federal financial regulators will conduct formal reviews of TSPs, with enhanced review procedures used for Multi-Regional Data Processing Servicers (MDPS) that have technology services relationships with multiple financial institutions of a size and scope as to present possible systemic risks to the financial institutions community.[13]

In turn, the processes through which financial institutions are expected to manage these risks is through (i) the creation and enforcement of technology services risk management policies and procedures, (ii) effective due diligence of TSPs, (iii) execution of strong technology services agreements with suitable protections for the financial institution, and (iv) effective monitoring of TSP performance in light of the financial institution's requirements and needs over the term of the contractual relationship.

Challenges, Solutions in Accessing the Cloud: Coming to Grips with Legal, Commercial Issues

Cloud computing is nothing more — and nothing less — than the furnishing or procurement of IT services through a new delivery channel. Therefore, the risk management, compliance and liability reduction principles that apply to financial institutions' technology services activities across the board logically apply with equal force to financial institutions' cloud computing activities, regardless of the types of services or applications that financial institutions may want to access through the cloud, or the public, private or hybrid nature of the cloud platform that financial firms would seek to access.

In turn, the legal, regulatory and transactional issues for financial institutions looking at a cloud delivery model will largely be the same as is the case for financial institutions obtaining IT services utilizing more traditional models, but the technology and the commercial environment for the delivery of cloud-based services make the solutions to those issues in many cases quite different. What may also be different about cloud-based services are the utilitarian nature of the services being provided, and the level of operational and MIS control that a financial institution may have to cede to a TSP that provides cloud-based services to it. It might be entirely possible for a financial institution to close down its servers, operating systems and applications, and purchase its entire IT architecture over the internet, but doing so plainly presents risk management issues of a different level of importance.

Can the technology issues currently associated with the cloud environment be resolved in a way that financial institutions across the board can comfortably avail themselves of cloud delivery solutions? There are significant legal and regulatory issues that will challenge a financial institution's efforts to avail itself of cloud service models, in particular public and hybrid models.

In prior publications on cloud computing activities, we have highlighted several major issues that are particularly associated with cloud computing activities, including privacy, data protection/integrity, and TSP negotiation issues, and how users of cloud services may need to approach these concerns.[14] These issues are just as real, if not more so, for financial institution users of cloud services, given the developing state of cloud technology, and the strong regulatory requirements and expectations associated with risk management of financial institutions' technology and business process outsourcing activities in general. In turn, the legal and regulatory environment in which financial institutions operate require a thoughtful and disciplined approach to the outsourcing of financial business processes ''into the cloud.''

So what should that approach look like? It means, first of all, following the risk identification and management, due diligence, vendor selection and documentation processes summarized above, and covered in existing regulatory guidance. In this regard, the banking agencies' Cloud Statement has highlighted several areas that the agencies believe are of particular interest for banking organizations that are users of third-party cloud computing services, including: (i) due diligence of cloud IT vendors; (ii) management of cloud IT vendors; (iii) auditing the vendor and its delivery of services; (iv) information security; (v) legal, regulatory and reputational risks; and (vi) business continuity planning. Those financial institutions that are familiar with the Agencies' existing IT guidance on outsourcing in general will find nothing new in these broad areas, but the Statement does highlight a number of specific issues that arise in the cloud IT environment.

Taking into account these various considerations, we offer some observations on the preferred path forward for financial institutions that are considering the acquisition of cloud-based IT services.

1. Develop a strong understanding of the business and legal risks specifically associated with cloud IT services. By IT industry standards, cloud-based services are still relatively new, although they are evolving and expanding very rapidly. In some respects, the nature of the key business risks associated with cloud computing – privacy of financial institution and financial institution customer information, security of cloud based data, business interruption/continuity issues – are really no different than they are traditional application or server-based IT systems, where these issues have long been just as real. But coming to grips and resolving these is-

[10] 15 U.S.C. § 6801.

[11] 12 U.S.C. §§ 1867(a), (c).

[12] FFIEC, IT Handbook, *Supervision of Technology Service Providers, supra.*

[13] *Id.*

[14] *See*, Morrison & Foerster LLP, *Privacy in the Cloud: A Legal Framework for Moving Personal Data to the Cloud* (Feb. 14, 2011); *Cloud Computing and Outsourcing: Is Data Lost in the Fog?* (June 15, 2009); MoFoTech Magazine (Supplement), *Get Your Head in the Cloud* (2010).

  BBR ISSN 0891-0634

sues requires a solid understanding of the specific technological features, advantages and drawbacks of cloud-based technology platforms, and the risks specifically associated with these services.

What has probably slowed the expansion of cloud-based services in the financial institutions community more than anything else are financial institution concerns about compliance with the regulatory requirements that apply to privacy of financial customer information, and the integrity and protection of that information. These requirements are relatively rigorous, and financial institutions cannot simply negotiate them away, as the Cloud Statement makes clear. At this time, TSP vendors in general may not have made the necessary strides in cloud technology development, or have not acquired a suitable appreciation of the demands that financial institutions face in this regard, to respond effectively to these core privacy and data protection concerns, although recent press reports suggest that some vendors are focusing specifically on these issues and attempting to offer solutions to them.[15]

■ ***Financial privacy issues.*** Regulated financial institutions across the board are subject to Federal and state financial privacy requirements that generally require the protection of customers' personal financial information, and limit the ability of financial institutions to share that information with third parties. While the Federal Gramm-Leach-Bliley Act and state laws generally will permit a financial institution to share customer information with a TSP provider in connection with the TSP providing services to the financial institution, in a cloud-based environment customer data may not be stored or retained at any specific location, or may be moved from one location to another by the TSP. In turn, the particular regulatory requirements applicable to a financial institution's customer data may be affected by where that data is stored. Moreover, the regulatory complications that may arise from where data is stored may become more complicated if that data can be stored outside of the United States, especially in a region such as the European Union, which has strict privacy and data protection regulatory regimens.

What has probably slowed the expansion of cloud-based services in the financial institutions community more than anything else are financial institution concerns about compliance with the regulatory requirements that apply to privacy of financial customer information, and the integrity and protection of that information.

Financial institutions contemplating the acquisition of cloud-based services that include customer information therefore must address the impact of the cloud delivery model on their financial privacy obligations. One possible way to do is to negotiate geographic limitations on where the TSP may store customer data, or obtain appropriate assurances that the TSP will comply with legal restrictions applicable to the financial institution with respect to its customer data. Obtaining these vendor commitments and assurances, however, may be easier said than done, because many cloud service providers thus far have been reluctant to agree to terms and conditions that sufficiently address these concerns.

■ ***Customer data protection issues.*** Federal law (again, the Gramm-Leach Bliley Act) requires financial institutions to adopt and implement measures that are reasonably designed to protect the integrity of, and safeguard, their customer data. In turn, current supervisory policies require regulated banking organizations and other financial institutions to take affirmative action to remedy breaches of data security, including notifications of customers affected by data breaches. The laws of almost every state have similar requirements, with the difference being that state laws often specifically require customer notification in the case of data breaches.

Cloud-based IT services are equally subject to these requirements, with the practical difference being that, in the case of cloud-based IT services, a financial institution's customer data may be housed in one or more remote locations, and may be able to move more freely across state lines or other jurisdictional boundaries. But if there is a breach of customer data security in the TSP's cloud, it doesn't matter whether the breach occurred in Portland, ME or Portland, OR, because the financial institution probably will have notification and other remedial obligations to its customers.

In part due to concerns such as these, a number of financial institutions may elect to limit their acquisition to cloud-based services to those services that do not relate to customers' personal financial data, or may see if they can obtain an agreement from a TSP to identify specific locations where cloud-based data will be maintained. But getting that agreement, as noted above, may be difficult to achieve. At the same time, regulatory expectations in this area are quite explicit, in that financial institutions are expected to adapt their information security policies, standards, and practices to incorporate the activities related to a cloud TSP. In this regard, specific information security measures such as continuous monitoring of high-risk situations, maintenance of comprehensive data inventories, the implementation of a suitable data classification process, and limiting access to customer data through effective identity and access management (particularly in public cloud environments), are key information security measures from the regulatory perspective.[16]

■ ***Business continuity issues.*** One of the key risks associated with any IT services is the risk of service interruption. This issue is no less important for cloud-based IT services, and unlike issues associated with privacy and data breach, business continuity risks are not limited to services involving customers' personal financial information. And, the risk of service interruptions may give financial institutions further pause about procuring cloud-based IT services, especially services that are core or ''mission critical'' to the financial institution.

[15] *See,* ''Cloud Compliance Tech Floods the Market,'' *American Banker* (Sept. 13, 2012).

[16] *See,* Cloud Statement.

Are cloud-based operating environments more susceptible to interruptions of services? The answer to this question currently may be inconclusive, but what may differ is the degree to which a service interruption may impact multiple organizations and affect the service restoration priority given to the financial institution — especially in the case of large providers of public cloud financial IT services — and the need to ensure the presence of cloud-specific response strategies and backup environments. These are important questions that financial institutions need to address early in the procurement process and for which a financial institution will absolutely need to have satisfactory answers. For example, a financial institution may need to arrange for independent backup data storage capabilities to protect against a wholesale loss of data in the event its cloud services ''go dark.''

2. Know what you are buying. Understanding the features of cloud-based services also means understanding, and consciously deciding upon, the types of cloud services the financial institution is buying. A public (multi-tenant) cloud platform has definite advantages in terms of cost and conservation of financial institution resources, as well as ready access to scalable services. A public cloud, however, may deprive the financial institution of flexibility and corporate leverage in its efforts to negotiate the types of services and data, business continuity and liability protections that it needs. By the same token, flexibility and leverage, and the ability to protect data and business processes, may be more available in a hybrid or private cloud environment, but almost certainly will entail higher costs for the financial institution.

One basic regulatory requirement for financial institutions that purchase any IT services from a TSP is the right of the financial institution's primary regulator to examine and supervise the provision of those services.

Similarly, a financial institution's business needs will influence the types of cloud services a financial institution acquires: infrastructure, systems or applications. There naturally are significant differences in these services, and it is important that the financial institution take steps to assure that its business needs align properly with the types of services a TSP is able and willing to offer.

3. Your regulators will want to fly inside the cloud. One basic regulatory requirement for financial institutions that purchase any IT services from a TSP is the right of the financial institution's primary regulator to examine and supervise the provision of those services. This supervision right includes the regulator's right, under the Bank Service Company Act and other regulatory requirements, to inspect and audit the TSP's activities and systems, and the level of risk that a TSP may pose to those financial institutions with which it does business.

In the realm of cloud computing services, this access right will be just as, if not more, important for financial institution regulatory agencies, especially if the delivery of cloud-based IT services becomes concentrated among a small number of large TSPs that each do business with hundreds of financial institution clients, and where the IT infrastructure and risk management systems of a single TSP may become a priority risk management issue for the financial regulatory agencies. Accordingly, a financial institution that wants to purchase cloud-based IT services will need to assure that its TSP understands and is willing to comply with these regulatory requirements. Similarly, a financial institution's right to audit cloud services, or request adequate assurances of the integrity of a TSP's internal controls environment, is another important consideration that a cloud services purchaser must address at the inception of an IT cloud services relationship. Audit rights, in particular, may be a challenge for a technology model such as the cloud platform, where financial data may be dispersed among various locations, and moved from location to location.

On top of these access requirements may be regulatory requirements — e.g., such as those imposed by FINRA on its member firms — that require financial institutions to formally oversee or supervise certain activities being performed on their behalf.[17] Being able to do so in a cloud-based IT environment may be more challenging, and is an issue that financial institutions need to explore with their TSPs at the outset of an IT services relationship.

4. Kick the tires before entering the cloud. What the foregoing considerations mean, in large part, is that financial institutions need to identify and resolve at an early stage the various legal, regulatory and risk mitigation issues embedded in a cloud-base IT relationship. This is a process that must be completed at the outset of a TSP relationship, not while the financial institution is well into the relationship. In turn, this requires a thoughtful, well-organized due diligence process that will assure not only that the right questions get asked, but also that any prospective TSP is able to answer these questions to the financial institution's satisfaction. In other words, the financial institution will want to know if the TSP will be able to provide the level of service and support that the financial institution requires to satisfy its risk mitigation and regulatory responsibilities to the financial institution's and its regulator's satisfaction. In this regard, the Cloud Statement highlights several particular areas that the bank regulators want a financial institution to address during the due diligence process, including (i) data classification, (ii) data segregation and (iii) data recovery.

5. Your TSP agreement is the foundation for a good cloud solution, but can you get the terms that you need? A financial institution that enters into a cloud IT services relationship not only must understand the relevant technology and associated legal and regulatory issues, but also the commercial and regulatory objectives and risks of a particular TSP relationship. In turn, the financial institution must select its TSP and negotiate its agreement with its objectives and risks firmly in mind.

A financial institution is best-positioned to protect its commercial and regulatory interests through the negotiation of a sound and enforceable technology services agreement that affords it adequate risk and liability protections, assurances of suitable service levels standards

[17] *See,* n.6 *supra*.

  BBR ISSN 0891-0634

and performance, and sufficient and timely remedies if things go wrong with the TSP relationship. Current experience, however, suggest that many public and hybrid cloud system TSPs have not reached the point of fully accommodating the particular business and regulatory obligations of highly-regulated financial institutions. In most TSP relationships, vendor terms and conditions are apt to be tilted in favor of the vendor on core matters (including service levels, business continuity responsibilities, rights of termination without cause, remedies for damages, and limitations on indemnifications). Vendors also will offer up standardized forms of agreements where their willingness to negotiate institution-specific terms and conditions may be relatively low. In turn, many financial institutions may lack the size or economic clout to negotiate terms that fully satisfy their commercial and legal/regulatory risk tolerances.

This vendor landscape, however, may change as regulatory expectations make plain that cloud technology vendors must be prepared to adapt to the regulatory environment in which financial institutions operate. For example, the Cloud Statement says that banking organization contracts with cloud IT service providers should address the parties' obligations with respect to compliance with privacy laws, for responding to and reporting about security incidents, and for fulfilling regulatory requirements to notify customers and regulators of any breaches.

To sum up, at least in the short term the financial institution market for broad-scale cloud IT services may be limited primarily to those financial institutions that are prepared to purchase a highly-customized but significantly more expensive private or semi-private cloud platform. But cloud technology offers the promise of very significant economies, and ready access to a wide array of on-demand IT services, that are strongly attractive to the financial institution community, and there are some indications that the TSP community may be waking up to the need to adapt their products and services to the demands of their regulated financial institution clients. Therefore, vendors that are able to focus on the needs and requirements of this highly promising client community will find themselves the winners in bidding for and obtaining this community's business.