March 2015

Nine Expectations for your next TSP Contract

Earnings Performance Consulting

M&A Integration | Risk & Compliance

For the Intelligent Banker

2015 Intelligent Bank Management Series

The 2015 Intelligent Bank Management Series focuses on insights, strategies and development priorities for improved profitability, operating efficiency, compliance and risk management at U.S. financial institutions.

© CMPG, LLC. All rights reserved.

Nine Expectations for Your Next TSP Contract

As the FFIEC wades into the deep waters of dictating contract terms and due diligence requirements for Transaction Service Providers (TSP), keep in mind that these prescribed expectations are for TSPs and not the vast majority of your vendor base.

Transaction Service Providers (TSP) are those vendors that support customer accounts and transaction processing against those accounts, such as core providers, card solutions processors, wire transfer providers, mortgage subservicers, etc. Below is the checklist of regulatory expectations for your TSP relationship contracts, along with our thoughts as to where this will be easily obtained, or become testy at the negotiation table.

Right to audit.

Agreements for years have provided for the right of the financial institution or its representatives to audit vendors. Some agreements require a fee to access reports like the SSAE16. The issue with audit reports is ensuring that you get the complete portfolio that covers the services you obtain. Have you received the report that covers the datacenter where your service offerings are being processed?

It has been our experience that audit reports addressing the TSPs' resiliency capabilities and interdependencies (e.g., subcontractors), BCP testing, and remediation efforts are not historically available documents. Vendors have been prepped to provide Executive Summary documents on BCP, but those in no way get down to the depth of information and expectation for the institution to assess the impact on the financial institution's own BCP plan. At a minimum, there needs to be an indexing of Recovery Time Objectives (RTO) between the TSP provider solutions and the financial

Learn more about how CMPG can assist you at

www.cmpg.com

or call us at

1-800-997-2674

to discuss the needs of your financial institution.

institution's business units and services being supported. As an example, your institution may place a near immediate RTO for collections activity, as this is directly tied to income and asset rights, yet as is often found, a collection system is a loan sub-system that has a much longer RTO from the vendor TSP provider.

Establishing and monitoring performance standards.

The requirement that contracts should define measurable service level agreements (SLAs) for the account or transaction services being provided is appropriate and not new, but it is one of the toughest aspects of vendor contract negotiation. Typically SLAs have a connection to financial penalties or an option to prematurely exit an agreement upon repeated failures. Rarely have we seen business continuity expectations, such as RTOs and Recovery Point Objectives (RPOs) written in contracts that would meet these new expectations.

Default and termination.

As stated above, while contracts should define events that constitute contractual default or more commonly breach, until now, the inability to meet BCP provisions or RTOs have rarely been explicitly defined as default or breach terms. This guidance and expectation will certainly be generating stomach acid with the TSP vendor's sales staff and legal team.

Vendor Subcontracting.

Contracts need to be specific as to whether subcontracting is allowable, and if so, should define the services that may be subcontracted. If subcontracting is allowable, is it restricted to only within the United States or does it support international subcontracting. If allowed, the TSP's contractual provisions should also apply to the subcontractor and should clearly state that the primary TSP has overall accountability for all services that the TSP and its subcontractors provide.

Contract provisions need to be expanded to include the business continuity capabilities of any subcontractors. It has been our experience that this has not historically been divulged or included in prior contracts.

The expectations for contracts are that the TSP's own due diligence process for engaging and monitoring subcontractors be detailed, and the notification requirements regarding changes to the TSP's subcontractors be written into the contract. Continuing, the contractual provisions should also address the right to audit and BCP testing requirements for subcontractors. Additionally, agreements should include the TSP's process for assessing the subcontractor's financial condition. Again, this depth of subcontractor evaluation has not historically been divulged or included in prior contracts.

Heightened Data Concerns for Foreign-based service providers.

The expectation is for financial institution to review data security controls of foreign-based TSPs or foreign-based subcontractors that back up and/or store data offshore. Because information security and data privacy standards may be different in foreign jurisdictions, the contract should clearly address the need for data security and confidentiality to, at a minimum, adhere to U.S. regulatory standards.

BCP testing.

While the expectation that has been made is that contracts address the financial institution's BCP testing requirements, the reality is that industry TSPs struggle with inclusive BCP testing with their clients. The development of TSP RTOs have not been historically up for debate with their customer community, as the arrangements for recovery and systemic interdependency often dictate recovery order. For example, it makes no sense to priority recover an Internet Banking solution without first recovering the underlying account processing application that provides Internet Banking its data feed and ability to transact.

While most contracts do define BCP testing frequency and the availability of test results, there has been reluctance for vendors to contractually commit to specified scheduled participation in the TSP's periodic BCP testing within contracts. For many, there are just too many clients to serve and participation in a BCP event is both time-consuming and frequently limited in scope, far below an expected actual BCP event dress rehearsal.

Data governance.

This expectation may be the easiest to accomplish. Contracts are expected to clearly define data ownership and handling expectations during the relationship and following the conclusion of the contract. This may include data classification, integrity, availability, transport methods, and backup requirements. In addition, expectations for data volume and growth should be addressed.

TSP updates.

While we have not seen this as a contractual provision as is being put forth, financial institution management has not shied away from engaging vendors on these topics. 'Empowerment' to request the TSP's response to relevant regulations, supervisory guidance, or other notices published by any of the federal banking agencies is expected to evolve into a standard set of verbiage with little to no value. This right has always existed, and it is our belief that certain vendors will not be compelled as result of a contractual clause to improve. Walk a mile with references and make sure you are very good at Due Diligence.

Security issues.

This could be the hardest expectation to accomplish. While contracts should clearly state the responsibility of the TSP to address security issues associated with services and, where appropriate, to communicate the issue(s) and solution(s) to its financial institution clients, the aspect of responsibility and financial accountability will interfere with getting this provision accepted.

The addition of an incident response plan and notification responsibilities for breaches in security that *may* materially affect financial institution clients only complicates financial accountability. The issue will come down to agreeing to the sharing of knowledge versus taking accountability for an incident or breach contractually.

To discuss the needs of your financial institution or learn more about CMPG services:

www.cmpg.com

1-800-997-2674

© CMPG, LLC. All rights reserved.