Systems Engineering at MITRE
CLOUD COMPUTING SERIES

Cloud SLA Considerations for the Government Consumer

Kevin Buck
Diane Hanf

MITRE

September 2010

Executive Summary

During the past year, much work has been done to provide a set of terms and definitions that will enable the common discussion of cloud computing. The National Institute of Standards and Technology (NIST) has defined emerging cloud service models to include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). They have further defined cloud deployment models as private cloud, shared community cloud, public cloud, and hybrid cloud.

Cloud computing presents the Federal Government with new opportunities, challenges, and risks. Some cloud computing benefits that have been identified include reducing capital costs for infrastructure (thereby converting capital expenditures to operating expense); adding resources more flexibly without continually undertaking time-intensive procurement activities; and reducing recurring licensing and on-going maintenance costs. In today's computing environment—where agility may be needed to accommodate unpredictable usage profiles—cloud computing promises to reduce some information technology (IT) complexities and provide adaptable provisioning mechanisms, such as pay-as-you-go self-service. Although the cloud may lessen the consumer's administrative burden, it also removes physical control of resources used. There are potential risks that also must be considered, including the application of proprietary technologies that can lead to service provider lock-in (i.e., significant switching challenges among providers) and limited choice.

This paper explores the role of service-level agreements (SLAs) in managing performance of Government procurements through public clouds (although some of the findings from this exploration also are relevant for community and private clouds). SLA best practices and lessons learned are explored, and context is provided regarding how SLAs currently are being applied within public cloud procurements. Commercial cloud SLAs often are written with an emphasis on limiting the vendors' liability and exposure to risk. For Government organizations making cloud procurement decisions, the opportunity to negotiate terms/conditions and the resulting cost should be factored into procurement decisions. This paper provides a detailed SLA Comparison Guide in Table 2.1 that can be applied to assess and compare vendor-offered SLAs and inform procurement decisions.

Table of Contents

THE BIG PICTURE: For Government organizations pursuing a cloud computing solution, SLAs are critical to defining the relationship between the cloud service provider and the consumer.

Cloud SLA Considerations for the Government Consumer

Kevin Buck
Diane Hanf

1.0 Outcome-Driven Cloud Procurement Decision-Making

During the past year, much work has been done to provide a set of terms and definitions that will enable the common discussion of cloud computing. For example, the National Institute of Standards and Technology (NIST) has identified five key characteristics of cloud computing. They are on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity, and measured success.[1] NIST has also defined service models[2] as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Common to these definitions is the perspective of the cloud consumer, where the physical implementation details are hidden, and the virtual aspects of the services are managed on the consumer's behalf. Not only can a consumer obtain each service individually, but many cloud providers offer value-added combinations of IaaS, PaaS, and SaaS. The cloud deployment model can be a private cloud, a shared community cloud, a public cloud, or a hybrid cloud environment. Among cloud computing offerors, there also is a class of cloud integrators who provide services that may range from executing the entire cloud transition to providing a single application migration to the cloud. Thus, cloud computing can take many forms, and service providers and consumers must consider the delivery model in the context of their architecture when structuring agreements between parties.

Before engaging with a provider, Government consumers should have a clear understanding of their cloud procurement objectives and desired outcomes. For example, cloud computing offers the ability to scale and provision computing power dynamically in a cost-efficient way and the opportunity for the consumer to make the most of that power without managing the underlying complexity of the technology. For Government consumers, cloud computing may provide the ability to focus energy and resources on core competencies by outsourcing capabilities that can be obtained more readily and cost effectively from cloud computing providers. Although some cloud computing characteristics, such as scalability on demand and streamlining of the data center, may be very attractive for Government consumers, there are some potential risks to consider:[3]

- Information from multiple organizations residing on the same hardware (often termed multi-tenancy)
- Information security and privacy
- Exposure to third-party liabilities
- Data and application compatibility and portability
- Ability to readily comply with statutory requirements, such as the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley (SOX)[4]
- Lagging open standards development
- Intellectual property rights.

As Federal Government organizations make decisions regarding cloud computing and various cloud procurement options, they should consider the type of provider/consumer relationship that will unfold over the duration of the cloud usage, and how it will align with overarching acquisition strategy.

In some cases, aspects of cloud computing procurement may be aided by the application of approaches that are markedly different from traditional, large-scale Federal acquisitions (e.g., limited competition and application of micro purchase procedures). The Federal Acquisition Regulation (FAR) and numerous agency-specific policies offer considerable flexibility for Government agencies/programs to apply approaches that best fulfill acquisition needs under certain circumstances. These approaches are guided by Federal regulations, agency policies, nature of the services/capabilities to be procured, and vendor contracting/payment options. Because cloud computing can accommodate smaller and less lengthy commitments between consumers and providers, Government consumers should consider the possibility of applying streamlined acquisition approaches for emerging requirements and situations where the Government would benefit from a trial cloud computing engagement. The degree to which the Government can streamline the acquisition of cloud computing offerings will depend on factors such as whether Simplified Acquisition Procedures (SAP) and possibly micro-purchase thresholds apply.[5]

2.0 Managing Cloud Computing Acquisition Performance

While a number of mechanisms are applied by the Federal Government to manage performance of contracts, service-level agreements (SLAs) are emerging as a primary means by which performance standards are codified for cloud computing procurements. As Jonathan Feldman, CIO for the City of Ashville, NC, suggests, "A well crafted service-level agreement is the best way to protect your company as it taps into cloud computing services."[6] SLAs can be a valuable form of protection for providers and consumers.

2.1 Anatomy Of A Good Service-Level Agreement

An SLA is a formal negotiated agreement between two parties. It is a contract between customers and their providers, and it should document a common understanding about agreement features such as priorities, responsibilities, and guarantees. Key objectives of SLAs include reducing areas of potential conflict and encouraging issue resolution before a dispute materializes.[7] SLAs typically are governed by a master agreement (e.g., a contract or "Terms of Service"); in the event of conflict between the terms of SLAs and the master agreement, the master agreement typically prevails.[8] The reader should note that SLAs are not compulsory for Government contracting. Many Government organizations will apply different SLAs for different operational capabilities procured.

Government agency experiences with applying SLAs for managing contract performance objectives have been mixed, and several steps can be taken to avoid common SLA pitfalls. SLAs must be applied consistently, maintained, and updated throughout the contract period of performance to ensure that performance objectives are achieved effectively. All SLAs supporting a particular effort should be managed collectively, and interdependencies should be identified and managed. To form a "meeting of the minds" between parties who may have competing agendas, SLAs should not be applied exclusively as a transactional and computer-generated communication of performance. SLAs also should be applied as a mechanism for managing how the provider and consumer are expected to communicate and coordinate with one another. (Figure 2-1 highlights some SLA elements that specifically address the relationship between the provider and consumer.) To ensure that SLAs are enforceable, they should be formalized at the same time as the governing contractual documents are created, negotiated, and approved. Because SLA administration and management can be resource-intensive, Government organizations should review SLAs periodically to ensure that the stated performance requirements are still essential to achievement of overarching outcomes.

For services acquired by a Government organization from another Government entity, SLAs typically are not applied. Instead, Memoranda of Understanding (MOU) and/or Inter-Agency Agreements (IAA) are applied. The FAR and agency-specific policies dictate the content of these agreements and whether an organization will utilize an MOU, an IAA, or both. Although SLAs typically are not applied to codify agreements between Government agencies, most recommendations within this report are relevant for other performance-related agreements, such as MOUs, IAAs, MOAs, and Expectation Management Agreements (EMAs).

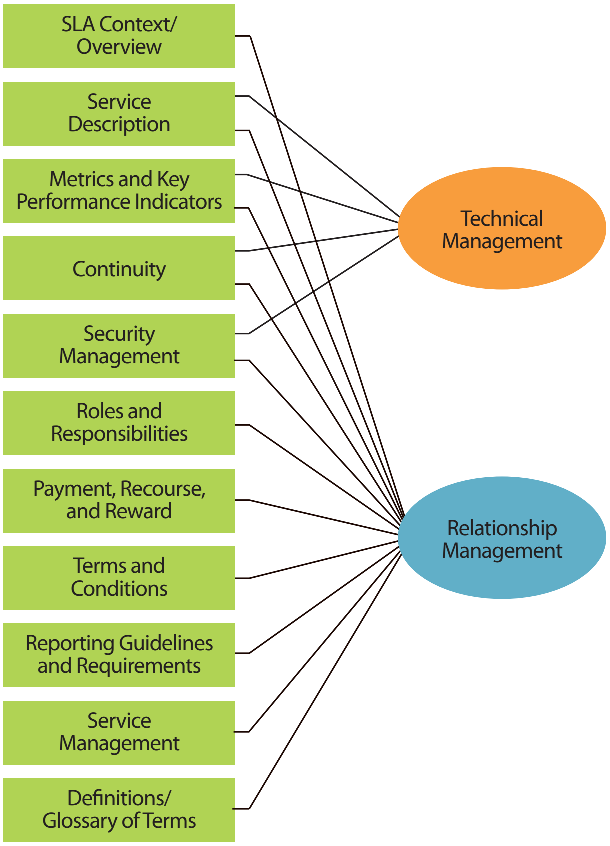
SLA Context/ Overview
Service Description
Metrics and Key Performance Indicators
Continuity
Security Management
Roles and Responsibilities
Payment, Recourse, and Reward
Terms and Conditions
Reporting Guidelines and Requirements
Service Management
Definitions/ Glossary of Terms
Technical Management
Relationship Management

Figure 2-1. Mapping of Cloud SLA Elements to Relationship and Technical Management Activities

The anatomy of a good SLA between a consumer and provider is that:

- It must communicate needs for relationship and technical management.
- The metrics collected are clearly defined and understood, observable, and controllable by the engaging parties.
- Real-world examples, including types of decisions that will need to be made, are provided.
- There is a cadence for revisiting the SLA with the possibility of exiting or renegotiation.
- Ranges of values, rather than point values, are possible or negotiated, and selected ranges are realistic in light of organizational needs (benchmarks, including an organization's own historical data, should be considered).
- Penalties and the process for compensation are executable.
- There is a realistic and effective strategy for transitioning out of poor performance situations.

To increase the effectiveness of SLAs, they should state in measurable terms:

- The service to be performed and outcome expectations
- Key Performance Indicators (KPIs) and the level of service that is acceptable for each
- The manner by which service is to be measured and how "success" is defined
- The parties involved and their responsibilities
- The reporting guidelines and requirements
- Incentives for the service provider to meet the agreed upon target levels of quality.

2.2 Service-Level Agreement Considerations For Government Procurements Through A Public Cloud

A key characteristic of cloud computing offerings is the degree to which SLAs can be negotiated. For this discussion, we define the following terms concerning the negotiation of the SLA:

Offeror Fixed—SLAs are fixed and the level of performance is not negotiable.

Offeror-Driven Negotiated—SLAs can be negotiated within advertised bounds.

Customer-Driven Negotiated—SLAs are fully negotiable.

In the current commercial cloud computing market, offeror fixed SLAs are the most prevalent. Some SLAs can be negotiated within advertised bounds. Potential government consumers of the first two categories of SLAs should evaluate the SLAs against their requirements and understand any gaps and associated risks. It is important to evaluate providers and decide on a best fit. A "best fit" may not be achieved initially, and consumers may need to change providers or performance management approaches. Alternatively, consumers may negotiate their SLAs. Fully negotiable, Customer-Driven SLAs are rarer, but are available to Government organizations that have unique requirements and sufficient funding to procure the capabilities. SLAs for these types of offerings are not as visible in the public domain as providers' standard SLAs, but they are important tool for acquisitions organizations to consider.

Currently, there is limited flexibility offered for the format and key elements of publicly available SLAs. Across the many SLAs that were reviewed in preparing this report, there is considerable variance regarding the details of performance levels and how risk is shared between provider/consumer. Many commercial cloud offerors present one-size-fits-all SLAs; for Government organizations with circumstances that require tailored approaches, this introduces risk. Additionally, a common risk is that "most SLAs are filled with legalese and contractual language that can make it difficult to quantify what exactly a vendor is offering." [9]

The more the vendor is in control of an SLA formulation, the greater the likelihood that the SLAs will be written to protect the vendor as a shield against litigation. Cloud computing consumers seek lower consumer costs and strong SLAs, while providers seek lower costs for providing the service. Currently, with offeror-fixed SLAs, the "balance" favors providers, and most SLAs that have been identified do not incorporate high SLA penalties. G. R. Gangadharan states:

"Currently, most cloud SLAs are rather immature and may be difficult for consumers to understand. Also, these SLAs are rather one-sided; they were drafted by providers and basically give them most of the rights and hardly any liability. Understanding the offerings and obligations of an SLA unambiguously will help consumers better meet their business needs through the prudent and informed use of cloud services."[10]

Because the current public cloud computing market predominantly involves offeror-fixed and offeror-driven negotiated SLAs, Federal agencies should include comparison of SLAs as a vendor selection criterion. When selecting an offering, procurement staff should consider how government consumer concerns are addressed, especially those relating to accountability and security. It is important to focus on at least three areas with SLAs: data protection, continuity, and costs. From a data protection perspective, the SLA should define who has access to the data and protections in place. However, government sponsors should not expect much SLA flexibility for contracts that do not represent a substantial dollar value to the vendor. When vendors respond to Government acquisition requests to customize performance levels and other aspects of SLAs, this will likely come at an increased cost. According to a recent Booz/Allen/Hamilton study:[11]

"Customers should apply the same SLA standards in a cloud computing environment that they would in an outsourcing requirement. When entering the tenuous nature of the cloud, however, customers must be increasingly vigilant in assessing their needs, what they are or are not willing to negotiate, and the price they are willing to pay for guarantees and assurances."

2.3 A Cloud Service-Level Agreement Comparison Guide

A key characteristic of the current public cloud market is that commercial cloud computing commodity/service providers often offer SLAs that are non-negotiable. In general, commercial cloud computing vendors would like to standardize their commitments (including performance levels) and relationships across their customer base. Certainly, this standardization creates stability in offerings for the vendors, economies-of-scale in commodity/service provisioning, and a limitation of vendor risk.

Because the Government will not be able to always dictate SLA elements or performance levels at an acceptable price, the Government should evaluate the offered SLA features carefully when deciding on cloud computing procurement options. Because vendors may not offer similar SLA structures, service offerings, performance levels, and negotiation opportunities, the Government should compare/contrast vendor SLAs. The *SLA Comparison Guide* illustrated in Table 2-1 identifies summary-level SLA elements that may be recommended for a Government organization, based on specific organizational considerations and the nature of service/capability to be procured through the cloud. Each summary-level SLA element identified in Table 2-1 is described in detail within Appendix A. The matrix was developed based on a comparison of SLA approaches and best practices. Some of the elements recommended for consideration in evaluating and comparing cloud computing SLAs may be incorporated in the Terms of Service, Terms of Use, or contract (e.g., "Service Agreement"). Appendix B of this report provides a list of example SLAs that are relevant for cloud computing. This matrix highlights elements within these examples that align with specific recommendations made within Table 2-1.

The SLA Comparison Guide incorporates recommendations for including elements within an SLA that clearly communicate relationships and technical agreements between providers and consumers. Although Government organizations often will not incorporate relationship considerations within SLAs, we offer them in this comprehensive SLA structure because they frequently are a critical dimension of SLAs to incentivize superior performance and reduce Government exposure to risks. Cloud computing SLAs do not need to incorporate every element identified within the *SLA Comparison Guide* or address them as comprehensively as described. We suggest that procurement staff apply the *SLA Comparison Guide* as an aid in determining whether cloud computing concerns and risks, which are specific to the particular Government organization's circumstances, are

Table 2-1. SLA Comparison Guide

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
SLA Context/ Overview	The SLA should identify the provider, the consumer, contact information, SLA purpose, and SLA background. Overall, SLAs should be simple, familiar, and easy to understand.[i]	Context/overview is an important historical record of the nature of support and obligations. Not all Government staff who may need to touch the SLA will be intimately familiar with the relationship of key performance obligations and overall service/capability commitments.	Theilmann, W., September 2008, "SLA@SOI-An Overview," SAP http://sla-at-soi.eu/wp-content/uploads/2008/12/slasoi-e28093-an-overview.pdf Delaney, J., 2004, The Outsourcing Revolution, 2004: *Protecting Critical Business Functions.*
Service Descriptions	The SLA should provide a clear and logical linkage of overall service/capability offerings, objectives, and key performance indicators (KPIs). This logical description should start with a clear overview of: • Baseline services • Optional services • Customer-unique services SLAs should be measurable and actionable.[ii] Service groups or other logical categorization of services should be identified, along with a description of the overall service strategy (e.g., service improvements). For each service group, this SLA element should identify: • Handling of service interruptions • User services such as administration and installation • Requirements to achieve performance levels described later in the SLA, including required capability (lower/upper limit) and allowed workload/usage of the service. Operational parameters that will govern the service delivery environment should be described. "These operational parameters may affect service performance and therefore must be defined and monitored. If operational parameters move outside the control of the service provider or users of the service exceed the limits of their specified operational parameters, then the SLA may need to be renegotiated. Examples include maximum number of concurrent on-line users; peak number of transactions per hour; and maximum number of concurrent user extracts or ad hoc queries." [iii]	The upfront service description should break down the offered services into service groups or some other logical categorization. Consumers should be wary of overly optimistic/vague promises and goals for performance that cannot be measured objectively.	Delaney, J., 2004, *The Outsourcing Revolution, 2004: Protecting Critical Business Functions.* Financial Management Line of Business, "Migration Planning Guidance, Version 1," http://www.fsio.gov/fsio/download/fmlob/mpgv1/1.2_-_Frequently_Asked_Questions.pdf Anderson, B., "Structuring Meaningful SLAs for IT Support," http://www.itmpi.org/assets/base/images/itmpi/StructuringMeaningfulSLAsforITSupportV5.pdf

Continuity or Outages	This SLA element should describe how service/capability continuity and outages will be managed by the provider.	Key questions that may need to be answered within the SLA include: • How is a service outage defined? • How is the customer compensated for an outage? • What level of redundancy is in place to minimize outages? • Will there be a need for scheduled downtime? • How often does the provider test disaster recovery and business continuity plans? The SLA should identify the burden of proof in circumstances when services/capabilities are not continuous, as agreed. As it specifically relates to cloud computing, proving cause of outage, for example, is difficult when usage typically traverses many network layers that may not be owned/controlled by the vendor. Consumers need to understand how difficult it will be to prove that an outage was not their fault and is instead a problem of the cloud vendor. When burden of proof is a particular risk area for a consumer, they should carefully consider whether the SLA is sufficiently explicit regarding roles/responsibilities in events that interrupt agreed upon continuous service. In some SLAs, continuity is addressed as part of Security Management.	Ohlhorst, F., June 16, 2009, "What to Look for in a Cloud Computing SLA," http://searchcio.techtarget.com.au/news/2240020663/What-to-look-for-in-a-cloud-computing-SLA Invokate, "Penalty-Based Outsource Supplier Management," http://www.solarsysconsulting.com/invokate/service_level_agreement.htm, accessed June 24, 2010.
Roles and Responsibilities	SLAs will often hold the consumer, not just the provider, accountable for certain actions: • Adhering to any related policies, processes and procedures. • Reporting problems using the problem reporting procedures described in the SLA. • Scheduling in advance all service related requests and other special services with the service provider. • Developing and maintaining system related documentation (this could also be a service provider responsibility). • Making customer representative(s) available when resolving a service related incident or request. • Communicating when system testing and/or maintenance may cause problems that could interfere with standard business functions.	Clear delineation of roles and responsibilities has been identified as a significant driver of SLA success. This element of the SLA should describe how the consumer can be a good citizen and maintain credibility with the service provider.	Karten, N., 2003, "Why SLAs Fail and How to Make Yours Succeed." Feldman, J., February 2010, "Cloud Contracts and SLAs," *InformationWeek Analytics,* http://analytics.informationweek.com/abstract/5/2274/Cloud-Computing/informed-cio-cloud-contracts-and-slas.html University of Minnesota, 2009, "IT Service Level Agreement–Best Practice," http://www.uservices.umn.edu/pmo/docs/Deploy/BEST_PRACTICE_Service_Level_Agreements.doc
Payment, Recourse, and Reward	The SLA should clarify: • When/how payment is to be made • What constitutes excused or excluded performance • Escalation procedures • How service-level bonuses and penalties are administered • Remedy circumstances and mechanisms.	The SLA should have negotiated financial penalties when an SLA violation occurs. If there is no repercussion when the provider fails to meet their SLA, the SLA is not as valuable to the consumer. Similarly, the consumer also should be willing to pay a reward for extraordinary service-level achievements that deliver real benefits.	Hiles, A., 2000, "Service Level Agreements: Winning a Competitive Edge for Support and Supply Services," Rothstein Associates, Inc., p.113.
Terms and Conditions	In cloud computing procurements, some of the sub-elements identified below (refer to Appendix A) may be provided in the "Terms of Service" or "Terms of Use" documentation rather than being directly incorporated in the SLA.	This SLA element should support a clear understanding of business risk for the cloud computing consumer.	

Reporting Guidelines and Requirements	SLAs should identify agreements regarding access to provider performance logs and reports, and performance and status reporting that will be provided.	Performance monitoring is an essential step in avoiding disagreements about who is responsible for performance failures.[iv]	Parera, D., April 21, 2008, “Put SOA to the Test,” *FCW.com*.
Service Management	The SLA may describe how (e.g., tools applied) the provider will manage overall service delivery for vendors. For example, the SLA may indicate the application of ITIL standards/processes.	Be able to account for assets in the cloud, get performance feedback for cloud-deployed assets. How automated is this, how much does the sponsor do vice the provider.	Torode, C., August 6, 2009, “Beware These Risks of Cloud Computing, from no SLAs to Vendor Lock,” *CIO News.*
Definitions/ Glossary of Terms	Include definitions of fees and aspects of service that are within the scope of the SLA.	“An effective SLA should include an unambiguous description of terminology and a concise definition of all the services provided. Clarity is paramount–you need to understand what the reports generated say. A very common problem with SLAs is a lack of agreement on the terminology and service definitions. More often than not, SLAs comprise of arcane service definitions and/or merely list the services bought and paid for, with no guarantees for quality of service.” [v]	Dimension Data, November 2009, “Is Your SLA Your Weakest Link?” p. 7, http://www.dimensiondata.com/Lists/Downloadable%20Content/IsYourSLAYourWeakestLinkOpinionPiece_129088975412137750.pdf.

addressed appropriately within cloud computing SLAs. Figure 2-1 identifies whether primary SLA elements, as reflected in the *SLA Comparison Guide,* support technical or relationship management aspects of cloud performance agreements.

By applying the guide as a comparison when reviewing available SLAs, the Government organization is better able to gauge the relative degree of comprehensiveness and rigor applied by candidate providers in their SLAs. Because the guide incorporates a synthesized assessment across a relatively broad spectrum of actual SLAs (including best practices and lessons learned), a Government organization is able to focus more attention on those particular aspects of a procurement that are of priority concern. Appendix C provides an example of how the comparison guide can support Government organization in making decisions regarding the selection of a cloud computing service provider.

3.0 Conclusions and Recommendations

Writing for GCN, Rutrell Yasin recently stated, “Agency officials cannot afford to ignore the movement to the cloud, especially because the Obama Administration has mandated that agencies look for greater efficiencies using cloud computing. As a result, agencies should start to develop a cloud strategy and identify candidates for pilot projects, experts say. Tasks that are well suited for the cloud include software development, email, collaboration and social media software, content management, and Web portal environments.” [12]

Based on the current cloud computing procurement environment, the approach to negotiating SLAs is a departure from how the Federal Government is accustomed to managing contracted IT service/capability performance. Vendors are, for the most part, defining SLA structure, elements, and performance levels. As such, Government agencies must include consideration of vendor-offered SLAs in making cloud computing procurement decisions. “service-level agreements span across the cloud and are offered by service providers as a service based agreement rather than a customer based agreement.” [13] According to F. Ohlhorst in *Assessing Cloud Providers*, “one of the first steps for choosing cloud service providers is to evaluate the level of service offered and the guarantees behind that service.” [14] Ohlhorst further recommends that SLAs be scrutinized under three lenses: data protection, continuity, and costs.

Cloud computing brings about a different measure for service performance as described below:[15]

The “pay-as-you-go” nature of cloud computing breaks the link between component and service performance: typically, organizations pay for capacity or throughput, rather than specific components. Plus, the highly dynamic nature of the computing

> *infrastructure that exists in the cloud makes traditional [configuration management database] CMDB (or simple list) based systems management virtually impossible to implement. All the traditional server and network reporting that shows 99.999 up-time will become secondary and probably irrelevant for future service-level management and reporting. What this means is that synthetic transaction monitoring—that is, generating, monitoring, and reporting on simulated service requests—will be of paramount importance.*[16]

SLAs from cloud computing service providers must emphasize service reliability rather than component reliability. Momentum for applying SLAs as a codification of a "meeting of the minds" between consumers and providers considerably increased with the advent of Performance-Based Acquisition (PBA), for which a key tenet is focusing on desired outcomes rather than the specifics of how those outcomes are achieved. In reviewing SLAs to support decisions regarding cloud offerings, Government organizations should pay more attention to whether ultimate goals will be achieved, and carefully weigh how important it is that specific approaches (e.g., application of specific software) are applied to achieve those goals.

Appendix A—Guide for Comparing Cloud Computing SLAs

Table A-1. SLA Context/Overview

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
SLA Context/ Overview	The SLA should identify the provider, the consumer, contact information, SLA purpose, and SLA background. Overall, SLAs should be simple, familiar, and easy to understand.[vi]	Context/overview is an important historical record of the nature of support and obligations. Not all Government staff who may need to touch the SLA will be intimately familiar with the relationship of key performance obligations and overall service/ capability commitments	Theilmann, W., September 2008, "SLA@ SOI-An Overview," SAP, http://sla-at-soi.eu/wp-content/uploads/2008/12/slasoi-e28093-an-overview.pdf Delaney, J., 2004, The Outsourcing Revolution, 2004: Protecting Critical Business Functions.
Provider and Consumer Contact Info	Each party should establish a principal communications POC who is available during normal business hours. Alternates should be identified for periods of unavailability (e.g., vacation, deployment, or other travel). Each primary POC should establish a secondary POC.	Consumers need to know who is specifically obligated to respond to complaints/ issues, including names, positions, and organizations. This SLA element should clarify whom the consumer can contact ASAP should something go awry.	Financial Management Line of Business, "Migration Planning Guidance, Version 1," http://www.fsio.gov/fsio/download/fmlob/mpgv1/1.2_-_Frequently_Asked_Questions.pdf
Purpose/ Background	The SLA should explain why the agreement is necessary and why the particular vendor is qualified to fulfill performance obligations.	This SLA element should provide insights into the scope of agreement coverage. It should provide a high-level summary of the service/capability offering.	HHS, EPIC SLA/MOU Template, Version 1.0, http://www.hhs.gov/ocio/eplc/EPLC%20Archive%20Documents/50-SLA%20and%20MOU/eplc_sla_mou_template.doc
Scope	The SLA should clearly describe what is in scope and what is not. Scope may be defined in a number of ways (e.g., specific provider assets to be applied).	This SLA element can provide insights into excused performance failures/degradation. Scope descriptions are critically important to determine whether future proposed SLA changes involve a scope change. Government consumers should be able to discern from the SLA whether it is addressing the overall cloud experience or whether it is focusing on particular instances of cloud engagement.	Itil & ITSM World, "The Service Level Agreement," http://www.itil-itsm-world.com/itil-sla.htm, accessed June 23, 2010 Nolle, T., May 22, 2009, "Meeting Performance Standards and SLAs in the Clouds," http://searchcloudcomputing.techtarget.com/tip/0,289483,sid201_gci1357087,00.html
Stakeholders	Key stakeholders (e.g., end-users, other consumers, regulatory agencies) and their roles in service/capability delivery should be identified. "Gotchas" include a failure to identify sub-contractors and consumers within foreign countries. The stakeholders section of the SLA should describe the vendor's process for supplier management.	Government consumers should be interested in which other Governments, organizations, and individuals are customers for this particular vendor's offering as described in the SLA. Consumers also should be interested if regulatory compliance plays a key role in service/capability delivery.	University of Minnesota, 2009, "IT Service Level Agreement – Best Practice," http://www.uservices.umn.edu/pmo/docs/Deploy/BEST_PRACTICE_Service_Level_Agreements.doc

Table A-2 Service Descriptions

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
Service Descriptions	The SLA should provide a clear and logical linkage of overall service/capability offerings, objectives, and key performance indicators (KPIs). This logical description should start with a clear overview of: • Baseline services • Optional services • Customer-unique services. SLAs should be measurable and actionable.[vii] Service groups or other logical categorization of services should be identified, along with a description of the overall service strategy (e.g., service improvements). For each service group, this SLA element should identify: • Handling of service interruptions • User services such as administration and installation • Requirements to achieve performance levels described later in the SLA, including required capability (lower/upper limit) and allowed workload/usage of the service. Operational parameters that will govern the service delivery environment should be described. "These operational parameters may affect service performance and therefore must be defined and monitored. If operational parameters move outside the control of the service provider or users of the service exceed the limits of their specified operational parameters, then the SLA may need to be renegotiated. Examples include maximum number of concurrent on-line users; peak number of transactions per hour; and maximum number of concurrent user extracts or ad hoc queries." [viii]	The upfront service description should break down the offered services into service groups or some other logical categorization. Consumers should be wary of overly optimistic/vague promises and goals for performance that cannot be measured objectively.	Delaney, J., 2004, "The Outsourcing Revolution, 2004: Protecting Critical Business Functions." Financial Management Line of Business, "Migration Planning Guidance, Version 1," http://www.fsio.gov/fsio/download/fmlob/mpgv1/1.2_-_Frequently_Asked_Questions.pdf Anderson, B., "Structuring Meaningful SLAs for IT Support," http://www.itmpi.org/assets/base/images/itmpi/StructuringMeaningfulSLAsforITSupportV5.pdf
Objectives	Service-Level Objectives (SLOs) are a means of measuring the performance of the service provider. They also are outlined as a way of avoiding disputes between the two parties based on misunderstanding. SLOs are specific measurable characteristics of the SLA (e.g., availability, throughput, response time, or quality). The SLO may be composed of one or more quality-of-service measurements that are combined to produce the SLO achievement value. For example, an availability SLO may depend on multiple components, each of which may have a Quality of Service (QOS) availability measurement. The combination of QOS measures into an SLO achievement value will depend on the nature and architecture of the service.	The SLA should not launch into tactical level performance metrics immediately. The service/capability performance obligations can be understood better if they are linked to overarching service/capability objectives. Often, a combination of metrics that are described later in the SLA will be aggregated and synthesized to assess the degree to which an objective has been achieved.	Karten, N., 2003, "Why SLAs Fail and How to Make Yours Succeed." Strum, R. and W. Morris, 2000, "Foundations of Service Level Management."

Service Inter-Dependencies	SLAs should reflect interdependencies among processes. "Achieving SLAs for application performance or availability will be impossible if demand, capacity, provisioning, and utilization are not effectively managed." [ix]	This SLA element can provide insights into excused performance failures/degradation. Consumers should be very interested in what other factors may influence service performance.	Shafer, P., "How SLAs drive, and don't drive, performance: strategic, technical and process limitations," http://www.iaccm.com/contractingexcellence.php?storyid=514, accessed June 23, 2010.
Customer Service Offered	Key questions that an SLA should answer include: • How can the consumer ask questions and obtain technical support (e.g., telephone, chat, email)? Does it cost extra? • Are additional technical and advisory services available? By what means and how quickly, will I be notified of significant changes, upgrades, or extended maintenance?	Consumers should want to know what other forms of support are available, beyond the computing capabilities that are included as part of the "service offering." These additional services may come at an additional cost.	"Checklist: Service Level Agreement," *IT Process Maps*, http://wiki.en.it-processmaps.com/index.php/Checklist_Service_Level_Agreement_(SLA), accessed June 30, 2010.
Optional Features	Optional features may include, for example, "… promises that certain types of transactions will take a certain length of time, management APIs, programmatic access to the health model of a service … the ability to pause or stop an application or a piece of one from running on the fly, and the ability to do things like trigger back-up of data at certain points in time." [x]	This SLA element helps clarify what is considered basic, built-in capability versus what is considered "extra," for which additional fees or tailored agreements may apply.	Hoover, J.N., October 30, 2008, "Will Microsoft Shake Up Cloud Computing SLAs?" *Plug Into the Cloud—Information Week*, http://www.informationweek.com/cloud-computing/blog/archives/2008/10/will_microsoft_2.html

Table A-3. Metrics and Key Performance Indicators

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
Metrics and Key Performance Indicators	SLAs must, at a minimum, represent guaranteed performance thresholds. An SLA should identify the metrics for which the provider's performance will be determined. Measurement method and levels of agreed upon performance should be comprehensively described. SLAs also may identify KPIs, which reflect desired performance targets. When stretch targets are incorporated in SLAs, the SLA should identify any compensation that will be provided to incentivize performance above and beyond.	For many consumers, this is considered the most important element of the SLA because it defines the performance agreement between the provider and consumer. KPIs, by definition, reflect desired performance targets.	Shafer, P., "How SLAs drive, and don't drive, performance: strategic, technical and process limitations," http://www.iaccm.com/contractingexcellence.php?storyid=514, accessed June 23, 2010.
Levels of Service Available	Levels of service should include both service measures and service criteria (i.e., conditions under which service will be measured and specific service levels promised).	"One of the most critical aspects in drafting and negotiating a cloud computing agreement is establishing appropriate service levels in relation to the availability and responsiveness of the software. Because the software is hosted by the vendor, outside the control of the client, service levels serve two main purposes. First, service levels assure the client that he/she can rely on the software in its business and provide appropriate remedies if the vendor fails to meet the agreed service levels. Second, service levels act as benchmarks that facilitate the vendor's continuous quality improvement process and provide incentives that encourage the vendor to be diligent in addressing issues." [xi] Multiple service levels could be defined. Specifics, such as hours and days when different levels of service will be applied or are available, should be defined. The SLA should provide a guarantee of the quality and performance of operational functions like availability, reliability, performance, maintenance, backup, disaster recovery, etc. that will now be under the vendor's control since the applications are running in the cloud and managed by the vendor.	Cain, C., February 12, 2010, "Basic Understanding Can Clear Fog Surrounding 'Cloud Computing' Agreements," *WTN News*, http://wistechnology.com/articles/7082/ Anderson, B., "Structuring Meaningful SLAs for IT Support," http://www.itmpi.org/assets/base/images/itmpi/StructuringMeaningfulSLAsforITSupportV5.pdf Financial Management Line of Business, "Migration Planning Guidance, Version 1," http://www.fsio.gov/fsio/download/fmlob/mpgv1/1.2_-_Frequently_Asked_Questions.pdf

Performance Metrics	SLAs may contain numerous service performance metrics with corresponding service-level objectives. Many IT-service related SLAs will align with IT Infrastructure Library (ITIL) specifications, and key areas of performance would include those related to service requests; incident management and continuity; problem resolution, change, release, capacity, and configuration management; availability; and security. Example types of performance metrics relevant for cloud computing include: • Response time—the average, median, or maximum time it takes a service to handle user requests • Transaction time—the time that elapses from when a service is invoked to transaction processing completed, including delays • Resolution rate—the time period between detection of a service problem and resolution of the problem (a sign of commitment for repair and recovery) • Reliability (as it relates to hardware and/or software configuration of services and the network connections between providers/consumers): – *Service-level violation rate*—expressed as the mean rate of SLA violation due to infringements of the agreed warranty levels – *Availability*—represented as the percentage of uptime for a service in a given observation period.	Some key considerations for Government cloud consumers include: • Selecting the appropriate metrics can be complicated because there can be many candidate metrics for consideration. The number and complexity of metrics to apply should depend on organizational experience with metrics, the type of performance to be incentivized, and the cost and effort of collection. • "… everything associated with an application experience isn't part of cloud computing. Cloud performance as measured at the point of application use is the sum of network performance, application performance, and cloud infrastructure performance." [xii] • Performance measures should not be contradictory. • Performance metrics drive service levels, which, in turn, drive cost. • Service, rather than component, reliability should be emphasized. Government consumers will have limited ability to select which particular vendor components will be applied to provide service. Some Government consumers will need a sense of confidence that their vendor understands that some aspects of desired delivery are uncertain.	Gangadharan, G.R., 2009, "Understanding SLAs for Cloud Services," *Clutter IT Journal,* Vol. 22, No. 6/7. Financial Management Line of Business, "Migration Planning Guidance, Version 1," http://www.fsio.gov/fsio/download/fmlob/mpgv1/1.2_-_Frequently_Asked_Questions.pdf Nolle, T., May 22, 2009, "Meeting Performance Standards and SLAs in the Clouds," http://searchcloudcomputing.techtarget.com/tip/0,289483,sid201_gci1357087,00.html Miller, R., January 15, 2008, "Reliability in the Cloud: SLAs will Matter," *Data Center Knowledge,* http://www.datacenterknowledge.com/archives/2008/01/15/reliability-in-the-cloud-slas-will-matter/
Quality Assurance, Performance Data Requirements, and Measurement Methodology	Measurement methods applied should be amenable to quantitative/objective assessment. Some SLAs will include a measurement-to-performance evaluation mapping. Examples of what the vendor may offer include methodologies applied to measure/estimate delay variations, packet loss, etc.	Some methodologies applied may be labor/resource intensive and may significantly influence service pricing. Government consumers should look for the vendor to apply less resource intensive and unambiguous data collection. This SLA element should answer questions such as: • How will the provider instrument the service provisioning to ensure that performance levels are achieved? • By what means and how frequently, will the provider audit/monitor performance? • How will the provider anticipate problems that may lead to SLA non-compliance? • How will traffic and performance be managed? • Who is responsible for making the measurements (consumer, provider, or both?) • Where in the larger system will the measurements be made? • What part of the measurements does each party control? • Why is this measure important? What decisions does this measure support? • When will the measurements be collected (e.g., continuously, periodically)?	Chappell, C., "Preparing for Cloud Computing: The Managed Services Revolution," http://www.ca.com/files/whitepapers/ca_cloud_computing_en_us_1108.pdf Camous, D., "Challenges to QoS and SLA Management," http://www.billingworld.com/articles/2002/04/challenges-to-qos-and-sla-management.aspx Sommers, J., et. al., 2007, "Efficient Network-Wide SLA Compliance Monitoring," SIGCOMM Proceedings, http://ccr.sigcomm.org/online/?q=node/251

Service-Level Improvement	The SLA may include stretch goals and/or performance improvement commitments. Often these performance ranges will be included in the SLA section associated with service levels. If improvements in service levels are identified, the SLA should clearly identify whether the improvements must be incentivized through additional compensation (monetary or otherwise) or whether the vendor is simply promising improvements by some specific point in the future. Service performance improvements and stretch goal achievement should be tied closely to the SLA element associated with incentivization and penalties.	Vendors may obligate themselves to future improvements in service levels. Government consumers may require that initial service levels be improved at various points during the service commitment, and the SLA should clearly identify a vendor's offering requires compensation for proposed future improvements. Initial pricing may include compensation for future service level improvements that are not sufficiently valued by the Government.	"ITIL Key Performance Indicators," IT Process Maps, http://wiki.en.it-processmaps.com/index.php/ITIL_Key_Performance_Indicators, accessed June 30, 2010.

Table A-4. Continuity or Outages

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
Continuity or Outages	This SLA element should describe how service/capability continuity and outages will be managed by the provider.	Key questions that may need to be answered within the SLA include: • How is a service outage defined? • How is the customer compensated for an outage? • What level of redundancy is in place to minimize outages? • Will there be a need for scheduled downtime? • How often does the provider test disaster recovery and business continuity plans? The SLA should identify the burden of proof in circumstances when services/capabilities are not continuous, as agreed. As it specifically relates to cloud computing, proving cause of outage, for example, is difficult when usage typically traverses many network layers that may not be owned/controlled by the vendor. Consumers need to understand how difficult it will be to prove that an outage was not their fault and is instead a problem of the cloud vendor. When burden of proof is a particular risk area for a consumer, they should carefully consider whether the SLA is sufficiently explicit regarding roles/responsibilities in events that interrupt agreed upon continuous service. In some SLAs, continuity is addressed as part of Security Management.	Ohlhorst, F., June16, 2009, "What to Look for in a Cloud Computing SLA," http://searchcio.techtarget.com.au/news/2240020663/What-to-look-for-in-a-cloud-computing-SLA Invokate, "Penalty-Based Outsource Supplier Management," http://www.solarsysconsulting.com/invokate/service_level_agreement.htm, accessed June 24, 2010.
Incident Response and Reporting	The SLA should identify what is considered an incident, how the vendor will respond to different types of incidents, and how the vendor will report and respond to incidents.	Key questions that may need to be answered within the SLA include: • How much maintenance notification will be provided? • What types of notifications are immediately provided? • How can the cloud consumer report security events and anomalies? • Is there a real time security monitoring (RTSM) service in place? • How long are security logs retained and who can access them? • How are severity levels and escalation procedures defined? • Does the provider collect incident metrics? The Government consumer should look for vendors to take responsibility for undertaking root cause analysis and fix for incidents that are within the control/responsibility of the vendor.	European Network and Information Security Agency, November 2009, "Cloud Computing–Benefits, Risks, and Recommendations for Information Security," http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport. Subramanian, K., August 6, 2009, "Will Government Alter the Cloud SLA Game?" Cloud Avenue, http://www.cloudave.com/1758/will-government-alter-the-cloud-sla-game/ Booz Allen Hamilton, December 2009, "Cloud Computing Security," http://www.boozallen.com/publications/article/cloud-computing-security

Disaster Recovery	The SLA should identify what constitutes a "disaster," what steps will be taken by the vendor when disaster strikes, and guarantees that the vendor provides for meeting service levels in spite of disaster. The SLA also should provide contact information and identify hours for contact during emergencies. The topic of disaster recovery may be addressed in the security section of the SLA, or possibly in a section identified as problem management/ resolution.	Key questions that should be answered by this SLA element include: • Does the vendor use a disaster recovery service? • What is the maximum number of hours of data that will be lost? • After a disaster, when will applications be made available and from where?	Hickey, A., March 19, 2010, "Cloud SLAs Add New Level of 'Confidence'," *ChannelWeb,* http://www.crn.com/news/applications-os/224000198/cloud-slas-add-new-level-of-confidence.htm "Disaster Recovery and Business Continuity," *The SLA Zone,* http://www.sla-zone.co.uk/disaster.htm, accessed June 29, 2010.
Outage Resolution	The SLA should define what constitutes an "outage" that would affect the consumer of the particular services/capabilities. Outage resolution will include commitments regarding timeframe for resolving outages.	The SLA should clearly describe what constitutes an outage with respect to the service being provided. For instance if an application goes off-line and data is lost, is that compensable? Outages due to scheduled maintenance should be discussed and understood. Key questions that should be answered by this SLA element include: • How will outages be monitored? • When and how do consumers report outages? • When will the vendor acknowledge outages and how? • How frequently will updates about outage resolution be provided? Consumers should ask themselves how much "planned" and "unplanned" outages they can tolerate.	Willis, J. M., March 23, 2009, "The Tale of Three Clouds SLA's," http://itknowledgeexchange.techtarget.com/cloud-computing/2009/03/23/the-tale-of-three-cloud-slas-2/. "Defining Service Level Agreements," http://www.dalnet.lib.mi.us/help/FootPrintsHelp/Defining_Service_Level_Agreements.htm, accessed June 24, 2010.
Continuity-Related Definitions	This may not be a separate subsection of the SLA, but SLAs should somewhere define terms associated with continuity.	Key terms that consumers should want clearly defined include continuity, outage, disaster, emergency, planned outage, unplanned outage, and high availability. "The agency's legal department needs to understand the differences between common SLA terms such as 'average configuration downtime' or 'network downtime' versus 'systems downtime.'" xiii	VeriSign, "Service Level Agreement," http://www.verisign.com/static/002488.pdf. Goertzel, K. et. al., December 2009, "Cloud Computing for Real," FedTech Magazine, http://www.fedtechmagazine.com/print_friendly.asp?item_id=663

Table A-5. Security Management

SLA Element	Desired Features and Potential “Gotchas”	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
Security Management	Consumers should expect that the SLA will address key areas of security risk, and especially the security of their data. SLAs should include a description of approaches that the provider will implement to enhance security.	Security has been identified as one of the key risk areas for Government cloud computing consumers. Consumers should be wary of claims by the provider that they will “guarantee” security as many legal issues surround obligations as they relate to security, privacy, uptime, storage, and transportation. In some SLAs, some aspects of Security Management will be addressed as part of continuity.	Booz Allen Hamilton, December 2009, “Cloud Computing Security,” http://www.boozallen.com/publications/article/cloud-computing-security UW ISchool, Winter 2010, “Can Cloud Computing Supplier Really Guarantee Data Security,” Info, Law, IP, & Ethics, Class Blog for IMT 550, http://brianrowe.org/IMT550/2010/03/17/can-cloud-computing-supplier-really-guarantee-data-security/
Vendor Security Controls	Ideally, SLAs should describe if/how the provider will monitor bad actors.	“The primary concern associated with cloud offerings is that customer data is stored offsite at the vendor’s data centers and therefore must be protected by the vendor’s security controls. An additional concern with cloud offerings is that data from multiple customers is potentially co-located in one facility—increasing the value of the data stored at the center.” [xvi] Consumers should identify if their specific circumstance compels having special security measures such as physical security to avoid physical tampering of data.	Booz Allen Hamilton, December 2009, “Cloud Computing Security,” http://www.boozallen.com/publications/article/cloud-computing-security Torode, C., August 6, 2009, “Beware These Risks of Cloud Computing, from no SLAs to Vendor Lock,” *CIO News.* Goertzel, K. et. al., December 2009, “Cloud Computing for Real,” *FedTech Magazine*, http://www.fedtechmagazine.com/print_friendly.asp?item_id=663.
Privacy Guarantees	This element of the SLA should include a description of any provider guarantees regarding use of personally identifiable information.	A key question that the SLA should answer: Does the vendor guarantee privacy of information?	Booz Allen Hamilton, December 2009, “Cloud Computing Security,” http://www.boozallen.com/publications/article/cloud-computing-security Torode, C., August 6, 2009, “Beware These Risks of Cloud Computing, from no SLAs to Vendor Lock,” *CIO News.*
Vendor Position Regarding Customer-Requested External Security Audits	Given the significant concerns regarding cloud security, providers are currently receiving many requests for external security audits to be performed. SLAs or related contractual documentation should identify the providers’ position regarding external security auditing.	“Although many vendors provide customers thorough descriptions of their existing security controls, few—if any—allow customers to perform a detailed audit of their security controls and standards.” [xv]	European Network and Information Security Agency, November 2009, “Cloud Computing–Benefits, Risks, and Recommendations for Information Security,” http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport. Booz Allen Hamilton, December 2009, “Cloud Computing Security,” http://www.boozallen.com/publications/article/cloud-computing-security Goertzel, K. et. al., December 2009, “Cloud Computing for Real,” *FedTech Magazine*, http://www.fedtechmagazine.com/print_friendly.asp?item_id=663.
Vulnerability Management	Some vendors are now including within their SLAs an indication of the maximum amount of time that the vendor will take to check and test systems after the announcement of a vulnerability. Other providers may prohibit port scans, vulnerability assessment, and penetration testing.	The SLA may provide insights into vendors’ commitment to address identified vulnerabilities proactively. The SLA should clearly identify whether port scans, vulnerability assessment, and penetration testing will be performed and/or are allowed.	European Network and Information Security Agency, November 2009, “Cloud Computing–Benefits, Risks, and Recommendations for Information Security,” http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport Booz Allen Hamilton, December 2009, “Cloud Computing Security,” http://www.boozallen.com/publications/article/cloud-computing-security nCircle Network Security, 2005, “nCircle’s 24 Hour SLA,” http://www.ncircle.com/pdf/resources/nCircle_24hr_SLA.pdf

Problem Resolution	SLAs may address provider, as well as consumer, commitments regarding resolution of problems at various places throughout the SLAs, depending upon the nature of the problem. Some SLAs will describe, in detail, the steps that will be taken throughout the resolution process from initial identification of a problem through ultimate resolution. The SLA descriptions may include customized processes depending upon the severity/priority of the problem.	Consumers should understand their obligations as they relate to reporting potential and realized problems. In addition, consumers should determine whether the SLA identifies timeframes and procedures as they relate to initial response, initial fix, and problem resolution. Because problems that are experienced may be symptoms of issues that may recur or increase in severity over time, consumers should identify whether the SLA, or other related contractual documentation, identifies vendor commitments to perform root cause analyses.	Booz Allen Hamilton, December 2009, “Cloud Computing Security,” http://www.boozallen.com/publications/article/cloud-computing-security Georgetown University McDonough School of Business, January 2010, “MSB Technology Center SLA,” http://technology.msb.edu/useful_info/sla.pdf
Data Ownership, Protection, and Control	Consumers should have an understanding of where and how data is stored. “Agencies should ensure the SLA clearly defines who has access to the data and the protections that are in place. The data and IT managers will need to understand how the provider’s infrastructure and services are used to provide persistent access to needed applications and data sets. Continuity is important. In a perfect world, a vendor could guarantee access 100 percent of the time, but, in reality, a guarantee like that is impossible. Organizations also should have a clear definition of who owns the data and should consider self-protecting data options as necessary.” [xvi]	“The primary concern associated with cloud offerings is that customer data is stored offsite at the vendor’s data centers and therefore must be protected by the vendor’s security controls. An additional concern with cloud offerings is that data from multiple customers is potentially co-located in one facility—increasing the value of the data stored at the center.” [xvii] Key questions that may need to be answered within the SLA include: • How is data encrypted? • What level of account access is present and how is access controlled? • What level of account access is present and how is access controlled? • Where is the data kept and in what country? • In what (standard) format is the data stored/exported? • How do I access my data or obtain copies of it?	Ohlhorst, F., June16, 2009, “What to Look for in a Cloud Computing SLA,” http://searchcio.techtarget.com.au/news/2240020663/What-to-look-for-in-a-cloud-computing-SLA Torode, C., August 6, 2009, “Beware These Risks of Cloud Computing, from no SLAs to Vendor Lock,” *CIO News.* Goertzel, K. et. al., December 2009, “Cloud Computing for Real,” *FedTech Magazine,* http://www.fedtechmagazine.com/print_friendly.asp?item_id=663.

Table A-6. Roles and Responsibilities

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
Roles and Responsibilities	SLAs will often hold the consumer, not just the provider, accountable for certain actions: • Adhering to any related policies, processes and procedures. • Reporting problems using the problem reporting procedures described in the SLA. • Scheduling in advance all service related requests and other special services with the Service Provider. • Developing and maintaining system related documentation (this could also be a service provider responsibility) • Making customer representative(s) available when resolving a service related incident or request. • Communicating when system testing and/or maintenance may cause problems that could interfere with standard business functions.	Clear delineation of roles and responsibilities has been identified as a significant driver of SLA success. This element of the SLA should describe how the consumer can be a good citizen and maintain credibility with the service provider.	Karten, N., 2003, "Why SLAs Fail and How to Make Yours Succeed." University of Minnesota, 2009, "IT Service Level Agreement–Best Practice," http://www.uservices.umn.edu/pmo/docs/Deploy/BEST_PRACTICE_Service_Level_Agreements.doc Feldman, J., February 2010, "Cloud Contracts and SLAs," *InformationWeek Analytics*, http://analytics.informationweek.com/abstract/5/2274/Cloud-Computing/informed-cio-cloud-contracts-and-slas.html.
Subcontractors and Third-Party Applications	An identified security risk associated with public cloud computing relates to hidden dependencies created by cross-cloud applications. "Hidden dependencies exist in the services supply chain (intra- and extra-cloud dependencies) and the cloud provider architecture does not support continued operation from the cloud when the third parties involved, subcontractors, or the customer company, have been separated from the service provider and vice versa." [xvii] • Customers … should review carefully any sub-contracting provisions in the services agreement." [xix]	Many cloud vendors rely on sub-contracts to expand the breadth of their own clouds. "For example, a vendor providing data storage services may rely on the servers of other cloud vendors, where it is efficient and cost-effective to do so. Similarly, an SaaS offering may be hosted on a platform that is sourced from a third party. Vendors give themselves the flexibility to do this by including broad sub-contracting rights in the services contract and by stating that they 'own or license' the services they are providing. Because third-party sub-contractors may not provide the same quality of service or the same security as the contracting party, a customer could face significant operational and legal issues. In addition, in the event of a dispute, the customer runs the risk that the vendor will seek to transfer liability to the third party–an entity with whom the customer has no privity of contract. Alternatively, the vendor may seek to avoid liability altogether for the conduct of the third party." [xx]	European Network and Information Security Agency, November 2009, "Cloud Computing–Benefits, Risks, and Recommendations for Information Security," http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport Levi, S., et. al., March 2010, "Cloud Computing: Understand the Business and Legal Issues," *Practical Law Company,* http://us.practicallaw.com/8-501-5479.

Table A-7. Payment, Recourse, and Reward

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
Payment, Recourse, and Reward	The SLA should clarify: • When/how payment is to be made • What constitutes excused or excluded performance • Escalation procedures • How service level bonuses and penalties are administered • Remedy circumstances and mechanisms.	The SLA should have negotiated financial penalties when an SLA violation occurs. If there is no repercussion when the provider fails to meet their SLA, the SLA is not as valuable to the consumer. Similarly, the consumer also should be willing to pay a reward for extraordinary service level achievements that deliver real benefits.	Hiles, A., 2000, "Service Level Agreements: Winning a Competitive Edge for Support and Supply Services," Rothstein Associates, Inc., page 113.
When/How Payment is Made	The actual billing cycle should be defined. Currently, cloud service pricing is primarily determined by differentiated levels of service. Pricing also can vary with respect to operating systems and geographical locations. Two emerging cloud computing pricing models include: • Usage-based model (e.g., Amazon EC2) • Subscription-based model (e.g., Google Apps Premier Edition) If different "pay plans" are offered, the SLA should identify which particular plan is in force (e.g., "Pay-as-You-Go," "Prepaid Plan"). The SLA should stipulate if the vendor reserves the right to charge based on different intervals of usage (e.g., hourly versus daily). Reference sometimes will be made to whatever the consumer agreed to on the on-line "customer sign-up." The SLA should identify if there are any distinctions in how/when payment is made for renewals. The SLA also should identify how overages will be handled from a payment perspective. The SLA should describe policies regarding refunds, and clear distinctions should be made between refunds and credits that may be issued because of outages and performance that does not meet the requirements outlined in the SLA.	The vendor will often garner as much flexibility for determining when/how charges will be billed and payments applied. The SLA should answer questions for the Government consumer as they relate to: • When must cancellations be submitted so that additional charges are not incurred? • What is the process to change payment plans? • Are basic services billed/paid differently than optional services (e.g., additional consulting support)? • How/when do I dispute bills? • What are the ramifications of paying bills late? • Can credits be used to pay past bills?	FedCloud, October 1, 2007, "Simple Storage Service," http://fedcloud.com/simple_storage_service.html

Excused/ Excluded Performance	The SLA should address factors that the provider will consider when determining what is within the provider's control (e.g., maintenance) or outside their control (e.g., force majeure clauses).	"Cloud customers must also be careful with how the FORCE MAJEURE clause of the services agreement is drafted. While these clauses typically excuse performance for natural disasters, in many cases they also excuse performance for any event beyond the vendor's control. For example, the Google Apps Premier Online Agreement provides that Google will not be responsible for inadequate performance to the extent caused by a condition beyond Google's reasonable control. Customers should consider whether such a clause provides the vendor with too much leeway to avoid liability in the event the services cannot be delivered. Customers should also should closely review any specific events identified by the vendor in the FORCE MAJEURE clause as being excused. In some cases, the language may be drafted so broadly as to excuse events that are (or should be) within the vendor's reasonable control or for which the vendor should bear the risk. In addition, customers should make sure that performance is excused only when the vendor has tried to implement an approved Business Continuity Plan, but was unable to do so because of the disaster." [xxi]	Levi, S., et. al., March 1020, "Cloud Computing: Understand the Business and Legal Issues," *Practical Law Company,* http://us.practicallaw.com/8-501-5479.
Escalation Procedures	The SLA should identify the process by which issues are raised and resolved (e.g., open a customer support case).	Consumers should pay close attention to following their contractually stipulated obligations to ensure that compensation for failures is not jeopardized. Escalation procedures may vary according to the criticality of the service in question and according to the severity of the issue (e.g., critical, major, minor).	Hiles, A., 2000, "Service Level Agreements: Winning a Competitive Edge for Support and Supply Services," Rothstein Associates, Inc., Annex A.
Service-Level Bonuses/ Penalties	The SLA should: • Document the methodology for measuring performance and calculating penalties and rewards. • Indicate whether consumers will be issued an automatic credit if a failure occurs. • Identify if/how the consumer may get out of the contract if the provider continuously and materially fails to meet the SLA. Some Government agencies overlook the idea that the provider will "manage to the money." For example, in a call center contract, agencies might set a service level of "answer 90 percent of calls within two minutes" without realizing that they are, in effect, telling the provider to ignore any call that has gone over two minutes in favor of one that could still be answered in two minutes.[xxii]	Government consumers should understand if there is anything that will effectively motivate providers to offer even better levels of performance. "SLAs should not be about trying to get money back from suppliers. If a supplier has a problem, it should have a certain time frame … to get back in the client's good graces. That encourages both sides to work toward achievable SLAs that benefit the business." [xxiii]	Delaney, J., 2004, The Outsourcing Revolution, 2004: *Protecting Critical Business Functions.* "IT Outsourcing Contracts FAQ: Establishing SLAs, Flexibility, and More," SearchCIO, TechTarget.com, http://www.russoft.org/docs/?doc=1838, accessed June 30, 2010. Drucker, D., June 26, 2009, "Cloud/SAAS Service Level Agreement Redux," SAAS 2.0, http://intacct.blogspot.com/2009/06/cloud-saas-service-level-agreement.html.

Remedy Circumstances and Mechanisms	The SLA should very specifically identify charge-back approaches (e.g., service credits) or other methods that will be applied to compensate the consumer for unexcused performance failures. It is not uncommon for an SLA to include increasingly stiffer penalties for increasingly extended periods of unavailability and slower response times. The SLA should answer such questions for Government consumers as: • Are charge-backs automatic? • Are remedies provided as a credit or as other compensation? • When will remedies be provided?	The definition of service credits and the supporting process for requesting credits varies across different cloud providers. Given the characteristically "available to the masses" nature of many cloud offerings and the typical lack of flexibility for SLA negotiation, Government agencies should require a clearly communicated schedule of credits and compensations.	Gangadharan, G. R., "Understanding SLAs for Cloud Services," *Cutter IT Journal,* Vol. 22, No. 6/7.

Table A-8. Terms, and Conditions

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
Terms and Conditions	In cloud computing procurements, some of the sub-elements identified below may be provided in the "Terms of Service" or "Terms of Use" documentation rather than being directly incorporated in the SLA.	This SLA element should support a clear understanding of business risk for the cloud computing consumer.	
Statement of Legal Authority and Identification of Governing and Other Applicable Agreements	Often, SLAs will include other documentation that is incorporated into the SLA by reference.	This element of the SLA is used to document the laws and legal codes that allow a provider to offer the services described in the SLA and enter into agreements of this nature with an agency	Financial Management Line of Business, "Migration Planning Guidance, Version 1," http://www.fsio.gov/fsio/download/fmlob/mpgv1/1.2_-_Frequently_Asked_Questions.pdf
Incorporation of Clauses from the Master Agreement	Identifies, by inclusion or by reference, clauses of the Master Agreement important to the SLA.	In instances where the SLA and the master agreement conflict, the master agreement prevails.	Financial Management Line of Business, "Migration Planning Guidance, Version 1," http://www.fsio.gov/fsio/download/fmlob/mpgv1/1.2_-_Frequently_Asked_Questions.pdf
Right to Change/ Renegotiate Terms	SLA should identify if/why/when providers can change terms of the SLA.	Consumers should want these conditions to be very specific so that there are no surprises. A noted driver of SLA weakness/ failure is lack of opportunity within the SLA for the consumer to make changes, as conditions warrant.	Karten, N., 2003, "Why SLAs Fail and How to Make Yours Succeed."
Limitations of Liability	Under these clauses, both the service provider and the service consumer disclaim liability for unforeseeable damages (network errors, hosting server problems) or indirect damages. Limitation of liability clauses often will include a ceiling for monetary liability.	Limitation of liability clauses often will focus on the undesirable results associated with use or inability to use a service; the cost of procuring substitute goods or services; and unauthorized access to or alteration of transmissions or data of consumers. "The vendor's limitation of liability provision is very important in a cloud computing engagement because virtually all aspects of data security are controlled by the vendor. Thus, the vendor should not be allowed to use a limitation of liability clause to unduly limit its exposure. Instead, a fair limitation of liability clause must balance the vendor's concern about unlimited damages with the client's right to have reasonable recourse in the event of a data breach or other incident." [xxiv]	Gangadharan, G.R., 2009, "Understanding SLAs for Cloud Services," *Clutter IT Journal,* Vol. 22, No. 6/7. Cain, C., February 12, 2010, "Basic Understanding Can Clear Fog Surrounding 'Cloud Computing' Agreements," *WTN News,* http://wistechnology.com/articles/7082/.
Indemnification	Indemnification clauses offer providers a means to defend consumers should third parties sue the consumer, alleging that the consumer's use of a service infringes or violates the third party's intellectual property rights. A service provider can indemnify the consumer for intellectual property rights infringement, but only to the extent that those infringement claims arise from the consumer's authorized use of the allowed service. If those claims arise because the consumer combined the allowed service with the consumer's own application/service, or modified or misused the allowed service, then the consumer is required to bear the cost of defending the infringement claims.	"The vendor should agree to defend and indemnify the client from any claim where the vendor breaches its obligations in regards to the confidentiality and security of the client's data. Any intentional breach should be fully indemnified, meaning that the client will have no "out of pocket" costs or expenses related to recovery of the data and compliance with any applicable notice provisions or other obligations required by data privacy laws. The client, not the vendor, should control any notices to its customers necessitated by a breach." [xxv]	Cain, C., February 12, 2010, "Basic Understanding Can Clear Fog Surrounding 'Cloud Computing' Agreements," *WTN News,* http://wistechnology.com/articles/7082/. Gangadharan, G.R., 2009, "Understanding SLAs for Cloud Services," *Clutter IT Journal,* Vol. 22, No. 6/7.

Breach of Service Agreement	The SLA should explain what constitutes breach of the service agreement on the part of the consumer. Once in breach of service, the SLA should also provide instructions for how the consumer can cure the breach.	Consumers should understand what constitutes breach of service as this can materially impact the ability of consumers to be compensated for unachieved performance levels, security incidents, and the consequences of outages and disasters.	ReliaCloud, February 8, 2010, "ReliaCloud SLA," http://www.reliacloud.com/legal/sla/.
Asset Ownership	The SLA should identify who owns and will retain ownership of key assets that will be employed to provide services/capability.	Government consumers should be especially interested if any third parties will own any aspects of assets that are applied for service/capability provisioning.	Booz Allen Hamilton, December 2009, "Cloud Computing Security," http://www.boozallen.com/publications/article/cloud-computing-security
Termination Clauses	SLA should be very specific regarding if/why consumers can terminate, and how much notice is required. Sample termination clauses from various cloud service offerings include: • Providers may suspend/terminate license to use any or all services for any reason or for no reason, at its own discretion at any time. • Providers shall have no obligation to continue to store the users' data during any period of suspension or termination or to permit users to retrieve the same. • Consumers can terminate agreements for any reason or no reason at all, at his/her convenience, by providing a written notice of termination in accordance with a notification period, typically 30 or 60 days.	Key questions that Government consumers should have answered in the SLA include: • Do I own my data if I subscribe to your service? • Will I get my data back if I decide to unsubscribe?	Gangadharan, G.R., 2009, "Understanding SLAs for Cloud Services," *Clutter IT Journal,* Vol. 22, No. 6/7.
Exit Strategy	If you must switch vendors or solutions, is there a smooth exit strategy in which you can recover your data and application code?	It is not uncommon for vendors to offer assistance in migrating away, including agreeing to retain data for a period of time (typically for a fee).	Torode, C., August 6, 2009, "Beware These Risks of Cloud Computing, from no SLAs to Vendor Lock," *CIO News.*

Table A-9. Reporting Guidelines and Requirements

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
Reporting Guidelines and Requirements	SLAs should identify agreements regarding access to provider performance logs and reports, and performance and status reporting that will be provided.	Performance monitoring is an essential step in avoiding disagreements about who is responsible for performance failures.[xxvi]	Parera, D., April 21, 2008, "Put SOA to the Test," *FCW.com.*
Access to Provider Performance and Audit Logs	The vendor should maintain an accessible website with continuous updates as to how the vendor is performing against their SLA, and how they should publish their SLA and their privacy policies. The best cloud vendors realize that their excellence in operations and their SLAs are real selling points.	"Although most cloud providers will record access to the system in specified log files, gaining access to audit logs can be a difficult process. In some instances, the cloud provider's logs may be insufficient for a particular agency's needs… Auditing becomes another crucial factor in assessing the agency's true needs and being able to meet ever-changing demands in service. Instead of accepting what the … provider sends the organization at the end of the month as a bill, an organization should understand that cloud computing is complex enough that a reasonable set of runtime information must be made available to substantiate the provider's claim for compensation. This point is particularly true in developing an SLA. If the agency's infrastructure is regularly adjusting to meet demands, it is essential to be able to verify that the infrastructure is reacting the way that was contracted …SLAs with providers should explicitly state that real-time auditing or logging (for accountability) will be performed and resulting reports will be made accessible. A tailored audit can provide the agency a clear understanding of where responsibilities lie." [xxvii]	Booz Allen Hamilton, December 2009, "Cloud Computing Security," http://www.boozallen.com/publications/article/cloud-computing-security Drucker, D., June 26, 2009, "Cloud/SAAS Service Level Agreement Redux," SAAS 2.0, http://intacct.blogspot.com/2009/06/cloud-saas-service-level-agreement.html Goertzel, K., et. al., December 2009, "Cloud Computing for Real," *FedTech Magazine,* http://www.fedtechmagazine.com/print_friendly.asp?item_id=663
Required Performance Reports	SLAs should identify if/how the vendor will report performance to consumers and regulators.	SLA performance reports should illustrate how a service provider is performing against their agreed-to service levels.	Apparent Networks, "Pathview and AppCritical for SLA Management and Compliance Ensure SLA Compliance for Higher Performance: Overview," http://www.apparentnetworks.com/solutions/by-it-initiative/sla-validation.aspx
Regulatory Compliance Responsibility	The SLA may identify if/how the vendor's offering complies with key regulations that are relevant to the consumer, including FISMA, HIPAA, and SOX reporting.	The SLA should answer such questions for Government consumers as: • Does the vendor undertake an SAS70 Type II Audit (a caution is that some vendors may overstate what this audit means–it does not certify that a system is secure)? • Does the vendor undergo annual third party security and penetration testing? Is the vendor Payment Card Industry (PCI) compliant?	Torode, C., August 6, 2009, "Beware These Risks of Cloud Computing, from no SLAs to Vendor Lock," *CIO News.*

Table A-10. Service Management

SLA Element	Desired Features and Potential “Gotchas”	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
Service Management	The SLA may describe how (e.g., tools applied) the provider will manage overall service delivery for vendors. For example, the SLA may indicate the application of ITIL standards/processes.	Be able to account for assets in the cloud, get performance feedback for cloud-deployed assets. How automated is this, how much does the sponsor do vice the provider.	Torode, C., August 6, 2009, “Beware These Risks of Cloud Computing, from no SLAs to Vendor Lock,” *CIO News.*

Table A-11. Definitions/Glossary of Terms

SLA Element	Desired Features and Potential “Gotchas”	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
Definitions/ Glossary of Terms	Include definitions of fees and aspects of service that are within the scope of the SLA.	“An effective SLA should include an unambiguous description of terminology and a concise definition of all the services provided. Clarity is paramount–you need to understand what the reports generated say. A very common problem with SLAs is a lack of agreement on the terminology and service definitions. More often than not, SLAs comprise of arcane service definitions and/or merely list the services bought and paid for, with no guarantees for quality of service.” [xviii]	Dimension Data, November 2009, “Is Your SLA Your Weakest Link?” p. 7, http://www.dimensiondata.com/Lists/Downloadable%20Content/IsYourSLAYourWeakestLinkOpinionPiece_129088975412137750.pdf

Appendix B—Service-Level Agreement (SLA) Examples Relevant for Cloud Computing

Title/Description (alphabetic)	**Example SLA Elements for Consideration**	**URL/Link**
Amazon Elastic Compute Cloud (EC2) SLA	A cloud computing SLA, with an example approach for describing **excused/excluded** performance	http://aws.amazon.com/ec2-sla/
Apps.Gov	A model Terms of Service (TOS) agreement, with an example approach for describing **limitations of liability** and **regulatory compliance responsibility**	https://forum.webcontent.gov/resource/resmgr/model_amendment_to_tos_for_g.pdf
Department of Health and Human Services (HHS) EPIC SLA/MOU Template, Version 1.0	An SLA template, with an example approach for introducing the SLA **purpose/background**	http://www.hhs.gov/ocio/eplc/EPLC%20Archive%20Documents/50-SLA%20and%20MOU/eplc_sla_mou_template.doc
Defense Information Systems Agency (DISA) Catalog of Services	A directory of services, with an example approach for differentiating **optional services** from basic services (performance levels and rates)	http://www.disa.mil/computing/documents/CatalogOfServices.pdf
FedCloud Amazon Simple Storage Service (S3) SLA	A cloud computing SLA, with an example approach for describing service credits and **when/how payment is to be made**	http://fedcloud.com/simple_storage_service.html
FedCloud Amazon Simple Storage Service (S3) SLA	A cloud computing SLA, with an example approach for describing **excused/excluded** performance	http://aws.amazon.com/s3-sla/
Georgetown University McDonough School of Business (MSB) SLA	An SLA, with an example approach describing provider **problem resolution** commitments	http://technology.msb.edu/useful_info/sla.pdf
GoGrid Cloud Hosting SLA	A cloud computing SLA, with an example approach for describing performance metrics	http://www.gogrid.com/legal/sla.php
nCircle's 24 Hour SLA, nCircle Network Security	An SLA, with an example vendor commitment to **vulnerability management** and vendor-offered compensation for SLA breaches	http://www.ncircle.com/pdf/resources/nCircle_24hr_SLA.pdf
Pathview and appCritical SLA Violation Reporting	An SLA, with an example approach for reporting **required performance**	http://www.apparentnetworks.com/Resources/Reports.aspx
Rackspace Cloud Acceptable Use Policy (AUP)	An SLA, with an example approach for describing **breach of service agreement** by the consumer.	http://www.rackspacecloud.com/legal/aup
ReliaCloud SLA and Terms of Service	A cloud computing SLA, with an example approach for describing **breach of service agreement** by the consumer	http://www.reliacloud.com/legal/tos/
VeriSign—SLA.	An SLA, with an example approach for defining key terms related to **continuity** and planned/unplanned outages	http://www.verisign.com/static/002488.pdf
Web Service-Level Agreement (WSLA) Language Specification	A Web services SLA template, which provides an example approach for **service descriptions, performance metrics,** and **measurement methodology**	http://www.research.ibm.com/wsla/WSLASpecV1-20030128.pdf

Appendix C—Example usage of SLA Guide

As an example usage of the SLA comparison guide, assume that a Federal Government organization has decided that continuing to host all of its datacenter capabilities internally is inefficient and diverts too many resources from achievement of the organization's core mission. The organization employs a business case analysis and is evaluating various options for externally hosting capabilities. Through a structured systems engineering process, the organization identifies specific requirements across categories such as performance, scalability, and security. They identify several community and public cloud computing offerings that may meet their needs. For this particular organization, data ownership and access is of critical concern. In addition, the cost of datacenter storage and functionality is a priority interest because the current in-house capability involves investment in, and maintenance of, considerable excess capacity that is rarely applied. The organization also is concerned about penalties associated with contract modification or early termination, should the organization later decide that a selected cloud offering does not fully meet its requirements. From the SLA comparison guide (refer to Table 2-1) and the companion description of guide sub-components (refer to Appendix A), the Government organization should be able to readily identify specific candidate provider SLA elements and sub-elements that deserve in-depth review and comparison across candidate provider SLAs, based on the priority concerns and needs described above. In this example, some of the key SLA elements include:

SLA Context/Overview (stakeholder description)— For example, the guide identifies that it is common for cloud computing SLAs to identify other consumers that are accessing the same services and applying the same cloud assets. If this type of description is available within offered SLAs, it can help address the organization's questions regarding which other enterprises will be accessing datacenter services and storing data within the same virtual environment.

Security Management (data ownership, protection, and control description)—For example, the guide makes it clear that data storage details, vendor obligations regarding data access, and data ownership should be fully described within any SLA offering.

Roles and Responsibilities—To ensure that there are no surprises for the Government organization when datacenter service issues arise and the consumer anticipates some form of compensation or remedy, the organization should carefully review typical expectations as described within the comparison guide regarding the responsibilities of the consuming Government organization as a good virtual datacenter citizen.

Payment, Recourse, and Reward—The SLA comparison guide identifies what the Government organization can expect regarding the degree of pricing and payment provided within typical SLAs. The guide highlights common methods that vendors will apply within their SLAs to describe potential penalties associated with contract modification/termination; this will be important for this Government organization as it wants to pilot a cloud offering on a trial basis.

Terms and Conditions

- The SLA comparison guide identifies rights to change/renegotiate terms and what the Government organization should expect from an SLA in terms of describing options for modifying procurements or early termination.
- In this hypothetical example, it could be possible that a candidate vendor SLA excessively limits vendor liability as it relates to a data breach. The guide can be a useful aid in understanding the reasonableness of such limitation.

Reporting Guidelines and Requirements—Since this Government organization is interested in performance requirements, the guide's descriptions of reporting responsibilities should be useful in determining the types of statistical performance information that will be made available by the vendor and when that data will be available. The guide offers some description to support an understanding of typical performance information that should be shared by the vendor.

By applying the guide as a comparison when reviewing available SLAs, the Government organization is able to gauge the relative degree of comprehensiveness and rigor applied by candidate providers in their SLAs better. Because the guide incorporates a synthesized assessment across a broad spectrum of actual SLAs, including best practices and lessons learned, a Government organization is able to focus more attention on those aspects of procurement that are of priority concern. Based on this organization's comparison of several offered SLAs to the comparison guide, gaps between what can/should be expected and what is offered may be identified. Application of the guide can assist Government consumers to eliminate some vendor offerings based on the magnitude and criticality of those gaps. For a down-selected list of candidates, the results of comparison can support the Government organization in determining whether there are particular gaps that should be discussed, and possibly negotiated, with the vendor.

References

[1] Mell, P. and T. Grance, October 7, 2009, “The NIST Definition of Cloud Computing,” http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

[2] Mell, P. and T. Grance, June 26, 2009, *Effectively and Securely Using the Cloud Computing Paradigm, NIST, Information Technology Laboratory.*

[3] Ibid, p. 3.

[4] U.S. Security and Exchange Commission, Spotlight on Sarbanes-Oxley Rulemaking and Reports, http://www.sec.gov/spotlight/sarbanes-oxley.htm, accessed June 21, 2010.

[5] https://www.acquisition.gov/far/05-13/html/Subpart%2013_3.html

[6] Feldman, J., February 2010, “Cloud Contracts and SLAs,” *Information Week Analytics.*

[7] U.S. General Services Administration’s Financial Systems Integration Office (FSIO), September 15, 2006, “Financial Management Line of Business Migration Planning Guidance, Version 1.0,” http://www.gsa.gov/portal/content/102256

[8] U.S. General Services Administration’s Financial Systems Integration Office (FSIO), September 15, 2006, “Financial Management Line of Business Migration Planning Guidance, Version 1.0,” http://www.gsa.gov/portal/content/102256

[9] Ohlhorst, F., June 16, 2009, “What to Look for in a Cloud Computing SLA” http://searchcio.techtarget.com.au/news/2240020663/What-to-look-for-in-a-cloud-computing-SLA

[10] Gangadharan, G. R., June 1, 2010, “Understanding SLAs for Cloud Services,” *Cutter IT Journal,* Vol. 22, No. 6/7, p. 51.

[11] Booz/Allen/Hamilton, 2009, “Cloud Computing Security: Government Acquisition Considerations for the Cloud Computing Environment,” p. 5, http://www.boozallen.com/media/file/Cloud-Computing-Security-Acquisition-Considerations.pdf.

[12] March 2010, “Don’t Look Down: The Path is Missing a Few Steps,” *GCN,* http://gcn.com/Articles/2010/03/15/Cloud-Computing-Missing-Steps.aspx?Page=6.

[13] “Service Level Agreements,” *IT-Tude.com,* http://www.it-tude.com/sla-article.html, accessed June 30, 2010.

[14] Ohlhorst, F., July 14, 2009, “Assessing Cloud Providers,” *ZDNet UK,* http://www.zdnet.co.uk/reviews/saas/2009/07/14/assessing-cloud-providers-39681045/.

[15] “Ensuring High Service Levels in Cloud Computing,” *Nimsoft,* http://www.nimsoft.com/whitepapers/downloads/Nimsoft-cloud-service-levels.pdf, accessed June 30, 2010.

[16] Hall, G., July 16, 2009, “Cloud Computing and ITIL: Service Delivery and Cloud SLAs,” *Cloud Storage Strategy,* http://cloudstoragestrategy.com/2009/07/cloud-computing-and-itil-measuring-the-quality-of-service-delivery.html.

Table References

[i] Delaney, J., 2004, *The Outsourcing Revolution, 2004: Protecting Critical Business Functions.*

[ii] Ibid.

[iii] Anderson, B., "Structuring Meaningful SLAs for IT Support,"
http://www.itmpi.org/assets/base/images/itmpi/StructuringMeaningfulSLAsforITSupportV5.pdf.

[iv] Perera, D., April 21, 2008, "Put SOA to the Test," *FCW.com.*

[v] Dimension Data, November 2009, "Is Your SLA Your Weakest Link?" p. 7,
http://www.dimensiondata.com/Lists/Downloadable%20Content/IsYourSLAYourWeakestLinkOpinionPiece_129088975412137750.pdf.

[vi] Delaney, J., 2004, *The Outsourcing Revolution, 2004: Protecting Critical Business Functions.*

[vii] Ibid.

[viii] Anderson, B., "Structuring Meaningful SLAs for IT Support,"
http://www.itmpi.org/assets/base/images/itmpi/StructuringMeaningfulSLAsforITSupportV5.pdf.

[ix] Shafer, P., "How SLAs drive, and don't drive, performance: strategic, technical and process limitations,"
http://www.iaccm.com/contractingexcellence.php?storyid=514, accessed June 23, 2010.

[x] Hoover, J.N., October 30, 2008, "Will Microsoft Shake Up Cloud Computing SLAs?" *InformationWeek,*
http://www.informationweek.com/cloud-computing/blog/archives/2008/10/will_microsoft_2.html.

[xi] Cain, C., February 12, 2010, "Basic Understanding Can Clear Fog Surrounding 'Cloud Computing' Agreements," *WTN News*,
http://wistechnology.com/articles/7082/

[xii] Nolle, T., May 22, 2009, "Meeting Performance Standards and SLAs in the Clouds,"
http://searchcloudcomputing.techtarget.com/tip/0,289483,sid201_gci1357087,00.html.

[xiii] Goertzel, K. et. al., December 2009, "Cloud Computing for Real," *FedTech Magazine,*
http://www.fedtechmagazine.com/print_friendly.asp?item_id=663.

[xiv] Ibid.

[xv] Ibid.

[xvi] Ibid.

[xvii] Ibid

[xviii] European Network and Information Security Agency, November 2009, "Cloud Computing–Benefits, Risks, and Recommendations for Information Security,"
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.

[xix] Levi, S., et. al., March 2010, "Cloud Computing: Understand the Business and Legal Issues," *Practical Law Company,*
http://www.skadden.com/content/Publications/Publications2008_0.pdf .

[xx] Ibid.

[xxi] Ibid.

[xxii] Delaney, J., 2004, *The Outsourcing Revolution, 2004: Protecting Critical Business Functions.*

[xxiv] "IT Outsourcing Contracts FAQ: Establishing SLAs, Flexibility, and More," *SearchCIO, TechTarget.com,*
http://www.russoft.org/docs/?doc=1838, accessed June 30, 2010.

[xxv] Cain, C., February 12, 2010, "Basic Understanding Can Clear Fog Surrounding 'Cloud Computing' Agreements," *WTN News*,
http://wistechnology.com/articles/7082/

[xxv] Ibid.

[xxvi] Perera, D., April 21, 2008, "Put SOA to the Test," *FCW.com.*

[xxvii] Goertzel, K. et. al., December 2009, "Cloud Computing for Real," *FedTech Magazine,*
http://www.fedtechmagazine.com/print_friendly.asp?item_id=663.

[xxviii] Dimension Data, November 2009, "Is Your SLA Your Weakest Link?" p. 7,
http://www.dimensiondata.com/Lists/Downloadable%20Content/IsYourSLAYourWeakestLinkOpinionPiece_129088975412137750.pdf

MITRE

www.mitre.org

MITRE
www.mitre.org