MITRE

Cloud SLA Considerations for the Government Consumer

Update to 2010 MITRE Paper, *Cloud Service Level Agreement Considerations for Government Consumers*

Approved for Public Release
Case Number 15-2504

Kevin Buck, Diane Hanf, and Daniel Harper

July 2015

Table of Contents

Figures and Tables

1 BACKGROUND

"Cloud SLA Considerations for the Government Consumer", published as part of MITRE's Systems Engineering Cloud Computing Series in 2010 by Kevin Buck and Diane Hanf, explored the role of Service Level Agreements (SLAs) in managing performance of government procurements through Public Clouds. Some of the findings from this exploration were also relevant for Community and Private Clouds. Based on recent interest in this report from the Office of Information Management Issues at the U.S. Government Accountability Office (GAO), the MITRE team is updating the analyses and recommendations based on investigations of the latest trends in Cloud SLA management within the federal government. This update includes a canvassing of the latest published literature and the results of a technical information exchange with over 50 MITRE representatives supporting federal government sponsors with Cloud implementations.

2 THE CLOUD ENVIRONMENT FOR FEDERAL GOVERNMENT TODAY

"The Cloud" typically includes services and actors who form a complex and dynamic Cloud ecosystem, which can involve multiple business arrangements and technical frameworks. These arrangements may result in aggregating SLAs across different services and their related metrics and Key Performance Indicators (KPIs) at both a single service level as well as at composite and aggregated levels.[1] Typical Cloud **deployment** models include Public, Private, Community, and Hybrid. As illustrated in Figure 2-1 below, typical Cloud **service** models include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

NIST Cloud Reference Architecture, 2014[2]

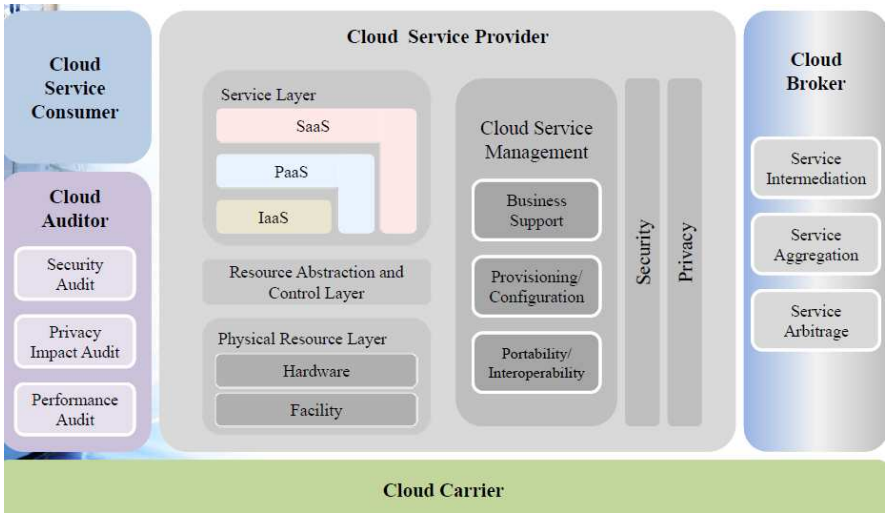


Figure 2-1. NIST Cloud Reference Architecture, 2014

General categories of Cloud actors include the Cloud Service Customer (user, administrator, business manager, and integrator), the Cloud Service Provider (operations manager, deployment manager, administrator,

[1] *"Enabling End-to-End Cloud SLA Management", Frameworx Best Practice, October 2014, TMForum.*
[2] *"CLOUD SERVICE LEVEL AGREEMENTS - Meeting Customer and Provider needs", Eric Simmon, NIST, January 2014*

business manager, customer support & care representative, inter-Cloud provider, security and risk manager, and network provider), and the Cloud Service Partner (developer, auditor, and broker).[3]

Due to the Cloud First policy of 2010, the federal government continues to increasingly adopt Cloud solutions despite some significant challenges.[4] Public sector spending on the Cloud is up by approximately 70% since 2012. Yet, misconceptions regarding security, data and allowable business practices when using Cloud services persist. In many cases, federal government agencies should not necessarily assume that Private Cloud is the only solution; Public and Hybrid Clouds can be viable and potentially lower cost options.

Perceived challenges in adopting Cloud strategies relate to cost, performance engineering, monitoring, security, and data ownership. The engineering problem space changes from specifying a solution to applying components that were designed for different clients and circumstances, with complex stakeholder relationships and no absolute guarantees. In many instances, the government consumer should conduct tradeoff analyses to assess operational suitability vs cost (savings). In adopting Cloud, many aspects of the consumer organization may be impacted, from culture and organizational change management to acquisition, engineering, and operations management. With many alternative IT solutions available today, the federal government must apply due diligence in knowing the vendor community, embracing the new capabilities, and understanding how to best apply these capabilities.

Many Chief Information Officers (CIOs) are reluctant to move IT workloads to the Cloud, in part because of persistent concerns about the security of the data in a hosted environment, as well as the geographic question of where the data will be stored. Data ownership clauses in contracts and termination conditions in SLAs remain top concerns for government Cloud buyers. Since the government is typically risk averse, it should expect explicit declarations of data ownership rights to confirm that data will not be lost when the service from a particular vendor is terminated.

The current Cloud ecosystem can be quite complex, especially when consumers obtain multiple Cloud services individually from different providers. This complexity can significantly increase the challenges associated with end-to-end SLA management. To reduce this complexity, some government entities seek to obtain a suite of Cloud services/capabilities from one vendor as a single ecosystem, which simplifies stakeholder interactions, performance monitoring and billing.

[3] *Cloud Standards Customer Council, April 2015. "Practical Guide to Cloud Service Agreements, v2.0".*

[4] *"Federal CIOs want SLA assurances from Cloud vendors", April 2015, CIO.com.*

3 CLOUD SERVICE MODELS FOR THE GOVERNMENT CONSUMER

Clouds that are available for the government consumer include Private Cloud, Shared Community Cloud, Public Cloud, and Hybrid Cloud. In 2010 service models included Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). While these models persist in 2015, there are some additional considerations impacting Cloud usage as practice and technology have matured.

3.1 PUBLIC / COMMUNITY CLOUDS

Public and Community Cloud providers typically provide packaged service offerings with predetermined SLAs. With such offerings, there is limited flexibility for the government to negotiate specific SLAs. The Cloud providers may allow the government to have certain desired features or performance levels – but at a premium price. The risks that the government will not obtain required service quality that meets mission expectations are considerable. The terms and conditions are often lengthy and increase this risk. A change in practice for the government might entail an engineering approach where the consumer focuses on technical-legal discussions to understand and get clarifications on the Cloud offerings and then designing to it rather than trying to drive SLAs that will increase costs.

As an example, if an agency wants to replicate data by running databases in the Cloud, but does not deliberately design a scheme to replicate among regions, one may erroneously think that a “green” rating means there is sufficient required availability. However, availability is insufficient if the Cloud capability had been designed within one region and that particular region fails. This is usually not what Cloud consumers expect when data is replicated. The Cloud vendor may not accept responsibility for this form of performance issue, claiming that the application was not designed correctly, i.e. data not replicated in different regions. Additionally, some Public IaaS offerings are limited in flexibility and may not immediately flex with demand. In light of prevailing data center practices, storage usage may still need to be monitored as a best performance management practice to ensure demand does not exceed capacity.

These examples show the government needs a deep technical understanding of the Cloud structure to effectively design for failover, since it is not necessarily an automatic feature in Cloud environments. A more defined best practice is needed for addressing failover and other performance needs, using Public Cloud SLAs as an input rather than trying to append to them to become an enforcement mechanism.

The IT function for the federal government in Cloud shifts from total control to managing and overseeing Cloud offerings. While staff may not lose their jobs, the reality is often a repurposing of positions from more technical to more managerial. The IT function now focuses on handling complex SLA relationships, and a MITRE recommended best practice is to stand up a forum to educate and shape the broader stakeholder community’s Cloud expectations and foster clear understanding of culture, roles and responsibilities, and cost versus control tradeoffs. A key performance management aspect that should be addressed is the development of methods to improve overall efficiencies while transitioning to Cloud-based solutions, and potentially planning for an expanded user base. A crucial part of such a discussion is how an organization plans and designs for continuous operations.

3.2 PRIVATE CLOUDS

Private Cloud solutions are more customizable and typically offer a greater degree of negotiable performance requirements as compared to the public/community Clouds. There are two scenarios for the Private Cloud: (1) The government IT department as the Private Cloud provider and manager (in-house) and (2) An outsourcing situation where a contractor provides and manages the Private Cloud. In either case, the government Cloud Manager should take the lead to identify business requirements for IT service performance and coordinate with the government IT technical lead and the Private Cloud provider (either in-house or external) to define the relevant performance metrics.

Since Private Cloud adoption is driven by the need for significant accountability across contributing IT components, there have been some instances of fee-based Private Clouds owned and operated by a federal entity. If the government Cloud Service Provider (CSP) does not meet expectations, it is certainly possible for funds to be returned; however, this may not be nearly as important as the impact of mission failure. What recourse does one government agency have when another government Cloud provider does not perform? While there can be monetary penalties considered, a $10K punishment is pretty meaningless if it then takes millions of dollars to fix the ensuing issues. While the course of action to implement depends upon whether the consumer seeks to punish or to fix, Government-to-Government SLA recourse is still limited with this type of Cloud offering.

3.3 HYBRID CLOUDS

Hybrid Clouds, which are an integrated offering of public and Private Clouds targeted at performing functions within an organization, must address the challenges presented in Public/Community Clouds, Private Clouds, and traditional non-Cloud services. In addition, hybrid Cloud SLAs must be unusually vigilant in articulating the potential conflicts and interdependencies in service quality levels across elements in different Cloud service models. For example, an IaaS SLA acquired in the Public Cloud that supports a SaaS provisioned in the government Private Cloud must be sufficient to meet the overall SaaS performance requirements.

4 A SURVEY OF CLOUD SERVICE AGREEMENT STRUCTURE AND CONTENT

The National Institute of Standards and Technology (NIST), International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) and the Cloud Standards Customer Council (CSCC) have recently produced guidance on SLA structure and content. The lexicon for structuring Cloud service provisioning agreements continues to evolve from the 2010 publication of the MITRE SLA Considerations paper, and the following description of approaches recommended by these organizations exposes the reader to several perspectives on Cloud agreement structure. Based on these recent developments, the SLA model contained in the 2010 MITRE publication has been extended to include considerations from Cloud standards bodies, councils, industry fora, practitioners and academia.

4.1 NIST

NIST lays out a general SLA framework: [5]

- **Master Service Agreement**

[5] *Simmon, E. (NIST), 28 Jan2014. "Cloud Service Level Agreements: Meeting Customer and Provider Needs".*

- Top level legal agreement between provider and customer covering general aspects.

- **Service Agreement**
  - *Generally, the service agreement is a legal document specifying the rules of the legal contract between a consumer and provider* (NIST SP 800-146)
- **Service Level Agreement**
  - Lower level agreement covering the performance aspects of a service, where a Cloud SLA is *"A document stating the technical performance promises made by the Cloud provider, how disputes are to be discovered and handled, and any remedies for performance failures.*" (NIST SP 800-146)

In the NIST *Cloud Computing Synopsis and Recommendations* Special Publication, the intent of the service agreements and service level agreements documents are combined and referred to as a Service Agreement. In this agreement framework, service agreements consist of three basic parts:

(1) A collection of promises made to the consumers about availability, remedies for failure to perform, data preservation and legal care of consumer information

(2) A collection of promises not made to the consumer, i.e., limitations about scheduled outages, force majeure events, service agreement changes, security, and service API changes

(3) A set of obligations that consumers must accept on acceptable use policies, licensed software, and timely payments

The recommendations offered by NIST to prospective Cloud adopters are integrated into Table 10-1 *Cloud Service Level Agreement Guide Overview*. NIST encourages consumers to discuss modifications to service agreements with the vendor if the terms of default do not address all of the consumer needs and to be aware that an agreement may specify that it can change its service level with advance notice. NIST cautions consumers to be ready to migrate workloads to alternate providers if service agreement changes are unacceptable.

4.2 ISO/IEC 17789:2014

ISO/IEC defines a **Cloud Computing Service Level Agreement** (Cloud **SLA**) as *a **Service Level Agreement** between a **Cloud Service Provider** and a **Cloud Service Customer** based on a taxonomy of **Cloud Computing** specific terms to set the quality of the Cloud services delivered.*

Cloud SLAs have business and technical properties and cover terms regarding the quality of service, security, performance and remedies for failures to meet the terms of the **SLA**. A **Cloud Service Provider** can also list within the Cloud **SLA** a set of promises explicitly not made to **Cloud service customers**, i.e., limitations, and obligations that **Cloud Service Customers** need to accept. This is a viewpoint shared by NIST.

ISO/IEC also acknowledges that the term *service agreement*, also known as a Master Service Agreement (MSA), Terms of Service (ToS), Terms and Conditions (T&C), or simply "the contract", is the higher order document in agreements between parties, and the **SLA** is subservient.

4.3 The Cloud Standards Customer Council

The CSCC has defined a Cloud Service Agreement (CSA) as having three major aspects—a customer agreement, an acceptable use policy (AUP) and a SLA. The customer agreement describes the overall relationship between the customer and the provider; the AUP prohibits activities that providers consider to be illegal or inappropriate; and the SLA describes the levels of technical performance, i.e., availability, serviceability or performance associated with the service. Note in this paper the terms SLA and CSA are used interchangeably.

4.4 MITRE Cloud Service Agreements Content

There are several prevalent themes in Cloud agreements:

- Overall relationships and context must be established between the consumer and provider,
- The levels of service must be described and established, and it should be understood what is offered and the limits to what is offered,
- It must be clearly understood what is acceptable use of the service, and
- It must be clearly understood what the customer must provide in return for the service.

The NIST, ISO/IEC and CSCC structures emerged after the MITRE 2010 paper was written. The MITRE 2010 paper contained an agreement organizational construct in which the major topics of an agreement between the provider and the consumer were called *elements* of the SLA, and it covered contextual, service level, acceptable usage, limitations, rights and obligations information. The 2010 agreement structure further decomposed one level deeper to include *sub-elements*. Since 2010, some *sub-elements* (*asterisked) emerged as major topics in today's Cloud adoption and now appear in the 2015 structure as top level *elements*. The top level *elements* and *sub-elements in the 2015 agreement structure are shown in the Agreement Elements and Sub-elements* table. We continue with this structure to provide continuity in applying both originally identified, as well as additionally identified, considerations for Cloud agreements since 2010.

Table 4-1 Agreement Elements and Sub-Elements

Element	Sub-Element
SLA Context/Overview	Provider and Consumer Contact Information
	Purpose Background
	Scope
	Stakeholders
***Business Policies**	Planned Maintenance
	Regulatory Compliance Responsibility
Service Descriptions	Business Level 103904 Objectives
	Service Level Objectives
	Service Interdependencies
	Customer Service Offered
	Optional Features
Metrics and Key Performance Indicators	Levels of Service Available
	Performance Metrics
	Quality Assurance, Performance Data Requirements
	Measurement Methods
	Service Level Improvement
Continuity or Outages	Incident Response and Reporting
	Disaster Recovery and Service Failure Management
	Outage Resolution
	Continuity-Related Definitions
Security and Risk Management	Vendor Security Controls
	Privacy Guarantees
	Vendor Position Regarding Customer-Requested External Security

Element	Sub-Element
	Controls
	Vulnerability and Consequence Assessment and Management
	Risk and Issue Resolution
	Data Ownership, Protection and Control
Roles and Responsibilities	Stakeholders' Roles and Responsibilities
	Subcontractors and Third-Party Application
Payment Recourse and Reward	When/How Payment Is To Be Made
	Excused/Excluded Performance
	Escalation Procedures
	Service Level Bonuses/Penalties
	Remedy Circumstance And Mechanisms
Terms and Conditions	Statement of Legal Authority And Identification of Governing And Other Applicable Agreements
	Incorporation of Clauses from The Master Agreement
	Right to Change/Renegotiate Terms
	Limitations of Liability
	Indemnification
	Breach of Service Agreement
	Asset Ownership
	Termination Clauses
Exit Strategy and Process	Exit Strategy and Process
Reporting Guidelines and Requirements	Access to Provider
	Performance and Audit Logs
	Required Performance Reports
	SLA Documentation
Service Management	Service Management
Definitions/Glossary of Terms	Definitions/Glossary Of Terms

This structure is the framework used in the rest of the paper to discuss best practice considerations and should be used as a guide to ensure that all aspects of the agreement are understood by the government consumer.

5 GOVERNMENT FLEXIBILITY TO DEVELOP AND NEGOTIATE SLAS

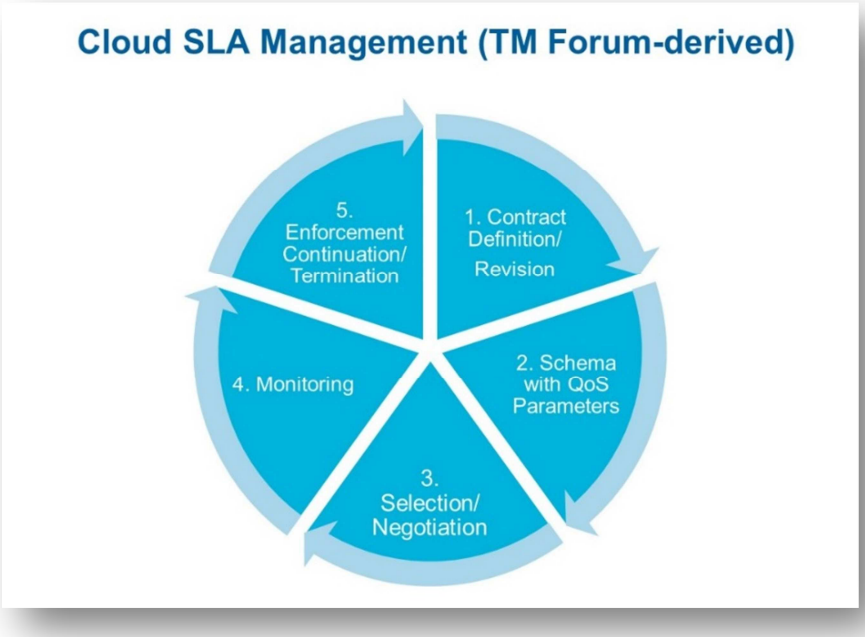
Various Cloud deployment models imply differing degrees of SLA customizability between the agency and the Cloud providers. Many commercial Cloud SLAs emphasize limiting the vendors' liability and exposure to risk. For government organizations making Cloud procurement decisions, the potentially limited opportunity to negotiate terms/conditions and the premiums paid for additional flexibility should be factored into procurement decisions. In many instances, vendors are defining SLA structure, elements, and performance levels. Government consumers should scrutinize SLAs under three lenses: data protection, continuity, and costs. They should pay close attention to whether ultimate goals will be achieved, and carefully weigh how important it is that specific approaches (e.g., use of specific monitoring software) are applied to achieve those goals.

According to the *Practical Guide to Cloud SLAs* written by the CSCC[6], the larger the customer deployment, the more power customers exert in negotiating stringent SLAs and the higher the subscription and upfront fees. Even in the case of SaaS acquisitions, large customers are successful in negotiating a stronger agreement. According to IBM in *Best Practices to Develop SLAs for Cloud Computing*, *"an SLA is not a one-way solution. One party — the Cloud service provider, for example — should not impose decisions about how things should be done, particularly when the other party — the Cloud service customer, for example — has different expectations about how the SLA should be formulated."*

The government is not a commercial operation, and does not view liabilities and penalties or recourse the same way; this drives some key distinctions in how service levels must be effectively negotiated. There are limitations to the amounts of money that can be demanded as recourse in cases of service provisioning degradation or failure even though the ultimate impact of this degradation or failure may be quite significant (e.g. failure to effectively launch a defensive strike against an enemy combatant). The government must establish trusted partnerships with its contractors so there is shared understanding and balanced distribution of risk and responsibility. The success of federal government Cloud procurement negotiations hinges on the consumer truly understanding and effectively communicating ultimate objectives from Cloud providers and capturing those in the SLA.

6 THE IMPORTANCE OF SLAs TO MANAGE PERFORMANCE

SLA Management is emerging as an area of significant complexity. As shown in Figure 6-1, which was derived from the TM Forum's description of Cloud SLA Management, SLA management involves defining or refining the contract, determining what the quality of service needs to be to support mission needs, selecting or negotiating with a provider, monitoring SLA performance and enforcing, continuing or terminating the



[6] *This council is a Cloud end-user advocacy group that focuses on the standards, security and integration issues associated with Cloud adoption.*

contract.

Figure 6-1. Cloud SLA Management

According to the *Practical Guide to Cloud SLAs*, the challenge of correlating metrics to higher-level functional guarantees is most significant for SaaS, which offers applications at higher levels of functionality. A vast majority of SaaS and PaaS providers simply offer no SLAs. The situation for IaaS is better than SaaS and PaaS, but most Public Cloud infrastructure services are available only through non-negotiable standard contracts. These SLAs strictly limit the provider's liability and the remedies do not provide significant benefit to consumers in case of service disruptions. Furthermore, most IaaS providers put the burden of SLA violation notification and credit request on their customers. Since a vast majority of the users of IaaS Public Clouds are small and medium businesses, the pressure on Cloud providers to offer stringent SLAs is minimal. SLAs provided by Cloud vendors are increasingly viewed by consumers as insufficient protection and skewed in favor of the provider.

ISO/IEC 17789 defines Cloud governance as the system by which the provision and use of Cloud services are directed and controlled:

> "The individual governance practices used by Cloud service customers and CSPs exist on a continuum from simple to sophisticated and are encapsulated within their role. It is the responsibility of each role to implement governance according to their needs."

Cloud governance is cited as a cross-cutting aspect because of the requirement for transparency and the need to rationalize governance practices with SLAs and other contractual elements of the Cloud service customer to CSP relationship.

> "The term external Cloud governance is used for some form of agreement between the Cloud service customer and the CSP concerning the use of Cloud services by customer. The agreement can make reference to a SLA which provides detailed information about functional and non-functional aspects of the services."

ISO/IEC cautions that depending on the charging model, the ability of the Cloud service to scale its use of resources in accordance with the terms of the SLA can also be an important facet of performance. They recommend that performance should have metrics defined in the SLA for each performance condition identified, and that these metrics should be monitored during operation of the Cloud service to ensure that the service meets the performance terms of the SLA.[7]

MITRE has established a community to focus on service management challenges in the Cloud.[8] Based on the widely-advertised benefits of Cloud Computing, Service Level Management (SLM) SLA assertions must provide a process for discussing, documenting, and agreeing upon expectations. The fact that underlying IT service components in the Cloud may not be visible or manageable by the IT department, and that several CSPs may be involved, make IT implementations particularly challenging. The increased level of complexity and abstraction associated with Cloud services also makes it more challenging to measure and manage end-to-end service performance. In addition, many parties and organizations are responsible for various components in the Cloud environment. The complex relationships and the often ambiguous boundaries make it challenging to delineate the roles and responsibilities between the customer and the CSP. Table 6-1 shows a set of metrics

[7] *"Cloud Computing Reference Architecture", ISO/IEC 17788:2014 , 15 October 2014*
[8] *D. Hui, M. Malayanur, The MITRE Corporation*

recommended by MITRE's Service Management Community that would be appropriate for each delivery model. This is only a subset of metrics that can be included in an SLA.

Table 6-1. Service Management Metrics

Performance Category	Service Model	Metric Title/Description
Critical Performance	*IaaS, PaaS*	• *Availability (Uptime)* • *Throughput* • *Response time*
Critical Performance	*SaaS*	• *Availability (Uptime)* • *Response time* • *Transaction time* *Most critical metrics are those of measuring the end-user experience in a SaaS environment, such as transaction time and availability. These metrics directly measure the application performance as the end-user experienced it, for example, the elapsed transaction time of retrieving an application response with requested data.*
Service Level Effectiveness	*All*	*Service Level Effectiveness:* • *Service-level violation rate* • *Service performance report frequency, accuracy, timeliness, reliability, and accessibility* • *Scheduled downtime*
Service Desk, Incident, and Problem Management		• *Time to resolve incidents* • *Time to respond to reported issues* • *Escalation expectations and procedures* • *Definition of incident category and severity* • *Communication, notification and alert mechanisms and process* • *Responsiveness and visibility of root cause analysis* • *Collaboration process on root cause analysis and proactive problem management*
Disaster Recovery (DR)		• *Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for Disaster Recovery situations* • *DR testing types, frequency, and process*
Security Management		• Federal Risk and Authorization Management Program (FedRAMP) *compliance (not applicable to community and Private Cloud services)* • *NIST compliance* • *Privacy compliance* • *Legal compliance* • *Cyber security issues and process* • *Proactive vulnerability avoidance and security enhancement measures* • *Government and Cloud provider collaboration expectations and process* • *Audit requirements and process*
Access Management		• *Unauthorized access identification, reporting, and remedies* • *Data encryption requirements* • *Configuration management* • *Visibility into interdependence* • *What may be accessible by government vs. provider*
Data Management		• *Data ownership* • *Data disposal requirements* • *Data formats* • *Physical location of data* • *Comingling of data*

One IBM developerWorks® author[9] identified the usefulness of three more metrics: user threshold levels, which sets the maximum number of users concurrently accessing an application; data requests threshold level, which sets the maximum number of data requests users can concurrently send to the application; and, resources threshold level, which sets the maximum amount of CPU, storage devices or disk space that can be allocated to each user. It is important to understand whether these performance limits are user or provider established when evaluating an SLA.

Additional metrics that have been recommended attempt to measure "elasticity" in terms of agility and the ability to scale up and down.[10]

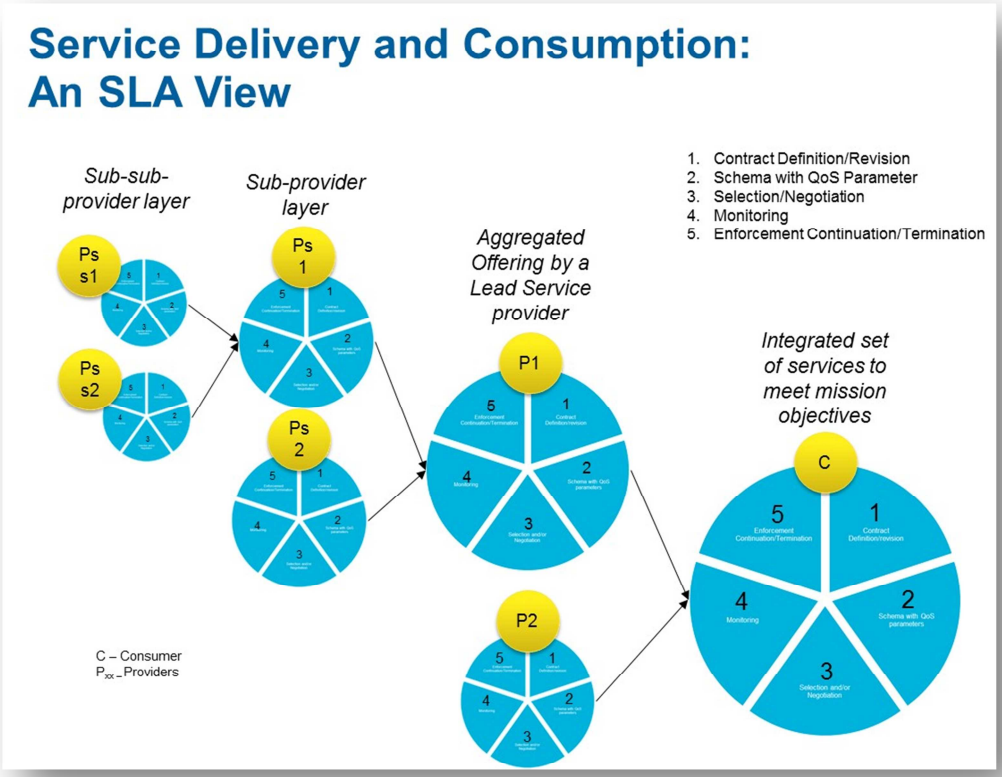


Figure 6-2. A Complex Cloud SLA Environment

The outcome of being able to utilize many Cloud services together, such as having a SaaS solution running over IaaS, -- that is then connected to a commercial network provider each with differing SLA parameters -- is that net performance results may not be readily understood especially when there is an outage. To handle the complexities of having multiple SLAs, it becomes important to have a standardized approach to developing the SLAs that can be shared among partners[11]. It also becomes important to have an SLA Integrator[12] or SLA Manager[13] who understands the agreements and their

[9] *"Best practices to develop SLAs for Cloud computing", Judith Myerson, IBM, 7 Jan2013*
[10] *SPEC Open Systems Group, Cloud Computing Working Group*
[11] *"Best practices to develop SLAs for Cloud computing", Judith Myerson, IBM, 7 Jan2013*
[12] *"Enabling End-to-End Cloud SLA Management", Frameworx Best Practice, October 2014, TMForum.*
[13] *The simple solution to managing complex or multiple Cloud SLAs, Judith Myerson Nov 6 2014, Tech Republic, http://www.techrepublic.com/article/the-simple-solution-to-managing-complex-or-multiple-Cloud-slas/*

implications in relation to the performance goals of the organization. Figure 6-2 shows a complex Cloud ecosystem in which multiple sub-providers and make up an offering and in turn that a consumer may need to be the integrator of multiple SLAs to meet mission performance needs. .

It is often unclear as to who should provide end-to-end SLA guarantees. Several Cloud Computing resellers and providers have indicated that they will provide the individual SLA components (e.g. compute, storage network); however, end-to-end SLA accountability belongs to the government consumer. Similarly Cloud integrators indicated that they provide solutions, not end-to-end SLA guarantees, unless they are included in the engineering/architecture design and decision processes and have complete control of the SLA components. This example clearly illustrates the need for an SLA Integrator or SLA Manager but is not yet clearly an established best practice. It is also noted that there will need to be more sophisticated tools to help SLA integrators and managers.

7 SECURITY CONSIDERATIONS IN SLAS FOR FEDERAL GOVERNMENT IN THE CLOUD

Security remains a significant federal government Cloud Computing challenge, and the biggest concern relates to implementation of security controls. The federal government has taken steps to address the security challenges with the Federal Risk and Authorization Management Program (FedRAMP), which provides a path for companies to achieve a security designation that is recognized across the government. FedRAMP guidance is updated frequently to address new threats[14]. Companies that obtain an authorization to operate from the Joint Authorization Board (JAB) -- comprised of the departments of Defense and Homeland Security and the General Services Administration--enjoy a "gold standard" of government security credentials. This, however, is only the beginning for many federal agencies in establishing a secure posture while using Cloud services. FedRAMP is a broader agency certification and currently only certifies Cloud providers for the handling of Controlled Unclassified Information (CUI). Many agencies have additional security requirements they must adhere to for CUI, some of which drive agency Cloud implementation (e.g. implement additional security controls) and operation costs (e.g. request additional monitoring) that may not have been part of a Cloud provider's offered SLA.

According to FedRAMP, the assurance or confidence that the risk from using external services is at an acceptable level depends on the trust that the organization places in the external service provider. The level of control is usually established by the terms and conditions of the contract or SLA with the external service provider and can range from extensive to very limited. A best practice is creating/maintaining a chain of trust. A chain of trust requires an organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The chain of trust can be complicated due to the number of entities participating in the consumer-provider relationship and the type of relationship between the parties. External service providers may also, in turn, outsource the services to other external entities, making the chain of trust even more complex and difficult to manage. Depending on the nature of the service, it may simply be unwise for the organization to place significant trust in the provider—not due to any inherent untrustworthiness on the provider's part, but due to the intrinsic level of risk in the service. Where a sufficient level of trust

[14] *Latest update is Rev 4, June 2014, which incorporates updated NIST SP 800-53 security controls.*

cannot be established in the external services and/or service providers, the organization employs compensating controls or accepts a greater degree of risk.

FedRAMP has developed a security contract clause template to assist federal agencies in procuring Cloud-based services. This template should be reviewed by a federal agency's Office of General Counsel (OGC) to ensure it meets all agency requirements, and then incorporate it in to the security assessment section of a solicitation. The clauses cover FedRAMP requirements for areas like the security assessment process and related ongoing assessment and authorization. The template also provides basic security requirements identifying CSP responsibilities for privacy and security, protection of government data, personnel background screening and security deliverables with associated timelines.[15]

The FedRAMP process discretely identifies some security control implementations as either the consumer's responsibility to implement, or as a shared responsibility between provider and consumer. Consumer security controls are incumbent upon the agency to implement and agencies are advised to consider security responsibilities in their program planning. Federal agencies must still make a risk-informed decision about the applicability of storing and using Federal data in an information system. Ultimately, the security clauses are templates; they should be reviewed against mission requirements and tailored if agency policy warrants modification. The FedRAMP process discretely identifies some security control implementations as either the consumer's responsibility or that of the CSP.

8 KEY BEST PRACTICE: ADOPT PERFORMANCE MANAGEMENT PRINCIPLES

Cloud provisioning experiences within the federal government strongly suggest that many agencies simply do not apply disciplined approaches for managing performance internally. Hosting in the Cloud does not replace or absolve the government's responsibility to effectively manage performance. In today's Cloud environment, it is strongly recommended that agencies first implement performance management best practices, establish a stable performance baseline description, and articulate the true outcomes expected from Cloud service provisioning before considering transition to the Cloud.

Federal agencies often face the following challenges in identifying and communicating the types of performance that are an effective indicator of progress in achieving strategic outcomes:

- Different aspects of performance are managed by multiple portfolio components.
- The portfolio spans numerous organizational boundaries and performance management cultures.
- Information security requirements and the classified nature of specific data constrain the free flow of information across the enterprise.
- Resources to effectively manage performance are constrained.
- There are numerous performance-management related regulations and other compliance requirements that view performance from many different dimensions.
- Inability of data collections systems and processes to effectively and efficiently accommodate performance management and reporting.

[15] *Note the FedRAMP Revision 4 Transition Guide v2.0 updated in June 2014 incorporates the latest The FedRAMP Joint Authorization Board updated the FedRAMP security controls baseline to align with the updated NIST SP 800-53 s*

It is worthwhile for the government to overcome these challenges because a well-functioning performance management process provides the means to determine:

- Which performance metrics should be monitored on an on-going basis to readily identify, at any point in time, progress in achieving ultimate mission and satisfying stakeholder needs;
- How status should be reported to provide a timely and clear performance snapshot to key decision-makers; and
- How performance status should influence programmatic, operational and investment decisions.

NIST, in their Special Publication 500-37 *Cloud Computing Service Metrics Description (draft)*, provides a structure for expressing Cloud metrics and reinforces the importance of metrics in the Cloud decision-making process when:

- Selecting Cloud services
- Defining and enforcing service agreements
- Monitoring Cloud services
- Accounting and Auditing

NIST, in establishing its Cloud computing standards efforts, has a high priority task to define and implement Cloud service metrics, standardize units of measurement for Cloud services, and recommends the use of a Cloud Service Measurement Index, *a quantifiable method of assessing Cloud service properties*[16] to be used to assess Cloud services.

A well-planned and functioning performance management process helps managers avoid some common performance measurement and monitoring pitfalls including:

- Scrambling to pull together metrics at the last minute to support an external reporting requirement
- An inability to trace metrics to stakeholder needs, mission, and strategic outcomes
- Devoting excessive resources to monitoring and managing performance
- Losing the forest for the trees with metrics: too many metrics and still a lack of understanding as to how the portfolio is actually performing
- The application of metrics that do not communicate and motivate the types of performance and supporting behavior desired

Key steps of the recommended continuous and iterative performance management process are illustrated below in Figure 8-1.

[16] "*CLOUD SERVICE LEVEL AGREEMENTS, Meeting Customer and Provider needs",* Eric Simmon, January 28th, 2014

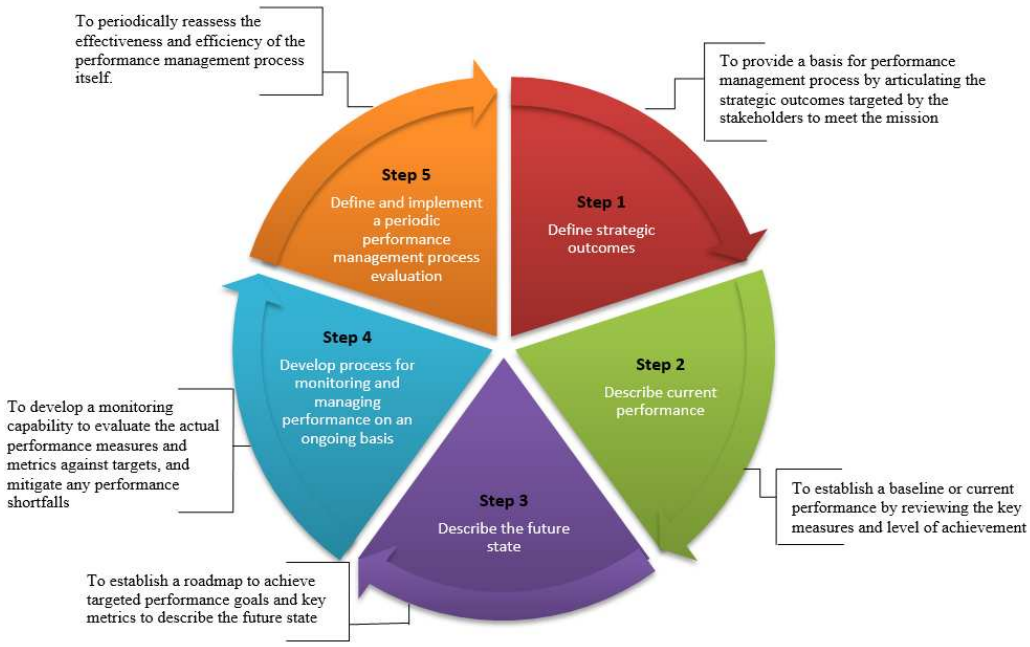


Figure 8-1. Key Performance Management Steps

Insufficient monitoring is a prevalent performance management weakness with government Cloud provisioning. In many instances, the root problem for government consumers is a genuine lack of SLA measurement and reporting maturity. Government agencies should establish an objective and independent monitoring process, along with explicit goals for proactive performance assessment. If a government consumer depends upon backups, a performance management best practice is to confirm that the backups occur as required through monitoring and testing. Data Cloud offerings may not adequately flex with demand changes, and storage usage may need to be aggressively monitored to ensure sufficient reserve capacity. It is the government's responsibility to articulate priorities for traffic, bandwidth, and capacity under different operating conditions.

Key Cloud consumer questions that should be consistently answered over the provisioning lifecycle include:

(a) Am I getting what I paid for?

(b) How are my users and mission impacted by degraded or disrupted service?

As previously discussed in this paper, some Cloud SLAs are more flexible than others, and the government consumer should be very well aware of limitations imposed by the contract or systems applied by the provider (e.g., limited APIs for data collection/analysis) that may significantly influence performance monitoring ability by the consumer. While Cloud vendors may offer tools and services to help monitor Cloud delivery, these tools and services may drive up provisioning costs.

Cloud providers typically will not offer a great deal of assistance to the government consumer in determining what should be monitored internally. Figure 8-2 recommends 5 steps that the government can implement to improve monitoring accuracy and value.

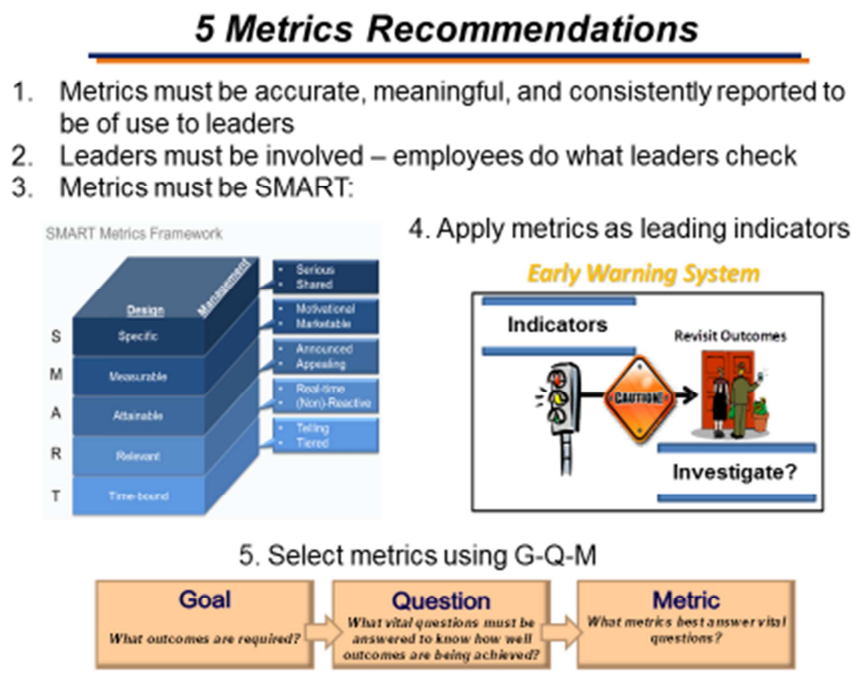


Figure 8-2. Key Performance Management Steps

9 EMERGING BEST PRACTICE: USE OF CLOUD SERVICE BROKERS AND AGENCY CLOUD PROGRAM MANAGEMENT OFFICES

Use of Cloud Service Brokers (CSBs) is still evolving, but it is a noteworthy emerging best practice. CSBs are defined by NIST Cloud Computing Reference Architecture (Special Publication 500-292) as *"intermediaries between CSPs, such as Amazon Web Services, and government customers […] would handle the details of negotiating contracts with vendors and acquire services on an agency's behalf*." Use of a C SB as a practice creates a layer of abstraction between the many Cloud vendors and the purchaser and leaves the task of comparison shopping to those who have the tools and are deeply invested in understanding cloud services and value. CSB can take on roles of advisor, integrator, or an aggregator. But NIST also identifies that CSBs can be focused on business brokering or technical brokering. Here is a demonstration that in this relatively young technology area that definitions are still emerging. According to Federal Computer Week, "*Four years later, notions about what constitutes a Cloud broker and what role it should play in the government market have changed considerably.* In some cases CSBs, "*are starting to resemble the systems integrators of the 1990s as they pull together comprehensive solutions for customers. In other situations, brokers are taking on a consulting role and serving as trusted Cloud advisers for their government clients*."[17]

To illustrate how Cloud Brokers are used in a government setting, NASA, considered a "Cloud pioneer" in the government, is discussed. NASA is working through a transition from private to public cloud

[17] *"Cloud brokers, the sequel" May 11, 2015, Federal Computer Week (http://fcw.com/articles/2015/05/15/Cloud-brokers-sequel.aspx)*

deployment using a Cloud broker/integrator, InfoZen[18]. They outline a way ahead where they will transition the CSB duties to an internal organization but still use a CSB in the capacity of an advisor. This demonstrates a path that organizations can take using CSBs. A 2013 NASA Inspector General report found that NASA has had some success establishing a broker but further recommended that NASA back this up with guidance to ensure others within the agency use the broker to help mitigate risk[19] NASA subsequently created the Jet Propulsion Laboratory Cloud Computing Commodity Board (CCCB), which "*oversees the long-term Cloud computing procurement strategy. This board meets monthly and is composed of members from IT, security, legal, finance, procurement, and export control, as well as end users*."[20]

Others are not as optimistic about CSBs: a recent Fierce Government IT article quotes one GSA official who contends, "*Agencies currently have no guidance for partnering and using a Cloud broker*.[21]"

With their deep knowledge of the cloud capabilities and value, CSBs can provide benefit and may be a future best practices; but to do so, more guidance may need to be formalized and further research as to how the best practice is to be defined is merited.

[18] *NASA Cloud Migration Saves Millions, Information Week Government, http://www.informationweek.com/Government/cloud-computing/nasa-cloud-migration-saves-millions/d/d-id/1306979*
[19] *NASA's Progress In Adopting Cloud Computing Technologies, July 2013, NASA Office of Inspector General*
[20] *"JPL's Cloud Computing Strategy", March 2015, http://www.nasa.gov/content/jpl-s-cloud-computing-strategy/*
[21] *"Waiting on FedRAMP for cloud brokers? Don't hold your breath," May 18, 2015 Fierce Government IT*

10 OVERVIEW OF SLA CONSIDERATIONS

The table reflects modifications and additions to the Cloud SLA Guide Overview table that was included in the 2010 MITRE paper. This table provides a summary of what is included within detailed tables in Appendix A. Modifications to the table from the original paper are highlighted using red font.

Table 10-1. Cloud SLA Guide 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. *(a)*	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.* • *(a) Delaney, J., 2004, "The Outsourcing Revolution, 2004: Protecting Critical Business Functions".*
Business Policies	The customer agreement, acceptable use policy, or SLA should address business policies associated with: • Guarantees • Acceptable Use Policy (AUP) • Excess Usage Billing • Service Activation • Governance • Change Notification and Management • Support, Prioritization, Escalation • Definition of Business Hours / Prime Time • Planned Maintenance • Renewals • Transferability • Subcontracted Services • Licensed Software • Industry-Specific Standards (e.g., HIPAA) • Country-Specific Laws & Regulations	Consumers should carefully assess whether the service agreement specifies compliance with appropriate laws and regulations governing consumer data. The use of Cloud services by a Cloud service customer means that the customer organization is placing some parts of its IT operations – and hence part of it business processes - in the hands of outside suppliers in the form of one or more CSPs. As a result of the interface(s) between the customer and the provider, there is a need for strong and detailed governance of the use of the Cloud services on the customer side. Business level policies expressed in the CSA require careful evaluation. Uptime and availability are another area where customer requirements and policies may not match up with the language of the vendor, and where location and jurisdiction may come into play. For example, if the uptime guarantee is for "regular business hours," then organizations with multiple locations in different time zones need to clarify whether the guarantee covers only the headquarters location or all regions. Similarly, "weekends" or "holidays" have different meanings in different countries. All of these policies will impact and influence the customer's Cloud strategy and business case. In many cases, these policies, as defined in the CSA, are non-negotiable and are similar across different Cloud providers. However, there will be instances where some of these policies can be negotiated and/or some of these policies differ sufficiently across	• *NIST SP 800-146, Cloud Computing Synopsis and Recommendations* • *Cloud Standards Customer Council, April 2015. "Practical Guide to Cloud Service Agreements, v2.0".*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
		different Cloud providers to warrant careful consideration by customers.	
Service Descriptions	The SLA should provide a clear and logical linkage of overall service/capability offerings, objectives, and KPIs. This logical description should start with a clear overview of: • Business Level Objectives • Service Level Objectives • Baseline services • Optional services • Customer-unique services One of the unique aspects of Cloud Provisioning is the capability to scale easily by providing autonomous provisioning. The description should be clear about any bounds associated with this capability. Most importantly, the SLA should identify which services are NOT covered. SLAs should be measurable and actionable *(b)*. Service groups or other logical categorization of services should be identified, and their interdependencies, along with a description of the overall service strategy (e.g., service improvements).	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. Understanding the deployment model differences establishes a firm foundation for understanding the rest of the SLA. 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." *(c)*	• *(b) Delaney, J., 2004, The Outsourcing Revolution, 2004: Protecting Critical Business Functions.* • *(c) Anderson, B., "Structuring Meaningful SLAs for IT Support," http://www.itservicemanagement-itil.com/wp-content/downloads/IT-support-Service-Level-Agreements.pdf.* • *Cloud Standards Customer Council, April 2015. "Practical Guide to Cloud Service Agreements, v2.0".* • *Financial Management Line of Business, "Migration Planning Guidance, Version 1," http://www.hud.gov/offices/cpo/contract/opc23053final/attachmnt/ATT16BFMLOBSLAOverview.pdf.* • *Practical Guide to Cloud SLAs, Cloud Standards Customer Council, 10Apr2012. Updated in "Practical Guide to Cloud Service Agreements, v2.0", April 2015. Step 3 of 7 steps.*
Metrics and Key Performance Indicators	Organizations must monitor and manage the Cloud services they use. For each level of service offered, effective service management and monitoring includes: • Auditing • Monitoring and reporting on a set of agreed to performance metrics • Measurement & metering methods • Service level improvement thresholds	• Is the provider's management system adequate? • Are you getting what you're paying for? • Can you change resources quickly?	• *Cloud Standards Customer Council, April 2015. "Practical Guide to Cloud Service Agreements, v2.0".*
Continuity and Outages	This SLA element should describe how service/capability continuity and outages will be managed by the provider. Techniques that can be incorporated in CSAs to avert service failure include: • Multiple redundant data centers	It is common to see a false sense of security among Cloud customers regarding disaster recovery planning. Just because agencies are using Cloud services does not absolve them of the need for serious disaster planning. Key questions that may need to be answered within the SLA	• *NIST SP 800-146, Cloud Computing Synopsis and Recommendations* • *Cloud Standards Customer Council, April 2015. "Practical Guide to Cloud Service Agreements, v2.0".* • *Ohlhorst, F., June16, 2009, "What to Look for in a*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
	• Replicated data stores • Multiple redundant networks • Multiple app instances • Automated failover	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.	*Cloud Computing SLA,"* http://searchcio.techtarget.com.au/news/2240020663/What-to-look-for-in-a-cloud-computing-SLA • http://www.solarsysconsulting.com/invokate/service_level_agreement.htm, *accessed June 24, 2010.*
Security Management	The government consumer must clearly understand the CSP's willingness to accommodate customer-requested external security controls. The government consumer should also understand the methods by which the CSP intends to manage vulnerabilities, as well as the CSP's position regarding data ownership, protection, and control. The SLA should specify information relating to the confidentiality and integrity of the services and the security controls which apply to the services. The SLA should specify how privacy and personally identifiable information will be handled in relation to the Cloud services.	Consumers should carefully examine the service agreement for any disclaimers relating to security or critical processing, and should also search for any language as to whether the provider recommends independent backup of data stored in their Cloud.	• *ISO/IEC 17789:2014, Cloud Computing Reference Architecture*
Roles and Responsibilities	Identify the Cloud actors. Identify the SLA Integrator/ Manager. Identify third party contributors. Coordinate and collaborate amongst the key stakeholders ensuring they understand what they contribute and have articulated what they need from the other stakeholders. Maintain adaptability and agility to work with the major Cloud players and the mission/business to make changes or	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. SLAs will often hold the consumer, not just the provider, accountable for certain actions: • Adhering to any related policies, processes and	• *Practical Guide to Cloud SLAs, Cloud Standards Customer Council, 10Apr2012. Updated in "Practical Guide to Cloud Service Agreements, v2.0", April 2015. Step 1 of 7 steps.* • *MITRE Service Management Challenges in the Cloud Wikipedia.* • *Karten, N., 2003, "Why SLAs Fail and How to Make Yours Succeed,"*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
	improvements as necessary. The SLA should articulate roles and responsibilities for each actor.	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.	*http://www.nkarten.com/WhySLAsFail-B8R.pdf* *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.*
Payment, Recourse, and Reward	The SLA should have negotiated financial penalties when an SLA violation occurs. If there is no repercussion when the provider fails to meet its 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. 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.	Since Cloud models offer opportunities to consider the use case of services scaling up or down in response to events and recognition of demand, payment, recourse and rewards actions should be appropriate and reward successful scaling efforts. Consumers should fully explore all opportunities in flexibility for payment methods, rewards, and recourse. Unless a specific service agreement has been negotiated with a provider, remedies for any failures are likely to be extremely limited; consumers may wish to formulate and negotiate remedies that are commensurate with damage that might be sustained.	• *Hiles, A., 2000, "Service Level Agreements: Winning a Competitive Edge for Support and Supply Services," Rothstein Associates, Inc., pg. 113.* • NIST SP 800-146, *Cloud Computing Synopsis and Recommendations*
Terms and Conditions	In Cloud Computing procurements, some of the sub-elements 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.	• *See Table A-8*
Exit Strategy and Process	The SLA should define the customer exit plan, including: • Procedures • Provider assistance • Fees • Retrieval of customer data • Business continuity during exit • Requirement for provider to delete/make inaccessible copies of customer data • Requirement for provider to cleanse log and audit data	An exit clause should be part of every SLA and describes the details of the exit process including the responsibilities of the Cloud provider and consumer in case the relationship terminates prematurely or otherwise. A detailed customer exit plan *"will ensure minimum business disruption for the customer and ensure a smooth transition. The exit process should include detailed procedures for ensuring business continuity, and should specify measurable metrics to ensure the Cloud provider is effectively implementing these procedures."*	• *Cloud Standards Customer Council, April 2015. "Practical Guide to Cloud Service Agreements, v2.0".*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
	• Retention of records for specified periods		
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.	Create transparency of end-to-end IT service quality levels via monitoring tools, reports, dashboards etc. Current practitioner experiences include having insufficient insight into service performance. Performance monitoring is an essential step in avoiding disagreements about who is responsible for performance failures *(d)*.	• *MITRE Service Management Challenges in the Cloud Wikipedia.* • *(d) 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. The SLA may address application of Information Technology Infrastructure Library (ITIL) approaches for addressing: • Auditing • Measurement and Metering • Provisioning • Change management • Upgrades and patching	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, http://searchcio.techtarget.com/news/1363821/Beware-these-risks-of-cloud-computing-from-no-SLAs-to-vendor-lock-in*
Definitions/ Glossary of Terms	Include definitions of fees and aspects of service that are within the scope of the SLA. When assessing vendor SLAs, pay close attention to the terms that are used in the service agreements. Common terms may be redefined by a Cloud provider in ways that are specific to that provider's offerings.	"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." *(e)*	• *(e) Dimension Data, November 2009, "Is Your SLA Your Weakest Link?" p 7, http://docs.noodls.com/viewDoc.asp?filename=37780%5CEXT%5C20100420007500706906 7101.pdf.* • *"Information technology — Cloud computing — Overview and vocabulary" (ISO/IEC 17788), October 2014,* • *http://www.iso.org/iso/catalogue_detail?csnumber=60544* *"Enabling End-to-End Cloud SLA Management", Frameworx Best Practice, October 2014, TMForum.* • *NIST SP 800-146, Cloud Computing Synopsis and Recommendations.*

11 SUMMARY OF RECOMMENDATIONS

Cloud business models have matured since 2010, and providers are self-organizing (e.g., Open data Center Alliance, Distributed Management Task Force) with a goal of aligning with one another and standardizing their offerings to speed adoption. Industry-driven consumer guidance (e.g., that provided by TM Forum, The CSCC) is emerging to help consumers make the right decisions about Cloud offerings. At the same time, standards organizations (e.g., NIST and ISO/IEC), who typically offer the foundations and expressions to promote clear, unambiguous customer-provider interactions in the Cloud industry are also just developing guidance (e.g. ISO/IEC Cloud SLA series of guidance is under development). There are common government services (e.g., FedRAMP and GSA Cloud Services) to alleviate the burden of government decision-making, but because these services offer to the lowest common denominator of government needs, each government entity must still evaluate and determine what its unique needs are. The result of this level of evolution of the Industry is that best practices are still emerging, and a government consumer bears the burden to collect and analyze many viewpoints to determine what its Cloud practices should be.

Therefore, to manage successful Cloud adoption requires the government to embrace a best practice of leveraging the afore-mentioned working groups, nonprofits and consortiums that have emerged over the last five years to support Cloud migration. These groups can provide some value to a Cloud adopter in the form of papers, webinars, current events and training and include representatives from industry, government and nonprofit entities. This approach can seem burdensome; the government should consider using information brokers to alleviate this burden.

To help alleviate the burden of sorting through the complexities of Cloud adoption, using an integrator/broker business approach is emerging. This model is akin to the system integrator role used in Department of Defense (DoD) large weapon system development where many subcontractors need to be managed by a single contractor to build a ship or aircraft. Many lessons and best practices can be transferred from the weapon system integrator domain with regards to how to successfully leverage an integrator/broker business model. With the transference of risk that occurs in this model, the government consumer must ensure that the performance needs (and how they support the mission) are clearly articulated, and the integrator/broker can act successfully on behalf of the government.

While waiting for reference architectures and model expressions to be published, the government consumer must rely on the tried and true principles of performance management when deploying to the Cloud. Because the government consumer initially viewed security as its primary risk area, most of the decision-support for Cloud adoption had been in this area. Now that the consumer is more informed about Cloud security capabilities, there could be a more focused effort toward establishing more detailed performance management guidelines for Cloud consumers to communicate to providers. Of note in the area of metrics is the emergence of an elasticity metric that shows how well the service responds to changing demand and understanding who (user or provider) sets user, data request and resource threshold limits. A Cloud Service Measurement Index (CSMI) can prove beneficial by providing a standard approach to evaluating a Cloud service. This metric is not yet embraced by government consumers as it too is just emerging. Providers are still learning about the needs of the government consumer and business models, and tools and methods are not yet embraced as best practice to address the government consumer's Cloud performance transparency and auditing needs. Regardless, the government can still benefit by assuming responsibility for, taking control of and meeting the intent of performance management principles to support mission needs.

Another key practice that a government consumer must embrace is that of ensuring that the technical design of the Cloud deployment fully accounts for continuity of mission needs. A misconception is that because it is the Cloud, that it is available continuously. Because Cloud offerings are usually a web of computing nodes, it is important that the government consumer deliberately identifies the need for and deploys an architecture that accounts for cut-over of processing loads when a region goes down. The government must also be explicit in the SLAs the levels and priorities expected in degraded operations situations.

Finally, the two key areas in which there is still a degree of perceived risk for government Cloud adopters are transportability between Clouds and physical data location. Transportability is important in the event that the government wants to move its workload due to termination of services and physical data location is important to ensure accountability for assets. These concerns have led consumers to hybrid Cloud solutions where perceived higher risk assets are in a Private Cloud while perceived lower risk assets are a Public Cloud. This type architecture, when populated with multiple vendors each with uniquely-expressed SLAs, leads to a management complexity that should be addressed by an SLA Manager who knows the landscape and understands the implications of net SLA on the organization's mission. Even if an organization chooses to put all its IT assets in a single Cloud, end-to-end performance is still its responsibility and it is in its best interest to have an organic SLA Manager. Another best practice that would address this risk is to ensure that all the organization's SLAs are as close to a standard as possible to ensure easy comparison and understanding of the net performance results of multiple SLAs.

APPENDIX A: DETAILED SLA TABLES

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. *(f)*	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.* • *(f) Delaney, J., 2004, The Outsourcing Revolution, 2004: Protecting Critical Business Functions.*
Provider and Consumer Contact Info	Identify key Cloud actors, which may include the Cloud Consumer, the Cloud Provider, the Cloud Carrier, the Cloud Auditor, and the Cloud Broker. Each party should establish a primary communications POC who is available during normal business hours. Alternates should be identified for periods of unavailability (e.g., vacation). 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.	• *Simmon, E. 28Jan2014 (NIST), "Cloud Service Level Agreements: Meeting Customer and Provider Needs".* • *Financial Management Line of Business, "Migration Planning Guidance, Version 1," http://www.hud.gov/offices/cpo/contract/opc23053final/attachmnt/ATT16BFMLOBSLAOverview.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 should also 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. Business Policies

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
Business Policies	The customer agreement, acceptable use policy, or SLA should address: • Governance • Maintenance Practice • Support, Prioritization, Escalation • Definition of Business Hours / Prime Time • Activations and Renewals • Industry-Specific Standards (e.g., Health Insurance Portability and Accountability Act. HIPAA) • Country-Specific Laws & Regulations All of the Public Cloud providers reviewed by the authors included acceptable use terms for both the Cloud provider and the Cloud consumer. For example, the Cloud consumer agrees not to install malware on the Cloud. The Cloud provider agrees not to violate the intellectual property rights of the consumer. In most cases, an Acceptable Use Policy is provided as a separate artifact on its own web page. The AUP sometimes overlaps with, or replaces, the Security/Privacy terms of the Customer Agreement.	The use of Cloud services by a Cloud service consumer means that the consumer organization is placing some parts of its IT operations – and hence part of its business processes - in the hands of outside suppliers in the form of one or more CSPs. As a result of the interface(s) between the consumer and the provider, there is a need for strong and detailed governance of the use of the Cloud services on the consumer side. Business level policies expressed in the CSA require careful evaluation. Uptime and availability are other areas where consumer requirements and policies may not match with the language of the provider, and where location and jurisdiction may come into play. For example, if the uptime guarantee is for "regular business hours," then organizations with multiple locations in different time zones need to clarify whether the guarantee covers only the headquarters location or all regions. Similarly, "weekends" or "holidays" have different meanings in different countries. All of these policies will impact and influence the consumer's Cloud strategy and business case. In many cases, these policies, as defined in the CSA, are non-negotiable and are similar across different Cloud providers. However, there will be instances where some of these policies can be negotiated and/or some of these policies differ sufficiently across different Cloud providers to warrant careful consideration by consumers.	• *Cloud Standards Customer Council, April 2015. "Practical Guide to Cloud Service Agreements, v2.0".* • *"Public Cloud Service Agreements: What to Expect and What to Negotiate", Cloud Standards Customer Council, 30Mar2013, Page 6.*
Maintenance Practice	Maintenance practices should be documented in the **SLA** for the **Cloud services** and should include the capability for the customer to report problems and request fixes and also a mechanism for the **CSP** to notify the customer of pending maintenance changes and their schedule.	The government needs to understand this schedule to ascertain the impact to mission of maintenance.	• *ISO/IEC 17789:2014, Cloud Computing Reference Architecture*
Regulatory Compliance Responsibility	The SLA may identify if/how the vendor's offering complies with key regulations that are relevant to the consumer, including Federal Information Security Management Act (FISMA), HIPAA, and Sarbanes-Oxley 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, http://searchcio.techtarget.com/news/1363821/Beware-these-risks-of-cloud-computing-from-no-SLAs-to-vendor-lock-in*

Table A- 3. 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 KPIs. This logical description should start with a clear overview of: • Baseline services • Optional services • Customer-unique services SLAs should be measurable and actionable *(g)*. Service groups or other logical categorization of services should be identified, along with a description of the overall service strategy (e.g., service improvements).	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. 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." *(h)*	• *(g) Delaney, J., 2004, The Outsourcing Revolution, 2004: Protecting Critical Business Functions.* • *Financial Management Line of Business, "Migration Planning Guidance, Version 1," http://www.hud.gov/offices/cpo/contract/opc23053final/attachmnt/ATT16BFMLOBSLAOverview.pdf.* • *(h) Anderson, B., "Structuring Meaningful SLAs for IT Support," http://www.itservicemanagement-itil.com/wp-content/downloads/IT-support-Service-Level-Agreements.pdf*
Objectives	When considering Business Level Objectives, customers must consider the policy and compliance requirements relevant to them when reviewing a CSA since there are interdependencies between the policies expressed in the CSA and the business strategy and policies developed across the lines of business. Service level objectives (SLOs) are 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	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. Performance goals within the context of Cloud computing are directly related to the efficiency and accuracy of service delivery by the Cloud provider.	• *Practical Guide to Cloud SLAs, Cloud Standards Customer Council, 10Apr2012. Updated in "Practical Guide to Cloud Service Agreements, v2.0", April 2015. Step 2 of 7 steps.* • *Karten, N., 2003, "Why SLAs Fail and How to Make Yours Succeed," http://www.nkarten.com/WhySLAsFail-B8R.pdf Strum, R. and W. Morris, 2000, "Foundations of Service Level Management."* • *"Practical Guide to Cloud Service Agreements, v2.0", April 2015. Step 4 of 7 steps.*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
	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. Identify critical performance objectives		
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." *(i)*	This SLA element can provide insights into excused performance failures/degradation. Consumers should be very interested in what other factors may influence service performance. A Cloud SLA Manager and/or Integrator should be assigned and should track and understand the implications of service interdependencies.	• *(i) 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	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. For many government entities seeking higher accountability, these technical and advisory services may be needed to get transparency in to performance	• 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?	• *"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." *(j)*	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.	• *(j) 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- 4. 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	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. 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.*" *(k)* 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.	• *(k) 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.itservicemanagement-itil.com/wp-content/downloads/IT-support-Service-Level-Agreements.pdf* • *Financial Management Line of Business, "Migration Planning Guidance, Version 1," http://www.hud.gov/offices/cpo/contract/opc23053final/attachmnt/ATT16BFMLOBSLAOverview.pdf.*
Performance Metrics	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	SLAs may contain numerous service performance metrics with corresponding CSCC. 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. 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	• *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.hud.gov/offices/cpo/contract/opc23053final/attachmnt/ATT16BFMLOBSLAOverview.pdf.* • *(l) 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,*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
	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. More specific metrics identified below:	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."(I)* • 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.	http://www.datacenterknowledge.com/archives/2008/01/15/reliability-in-the-cloud-slas-will-matter/.
Quality Assurance, Performance Data Requirements, and Measurement Methods	The SLA must define how all of the individual measurements will be applied to determine if delivery against the SLA was satisfactorily achieved. Often, there is a gap in measurement and higher level functional guarantees. To address this gap, NIST, for example, has created a Cloud Service Measurement Index (SMI). This index is a quantifiable method of assessing Cloud service properties. It specifically identifies how levels of performance are aggregated and weighted. 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.	The government consumer and the provider will want a very clear understanding of what truly matters when determining whether consumer expectations were achieved. 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?	• *Cloud Standards Customer Council, April 2015. "Practical Guide to Cloud Service Agreements, v2.0* • *Simmon, E. (NIST), 28Jan2014. "Cloud Service Level Agreements: Meeting Customer and Provider Needs". Public version of the SMI available here: http://csmic.org/* • *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/archives/Challenges-to-QoS-and-SLA-Management.html.* • *Sommers, J., et. al., 2007, "Efficient Network-Wide SLA Compliance Monitoring," SIGCOMM Proceedings, http://ccr.sigcomm.org/online/?q=node/251.*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
		• When will the measurements be collected (e.g., continuously, periodically)?	
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 incentives 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- 5. 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. In Public Cloud agreements, consumers must fully understand the impact that potential suspension of services will have on their data and business services, and on their own clients, and should develop a plan to ensure business continuity in such an event. A suspension of services clause should be part of every Customer Agreement and should describe in detail the circumstances under which Cloud providers can suspend services to a consumer. Reasons for suspension will typically include: · Breach of contract, including payment delinquency · Behavior posing a security risk to the service or any third party · Actions that may subject the Cloud provider to liability · Usage that represents a direct or indirect threat to the provider's network function or integrity, or to anyone else's use of the service In most cases, suspension of service is applied to the minimum necessary portion of the service and will only be in effect for as long as reasonably necessary to address the issues giving rise to the suspension. Advance notice is typically given before service is suspended, except in emergency situations. Consumers are typically given 30 to 60 days to address the reasons for suspension before termination of service is initiated.	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.	• *"Public Cloud Service Agreements: What to Expect and What to Negotiate", Cloud Standards Customer Council, 30Mar2013, Page 9.* • *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?	• *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,*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
		• 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.	*http://www.cloudave.com/link/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 and Service Failure Management	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? • Prepare for and manage service failure, determining what remedies should be provided and what are the liability limitations	• *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.* • *Cloud Standards Customer Council, April 2015. "Practical Guide to Cloud Service Agreements, v2.0", http://cloud-council.org/resource-hub.htm#practical-guide-to-cloud-service-agreements-version-2*
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.'*" *(m)*	• *VeriSign, "Service Level Agreement," http://www.verisign.com/static/002488.pdf.* • *(m) 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. 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 and Risk 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. Evaluate security and privacy requirements. Security evaluation should include consideration of: • Asset sensitivity • Understanding the legal and regulatory requirements, especially on data breaches • Establishing security metrics • Implementing policies and procedures against the unauthorized use of data • Including technical measures such as IP range blocking, etc. • Assessing provider security capabilities • Assessing provider governance • Assessing provider security compliance	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 /.* • *Cloud Standards Customer Council, April 2015. "Practical Guide to Cloud Service Agreements, v2.0".Step 5 of 7 steps*
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." *(n)* 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, http://searchcio.techtarget.com/news/1363821/Beware-these-risks-of-cloud-computing-from-no-SLAs-to-vendor-lock-in* • *(n) 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.	• Does the vendor guarantee privacy of information? • What PII is being stored? • Where is it being stored? • Where is the customer based? • Where is the provider based? • Where are the users of the data located? • What is the citizenship of the people whose data is being	• *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, http://searchcio.techtarget.com/news/1363821/Be*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
		stored? • Based on all this, which laws and regulations apply? • Are they addressed in the SLA? • What are the rules about data movement, backup, and retention? • Do these processes risk violating the laws and regulations?	ware-these-risks-of-cloud-computing-from-no-SLAs-to-vendor-lock-in • *Cloud Standards Customer Council, April 2015. "Practical Guide to Cloud Service Agreements, v2.0".*
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.*" *(o)*	• *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.* • *(o) 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.*
Data Ownership, Protection, and Control	The duty of care a Cloud provider has to its clients and their data is partly governed by the data protection legislation applicable in the user's local jurisdiction and also in those jurisdictions in which its data may reside or is made available. Consumers should carefully consider these legal requirements	"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"	• *Cloud Standards Customer Council, April 2015. "Practical Guide to Cloud Service Agreements, v2.0".* • *"Public Cloud Service Agreements: What to Expect and What to Negotiate", Cloud Standards Customer Council, 30 Mar2013 http://www.cloud-council.org/PublicCloudServiceAgreements2.pdf*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
	and how the SLA their provider(s) offers deals with issues such as movement of data to offer multisite redundancy across several jurisdictions. Cloud consumers should: • Ensure that the agreement allows the consumer to specify the physical location of their security-sensitive content, or content subject to data residency requirements (specifically acceptable locations vary across industries and national legislations). • Ensure that the Cloud provider will not access the consumer's data, except when required by law and duly requested by law enforcement authorities. • Under such circumstances, ensure that the agreement specifies that the Cloud provider will give immediate notice, allowing the consumer an opportunity to file for a stay of the request.	*(p)*. Key data policies to consider include data preservation, data redundancy, data location, data seizure, and data privacy. 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? • Is data backed up; if so how/when? • 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? 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*." *(p)*	• *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,* http://searchcio.techtarget.com/news/1363821/Beware-these-risks-of-cloud-computing-from-no-SLAs-to-vendor-lock-in • *(p) Goertzel, K. et. al., December 2009, "Cloud Computing for Real," FedTech Magazine,* http://www.fedtechmagazine.com/print_friendly.asp?item_id=663.

Table A- 7. 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	Identify the Cloud actors. Identify the SLA Integrator/Manager. Coordinate and collaborate amongst the key stakeholders ensuring they understand what they contribute and have articulated what they need from the other stakeholders. 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. For consumers to understand specific roles and responsibilities explicitly or implicitly stated in a Cloud SLA, it is important that they are aware of the various actors that can potentially participate in a Cloud Computing environment. The National Institute of Standards and Technology (NIST) Reference Architecture 1 identifies 5 unique Cloud actors: 1. *Cloud Consumer*. The person or organization that maintains a business relationship with, and uses service from, Cloud providers. 2. *Cloud Provider*. The person, organization or entity responsible for making a service available to Cloud consumers. 3. *Cloud Carrier*. The intermediary that provides connectivity and transport of Cloud services from Cloud providers to Cloud consumers. 4. *Cloud Broker*. An organization that manages the use, performance and delivery of Cloud services, and negotiates relationships between Cloud providers and Cloud consumers. *Cloud Auditor*. A party that can conduct independent assessments of Cloud services, information system operations, performance and security of the Cloud implementation.	• *Practical Guide to Cloud SLAs, Cloud Standards Customer Council, 10 Apr 2012. Updated in "Practical Guide to Cloud Service Agreements, v2.0", April 2015. Step 1 of 7 steps.* • *Karten, N., 2003, "Why SLAs Fail and How to Make Yours Succeed," http://www.nkarten.com/WhySLAsFail-B8R.pdf* • *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 subcontractor provisioning to the services. Cross-Cloud applications also contribute to risk. "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." *(q)* • Customers … should review carefully any sub-contracting provisions in the services agreement." *(r)*	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, a 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.*" *(r)*	• *(q) 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.* • *(r) 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- 8. 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. When evaluating the service commitments of Cloud providers, consumers should take the following steps: • Analyze service availability guarantees and associated credits. • Find the observation period over which commitments are measured, and understand the business impact of a single outage corresponding to the maximum downtime occurring once during that time window. • Analyze service credit calculations and maximum credit limits. • Compare service credit processes, particularly the timeframe within which incidents must be reported and the type of information required to prove that a failure occurred. • Examine commitment exclusions. • Automate the process for detecting and logging service outages, for example using tools that exercise the Cloud service through periodic dummy transactions, recording the response time as well as detecting failures.	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. New pricing structures are emerging and involve application of a Cloud Price Index. *"We combine performance benchmark data on Hadoop, MySQL, Cassandra and MongoDB with Cloud Price Index data, and find assessing Cloud value is a tricky task with variable results. Virtual machines of the same approximate size deliver different price-performances, not just between providers, but also on the same provider at different times of the day. And although we find in general, scaling horizontally is better value than scaling vertically, in some instances the opposite seems true."(s)*	• *Hiles, A., 2000, "Service Level Agreements: Winning a Competitive Edge for Support and Supply Services," Rothstein Associates, Inc., page 113.* • *"Public Cloud Service Agreements: What to Expect and What to Negotiate", Cloud Standards Customer Council, 30 Mar2013 http://www.cloud-cocil.org/PublicCloudServiceAgreements2.pdf* • *(s) "Cloud price-performance under pressure", Research 451, Owen Rogers, 15Mar2015*
When/how payment is to be 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: 1. Usage-based model (e.g., Amazon EC2) 2. Subscription-based model (e.g., Google Apps Premier Edition) If different "pay plans" are offered, the SLA should	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	• *"Cloud Computing Reference Architecture", ISO/IEC 17788:2014 , 15 October 2014* • *FedCloud, October 1, 2007, "Simple Storage Service," http://fedcloud.com/simple_storage_service.html.*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
	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 signup." 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.	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?	
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 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*." *(t)*	• *(t) Levi, S., et. al., March 2010. "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	• *Hiles, A., 2000, "Service Level Agreements: Winning a Competitive Edge for Support and Supply Services," Rothstein Associates, Inc., Annex A.*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
		criticality of the service in question and according to the severity of the issue (e.g., critical, major, minor).	
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's gone over two minutes in favor of one that could still be answered in two minutes. *(u)*	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." *(v)*	• *(u) Delaney, J., 2004. "The Outsourcing Revolution, 2004: Protecting Critical Business Functions."* • *(v) "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 definition of service credits and the supporting process for requesting credits vary 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. 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?	• *Gangadharan, G. R., "Understanding SLAs for Cloud Services," Cutter IT Journal, Vol. 22, No. 6/7.*

Table A- 9. 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. These can cover: • Guarantees • Acceptable Use Policy (AUP) • Service Activation • Legal Authority & Governance • Change Notification and Management policies • Support, Prioritization, Escalation policies • Definition of Business Hours / Prime Time • Transferability • Licensed Software	This SLA element should support a clear understanding of business risk for the Cloud Computing consumer.	*Cloud Standards Customer Council, April 2015. "Practical Guide to Cloud Service Agreements, v2.0".*
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.hud.gov/offices/cpo/contract/opc23053final/attachmnt/ATT16BFMLOBSLAOverview.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. MSA should allow for comparison amongst different CSPs. Can be tailored once specific supplier is identified. Use of Commercial Framework Usage Model or similar tools can help government to design an appropriate MSA.	• *Recorded Webinar (panel discussion): Cloud SLAs: What You Should Be Asking Distributed Management Task Force," April 17, 2013 http://dmtf.org/education/webinars* • *Financial Management Line of Business, "Migration Planning Guidance, Version 1," http://www.hud.gov/offices/cpo/contract/opc23053final/attachmnt/ATT16BFMLOBSLAOverview.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," http://www.nkarten.com/WhySLAsFail-B8R.pdf*
Limitations of	Under these clauses, both the service provider and	Limitation of liability clauses often will focus on the	• *Gangadharan, G.R., 2009, "Understanding SLAs for*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
Liability	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. When evaluating liability limitations, consumers should: • Carefully review the provider's *aggregate liability,* since this amount differs across providers. • Ensure that the disclaimers exclude cases where the provider is negligent. • Compare the indemnification and disclaimer clauses to ensure there are not significant differences between the Public Cloud providers being considered. • Verify that the indemnification clause is reciprocal – it is not just the consumer protecting the provider, but the other way around too.	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.*" *(w)*	*Cloud Services," Clutter IT Journal, Vol. 22, No. 6/7.* • *(w) Cain, C., February 12, 2010, "Basic Understanding Can Clear Fog Surrounding 'Cloud Computing' Agreements," WTN News, http://wistechnology.com/articles/7082/.* • "Public Cloud Service Agreements: What to Expect and What to Negotiate", Cloud *Standards Customer Council, 30 Mar2013 http://www.cloud-council.org/PublicCloudServiceAgreements2.pdf*
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.*" *(x)*	• *(x) 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	Government consumers should be especially interested if any third parties will own any aspects of assets that are applied	• *Booz Allen Hamilton, December 2009, "Cloud Computing Security," http://www.boozallen.com/publications/article/cloud-computing-security.*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
	provide services/capability.	for service/capability provisioning.	
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; and • 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? Even if termination is triggered by a specific event, it should be well-planned up front. What are other potential providers that can meet my business and technical needs? How long will it take to acquire a new CSP?	• *Gangadharan, G.R., 2009, "Understanding SLAs for Cloud Services," Clutter IT Journal, Vol. 22, No. 6/7.* • *Recorded Webinar (panel discussion): Cloud SLAs: What You Should Be Asking Distributed Management Task Force," April 17, 2013 http://dmtf.org/education/webinars*

Table A- 10. Exit Strategy and Process

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
Exit Strategy and Exit Process[22]	If you must switch vendors or solutions, is there a smooth exit strategy in which you can recover your data and application code? The SLA should define the customer exit plan, including: • Procedures • Provider assistance • Fees • Retrieval of customer data • Business continuity during exit • Requirement for provider to delete/make inaccessible copies of customer data • Requirement for provider to cleanse log and audit data • Retention of records for specified periods	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). An exit clause should be part of every CSA and describe the details of the exit process including the responsibilities of the Cloud provider and consumer in case the relationship terminates prematurely or otherwise. A detailed customer exit plan "will ensure minimum business disruption for the customer and ensure a smooth transition. The exit process should include detailed procedures for ensuring business continuity, and should specify measurable metrics to ensure the Cloud provider is effectively implementing these procedures." ***(y)***	• *Torode, C., August 6, 2009, "Beware These Risks of Cloud Computing, from no SLAs to Vendor Lock," CIO News, http://searchcio.techtarget.com/news/1363821/Beware-these-risks-of-cloud-computing-from-no-SLAs-to-vendor-lock-in* • *Recorded Webinar (panel discussion): Cloud SLAs: What You Should Be Asking Distributed Management Task Force," April 17, 2013 http://dmtf.org/education/webinars* • *(y) Cloud Standards Customer Council, April 2015. "Practical Guide to Cloud Service Agreements, v2.0".*

[22] *Section promoted to higher level to align with Cloud Standards Customer Council best practices.*

Table A- 11. 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	While every Cloud vendor offers different systems for visualizing data and its implications (web based, e-mail based, live, reactive, portal-based), consumers should demand from any Cloud SLA a minimum set of capabilities: 1. *Cloud Performance Management*. This domain focuses on the response times for systems within the Cloud architecture and between the Cloud and the target user systems. 2. *Load Performance*. This domain focuses on measurements and timings for when the Cloud is under stress, either intentional or unintentional. As systems can perform differently when under different loads, and the interactions and dependencies of a complex Cloud are often unknown in advance, it's important to visualize data both in a steady state as well as under load. 3. *Hybrid and Inter-Cloud Performance*. As many Clouds consist of different subsystems, often sourced from different Cloud providers, it is critical to visualize data about the interactions between those hybrid Cloud components. 4. *Application Performance*. This domain focuses on the applications executed from the Cloud, particularly internal processing benchmarks as well as end-user experience measurement. 5. *Problem Notification*. This domain focuses on monitoring and reporting failures and issues with the Cloud system. Addressed are issues with prioritization, notification and severity level assessment.	Performance monitoring is an essential step in avoiding disagreements about who is responsible for performance failures. *(z)* SLAs should identify agreements regarding access to provider performance logs and reports, and performance and status reporting that will be provided.	• *Practical Guide to Cloud SLAs Version 1.0, Cloud Standards Customer Council, 2011, page 29.* • *(z) 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 its SLA, and how it should publish its SLA and its 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	• *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.* • *(aa) Goertzel, K., et. al., December 2009. "Cloud computing for Real," FedTech Magazine, http://www.fedtechmagazine.com/print_friendly.asp?item_id=663.*

		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." (aa)	
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.*
SLA Documentation	Maintain SLA and other related documents	For a Public Cloud, a formal SLA document must be signed by both the government agency and the Cloud provider along with the contract to signify the binding nature of the agreements. In a community or Private Cloud, a formal SLA may or may not be presented to the Cloud consumer. In a government-operated community Cloud, the Cloud consumer should demand the performance expectations and all other relevant SLA terms be documented in a formal document such as a memorandum of understanding (MOU) or the interagency agreement (IAA). For an internally-operated Private Cloud, it may be acceptable to have less stringent documentation and expectations, such as setting SLOs rather than the binding targets in SLAs. The Cloud consumer should consider the increased risks involved and employ mitigation strategies appropriate for the agency.	• *MITRE Service Management Challenges in the Cloud Wikipedia.*

Table A- 12. 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	Identify and implement service management requirements .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. When evaluating service management policies, consumers should consider the following: • Consumers have the ultimate responsibility to fully understand the agreements, terms, responsibilities, activities and accountability related to service management. • Consumers must precisely define their objectives and ensure that the provider offers the level of support necessary to meet these objectives. • Customizations or supplementary agreements may be needed to address specific service management objectives and concerns, but obtaining them is unlikely or at best difficult. For services requiring such specific provisions, alternative deployment models should be considered, such as a private or hybrid Cloud. • Consumers need to consider the provider's commitments to stability of functionality over time, including APIs and Web services, and how changes can impact TCO and their customers' experience. • Consumers must examine in detail the definitions and potential impact of each service metric, and the extent to which the metric represents a serious commitment, based on how credits for outages are calculated. • Consumers should ask questions related to service management maturity in the various topic areas (service management, metrics, etc.) to distinguish actual capabilities from marketing	The fundamental goals of any Cloud Computing environment are to reduce cost, improve flexibility and increase reliability of the delivery of a service. Critical to meeting these goals is a uniform, straightforward, transparent and extensible system for managing and monitoring Cloud services. Reference outlines some key considerations in service management when entering into a SLA with a Cloud Computing provider. Every computing system requires internal controls, management, automation and self-healing in order to operate in today's interconnected world, and the Cloud is no different. Although the standards for SLA language for service management are evolving, it is of upmost importance to include provisions for the considerations outlined below in your agreements. Identify service management requirements, including what should be monitored and reported, and what should be metered. They also include how rapid provisioning should be and how resource change should be managed. This allows the government to be able to account for assets in the Cloud, get performance feedback for Cloud-deployed assets. Express how automated management should be and how much the consumer does vice the provider. In addition to performance metrics and SLAs, the process of managing SLM and the integration with Cloud providers, Cloud auditors, and other relevant entities must be agreed-upon and documented. It is essential that the SLAs are reviewed regularly for higher effectiveness and efficiency. Compared to other services, the government should employ even more rigorous management disciplines in SLM for Cloud services because of the increased responsibilities placed in the Cloud providers. SLM must be working closely with other processes, such as capacity management, incident and problem management, and change management to understand the overall effectiveness of the service and drive necessary changes in the SLAs to achieve the goals set forth for the Cloud-based IT service.	• *Practical Guide to Cloud SLAs, Cloud Standards Customer Council, 10Apr2012. Updated in "Practical Guide to Cloud Service Agreements, v2.0", April 2015. Step 7 of 7 steps.* • *Torode, C., August 6, 2009, "Beware These Risks of Cloud Computing, from no SLAs to Vendor Lock," CIO News, http://searchcio.techtarget.com/news/1363821/Beware-these-risks-of-cloud-computing-from-no-SLAs-to-vendor-lock-in* • *"Public Cloud Service Agreements: What to Expect and What to Negotiate", Cloud Standards Customer Council, 30 Mar2013 http://www.cloud-council.org/PublicCloudServiceAgreements2.pdf*

SLA Element	Desired Features and Potential "Gotchas"	Why Should the Government Value this Element and What Key Questions Should be Answered?	For Further Information
	claims. • Consumers should not totally outsource service management; they need to retain in-house the service management expertise required to monitor and improve Cloud performance.		
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.

Table A- 13. 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 are comprised of arcane service definitions and/or merely list the services bought and paid for, with no guarantees for quality of service."	• *Quote from Dimension Data, November 2009, "Is Your SLA Your Weakest Link?" p 7, http://docs.noodls.com/viewDoc.asp?filename=37780%5CEXT%5C20100420007500706906 7101.pdf* • *"Information technology — Cloud computing — Overview and vocabulary" (ISO/IEC 17788), October 2014, http://www.iso.org/iso/catalogue_detail?csnumber=60544* • *"Enabling End-to-End Cloud SLA Management", Frameworx Best Practice, October 2014, TMForum. Appendix B.* • *Section 6.2 Service Level Agreement Taxonomy*

APPENDIX B: ACRONYMS

Table B- 1. Cloud Acronyms

Acronym	Description
API	Application Programming Interface
AWS	Amazon Web Services
AUP	Acceptable Use Policy
CCCB	Cloud Computing Commodity Board
CSMI	Cloud Service Measurement Index
CSCC	Cloud Standards Customer Council
CSB	Cloud Service Brokers
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
DOD	Department of Defense
FISMA	Federal Information Security Management Act
FedRAMP	Federal Risk and Authorization Management Program
GAO	Government Accountability Office
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure As A Service
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC
JAB	Joint Authorization Board
KPI	Key Performance Indicators
MOU	Memorandum of Understanding
MSA	Master Service Agreement
NASA	National Aeronautics and Space Agency
NIST	National Institute of Standards and Technology
OGC	Office of General Counsel
OMB	Office of Management and Budget
PaaS	Platform As A Service
PAP	Priority Action Plans
PCI	Payment Card Industry
PII	Personally Identifiable Information
QOS	Quality of Service
RPO	Recovery Point Objective
RTO	Recovery Time Objective

Acronym	Description
SaaS	Software as a Service
SLA	Service Level Agreement
SLM	Service Level Management
SLO	Service Level Objectives
SOX	Sarbanes-Oxley
T&C	Terms and Conditions
TCO	Total Cost of Ownership
ToS	Terms of Service

APPENDIX C: KEY REFERENCES

Since 2010, numerous publications and other reference documentation related to Cloud SLAs have been produced. Many of these have been referenced in Appendix A of this report. Additional references that influenced MITRE's updated position regarding Cloud SLAs for the government consumer are identified in Table C-1 below.

Table C- 1. Best Practices Guidance and Regulations

Reference	Brief Description
NIST US Government Cloud Computing Technology Roadmap, Volumes I-III SP 500-293, October 2014	***Volume I High-Priority Requirements to Further USG Agency Cloud Computing Adoption,*** frames the discussion and introduces the roadmap in terms of : 1. Prioritized strategic and tactical requirements that must be met for USG agencies to further Cloud adoption; 2. Interoperability, portability, and security standards, guidelines, and technology that must be in place to satisfy these requirements, and; 3. Recommended list of Priority Action Plans (PAPs) as candidates for development and implementation, through voluntary self-tasking by the Cloud Computing stakeholder community. **Volume II, Useful Information for Cloud Adopters** describes a conceptual Cloud Computing Reference Architecture and Taxonomy, presents USG, Business Use Cases and technical Cloud use cases, identifies existing applicable standards and guidance, specifies high-priority standards, guidance, and technology gaps. It also summarizes work completed in the area of SLAs, and provides insight into the rationale for the list of action plans which are recommended for voluntary self-tasking by government and private sector organizations. **Volume III, Technical Considerations for USG Cloud Computing Deployment Decisions,** is released as a draft volume. Volume III was developed with input from US Federal agencies and the Federal Cloud Computing Standards and Technology Working Group. Volume III is intended to serve as a guide for decision makers who are planning and implementing Cloud Computing solutions by explaining how the technical work and resources in Volume II can be applied, consistent with the Federal Cloud Computing Strategy "Decision Framework for Cloud Migration." The current draft version defines and proposes a methodology and process, and proof-of-concept examples.

Reference	Brief Description
NIST US Cloud Computing Standards Roadmap, Version 2 SP 500-291, July 2013	The NIST Cloud Computing Standards Roadmap Working Group has surveyed the existing standards landscape for interoperability, performance, portability, security, and accessibility standards/models/studies/use cases/conformity assessment programs, etc., relevant to Cloud Computing. Where possible, new and emerging standardization work has also been tracked and surveyed. Using this available information, current standards, standards gaps, and standardization priorities are identified within this document.
"Cloud Computing in Government", On the Frontlines Magazine, May 2014	Series of articles describing Cloud Computing best practices and lessons learned. Describes NIST, OMB, and FedRAMP approaches to tackling Cloud challenges.
NIST Special Publication 500-307 Cloud Computing Service Metrics Description, 2015	To be successful in procuring Cloud services, one must have requirements that are clear, create SLAS which reflect these requirements and be measureable in order to validate the delivery of these services along with their performance and remedies. As part of the decision making framework for moving to the Cloud, having data on measurable capabilities, for example - quality of service, availability and reliability, give the Cloud service customer the tools and opportunity to make informed choices and to gain an understanding of the service being delivered. NIST's definition of Cloud Computing describes a "Measured Service" as being one of the five essential characteristics of the Cloud Computing model. To describe a "measured service", one needs to identify the Cloud service properties that have to be measured and what their standards of measurement or metrics are.
"Cloud Computing Reference Architecture", ISO/IEC 17788:2014 , 15 October 2014	The reference architecture includes the Cloud Computing roles, Cloud Computing activities, and the Cloud Computing functional components and their relationships.
Special Publication 800-146, Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology/May 2012	This document reprises the NIST-established definition of Cloud computing, describes Cloud computing benefits and open issues, presents an overview of major classes of Cloud technology, and provides guidelines and recommendations on how organizations should consider the relative opportunities and risks of Cloud computing
Federal Cloud Computing Strategy. Federal CIO/8 February 2011.	Articulates benefits, considerations and tradeoffs of Cloud computing; provides a decision framework, highlights Cloud computing implementation resources, identifies government activities and roles for catalyzing Cloud adoption.
Updated Guidance on the Acquisition and Use of Commercial Cloud Services. DoD CIO Policy Memo	Allows DoD components to acquire Cloud services directly. Directs FedRAMP as the minimum security baseline, adherence to DoD Cloud Computing Security Guide,, requires DISA to review CSPs interested in hosting Sensitive Data, requires a DISA provided Cloud Access Point for Sensitive Data, holds Components responsible for Cyber Defense and sharing of Cyber defense information
"Cloud Computing Overview and Vocabulary", ISO/IEC 17789:2014, 15 October 2014	This Recommendation / International Standard provides an overview of Cloud Computing along with a set of terms and definitions. It is a terminology foundation for Cloud Computing standards. Applicable to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations).

Table C- 2. Case Studies and Examples

Reference	Brief Description
DISA SLA Template	Contains detailed specific metrics spelled out. All references circa 2012 or earlier and includes a suggested format for a weekly Operations Report, which will be used to verify compliance with, the SLAs. It is the basis for creating effective Cloud Computing contracts for the federal government.
NASA'S progress in adopting Cloud-computing Technologies, Office of Audits. 29 July2013.	An audit whose objective was to evaluate the efficacy of NASA's efforts to shift from a Private Cloud to Public Cloud offerings. The report evaluated whether NASA had implemented: 1. An Agency-wide governance model with processes to manage life-cycle activities for transitioning to a Cloud-computing model for delivery of IT services 2. Practices to evaluate security and risks within the Cloud-computing model along with the appropriate control mechanisms that reduce these risks to acceptable levels.
"*Concept Of Operations (CONOPS) for Cloud computer network defense (CND)", 3Apr2015*	This Cloud Computer Network Defense (CND) CONOPS defines a set of reporting and incident handling procedures for the 64 organizations that will defend the DODIN in the Cloud, as specified in the Cloud Computing SRG's 65 section on Computer Network Defense and Incident Response. These CONOPS define how Mission 66 Owners, Mission CND, Boundary CND, CSPs, and JFHQ-DODIN cooperate in 67 response to cyber incidents and events in accordance with CJCSM 6510.01B and provides complementary SLA guidance
DHS Security Architecture Appendix: Secure Cloud Computing Version 1.0 July 20, 2012	The DHS Secure Cloud Computing Architecture Appendix to the DHS Enterprise Security Architecture (ESA) discusses adoption of Cloud Computing architectures, their underlying and supporting technologies and the various Cloud deployment models. It addresses Cloud security challenges and vulnerabilities and makes recommendations for mitigating identified vulnerabilities and weaknesses, or when more practical, provides suggestions for avoiding less secure practices that could incur or increase risks.
Office of Inspector General U.S. Postal Service: Management of Cloud Computing Contracts Environment Audit Report September 2014	This audit reviewed Cloud computing contracts with a goal of getting insight in to in to how well the federal government is protecting its data, progress towards adopting Cloud computing and Cloud service contracts compliance with applicable standards and evaluation of management's efforts to adopt Cloud computing technologies. The audit found that the Postal Service's Cloud Computing contracts did not comply with all applicable Postal Service's standards.

Table C- 3. Contracts and Acquisition

Reference	Brief Description
Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. Queen Mary School of Law Legal Studies, September 2010.	Cloud computing offers an attractive solution to customers keen to acquire computing infrastructure without large up-front investment, particularly in cases where their demand may be variable and unpredictable. But the greater flexibility of a Cloud computing service as compared with a traditional outsourcing contract is balanced by less certainty for the customer in terms of the location of data placed into the Cloud and the legal foundations of any contract with the provider. This paper reports on a detailed survey and analysis of the Terms and Conditions offered by Cloud computing providers.
"Creating Effective Cloud Computing Contracts for the Federal Government", CIO Council/Chief Acquisition Officers Council, 24Feb2012.	This paper is the next step in providing Federal agencies more specific guidance in effectively implementing the "Cloud First" policy and moving forward with the "*Federal Cloud Computing Strategy*" by focusing on ways to more effectively procure Cloud services within existing regulations and laws. Since the federal government holds the position as the single largest purchaser in this new market, Federal agencies have a unique opportunity to shape the way that Cloud Computing services are purchased and consumed.
"Management of Cloud Computing Contracts and Environment", Postal Service, Office of Inspector General, 4Sep2014.	Objectives were to determine if the U.S. Postal Service's Cloud service contracts comply with applicable standards and evaluate management's efforts to adopt Cloud Computing technologies. The Postal Service's Cloud Computing contracts did not comply with all applicable Postal Service's standards. Specifically, the Postal Service has not defined "Cloud Computing" and "hosted services," established an enterprise-wide inventory of Cloud Computing services, required suppliers and their employees to sign non-disclosure agreements, or included all required information security clauses in its contracts. In addition, management did not appropriately monitor applications to ensure system availability. Management also did not complete the required security analysis process for three Cloud services reviewed and did not follow Postal Service policy requiring CSPs to meet federal government guidelines. This occurred because no group is responsible for managing Cloud services, and personnel were not aware of all policy and contractual obligations. Without proper knowledge of and control over applications in the Cloud environment, the Postal Service cannot properly secure Cloud Computing technologies and is at increased risk of unauthorized access and disclosure of sensitive data. We claimed $33,517,151 in contractual costs for the Postal Service not following their policy and contract requirements.

Table C- 4. Emerging Topics

Reference	Brief Description
"A Decision Process for Applying Cloud Computing in Federal Environments", Raines/Pizette, MITRE, 2010	This paper defines an engineering decision process for applying Cloud Computing services in a federal government context and explores important activities such as: Scoping a Cloud capability effort Determining which Cloud services will benefit an organization Establishing a business case for Cloud services Defining detailed requirements for Cloud services Determining when to use internal Private Clouds or external Public Clouds Assessing when to use community Cloud offerings provided by other government entities Understanding when it is appropriate to design and build an internal Private Cloud.
"Introducing CSMIC SMI: Defining Globally Accepted Measures for Cloud Services" (http://csmic.org/)	There is growing popularity for adopting Cloud Computing and a trend toward outsourcing IT-enabled services. Senior decision-makers, especially CIOs are concerned about the impact of this change on their ability to select and manage service providers who will meet their requirements and deliver high performance. While there may be obvious operational, cost and other benefits, selecting the right provider(s) in the absence of standard measures that allow for objective comparison of their capabilities, puts IT leaders and their organizations at risk of missing the full value of Cloud services.

Table C- 5. Security

Reference	Brief Description
"Security Guidance for Critical Areas of Focus in Cloud Computing, V3.0" Cloud Security Alliance	The aim of this guide is to provide a practical reference to help enterprise information technology (IT) and business decision makers analyze the security implications of Cloud Computing on their business. The paper includes a list of steps, along with guidance and strategies, designed to help these decision makers evaluate and compare security offerings from different Cloud providers in key areas.
"Proposal for standard Cloud Computing Security SLAs – Key Metrics for Safeguarding Confidential Data in the Cloud", *Author: Michael Hoehl, mmhoehl@gmail.com*	This document explores Security SLA standards and proposes key metrics for customers to consider when investigating Cloud solutions for business applications.
"One Cloud Does Not Fit All: Adopting a Secure Cloud for Government", Scott Renda, OMB, 13May2014	Provides factors to consider in Cloud type, and deciding on what to send to the Cloud: Cost Platform maturity Volume of data or network bandwidth requirements Connectivity and availability Public CSP's support Security
"Security for Cloud Computing - Ten Steps to Ensure Success, Version 2.0", Cloud Standards Customer Council, March 2015.	The aim of this guide is to provide a practical reference to help enterprise information technology (IT) and business decision makers analyze the security implications of Cloud Computing on their business. The paper includes a list of steps, along with guidance and strategies, designed to help these decision makers evaluate and compare security offerings from different Cloud providers in key areas.
"DEPARTMENT OF DEFENSE (DoD) CLOUD COMPUTING SECURITY REQUIREMENTS GUIDE (SRG)", Version 1, Release 1, 12 January 2015, Developed by the Defense Information Systems Agency (DISA) for the Department of Defense (DoD)	Provides security requirements and guidance to non-DoD owned and operated CSPs that wish to have their service offerings included in the DoD Cloud Service Catalog. Establishes a basis on which DoD will assess the security posture of a non-DoD CSP's service offering, supporting the decision to grant a DoD Provisional Authorization (PA) that allows a non-DoD CSP to host DoD missions. Defines the policies, requirements, and architectures for the use and implementation of commercial Cloud services by DoD Mission Owners. Provides guidance to DoD Mission Owners and Assessment and Authorization officials (formerly Certification and Accreditation) in planning and authorizing the use of a CSP.

Table C- 6. Cloud General

Reference	Brief Description
"Cloud First Consumer Guide", Beacon Report	Which IT programs and applications are going to the Cloud and why? If the move to the Cloud is boosting efficiency or providing other benefits? What hurdles migration has presented and whether the efforts have proved successful? What types of vendors are yielding reliable results in the Cloud? What guidance and recommendations can agencies offer now that they are well on their way to the Cloud?
"5 Things You Need to Ask When Planning for the Hybrid Cloud", GameChanger.	Here are five questions that every agency IT person should ask during a journey to the hybrid Cloud: 1. Will my hybrid Cloud implementation scale as our agency's needs grow? 2. How reliable is our hybrid Cloud? 3. Is our hybrid Cloud as secure as it can be? 4. How easy is it to move between Clouds? 5. How much visibility and control will we have?

Table C- 7. SLA General

Reference	Brief Description
Practical Guide to Cloud SLAs Version 2.0, Cloud Standards Customer Council, April 10, 2012	Provides a practical reference to help enterprise IT and business decision makers as they analyze and consider SLAs from different CSPs. Provides guidance on what to expect and what to be aware of as they evaluate SLAs from their Cloud Computing providers. Provides a checklist of key criteria for evaluating and comparing SLAs from different providers. Gives a 10-step process for evaluating Cloud SLAs: 1. Understand roles and responsibilities 2. Evaluate business level policies 3. Understand service and deployment model differences 4. Identify critical performance objectives 5. Evaluate security and privacy requirements 6. Identify service management requirements 7. Prepare for service failure management 8. Understand the disaster recovery plan 9. Define an effective governance process 10. Understand the exit process
"Best practices to develop SLAs for Cloud computing", Judith Myerson, IBM, 7Jan2013	This article recommends a standardized approach to developing SLAs that can be agreed to by all partners and suggest that there are three (3) new terms that should be considered for inclusion in SLAs: user threshold level, data requests threshold level and resources threshold level. *Knowing who sets the threshold levels is important when the consumers evaluate the SLAs.*
"Public Cloud Service Agreements: What to Expect and What to Negotiate", Cloud Standards Customer Council, 30Mar2013	This paper provides Cloud consumers with a pragmatic approach to understand and evaluate Public Cloud service agreements. The recommendations in this paper are based on a thorough assessment of publicly available agreements from several leading Public Cloud providers.
"CLOUD SERVICE LEVEL AGREEMENTS - Meeting Customer and Provider needs", Eric Simmon, NIST, 28 Jan 2014	This presentation discusses the NIST Cloud Computing Roadmap Requirements priorities related to SLAs: ***Requirement 3***: Develop Technical specifications to enable development of consistent, high-quality SLAs. Develop a controlled and standardized vocabulary of Cloud SLA terms and definitions. Ensure consistency in guidance and policy regarding SLA relevant terms and definition. **Requirement 10**: Define and implement Cloud service metrics. Standardize Units of Measurement for Cloud services. This presentation also talks about the challenges with current SLAs, a three-part decision process for laying out requirements for the Cloud service, and discusses a CSMI to be used to assess a Cloud service Incorporate Cloud Service Units of Measurement consistently in SLAs. It also goes over standardized approach for developing metrics definitions and formats

Reference	Brief Description
Recorded Webinar (panel discussion): Cloud SLAs: What You Should Be Asking Distributed Management Task Force," April 17, 2013 http://dmtf.org/education/webinars	April 2013 panel discussion hosted by Distributed Management Task Force in which experts provide some considerations on what to ask Cloud providers when evaluating their SLAs.
"Enabling End-to-End Cloud SLA Management", Frameworx Best Practice, October 2014, TMForum.	The purpose of this document is to demystify the processes and methodologies to establish Cloud SLA and to identify interoperable standards required to facilitate end-to-end Cloud SLA management in a complex Cloud ecosystem. This Technical Report (TR178), while organized by the TM Forum, takes an outside-in look by reviewing existing relevant industry work (DMTF, OGF, NIST, CSMIC, ITU-T, ISMA, OASIS and other), then compared with the best practices from the TM Forum SLA management Handbook [TMF GB917] which has been developed over the last decade for the communication service providers. It then recommends a set of business considerations, architecture design principles and standards that are required for managing SLA end-to-end in this highly dynamic Cloud ecosystem.