Project Planning and Management (PPM) V2.0

Project Type Guide

Software-as-a-Service

Version 1.1

January 2014

Project Type Guide

Summary: Software-as-a-Service (SaaS)

In exploring new Information Technology (IT) models to drive enterprise consolidation and shared services, the Software-as-a-Service (SaaS) model for application hosting and deployment offers the potential for increased efficiency, lower costs, and shorter implementation schedules. For the purposes of this guide, SaaS is defined as software deployed as a hosted service and accessed over the Internet. SaaS solutions generally enable agencies to quickly and easily acquire essential business applications without significant up-front capital investments in hardware, perpetual software licenses, or application development costs. This option allows for variability of fixed costs. Moving to a SaaS model offers agencies the opportunity to implement solutions on-demand: pay by the drink/pay by the user. On-demand solutions have historically allowed organizations to avoid extended deployment cycles with added consulting, maintenance, and support costs over time. Other common terms for SaaS applications are: hosted software, on-demand software, or cloud computing. In all cases, SaaS providers run the applications on their servers and provide managed and controlled access to the applications.

It is assumed that HUD will most often be a consumer of a SaaS solution.

Other Related Approaches: Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS)

Platform-as-a-Service is a model for running applications without the bother of maintaining the hardware and software infrastructure. Enterprises of all sizes have adopted PaaS solutions for simplicity, scalability, and reliability. PaaS eliminates the expense and complexity of evaluating, buying, configuring, and managing all the hardware and software needed for custom-built applications. In the PaaS model, cloud providers deliver a computing platform typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offerings, the underlying computer and storage resources scale automatically to match application demand such that the cloud user does not have to allocate resources manually.

In the most basic cloud-service model, providers of Infrastructure-as-a-Service (IaaS) offer computers - physical or (more often) virtual machines - and other resources. IaaS is a model in which an organization outsources the equipment used to support operations, including storage, hardware, servers, and networking components. The service provider owns the equipment and is responsible for housing, running, and maintaining it. The customer organization typically pays on a utility computing basis. To deploy their applications, cloud users install operating system images and their application software on the cloud infrastructure. In this model, the cloud user patches and maintains the operating systems and the application software.

At HUD, the usage of these two types of cloud computing options is in its infancy. At this point, project type guides will not be developed for these models. If HUD chooses to follow an IaaS or PaaS model as a solution, the project team should work with the Office of Customer Relationship and Performance Management (OCPRM) within OCIO to tailor the Project Planning and Management (PPM) Life Cycle accordingly.

Why Tailor the Project Planning and Management Life Cycle for the SaaS Project Type

The PPM Life Cycle was developed as HUD's standard for IT program and project governance. Part of the value of this process includes the ability to tailor it when needed to accommodate the various ways of deploying technology solutions. For each project type certain artifacts may become more important or less important, which is where tailoring opportunities exist.

The degree of tailoring will vary based on the amount of vendor resources, services, and tools needed to implement the hosted application. For example, a SaaS application that requires no data conversion activities and no configuration of screens or reports will require fewer artifacts than a SaaS application that does. With SaaS applications, it may be as simple as the vendor provisioning HUD system administrators and activating the hosted system licenses.

PPM Guidance and SaaS

IT project governance (like PPM) exists not only to ensure the required information is documented and provided to justify financial investment in a project, but to guarantee that proactive risk management exists throughout the project. With a SaaS approach for technology solutions, the assumption is no different. However, with SaaS, IT and business resources are offered a great deal of agility on project execution which can prove hard to manage with historical IT governance processes. As you will see in the artifacts required for SaaS, a great deal of importance is placed on the security and privacy artifacts as government-owned data (potentially) will be managed offsite within a non-government entity's infrastructure and relevant applications. Outsourced and public SaaS clouds perform more application-level logic at provider facilities compared with traditional computing and software distribution solutions. Listed below are important things to keep in mind for SaaS projects.

SaaS Projects – Things to Keep in Mind

- The agility of a SaaS solution may be attractive to the business such that the business moves forward alone to resolve pressing business needs resulting in a failure to get IT involved.
- SaaS projects can start small and grow big, affecting issues such as data duplication, identity management, incident management, and integration.
- SaaS appears to be cost effective but lacks maturity on total cost of ownership models used for the approach, which may impact the ROI.
- An organization's current architectural structure may not have the capacity to accommodate SaaS services.
- An organization using SaaS is outsourcing the operational aspects of its software and incomplete Service Level Agreements (SLAs) may impact agency expectations on SaaS vendor performance. Strong emphasis must be placed on vendor management.
- With SaaS, there is significant HUD responsibility to ensure security and privacy standards exist and are continuously met (need to determine boundaries where SaaS vendor security responsibilities end).
- SaaS projects must ensure that the right security levels and access policies are consistently applied.
- Vendor selection and contingency planning should address general interoperability and portability if moving from one vendor to another or back to an internal solution ("disentanglement").
- SaaS projects need to consider and plan for the potential complexity and risks associated with data management, security, and privacy (potential loss of data or data breach).
- The funding and budget process moving from a capital investment to an operational expense is not always easy in a government environment.

- SaaS projects may lead to a potential loss of agency control of provisioning and operational processes from personnel practices through data handling practices, and policies/operational procedures.
- A SaaS solution often means limitations in flexibility for customer configuration and customization.
- Network latency may differ compared to performance within internal enterprise networks.

The following table depicts the tailored PPM approach for Software-as-a-Service technology projects. This should be used as a starting point and should be modified as needed per the particulars of the project.

Artifact	Rationale/ Comments
Initiation Phase – Project Validation Review	
Project Initiation Form	The Project Initiation Form is required for all projects. This document references original funding approval and alerts OCIO that the business is ready to begin the approved project.
Project Charter	The Project Charter is required for all projects and includes Integrated Project Team (IPT) content.
WBS/Project Schedule – High Level	The Project Schedule is required for all projects; this initial submission can be high-level but more detail is required during the Planning Phase due to project reporting and milestone reporting requirements.
Procurement Management Plan	The Procurement Management Plan addresses the project's strategy for managing acquisitions. The content serves as the roadmap for effectively planning and managing acquisitions and should document the types of contracts to be used, address contract risks, determine dates for deliverables, and coordinate with other processes, such as scheduling and performance reporting. Additionally, early identification of metrics to be used in managing and evaluating contractors helps to ensure that business needs are addressed through contract support. The Procurement Management Plan documents the project team's planned approach prior to engagement with HUD's Office of the Chief Procurement Officer (OCPO). OCPO will assist the project with developing an Acquisition Plan for the actual acquisition itself (if needed). The investment-level Acquisition Strategy, part of the annual OMB 300 business case process, should be in alignment with the Procurement Management Plan and acquisition-specific Acquisition Plan(s). Note that projects consisting of more than one contract will complete multiple Acquisition Plans over the duration of the project as part of HUD's acquisition process. A Procurement Management Plan is required for projects that consist of more than one contract. If only one contract is being used for a project, the project team can complete the Procurement Management component of the Project Management Plan in lieu of a standalone Procurement Management Plan. An Acquisition Plan will also be created as part of HUD's acquisition process.
Planning Phase – Project Baseline Review	
Project Tailoring Agreement	This document is required for all projects and documents which PPM artifacts the project will be completing; the SaaS version will be used as the starting point for any additional tailoring opportunities.
Project Management Plan (PMP)	The Project Management Plan (PMP) serves as the primary source of information for planning, executing, monitoring, controlling, and closing a project. It provides detailed plans, processes, and procedures for executing, managing, and controlling project life cycle activities. It provides necessary information to improve the level of

	communication and understanding between all project team members and stakeholders, and may consist of other subsidiary management documents. For the SaaS project type, the content of the subsidiary management document (e.g., Communications Management Plan, Risk Management Plan, Requirements Management Plan, and Quality Assurance Plan) may be incorporated into the PMP in lieu of a separate subsidiary management document. Use good judgment when making this decision – if the SaaS solution is of high mission criticality or is a large effort cost-wise, it is important to consider retaining some of the documents as separate subsidiary management documents.
Requirements Definition/ Concept of Operations Document	This document is required for all projects and defines the detailed project/solution requirements. For SaaS project types, relevant content from the Concept of Operations (CONOPS) PPM template can be included as an initial section of the Requirements Definition document. A CONOPS depicts high-level requirements that provide a mechanism for users to describe their expectations of the solution. Use good judgment when making this decision – if the SaaS solution is of high mission criticality or is a large effort cost-wise, it is important to consider a separate CONOPS.
Requirements Traceability Matrix (RTM)	According to leading practices, the development of an RTM is intended to link business needs outlined in high-level requirements to more detailed requirements. Traceability refers to the ability to follow a requirement from origin to implementation and is critical to understanding the interconnections and dependencies among the individual requirements and the impact when a requirement is changed. Further, using attributes (e.g. unique identifier, priority level, status, completion date) in the matrix helps define the requirement to ensure traceability. Establishing and maintaining traceability is important for understanding the relationship between and among requirements – from business requirements initially established to the test cases executed to validate the resulting product.
Risk Management Log	This document is required for all projects; content within this document will feed the annual OMB 300 submission as it asks for project-level risks.
Independent Verification and Validation Plan (IV&V Plan)	An IV&V Plan describes the approach for having an independent third party check that the solution/service meets specifications and that it fulfills its intended purpose. Verification ensures that the solution was selected according to the requirements and other specifications, while validation ensures that the delivered solution/service actually meets the customer's needs and that the specifications were correct in the first place. Validation confirms that the product, as provided, will fulfill its intended use. IV&V activities are critical components of a sound quality management process. Currently at HUD, IV&V guidance is being revised. When the new guidance is finalized, this content will be updated to reflect new requirements.
Solution Architecture Document	Enterprise Architecture best practice is that all applications and systems must fit within the overarching architectural plan. HUD's enterprise architecture is flexible enough to incorporate SaaS and various types of solutions. The Solution Architecture document will depict the initial and future relationship between the SaaS solution and HUD's enterprise architecture.
FIPS 199 **Note: This requirement may vary depending on the categorization and type of information in the system. Security IPT members will*	FIPS Publication 199 defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest.

help determine if this artifact is needed based on the particulars of the SaaS application.	
Initial Privacy Assessment **Note: This requirement may vary depending on the type of information in the system. Privacy IPT members will help determine if this artifact is needed based on the particulars of the SaaS application.*	An Initial Privacy Assessment (IPA) is a required document designed to assess whether a Privacy Impact Assessment (PIA), a Privacy Act system of records notice (SORN), and/or other related privacy documents are required. The responses to the IPA will provide a foundation for both a PIA and a SORN should either or both be required, and will also help to identify any policy concerns.
System of Records Notice **Note: This requirement may vary depending on the type of information in the system. Privacy IPT members will help determine if this artifact is needed based on the particulars of the SaaS application.*	This document may or may not be needed based on the answers to the IPA. A System of Records is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. The Privacy Act requires each agency to publish notice of its systems of records in the Federal Register. This notice is critical to the production of the system, and is generally referred to as a system of records notice (SORN).
Privacy Impact Assessment **Note: This requirement may vary depending on the type of information in the system. Privacy IPT members will help determine if this artifact is needed based on the particulars of the SaaS application.*	This document may or may not be needed based on the answers to the IPA. Any new system that will contain personal information on members of the public requires a PIA, per OMB requirements (this covers both major and non-major systems).
Execution & Control Phase – Operational Readiness Review and As Needed Reviews	
Technical Design Document (TDD)	A SaaS implementation will typically require less design effort and decision-making given that the web-based software already exists and may not allow for customization or significant configuration. SaaS implementation efforts, however, may still require design activities to ensure that data conversion and implementation methodologies and tools are defined and that system interfaces are designed (if applicable). This artifact may not be required depending on the nature of the solution.
Interface Control Document (ICD)	The ICD presents the information required to define the SaaS application interface(s) with other systems located within HUD's infrastructure (if applicable), as well as any rules for communicating with those interfacing systems. The ICD communicates all possible inputs to and outputs from the application and describes the interface(s) (not the characteristics) of the systems that use them to connect. This document will not be needed if there are no interfaces with other systems. If interfaces exist and if the SaaS solution is inside the HUD boundary, then an ICD is needed. If it is not within the HUD boundary, then the requirement for an Interconnection Security Agreement (ISA) may be triggered. It is best to consult with the Security IPT member on proper direction.
Change Management Log	The Change Management Log contains information regarding any potential change to the scope, schedule, resources, etc. for the project. The document is maintained over the course of the project.
Implementation Plan	The Implementation Plan is an outline of the activities necessary to ensure that the solution/service is available for use by its end users as originally planned. The Implementation Plan addresses all necessary software, hardware, data, documentation, training, and required process/organizational changes. Training may

	be minimal but the plan/approach should be documented within the Implementation Plan. From a risk management perspective, training helps ensure end user adoption and usage of solution. Use good judgment when making this decision – if the SaaS solution is of high mission criticality, affects many users, or is a large effort cost-wise, it is important to consider a separate Training Plan.
Test Plan & Test Reports	Test planning is the practice of preparing for the testing phase of product development/configuration to ensure that the solution/service satisfies the client's requirements as agreed upon in the requirements and design specification documents. Test Reports summarize the results of the different types of testing performed for an automated system (e.g. unit testing, system testing, user acceptance testing, ad hoc testing, regression testing, performance and/or stress testing, and end-to-end testing). If the SaaS application requires effort on HUD's side for integration and/or adding functionality to HUD applications, then testing will be required on that functionality and any interfaces, etc. If the vendor is only performing activities such as provisioning HUD system administrators and activating the hosted system licenses, then testing is minimal (conducted by the vendor) and no artifact is required. Be aware that with a SaaS application, periodic vendor releases may entail minimal testing activity on the customer side. These artifacts may or may not be applicable based on the particulars of the SaaS solution. At the minimum, the project should produce SaaS application compliance with Section 508 rules (often provided by the SaaS vendor).
Data Conversion Plan	SaaS implementations tend to be simpler and thus the data conversion process is usually more condensed. That is, the standard process for SaaS data conversion is to convert the data once and to convert only baseline information. More detailed data imports can be done but are typically outside the norm. This document will not be needed if there is no initial migration/ conversion of data to the SaaS application.
User Manual	The User Manual is written using non-technical language and should include the key features and/or functions of the solution/service. The manual should explain how a business user operates the solution and should include sufficient detail and plain language such that all levels of business users can easily understand how to use the solution/service.
Security Assessment and Authorization to Operate (ATO) Request **Note: This requirement may vary depending on the type of information in the system. Security IPT members will help determine what artifacts are needed based on the particulars of the application.*	Information systems software, hardware, and equipment developed by or sold to Federal agencies must undergo a security assessment and receive an Authorization to Operate (ATO) before the system is operational. This is a mandatory requirement. The SaaS provider should produce this documentation for the project. The process was recently revised and now culminates in the signing of the ATO request by HUD's Chief Information Security Officer (CISO). For SaaS applications, the Security IPT member will provide the latest guidance from the HUD Chief Information Security Officer (CISO) on the security assessment and ATO requirements for a SaaS solution, which will likely depend on the boundary of the system. Generally, the package will include information such as: 1) System Security Plan: Provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements. OMB requires all Federal agencies to incorporate a security plan that is consistent with NIST guidance on security planning.

	2) Security Risk Assessment: Provides the inputs for the development of the Security Plan. 3) Security Test and Evaluation Plan/Report: Security Test and Evaluation (ST&E) (often times referred to as Certification Test & Evaluation) is a requirement within all Certification and Accreditation (C&A) processes. ST&E is the Independent Verification and Validation (IV&V) of a security control on a system to determine if it was properly implemented and if it is working correctly. While providing this service, organizations must leverage a variety of standards such as NIST 800-115 to properly perform the testing. 4) Business Impact Analysis (BIA): The BIA is a key step in the contingency planning process. The BIA enables the project team to fully characterize the system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities. The purpose of the BIA is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components. Key steps are listing critical IT resources, identifying disruption impacts and allowable outage times, and developing recovery priorities. 5) Contingency Plan: Contingency planning establishes thorough plans, procedures, and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster. For SaaS applications, contingency planning also covers continuity of the system, getting full access to HUD's data, and questions such as: • What happens if the SaaS provider goes out of business? • What if the provider terminates the contract? • What happens if the solution owner wants to switch providers? *Note: A potential, emerging approach worth investigating based on the functionality and mission criticality is software escrow. Traditionally, software escrow is a service whereby a trusted third-party has access to the vendor's source code and the customer's software license agreement allows the customer to gain legal access to* said source code in the event of business failure by the vendor. 6) E-Authentication Risk Assessment: OMB requires agencies to review new and existing electronic transactions to ensure the authentication processes provide the appropriate level of assurance. Criteria for an e-authentication application include: 1) is web-based 2) requires authentication 3) extends beyond the borders of the enterprise (e.g. multi-agency, government-wide, or public facing). 7) Memorandum of Understanding (MOU): The MOU defines the responsibilities of the participating organizations involved with a system interconnection. The organizations that own and operate the connected systems should establish an MOU that defines the responsibilities of both parties in establishing, operating, and securing the interconnection. 8) Interconnection Security Agreement (ISA): The ISA is a security document that specifies the technical and security requirements for establishing, operating, and maintaining a system interconnection with an external information system, i.e., residing outside the HUD infrastructure. A system interconnection is defined as the direct connection of two or more IT systems for the purpose of sharing data and other information resources. ISAs are used for planning, establishing, maintaining, and terminating interconnections between IT systems that are owned and operated

	by different organizations, including organizations within a single Federal agency. 9) Authorization to Operate (ATO) Request: All IT systems are required to obtain a signed ATO prior to full start up. For SaaS applications, the Security IPT member will provide the latest guidance from the HUD Chief Information Security Officer (CISO) on whether or not the ATO is required for a SaaS solution, which will likely depend on the boundary of the system. The ATO represents the formal management approval to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets based on the implementation of an agreed-upon set of security controls.
Close Out Phase – Project Close Out Review	
Project Completion Report	This document finalizes project activities and includes lessons learned content for the benefit of subsequent projects which is especially important for SaaS projects since HUD is only starting to deliver projects via this method. It also asks for information on project administrative and contract closure activities. The Project Completion report should be supplemented with how the project worked with the SaaS provider to obtain periodic and frequent reporting on usage depending on the subscription method (number of users, "by the drink," etc.). It should also be supplemented with the plan for how HUD will track contractual SLAs.

Guidance on Software-as-a-Service and Using Federal IT Shared Services

In May 2012, OMB released the Federal IT Shared Services Strategy to provide agencies with guidance for identifying and operating shared services for commodity, support, and mission IT functions. That strategy recommended a phased approach for implementing shared services, (e.g., "crawl-walk-run") beginning with intra-agency commodity IT, to allow agencies to gain proficiency and then evolve to support and mission IT areas.

Shared-First is a transformational government business model aimed at rooting out waste and duplication across the Federal IT portfolio which encompasses a number of initiatives: CIO authorities, procurement reform, PortfolioStat, and IT shared services strategy. It is a compelling approach for Federal agencies today that are facing growing mission requirements in an environment of declining resources. Shared-First drives organizations to provide service delivery of equal or higher quality at equal or lower costs. Identifying and pursuing opportunities for shared services is one method to reduce operating costs by leveraging shared platforms and service delivery.

If, through the course of an alternatives analysis, a decision to transition to a Federal shared service solution is made, then a project team needs to be formalized to proceed with developing a project plan and negotiating the Service Level Agreement (SLA) and/or Interagency Agreement (IAA). Both business and IT staff should participate in this effort. Refer to http://cio.gov/wp-content/uploads/downloads/2013/04/CIOC-Federal-Shared-Services-Implementation-Guide.pdf for the most recent guidance on shared service implementations.

There are several methods that consuming agencies may use to fund shared services. These methods are determined in part by the type of service being procured and the provider's offering. At HUD, a project will most likely take advantage of Interagency Agreements (IAA) and Service Level Agreements (SLAs). When HUD makes a decision to transition to an inter-agency shared service and has determined its funding approach, the customer/partner agency and shared service provider need to negotiate, agree, and formally document the services and service levels to be provided. The agreement needs to include, at a minimum, a project title, names of the parties to the agreement, the purpose of the agreement, a "programmatic" authority for all Federal parties, the duration of the agreement, a termination provision, a dispute resolution provision, contacts for the

parties, and signatories for the parties. If funding will be transferred from one agency to another, then the agreement also needs to contain an authority to transfer funds, the amount being transferred, and a clause describing collection of costs upon cancellation.

This information is provided in one of several types of agreements: (a) Memorandum of Understanding (MOU); (b) Memorandum of Agreement (MOA); and (c) Interagency Agreement (IAA).

Action	MOU	MOA	IAA
Establish a non-financial relationship	X	X	X
Order a service			X
Terms & Conditions			X
Requirements and Funding Information			X

Some agencies draw distinctions among different agreement types, while others focus only on the content in the agreement. Typically, a MOU or MOA may be used whenever there is agreement to exchange information or coordinate programs. Each party is responsible for contributing its own efforts and resources (sometimes characterized as "in-kind-contributions") and neither party exchanges funds, personnel, property, services, or any kind of financial commitment or obligation. A MOU is the more formal of the two and is used to discuss an agreement in a broad spectrum outlining the overall goal so it is clear, while a MOA identifies and appoints responsibility to the certain parties involved in a detailed manner to alleviate any ambiguity of who is to do what.

An IAA is used to document reimbursable agreements; when one Federal agency pays another Federal agency. OMB, the Office of Federal Financial Management, and the Financial Management Service (FMS) bureau of the Department of the Treasury have worked together to develop a standard IAA form. It is composed of two parts. The General Terms and Conditions Section is the partnership document of the recommended standard IAA that sets the relationship between the parties, and is similar in substance to a MOU or MOA. The Order Section contains specific information about the product(s)/service(s) being purchased based on a bona fide need, the buyer's funding information, accounting methodology, shipping information, and points of contact for the buyer and seller. For further guidance, refer to http://fms.treas.gov/finstandard/forms.html.

It is important to note that HUD requires the use of the standard IAA form as the Office of the Chief Procurement Officer (OCPO) uses it as its standard.

Below are some best practices to consider when drafting an agreement. In addition, guidance on how to negotiate an IAA is provided by the FMS bureau of the Department of the Treasury.

- **Formalize Communications** – The IAA should include processes and structure for regular ongoing, emergency and priority alerts, and escalation paths to be established.
- **Service Definition and Delivery** – The team should define the expected business outcome of the services first, and then set the SLA.
- **Governance and Performance Measurement** – The IAA should state contractually the frequency of service level reporting, which should be at least on a monthly basis depending on the service. The team should inquire about the use of online dashboards the service provider may offer to manage and track service delivery in near-real time.
- **Liability** – The IAA should consider cross-indemnification while insisting that the service provider provide all reasonable due diligence according to a set of industry standards (COBIT, ITIL, ISO, or other standards), and state that by not performing due diligence and adhering to an agreed-upon standard that the service provider may be open to liability.

- **Negotiate Incentives and Penalties** – The service provider should be driven to meet the established customer expectations and even exceed it by adopting performance-based pricing criteria. If performance of the service provider exceeds expectations, then incentives should be given; conversely, appropriate penalties should be imposed if objectives are consistently missed. One strategy for penalties and incentives in SLAs is for the service provider to put the penalty into a "bank" if there is an issue. As long as the service provider makes a determined effort and meets the SLA within an agreed-upon time limit (depending on the severity of the lapse and criticality of the service), the customer absolves the provider of the penalty.
- **Ensure a Return Path** – In case things do not occur according to expectations, the IAA should ensure there is an exit strategy. The reputation of the service provider is at stake and it will usually work with the customer to fix problems.
- **Termination Costs** – Limiting the amount of termination costs that will be paid is an incentive for the service provider to make the deal work and satisfy the customer in the initial transition years.

A separate but related document is the service level agreement (SLA). The SLA defines the performance measures the service provider agrees to follow. Service levels are derived from customer/partner agency requirements and the need to match service provider capabilities. The SLA is part of an overall service management approach and serves as a consistent interface to the business for all service- and performance-related issues. Service Level Management will help establish and enhance relationships and communication between the shared service provider and the customer/partner agency.

The SLA is typically incorporated by reference in the IAA. This helps to ensure that the service levels defined are part of the business arrangement between the service provider and customer.

Service Level Management entails several best practices that the service provider should have in place, including:

- Establishing and maintaining SLAs that document service level targets as well as roles and responsibilities of the service provider and the customer/partner agency;
- Measuring, reporting, and notifications on service performance vs. agreed upon service levels, and on service workload characteristics such as number of customer/partner agencies, volume, and resource utilization;
- Providing feedback on reasons and details of actions to be taken to prevent recurrence (e.g., in cases where service level targets are not met);
- Monitoring and improving customer/partner agency satisfaction with the services that are provided; and
- Providing inputs into service improvement plans.

OMB has established standard migration planning guidance for using Federal shared service providers and developing a standard SLA template. The link provided is for the Financial Management Line of Business: http://www.hud.gov/offices/cpo/contract/opc23053final/attachmnt/ATT16BFMLOBSLAOverview.pdf.