Project Planning and Management (PPM) V2.0

Project Type Guide

Commercial-off-the-Shelf (COTS)
Government-off-the-Shelf (GOTS)

Version 1.1
January 2014

Project Type Guide

Summary: Commercial-off-the-Shelf (COTS)/Government–off-the-Shelf (GOTS)

Commercial-off-the-Shelf (COTS) refers to *commercially-developed*, prepackaged software or hardware solutions that are typically purchased or leased from a third party vendor. A COTS product can be procured or utilized under a government contract in the same, precise form as the version available to the general public, and is then configured according to customer needs. **Government-off-the-Shelf** (GOTS) refers to software and hardware products that are developed and owned by a *government entity* and ready to use to meet unique Federal requirements. Both COTS and GOTS products provide an effective alternative to custom development and provide efficient and effective means for HUD to meet Federal Information Technology (IT) directives such as Shared First and Commodity IT.

Several COTS advantages include:

- Applications usually provided at a reduced cost
- More reliable when compared to custom-built software due to proven usage by other organizations
- System documentation provided with application
- Higher complexity since industry specialists developed the software
- Marketplace-driven application development and competition improves product quality

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

The Project Planning and Management (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 COTS/GOTS application. For example, the procurement and implementation of a new COTS application requires more effort and additional steps than the procurement of additional licenses for an existing COTS application. Additionally, project tailoring is beneficial since different COTS and GOTS applications will usually require different levels of configuration to meet program area needs.

PPM Guidance and COTS/GOTS Solutions

IT project governance (like PPM) exists not only to ensure 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 COTS/GOTS approach for technology solutions, the assumption is no different. However, with COTS or GOTS solutions, IT and business resources are saved substantial time and effort since the product usually needs only to be configured.

As you will see in the artifacts required for COTS/GOTS projects, a great deal of importance is placed on developing requirements and requirements analysis. Thorough requirements analysis ensures that the COTS/GOTS solution will address the business needs of the project. Additionally, substantial importance should be placed on proper analysis of the future solution architecture and interfaces, since COTS/GOTS solutions can present particular challenges for enterprise technology integration. That is why it is crucial for the project team to engage HUD's Enterprise Architecture team early on in the process to ensure the solution is in line with HUD's target architecture. Listed below are important things to keep in mind for COTS/GOTS projects.

COTS/GOTS Projects – Things to Keep in Mind

- The ability of a COTS/GOTS solution to effectively meet business needs is based on the accurate identification of solution requirements. Attention should be paid to thorough completion of the Concept of Operations, Requirements Definition, Requirements Traceability Matrix, and Solution Architecture documentation. If the program area is implementing multiple modules of a COTS/GOTS solution, it makes sense if some of the artifacts are at the system-as-a-whole level vs. the module level (if each module is being implemented as a separate project). For example, a Concept of Operations document provides the most value at the integrated solution level vs. the level depicting a smaller piece of the larger solution.
- The robust functionality of the COTS/GOTS solution is irrelevant if it does not meet most core requirements generated from the defined business need.
- Licenses for an existing COTS solution can be either enterprise-wide or based on user count with each option offering different pricing. IT Project Managers (IT PMs) should check with their Customer Relationship Coordinator (CRC) for assistance in finding out information on current licensing if leveraging an existing COTS solution.
- Since COTS/GOTS products are tried and tested in a commercial or government environment, their maintenance costs are often less than a custom-developed solution which requires thorough system testing.
- Since COTS/GOTS products require configuration rather than full scale development, they can often be implemented faster and at a lower cost than a custom-developed solution.
- A GOTS solution often demands less configuration than a COTS solution since it was developed by a Federal agency to meet unique Federal requirements and is already being leveraged in some way. Hence a GOTS implementation can be less risky than a COTS implementation.
- If sustainment or enhancement of the COTS/GOTS solution is delegated to a vendor, funds must be available in future years for continuing upgrades.
- Plan for life-cycle sustainment of all solutions, COTS or GOTS, up front. Requests for Proposals (RFPs) should state that a system will receive scheduled technology refreshes rather than assume a system is frozen in its original configuration.
- Agencies are increasingly leveraging Shared Services via the cloud as a cost-efficient and effective alternative to COTS services.

The following table depicts the tailored PPM approach for COTS/GOTS 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 (PIF)	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	The Procurement Management Plan addresses the project's strategy for managing

Plan	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 (PTA)	This document is required for all projects and documents which PPM artifacts the project will be completing; the COTS/GOTS 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 COTS/GOTS project type, the content of the subsidiary management document (e.g., Communications Management Plan, Risk Management Plan, Requirements Management Plan, 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 COTS/GOTS solution has a high mission criticality or is a large effort cost-wise, it is important to consider retaining some of the documents as subsidiary management documents.
Concept of Operations Document (CONOPS)	A CONOPS depicts high-level requirements that provide a mechanism for users to describe their expectations of the solution. The CONOPS is used as input to the development of formal testable system and software requirements specifications. A CONOPS provides the most value when depicting the integrated solution. So, if a program area is implementing a large system via a program which contains multiple projects within it, it would be expected that the CONOPS be produced at that program level to show how the entire system and its parts would operate.
Requirements Definition Document	This document is required for all projects and defines the detailed project/solution requirements (business, functional, technical).
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 installed and configured or built according to the requirements and design specifications, while validation ensures that the delivered solution actually meets the customer's needs and that the specifications were correct in the first place. Validation ensures that 'you built the right thing'. Verification ensures that 'you built it right'. 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	HUD applications must be in alignment with HUD's Enterprise Architecture. The Solution Architecture document will depict the initial and future relationship between the current solution and HUD's architecture. The document ensures that the COTS/GOTS solution architecture is in compliance with HUD enterprise architecture principles, best practices, and conceptual target application architectures. The target state includes business, enabling, and support services that are either re-used from the current portfolio, leveraged from existing enterprise services, or established as new services via projects to develop them.
FIPS 199 **Note: This requirement may vary depending on the categorization and type of information in the system. Security IPT members will help determine if this artifact is needed based on the particulars of the COTS/GOTS application.*	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.
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 COTS/GOTS 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*	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

particulars of the COTS/GOTS application.	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 COTS/GOTS 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)	The TDD describes the system requirements, operating environment, system architecture, subsystem architecture, files design, database design, input formats, output layouts, human-machine interfaces, detailed design, processing logic, and external interfaces for the IT system. For a COTS/GOTS implementation, this document would focus on details needed for appropriate configuration for integration with other systems.
Interface Control Document (ICD)	The ICD presents the information required to define the COTS/GOTS interface(s) with other systems located within the HUD 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 COTS/GOTS application in order to give the solution development team guidance to ensure the application fits well into its operating environment.
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 COTS/GOTS solution 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. The training plan/approach may be documented within the Implementation Plan. From a risk management perspective, training helps ensure end user adoption and usage of the solution. Use good judgment when making this decision – if the COTS/GOTS solution has a 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 of product development/configuration activities to ensure that the solution satisfies the customer'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 project teams are using automated tools to track and document testing activities, it is acceptable to substitute tool-specific test result reports if they meet the information requirements of the PPM template.
Data Conversion Plan	The Data Conversion Plan describes the strategy, preparation, and specifications for converting and/ or migrating data from the source system or systems to the new COTS/GOTS system.

User Manual	The User Manual is written using non-technical terminology and should include the key features and or functions of the solution. 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.
Operations and Maintenance (O&M) Manual	The O&M Manual contains information and strategies designed to guide stakeholders in the normal use and maintenance of the IT system. The manual facilitates actions and responses to events that may arise during normal solution operations and maintenance and contains detailed information on the control requirements, scheduling information, and operating procedures necessary to successfully initiate and run the solution. It also provides maintenance personnel with the information necessary to maintain the solution effectively. The manual provides the definition of the software support environment, the roles and responsibilities of maintenance personnel, and the regular activities essential to the support and maintenance of program modules, job streams, and database structures.
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 COTS/GOTS 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[1]. The COTS/GOTS provider should produce applicable 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). 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

[1] The Federal requirement for security assessments and Authorizations to Operate apply at the information system level and not necessarily at the software, platform, or operating system level. The requirement for an ATO may not apply to the COTS or GOTS tool if it is a component of a larger information system. For instance, Microsoft Office does not require a unique ATO because it is covered under the ATO for HUD's Local Area Network (LAN). Alternatively, HUD's personnel system, HIHRTS, is GOTS and is covered by the ATO from U.S. Treasury. The ATO decision depends on the boundaries for the information system under development. For more information, please see NIST SP 800-37 (http://csrc.nist.gov/publications/PubsSPs.html).

	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 COTS/GOTS applications, contingency planning also covers continuity of the product's availability and to questions such as: • What happens if the COTS/GOTS vendor or provider goes out of business and no longer supports the product? • What happens if the solution owner wants to switch COTS solutions? 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. An interconnection in a COTS/GOTS situation could, for example, be a link from the system to Pay.gov. 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. 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. It also asks for information on project administrative and contract closure activities.