Project Planning and Management (PPM) V2.0

Project Type Guide

Custom Development

Version 1.1

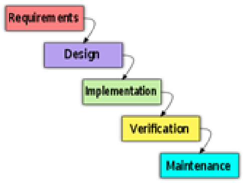
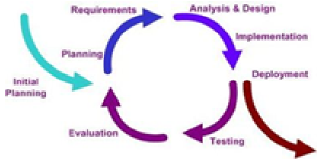
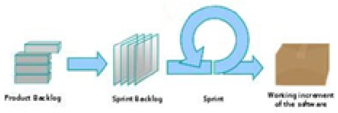
January 2014

Project Type Guide

Summary: Custom Development

Custom software development involves building an application from the ground up, rather than using an existing product to meet new user requirements. Existing products include Commercial-off-the-Shelf (COTS), Government-off-the-Shelf (GOTS), Software-as-a-Service (SaaS), and Federal shared service solutions. In the Federal government, as well as in the private sector, custom development is used less frequently than in the past because of the proliferation of commercially available alternative solutions that have already been used successfully by other organizations. Custom software development is now typically reserved for those requirements that cannot be met by currently available solutions.

The most popular approaches project teams take when delivering a custom-developed solution include:

	Waterfall	Iterative	Agile
Overview	▪ Majority of software features delivered in one release at the end (often after 3-12 months) ▪ Sequential process where each stage is completed before proceeding to the next  Requirements Design Implementation Verification Maintenance	▪ Working solution is extended and refined through a set of incremental changes ▪ Multiple releases managed in parallel with each at different points of development lifecycle  Requirements Analysis & Design Implementation Planning Deployment Initial Planning Evaluation Testing	▪ Adheres to basic Iterative principles (e.g., refinement of working solution) ▪ Places even greater emphasis on flexibility and co-development of product with product owner  Product Backlog Sprint Backlog Sprint Working increment of the software
Key differences	▪ No scope changes due to sequential execution of development phases ▪ Testing occurs once development is completed	▪ Scope is flexible but changes do not occur mid-sprint ▪ Testing occurs during defined phase at end of each iteration	▪ Scope changes occur at any time based on business feedback ▪ Testing is performed continuously during development
When to use	▪ Large, complex systems with high technical risk ▪ Rollout of new architecture/ replacement of core technologies ▪ Premium quality prioritized over predictable timelines	▪ Complex development tasks (e.g., front-end applications with numerous user interactions) ▪ Known technology/architecture ▪ Volatile/changing requirements ▪ Fast time to market required	▪ Numerous, small feature increments ▪ Known technology/architecture ▪ Volatile/changing requirements ▪ Fast time to market required

Source: NGMS Iterative Operating Model and Playbook, July 2013

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. The degree of tailoring will vary based on the amount of vendor resources, services, and tools needed to build and implement the application. For each project type certain artifacts may become more important or less important, which is where tailoring opportunities exist. For example, the development and implementation of a new custom-built software application requires a more extensive Requirements Definition document, Technical Design document, and testing documentation than other project types. In general, less tailoring opportunities will exist for this project type versus other project types due to the higher levels of risk typically involved in custom-developed solutions. Tailoring is to ensure that the right deliverables are created for the specific project type and that project teams are not doing extra work or activities to be compliant with something that is not relevant. For very small mini-applications that are custom-developed, the project team should review the Custom Development Project Tailoring Agreement and propose an approach to the TRC Sub-committee (TRC) for review and acceptance at the beginning of the Planning Phase.

PPM Guidance and Custom Development

IT project governance (like PPM) exists not only to ensure the required information is documented and provided to initially (and continuously) justify financial investment in a project, but to guarantee that proactive risk management exists throughout the project. With a custom development approach for technology solutions, the assumption is no different. However, custom development requires the most PPM deliverables as compared to a COTS/GOTS product which has been used by commercial and government clients and has been certified by the vendor prior to its sale.

As you will see in the artifacts required for custom development projects, a great deal of importance is placed on developing and documenting business, functional, and technical requirements, technical design, and the testing process and results. Thorough requirements, technical design, testing process, test plan, and test cases help ensure that the custom-developed solution will address the business needs of the project. Additionally, substantial importance should be placed on proper analysis of the solution architecture and interfaces. Early interface identification allows project team members to work proactively with other system owners impacted by the solution. Listed below are important things to keep in mind for custom development projects.

Custom Development Projects – Things to Keep in Mind

To develop a cost effective solution for HUD that meets both HUD's mission and stays within budget, all sources of reusable code, applications, cloud computing models, and COTS/GOTS software should be investigated prior to making a decision to custom-build code for the project. This best practice ensures the most cost-effective and efficient use of resources, and will decrease the number of duplicative and overlapping software systems. The choice to develop a customized application should be balanced against the availability of other solutions, project cost, resources, and time constraints. The theme used in arriving at any project type decision should be "reuse before you buy, and buy before you build." The analysis of alternatives is especially important as it relates to guidance in the past several years from OMB regarding usage of cloud computing and shared services solutions when looking to move forward with an information technology investment.

The following is a list of software alternatives that should be considered at a minimum:

- Commercial-off-the-Shelf (COTS) - Commercially-developed, prepackaged software or hardware solutions (see COTS/GOTS Project Type Guide)
- Government-off-the-Shelf (GOTS) - Software and hardware products that are developed and owned by a government entity (see COTS/GOTS Project Type Guide)
- Software-as-a-Service (SaaS) – Existing, commercially available software that can be accessed over the internet and purchased as a service or through shared services arrangements with other Federal agencies (see SaaS Project Type Guide)

Because of the risk involved in developing a custom-built software product, it is particularly important to complete a thorough analysis of alternatives which is documented in the Project Charter. The analysis of alternatives will help the project team decide on the best project type. Some of this analysis will likely have taken place during the budget formulation process in which the funding for the project was originally requested. The following are some typical factors that should be considered when making a decision about using custom development:

- Project scope and objectives
- Return on Investment (ROI) and payback period
- Users' computing environment
- High-level requirements
- Assumptions, constraints, and limitations
- Platform options
- Security and recovery objectives
- Risk factors
- Technological factors
- Available resources and budget
- Life Cycle Cost Estimate (LCCE)
- Future growth needs
- Expected long-term benefits
- Compliance with HUD IT Strategic Plan and Enterprise Roadmap

Once a decision has been made that custom software development is the best alternative, efforts should be made to reduce the risk inherent in developing a custom-built product. This includes considering development approaches in which functional components are designed, developed, tested, and user-accepted in a short time period. This is usually less risky than designing and developing the entire application over a long period of time before functionality can be tested and accepted by users.

HUD’s Application Release Process

The HUD Application Release Tracking System (HARTS) is an application used by the HUD development community as a means for creating application releases and checking their status throughout the release process. This application is also used by the HUD Test Center (HTC) staff for tracking LAN, Internet/Intranet, Client/Server, Lotus Notes, and Mainframe software releases into HUD's infrastructure. HARTS maintains release workflow and all associated documentation (Checklists, Instructions, Validation Verification Test (VVT) Plan, Test and Evaluation Report and Test Scripts).

All HARTS release requests must be submitted in advance and project teams should check the latest guidance referencing the recommended timeframe so that they can plan accordingly given their project timelines.

The following table depicts the tailored PPM approach for custom-developed 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 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 Custom Development version will be used as the starting point for any additional tailoring opportunities.
Project Management Plan (PMP)	The 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. With some project types, the content of the subsidiary management document (e.g., Communications Management Plan, Risk Management Plan) may be incorporated into the PMP in lieu of a separate subsidiary management document. Based on the scope, size, complexity, and duration of a custom-developed solution, this opportunity may exist as well, but should be reserved only for small development efforts with very fast deployment timeframes.
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	This document is required for all projects and defines the detailed project/solution

Document	requirements (business, functional, technical).
Requirements Management Plan	The Requirements Management Plan is used to document the information necessary for effectively managing project requirements from definition to delivery.
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 Plan (RMP)	A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project's objectives. Risk management is the process of identifying, assessing, responding to, monitoring and controlling, and reporting risks. The RMP defines how risks associated with the project will be identified, analyzed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the life cycle of the project. Effective risk management is critical to custom development projects as they typically have the highest risk profile of all project types.
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.
Quality Assurance Plan	The purpose of this document is to specify the quality assurance activities and responsibilities for ensuring that the project meets the user requirements and conforms to HUD's Information Technology Management (ITM) Framework.
Communications Management Plan	The purpose of this document is to define the communications goals and strategies of the project. Its overall objective is to promote the success of a project by meeting the information needs of project stakeholders and it outlines the goals of the communications efforts to reach and inform each group.
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 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 custom-developed 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 custom-developed 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 custom-developed 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 custom-developed 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 custom-developed 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. It presents and tracks the information required to develop an effective architecture and system design, giving the development team guidance on the architecture of the system to be developed. All systems must demonstrate traceability to the Federal Enterprise Architecture (FEA).
Interface Control Document (ICD)	The ICD presents the information required to define the 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 custom-developed application in order to give the design and 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 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.
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(s) to the new system.
Training Plan	The Training Plan describes the types of training that will be provided, how the training will be developed and delivered, the schedule, and any other information needed to ensure that users at all levels are prepared to use the system effectively.
User Manual	The User Manual is written using non-technical language 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 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 process was recently revised and now culminates in the signing of the Approval to Operate (ATO) request by HUD's Chief Information Security Officer (CISO). The artifacts required for the ATO package may vary based on the details of the custom-developed application. 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 custom-developed applications, contingency planning also covers continuity of the availability of the vendor who led the code development activities and to other questions:

- What happens if the custom development vendor goes out of business and no longer supports the product? How does knowledge transfer occur?
- What happens if the solution owner wants to switch to another solution?

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 custom development 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.