VistA Adaptive Maintenance VAEC Security (VAM)

Contractor Project Management Plan



Department of Veterans Affairs

Office of Information & Technology (OIT)

Contract No: VA118-16-D-1009

Task Order: 36C10B19F10090015

January 2020

Version 1.11

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 01/30/2020 | 1.11 | Final Contractor Project Management Plan | AbleVets |
| 01/03/2020 | 1.10 | Updated Contractor Project Management Plan | AbleVets |
| 12/03/2019 | 1.9 | Updated Contractor Project Management Plan | AbleVets |
| 11/04/2019 | 1.8 | Updated Contractor Project Management Plan | AbleVets |
| 10/03/2019 | 1.7 | Updated Contractor Project Management Plan | AbleVets |
| 09/03/2019 | 1.6 | Updated Contractor Project Management Plan | AbleVets |
| 08/02/2019 | 1.5 | Updated Contractor Project Management Plan | AbleVets |
| 07/03/2019 | 1.4 | Updated Contractor Project Management Plan | AbleVets |
| 06/03/2019 | 1.3 | Updated Contractor Project Management Plan | AbleVets |
| 05/03/2019 | 1.2 | Updated Contractor Project Management Plan | AbleVets |
| 04/03/2019 | 1.1 | Updated Contractor Project Management Plan | AbleVets |
| 03/04/2019 | 1.0 | Initial draft of the document | AbleVets |

CLIN Satisfaction Statement

This document is submitted in satisfaction of CLIN 0001AA.

Artifact Rationale

The Project Management Plan (PMP), according to the Guide to the Project Management Body of Knowledge (PMBOK®), is a formal, approved document used to guide both project execution and project control. The primary uses of the PMP are to document planning assumptions and decisions; facilitate communication among stakeholders; and document approved scope, cost, and schedule baselines. By showing the major products, milestones, activities, and resources required on the project, it is also a statement of how and when a project's objectives are to be achieved.

The project manager creates the PMP following input from the project team and key stakeholders. The plan should be agreed on and approved by at least the project team and its key stakeholders.

The PMP is mandatory for all projects. While it is a project-level document, it should be updated as necessary, including for each increment.

Table of Contents

[1. Introduction 1](#_Toc31114760)

[1.1. Project Overview 1](#_Toc31114761)

[1.2. Project Scope 1](#_Toc31114762)

[1.3. Goals and Objectives 3](#_Toc31114763)

[1.4. Technical Approach 3](#_Toc31114764)

[2. Project Organization 4](#_Toc31114765)

[2.1. Stakeholders and Key Personnel 5](#_Toc31114766)

[3. Testing 6](#_Toc31114767)

[4. Monitoring and Control Mechanisms 6](#_Toc31114768)

[4.1. Budget Monitoring 6](#_Toc31114769)

[4.2. Schedule Monitoring 7](#_Toc31114770)

[4.3. Risk Monitoring 7](#_Toc31114771)

[5. High-Level Build Schedule 7](#_Toc31114772)

[6. Project Success Criteria 7](#_Toc31114773)

[7. Communication Management Plan 8](#_Toc31114774)

[8. Risk Management Plan 8](#_Toc31114775)

[8.1. Risk Identification 9](#_Toc31114776)

[8.2. Risk Analysis 9](#_Toc31114777)

[8.2.1. Risk Probability 9](#_Toc31114778)

[8.2.2. Risk Impact 9](#_Toc31114779)

[8.2.3. Risk Severity 10](#_Toc31114780)

Table of Figures

[Figure 1: Project VA Organizational Chart 4](#_Toc28945258)

[Figure 2: EAC Tool 6](#_Toc28945259)

Table of Tables

[Table 1: PWS Task Areas 2](#_Toc28945260)

[Table 2: VA Stakeholders 5](#_Toc28945261)

[Table 3: Risk Probability Matrix 9](#_Toc28945262)

[Table 4: Risk Impact Matrix 9](#_Toc28945263)

[Table 5: Risk Severity Matrix 10](#_Toc28945264)

# Introduction

This Contractor Project Management Plan (CPMP) lays out the approach, timeline, and tools to be used to deliver the Veterans Health Information Systems and Technology Architecture (VistA) Adaptive Maintenance VA Enterprise Cloud (VAEC) Security (VAM) project.

The CPMP defines how Project VAM is executed, monitored, controlled, and closed in accordance with the Performance Work Statement (PWS), and will be progressively updated throughout the Period of Performance (PoP).

Additionally, the CPMP details the strategy for the coordination and execution of planned, routine, and ad hoc data collection reporting requests, as identified in the PWS, and is meant to serve as a communication vehicle for ensuring the key VAM stakeholders share a common understanding of the project.

The milestones identified in the CPMP are supported by the project schedule, a separate document that specifies planned dates for performing tasks and activities.

## Project Overview

VAM is a cloud-native Platform as a service (PaaS) deployed entirely and exclusively within the Federal Risk and Authorization Management Program (FedRAMP), Health Insurance Portability and Accountability Act of 1996 (HIPAA)-compliant VA Enterprise Cloud (VAEC), leveraging the Amazon Web Services (AWS) commercial cloud infrastructure and services.

VAM provides comprehensive, commercial cloud-based monitoring and security for all clients, applications, and users of the VistA Remote Procedure Call (RPC) interface. VAM is operationalized and scaled for Enterprise Production use for all VistA systems migrated to the VAEC, leveraging FedRAMP High, VAEC-approved AWS Kinesis and AWS CloudWatch Logs.

VAM is a passive monitoring PaaS that mirrors VistA RPC traffic via AWS Kinesis to the AWS CloudWatch Logs, which is then interpreted by the RPC Monitor. AWS CloudWatch Logs are FedRAMP High certified and store all data in an encrypted form.

VAM is a 100% cloud-native, legacy-free, and non-invasive PaaS. VAM requires no change to any VistA system, nor to any end user client or application, allowing VAM to be safely and reliably deployed and scaled Enterprise-wide with minimal to no risk. Should VAM (RPC Mirror or Monitor) be disabled or deactivated, all RPC traffic flows between VistA and all its clients as usual, only without monitoring.

All of VAM’s functionality is contained exclusively and entirely as a PaaS within the VAEC, thus inheriting all security and compliance controls of the Federal Information Security Management Act of 2002 (FISMA) High VAEC. VAM has neither a connection with, nor does it share any information with, any organization, application, or system outside of the VAEC.

## Project Scope

The scope of the project includes the planning, development, design, integration, testing, implementation, and management of centralized services that provide comprehensive, real-time, 24/7 monitoring and security for all Veteran data in all VistA systems migrated to the VAEC.

Team AbleVets will complete the audit, analysis, and translation of the entire VistA RPC interface into a modern, machine-processable form, operationalized and scaled for Production Enterprise’s use on the VAEC CloudWatch monitoring tool.

Table 1 details Project VAM’s task areas, as stated in the PWS.

Table : PWS Task Areas

| PWS/TASK | Summary of Task Requirements |
| --- | --- |
| 5.1 Project Management | 1. CLIN 0001AA CPMP 2. CLIN 0001AB Monthly Progress Report 3. CLIN 0001AC VA Privacy and Information Security Awareness and Rules of Behavior Training Certificate 4. CLIN 0001AD Signed Contractor Rules of Behavior 5. CLIN 0001AE VA HIPAA Certificate of Completion 6. CLIN 0001AF Weekly Onboarding Status Report |
| 5.2 Adaptive Maintenance Services | 1. CLIN 0002AA Comprehensive RPC Interface Audit Report 2. CLIN 0002AB MUMPS RPC to JSON Model Data Definition 3. CLIN 0002AC Version Description Document (VDD) 4. CLIN 0002AD Automated CloudWatch Configuration 5. CLIN 0002AE Security Vulnerability Report |
| 5.3 Testing | 1. CLIN 0003AA Master Test Plan 2. CLIN 0003AB RPC Interface Test Suite |
| 5.4 Assessment and Authorization (A&A) Support | 1. Update the following VAEC A&A artifacts quarterly, as applicable. 2. System Security Plan 3. Security Configuration Plan 4. Information System Contingency Plan 5. Incident Response Plan 6. Privacy Impact Assessment 7. Risk Assessment 8. Security Configuration Checklist (SCC) 9. System Interconnection Agreements (MOU and Interconnection) 10. Interconnection Security Agreement 11. Signatory Authority |
| 5.5 Initial Operating Capability (IOC) Support | 1. CLIN 0005AA Production Operations Manual 2. CLIN 0005AB Deployment, Installation, Backout, and Rollback Guide 3. CLIN 0005AC User Guide |
| 5.6 Release and Deployment Support | 1. CLIN 0006AA Capacity, Performance, and Scalability Assessment for National Deployment |

## Goals and Objectives

The primary objective of Project VAM is to assist VA in strengthening its cybersecurity profile by enhancing the protection of Veteran data. The successful execution and completion of the project resolve the following aims:

* Reduce the cost and complexity of the maintenance of VistA systems
* Resolve severe security vulnerabilities of all VistA systems migrated to VAEC
* Full utilization of the scaling and features of VA’s new commercial cloud capabilities
* Ensure the safe, secure, and seamless continuity of Veteran care and services as VistA systems are migrated to VAEC

## Technical Approach

Project VAM will provide enhanced Veteran data security via VistA RPC content audit and monitoring so that all VAEC-deployed VistA systems are adequately secured.

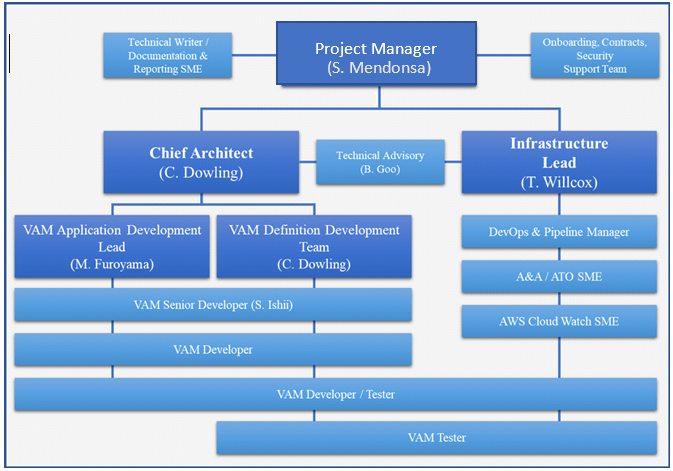
Team AbleVets will:

1. Complete the analysis of the MUMPS code for the remainder of the 5500 RPC interfaces and perform modeling to identify, for each RPC:
   1. The types, categories, and volumes of data it accesses (Does the RPC affect pharmacy, laboratory or other clinical applications only or does it affect all/most VistA applications?)
   2. The actions it performs (Does it perform read only functions or does it also allow write access to the patient record?)
   3. The sensitivity of the data it handles (Is the data Protected Health Information (PHI) or non-PHI?)
   4. The consumers (end users, applications, and clients) accessing the system (Is it a legitimate end user, or a rogue client/intruder?)
2. Execute, document, and provide the results of a comprehensive audit of the VistA RPC interface (all 5,500 MUMPS RPC calls)
3. Translate the MUMPS code into a machine-processable form for implementation within the VAEC-resident CloudWatch tool
4. Deliver a MUMPS RPC to JSON model data definition that represents the outcome of the audit and MUMPS to JSON model translation
5. Deliver a quarterly Version Description Document (VDD) that details the progress toward completion of the audit and model translation for all 5,500 VistA RPCs
6. Scale the interface monitor for Production deployment
7. Provide a CloudWatch configuration that automates the capture, storage, monitoring, and audit of all RPC traffic in the VAEC-resident CloudWatch tool on a continuous basis
8. Pull RPC traffic from CloudWatch, and based on a comprehensive audit, automatically classify and quantify RPC traffic to:
   1. Identify all clients accessing VistA data via the RPC interface
   2. Identify all users accessing VistA data via the RPC interface
   3. Identify and audit all types, volumes and categories of data accessed via the RPC interface, with an indication of sensitivity
9. Configure CloudWatch to generate real-time alerts and alarms based on identified vulnerability and sensitivity conditions of RPC traffic
10. Demonstrate the success of the automated CloudWatch configuration’s operational performance by providing a fully automated validation of the RPC interface audit
11. Produce a Security Vulnerability Report including:
    1. The number and type of clients accessing Veteran data
    2. The number and type of users accessing Veteran data
    3. The volume, types, and sensitivity of data accessed

# Project Organization

The organizational structure of Team AbleVets (Figure 1) is designed to ensure appropriate management and technical leadership in all key areas.

Figure : Project VA Organizational Chart



At the operational level, the AbleVets PM and Chief Architect are responsible for leading the development and delivery of all contractual project artifacts. They are accountable for the program, for ensuring the delivery of high-quality artifacts, and for supporting the client throughout all contractual activities.

## Stakeholders and Key Personnel

Stakeholders (Table 2) have different interests in and expectations for Project VAM; they must be identified in the beginning of the project and continuously validated in order to meet all stakeholder requirements. Identifying stakeholder expectations:

* Provides Team AbleVets with an understanding of the stakeholders’ perspective
* Ensures that all stakeholders’ expectations are addressed
* Instills stakeholder trust and cooperation
* Defines Team AbleVets’ approach to satisfy project requirements and validate the design throughout the project lifecycle

Table : VA Stakeholders

|  |  |  |  |
| --- | --- | --- | --- |
| Office of Information and Technology (OIT) | | | |
| Team Member | Contact Information | Proxy | Role |
| Dr. Rafael Richards | [Rafael.Richards@va.gov](mailto:Rafael.Richards@va.gov) 202-469-1527 | Cheryl Owsley | Business Owner |
| Christopher Brown | Christopher.brown1@va.gov | Cheryl Owsley | System Owner |
| Cheryl Owsley | Cheryl.Owsley@va.gov | Dr. Richards | VA Project Manager (PM) |
| Dana Newcomb | [Dana.Newcomb@va.gov](mailto:Dana.Newcomb@va.gov) 732-440-9680 | Josh McGarry | Contracting Officer |
| Amanda J. Bleses | Amanda.Bleses@va.gov  732-795-1054 | Cheryl Owsley | Contract Specialist |
| Robert Goode | [Robert.Goode@va.gov](mailto:Robert.Goode@va.gov) 202-461-4304 | Cheryl Owsley | Contracting Officer’s Representative (COR) |
| Bobbi Begay | Bobbi.Begay@va.gov | Chery Owsley | Information Security Officer |
| Team AbleVets | | | |
| Team Member | Contact Information | Proxy | Responsibility |
| Jeff Miller | Jeffrey.Miller7@va.gov 703-400-6859 | Avinay Vaswani | Account Vice President, AbleVets |
| Tom Willcox | Tom.Willcox@ablevets.com 703-915-7688 | Savio Mendonsa | CIO, AbleVets |
| Jim McCartin | James.McCartin@ablevets.com  703-898-8884 | Avinay Vaswani | Portfolio Director, AbleVets |
| Savio Mendonsa | Savio.Mendonsa@va.gov 571-385-0048 | Christy Lentile | PM, AbleVets |
| Conor Dowling | Conor.Dowling@va.gov 310-980-7954 | Mike Furoyama | Software Architect, Caregraf |
| Renton Nip | RNip@hawaiirg.com 808-927-0999 | Mike Furoyama | Manager, HRG |
| Mike Furoyama | Michael.Furoyama@va.gov | Conor Dowling | Sr. Developer, HRG |

At a strategic level, the VA PM is responsible for providing the overall programmatic direction to Team AbleVets. The VA PM and COR are the final approval authority for all VAM deliverables. In addition, the VA PM is responsible for:

* Monitoring the contract to ensure that Team AbleVets successfully meets its obligations
* Monitoring Team AbleVets’ performance to ensure the services provided meet required standards
* Managing any and all changes permitted under the contract
* Managing changes that are not identified in the contract

# Testing

The *CLIN 0003AA VAM Master Test Plan* details all testing activities and summarizes the testing approach, key objectives, test tools, and test data output. The test plan introduces:

* Test Strategy: The rules upon which testing is based, and the process for establishing valid tests to output sound test data. The test strategy addresses the scheduling of test events, the IOC entry and exit criteria, and test data management
* Execution Strategy: Details how the test activities are performed
* Test Management Plan: Describes the design, execution, and process for test event issue resolution

An RPC interface test suite has been created for developer-level tests, with execution schemes, for the following functional components:

* Traffic Mirror Monitor

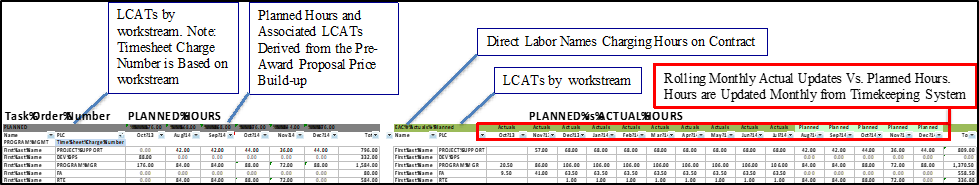
# Monitoring and Control Mechanisms

The purpose of monitoring and control mechanisms is to provide an understanding of the project’s progress so that appropriate corrective actions can be taken when the project’s performance deviates significantly from the plan.

## Budget Monitoring

The AbleVets Estimate at Completion (EAC) tool (Figure 2) is used to define the cost to complete any given level of effort in the Work Breakdown Structure (WBS), and depicts planned financial elements (number/type of project staff, projected number of hours per week/month, and labor rate) throughout the duration of the contract. After the contract award, the budget is updated monthly, displaying planned financial information against actuals. The AbleVets PM reviews the VAM EAC tool (budget) each month to ensure the project remains within allocated funding limits.

Figure : EAC Tool



## Schedule Monitoring

The project schedule is monitored weekly to ensure project tasking and activities are completed on the prescribed dates. Regular reviews of the schedule allow for the early identification of potential issues before they become risks. Monitoring the project schedule optimizes the use of resources, aids in managing unexpected changes, ensures Team AbleVets is task-focused, and ensures that project tasks are executed in the correct order. Schedule monitoring includes:

* Updating tasks, due dates, dependencies, resources and percentage of completion
* Adding/revising tasks, as needed
* Ensuring changes do not impact the critical path
* Calculating the amount of slack on the critical path
* Ensuring enough time to complete high-risk tasks
* Validating that all project milestones are met

## Risk Monitoring

Risk monitoring involves the continuous evaluation of risks. All project team members are responsible for the identification, monitoring, and mitigation of risks. The AbleVets PM is responsible for tracking and validating risk mitigation plans and updating the Risk Registry.

# High-Level Build Schedule

The high-level build schedule is available within the [GitHub](https://github.com/vistadataproject/RPCDefinitionToolkit/blob/master/README.md) tool.

# Project Success Criteria

The success of the project VAM is based upon meeting contractual requirements, exceeding VA expectations, and developing positive working relationships with all stakeholders. Project success criteria includes, but is not limited to:

* Customer satisfaction
* Effective decision making
* Managing change
* Crafting project schedules with realistic and obtainable delivery dates
* Minimal/no scope creep
* Effective coordination with subcontractors
* Effective communication with the integrated project team
* Immediate communication of project issues
* Openly discussing issue resolution
* Meeting user requirements
* Executing the project within budget
* Meeting project milestones
* Meeting quality criteria
* Producing an easily maintainable product

# Communication Management Plan

AbleVets uses a comprehensive bi-directional communication approach that strategically engages stakeholders. Establishing and maintaining formal and informal communication channels with our clients and team is a key to success. AbleVets understands that quality communication includes formal and informal mechanisms, both face-to-face and through electronic media, and ensures stakeholder involvement.

Team AbleVets conducts weekly status meetings to:

* Review strategic or Enterprise news that impacts the project
* Review the status of all open action items
* Report all closed action items
* Review the key milestones and activities from the previous week, and the plan for the upcoming week
* Review the technical status, deployment/infrastructure status, and management processes
* Discuss contractual or other items that warrant discussion
* Confirm all new action items captured in the current week’s meeting

# Risk Management Plan

A risk is defined as an uncertain event or condition that has a probability of occurring and could have either a positive or negative impact to at least one of the project’s objectives, should that risk occur. A risk may have one or more causes and, if it occurs, could impact one or more tasks. All projects assume some element of risk, and it is through risk management where tools and techniques are applied to monitor and track those events that have the potential to impact the outcome of a project.

Risk management focuses on identifying potential problems before they occur. Proper planning for and handling of risks helps avoid adversely impacting the project’s objectives and goals. Risk identification, tracking, monitoring, managing, and resolution occur continuously throughout the lifecycle of a project, and include the following four steps:

* Identify the Risk: The effort associated with identifying a risk and its potential impact on the project and documenting the risk’s characteristics.
* Analyze the Risk: The effort associated with evaluating the probability of occurrence, the impact on the project, and ranking the severity of the risk.
* Plan the Response: The effort associated with developing mitigation and contingency plans to minimize or eliminate the impact of a risk. Mitigation strategies are developed for risks determined to have an impact on the project. Mitigation activities are tracked until either the risk exposure has been satisfactorily reduced, or the risk is averted.
* Monitor and Control the Risk: The effort associated with making decisions to initiate the appropriate controls and tracking a risk until it is no longer a threat.

## Risk Identification

The primary purpose of risk management is identifying a potential impact early enough to avoid an impact to the project’s success. Risks are identified and documented by the entire project team. The daily Scrum includes discussion of the details surrounding newly identified risks, and the advancement of mitigation plans in progress.

Team AbleVets will estimate the probability and the impact of all newly identified risks. The severity of each risk is based upon the probability of occurrence and potential impact. High severity risks will be documented and tracked in the Risk Registry.

## Risk Analysis

Risk analysis encompasses the evaluation of probability, impact, severity, and prioritization. The purpose of risk analysis is to bolster the risk definition into decision-making information. During the analysis, risks are evaluated in detail to assess their severity, impact, and if/how risks relate to each other. Risk mitigation plans are determined and documented after analysis.

### Risk Probability

The probability of a risk occurring within a given unit of time (per day, per two-week Sprint, per month, during the project) is a subjective estimation, based on an analysis by the project team or the risk owner. The probability estimate requires knowledge of the activity, experience, or historical data. The Risk Probability Matrix (Table 3) details the five risk probability ranks. The distribution of the 20-40-60-80 rule is the basis for the probability ranks used in quantitative analysis.

Table : Risk Probability Matrix

| Risk Probability Rank | Likelihood of Event |
| --- | --- |
| 5 – Almost Certain | > 80% – Risk event expected to occur |
| 4 – Likely | 60-80% – Risk event more likely to occur |
| 3 – Moderate | 40-60% – Risk event may or may not occur |
| 2 – Unlikely | 20-40% – Risk event less likely to occur |
| 1 – Rare | < 20% – Risk event not expected |

### Risk Impact

The impact to the project if a risk occurs is estimated in terms of the criteria that are important the stakeholders. The Risk Impact Matrix (Table 4) is used to rate the impact of each risk as it relates to safety, financial, schedule, adverse image/publicity and customer service/business interruption.

Table : Risk Impact Matrix

| Risk Impact Rank | Cost or Schedule impact | Scope or Quality |
| --- | --- | --- |
| 5 – Potentially Catastrophic | GREATER THAN 20% | Final contract deliverables fail to meet customer needs. |
| 4 – Major | 10 – 20% | Final contract deliverables’ content and quality are unacceptable to customer. |
| 3 –Moderate | 5 – 10% | Major impact to the final contract deliverables’ content and quality that require customer approval. |
| 2 – Minor | LESS THAN 5% | Relatively minor impact to contract deliverables’ content and quality. |
| 1 – Insignificant | No or negligible variance | Very minor impact to contract deliverables’ content and quality. |

### Risk Severity

The severity of a risk is determined by its probability and impact. Severity is calculated by the likelihood of occurrence and impact using the Risk Severity Matrix (Table 5). Risks that fall within the red zone (high risk) are documented, and the response from Program Management is used to determine the necessity of a code change. If the risk mitigation requires development work, it will be added to the project backlog.

Table : Risk Severity Matrix

|  |  | **Risk Consequence (Severity)** | | | | |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | Insignificant | Minor | Moderate | Major | **Severe** |
| **Risk Consequence (Severity)** | Almost Certain | LOW | MEDIUM | HIGH | HIGH | HIGH |
| Likely | LOW | MEDIUM | MEDIUM | HIGH | HIGH |
| Moderate | LOW | LOW | MEDIUM | MEDIUM | HIGH |
| Unlikely | LOW | LOW | LOW | MEDIUM | MEDIUM |
| Rare | LOW | LOW | LOW | LOW | MEDIUM |