VistA Adaptive Maintenance VAEC Security (VAM)

Monthly Progress Report



June 2019

Version 1.3

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 06/03/2019 | 1.3 | Updates for May 2019 | AbleVets |
| 05/03/2019 | 1.2 | Updates for April 2019 | AbleVets |
| 04/03/2019 | 1.1 | Updates for March 2019 | AbleVets |
| 03/04/2019 | 1.0 | Initial version of the document | AbleVets |

Table of Contents

[1. Introduction 1](#_Toc10190239)

[2. Work Completed 1](#_Toc10190240)

[3. Work Planned 1](#_Toc10190241)

[4. Risks and Issues 2](#_Toc10190242)

[A. Appendix: Project Deliverables 3](#_Toc10190243)

[B. Appendix: Acronyms and Abbreviations 4](#_Toc10190244)

Table of Tables

[Table 1: Risks and Issues 2](#_Toc10190245)

[Table 2: PWS Project Deliverables 3](#_Toc10190246)

[Table 3: ATO Artifacts 3](#_Toc10190247)

[Table 4: Acronyms and Abbreviations 4](#_Toc10190248)

# Introduction

The Veterans Health Information Systems and Technology Architecture (VistA) Adaptive Maintenance (VAM) System is a cloud-smart, cloud-native application developed and deployed in the dedicated 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 that access VistA data using VistA’s Remote Procedure Call (RPC) interface. VAM is operationalized and scaled for Production Enterprise’s use in the VAEC leveraging AWS Kinesis, and provides comprehensive, commercial, cloud-based VistA RPC interface monitoring and security for all VistA systems migrated to the VAEC. VAM is 100% legacy-free, cloud-native, and non-invasive, allowing it to be scaled and deployed Enterprise-wide without requiring changes to any VistA system.

This Project VAM Monthly Progress Report covers the Period of Performance (PoP) from May 1 through May 31, 2019.

# Work Completed

The work detailed below was completed during the May 1 through May 31, 2019 PoP.

* Facilitated multiple, weekly status meetings to discuss Team AbleVets’ progress. Meeting minutes can be found on the [Project VAM workspace](https://github.com/vistadataproject/VAMProjectManagement/tree/master/Documents/weekly_meeting_minutes) of GitHub.
* Analyzed the system logs from version D4 of the RPC Definition and Toolkit that capture logins and usage, currently in VistA, to enhance definitions. The logs will provide the basis for the Security Vulnerability Report and are scheduled to be deployed on June 7, 2019.
* Prepared the test framework for delivery with the D4 system logs on June 7, 2019.
* Updated and delivered the PWS artifacts detailed in Table 2 on May 2, 2019
* Created the System Boundary document and updated the VAM architecture diagram.
* Revised Project VAM’s RiskVision profile by updating the details for the new scope of work, adding new team members, and removing former team members. Reviewed and answered all questions regarding RiskVision templates and controls and submitted them to the VA Project Manager (PM), Business Owner, System Owner, Information Security Officer (ISO), and Product Owner for their review and signatures.
* Created the documentation in support of the Authority to Operate (ATO) process. Submitted the documents for final signatures from the PM, System Owner, ISO, and Product Owner.
* Submitted a request for and received the access to the VAM Pre-Production and Production Environment in the VAEC AWS.

# Work Planned

The work detailed below is planned for the June 1, 2019 to June 30, 2019 PoP.

* Facilitate weekly status meetings
* Continue updating RiskVision
* Submit all relevant information and documentation for the processing of the ATO
* Update project documentation and prepare same for delivery
* Continue analysis of the version D4 logs and enhancement of definitions
* Continue preparation of the test framework
* Configure the VAM Pre-Production environment for scans.

# Risks and Issues

Table 1 lists the currently known risks and issues. Each item will be resolved prior to the delivery of the D4 build on June 7, 2019.

Table 1: Risks and Issues

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Issue Number and Category | Due Date | Issue Description | Risk | Mitigation Plan |
| VAM-R18 (PWS Dashboard)  Release Process | 06/30/2019 | Identify a Release Manager and release process. | Without a VA Release Manager there is no point of approval so that the deployment can move forward.  Without a release process the release workflow and acceptance criteria cannot be defined. | Identify the VA Release Manager; formulate and formalize the release process in GitHub. |
| VAM-R10 (ATO Dashboard)  Technical | 8/30/2019 | Receive an ATO | We cannot move to IOC Production without the ATO. | Team AbleVets will continue to refine the RiskVision profile and ATO documentation with guidance from the PM and ISO. |
| VAM-R17 (IOC Dashboard)  Technical | 10/31/2019 | Configure the VAEC IOC environments at Valley Coastal, TX and Omaha, NE | We cannot deliver Dev-Int Build 4 unless there are IOC environments configured. | Migrate the two identified IOC VistA environments to VAEC and establish connectivity. |

1. Appendix: Project Deliverables

Table 2 and Table 3 list the project deliverables required by the PWS, and the deliverables necessary for the processing of the ATO.

Table : PWS Project Deliverables

|  |  |
| --- | --- |
| CLIN | Artifact |
| 0001AA | Contractor Project Management Plan (CPMP) v1.2 |
| 0001AB | Monthly Progress Report v1.2 |
| 0001AF | Weekly Onboarding Status Report |
| 0002AA | Comprehensive RPC Interface Audit Report |
| 0002AB | Massachusetts General Hospital Utility Multi-Programming System (MUMPS) RPC to JavaScript Object Notation (JSON) Model Data Definition |
| 0002AC | Version Description Document (VDD) |
| 0002AD | Automated CloudWatch Configuration |
| 0002AE | Security Vulnerability Report |
| 0003AA | Master Test Plan v2 |
| 0003AB | RPC Interface Test Suite |
| 0005AA | Production Operations Manual (POM) |
| 0005AB | Deployment and Installation Guide |
| 0005AC | User Guide |

Table : ATO Artifacts

|  |  |
| --- | --- |
| Business Impact Analysis (BIA) | Security Impact Analysis (SIA) |
| Configuration Management Plan (CM Plan) | Signatory Authority |
| Disaster Recovery Plan (DRP) | System Design Document (SDD) |
| Incident Response Plan (IRP) | System Owner Attestation |
| Information Security Contingency Plan (ISCP) | System Owner Responsibilities |
| Privacy Impact Assessment (PIA) | System Security Categorization Report (SSC) |
| Privacy Threshold Analysis (PTA) | System Security Plan (SSP) |
| Risk Assessment |  |

1. Appendix: Acronyms and Abbreviations

Table 4 lists the acronyms and abbreviations used in this document with their descriptions.

Table : Acronyms and Abbreviations

|  |  |
| --- | --- |
| Acronym | Description |
| **ATO** | Authority to Operate |
| **AWS** | Amazon Web Services |
| **BIA** | Business Impact Analysis |
| **CM** | Configuration Management |
| **CPMP** | Contractor Project Management Plan |
| **DRP** | Disaster Recovery Plan |
| **FedRAMP** | Federal Risk and Authorization Management Program |
| **HIPAA** | Health Insurance Portability and Accountability Act of 1996 |
| **IOC** | Initial Operating Capability |
| **IRP** | Incident Response Plan |
| **ISCP** | Information Security Contingency Plan |
| **ISO** | Information Security Officer |
| **JSON** | JavaScript Object Notation |
| **MUMPS** | Massachusetts General Hospital Utility Multi-Programming System |
| **PIA** | Privacy Impact Assessment |
| **PM** | Project Manager |
| **POM** | Production Operations Manual |
| **PoP** | Period of Performance |
| **PTA** | Privacy Threshold Analysis |
| **PWS** | Project Work Statement |
| **RPC** | Remote Procedure Call |
| **SIA** | Security Impact Analysis |
| **SDD** | System Design Document |
| **SSC** | System Security Categorization Report |
| **SSP** | System Security Plan |
| **VA** | Department of Veterans Affairs |
| **VAEC** | VA Enterprise Cloud |
| **VAM** | VistA Adaptive Maintenance |
| **VDD** | Version Description Document |
| **VistA** | Veterans Health Information Systems and Technology Architecture |