VistA Adaptive Maintenance VAEC Security (VAM)

Monthly Progress Report



Department of Veterans Affairs

August 2019

Version 1.5

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 08/02/2019 | 1.5 | Updates for July 2019 | AbleVets |
| 07/03/2019 | 1.4 | Updates for June 2019 | AbleVets |
| 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](#_Toc15895831)

[2. Work Completed 1](#_Toc15895832)

[3. Work Planned 3](#_Toc15895833)

[4. Risks and Issues 4](#_Toc15895834)

[A. Appendix: Acronyms and Abbreviations 5](#_Toc15895835)

Table of Tables

[Table 1: PWS Project Deliverables 2](#_Toc15895836)

[Table 2: ATO Artifacts 2](#_Toc15895837)

[Table 3: Risks and Issues 4](#_Toc15895838)

[Table 4: Acronyms and Abbreviations 5](#_Toc15895839)

# Introduction

The Veterans Health Information Systems and Technology Architecture (VistA) Adaptive Maintenance (VAM) System 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.

# Work Completed

The work detailed below was completed during the July 1 through July 31, 2019 Period of Performance (PoP).

* Updated Project VAM’s RiskVision profile by adding the Logical and Physical System Boundary document and dataflow diagrams as evidence of multiple RiskVision controls.
* Updated Project VAM’s RiskVision profile by updating the new project description, provided by the Business Owner.
* Reviewed and updated all controls in RiskVision. Updated the documentation in support of the Authority to Operate (ATO) process. Submitted the documents in batches and received final signatures for the documents from the Project Manager, Privacy Officer, System Owner, Information Systems Officer, Privacy Impact Assessment (PIA) support team, and Business Owner.
* Deployed the VAM Pre-Production and Production instances in the VAEC AWS.
* Received the results of the Nessus scan.
* Began remediating the issues found in the Nessus scan and resubmitted a request for a new Nessus scan.
* Received the Secure Code review results.
* Began remediating the issues found in the Secure Code review and resubmitted a request for a new Secure Code review.
* Received the results of the Quality Code scan.
* Began remediating the issues found in the Quality Code scan and resubmitted a request for a new Quality Code scan.
* Submitted Plans of Action and Milestones (POAMs) to the Information Systems Officer (ISO) for her signature. The POAMs indicate that VAM is not required to perform the database scan, complete the Independent Safety Assessment (ISA)-Memorandum of Understanding (MOU), perform the Web Application Security Assessment (WASA) scan, or the Threat Model and Secure Design review.
* Began to process the ATO package within the Enterprise Mission Assurance Support Service (eMASS) system.
* 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.
* Delivered the Weekly Onboarding Status Report on July 3, 10, 17, 24, and 31, 2019.
* On July 03, 2019 updated and delivered the PWS artifacts detailed in Table 1 below.

Table 1: PWS Project Deliverables

|  |  |
| --- | --- |
| CLIN | Artifact |
| [0001AA](https://github.com/vistadataproject/VAM2ProjectManagement/blob/master/Documents/source/CLIN%200001AA%20VAM%20Contractor%20Project%20Management%20Plan%20v%201%204.docx) | Contractor Project Management Plan (CPMP) v1 4 |
| [0001AB](https://github.com/vistadataproject/VAM2ProjectManagement/blob/master/Documents/source/CLIN%200001AB%20VAM%20Monthly%20Progress%20Report%20v1%204.docx) | Monthly Progress Report v1 4 |
| [0003AA](https://github.com/vistadataproject/VAM2ProjectManagement/blob/master/Documents/source/CLIN%200003AA%20VAM%20Master%20Test%20Plan%20v1%204.docx) | Master Test Plan v1 4 |

* Created the final documentation detailed in Table 2 below, in support of the Authority to Operate (ATO) process. Submitted documents in batches and received final signatures, as applicable, for these documents from the PM, Privacy Officer, System Owner, ISO, PIA Support Group, and Business Owner.

Table 2: 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 |  |

# Work Planned

The work detailed below is planned for the August 1, 2019 to August 31, 2019 PoP.

* Continue updating the Project VAM eMASS profile for ISO review
* Submit all relevant information and documentation for the processing of the ATO
* Complete the analysis of the version D5 logs and enhancement of definitions
* Begin the analysis of the version D6 change crumbs
* Continue updating the test framework
* Obtain all required scans for the VAM environments in AWS
* Facilitate weekly status meetings
* Update project documentation and prepare same for delivery

# Risks and Issues

Table 3 lists the currently known risks and issues. Each item will be resolved prior to the delivery of Build 4 in January of 2020.

Table : Risks and Issues

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Issue Number and Category | Due Date | Issue Description | Risk | Mitigation Plan |
| VAM-R10 (ATO Dashboard) | 10/31/2019 | Receive VA approval for the ATO package by 10/31/2019. | If ATO approval is not received by 10/31/2019, the VAM deployment to IOC Production will be delayed. | Team AbleVets will submit all ATO documentation to eMASS by 8/30/2019, ensuring VA has sufficient time to review and approve the ATO package by 10/31/2019. |
| VAM-R17 (IOC Dashboard)  Technical | 10/31/2019 | Access to the VistA environments in VAEC is required for Build 4. | If Team AbleVets does not obtain access to the Vista environments in VAEC by 9/30/2019, then they cannot deploy or test Build 4 in the IOC Pre-Production environment, resulting in a day-for-day schedule slip that will impact the Production deployment date. | Upon completion of the VA migration of VistA environments to VAEC, Team AbleVets will immediately submit access requests and elevate the requests as needed. Once access is granted, Team AbleVets will deploy and test Build 4. |

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 |
| **CSOC** | Cybersecurity Operations Center |
| **DRP** | Disaster Recovery Plan |
| **eMASS** | Enterprise Mission Assurance Support Service |
| **FedRAMP** | Federal Risk and Authorization Management Program |
| **FISMA** | Federal Information Security Management Act of 2002 |
| **HIPAA** | Health Insurance Portability and Accountability Act of 1996 |
| **IOC** | Initial Operating Capability |
| **IRP** | Incident Response Plan |
| **ISA** | Independent Safety Assessment |
| **ISCP** | Information Security Contingency Plan |
| **ISO** | Information Security Officer |
| **JSON** | JavaScript Object Notation |
| **MOU** | Memorandum of Understanding |
| **MTP** | Master Test Plan |
| **MUMPS** | Massachusetts General Hospital Utility Multi-Programming System |
| **PaaS** | Platform as a Service |
| **PIA** | Privacy Impact Assessment |
| **PM** | Project Manager |
| **POAM** | Plan of Action and Milestones |
| **POM** | Production Operations Manual |
| **PoP** | Period of Performance |
| **PTA** | Privacy Threshold Analysis |
| **PWS** | Performance 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 |
| **WASA** | Web Application Security Assessment |