|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  | **DEPARTMENT OF VETERANS AFFAIRS** | | |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  | **Risk Assessment** | | |  |
|  | **VistA Adaptive Maintenance (VAM)** | | |  |
|  |  |  |  |  |
|  | Generated September 11, 2018 | | |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **Executive Summary** | | | | | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | The VistA Adaptive Maintenance (VAM) is a Major Application owned by Dick Rickard, that has been determined to have a security categorization of High in accordance with Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | The periodic assessment of risk to agency operations or assets resulting from the operation of an information system is an important activity required by the Federal Information Security Management Act (FISMA). This Risk Assessment was prepared in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Guide for Conducting Risk Assessments. It summarizes the risks associated with the vulnerabilities identified by control deficiencies and Enterprise Risk Manager (ERM) related risks. All inputs to the risk assessment process were analyzed to provide an assessment of the security controls implemented to protect the confidentiality, integrity, and availability of the system and its information. The table below provides the total number of security risks, by risk level and control category. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  |
|  | **Table 1: Summary of System Risks** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | NIST 800-53 Control Families | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  |  |
|  |  | Risk Level | Management | | | | Operational | | | | | | | | | | | Technical | | | | Privacy | | | | | | | | | | Total |  |  |
|  |  | CA | PL | RA | SA | AT | CM | | CP | | IR | MA | MP | PE | PS | SI | AC | AU | IA | SC | AP | AR | DI | DM | | IP | SE | TR | UL | |  |  |
|  |  | High | 0 | 0 | 0 | 0 | 0 | 0 | | 0 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | 0 | 0 | 0 | 0 | | 0 |  |  |
|  |  | Medium | 0 | 0 | 0 | 0 | 0 | 0 | | 0 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | 0 | 0 | 0 | 0 | | 0 |  |  |
|  |  | Low | 1 | 0 | 0 | 0 | 0 | 0 | | 0 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | 0 | 0 | 0 | 0 | | 1 |  |  |
|  |  | Total | 1 | 0 | 0 | 0 | 0 | 0 | | 0 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | 0 | 0 | 0 | 0 | | 1 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **1.0 Introduction** | | | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | The periodic assessment of risk to agency operations or assets resulting from the operation of an information system is an important activity required by FISMA. This Risk Assessment was prepared in accordance with NIST SP 800-30, Guide for Conducting Risk Assessments. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | |  |  | | --- | --- | | **1.1 Purpose** |  | |  |  | | This Risk Assessment provides the system's stakeholders with an assessment of the adequacy of the management, operational, and technical controls used to protect the confidentiality, integrity, and availability of the system and the data it stores, transmits or processes. VA requires Risk Assessments to be performed for systems that are new, undergoing major modifications, applying changes which increase security risks, moving to a higher system security categorization, or have serious security violations as a result of an adverse security evaluation and/or audit. For a new system or a system undergoing a major modification, a Risk Assessment should be developed as part of the system development lifecycle. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Page 2 of | | | | | 21 | | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  | |  |  | | --- | --- | | **1.2 Scope** |  | |  |  | | null | | | | | |  |
|  |  |  |  |  |  |
|  | |  |  | | --- | --- | | **1.3 Structure** |  | |  |  | | The remainder of the report is structured as follows:  Section 2 - provides a system description including the business purpose, data handled, etc.  Section 3 - provides an overview of the methodology used to create this Risk Assessment.  Section 4 - provides a summary of Risk Assessment results  Appendices provide a table of acronyms used and documents referenced in the formulation of this Risk Assessment and its methodology. | | | | | |  |
|  | **2.0 System Characterization** |  |  |  |  |
|  |  |  |  |  |  |
|  | The VistA Adaptive Maintenance (VAM) is a Major Application owned by Dick Rickard, that has been determined to have a security categorization of High in accordance with Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems. | | | |  |
|  |  |  |  |  |  |
|  | |  |  | | --- | --- | | **2.1 Description** |  | |  |  | | The purpose of the VistA Adaptive Maintenance (VAM) project is to establish a secure, sustainable, high-performing, cloud-based service to implement provider workflow logic back-end processing and storage. The VAM service will replicate the Remote Procedure Call (RPC) functionality currently provided via VistA in a modern, well-documented platform (i.e., Node.js and NoSQL database). VAM will enable the incremental transition of clinical workflow logic out of VistA into VAM services, while maintaining full compatibility with current VistA clients such as CPRS. VAM will be hosted in production within the VA’s Enterprise Cloud (VAEC) using the Amazon Web Services (AWS) service provider. | | | | | |  |
|  |  |  |  |  |  |
|  | |  |  | | --- | --- | | **2.2 System Environment** |  | |  |  | | VISTA Adaptive Maintenance (VAM) VAM will be deployed within the VA’s Enterprise Cloud using Amazon Web Services (AWS) and Amazon CloudWatch. | | | | | |  |
|  |  |  |  |  |  |
|  | **3.0 Risk Assessment Approach** |  |  |  |  |
|  |  |  |  |  |  |
|  | This section contains information on what sources of input were used as part of this Risk Assessment and the methodology employed to process the threats and vulnerabilities identified during the assessment. | | | |  |
|  |  |  |  |  |  |
|  | **3.1 Risk Assessment Team** |  |  |  |  |
|  |  |  |  |  |  |
|  | The table below contains information on the individuals and organizations who participated in the development of this Risk Assessment Report. | | | |  |
|  |  |  |  |  |  |
|  |  |  | Page 3 of | 21 |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |
|  | **Table 3: Risk Assessment Team Members** | | | | | | | |  |
|  | Name | Role | | Email Address | | Phone | | |  |
|  | Charles Adejumo | Information Security Officer (ISO) | | Charles.Adejumo@va.gov | | 703 645-0420 | | |  |
|  | Bobbi Begay | Information Security Officer (ISO) | | Bobbi.Begay@va.gov | | 303.331.7837 | | |  |
|  | Dick Rickard | System Owner | | Richard.Rickard@va.gov | |  | | |  |
|  | Badhan Mandal | System Steward | | badhan.mandal@va.gov | |  | | |  |
|  | Dick Rickard | System Steward | | Richard.Rickard@va.gov | |  | | |  |
|  | John Allen | System Steward | | john.allen4@va.gov | | 703-407-5437 | | |  |
|  |  |  |  |  |  |  |  |  |  |
|  | **3.2 e-Authentication** | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Guidance from the Office of Management and Budget (OMB), contained in M-04-04 E-Authentication Guidance for Federal Agencies, requires agencies to review new and existing electronic transactions to ensure that authentication processes being used provide the appropriate level of assurance. VA system owners are responsible for compliance with this process. Step one of this process is to establish whether a system meets the established criteria for systems requiring an e-authentication risk assessment. The table below facilitates this first step by asking two questions about this system. | | | | | | | |  |
|  | **Table 4: e-Authentication Criteria** | | | | | | | |  |
|  | *e-Authentication Criteria Question* | | | | | | *Answer* | |  |
|  | Does this system allow access by human users, either VA or non-VA, communicating through an external, non-VA-controlled network? Note that access through the VA VPN should be considered VA-controlled. | | | | | | N/A | |  |
|  | Does the system require user authentication to perform any transactions (e.g., viewing, adding, modifying, or deleting information)? | | | | | | N/A | |  |
|  | If the answers to both questions are yes for a system, then the second step must be performed. This step entails the completion of an e-authentication risk assessment to determine the system's compliance with OMB M-04-04 and NIST 800-63 guidance. | | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |
|  | **3.3 Inputs to this Risk Assessment** | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | The following documents and methods were used to determine current system vulnerabilities as part of this risk | | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | Page 4 of | | | 21 |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  | **Table 5: Risk Assessment Inputs** | | | | | | |  |
|  | *Input* | *Description* | *Version* | *Date* | *File Name* | | |  |
|  | System Owner Responsibilities - VAM | System Owner Responsibilities Memo | 1 | May 29, 2018 | System Owner Responsibilities - VAM.pdf | | |  |
|  | System Owner Attestation - VAM | System Owner Attestation Memo | 1 | May 29, 2018 | System Owner Attestation - VAM.pdf | | |  |
|  | VAM SDD v1.0.0 | VAM SDD v1.0.0 | 1 | July 26, 2018 | VAM SDD Document NEW.docx | | |  |
|  | VAM System Boundary | VAM System Boundary | 1 | August 06, 2018 | VAM System Boundary.docx | | |  |
|  | VAM Software Configuration Management Plan (CMP)\_FINAL | VAM Software Configuration Management Plan (CMP)\_FINAL | 1 | August 23, 2018 | CLIN 0001AH VAM Configuration Management Plan v 1.2.docx | | |  |
|  | VAM Security Categorization\_Signed | VAM Security Categorization\_Signed | 1 | August 28, 2018 | VAM Security Categorization PORev'd0821-2018 and ISSO sig.pdf | | |  |
|  | Standard PTA-VAM signed 8-28-2018 | PTA | 1 | August 29, 2018 | Standard PTA-VAM signed 8-28-2018.pdf | | |  |
|  | Business Impact Analysis VAM Signed | Business Impact Analysis VAM Signed | 1 | September 09, 2018 | Business Impact Analysis VAM Signed.pdf | | |  |
|  | Fortify\_Scan\_Results\_router\_August\_2018 | Fortify\_Scan\_Results\_router\_August\_2018 | 1 | September 10, 2018 | Fortify\_Scan\_Results\_router.pdf | | |  |
|  | Fortify\_Scan\_Results\_vics\_server\_August\_2018 | Fortify\_Scan\_Results\_vics\_server\_August\_2018 | 1 | September 10, 2018 | Fortify\_Scan\_Results\_vics\_server.pdf | | |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | Page 5 of | 21 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  | |  |  | | --- | --- | | **3.4 Methodology** |  | |  |  | | This section describes the methodology used to conduct the security assessment for the system. The methodology consists of the following steps:  Step 1: Identify Threats  Step 2: Identify Vulnerabilities  Step 3: Analyze Risks  Step 4: Identify Recommended Corrective Actions  Step 5: Document Results | | | | |  |
|  |  |  |  |  |
|  | |  |  | | --- | --- | | **3.4.1 Step 1: Identify Threats** |  | |  |  | | This step begins with compiling a threat statement listing potential threat-sources that are applicable to the system. The following table provides an overview of the threat sources considered for the system risk assessment. | | | | |  |
|  |  |  |  |  |
|  |  | Page 6 of | 21 |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  | **Table 6: Threat Source List** | | | | | | |  |
|  | *Applies* | *Threat ID* | *Categories* | *Source* | *Definition* | | |  |
|  | No | T-01 | VA Environment Risk | Component Failure | Computer or systems component failures that require replacement | | |  |
|  | No | T-02 | VA Environment Risk | Dust/Debris | Dust or debris within a facility with access to systems and components | | |  |
|  | No | T-03 | VA Environment Risk | HVAC Failure | Failure of the heating, ventilation or cooling systems within a facility (e.g., temperature below 68 degrees, above 74 degrees, or rapid changes in temperature) | | |  |
|  | No | T-04 | VA Environment Risk | Indoor Humidity | Humidity inside of the facility above normal operating conditions (e.g., relative humidity below 40% or above 50% (temperature between 68-74 degrees)) | | |  |
|  | No | T-05 | VA Environment Risk | Power Failure | Failure of the external power supplying thefacility (e.g., brownout, blackout, voltage dip/spike) | | |  |
|  | No | T-06 | VA Environment Risk | Water Damage | Water within a VA facility that is not contained in the feed or drain lines | | |  |
|  | No | T-07 | VA Environment Risk | Vibration | Vibration of VA facilities or systems, not classified as a earthquake | | |  |
|  | No | T-08 | VA Human | Biological Release | Release of a biological toxin at or near the facility | | |  |
|  | No | T-09 | VA Human | Burglary/Break In | Unauthorized access to the facility with the intent to steal | | |  |
|  | No | T-10 | VA Human | Civil Unrest | Actions by the civilian population that cause people to feel unsafe to be outside their homes | | |  |
|  | No | T-11 | VA Human | Hacker, Cracker | Use of a computer system without proper authorization with the intent to cause harm or theft | | |  |
|  | No | T-12 | VA Human | HAZMAT Release/Spill | Release or spill of hazardous chemicals or materials at or near a facility | | |  |
|  | No | T-13 | VA Human | Human Health Emergency | Actions that cause the health of VA staff, contractors, or suppliers to be degraded as to make   them unavailable (e.g., flu, pandemic, meningitis) | | |  |
|  | No | T-14 | VA Human | Malicious Code | Malicious computer software that interferes with normal computer functions | | |  |
|  | No | T-15 | VA Human | Password Privacy Negligence | Users, systems, or software not following VA standards for password privacy | | |  |
|  | No | T-16 | VA Human | Personnel Unavailable | Actions that cause staff to be unavailable to work | | |  |
|  | No | T-17 | VA Human | Sabotage | Purposeful acts by non-VA staff to destroy VA facilities or capabilities | | |  |
|  | No | T-18 | VA Human | System Intrusion, Break-Ins | Unauthorized access to the system by a human | | |  |
|  | No | T-19 | VA Human | System Misconfiguration | System hardware, software, or parameters not configured properly | | |  |
|  | No | T-20 | VA Human | System Penetration | Actions by software to gain unauthorized access to a system | | |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | Page 7 of | 21 |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  | *Applies* | *Threat ID* | *Categories* | *Source* | *Definition* | | |  |
|  | No | T-21 | VA Human | System Tampering | Malicious actions to modify the normal configuration of a system | | |  |
|  | No | T-22 | VA Human | Terrorist | Actions by outside parties against the U.S. with the intent to cause fear in the population | | |  |
|  | No | T-23 | VA Human | User Negligence | Unintentional acts by authorized VA system users that cause harm to the VA | | |  |
|  | No | T-24 | VA Human | User Sabotage | Intentional acts by VA authorized users of VA systems to destroy VA facilities or capabilities | | |  |
|  | No | T-25 | VA Natural | Blizzard | Storm classified by the National Weather Service as a blizzard with significant snow, ice, wind, and cold | | |  |
|  | No | T-26 | VA Natural | Dam Failure | Failure of a dam leading to significant threat of water and debris damage to the facility, suppliers, or VA staff homes | | |  |
|  | No | T-27 | VA Natural | Earthquake | Earthquake at or near the facility | | |  |
|  | No | T-28 | VA Natural | Extreme Cold | Extremely low temperatures outside of the facility | | |  |
|  | No | T-29 | VA Natural | Extreme Heat | Extremely high temperatures outside of the facility | | |  |
|  | No | T-30 | VA Natural | Fire | Fire affecting a portion of or the entire facility | | |  |
|  | No | T-31 | VA Natural | Flood | A rising level of water outside or near a facility | | |  |
|  | No | T-32 | VA Natural | Hail | Storm classified by the National Weather Service as hail | | |  |
|  | No | T-33 | VA Natural | Hurricane | Storm classified by the National Weather Service as a hurricane | | |  |
|  | No | T-34 | VA Natural | Landslide | Movement of earth’s surface that can cause damage to a facility | | |  |
|  | No | T-35 | VA Natural | Lightning Strike | Lightning strike on the facility | | |  |
|  | No | T-36 | VA Natural | Thunderstorm | Storm classified by the National Weather Service as a thunderstorm | | |  |
|  | No | T-37 | VA Natural | Tornado | Storm classified by the National Weather Service as a tornado | | |  |
|  | No | T-38 | VA Natural | Tsunami | Storm classified by the National Weather Service as a tsunami | | |  |
|  | No | T-39 | VA Natural | Volcano | Eruption of a volcano near a VA facility | | |  |
|  | No | T-40 | VA Natural | Winter Weather Hazards | Winter weather (e.g., cold, snow, ice) that impacts the normal, safe operation of the VA | | |  |
|  | No | T-45 | VISTA | VISTA Cache Svs Accts password change | VISTA Cache Service Accounts with passwords not changed within three years as required | | |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | Page 8 of | 21 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  | |  |  | | --- | --- | | **3.4.2 Step 2: Identify Vulnerabilities** |  | |  |  | | The goal of this step is to develop a list of vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources. The identification of vulnerabilities can take many forms based on various types of risk assessments. For a list of documents and methods used to determine the vulnerabilities within the system, see Section 3.3.  Findings identified as part of the risk assessment activities mentioned in Section 3 were reviewed and grouped into risks by NIST 800-53 controls or by findings that were related to one another.  The following table contains all of the vulnerabilities found during the risk assessment review and includes any compensating measures already in place to mitigate the vulnerability. | | | | |  |
|  |  |  |  |  |
|  |  | Page 9 of | 21 |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  | **Table 7: System Vulnerability List** | | | | | |  |
|  | *Vulnerability Source* | *NIST 800-53 Control or VA Policy* | *Vulnerability Description* | *Response* | | |  |
|  | NIST 800-53 RMF - Information System (VistA Adaptive Maintenance (VAM) Assessing) | CA-08.1 Penetration Testing | Obtain VAM Pen Test |  | | |  |
|  | NIST 800-53 RMF - Information System (VistA Adaptive Maintenance (VAM) Assessing) | Database Scan Pre-Prod (Beta) | PENDING- Database Scan Pre-Prod (Beta) |  | | |  |
|  | NIST 800-53 RMF - Information System (VistA Adaptive Maintenance (VAM) Assessing) | ISCP Tabletop/Exercise | ISCP Tabletop/Exercise will need to be coordinated by the ISO with the AWS team. |  | | |  |
|  | NIST 800-53 RMF - Information System (VistA Adaptive Maintenance (VAM) Assessing) | Nessus Scan - Pre-Prod (Beta) Environment | null |  | | |  |
|  | NIST 800-53 RMF - Information System (VistA Adaptive Maintenance (VAM) Assessing) | PIA- Pending signature from PO | PIA is in pending signature from PO. |  | | |  |
|  | NIST 800-53 RMF - Information System (VistA Adaptive Maintenance (VAM) Assessing) | Secure Code Review (HP Fortify Scan) | Obtain the VAM - Secure Code Review (HP Fortify Scan) |  | | |  |
|  | NIST 800-53 RMF - Information System (VistA Adaptive Maintenance (VAM) Assessing) | Secure Design Review (Microsoft Threat Modeling Tool) | Need to obtain VAM Secure Design Review (Microsoft Threat Modeling Tool) |  | | |  |
|  | NIST 800-53 RMF - Information System (VistA Adaptive Maintenance (VAM) Assessing) | VAM DRP - TEST | VAM DRP - TEST needs to be scheduled by ISO. |  | | |  |
|  | NIST 800-53 RMF - Information System (VistA Adaptive Maintenance (VAM) Assessing) | VAM DRP- Pending Signature from ISO/PO | VAM DRP- Pending Signature from ISO/PO |  | | |  |
|  | NIST 800-53 RMF - Information System (VistA Adaptive Maintenance (VAM) | VAM IRP - Pending signature from ISO | Pending signature from ISO. Scheduled completion date is 10/26/18. |  | | |  |
|  |  |  |
|  |  |  |  |  | Page 10 of | 21 |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  | *Vulnerability Source* | *NIST 800-53 Control or VA Policy* | *Vulnerability Description* | *Response* | | |  |
|  | Assessing) |  |  |  |  |  |  |
|  | NIST 800-53 RMF - Information System (VistA Adaptive Maintenance (VAM) Assessing) | VAM ISCP - Pending signature from ISO | The ISCP is pending signature from the ISO. Scheduled Completion Date is expected to be 10/26. |  | | |  |
|  | NIST 800-53 RMF - Information System (VistA Adaptive Maintenance (VAM) Assessing) | WASA Testing - Pre-Prod (Beta) Environment | PENDING to receive WASA Testing - Pre-Prod (Beta) Environment |  | | |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  | Page 11 of | 21 |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  | **3.4.3 Step 3: Analyze Risk** |  |  |  |  |
|  |  |  |  |  |  |
|  | The risk analysis for each vulnerability consists of assessing the threats and compensating controls to determine the likelihood that vulnerability could be exploited and the potential impact should the vulnerability be exploited. A general depiction of the analysis is shown in Figure 1, where risk is the intersection of a threat and vulnerability, influenced by likelihood and impact | | | |  |
|  | |  |  |  | | --- | --- | --- | | **Figure 1: Components of Risk** | | | |  |  |  | | Essentially, risk is proportional to both likelihood of exploitation and possible impact. The following sections provide a brief description of each component used to determine the risk. | | | | | | |  |
|  |  |  |  |  |  |
|  |  |  | Page 12 of | 21 |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |
|  | **3.4.3.1 Likelihood** | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | The likelihood that a given vulnerability will be exploited by a threat is determined by analyzing the effectiveness of compensating controls against the threat capability. Compensating controls consist of measures in place that assist in mitigating the magnitude of a given vulnerability. Threat capability is defined as the means, opportunity, and motive of a given threat agent. Threat capabilities are defined in the table below. | | | | | | | |  |
|  | **Table 8: Threat Capability Components** | | | | | | | |  |
|  | *Component* | *Description* | | | | | | |  |
|  | Means | Means is the mechanism for fulfillment in exploiting the vulnerability. Threat agents are continuously achieving a higher level of means due to the level of sophistication available in easily obtained intrusion tools. | | | | | | |  |
|  | Opportunity | The opportunity for attack is determined by the threat agents’ level of access to the system. One of the greatest opportunity differences between threat agents is an insider versus an outsider to the organization, with the insider having far more opportunity to exploit vulnerabilities. | | | | | | |  |
|  | Motive | The motive of a threat agent is his or her desire to exploit a vulnerability. Motive can be influenced by the sensitivity of data, desire for monetary gain, or the potential public implications of an attach against a highly visible organization. | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Once the threat capability and compensating control effectiveness is assessed, for the vulnerability, the overall likelihood of the threat exploiting the vulnerability is determined using the matrix in the following table. | | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |
|  | **Table 9: Likelihood Matrix** | | | | | | | |  |
|  |  | *Compensating Control Effectiveness* | | | | |  |  |  |
|  | *Threat Capability* | Low | | Medium | High | |  |  |  |
|  | High | High | | High | Medium | |  |  |  |
|  | Medium | Medium | | Medium | Low | |  |  |  |
|  | Low | Low | | Low | Low | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | The likelihood of the vulnerability being exploited is the intersection of the threat capability category and the compensating control effectiveness category. For example, if the compensating control effectiveness is “High”, the resulting likelihood of exploitation is “Medium” likelihood for a “High” threat capability, “Low” likelihood for a “Medium” threat capability. The table below shows the definitions for each likelihood level. Note that a “High” effectiveness for compensating controls cannot completely reduce the likelihood of exploitation of a “High” capability threat. | | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |
|  | **Table 10: Likelihood Descriptors** | | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |
|  | *Likelihood* | *Description* | | | | | | |  |
|  | High | The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective. | | | | | | |  |
|  | Medium | The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability. | | | | | | |  |
|  | Low | The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | Page 13 of | | 21 |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |
|  | **3.4.3.2 Impact** | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Impact refers to the magnitude of potential harm that may be caused by successful exploitation. It is determined by the value of the resource at risk, both in terms of its inherent (replacement) value, its importance (criticality) to VA’s business missions, and the sensitivity of data contained within the system. The results of the system security categorization will be used to determine individual impact estimations for each finding. The level of impact is rated as High, Moderate, or Low and a description for each level of impact is provided in the following table. | | | | | | | |  |
|  | **Table 11: Impact Definitions** | | | | | | | |  |
|  | *Magnitude of Impact* | *Impact Definition* | | | | | | |  |
|  | High | Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization’s mission, reputation, or interest; or (3) may result in human death or serious injury. | | | | | | |  |
|  | Medium | Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization’s mission, reputation, or interest; or (3) may result in human injury. | | | | | | |  |
|  | Low | Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization’s mission, reputation, or interest. | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |
|  | **3.4.3.3 Risk Level** | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | The risk level for the finding is the intersection of the likelihood value and impact value as depicted in the following table. If a risk is evaluated as high, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan should put in place as soon as possible. If a risk is rated as medium, corrective actions are needed and a plan should be developed to incorporate these actions within a reasonable period of time. And finally, if a risk is categorized as low, officials should decide whether corrective action is required or if the risk should be accepted. | | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |
|  | **Table 12: Risk Level Matrix** | | | | | | | |  |
|  |  | *Impact* | | | | |  |  |  |
|  | *Likelihood* | High | | Moderate | Low | |  |  |  |
|  | High | High | | Medium | Low | |  |  |  |
|  | Medium | Medium | | Medium | Low | |  |  |  |
|  | Low | Low | | Low | Low | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | Page 14 of | | 21 |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  | **3.4.4 Step 4: Identify Recommended Corrective Actions** | | | |  |
|  |  |  |  |  |  |
|  | The finding and associated risk level was used to determine the recommendations that should be applied as a means to mitigate the risk. When identifying recommendations, the following were taken into consideration: level of effort, costs, emerging technologies, time constraints, and feasibility. | | | |  |
|  |  |  |  |  |  |
|  | **3.4.5 Step 5: Document Results** | | | |  |
|  |  |  |  |  |  |
|  | The results of the risk assessment were documented providing the finding, recommended corrective actions, likelihood, impact, and risk level. Refer to Section 4.0 for the risk assessment results. | | | |  |
|  | **4.0 Risk Assessment Results** |  |  |  |  |
|  |  |  |  |  |  |
|  | This section documents the technical and non-technical security risks to the system. These risks have been determined by applying the methodology outlined in Section 3 of this document to the vulnerabilities identified by the various risk assessment activities that have been performed for the system (e.g., documentation reviews, interviews, etc). The risk assessment results for the system are documented in the following table. The following provides a brief description of the information documented in each column:   1. **Identifier:** Provides a unique number for each risk.  2. **Risk:** Provides a brief description of the risk.  3. **Recommended Corrective Action:** Provides a brief description of the corrective action(s) recommended for mitigating the risks associated with the finding.  4. **Likelihood:** Provides the likelihood of a threat exploiting the vulnerability. This is determined by applying the methodology outlined in Section 3 of this document.  5. **Impact:** Provides the impact of a threat exploiting the vulnerability. This is determined by applying the methodology outlined in Section 3 of this document.  6. **Risk Level:** Provides the risk level (high, medium, low) for the vulnerability. This is determined by applying the methodology outlined in Section 3 of this document. The risks identified in the table below are based on security vulnerabilities identified from various sources outlined in Section 3.3 of this document. | | | |  |
|  |  |  |  |  |  |
|  |  |  | Page 15 of | 21 |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |
|  | **Table 13: Risk Assessment Results** | | | | | | | |  |
|  | *Risk ID* | *Risk* | *Recommended Corrective Action* | *Likelihood* | | *Impact* | *Risk* | |  |
|  | N/A | Not Provided | - |  | |  |  | |  |
|  | CA-08.1 | Obtain VAM Pen Test | - | Low | | Medium | Low | |  |
|  | N/A | ISCP Tabletop/Exercise will need to be coordinated by the ISO with the AWS team. | - | Low | | Medium | Low | |  |
|  | N/A | Need to obtain VAM Secure Design Review (Microsoft Threat Modeling Tool) | - | Low | | Medium | Low | |  |
|  | N/A | Not Provided | - | Low | | Medium | Low | |  |
|  | N/A | Obtain the VAM - Secure Code Review (HP Fortify Scan) | - | Medium | | Medium | Medium | |  |
|  | N/A | PENDING to receive WASA Testing - Pre-Prod (Beta) Environment | - | Medium | | Medium | Medium | |  |
|  | N/A | PENDING- Database Scan Pre-Prod (Beta) | - | Low | | Medium | Low | |  |
|  | N/A | PIA is in pending signature from PO. | - | Medium | | Medium | Medium | |  |
|  | N/A | Pending signature from ISO. Scheduled completion date is 10/26/18. | - | Low | | Medium | Low | |  |
|  | N/A | The ISCP is pending signature from the ISO. Scheduled Completion Date is expected to be 10/26. | - | Low | | Medium | Low | |  |
|  | N/A | VAM DRP - TEST needs to be scheduled by ISO. | - | Low | | Medium | Low | |  |
|  | N/A | VAM DRP- Pending Signature from ISO/PO | - | Low | | Medium | Low | |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | Page 16 of | | | 21 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  | Appendix A Acronyms List | | | |
|  |  |  |  |  |
|  | **3DES** Triple Data Encryption Standard (168 Bit) **ACIO** Associate Chief Information Officer **AC**L Access Control List **ADPAC** Automated Data Processing Applications Coordinator **AES** Advanced Encryption Services **AHMIA** American Health Information Management Association **AIS** Automated Information System(s) **AISO** Alternate Information Security Officer **ANSI** American National Standards Institute **AO** Authorizing Official **ATO** Authority to Operate **C&A** Certification & Accreditation **CBOC** Community Based Outpatient Clinic **CEO** Chief Executive Officer **CIO** Chief Information Officer **CIRT** Computer Incident Response Team **CMT** Cryptographic Module Testing (lab) **CMVP** Cryptographic Module Validation Program **COOP** Continuity of Operation Plan **COTS** Commercial Off-The- Shelf **CSE** Communications Security Establishment **CSP** Critical Security Parameters **DES** Data Encryption Standard **DNS** Domain Name Systems **DOD** Department of Defense **DRP** Disaster Recovery Plan **DSA** Digital Signature Algorithm **DSS** Digital Signature Standard **DTR** Derived Test Requirement **ECDSA** Elliptic Curve Digital Signature Algorithm **EDC** Error Detection Code **EFP** Environmental Failure Protection **EFT** Environmental Failure Testing **E-MAIL** Electronic Mail **EMC** Electromagnetic Compatibility **EMI** Electromagnetic Interference **FAX** Facsimile **FC** Fibre Channel **FIPS** Federal Information Processing Standard **FISMA** Federal Information Security Management Act of 2002 **FOIA** Freedom of Information Act **FOUO** For Official Use Only **FSM** Finite State Machine **GAO** General Accounting Office **GD** Government Division **GISRA** Government Information Security Reform Act **GSA** General Services Administration **HIPAA** Health Insurance Portability and Accountability Act of 1996 **HMAC** Keyed-hash Message Authentication Code **I&A** Identification and Authentication **IATO** Interim Authority to Operate **IDS** Intrusion Detection System **IG** Inspector General **IP** Internet Protocol **IRM** Information Resources Management **IPSEC** Internet Protocol Security | | | |
|  |  |  |  |  |
|  |  | Page 17 of | 21 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  | **IMRB** Internet Management Review Board **IP** Internet Protocol **IRM** Information Resources Management **IRS** Internal Revenue Service **ISO** Information Security Officer **IT** Information Technology **JCAHO** Joint Commission on Accreditation of Healthcare Organizations **KAT** Known Answer Test **LAN** Local Area Network **LEC** Local Exchange Company **MISS** Medical Information Security Service **MOU** Memorandum Of Understanding **MUMPS** Multi-User MEMS Processes **NIST** National Institute of Standards and Technology **NVLAP** National Voluntary Laboratory Accreditation Program **OI** Office of Information **OIG** Office of Inspector General **OMB** Office of Management and Budget **PBX** Private Branch Exchange **PFSS** Patient Financial Services System **PIN** Personal Identification Number **PIX** Private Internet Exchange (Cisco) **PKCS** #1 Public Key Cryptography Standards **PPD** Port Protection Device **RISO** Regional Information Security Officer **RNG** Random Number Generator **SAM** Security Account Manager **SBU** Sensitive But Unclassified **SHA** Secure Hash Algorithm **SSA** Social Security Administration **SSAA** System Security Authorization Agreement **SSH** Secure Shell **SSL** Secure Sockets Layer **ST&E** Security Test & Evaluation **TE** Test Evidence **VA** Veterans Affairs **VAOIG** Veterans Affairs Office of Inspector General **VE** Vendor Evidence **VHA** Veterans Health Administration **VISN** Veterans Integrated Service Network **VISTA** Veterans Health Information Systems and Technology **VMS** Virtual Memory System **VPN** Virtual Private Network **WAN** Wide Area Network | | | |
|  |  |  |  |  |
|  |  | Page 18 of | 21 |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | Page 19 of | 21 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  | Appendix B References | | | |
|  |  |  |  |  |
|  |  | Page 20 of | 21 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  | VA Directive 6500, "Managing Information Security Risk: VA Information Security Program VA Handbook 6500, "Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program VA Directive and Handbook 0710, “Personnel Suitability and Security Program” VA Directive and Handbook 0730, “Security and Law Enforcement” VA Directive and Handbook 6102, “Internet/Intranet Services” VA Directive 6502, “VA Enterprise Privacy Program” NIST SP 800-12, “An Introduction to Computer Security: The NIST Handbook” NIST SP 800-18, Revision 1, “Guide for Developing Security Plans for Federal Information Systems” NIST SP 800-23, “Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products” NIST SP 800-27, Rev A, “Engineering Principles for Information Technology Security (A Baseline for Achieving Security)” NIST SP 800-28 Version 2, “Guidelines on Active Content and Mobile Code” NIST SP 800-30 Revision 1, “Guide for Conducting Risk Assessments” NIST SP 800-34, Revision 1, “Contingency Planning Guide for Federal Information Systems” NIST SP 800-35, “Guide to Information Technology Security Services” NIST SP 800-36, “Guide to Selecting Information Security Products” NIST SP 800-37, Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach” NIST SP 800-40, Revision 3, “Guide to Enterprise Patch Management Technologies” NIST SP 800-46, Revision 1, “Guide to Enterprise Telework and Remote Access Security” NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems” NIST SP 800-48, Revision 1, “Guide to Securing Legacy IEEE 802.11 Wireless Networks” NIST SP 800-50, “Building an Information Technology Security Awareness and Training Program” NIST SP 800-53, Revision 4 Final, “Security and Privacy Controls for Federal Information Systems and Organizations” NIST SP 800-53A, Revision 4 Final, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans" NIST SP 800-56A, Revision 2, “Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography” NIST SP 800-57, Part 1-3, “Recommendation for Key Management” NIST SP 800-60, Revision 1, “Guide for Mapping Types of Information and Information Systems to Security Categories” NIST SP 800-61, Revision 2, “Computer Security Incident Handling Guide” NIST SP 800-63-2, “Electronic Authentication Guideline” NIST SP 800-64, Revision 2, “Security Considerations in the Information System Development Life Cycle” NIST SP 800-73-3, "Interfaces for Personal Identity Verification (4 Parts) NIST SP 800-78-3, "Cryptographic Algorithms and Key Sizes for Personal Identity Verification (PIV) NIST SP 800-88, Revision 1, "Guidelines for Media Sanitization" NIST SP 800-116, "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS) NIST SP 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) NIST SP 800-124, Revision 1, "Guidelines for Managing the Security of Mobile Devices on the Enterprise" NIST SP 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations" | | | |
|  |  |  |  |  |
|  |  | Page 21 of | 21 |  |