U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT AVMED HEALTH PLAN

Report Number 1C-ML-00-17-027
December 18, 2017

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at AvMed Health Plan

Report No. 1C-ML-00-17-027 **December 18, 2017**

Why Did We Conduct the Audit?

AvMed Health Plan (AvMed) contracts with the U.S. Office of Personnel Management as part of the Federal Employees Health Benefits Program (FEHBP).

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in AvMed's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by AvMed to process and store data related to medical encounters and insurance claims for FEHBP members.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the IT security controls of AvMed determined that:

- AvMed has an adequate risk assessment methodology in place. However, AvMed could make improvements in this area with more thorough vendor management and risk acceptance policies and procedures.
- Physical access controls could be improved to prevent unauthorized access to AvMed's data centers. Furthermore, logical access controls could be improved [redacted]
- AvMed could improve its network security posture by restricting access from [redacted] and improving network segmentation controls.
- Network monitoring policies and procedures are in place to detect and investigate security events. Furthermore, AvMed has a thorough incident response program in place.
- AvMed does not conduct full scope vulnerability scanning of its server network and does not have formally documented security configuration standards for its servers. In addition, AvMed does not have policies and procedures to ensure only supported software is used.
- AvMed maintains adequate disaster recovery and business continuity plans. However, its contingency plans are not tested routinely.
- AvMed has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately.

ABBREVIATIONS

AvMed	**AvMed Health Plan**
CFR	**Code of Federal Regulations**
COBIT	**Control Objectives for Information and Related Technologies**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information Security Controls Audit Manual**
GAO	**U.S. Government Accountability Office**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology's Special Publication**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
VPN	**Virtual Private Network**

TABLE OF CONTENTS

I. BACKGROUND

This final report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) data by AvMed Health Plan (AvMed).

The audit was conducted pursuant to FEHBP contracts CS 2876; 5 U.S.C. Chapter 89; and 5 Code of Federal Regulations (CFR) Chapter 1, Part 890. The audit was performed by the U.S. Office of Personnel Management's (OPM) Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended.

The FEHBP was established by the Federal Employees Health Benefits Act, enacted on September 28, 1959. The FEHBP was created to provide health insurance benefits for federal employees, annuitants, and qualified dependents. The provisions of the Act are implemented by OPM through regulations codified in Title 5, Chapter 1, Part 890 of the CFR. Health insurance coverage is made available through contracts with various carriers that provide service benefits, indemnity benefits, or comprehensive medical services.

This was our first audit of AvMed's information technology (IT) general and application controls. All AvMed personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit was greatly appreciated.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in AvMed's IT environments. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network security;
- Configuration management;
- Contingency planning; and
- Application controls specific to AvMed's claims adjudication system.

SCOPE AND METHODOLOGY

This performance audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of AvMed's internal controls through interviews and observations, as well as inspection of various documents, including IT and other related organizational policies and procedures. This understanding of AvMed's internal controls was used in planning the audit by determining the extent of compliance testing and other auditing procedures necessary to verify that the internal controls were properly designed, placed in operation, and effective.

The scope of this audit centered on the information systems used by AvMed to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Miami, Florida.

The onsite portion of this audit was performed in March and April of 2017. We completed additional audit work before and after the on-site visits at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at AvMed as of May 2017.

In conducting our audit, we relied to varying degrees on computer-generated data provided by AvMed. Due to time constraints, we did not verify the reliability of the data used to complete some of our audit steps, but we determined that it was adequate to achieve our audit objectives. However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable.

In conducting this review, we:

- Gathered documentation and conducted interviews;
- Reviewed AvMed's business structure and environment;
- Performed a risk assessment of AvMed's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM); and
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, we used judgmental sampling in completing our compliance testing.

Various laws, regulations, and industry standards were used as a guide for evaluating AvMed's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;
- U.S. Office of Management and Budget (OMB) Circular A-130, Appendix III;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- Control Objectives for Information and Related Technologies (COBIT) 5: A Business Framework for the Governance and Management of Enterprise IT;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, An Introduction to Computer Security: The NIST Handbook;

- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;

- 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 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy;

- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and

- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether AvMed's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, AvMed was not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. SECURITY MANAGEMENT

The security management component of this audit involved the examination of the policies and procedures that are the foundation of AvMed's overall IT security program. We evaluated AvMed's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

AvMed maintains a series of thorough IT security policies and procedures.

AvMed has implemented a series of formal policies and procedures that comprise its security management program. AvMed has developed a risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. AvMed has also implemented adequate human resources policies and procedures related to hiring, training, transferring, and terminating employees.

The following sections document opportunities for improvement related to AvMed's security management program.

1) Vendor Risk

AvMed contracts with external vendors to manage several business processes related to health claims processing. Potential security risks with these vendors are managed through a vendor assessment process that AvMed recently implemented. However, vendors that entered into a contract with AvMed prior to the implementation of this assessment process have not yet been subject to this review.

NIST SP 800-53, Revision 4, states that "Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities)." Failure to conduct risk assessments on all vendors to identify relevant threats, vulnerabilities, impacts, and likelihoods could leave AvMed unknowingly susceptible to adverse events.

Recommendation 1

We recommend that AvMed conduct risk assessments on all of its vendors to identify relevant risks to the organization. AvMed should also implement a process to monitor the vendor's remediation efforts for any identified risks.

AvMed Response:

"The Plan agrees with the recommendation. AvMed will extend its current 3rd Party Vendor Risk Assessment program to include all relevant vendors and incorporate monitoring processes for vendor risk remediation, to be implemented by June 1, 2018."

OIG Comment:

As part of the audit resolution process, we recommend that AvMed provide OPM's Healthcare and Insurance Audit Resolution Group with evidence when it has fully implemented this recommendation. This statement applies to subsequent recommendations in this audit report that AvMed agrees to implement.

2) Risk Acceptance

AvMed conducts security assessments on an annual basis to identify risks that may exist in information systems or processes. Risk mitigation strategies are implemented in response to risks identified from the security assessments. However, AvMed does not have a formal process to document, routinely monitor, and accept the risk from threats that cannot be fully addressed or mitigated at the time they are discovered.

NIST SP 800-100 states that "Because it is impracticable to eliminate all risk, it is important to note that even after the controls have been selected and implemented, some degree of residual risk will remain. The remaining residual risk should be analyzed to ensure that it is at an acceptable level." Failure to document and accept residual risk could result in risks remaining in the information system that are not known about or adequately controlled.

Recommendation 2

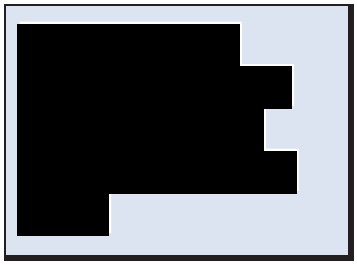
We recommend that AvMed implement an entity-wide risk acceptance program. This process should include policies and procedures to evaluate and formally accept the risk that remains after implementing security controls.

AvMed Response:

"The Plan agrees with the recommendation. AvMed will extend its current Risk Management program to incorporate a formal risk acceptance policy and procedure, to be implemented by December 31st, 2017."

B. ACCESS CONTROLS

Access controls are the policies, procedures, and techniques used to prevent or detect unauthorized physical or logical access to sensitive resources.



We examined the physical access controls at AvMed's facilities and datacenter. We also examined the logical access controls protecting sensitive data in AvMed's network environment and applications.

The access controls observed during this audit include, but are not limited to:

- Procedures for appropriately granting and removing physical access to facilities and the datacenter;
- Procedures to appropriately grant and adjust logical access to applications and software resources; and
- Routinely reviewing user access.

The following sections document opportunities for improvement related to AvMed's physical and logical access controls.

1. Privileged User Authentication

[redacted]

Recommendation 3

[redacted]

AvMed Response:

"The Plan agrees with the recommendation. [redacted]

2. Remote Access

Remote access to AvMed's information systems is granted via a virtual private network (VPN). [redacted]

[redacted]

Recommendation 4

[redacted]

AvMed Response:

"The Plan agrees with the recommendation. [redacted]

3. Segregation of Duties

AvMed employees are assigned access rights to information systems based on their job requirements. The specific access rights are documented in a "job code" for each unique position, and additional access rights may be granted with justification and approval. We were told that AvMed considered segregation of duties conflicts for roles in the finance and human resources departments. However, conflicting roles were not identified in areas such as claims processing and system administration that could present additional risk if assigned to one person.

FISCAM suggests that "organizations adopt segregation of duties control matrices as a guideline of the job responsibilities that should not be combined." Failure to properly identify conflicting roles increases the risk that employees are granted excess privileges that could be misused.

Recommendation 5

We recommend that AvMed create a segregation of duties matrix that identifies the roles for claims processors and IT administrators that could cause a segregation of duties conflict. We further recommend that AvMed review its current job codes to ensure that no segregation of duties conflicts exist.

AvMed Response:

"The Plan agrees with the recommendation. AvMed is developing matrices for both Claims Processors and IT Administrators along with a job code review, to be implemented by March 31, 2018."

4. Datacenter Physical Access

AvMed's primary datacenter is located within [redacted]. The secondary datacenter is located in [redacted]. Access to the primary and secondary datacenters is controlled by [redacted]. However, we expect datacenters of all FEHBP contractors to have the following controls that were not present at these AvMed facilities:

- [redacted]
- [redacted]

NIST SP 800-53, Revision 4, provides guidance for adequately controlling physical access to information systems containing sensitive data. Failure to implement adequate datacenter access controls increases the risk that unauthorized individuals can gain physical access to server hardware and networking equipment. Direct physical access could allow someone to bypass logical access controls and take over sensitive systems.

Recommendation 6

We recommend that AvMed implement [redacted] and technical controls to [redacted] at its primary and secondary datacenters.

AvMed Response:

"The Plan partially agrees with the recommendation. [redacted]

OIG Comment:

The solution described in the AvMed response appears to directly address our recommendation. AvMed should provide OPM's Healthcare and Insurance Audit Resolution Group with evidence when it has fully implemented this recommendation.

C. NETWORK SECURITY

Network security includes the policies and controls used to prevent or monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. We evaluated AvMed's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans that we performed during this audit.

We observed the following controls in place:

- Preventive controls at the network perimeter;
- Security event monitoring throughout the network; and
- A documented incident response program.

The following section documents several opportunities for improvement related to AvMed's network security controls.

1) Network Segmentation

AvMed has a firewall to control connections with systems outside of its network, and uses virtual local area networks to segment portions of its internal network. [redacted]

NIST SP 800-41, Revision 1, advises that, "Focusing attention solely on external threats leaves the network wide open to attacks from within. These threats may not come directly from insiders, but can involve internal hosts infected by malware or otherwise compromised by external attackers. Important internal systems should be placed behind internal firewalls." [redacted] increases the risk that a system could be compromised and allow unauthorized access to sensitive servers and data.

Recommendation 7

We recommend that AvMed [redacted]

AvMed Response:

"The Plan partially agrees with the recommendation. [redacted]

OIG Comment:

The solution described in the AvMed response appears to directly address our recommendation. AvMed should provide OPM's Healthcare and Insurance Audit Resolution Group with evidence when it has fully implemented this recommendation.

2) Network Access Controls

[redacted] This issue is compounded by the [redacted] discussed above. However, we were told that AvMed has a project in place to install technical tools to address this issue by the end of 2017.

NIST 800-53, Revision 4, states that an information system should uniquely identify and authenticate devices before establishing a network connection. Failure to control access to network ports could allow unauthorized users or devices to connect to sensitive network resources.

Recommendation 8

We recommend that AvMed implement network access controls to [redacted].

AvMed Response:

"The Plan agrees with the recommendation. AvMed is deploying a NAC-based solution with technical controls for [redacted]."

3) Administrator Rights

[redacted]

Unrestricted local administrator rights increase the risk of employees bypassing security policies.

FISCAM states that "Broad or special access privileges, such as those associated with operating system software that allow normal controls to be overridden, are only appropriate for a small number of users who perform system maintenance or manage emergency situations." Failure to restrict local administrator rights increases the risk

of employees bypassing security policies resulting in unapproved software installation and system misconfiguration.

Recommendation 9

We recommend that AvMed limit the number of personnel who have administrator rights and privileges on their workstations to those with a need based on their job function.

AvMed Response:

"The Plan agrees with the recommendation. AvMed is deploying a solution with technical controls which will restrict local administrative rights to a small number of IT administrative personnel, to be implemented by December 31, 2017."

4) Vulnerability Scanning

AvMed has contracts with a third-party to perform quarterly vulnerability scans on its external facing systems. However, authenticated vulnerability scans are not currently conducted on internal systems. AvMed has recently purchased a vulnerability scanning tool to conduct scans. While this is a step in the right direction, policies and procedures need to be developed to manage the vulnerability scanning process.

NIST SP 800-53, Revision 4, states that the organization should scan for "vulnerabilities in the information system and hosted applications [on a routine basis] and when new vulnerabilities potentially affecting the system/applications are identified and reported." Failure to maintain a comprehensive internal vulnerability scanning program increases the risk that system flaws would not be identified, leaving AvMed susceptible to attacks.

Recommendation 10

We recommend that AvMed develop policies and procedures to routinely perform authenticated scans on all servers and workstations in its networking environment.

AvMed Response:

"The Plan agrees with the recommendation. AvMed is currently developing policies and procedures for the routine performance of authenticated scans on Servers and Workstations in our networking environment, to be implemented by March 31, 2018[.]"

5. Vulnerability Management

As noted above, AvMed does not conduct authenticated scans on all assets within its networking environment. Furthermore, AvMed does not have a process in place to track or remediate known vulnerabilities.

NIST SP 800-53, Revision 4, states that an organization must identify, report, and correct information system flaws.

FISCAM states "When weaknesses are identified, the related risks should be reassessed, appropriate corrective or remediation actions taken, and follow-up monitoring performed to make certain that corrective actions are effective." Failure to track known vulnerabilities increases the risk that weaknesses are not corrected within AvMed's documented remediation timeframes.

Recommendation 11

We recommend that AvMed implement a process to centrally track the current status of security weaknesses identified during vulnerability scans.

AvMed Response:

"The Plan agrees with the recommendation. AvMed is developing a Vulnerability Management Lifecycle process which will identify vulnerabilities, report on and assess risk, and track and enforce the progress of remediation activities, to be implemented by March 31, 2018."

6. OIG Vulnerability Scanning

We conducted credentialed vulnerability and configuration compliance scans on a sample of servers in AvMed's network environment. The specific vulnerabilities that we identified were provided to AvMed in the form of an audit inquiry, but will not be detailed in this report.

NIST SP 800-53, Revision 4, states that organizations must remediate legitimate vulnerabilities identified in information systems and hosted applications. Failure to remediate vulnerabilities increases the risk that hackers could exploit system weaknesses for malicious purposes.

Recommendation 12

We recommend that AvMed remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided to them.

AvMed Response:

"The Plan agrees with the recommendation. AvMed is developing a Vulnerability Management Lifecycle process which will track and enforce the progress of remediation activities of technical weaknesses identified during the audit, to be implemented by March 31, 2018."

D. CONFIGURATION MANAGEMENT

Configuration management involves the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard. We evaluated AvMed's management of the configuration of its computer servers and databases. Our review found the following controls in place:

AvMed does not have defined security configuration standards for its server operating systems.

- Documented system change control process, and
- Change advisory board approval process.

The sections below document areas for improvement related to AvMed's configuration management controls.

1) Security Configuration Standards

AvMed uses pre-established system images to establish the initial configuration of new servers in its environment. Servers are then further configured according to functional requirements. However, AvMed does not have defined security configuration standards for its server operating systems. Security configuration standards are formally approved documents that list the specific security settings for each operating system that an organization uses to configure its servers.

NIST SP 800-53, Revision 4, states that an organization should establish and document "configuration settings for information technology products employed within the information system … that reflect the most restrictive mode consistent with operational requirements …." In addition, NIST SP 800-53, Revision 4, states that an organization must develop, document, and maintain a current baseline configuration of the information system.

Failure to establish approved system configuration settings increases the risk that the systems are not configured in a secure manner.

Recommendation 13

We recommend that AvMed document approved security configuration standards for all operating system platforms and databases deployed in its technical environment.

AvMed Response:

"The Plan agrees with the recommendation. AvMed is currently developing standards for currently deployed OS platforms and Databases. These standards will be developed using industry-standard benchmarks, to be implemented by March 31, 2018."

2) Security Configuration Auditing

As noted above, AvMed does not maintain approved security configuration standards for its operating platforms, and therefore it cannot effectively audit its system's security settings (i.e., there are no approved settings to which to compare the actual settings).

NIST SP 800-53, Revision 4, states that an organization must monitor and control changes to the configuration settings in accordance with organizational policies and procedures. FISCAM requires current configuration information to be routinely monitored for accuracy. Monitoring should address the baseline and operational configuration of the hardware, software, and firmware that comprise the information system. Failure to implement a configuration compliance auditing program increases the risk that servers are not configured appropriately; left undetected this can create a potential gateway for unauthorized access or malicious activity.

Recommendation 14

We recommend that AvMed implement a process to routinely audit the configuration settings of servers to ensure they are in compliance with the approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 13 are in place.

AvMed Response:

"The Plan agrees with the recommendation. AvMed will be implementing a Baseline Configuration scanning process to ensure adherence to approved standards as indicated in recommendation 13, to be implemented by June 1, 2018."

3) System Lifecycle Management

Our vulnerability assessment and review of AvMed's system inventory determined that [redacted] of AvMed's servers run on unsupported operating systems. AvMed provided us evidence that it is tracking unsupported operating systems. However, no policies or procedures exist that provide guidance on upgrading to supported software versions prior to the end of vendor support. Software vendors typically announce projected dates (known as end-of-life dates) for when they will no longer provide support or distribute security patches for their products. In order to avoid the risk associated with operating unsupported software, organizations must have a methodology in place to phase out software before it reaches its end-of-life date.

NIST SP 800-53, Revision 4, recommends that organizations replace "information system components when support for the components is no longer available from the developer, vendor, or manufacturer …." NIST SP 800-53, Revision 4, also states that "Unsupported components … provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components." Failure to upgrade system software leaves information systems open to known vulnerabilities without any remediation available.

Recommendation 15

We recommend that AvMed develop policies and procedures to ensure that information systems are upgraded to supported software versions prior to the end of vendor support.

AvMed Response:

"The Plan agrees with the recommendation. AvMed is developing policies and procedures which will provide proactive guidance on mitigating the risk of production OS platforms running beyond vendor supported dates, to be implemented by 12/31/2017[.]"

E. CONTINGENCY PLANNING

Contingency planning includes the policies and procedures that ensure adequate availability of information systems, data, and business processes. We reviewed the following elements of AvMed's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disruptive events occur:

AvMed maintains thorough disaster recovery and business continuity plans.

- Disaster recovery plan (e.g., recovery of hardware and software infrastructure);
- Business continuity plan (e.g., people and business processes);
- Disaster recovery plan tests; and
- Emergency response procedures.

We determined that the contingency planning documentation contained the critical elements suggested by NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems." AvMed has identified and prioritized the systems and resources that are critical to business operations, and has developed detailed procedures to recover those systems and resources.

The following section describes an area for improvement related to AvMed's contingency planning controls.

1) Business Continuity Plan and Disaster Recovery Plan Testing

AvMed does not perform business continuity plan testing on a routine basis to determine the effectiveness of the plan and the organizational readiness to execute the plan. Also, AvMed does not perform routine disaster recovery plan testing to ensure the timely recovery of its critical infrastructure.

NIST SP 800-34, Revision 1, states that contingency plan testing "helps [to] evaluate the viability of plan procedures, determine the ability of recovery staff to implement the plan, and identify deficiencies in the plan. Testing should occur at least annually and when significant changes are made to the IT system, supported business process(s), or the [IT contingency plan]." NIST SP 800-53, Revision 4, states that the organization must review the contingency plan test results and initiate corrective action.

Failure to test the business continuity plan and disaster recovery plan on a routine basis increases the risk that AvMed will not be able to continue business operations if unexpected events occur.

Recommendation 16

We recommend that AvMed routinely test its business continuity plan and disaster recovery plan, document the results, and use the results to update and improve the business continuity and disaster recovery plans.

AvMed Response:

"The Plan agrees with the recommendation. AvMed has conducted testing of its Business Continuity and Disaster Recovery plans, completed July 2017. Routine testing of AvMed's Business Continuity and Disaster Recovery plans will be conducted hereafter."

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting AvMed's claims adjudication process. AvMed prices and adjudicates claims using a commercially available claims processing application called Amisys. We reviewed the following processes related to claims adjudication: application configuration management, claims processing, member enrollment, and provider debarment.

1) Application Configuration Management

We evaluated the policies and procedures governing application development and change control over AvMed's claims processing systems.

AvMed has implemented policies and procedures related to application configuration management, and has also adopted a system development life cycle methodology that IT personnel follow during routine software modifications.

We observed the following controls related to testing and approval of software modifications:

- Policies and procedures that allow modifications to be tracked throughout the change process;

- Unit, integration, and user acceptance testing are conducted in accordance with industry standards; and

- A group independent from the software developers moves code between development and production environments to ensure separation of duties.

Nothing came to our attention to indicate that AvMed has not implemented adequate controls related to the application configuration management process.

2) Claims Processing System

We evaluated the business process controls associated with AvMed's claims processing system that ensure the completeness, accuracy, and confidentiality of transactions and data. We determined that AvMed has implemented policies and procedures to help ensure that:

- Claims are properly input and tracked to ensure timely processing;

- Claims are monitored as they are processed through the system with real time tracking of the system's performance; and

- Claims scheduled for payment are actually paid.

Nothing came to our attention to indicate that AvMed has not implemented adequate controls over its claims processing system.

3) Enrollment

We evaluated AvMed's procedures for managing its database of member enrollment data. Enrollment information is received electronically or in paper format and is either manually or

automatically loaded into the claims processing system. All enrollment transactions are fully audited to ensure information is entered accurately and completely.

Nothing came to our attention to indicate that AvMed has not implemented adequate controls over the enrollment process.

4) Debarment

AvMed has documented procedures for reviewing provider files for debarments and suspensions. AvMed's Audit Services & Investigations department downloads the OPM OIG debarment list monthly and compares the list to its provider information system to confirm any debarred providers. A flag is then installed in the claims system so that a hard edit will occur for any claim submitted by the debarred provider. Any claim submitted by a debarred provider adjudicates through the OPM OIG debarment process to include initial notification, a 15-day grace period, and then denial.

Nothing came to our attention to indicate that AvMed has not implemented adequate controls over the debarment process.

APPENDIX

AvMed Embrace better health.

October 25, 2017

OPM Team,

Below are the AvMed comments to the Draft Audit Report for your team's review.

Recommendation 1
We recommend that AvMed conduct risk assessments on all of its vendors to identify relevant risks to the organization. AvMed should also implement a process to monitor the vendor's remediation efforts for any identified risks.

AvMed Response

The Plan agrees with the recommendation. AvMed will extend its current 3rd Party Vendor Risk Assessment program to include all relevant vendors and incorporate monitoring processes for vendor risk remediation, to be implemented by June 1, 2018.

Recommendation 2
We recommend that AvMed implement an entity-wide risk acceptance program. This process should include policies and procedures to evaluate and formally accept the risk that remains after implementing security controls.

AvMed Response

The Plan agrees with the recommendation. AvMed will extend its current Risk Management program to incorporate a formal risk acceptance policy and procedure, to be implemented by December 31st, 2017.

Recommendation 3
[redacted]

AvMed Response

The Plan agrees with the recommendation. [redacted]

Recommendation 4
[redacted]

AvMed Response

The Plan agrees with the recommendation. [redacted]

Recommendation 5
We recommend that AvMed create a segregation of duties matrix that identifies the roles for claims processors and IT administrators that could cause a segregation of duties conflict. We further recommend that AvMed review its current job codes to ensure that no segregation of duties conflicts exist.

AvMed Response

The Plan agrees with the recommendation. AvMed is developing matrices for both Claims Processors and IT Administrators along with a job code review, to be implemented by March 31, 2018.

Recommendation 6
We recommend that AvMed implement [redacted] and technical controls to [redacted] at its primary and secondary datacenters.

AvMed Response

The Plan partially agrees with the recommendation. [redacted]

Recommendation 7
We recommend that AvMed [redacted]

AvMed Response

The Plan partially agrees with the recommendation. [redacted]

Recommendation 8
We recommend that AvMed implement network access controls to [redacted]

AvMed Response

The Plan agrees with the recommendation. AvMed is deploying a NAC-based solution with technical controls for [redacted]

Recommendation 9
We recommend that AvMed limit the number of personnel who have administrator rights and privileges to those with a need based on their job function.

AvMed Response

The Plan agrees with the recommendation. AvMed is deploying a solution with technical controls which will restrict local administrative rights to a small number of IT administrative personnel, to be implemented by December 31, 2017.

Recommendation 10
We recommend that AvMed develop policies and procedures to routinely perform authenticated scans on all servers and workstations in its networking environment.

AvMed Response

The Plan agrees with the recommendation. AvMed is currently developing policies and procedures for the routine performance of authenticated scans on Servers and Workstations in our networking environment, to be implemented by March 31, 2018

Recommendation 11
We recommend that AvMed implement a process to centrally track the current status of security weaknesses identified during vulnerability scans.

AvMed Response

The Plan agrees with the recommendation. AvMed is developing a Vulnerability Management Lifecycle process which will identify vulnerabilities, report on and assess risk, and track and enforce the progress of remediation activities, to be implemented by March, 31, 2018.

Recommendation 12
We recommend that AvMed remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided to AvMed.

AvMed Response

The Plan agrees with the recommendation. AvMed is developing a Vulnerability Management Lifecycle process which will track and enforce the progress of remediation activities of technical weaknesses identified during the audit, to be implemented by March, 31, 2018.

Recommendation 13
We recommend that AvMed document approved security configuration standards for all operating system platforms and databases deployed in its technical environment.

AvMed Response

The Plan agrees with the recommendation. AvMed is currently developing standards for currently deployed OS platforms and Databases. These standards will be developed using industry-standard benchmarks, to be implemented by March, 31, 2018.

Recommendation 14
We recommend that AvMed implement a process to routinely audit the configuration settings of servers to ensure they are in compliance with the approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 13 are in place.

AvMed Response

The Plan agrees with the recommendation. AvMed will be implementing a Baseline Configuration scanning process to ensure adherence to approved standards as indicated in recommendation 13, to be implemented by June, 1, 2018.

Recommendation 15
We recommend that AvMed develop policies and procedures to ensure that information systems are upgraded to supported software versions prior to the end of vendor support.

AvMed Response

The Plan agrees with the recommendation. AvMed is developing policies and procedures which will provide proactive guidance on mitigating the risk of production OS platforms running beyond vendor supported dates, to be implemented by 12/31/2017

Recommendation 16
We recommend that AvMed routinely test its business continuity plan and disaster recovery plan, document the results, and use the results to update and improve the business continuity and disaster recovery plans.

AvMed Response

The Plan agrees with the recommendation. AvMed has conducted testing of its Business Continuity and Disaster Recovery plans, completed July 2017. Routine testing of AvMed's Business Continuity and Disaster Recovery plans will be conducted hereafter.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone:

Toll Free Number:	(877) 499-7295
Washington Metro Area:	(202) 606-2423

By Mail:

Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100