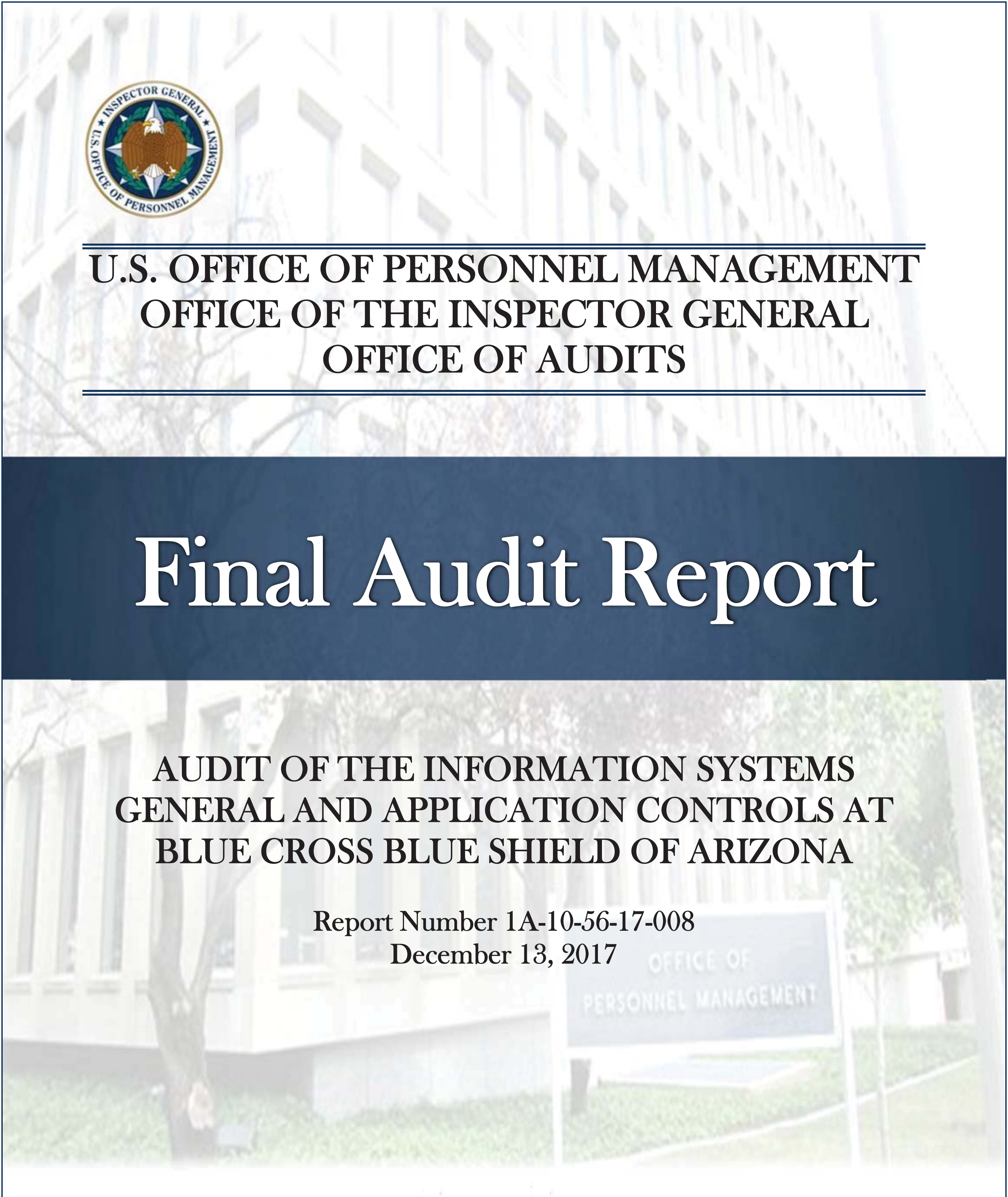

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT BLUE CROSS BLUE SHIELD OF ARIZONA

Report Number 1A-10-56-17-008
December 13, 2017

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Blue Cross Blue Shield of Arizona

Report No. 1A-10-56-17-008 **December 13, 2017**

Why Did We Conduct the Audit?

Blue Cross Blue Shield of Arizona (BCBSAZ) 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 BCBSAZ's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by BCBSAZ to process and store data related to 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 BCBSAZ determined that:

- BCBSAZ has established an adequate security management program.
- Physical access controls could be improved to prevent unauthorized physical access to [redacted]. Furthermore, logical access controls could be improved by implementing [redacted].
- BCBSAZ has not formally documented a firewall policy, and therefore it is unable to effectively audit its current firewall configuration settings against an approved standard.
- BCBSAZ does not conduct full scope vulnerability scanning using privileged access. Our independent vulnerability scanning exercise identified [redacted] servers that contained vulnerabilities, [redacted]. In addition, [redacted] workstations were running unsupported software.
- BCBSAZ has formally documented security configuration standards for its servers.
- BCBSAZ maintains adequate disaster recovery and business continuity plans, and its contingency plans are tested routinely. However, we believe that BCBSAZ's primary and backup data centers should be greater distances from each other.
- BCBSAZ has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately.

ABBREVIATIONS

BCBSAZ	Blue Cross Blue Shield of Arizona
CFR	Code of Federal Regulations
DMZ	Demilitarized Zone
FEHBP	Federal Employees Health Benefits Program
FEP	Federal Employee 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

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 Blue Cross Blue Shield of Arizona (BCBSAZ).

The audit was conducted pursuant to FEHBP contract CS 1039; 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 second audit of the information technology (IT) general and application controls at BCBSAZ. The previous audit resulted in Report No. 1A-10-56-06-007, dated November 16, 2006. All findings from the previous audit have been closed.

All BCBSAZ 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 BCBSAZ'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 BCBSAZ's claims processing 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 BCBSAZ'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 BCBSAZ'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 BCBSAZ to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Phoenix, Arizona.

The onsite portion of this audit was performed in January and February 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 BCBSAZ as of February 2017.

In conducting our audit, we relied to varying degrees on computer-generated data provided by BCBSAZ. 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 BCBSAZ's business structure and environment;
- Performed a risk assessment of BCBSAZ'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 BCBSAZ'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;
- 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 BCBSAZ's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, BCBSAZ was not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMNDATIONS

A. SECURITY MANAGEMENT

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

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

BCBSAZ has documented policies that outline its enterprise security management framework. BCBSAZ has also developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. BCBSAZ also has implemented human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that BCBSAZ does not have an adequate security management program.

B. ACCESS CONTROLS

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

We examined the physical access controls at BCBSAZ's facilities and data centers. We also examined the logical access controls protecting sensitive data in BCBSAZ's network environment and claims processing related applications.

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

- Procedures for appropriately granting, adjusting, and removing physical access to facilities and the data center;

- Procedures for appropriately granting, adjusting, and removing logical access to applications and software resources; and

- Robust physical and environmental controls within the primary data center.

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

1) [redacted] Physical Access Controls

As mentioned above, the primary data center has robust physical access controls that include multi-factor authentication and [redacted]. Access to the [redacted] requires multi-factor authentication, [redacted]

NIST SP 800-53, Revision 4, provides guidance for adequately controlling physical access to information systems containing sensitive data. Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to confidential data.

Recommendation 1

We recommend that BCBSAZ implement [redacted].

BCBSAZ Response:

"BCBSAZ agrees with this recommendation. BCBSAZ will work with our vendor [redacted]. The target implementation date is [redacted]."

OIG Comment:

As a part of the audit resolution process, we recommend that BCBSAZ 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 BCBSAZ agrees to implement.

2) Privileged User Authentication

Access to privileged user (system administrator) accounts at BCBSAZ requires multi-factor authentication when accessing systems from a remote location. However, [redacted]

[redacted]. We expect all FEHBP contractors to require [redacted] regardless of where the user is physically located. [redacted]

NIST SP 800-53, Revision 4, necessitates that [redacted] Failure to require [redacted] increases the risk of unauthorized access to sensitive data and the ability to modify system controls.

Recommendation 2

We recommend that BCBSAZ require [redacted].

BCBSAZ Response:

"Multi-factor authentication is in place. We have reviewed this recommendation and agree that BCBSAZ should [redacted]***. The target implementation date is*** [redacted]***."***

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 the BCBSAZ's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans 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 sections document several opportunities for improvement related to BCBSAZ's network security controls.

1) Documented Firewall Policy and Configuration Review

BCBSAZ has firewalls placed at key locations [redacted]. However, BCBSAZ has not formally documented a policy that specifies the [redacted] by the organization and the approved settings that are needed to harden the firewalls on the network.

BCBSAZ does not have a firewall policy, and no firewall configuration reviews are conducted.

NIST 800-41, Revision 1, states that "A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies." NIST 800-41, Revision 1, also states that rulesets should be reviewed or tested periodically to make sure that the firewall rules are in compliance with the organization's policies.

BCBSAZ is unable to effectively audit its current firewall configuration without an approved policy or standard because it does not have a baseline against which to compare the actual/current settings. Failure to document an approved firewall policy increases the risk that the firewall does not properly [redacted]. Additionally, failure to audit firewall configurations against a firewall policy or configuration standard increases the risk that unauthorized changes to the firewalls' configuration remain undetected.

<u>Recommendation 3</u>

We recommend that BCBSAZ document and approve a firewall policy customized to its technical environment that specifies the [redacted] by the organization and the approved settings of the firewalls.

<u>BCBSAZ Response:</u>

"BCBSAZ currently has technical practices in place that manage customized firewalls configurations. We accept the recommendation to develop a policy that requires documentation of our firewall configuration standards by [redacted]."

Recommendation 4

We recommend that BCBSAZ perform routine audits of its current firewall configurations against an approved firewall policy. Note – this recommendation cannot be implemented until the controls from Recommendation 3 are in place.

BCBSAZ Response:

"BCBSAZ currently has technical practices in place that manage customized firewalls configurations. We accept the recommendation to regularly audit against our documented firewall configuration standards and will begin doing so by [redacted]***."***

2) Authenticated Vulnerability Scans

BCBSAZ conducts routine vulnerability scanning only on [redacted]. Furthermore, not all of the scans performed on [redacted] are run with the privileged access necessary to conduct a thorough scan. BCBSAZ indicated that it plans to expand its vulnerability scanning program and perform authenticated scans on all servers by the [redacted]

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 ... ." NIST also advises that "The information system implements privileged access authorization … for … vulnerability scanning activities. … Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning."

Failure to perform full scope vulnerability scanning using privileged access increases the risk that BCBSAZ's systems could be compromised and sensitive data stolen or destroyed.

Recommendation 5

We recommend that BCBSAZ implement a process to routinely conduct vulnerability scans on its [redacted] and ensure the scans are conducted with sufficient access to perform a thorough scan.

BCBSAZ Response:

"BCBSAZ accepts the recommendation to enhance vulnerability scanning. The target implementation date is [redacted]."

3) Server Vulnerabilities

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

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

Recommendation 6

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

BCBSAZ Response:

"BCBSAZ has standard processes to regularly identify, risk assess, and remediate legitimate vulnerabilities. We have mitigating controls in place to protect our internal resources. We accept the recommendation and remediation efforts or documented risk acceptances are in progress. The target completion date is [redacted]."

4) Server Audit Logs

BCBSAZ policy requires systems to automatically generate audit logs and send them to a centralized system for analysis. The results of our configuration compliance scans identified [redacted] servers that [redacted].

FISCAM states that “significant events, including access to and modification of sensitive or critical system resources, should be logged.” Failure to log [redacted] impairs an organization's ability to detect and respond to [redacted] in an effective manner.

Recommendation 7

We recommend that BCBSAZ ensure that all servers are configured to [redacted]

BCBSAZ Response:

“Our policy at BCBSAZ is to [redacted]***. We accept the recommendation to ensure the standard is consistently applied*** [redacted] ***The target implementation date is*** [redacted]***.”***

D. CONFIGURATION MANAGEMENT

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

BCBSAZ has a documented Server Hardening Standard. However, security configuration auditing is not conducted.

- Documented Server Hardening Standard; and
- A thorough change management process.

The sections below document areas for improvement related to BCBSAZ’s configuration management controls.

1) Security Configuration Auditing

BCBSAZ configures servers using a standard image that is created using its Server Hardening Standard. BCBSAZ runs automated scripts for basic account and system maintenance tasks [redacted] However, it does not routinely audit server configurations against the Server Hardening Standard.

NIST SP 800-128 states that “SecCM [Security-focused configuration management] monitoring may be supported by numerous means, including, but not limited to ... Scanning to identify disparities between the approved baseline configuration and the actual configuration for an information system." NIST SP 800-128 also states that "If an information system is inconsistent with approved configurations as defined by the organization's baseline configurations … the organization may be unaware of potential vulnerabilities and not take actions that would otherwise limit those vulnerabilities and protect it from attacks."

Recommendation 8

We recommend that BCBSAZ implement a process to routinely audit the configuration settings of all operating platforms deployed in its technical environment to ensure they are in compliance with the approved Server Hardening Standard.

BCBSAZ Response:

"BCBSAZ has processes in place to implement approved security settings. We accept the recommendation to routinely audit security configuration settings to ensure compliance. The target implementation date is [redacted]."

2) User Workstation Application Management

BCBSAZ employees are not permitted to install applications on their workstations. This policy is enforced by restricting administrator rights on their user accounts. In certain cases the employee may be granted an exception to have administrator rights on their personal workstation. In these cases it is the user's responsibility to [redacted]) any applications that they install. However, our test work identified multiple workstations that were [redacted].

NIST SP 800-53, Revision 4, states that the organization should establish "[policies] governing the installation of software by users … Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both." Failure to properly manage software installations could expose the organization to vulnerable applications.

Recommendation 9

We recommend that BCBSAZ implement additional controls to ensure that software applications installed on user workstations are [redacted]

BCBSAZ Response:

"BCBSAZ accepts the recommendation to continue to enhance our controls around [redacted] The target completion date is [redacted]."

3) Server Patch Management

Software security patches are deployed to servers in the BCBSAZ network environment through a process outlined in documented policies and procedures. However, our vulnerability scans discovered [redacted] servers [redacted] that were not patched in compliance with the policies. The [redacted] indicates that there is a systemic control issue with BCBSAZ's patch management process.

NIST SP 800-53, Revision 4, states that organizations must identify, report, and correct information system flaws and install security-relevant software and firmware updates promptly. Failure to promptly install important updates increases the risk that vulnerabilities will not be remediated and sensitive information could be stolen.

Recommendation 10

We recommend that BCBSAZ implement additional controls to its patch management methodology to ensure that servers are updated with appropriate patches, service packs, and hotfixes in a timely basis.

BCBSAZ Response:

"BCBSAZ accepts the recommendation as it relates to patch management methodology and will enhance our process to strengthen patch compliance reporting which will include regular audits and remediation follow up. The target implementation date is [redacted]"

4) System Lifecycle Management

BCBSAZ's computer server inventory indicates that [redacted] servers are running unsupported versions of operating systems. Software vendors typically announce projected 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 process to anticipate end-of-life dates and phase out the deployment of such software prior to this window of exposure.

BCBSAZ has a continuous refresh process that aims to update systems every [redacted] However, it does not have formal policies and procedures to ensure that the process requirements are being met. BCBSAZ has planned upgrades for many of the outdated systems [redacted] However, [redacted]

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 could leave information systems vulnerable to known attacks without the possibility of remediation.

Recommendation 11

We recommend that BCBSAZ develop policies and procedures to ensure that information systems are upgraded to current versions prior to support for that software ending.

BCBSAZ Response:

"BCBSAZ accepts the recommendation to strengthen our policies and procedures related to software currency. The target implementation date is [redacted]***."***

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 BCBSAZ's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disruptive events occur:

BCBSAZ maintains and routinely tests its 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);

- Contingency 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." BCBSAZ 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. However, one opportunity for improvement related to BCBSAZ's contingency planning program is described below.

1) Primary and Backup Data Center Proximity

BCBSAZ's primary data and backup data centers are located less than a mile apart from each other. BCBSAZ stated that it conducted a study that determined it was acceptable to locate the data centers in such close proximity. We reviewed the study and determined that it did not contain sufficient evidence to make a fully informed risk-based decision. This study was conducted approximately ten years ago and did not involve a risk assessment.

NIST 800-34, Revision 1, states that, "Alternate processing facilities provide a location for an organization to resume system operations in the event of a catastrophic event that disables or destroys the systems primary facility."

Having the primary and backup data centers in such close proximity increases the risk that a single event could disrupt both data centers simultaneously.

Recommendation 12

We recommend that BCBSAZ conduct a risk assessment to identify the risks involved in having the primary and backup data center in close proximity and then make a determination if the risk is acceptable.

BCBSAZ Response:

"BCBSAZ accepts this recommendation. An independent third party will be engaged to evaluate and quantify the risk. The assessment will be completed by [redacted]***."***

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting BCBSAZ's claims adjudication process. BCBSAZ prices and adjudicates claims using a locally operated claims processing system and the BCBS Association's nationwide Federal Employee Program (FEP) Direct system. We reviewed the following processes related to the claims adjudication process: application configuration management, claims processing, and provider debarment.

1) Application Configuration Management

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

BCBSAZ has implemented policies and procedures related to application configuration management, and has also adopted a thorough system development life cycle methodology that IT personnel follow during software modifications. We observed the following controls related to testing and approvals of software modifications:

- Policies and procedures that allow modifications to be tracked throughout the change process;
- Unit, system, and user acceptance testing are conducted in accordance with a documented testing strategy; and
- A group independent from the software developers move code between development and production environments to ensure separation of duties.

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

2) Claims Processing System

We evaluated the input, processing and output controls associated with BCBSAZ's claims processing system. We determined that BCBSAZ has implemented policies and procedures to help ensure that:

- Paper claims that are received in the mail processing facilities are 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 BCBSAZ has not implemented adequate controls over its claims processing systems.

3) Debarment

BCBSAZ has documented procedures for reviewing the provider file for debarments and suspensions. BCBSAZ is notified by OPM that an update to the debarment list is available. BCBSAZ personnel review the list to determine if any debarred providers have active contracts with BCBSAZ. If an active provider is determined to be debarred, BCBSAZ personnel will update the provider file in FEP Direct and the corresponding provider file within the local claims processing system. BCBSAZ adheres to the OPM OIG debarment guidelines to include initial member notification, a 15-day grace period, and then denial of subsequent claims.

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

4) Application Controls Testing

We conducted a test on BCBSAZ's claims adjudication application to validate the system's processing controls. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which BCBSAZ's system adjudicated the claims.
Our test results did not identify any issues that have not been previously documented in prior OIG audits of BCBS organizations.

APPENDIX

July 28, 2017

[redacted], Auditor-in-Charge
Claims & IT Audits Group,
U.S. Office of Personnel Management (OPM)
1900 E Street, Room 6400
Washington, D.C. 20415-1100

BlueCross BlueShield Association

An Association of Independent
Blue Cross and Blue Shield Plans

Federal Employee Program
1310 G Street, N.W.
Washington, D.C. 20005
202.942.1000
Fax 202.942.1125

Reference: OPM DRAFT IT AUDIT REPORT
Blue Cross Blue Shield of Arizona (BCBSAZ)
Audit Report Number 1A-10-56-17-008
(Dated March 26, 2017)

The following represents the Plan's response as it relates to the recommendations included in the draft report.

A. SECURITY MANAGEMENT

No recommendation noted.

B. ACCESS CONTROLS

1. Backup Data Center Physical Access Controls

Recommendation 1

We recommend that BCBSAZ implement [redacted]

Plan Response

BCBSAZ agrees with this recommendation. [redacted] The target implementation date is [redacted].

2. Privileged User Authentication

Recommendation 2

We recommend that BCBSAZ require [redacted].

Plan Response

Multi-factor authentication is in place. We have reviewed this recommendation and agree that BCBSAZ should [redacted]. The target implementation date is [redacted].

C. NETWORK SECURITY

1. Documented Firewall Policy and Configuration Review

Recommendation 3

We recommend that BCBSAZ document and approve a firewall policy customized to its technical environment that specifies the [redacted] by the organization and the approved settings of the firewalls.

Plan Response

BCBSAZ currently has technical practices in place that manage customized firewalls configurations. We accept the recommendation to develop a policy that requires documentation of our firewall configuration standards by [redacted].

Recommendation 4

We recommend that BCBSAZ perform routine audits of its current firewall configurations against an approved firewall policy.

Note – this recommendation cannot be implemented until the controls from Recommendation 3 are in place.

Plan Response

BCBSAZ currently has technical practices in place that manage customized firewalls configurations. We accept the recommendation to regularly audit against our documented firewall configuration standards and will begin doing so by [redacted]

2. Authenticated Vulnerability Scans

Recommendation 5

We recommend that BCBSAZ implement a process to routinely conduct vulnerability scans on its [redacted] and ensure the scans are conducted with sufficient access to perform a thorough scan.

Plan Response

BCBSAZ accepts the recommendation to enhance vulnerability scanning. The target implementation date is [redacted]

3. Server Vulnerabilities

Recommendation 6

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

Plan Response

BCBSAZ has standard processes to regularly identify, risk assess, and remediate legitimate vulnerabilities. We have mitigating controls in place to protect our internal resources. We accept the recommendation and remediation efforts or documented risk acceptances are in progress. The target completion date is [redacted]

4. Server Audit Logs

Recommendation 7

We recommend that BCBSAZ ensure that all servers are configured to [redacted].

Plan Response

Our policy at BCBSAZ is to [redacted]. We accept the recommendation to ensure the standard is consistently applied [redacted] The target implementation date is [redacted]

D. CONFIGURATION MANAGEMENT

1. Security Configuration Auditing

Recommendation 8

We recommend that BCBSAZ implement a process to routinely audit the configuration settings of all operating platforms deployed in its technical environment to ensure they are in compliance with the approved security configuration standards.

Plan Response

BCBSAZ has processes in place to implement approved security settings. We accept the recommendation to routinely audit security configuration settings to ensure compliance. The target implementation date is [redacted].

2. User Workstation Application Management

Recommendation 9

We recommend that BCBSAZ implement additional controls to ensure that software applications installed on user workstations are [redacted].

Plan Response

BCBSAZ accepts the recommendation to continue to enhance our controls around [redacted]. The target completion date is [redacted]

3. Server Patch Management

Recommendation 10

We recommend that BCBSAZ implement additional controls to its patch management methodology to ensure that servers are updated with appropriate patches, service packs, and hotfixes in a timely basis.

Plan Response

BCBSAZ accepts the recommendation as it relates to patch management methodology and will enhance our process to strengthen patch compliance reporting which will include regular audits and remediation follow up. The target implementation date is [redacted].

4. **System Lifecycle Management**

Recommendation 11

We recommend that BCBSAZ develop policies and procedures to ensure that information systems are upgraded to current versions prior to support for that software ending.

Plan Response

BCBSAZ accepts the recommendation to strengthen our policies and procedures related to software currency. The target implementation date is [redacted].

E. CONTINGENCY PLANNING

Recommendation 12

We recommend that BCBSAZ conduct a risk assessment to identify the risks involved in having the primary and backup data center in close proximity and then make a determination if the risk is acceptable.

Plan Response

BCBSAZ accepts this recommendation. An independent third party will be engaged to evaluate and quantify the risk. The assessment will be completed by [redacted]

F. Claims Adjudication

No recommendation noted.

We appreciate the opportunity to provide our response to each of the recommendations in this report and request that our comments be included in their entirety and are made a part of the Final Audit Report. If you have any questions, please contact me at [redacted] or [redacted] at [redacted].

Sincerely,

[redacted]

[redacted], CISA
Managing Director, FEP Program Assurance

cc: [redacted], OPM
[redacted], FEP

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