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 SHIELD OF CALIFORNIA

Report Number 1A-10-67-16-040
January 24, 2017

EXECUTIVE SUMMARY

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

Report No. 1A-10-67-16-040 **January 24, 2017**

Why Did We Conduct the Audit?

Blue Shield of California (BSC) 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 BSC's information technology (IT) environment. This engagement was a follow-up audit where we performed test work that we were restricted from completing during a prior audit of BSC (Report No. 1A-10-67-14-006).

What Did We Audit?

The scope of this audit centered on the information systems used by BSC to process and store data related to insurance claims for FEHBP

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

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

- BSC has implemented an incident response and network security program. BSC has also implemented preventative controls at its network perimeter and performs security event monitoring throughout the network. However, we noted one area of concern related to BSC's network security controls:
  - BSC's information systems have not been subject to full-scope credentialed vulnerability scans.
- BSC has developed formal configuration management policies. However, we noted several areas of concern related to BSC's configuration management controls:
  - BSC's IT environment contains systems that are running on unsupported operating platforms.
  - BSC has not maintained, documented, and approved configuration standards for each operating platform used in its environment.
  - BSC's configuration compliance auditing program could be improved by incorporating the documented configuration standards mentioned above and by using appropriate credentials when performing compliance scanning.

ABBREVIATIONS

the Act	**The Federal Employees Health Benefits Act**
BSC	**Blue Shield of California**
BCBS	**Blue Cross Blue Shield**
BCBSA	**Blue Cross Blue Shield Association**
CFR	**Code of Federal Regulations**
DO	**Director's Office**
FEHBP	**Federal Employees Health Benefits Program**
FEP	**Federal Employee Program**
FISCAM	**Federal Information Systems Control 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**
Plan	**Blue Shield of California**

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY i

ABBREVIATIONS ii

I. **BACKGROUND** 1

II. **OBJECTIVES, SCOPE, AND METHODOLOGY** 2

III. **AUDIT FINDINGS AND RECOMMENDATIONS** 5

A. Network Security 5

B. Configuration Management 7

APPENDIX: Blue Shield of California's November 18, 2016, response to the draft audit report, issued September 16, 2016.

REPORT FRAUD, WASTE, AND MISMANAGEMENT

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) claims by Blue Shield of California (BSC or Plan).

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 (the 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.

The Blue Cross Blue Shield Association, on behalf of participating Blue Cross and Blue Shield (BCBS) plans, has entered into a Government-wide Service Benefit Plan contract (CS 1039) with OPM to provide a health benefit plan authorized by the FEHB Act. The Association delegates authority to participating local BCBS plans throughout the United States, such as BSC, to process the health benefit claims of its federal subscribers.

The Association has established a Federal Employee Program (FEP) Director's Office (DO) in Washington, D.C. to provide centralized management for the Service Benefit Plan. The FEP DO coordinates the administration of the contract with the Association, member BCBS plans, and OPM.

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 BSC's information technology (IT) environment. We accomplished these objectives by reviewing IT security controls related to BSC's network security and configuration management.

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 BSC'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 BSC'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.

This engagement was a follow-up audit where we performed test work related to network security and configuration management that BSC restricted us from completing during a prior audit (Report No. 1A-10-67-14-006, issued July 9, 2014). All recommendations from the prior audit have been closed. The business processes reviewed are primarily located in BSC's El Dorado Hills, California, facility.

The on-site portion of this audit was performed in May of 2016. We completed additional audit work before and after the on-site visit 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 controls in place at BSC as of June 2016.

In conducting our audit, we relied to varying degrees on computer-generated data provided by BSC. 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 BSC's business structure and environment;

- Performed a risk assessment of BSC'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 to evaluate BSC'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;

- Information Technology Governance Institute's COBIT: Control Objectives for Information and Related Technology;

- GAO's FISCAM;

- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security: The NIST Handbook;

- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology 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 BSC's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, BSC was not in complete compliance with all standards as described in the "Audit Findings and Recommendations" section of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. NETWORK SECURITY

Network security includes the policies and controls in place to manage and monitor the activity of a computer network and network-accessible resources.

We noted that BSC has implemented the following network security controls:

- A variety of controls protect and monitor the network perimeter. The interior network is segmented into multiple zones with different levels of trust, and unless specifically allowed, all cross traffic is denied;

- Security event monitoring is present throughout the network. BSC has contracted with a third party for network monitoring. This service includes consultation for system design, implementation, and ongoing monitoring and maintenance. The overall solution provides prevention services for HTTP/HTTPS based attacks, as well as protection against lateral attacks across the network; and

- A documented incident response program. BSC has implemented a Cyber Defense Center with standardized procedures and provides training in response activities and forensics.

The following section documents opportunities for improvement related to BSC's vulnerability management program.

1) Vulnerability Management

We initiated this audit to follow-up on concerns we raised during a 2014 IT audit of BSC regarding the organization's vulnerability management program. In the prior audit, BSC prohibited us from performing automated vulnerability scans on its computer servers – a routine step in all of our IT audit engagements. In an alternate effort to meet our audit objective we asked BSC to perform these scans on our behalf. However, BSC was unable to successfully perform the scans on 75 percent of the servers we selected, nor was it able to produce historical scans of the selected servers. As a result, we were unable to independently attest that BSC had a vulnerability management program in place.

During this current audit, BSC willingly allowed us to perform our own automated vulnerability scans and to thoroughly review its vulnerability management program.

Our test work in this area began with interviewing BSC personnel to learn about the organization's procedures for performing vulnerability scans. During the interview we were told that every computer server is scanned on a monthly basis, and that the scans are performed using privileged user credentials that allow the scanning tool to collect all of the data necessary for a comprehensive scan.

We subsequently requested evidence to support the statements made in the interview. Specifically, we requested three iterations of historical vulnerability scan reports (scans from three different months) for a sample of 20 servers. In response, BSC provided us with screenshots (images) of the scanning tool's configuration settings and a statement indicating that the images "*show that all systems in the list are being subject to vulnerability scans*" and that "*credentialed scans are being performed*."

BSC's vulnerability scan reports indicated that [redacted] servers sampled were scanned during the three months tested.

However, this evidence did not fully support BSC's statements, and we insisted BSC provide the full historical scan reports as we had originally requested. BSC ultimately provided the scan reports, and these reports indicated that [redacted] servers were subject to a vulnerability scan during any of the three months, and [redacted] was subject to a scan in more than one month. In addition, the content of the scan reports made it apparent that these scans were not run with the privileges necessary to perform a thorough analysis. BSC subsequently provided a statement acknowledging that its original attestation that *"all scans are credentialed"* was not accurate, as the historical vulnerability scans were, in fact, not run with the credentials necessary to perform a thorough scan.

The vulnerability scans that we independently performed during this audit identified several vulnerabilities that could have been previously detected by BSC had it been routinely running credentialed vulnerability scans on its servers. The 2014 audit report states that BSC "has not implemented a full scope vulnerability management program for servers housed in the data center it maintains. . . ." The test work performed during this audit indicates that this statement is still applicable.

NIST SP 800-53, Revision 4, requires that an organization "Scans for vulnerabilities in the information system and hosted applications" on an organization defined frequency, and that "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 with proper privileged user credentials significantly decreases BSC's ability to identify and remediate security vulnerabilities.

Recommendation 1

We recommend that BSC implement a comprehensive vulnerability management program that includes routine credentialed vulnerability scans against all servers.

BSC Response:

"BSC agrees with this recommendation. BSC worked on the implementation of credentialed vulnerability scanning after the OIG completed [its] on-site [fieldwork] and completed the implementation prior to the issuance of the draft report."

OIG Comment:

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

B. CONFIGURATION MANAGEMENT

Configuration management controls are the activities focused on establishing and maintaining the integrity of information systems through control of processes for initializing, changing, and monitoring the configurations of those systems throughout the system development life cycle. We evaluated BSC's configuration management program as it relates to the systems that support the processing of FEHBP claims, and determined that the following controls were in place:

- Configuration management policies and procedures that include defined roles and responsibilities for the different stakeholders involved in the configuration management process; and

- Procedures for ensuring software patches are installed in a timely manner.

Although BSC has a configuration management program in place, the following sections document several areas where this program could be improved.

1) System Lifecycle Management

BSC has a policy in place that states that all operating platforms in its environment must not have reached their "end-of-life" and that there must be a vendor, organization, or other entity providing ongoing security patches. However, our analysis of BSC's system inventory revealed that [redacted]

BSC's system inventory included operating systems that are unsupported, [redacted]

Software vendors typically advertise the dates that they will no longer provide support or distribute security patches for their products (referred to as end-of-life dates). In order to avoid the risk associated with having critical business operations dependent on unsupported software, organizations must have a process in place to anticipate end-of-life dates and phase out such software prior to this window of exposure.

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 result in information systems containing security vulnerabilities to which no remediation is available.

Recommendation 2

We recommend that BSC decommission all unsupported operating systems in its environment, and that it update its policies and procedures to include additional controls ensuring that software is phased out before its end-of-life date.

BSC Response:

"BSC agrees with this recommendation. BSC has been addressing the decommissioning of end-of-life systems. BSC has identified the remaining operating systems which are end-of-life and action plans to retire them are being finalized. Action plans for these systems and any necessary associated security exception documentation will be completed by

[redacted]. ***Additionally, by*** [redacted]***, BSC will also enhance our processes to ensure software is phased out before its end-of-life date."***

2) Configuration Standards

Our 2014 audit determined that BSC did not maintain, document, or approve configuration standards for all operating systems used in its environment. In response to the 2014 draft audit report, BSC stated that it had implemented a new policy where the Center for Internet Security (CIS) benchmarks would be used as a guide for developing configuration standards for all of its servers. We noted in the 2014 final audit report that this was an improvement, but that evidence was still needed to indicate that BSC's configuration standards had been customized to "include approved deviations and exceptions from CIS standard benchmarks." The prior recommendation was subsequently closed when BSC provided evidence that it had developed comprehensive configuration standards that were customized to the BSC environment and addressed deviations from the CIS benchmarks.

As part of this current audit we again requested copies of BSC's configuration standards. In response, BSC provided us with a limited sample of approximately 40 settings, but the response did not include the approved value of each setting. For example, the response listed a configurable setting of "maximum password age," but did not indicate the actual value that BSC had approved for this setting (i.e., how many days before a user is forced to change their password).

The documentation provided by BSC during this audit does not indicate that the organization has comprehensive operating system configuration standards in place. The list of approximately 40 values that we were provided is far less comprehensive than a typical configuration standard (e.g., the CIS benchmark), and did not include the exceptions that were described in the documentation that BSC had previously provided to OPM in an effort to close the 2014 audit recommendation. It appears that BSC stopped following (or did not fully implement) the configuration standard framework that it established in response to the 2014 audit finding.

NIST SP 800-53, Revision 4, identifies the need for an organization to establish, implement, document deviations, and monitor configuration settings. It also states that configuration settings must include "(i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections."

BSC has not developed and approved configuration standards for each operating system.

Failure to establish thorough system configuration standards increases the risk that information systems may not meet performance or security requirements defined by the organization.

Recommendation 3

We recommend that BSC formally document and approve a set of configuration standards for each operating platform in its network environment, and that the settings reflect the most restrictive mode consistent with the operational requirements. If BSC leverages existing configuration standards (e.g., CIS benchmarks) as a guide, then BSC's standards should document the deviations and exceptions required for its unique technical environment.

BSC Response:

"BSC agrees with this recommendation. BSC has defined, risk-based configuration standards for security for hardening for each operating platform in our network environment. By [redacted], BSC will update our hardening framework to ensure that our configuration standards are refreshed as new/updated CIS Benchmarks are published."

3) Compliance Auditing

BSC could improve its procedures by auditing the current configuration of its computer servers against an approved standard. Our 2014 audit report indicated that BSC conducted compliance audits on its servers using generic CIS benchmarks, but that these audits were not fully effective as there was not a BSC-specific standard to audit against. We recommended that BSC routinely audit security configuration settings using its own approved baselines. This recommendation was subsequently closed when BSC provided evidence that it had developed customized configuration standards and was routinely auditing against those standards using an automated scanning tool.

As part of this audit we evaluated this new process and identified several areas of concern with BSC's compliance auditing methodology:

- There were multiple servers scanned with the wrong configuration standard (e.g., [redacted] systems were audited against [redacted] settings). Auditing a [redacted] system with a [redacted] configuration standard will produce little to no meaningful results. In effect, these systems are not being subjected to compliance auditing at all;

- Multiple scans were performed without the necessary privileges to perform a thorough analysis. Scans performed without system credentials that allow the scanning tool to authenticate to the scan target may not be able to collect the information necessary to audit each configuration setting;

- As stated in the section above, BSC has not documented comprehensive operating system configuration standards that are customized to its specific environment. Compliance audits performed against generic standards are only minimally effective; and

- We did not receive evidence that [redacted]

FISCAM states that organizations should require, "Current configuration information [to] be routinely monitored for accuracy. Monitoring should address the current baseline and operational configuration of the hardware, software, and firmware that comprise the information system."

Failure to implement a thorough configuration compliance auditing program increases the risk that insecurely configured servers exist undetected.

Recommendation 4

We recommend that BSC routinely audit all of its servers and [redacted] against the comprehensive configuration standards established in response to Recommendation 3. If automated scanning tools are used to perform these audits, BSC should ensure that the tools have the appropriate system privileges to perform a thorough scan.

BSC Response:

"BSC agrees with this recommendation. By [redacted], BSC will enhance the routine audits of all of our servers and [redacted] to ensure they are utilizing appropriate configuration standards and that the tools used for the configuration scanning have appropriate privileges to perform the scans."

APPENDIX

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

November 18, 2016

[redacted]
Chief, Information Systems Audit Group
U.S. Office of Personnel Management (OPM)
1900 E Street, Room 6400
Washington, D.C. 20415-1100

Reference: OPM DRAFT IT AUDIT REPORT
Blue Shield of California (BSC) Follow-up
Audit Report Number 1A-10-67-16-040
(Dated September 16, 2016)

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

A. Network Security

1. Vulnerability Management

Recommendation 1

We recommend that BSC implement a comprehensive vulnerability management program that includes routine credentialed vulnerability scans against all servers.

Plan Response

BSC agrees with this recommendation. BSC worked on the implementation of credentialed vulnerability scanning after the OIG completed their on-site and completed the implementation prior to the issuance of the draft report.

B. Configuration Management

2. System Lifecycle Management

Recommendation 2

We recommend that BSC decommission all unsupported operating systems in its environment, and that it update its policies and procedures to include additional controls ensuring that software is phased out before its end-of-life date.

Plan Response

BSC agrees with this recommendation. BSC has been addressing the decommissioning of end-of-life

systems. BSC has identified the remaining operating systems which are end-of-life and action plans to retire them are being finalized. Action plans for these systems and any necessary associated security exception documentation will be completed by [redacted]. Additionally, by [redacted], BSC will also enhance our processes to ensure software is phased out before its end-of-life date.

3. Configuration Standards

Recommendation 3

We recommend BSC formally document and approve a set of configuration standards for each operating platform in its network environment, and that the settings reflect the most restrictive mode consistent with the operational requirements. If BSC leverages existing configuration standards (e.g., CIS benchmarks) as a guide, then BSC's standards should document the deviations and exceptions required for its unique technical environment.

Plan Response

BSC agrees with this recommendation. BSC has defined, risk-based configuration standards for security for hardening for each operating platform in our network environment. By [redacted], BSC will update our hardening framework to ensure that our configuration standards are refreshed as new/updated CIS Benchmarks are published.

4. Compliance Auditing

Recommendation 4

We recommend BSC routinely audit all of its servers and [redacted] against the appropriate configuration standards. If automated scanning tools are used to perform these audits, BSC should ensure that the tools have the appropriate system privileges to perform a thorough scan.

Plan Response

BSC agrees with this recommendation. By [redacted], BSC will enhance the routine audits of all of our servers and [redacted] to ensure they are utilizing appropriate configuration standards and that the tools used for the configuration scanning have appropriate privileges to perform the scans.

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], FEP
[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