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 Arkansas Blue Cross Blue Shield

Report Number 1A-10-44-21-017
November 15, 2021

Executive Summary

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

Report No. 1A-10-44-21-017 **November 15, 2021**

Why Did We Conduct the Audit?

Arkansas Blue Cross Blue Shield (ABCBS) 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 ABCBS's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by ABCBS 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 ABCBS's IT security controls determined that:

- Management of ABCBS's network inventory could be improved.
- Segregation of duty risk assessments have not been performed for provisioned entitlements.
- ABCBS is working toward completing vendor risk assessments.
- Adequate physical and logical access controls are in place.
- [redacted]
- [redacted]
- The enterprise security event monitoring and incident response programs are adequate.
- The contingency planning program is adequate.
- ABCBS has adequate application change control policies and procedures.

Abbreviations

ABCBS	**Arkansas Blue Cross Blue Shield**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information System Controls Audit Manual**
GAO	**U.S. Government Accountability Office**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology Special Publication**
OIG	**Office of the Inspector General**
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 Arkansas Blue Cross Blue Shield (ABCBS).

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 or comprehensive medical services.

This was our initial audit of the information technology (IT) general security and application controls at ABCBS. All ABCBS 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 make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit were 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 ABCBS's IT environment. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network security;
- Security event monitoring and incident response;
- Configuration management;
- Contingency planning; and
- Application controls specific to ABCBS'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 ABCBS's internal controls through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of ABCBS'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 ABCBS to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Little Rock, Arkansas.

Due to social distancing guidance related to COVID-19, all audit work was completed remotely. The remote work performed included teleconference interviews of subject matter experts, documentation reviews, and remote testing of the general and application controls in place over ABCBS's information systems. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general controls in place at ABCBS as of May 2021.

In conducting our audit, we relied to varying degrees on computer-generated data provided by ABCBS. 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.

We used the judgmental sampling technique throughout the audit. Results of judgmentally selected samples cannot be projected to the population since it is unlikely that the results are representative of the population as a whole.

In conducting this audit, we:

- Performed a risk assessment of ABCBS'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);
- Gathered documentation and conducted interviews;
- Reviewed ABCBS's business structure and environment; 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 ABCBS's control structure. These criteria included, but were not limited to, the following publications:

- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations; and
- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall policy.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether ABCBS's practices were consistent with applicable standards. While generally compliant with respect to the items tested, ABCBS 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 an examination of the policies and procedures of ABCBS's overall IT security program. We evaluated ABCBS's ability to develop security policies, manage risk, assign security related responsibility, and monitor the effectiveness of various system related controls.

ABCBS has developed adequate IT security policies and procedures. ABCBS has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments.

However, we noted the following opportunities for improvement related to ABCBS's security management program.

1. Network Inventory Management

The ABCBS Systems Lifecycle Management Policy states that the information asset inventory shall be maintained to include all systems, services, hardware, software, and related equipment used in the operation of all lines of business. We were told that there is a project in place to identify the IT assets unaccounted for and incorporate them into the configuration management database by the first quarter of 2022.

NIST SP 800-53, Revision 5, states that organizations should "Develop and document an inventory of system components ,,, ." NIST also says that the organization should "Maintain the currency, completeness, accuracy and availability of the information system components ....."

Failure to maintain an accurate network inventory increases the risk that IT assets in the environment may be exploitable.

Recommendation 1

We recommend that ABCBS complete its project to ensure that a complete and accurate inventory is maintained for all IT assets.

ABCBS's Response:

"ABCBS agrees with the recommendation and will have this implemented by June 30, 2022."

OIG Comments:

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

2. Segregation of Duty Risk Assessments

ABCBS's Access Control Policy states that access shall be granted based on the principles of need-to-know, segregation of duties, and least privilege, allowing the lowest level of access to a user, process, or program to meet business needs. We were provided an entitlement dictionary [redacted] routine reviews to ensure roles are needed, [redacted] ABCBS is currently in the process of reviewing, updating, and implementing stronger role-based access controls.

NIST SP 800-53, Revision 5, states that organizations should "Identify and document . duties of individuals requiring separation . ."

[redacted]

Recommendation 2

We recommend that ABCBS assess segregation of duty risks to the organization's application roles.

ABCBS's Response:

"ABCBS agrees with the recommendation and will have this implemented by December 31, 2022."

3. Vendor Risk Assessments

The vendor risk management program could be improved.

The Third-Party Security Due Diligence Policy established a mandate to evaluate and identify information security risks associated with conducting business with contracted parties. The policy states that due diligence of external parties may be conducted via various methods and that due diligence assessments are required prior to the establishment of a third-party relationship. We requested evidence of vendor questionnaires prior to contracting, evidence of risk ranking vendors, and ongoing risk assessments for vendors who store FEHBP member data. We were told that ABCBS has recently implemented a Third-Party Risk Management process used to assess vendors; however, the program has not been fully implemented. Work remains to identify the most critical vendors and implement assessments on an annual basis.

NIST SP 800-53, Revision 5, states that a risk assessment should include the likelihood and harm from the disclosure of the information a system processes, stores, or transmits. NIST also states that the organization should "Assess and review the supply chain related risks associated with the suppliers or contractors . . . or service they provide . ."

Failure to perform routine assessments of vendors increases the risk of FEHBP member data misuse and an increase in the likelihood of a potential breach.

Recommendation 3

We recommend that ABCBS perform risk assessments of its vendors prior to the establishment of a contract and routinely afterward in accordance with NIST and its own policy.

ABCBS's Response:

"ABCBS agrees with the recommendation and will have this implemented by July 31, 2022."

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 ABCBS's facilities and data center. We also examined the logical access controls protecting sensitive data in ABCBS's network environment and claims processing applications.

The access controls observed during this audit included, but were not limited to:

- Routine access audits for secure areas;
- Procedures for appropriately granting and removing physical access to facilities and data centers; and
- Procedures for appropriately granting and adjusting logical access to applications and software resources.

Nothing came to our attention to indicate that ABCBS has not implemented adequate controls over its access control processes.

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 ABCBS's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans performed during the audit.

We observed the following controls in place:

- Perimeter controls protecting public and partner network connections;
- Network access controls to prevent unauthorized devices on the internal network; and
- Documented policies and procedures to identify and respond to information security incidents.

The following sections document opportunities for improvement related to ABCBS's network security controls.

1. Vulnerability Management

ABCBS conducted credentialed vulnerability and configuration compliance scans on a sample of servers in its network environment on our behalf. We chose a sample of 181 servers from a universe of 268. The sample selection included a variety of system functionality and operating systems across production, test, and development. The judgmental sample was drawn from systems that store and/or process Federal member data, as well as other systems in the same general control environment that contain Federal member data. The results of the judgmentally selected sample were not projected to the population since it is unlikely that the results are representative of the population.

[redacted]

[redacted]

NIST SP 800-53, Revision 5, states that organizations should scan for vulnerabilities in the information system and hosted applications, analyze the reports, and remediate legitimate vulnerabilities.

[redacted]

Recommendation 4

[redacted]

ABCBS's Response:

"ABCBS agrees with the recommendation and has fully resolved and addressed all patches, vulnerabilities and security concerns noted by the OIG Audit Inquiry. ABCBS will provide the support evidence on the upcoming OPM Audit Resolution & Compliance update."

2. Firewall Ruleset Review

ABCBS's Firewall Management Policy states that all new configuration rules beyond a baseline hardened configuration that allows traffic to flow through shall be documented and recorded.

[redacted]

NIST SP 800-41, Revision 1, states that rulesets should be reviewed or tested periodically to make sure that the firewall rules are in compliance with the organization's policies.

[redacted]

Recommendation 5

[redacted]

ABCBS's Response:

"ABCBS agrees with the recommendation and will have this implemented by August 31, 2021."

D. Security Event Monitoring and Incident Response

Security event monitoring involves the collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the investigation and reporting of such activity. Incident response consists of an incident response plan identifying roles and responsibilities, response procedures, training, and reporting.

Our review of ABCBS's security event monitoring and incident response programs identified the following controls in place:

- Adequate procedures to collect logs and analyze events;
- Technical controls to monitor incoming and outgoing network traffic; and
- A documented incident response plan.

Nothing came to our attention to indicate that ABCBS has not implemented adequate security event monitoring and incident response controls.

E. 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. ABCBS employs a team of technical personnel who manage system software configuration for the organization. We evaluated ABCBS's management of the configuration of its computer servers and databases.

We observed the following controls in place:

- An adequately documented configuration management policy;
- A documented and approved exception process; and
- An established patch management process.

However, we noted the following opportunities for improvement related to ABCBS's configuration management controls.

1. Security Configuration Standards

ABCBS has a project in place to evaluate, implement, and audit security configuration standards.

Security configuration standards are formally approved documents that list specific security settings. ABCBS's Baseline Configuration Policy states that system configurations are to be built using government and industry standards including Defense Information Systems Agency Security Technical Implementation Guides and Center for Internet Security Benchmarks. The policy further states that deviations from the baseline configurations will be documented and approved. We were told that the implementation of the security configuration settings is a new process and is currently being evaluated and implemented. We were provided a project plan that is scheduled to be completed in September of 2021.

NIST SP 800-53, Revision 5, states that the organization should "Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements . ." NIST further states that the organization should "Identify, document, and approve any deviations from established configuration settings . ."

Failure to establish approved security configuration standards increases the risk that systems may not be configured in a secure manner.

Recommendation 6

[redacted]

ABCBS Response:

"ABCBS agrees with the recommendation and will have this implemented by July 31, 2022."

OIG Comments:

In response to the draft audit report, ABCBS provided evidence of its documented compliance auditing process, compliance status, and risk exceptions in place while evaluation and remediation efforts are addressed. While we recognize that some work has been completed, ABCBS has not provided evidence that the specific deviations from its baseline configurations have been documented. We continue to recommend that

ABCBS implement security configuration standards by documenting the specific deviations from its benchmarks.

2. Security Configuration Auditing

[redacted]

NIST SP 800-53, Revision 5, states that the organization should "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 security configuration auditing program increases the risk that systems are not configured appropriately and left undetected can create a potential gateway for unauthorized access or malicious activity.

Recommendation 7

[redacted]

ABCBS's Response:

"ABCBS agrees with the recommendation and will have this implemented by July 31, 2022."

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

ABCBS has adequate controls over contingency planning.

The controls observed during this audit included, but were not limited to:

- Environmental controls to minimize disruptions;
- Alternate processing site with controls equivalent to the primary site and sufficient resources to transfer and resume operations; and
- Adequately documented disaster recovery plan tests.

Nothing came to our attention to indicate that ABCBS has not implemented adequate contingency planning controls.

G. Application Change Control

We evaluated the policies and procedures governing ABCBS's application development and change control process.

ABCBS 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 approvals of software modifications:

- An adequately documented application change control process;
- Unit, integration, and user acceptance testing 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 adequate controls have not been implemented over the application change control process.

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

August 22, 2021

Matthew Antunez, Auditor-In-Charge
Information Systems Audits Group
U.S. Office of Personnel Management (OPM)
1900 E Street, NW
Room 6400
Washington, D.C. 20415-1100

Reference: OPM Draft IT Audit Report
Arkansas Blue Cross Blue Shield (ABCBS)
Audit Report Number 1A-10-44-21-017
Dated June 22, 2021

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

A. Security Management

Network Inventory Management

Recommendation 1

We recommend that ABCBS complete its project to ensure that a complete and accurate inventory is maintained for all IT assets.

Plan Response

ABCBS agrees with the recommendation and will have this implemented by June 30, 2022.

Segregation of Duty Risk Assessments

Recommendation 2

We recommend that ABCBS assess segregation of duty risks to the organization's application roles.

Plan Response

ABCBS agrees with the recommendation and will have this implemented by December 31, 2022.

Vendor Risk Assessments

Recommendation 3

We recommend that ABCBS perform risk assessments of its vendors prior to the establishment of a contract and routinely afterward in accordance with NIST and its own policy.

Plan Response

ABCBS agrees with the recommendation and will have this implemented by July 31, 2022.

B. Access Controls

No recommendation noted.

C. Network Security

Vulnerability Management

Recommendation 4

[redacted]

Plan Response

ABCBS agrees with the recommendation and has fully resolved and addressed all patches, vulnerabilities and security concerns noted by the OIG Audit Inquiry. ABCBS will provide the support evidence on the upcoming OPM Audit Resolution & Compliance update.

Firewall Ruleset Review

Recommendation 5

[redacted]

Plan Response

ABCBS agrees with the recommendation and will have this implemented by August 31, 2021.

D. Security Event Monitoring and Incident Response

No recommendation noted.

E. Configuration Management

Security Configuration Standards

Recommendation 6

[redacted]

Plan Response

ABCBS agrees with the recommendation and will have this implemented by July 31, 2022.

Security Configuration Auditing

Recommendation 7

[redacted]

Plan Response

ABCBS agrees with the recommendation and will have this implemented by July 31, 2022.

F. Contingency Planning

No recommendation noted.

G. Application Change Control

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]

Sincerely,

[redacted]
Managing Director, FEP Program Assurance

cc: Eric Keehan, OPM
[redacted]

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