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 and Blue Shield of Kansas

Report Number 2022-ISAG-0020

December 14, 2022

Executive Summary

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

Report No. 2022-ISAG-0020 **December 14, 2022**

Why Did We Conduct the Audit?

Blue Cross and Blue Shield of Kansas (BCBSKS) 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 BCBSKS's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by BCBSKS to process and store data related to medical encounters and insurance claims for FEHBP members as of May 2022**.**

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of BCBSKS's IT security controls determined that:

- BCBSKS has an adequate security management program in place.
- BCBSKS has adequate physical and logical access controls in place.
- BCBSKS has [redacted].
- BCBSKS's enterprise security event monitoring and incident response programs are adequate.
- BCBSKS needs to [redacted].
- BCBSKS needs to [redacted]
- BCBSKS has adequate controls over its contingency planning program.
- BCBSKS has adequate application change control policies and procedures.

Abbreviations

BCBSKS	**Blue Cross and Blue Shield of Kansas**
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 Blue Cross and Blue Shield of Kansas (BCBSKS), plan codes 10 and 11.

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 initial audit of the information technology (IT) general security and application controls at BCBSKS. All BCBSKS 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 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 BCBSKS'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 BCBSKS'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 BCBSKS'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 BCBSKS'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 BCBSKS to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Topeka, Kansas.

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 review, and remote testing of the general controls in place over BCBSKS's information systems. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at BCBSKS as of May 2022.

In conducting our audit, we relied to varying degrees on computer-generated data provided by BCBSKS. 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 judgmental, random selection, or statistical sampling methods as appropriate throughout the audit. Results of judgmentally or randomly 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 BCBSKS'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 BCBSKS's business structure and environment; and
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended.

Various laws, regulations, and industry standards were used as a guide to evaluate BCBSKS's control structure. These criteria included, but were not limited to, the following publications:

- GAO's FISCAM; and
- 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.

Compliance with Laws and Regulations

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

BCBSKS has implemented a series of formal policies and procedures that govern its security management program. BCBSKS has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. BCBSKS also has implemented security awareness and training policies and procedures.

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

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 BCBSKS's facilities and data centers. We also examined the logical access controls protecting sensitive data on BCBSKS's network environment and applications.

We observed the following controls in place:

- Routine access audits performed for secure areas;
- Multi-factor authentication for privileged and remote access; and
- Routine reviews of logical access to critical systems.

Nothing came to our attention to indicate that BCBSKS has not implemented adequate access controls.

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 BCBSKS'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 to secure connections to external networks;
- Technical controls to secure endpoints; and
- Documented policy to prevent non-company devices from connecting to the network.

However, we noted the following opportunities for improvement related to BCBSKS's network security controls.

1. Historical Vulnerability Scanning

Auditors requested historical vulnerability scans for a sample of BCBSKS servers. BCBSKS provided evidence that credentialed scans were performed [redacted]

BCBSKS could improve its vulnerability management process.

[redacted]

Recommendation 1:

We recommend that BCBSKS improve its [redacted]

BCBSKS's Response:

"BCBSKS has provided evidence that this recommendation has been implemented (Attachment 1)."

OIG Comments:

In response to the draft report, we received evidence that the vulnerability scanning tool is configured to perform credentials scans. However, during the audit, we observed that most of the servers were scanned with credentials except for the servers we identified.

Therefore, we feel that more appropriate evidence would be credentialed vulnerability scan results on the systems we identified during the audit.

As a part of the audit resolution process, please provide OPM's Healthcare and Insurance Office, Audit Resolution and Compliance group with evidence that BCBSKS has fully implemented this recommendation.

2. OIG Vulnerability Scanning

BCBSKS conducted credentialed vulnerability and configuration compliance scans on a sample of servers in BCBSKS's network environment on our behalf. We judgmentally selected a sample of [redacted]. 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]

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 2:

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

BCBSKS's Response:

"BCBSKS acknowledges this recommendation and will work with OPM Audit Compliance and Resolution to close it."

OIG Comments:

As a part of the audit resolution process, please provide OPM's Healthcare and Insurance Office, Audit Resolution and Compliance group with evidence that BCBSKS has fully implemented this recommendation. This statement also applies to the subsequent recommendation in this audit report that BCBSKS agrees to implement.

D. Security Event Monitoring and Incident Response

BCBSKS has an adequate event monitoring program.

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.

We observed the following controls in place:

- Security event monitoring throughout the network;
- A log analysis process; and
- A documented incident response program.

Nothing came to our attention to indicate that BCBSKS 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. BCBSKS employs a team of technical personnel who manage system software configuration for the organization. We evaluated BCBSKS's management of the configuration of its computer servers and databases.

We observed the following controls in place:

- A configuration management policy; and
- An established change management process.

However, we noted the following opportunity for improvement related to BCBSKS's configuration management process.

1. Configuration Management Procedures

BCBSKS has a documented configuration management policy and vulnerability scanning procedures. However, BCBSKS has not developed procedures for implementing security configuration settings, nor procedures for auditing the security configuration settings.

NIST SP 800-53, Revision 5, states that organizations should, "develop, document and disseminate ... procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls"

A lack of documented, approved procedures increases the likelihood that key elements in the creation process of future configuration baselines may be omitted and that configuration settings may not be properly audited.

Recommendation 3:

We recommend that BCBSKS create procedures documenting the process to create security configuration settings for each operating system in its environment.

BCBSKS's Response:

"BCBSKS acknowledges this recommendation and will work with OPM Audit Compliance and Resolution to close it."

Recommendation 4:

We recommend that BCBSKS create procedures documenting the process to audit and verify the security configuration settings for each operating system in its environment.

BCBSKS's Response:

"BCBSKS acknowledges this recommendation and will work with OPM Audit Compliance and Resolution to close it."

2. Security Configuration Settings

BCBSKS has documented security standards that provide a high-level guide or requirement for some configuration settings. [redacted]

BCBSKS does not have documented security configuration settings for all systems.

Security configuration settings are formally approved documents that list specific security settings for each operating system that an organization uses to configure its servers.

NIST SP 800-53, Revision 5, states that an organization should [redacted]

[redacted]

Recommendation 5:

We recommend that BCBSKS [redacted] deployed in its technical environment.

BCBSKS's Response:

"BCBSKS acknowledges this recommendation and will work with OPM Audit Compliance and Resolution to close it."

3. Security Configuration Auditing

As noted above, BCBSKS does [redacted]

NIST SP 800-53, Revision 5, states that an organization must [redacted]

Failure to perform [redacted]

Recommendation 6:

We recommend that BCBSKS implement a routine process [redacted]

BCBSKS's Response:

"BCBSKS acknowledges this recommendation and will work with OPM Audit Compliance and Resolution to close it."

F. Contingency Planning

BCBSKS has adequate controls over contingency planning.

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

We observed the following controls in place:

- Documented contingency plans;
- Adequate contingency plan testing and follow-up; and
- Data center emergency response procedures.

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

G. Application Change Control

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

BCBSKS 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 adequate application change review and approval process;
- Adequate segregation of duties to implement changes; and
- Specialized training for developers.

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

September 13, 2022

Julius Rios, 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
Blue Cross Blue Shield of Kansas (BCBSKS)
Audit Report Number 2022-ISAG-0020
(Dated July 29, 2022)

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

A. SECURITY MANAGEMENT

No recommendations noted.

B. ACCESS CONTROLS

No recommendation noted.

C. NETWORK SECURITY

Historical Vulnerability Scanning

Recommendation 1

We recommend that BCBSKS improve [redacted]

Plan Response

BCBSKS has provided evidence that this recommendation has been implemented (Attachment 1).

OIG Vulnerability Scanning

Recommendation 2

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

Plan Response

BCBSKS acknowledges this recommendation and will work with OPM Audit Compliance and Resolution to close it.

D. SECURITY EVENT MONITORING AND INCIDENT

No recommendation noted.

E. CONFIGURATION MANAGEMENT

Recommendation 3

We recommend that BCBSKS create procedures documenting the process to create security configuration settings for each operating system in its environment.

Plan Response

BCBSKS acknowledges this recommendation and will work with OPM Audit Compliance and Resolution to close it.

Recommendation 4

We recommend that BCBSKS create procedures documenting the process to audit and verify the security configuration settings for each operating system in its environment.

Plan Response

BCBSKS acknowledges this recommendation and will work with OPM Audit Compliance and Resolution to close it.

Security Configuration Settings

Recommendation 5

We recommend that BCBSKS [redacted]

Plan Response

BCBSKS acknowledges this recommendation and will work with OPM Audit Compliance and Resolution to close it.

Security Configuration Auditing

Recommendation 6

We recommend that BCBSKS implement a routine process [redacted]

Plan Response

BCBSKS acknowledges this recommendation and will work with OPM Audit Compliance and Resolution to close it.

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 (202) 942-1285 or Hoan Mai at (202) 942-1282.

Sincerely,

Kim King
Managing Director, FEP Program Assurance

cc: Eric Keehan, OPM
Hoan Mai, FEP
Amanda Tucker, 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: https://oig.opm.gov

By Phone: Toll Free Number: (877) 499-7295

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