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 Kansas City

Report Number 1A-10-42-21-011
November 15, 2021

Executive Summary

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

Report No. 1A-10-42-21-011 **November 15, 2021**

Why Did We Conduct the Audit?

Blue Cross Blue Shield of Kansas City BCBSKC) 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 BCBSKC's information technology (IT) environment.

What Did We Audit?

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

- BCBSKC has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified during risk assessments. BCBSKC also performs risk assessments of its third-party vendors.
- BCBSKC has adequate physical and logical access controls in place to grant, adjust, and remove access to facilities and information systems.
- BCBSKC has perimeter controls in place to protect from external threats. However, [redacted]
- BCBSKC has an established incident response program.
- BCBSKC [redacted]
- [redacted]
- BCBSKC has contingency plans in place for claims-related operations.
- BCBSKC has documented and implemented an application change control process.

Abbreviations

BCBSKC	**Blue Cross Blue Shield of Kansas City**
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 Blue Shield of Kansas City (BCBSKC).

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 BCBSKC. All BCBSKC 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 BCBSKC'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 BCBSKC'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 BCBSKC'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 BCBSKC'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 BCBSKC to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Kansas City, Missouri.

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 BCBSKC'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 BCBSKC as of April 2021.

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

To conduct our vulnerability and compliance scan exercise, we chose a sample of 150 servers from a universe of approximately 1,600. The sample selection included a variety of system functionality and operating systems across production, test, development, and disaster recovery environments. The judgmental sample was drawn from systems that store, process, or forward 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.

In conducting this audit, we:

- Performed a risk assessment of BCBSKC'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 BCBSKC'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 in evaluating BCBSKC's control structure. These criteria included, but were not limited to, the following publications:

- GAO's FISCAM, and

- National Institute of Standards and Technology 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 BCBSKC's practices were consistent with applicable standards. While generally compliant with respect to the items tested, BCBSKC 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 BCBSKC's overall IT security program. We evaluated BCBSKC's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

BCBSKC creates remediation plans to address weaknesses identified in risk assessments.

BCBSKC has developed adequate IT security policies and procedures. BCBSKC has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. BCBSKC has also implemented an adequate vendor management program to assess and monitor risks associated with third-party activities.

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

B. Access Controls

1. Logical Access

Logical access controls are policies, procedures, and techniques used to inhibit or identify unauthorized access to an organization's system, applications, processes, and information.

We examined logical access controls protecting BCBSKC's network environment andclaims processing applications during this audit.

We observed the following controls in place:

- Identification and authentication policies and procedures to gain access to BCBSKC's systems;
- Procedures and policies for granting, removing, and adjusting system and application access; and
- Procedures and policies for the review and audit of user accounts.

Nothing came to our attention to indicate that BCBSKC has not implemented adequate controls over their access control process.

2. Physical Access

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

We examined the physical access controls at BCBSKC's facilities and data centers and observed the following controls in place:

- Identification and authentication policies and procedures to gain access to BCBSKC's facilities;
- Procedures and policies for granting, removing, and adjusting facility and data center access; and
- Procedures and policies for the review and audit of physical access permissions.

Nothing came to our attention to indicate that BCBSKC has not implemented adequate prevention and detection controls related to physical access.

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 BCBSKC'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:

- Preventive controls at the network perimeter;
- Adequate remote access controls; and
- Internal controls to filter web content.

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

1. Credentialed Vulnerability Scanning

BCBSKC conducts routine vulnerability scans on its systems. Most systems in the environment have an agent installed to authenticate the vulnerability scanning tool.

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation 1

We recommend that BCBSKC improve the current vulnerability scanning process to [redacted]

BCBSKC's Response:

BCBSKC agrees with the recommendation and plans to complete implementation ofthis by December 31, 2021.

OIG Comments:

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

2. Vulnerabilities Identified from OIG Scans

BCBSKC conducted [redacted] scans on a sample of servers and workstations in its network environment on our behalf. The specific vulnerabilities that we identified were provided to BCBSKC in the form of an audit inquiry, but will not be detailed in this report. [redacted] Documented risk exceptions are used in accordance with BCBSKC policies for any patches that cannot be applied within the required timeframe.

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

[redacted]

[redacted]

Recommendation 2

We recommend that BCBSKC remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry.

BCBSKC's Response:

"BCBSKC agrees with the recommendation and has a project initiated to integrate its vaulting and vulnerability scan tools to automate the authentication process. The project is targeted for completion by December 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 BCBSKC's security event monitoring and incident response programs identified the following controls in place:

- Controls to monitor security events throughout the network;
- Policies and procedures for analyzing security events; and
- A documented incident response program.

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

We observed the following controls in place:

- Documented policies and procedures;
- A documented system change control process; and
- An established patch management process.

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

1. Security Configuration Standards

Security configuration standards are formally approved documents that list specific security settings. [redacted]

NIST SP 800-53, Revision 5, states that an organization should establish and document "configuration settings for information technology products and platforms . to meet with operational requirements."

In addition, NIST SP 800-53, Revision 5, states that an organization should develop, document, and maintain a current baseline configuration of the information system.

[redacted]

Recommendation 3

We recommend that [redacted]

BCBSKC's Response:

"BCBSKC agrees with the recommendation and has a project initiated to develop tailored security standards for each operating system in its environment. The project is targeted for completion by December 31, 2021."

2. Security Configuration Auditing

[redacted]

[redacted]

[redacted]

NIST SP 800-53, Revision 5, states that an 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."

[redacted]

Recommendation 4

[redacted]

BCBSKC's Response:

"BCBSKC agrees with the recommendation and has a project initiated to develop and implement configuration setting compliance monitoring processes. The project is targeted for completion by December 31, 2021."

3. System Lifecycle Management

[redacted]

NIST SP 800-53, Revision 5, 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 5, also states that "unsupported components . can result in an opportunity for adversaries to exploit weaknesses in the installed components."

[redacted]

Recommendation 5

[redacted]

BCBSKC's Response:

"BCBSKC agrees with the recommendation and is working with their vendors and business partners to remove or upgrade any unsupported operating systems. The project is targeted for completion by December 31, 2021."

F. Contingency Planning

Contingency planning includes the policies and procedures that ensure adequate availability of information systems, data, and business processes. We reviewed BCBSKC's contingency planning documentation and processes to prevent or minimize interruptions to business operations if disruptive events were to occur. We identified the following controls in BCBSKC's contingency planning process:

BCBSKC has implemented plans to minimize business disruptions from adverse events.

- Contingency plans including disaster recovery and business continuity plans;
- Contingency plan testing and follow-up; and
- A documented data backup process.

Nothing came to our attention to indicate that BCBSKC has not implemented adequate controls over the contingency planning process.

G. Application Change Control

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

BCBSKC has implemented policies and procedures related to application configuration management, and also has 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:

- A documented application change control process;
- Unit, integration, and user acceptance testing are conducted in accordance with industry standards; and
- A group independent from the software developers moves code between development and production environments to ensure separation of duties.

Nothing came to our attention to indicate that BCBSKC has not implemented adequate controls over the application configuration management 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

June 28, 2021

Martin Wiley, 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 Kansas City (BCBSKC)
Audit Report Number 1A-10-42-21-011
Dated May 3, 2021

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

No recommendation noted.

C. Network Security

Credential Vulnerability Scanning

Recommendation 1

We recommend that BCBSKC improve the current vulnerability scanning process to [redacted]

Plan Response

BCBSKC agrees with the recommendation and has a project initiated to integrate its vaulting and vulnerability scan tools to automate the authentication process. The project is targeted for completion by December 31, 2021.

Vulnerabilities Identified by OIG Scans

Recommendation 2

We recommend that BCBSKC remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry.

Plan Response

BCBSKC agrees with the recommendation and has a project initiated to integrate its vaulting and vulnerability scan tools to automate the authentication process. The project is targeted for completion by December31, 2021.

D. Security Event Monitoring and Incident Response

No recommendation noted.

E. Configuration Management

Security Configuration Standards

Recommendation 3

We recommend that [redacted]

Plan Response

BCBSKC agrees with the recommendation and has a project initiated to develop tailored security standards for each operating system in its environment. The project is targeted for completion by December 31, 2021.

Security Configuration Auditing

Recommendation 4

We recommend that [redacted]

Plan Response

BCBSKC agrees with the recommendation and has a project initiated to develop and implement configuration setting compliance monitoring processes. The project is targeted for completion by December 31, 2021.

System Lifecycle Management

Recommendation 5

We recommend that [redacted]

Plan Response

BCBSKC agrees with the recommendation and is working with their vendors and business partners to remove or upgrade any unsupported operating systems. The project is targeted for completion by December 31, 2021.

F. Contingency Planning

No recommendation noted.

G. Applications 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] 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