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 of Idaho

Report Number 2023-ISAG-003

August 10, 2023

Executive Summary

Audit of the Information Systems General and Application Controls at Blue Cross of Idaho.

Report No. 2023-ISAG-003 **August 10, 2023**

Why Did We Conduct the Audit?

Blue Cross of Idaho (BCI) is contracted by the U.S. Office of Personnel Management to provide health insurance benefits for Federal employees, annuitants, and their dependents as part of the Federal Employees Health Benefits Program (FEHBP).

The objective of this audit was to determine if BCI has implemented adequate general and application controls to protect the confidentiality, integrity, and availability of FEHBP data processed and stored by its information systems.

What Did We Audit?

The scope of this audit included all BCI information systems operating in the general control environment where FEHBP data is processed and stored as of May 2023.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

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

- BCI could [redacted]
- BCI has implemented adequate logical access controls.
- BCI has implemented adequate physical access controls.
- BCI has implemented adequate data center controls.
- BCI could [redacted]
- BCI has some [redacted]
- BCI has implemented adequate security event monitoring and incident response controls.
- BCI has [redacted]
- BCI has [redacted]
- BCI has implemented adequate contingency planning controls.
- BCI has implemented adequate system development lifecycle controls.

Abbreviations

BCI	**Blue Cross of Idaho**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information System Controls Audit Manual**
GAGAS	**Generally Accepted Government Auditing Standards**
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**
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 Blue Cross of Idaho's (BCI) general and application controls over its information systems operating in the general information technology (IT) control environment where Federal Employees Health Benefits Program (FEHBP) data is processed and stored as of May 2023.

The FEHBP was established by the Federal Employees Health Benefits Act (Public Law 86-382), enacted on September 28, 1959. The FEHBP was created to provide health insurance benefits for Federal employees, annuitants, and their dependents. Health insurance coverage is made available through contracts with various health insurance carriers that provide service benefits, indemnity benefits, or comprehensive medical services.

The provisions of the Federal Employees Health Benefits Act are implemented by the U.S. Office of Personnel Management (OPM) through regulations that are codified in Title 5, Chapter 1, Part 890 of the Code of Federal Regulations (CFR).

FEHBP contracts include provisions stating that an authorized representative of the Contracting Office may use National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (or its current equivalent) requirements as a benchmark for conducting audits of a health insurance carrier's information systems and may recommend that the carrier adopt a best practice drawn from NIST SP 800-53 (or its current equivalent) to information systems that directly process FEHBP data and all other information systems in the same general IT environment.

The audit was conducted pursuant to BCI's FEHBP contract CS 1039; 5 U.S.C. Chapter 89; and 5 CFR Chapter 1, Part 890. The audit was performed by OPM's Office of the Inspector General (OIG), as established and authorized by the Inspector General Act of 1978, as amended (5 U.S.C. §§ 401-424).

This was our initial audit of the information systems general and application controls at BCI. All BCI 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. Objective, Scope, and Methodology

Objective

The objective of this audit was to determine if BCI has implemented adequate general and application controls over its information systems to protect the confidentiality, integrity, and availability of FEHBP data.

Scope and Methodology

This performance audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States. GAGAS requires that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

The scope of this audit included all BCI information systems operating in the general IT control environment where FEHBP data is processed and stored as of May 2023.

Due to resource limitations, we were not able to assess the entire BCI information systems control environment. Therefore, the scope of our work was limited to high-risk areas identified during the planning phase of our audit. Accordingly, we performed a risk assessment of BCI's information systems environment and applications during the planning phase of the audit to develop an understanding of BCI's internal controls. Using this risk assessment, additional audit steps were developed, as appropriate, to verify that the internal controls were properly designed, placed in operation, and effective.

Our audit program was based on procedures contained in the U.S. Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual* (FISCAM) and NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations.*

NIST SP 800-53 controls were selected for testing based on risk, applicability, and overall impact to the organization's IT security posture. These controls have been organized into the following audit sections:

- Enterprise Security;
- Logical Access;
- Physical Access;
- Data Center;
- Network Security;
- Security Event Monitoring and Incident Response;

- Configuration Management;
- Contingency Planning; and
- System Development Lifecycle.

For each of our audit sections, FISCAM identifies critical elements that represent tasks essential for establishing adequate controls. For each critical element, there is a discussion of the associated objectives, risks, and critical activities, as well as related control techniques and audit concerns.

NIST SP 800-53A, Revision 5 *Assessing Security and Privacy Controls in Information Systems and Organizations* includes a comprehensive set of procedures for assessing the effectiveness of security and privacy controls defined in NIST SP 800-53. We used these potential assessment methods and artifacts, where appropriate, to evaluate BCI's internal controls. This includes interviews, observations, control tests, and inspection of computer-generated data and various documents, including IT and other related organizational policies and procedures.

When our objective involved the assessment of computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable. However, due to time constraints, we did not verify the reliability of data used to complete some of our audit steps when we determined that the evidence was adequate to achieve our audit objectives.

Control tests were performed to determine the extent to which established controls and procedures are functioning as intended. Where appropriate, control tests utilized judgmental sampling methods. 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.

All audit work was completed remotely. The remote work performed included interviews of staff, documentation reviews, and testing of the general and application controls in place over BCI's information systems. The business processes reviewed are primarily located in Meridian, Idaho.

The findings, recommendations, and conclusions outlined in this report are based on the status of information systems general and application controls in place at BCI as of May 4, 2023.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether BCI's information system general and application controls were consistent with applicable standards. Various laws, regulations, and industry standards were used as a guide to evaluate BCI's control structure. These criteria included, but were not limited to, the following publications:

- GAO’s FISCAM;
- NIST SP 800-53, Revision 5; and
- BCI’s policies and procedures.

While generally compliant with respect to the items tested, BCI was not in compliance with all standards, as described in section III of this report.

III. Audit Findings and Recommendations

A. Enterprise Security

Enterprise security controls include the policies, procedures, and techniques that serve as the foundation of BCI's overall IT security program. We evaluated BCI's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

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

- Formally documented risk assessment policies;
- Routine information security risk assessments; and
- Routine security awareness training is administered.

However, we identified the following opportunity for improvement related to BCI's enterprise security controls.

1. Risk Assessment

BCI conducts enterprise-wide and vendor risk assessments. Further, BCI conducts penetration tests and routine vulnerability scanning. . BCI's *Risk Management* policy states that the Cybersecurity Risk Management department conducts risk assessments of potential threats and vulnerabilities to the confidentiality, integrity, and availability of sensitive information.

NIST SP 800-53, Revision 5, control RA-3 states that the organization should conduct a risk assessment to determine the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits and determine the likelihood and impact of adverse effects.

Recommendation 1:

We recommend that BCI

BCI's Response:

"BCID acknowledges the recommendation and is in the process of remediating it."

OIG Comments:

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

B. Logical Access

BCI provisions logical access based on valid authorizations.

Logical access controls include the policies, procedures, and techniques used to detect and prevent unauthorized logical access to information systems or modification, loss, and disclosure of sensitive data. We evaluated the logical access controls protecting sensitive data on BCI's network environment and applications supporting the FEHBP claims processing business function.

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

- System access is authorized based on valid access authorizations;
- System accounts are monitored; and
- Acceptable use is adequately documented.

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

C. Physical Access

BCI has implemented adequate physical access controls.

Physical access controls include the policies, procedures, and techniques used to prevent or detect unauthorized physical access to facilities which contain information systems and sensitive data. We evaluated the controls protecting physical access to BCI's facilities and data centers.

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

- Physical access to the headquarters facility is controlled using a badge access system;

- Policies and procedures for granting, removing, and adjusting physical access; and
- Routine audits and reviews to ensure employee access is appropriate.

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

D. Data Center

Data center controls include the policies, procedures, and techniques used to protect information systems from environmental damage and provide network resiliency. We evaluated the data center controls at BCI's primary and back-up data centers.

BCI has implemented adequate data center controls.

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

- Data center physical access is monitored;
- Environmental controls maintain temperature and humidity; and
- Alternate telecommunication services provide network redundancy.

Nothing came to our attention to indicate that BCI has not implemented adequate data center controls.

E. Network Security

Network security controls include the policies, procedures, and techniques used to prevent or monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. We evaluated BCI's controls related to network design, data protection, and systems monitoring.

BCI has [redacted]

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

- Perimeter controls secure connections to external networks;
- Split tunneling is prevented; and
- Adequate firewall change management procedures are in place.

1. Network Access Controls

BCI

However, BCI

NIST SP 800-53, Revision 5, control IA-3 states that an information system uniquely identifies and authenticates devices before establishing a network connection.

Recommendation 2:

We recommend that BCI

BCI's Response:

"BCID acknowledges the recommendation and is in the process of remediating it."

2. Missing Security Patches

BCI performed credentialed vulnerability scans on a sample of servers and workstations in its network environment on our behalf. We chose a sample of servers from a universe of approximately servers. The sample selection included a variety of system functionality and operating systems across production, test, and development environments. 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.

NIST SP 800-53, Revision 5, control SI-2, states that the organization "install security-relevant software and firmware updates within [an organization-defined time period] of the release of the updates … ."

[redacted]

Recommendation 3:

We recommend that BCI [redacted]

BCI's Response:

"BCID acknowledges the recommendation and is in the process of remediating it."

F. Security Event Monitoring and Incident Response

BCI has implemented adequate controls related to security event monitoring and incident response.

Security event monitoring controls include the policies, procedures, and techniques used for 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 controls include the policies, procedures, and techniques used to establish and implement an incident response plan which defines roles and responsibilities, response procedures, training, and reporting. We evaluated BCI's controls related to event log collection and security incident detection, response, and reporting.

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

- Controls to monitor security events throughout the network;
- Documented incident response plans and playbooks; and
- A documented incident response plan test.

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

G. Configuration Management

BCI has [redacted]

Configuration management controls include the policies, procedures, and techniques used to develop, implement, and maintain secure, risk-based system configurations and ensure that systems are configured according to these standards. We

evaluated BCI's configuration management of its end-user devices, servers, databases.

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

- Established configuration management policy;
- Documented system configuration change decisions; and
- An adequate patch management policy.

However, [redacted]

1. Configuration Setting Management

We were told that BCI configures its systems with the Center for Internet Security benchmarks. [redacted]

NIST SP 800-53, Revision 5, control CM-6 states that the organization should "Identify, document, and approve any deviations from established configuration settings for [organization-defined system components] based on [organization-defined operational requirements] … ." NIST further states that changes to configuration settings should be monitored and controlled.

[redacted]

Recommendation 4:

We recommend that BCI [redacted]

BCI's Response:

"BCID acknowledges the recommendation and is in the process of remediating it."

Recommendation 5:

We recommend that BCI develop and implement procedures to perform compliance scanning and remediate settings that are not in compliance with organizational standards.

BCI's Response:

"BCID acknowledges the recommendation and is in the process of remediating it."

2. Unsupported Software

[redacted]

NIST SP 800-53, Revision 5, control SA-22, states that the organization should "Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or" acquire an alternative source for continued support.

[redacted]

Recommendation 6:

We recommend that BCI [redacted]

BCI's Response:

"BCID acknowledges the recommendation and is in the process of remediating it."

Recommendation 7:

We recommend that [redacted].

Note – this recommendation cannot be implemented until the controls from Recommendation 6 are in place.

BCI's Response:

"BCID acknowledges the recommendation and is in the process of remediating it."

H. Contingency Planning

BCI has implemented adequate contingency planning controls.

Contingency planning controls include the policies, procedures, and techniques that ensure continuity and recovery of critical business operations and the protection of data in the event of a service impacting incident. We evaluated BCI's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when service impacting events occur.

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

- Plans for the continuance of critical business functions in the event of a disruption;
- Routine user-level and system-level data backups; and
- Backup data reliability and integrity testing.

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

I. System Development Lifecycle

BCI has implemented adequate system development lifecycle controls.

System development lifecycle controls include the policies, procedures, and techniques related to the secure and controlled internal development of software supporting claims adjudication and sensitive web applications. We evaluated BCI's software development and change control policies and procedures and controls related to secure software development.

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

- Documented software change management policies;
- Documented software development procedures; and
- Source code security and quality analyses for internally developed software.

Nothing came to our attention to indicate that BCI has not implemented adequate system development lifecycle controls.

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

July 14, 2023

Matthew Antunez, 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 of Idaho (BCID)
Audit Report Number 2023-ISAG-0030
(Dated May 15, 2023)

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

A. ENTERPRISE SECURITY

Risk Assessment

Recommendation 1

We recommend that BCI [redacted].

Plan Response
BCID acknowledges the recommendation and is in the process of remediating it.

B. LOGICAL ACCESS

No recommendations noted.

C. PHSYICAL ACCESS

No recommendations noted.

D. DATA CENTER

No recommendations noted.

E. NETWORK SECURITY

Network Access Control

Recommendation 2

We recommend that BCI [redacted]

Plan Response

BCID acknowledges the recommendation and is in the process of remediating it.

Missing Security Patches

Recommendation 3

We recommend that BCI [redacted]

Plan Response

BCID acknowledges the recommendation and is in the process of remediating it.

F. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

No recommendation noted.

G. CONFIGURATION MANAGEMENT

Configuration Setting Management

Recommendation 4

We recommend that BCI [redacted]

Plan Response

BCID acknowledges the recommendation and is in the process of remediating it.

Recommendation 5

We recommend that BCI [redacted]

Plan Response

BCID acknowledges the recommendation and is in the process of remediating it.

Unsupported Software

Recommendation 6

We recommend that BCI [redacted]

Plan Response

BCID acknowledges the recommendation and is in the process of remediating it.

Recommendation 7

We recommend that BCI [redacted]. Note – this recommendation cannot be implemented until the controls from Recommendation 6 are in place.

Plan Response

BCID acknowledges the recommendation and is in the process of remediating it.

H. CONTINGENCY PLANNING

No recommendations noted.

I. SYSTEM DEVELOPMENT LIFECYCLE (SDLC)

No recommendation noted.

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

Sincerely,

[redacted]
Managing Director, FEP Program Assurance

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/contact/hotline

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