U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT BLUE CROSS BLUE SHIELD OF MICHIGAN

Report Number 1A-10-32-18-046
May 16, 2019

EXECUTIVE SUMMARY

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

Report No. 1A-10-32-18-046 **May 16, 2019**

Why Did We Conduct The Audit?

Blue Cross Blue Shield of Michigan (BCBSM) 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 BCBSM's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by BCBSM 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 the IT security controls of BCBSM determined:

- BCBSM has an adequate security management program.
- [redacted] using a [redacted]. However, controls should be in place to require [redacted]
- [redacted] are not routinely audited.
- BCBSM should [redacted] from user controlled systems.
- Technical controls to [redacted] are not uniformly in place.
- Our vulnerability scans indicated the presence of vulnerabilities [redacted]
- BCBSM does not have documented and approved [redacted] for its operating systems.
- BCBSM is unable to routinely audit [redacted] have not been documented or approved.
- BCBSM has [redacted] in its environment.
- BCBSM has an adequate contingency planning process.
- Nothing came to our attention to indicate BCBSM has not implemented adequate controls related to claims adjudication.

ABBREVIATIONS

BCBSM	**Blue Cross Blue Shield of Michigan**
CFR	**Code of Federal Regulations**
COBIT	**Control Objectives for Information and Related Technologies**
FEHBP	**Federal Employees Health Benefits Program**
FEP	**Federal Employee 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's Special Publication**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY i

ABBREVIATIONS ii

I. **BACKGROUND** 1

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

III. **AUDIT FINDINGS AND RECOMMENDATIONS** 5

A. SECURITY MANAGEMENT 5

B. ACCESS CONTROLS 5

1. [redacted] 6

C. NETWORK SECURITY 7

1. [redacted] 7
2. [redacted] 8
3. [redacted] 9
4. Vulnerability Scanning 10

D. CONFIGURATION MANAGEMENT 11

1. [redacted] Standards 11
2. [redacted] Auditing 12
3. [redacted] Management 13

E. CONTINGENCY PLANNING 14

F. CLAIMS ADJUDICATION 14

1. Application Configuration Management 14
2. Claims Processing System 15
3. Debarment 15

APPENDIX: Blue Cross Blue Shield of Michigan's April 4, 2019, response to the draft audit report, issued February 6, 2019.

REPORT FRAUD, WASTE, AND MISMANAGEMENT

I. BACKGROUND

This final report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) data by Blue Cross Blue Shield of Michigan (BCBSM).

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 first audit of BCBSM's information technology (IT) general and application controls.

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 BCBSM's IT environments. We accomplished these objectives by reviewing the following areas:

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

The onsite portion of this audit was performed in August and September of 2018. We completed additional audit work before and after the on-site visit at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at BCBSM as of [redacted] 2018. In conducting our audit, we relied to varying degrees on computer-generated data provided by BCBSM. Due to time constraints, we did not verify the reliability of the data used to complete some of our audit steps, but we determined that it was adequate to achieve our audit objectives.

However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable.

In conducting this audit we:

- Gathered documentation and conducted interviews;
- Reviewed BCBSM's business structure and environment;
- Performed a risk assessment of BCBSM's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM); and
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, we used judgmental sampling in completing our compliance testing.

Various laws, regulations, and industry standards were used as a guide to evaluating BCBSM's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;
- U.S. Office of Management and Budget (OMB) Circular A-130, Appendix III;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- Control Objectives for Information and Related Technologies (COBIT) 5: A Business Framework for the Governance and Management of Enterprise IT;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Revision 1, An Introduction to Information Security;
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;

- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-44, Version 2, Guidelines on Securing Public Web Servers;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and
- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide.

COMPLIANCE WITH LAWS AND REGULATIONS

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

BCBSM has implemented a series of formal policies and procedures that govern its security management program. BCBSM has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. BCBSM has also implemented human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that BCBSM 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 BCBSM's facilities and data center. We also examined the logical access controls protecting data in BCBSM's network environment and applications.

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

- Procedures for appropriately granting and removing physical access to facilities and the datacenter, and

- Procedures for appropriately granting and adjusting logical access to applications and software resources.

The following section documents an opportunity for improvement related to BCBSM's logical access controls.

1. [redacted]

BCBSM issues a [redacted] that require access to sensitive systems. BCBSM information systems require [redacted] for access [redacted] however, all [redacted] and regular users are able to access systems on the local network via [redacted]. Although this control adds security value, we expect all FEHBP contractors to require [redacted] to information systems. The federal government requires [redacted] for all information system users. Although BCBSM is not a government entity, it does process [redacted] of [redacted] Therefore, we recommend that BCBSM implement this control for [redacted]

BCBSM does [redacted] for local access

[redacted] states that information systems should implement [redacted]

Failure to [redacted] the risk [redacted] could be compromised and that unauthorized users could access sensitive and proprietary data.

Recommendation 1

We recommend that BCBSM [redacted] all information systems.

BCBSM's Response:

"BCBSM acknowledges this recommendation. BCBSM's [redacted] plan includes activities to further implement [redacted]

[redacted]

OIG Comments:

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

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 the BCBSM network security program and reviewed the results of several automated vulnerability scans performed during this audit.

We observed the following controls in place:

- Perimeter controls protecting public and partner network connections;
- Security event monitoring throughout the network; and
- A documented incident response program.

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

1. [redacted]

BCBSM has various information security policies that provide guidance on [redacted] The Plan also maintains a documented change control process to formally request and approve changes to [redacted] BCBSM uses the change control process to document [redacted] We were told that BCBSM intends to [redacted]

[redacted] states that [redacted] should be reviewed or tested periodically to make sure that the [redacted] are in compliance with the organization's policies.

[redacted], also states that "Each review should include a detailed examination of [redacted], particularly who [redacted]

Failure to audit [redacted] against a [redacted] increases the risk [redacted] to the [redacted] remain that undetected.

Recommendation 2

We recommend that BCBSM [redacted] its current [redacted] against the approved [redacted]

BCBSM's Response:

"BCBSM acknowledges this recommendation. [redacted]

BCBSM has [redacted] ***controls in place, for its*** [redacted] ***. On a continuous basis, using sophisticated toolsets,*** [redacted] ***analyzes*** [redacted] ***and recommends enhancements to*** [redacted] ***Updates are promptly implemented.*** [redacted] ***are made in accordance with BCBSM's*** [redacted] ***process and all*** [redacted] ***are*** [redacted] ***are recurrently reviewed*** [redacted]

2. [redacted]

BCBSM uses firewalls to control connections with systems outside of its network. [redacted] However, we were told that there is [redacted] We were also told the Plan is aware [redacted] In addition to [redacted] The Plan noted that [redacted]

BCBSM does not [redacted]

[redacted] advises that, "Focusing attention [redacted] on [redacted] may not come directly [redacted] Important [redacted] should be [redacted]

Failure to [redacted] increases the risk that a system could be compromised and allow access to sensitive servers and data.

Recommendation 3

We recommend that BCBSM [redacted] in order to [redacted]

BCBSM's Response:

"BCBSM acknowledges this recommendation. Under BCBSM's [redacted] plan, and as aligned with the [redacted], BCBSM plans to issue revised [redacted] BCBSM's [redacted] will [redacted] the [redacted] as appropriate and as aligned with the [redacted] BCBSM will act to further [redacted]

BCBSM will provide pertinent revised [redacted]

3. [redacted]

BCBSM does not have technical controls uniformly in place to [redacted] This issue is compounded by [redacted] discussed above. However, BCBSM has previously identified this weakness and management is evaluating options.

[redacted] states that an information system should [redacted]

[redacted]

Recommendation 4

We recommend that BCBSM implement [redacted]

BCBSM's Response:

"BCBSM acknowledges this recommendation. BCBSM has [redacted] currently in place, to mitigate the risks associated with [redacted] However, BCBSM will develop and propose a plan [redacted]

4. Vulnerability Scanning

We conducted credentialed vulnerability and configuration compliance scans on a sample of servers in BCBSM's network environment. [redacted]

Recommendation 5

We recommend that BCBSM [redacted]

BCBSM's Response:

"BCBSM acknowledges this recommendation. Under BCBSM's [redacted] plan, and as aligned with [redacted] BCBSM plans to issue revised [redacted]

[redacted] ***BCBSM will maintain compliance with the*** [redacted] ***for*** [redacted]

[redacted]

D. CONFIGURATION MANAGEMENT

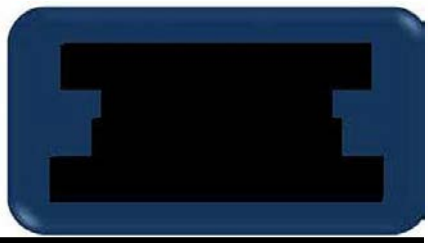
Configuration management involves the policies and procedures used to ensure that systems are configured according to a consistent and approved risk based standard. BCBSM employs a team of technical personnel who manage system software configuration for the organizations. We evaluated BCBSM's management of the configuration of its computer servers and databases. Our review found the following controls in place:

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

The sections below document areas for improvement related to BCBSM's configuration management controls.

1. [redacted] Standards

BCBSM has a documented policy that requires security requirements and controls to be defined for new and existing systems. BCBSM follows a standard process to install and setup new servers. [redacted]



[redacted] states that an organization should [redacted]

In addition, [redacted] states that an organization must [redacted]

Failure to establish approved [redacted] increases the risk that the system may not be configured in a secure manner.

Recommendation 6

We recommend that BCBSM [redacted]

BCBSM's Response:

"BCBSM acknowledges this recommendation. Under BCBSM's [redacted], activities are identified and in progress [redacted] BCBSM will [redacted]

2. [redacted] Auditing

As noted above, BCBSM does not maintain [redacted] for its [redacted], and therefore it [redacted]

[redacted] states that an organization must monitor and control changes to the [redacted] in accordance with organizational policies and procedures.

[redacted]

Failure to implement a [redacted]

Recommendation 7

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

BCBSM's Response:

"BCBSM acknowledges this recommendation. BCBSM will formalize its current [redacted] program [redacted] such that BCBSM's [redacted]

3. [redacted] Management

[redacted]

[redacted]

Failure [redacted] leaves information systems open to known vulnerabilities without any remediation available.

Recommendation 8

We recommend that BCBSM update its [redacted]

BCBSM's Response:

"BCBSM acknowledges this recommendation. Under BCBSM's [redacted] plan, and as aligned with [redacted] BCBSM plans to [redacted]

BCBSM will provide pertinent [redacted] BCBSM will also [redacted] The plan will [redacted]

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

- Disaster recovery plan (e.g., recovery of hardware and software infrastructure);
- Business continuity plan (e.g., people and business processes);
- Disaster recovery plan tests; and
- Emergency response procedures.

We determined that the contingency planning documentation contained the critical elements suggested by NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems." BCBSM has identified and prioritized the systems and resources that are critical to business operations, and has developed detailed procedures to recover those systems and resources.

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

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting BCBSM's claims adjudication process. BCBSM prices and adjudicates claims using [redacted] We reviewed the following processes related to claims adjudication: application configuration management, claims processing, and provider debarment.

1. Application Configuration Management

We evaluated the policies and procedures governing application development and change control over BCBSM's claims processing systems.
BCBSM has implemented policies and procedures related to application configuration management, and 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 approval of software modifications:

- Policies and procedures that allow modifications to be tracked throughout the change process;

- Unit, integration, and user acceptance testing are conducted in accordance with industry standards; and

- A group independent from the [redacted] to ensure separation of duties.

Nothing came to our attention to indicate that BCBSM has not implemented adequate controls related to the application configuration management process.

2. Claims Processing System

We evaluated the business process controls associated with BCBSM's claims processing system to ensure the completeness, accuracy, and confidentiality of transactions and data.

We determined that BCBSM has implemented policies and procedures to help ensure that:

- Claims are properly input and tracked to ensure timely processing;

- Claims are monitored as they are processed through the system with real time tracking of the system's performance; and

- Claims scheduled for payment are actually paid.

Nothing came to our attention to indicate that BCBSM has not implemented adequate controls over its claims processing systems.

3. Debarment

BCBSM has documented procedures for reviewing provider files for debarments and suspensions. [redacted] When the debarment list is updated, BCBSM sends notification to any member who has seen this provider within the previous year. The member is then given 90 days to find a new provider before claims are rejected. If a debarred provider submits a claim, this claim will hit an edit, to be reviewed by a claims processor. The processing guides used by BCBSM include guidance on the 15-day OIG mandated grace period.

Nothing came to our attention to indicate that BCBSM has not implemented adequate controls over the debarment 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

April 4, 2019

[redacted], 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 Michigan (BCBSM or the "Plan")
Audit Report Number 1A-10-32-18-046
(Dated February 6, 2019)

The following sets forth BCBSM's response as it relates to OPM's recommendations included in the draft audit report referenced above.

A. SECURITY MANAGEMENT

No recommendation noted.

B. ACCESS CONTROLS

1. [redacted]

Recommendation 1

We recommend that BCBSM require [redacted] information systems.

Plan Response

BCBSM acknowledges this recommendation. BCBSM's [redacted] plan includes activities to further implement [redacted]

[redacted]

C. NETWORK SECURITY

1. [redacted]

Recommendation 2

We recommend that BCBSM [redacted] its current [redacted] against the approved [redacted]

Plan Response

BCBSM acknowledges this recommendation. On [redacted], BCBSM increased [redacted]

BCBSM has [redacted] controls in place, for its [redacted] On a continuous basis, using sophisticated toolsets, [redacted] analyzes [redacted] and reco [redacted] Updates are promptly implemented. [redacted] are made in accordance with BCBSM's [redacted] process and all [redacted] are [redacted] are recurrently reviewed [redacted]

2. [redacted]

Recommendation 3

We recommend that BCBSM [redacted] in order to [redacted]

Plan Response

BCBSM acknowledges this recommendation. Under BCBSM's [redacted] plan, and as aligned with the [redacted] BCBSM plans to issue revised [redacted]. BCBSM's [redacted] will [redacted] the [redacted]. As appropriate and as aligned with the [redacted] BCBSM will act to further [redacted]

BCBSM will provide pertinent revised [redacted]

3. [redacted]

Recommendation 4

We recommend that BCBSM implement [redacted]

Plan Response

BCBSM acknowledges this recommendation. BCBSM has [redacted] currently in place, to mitigate the risks associated with [redacted] However, BCBSM will develop and propose a plan to [redacted]

4. Vulnerability Scanning

Recommendation 5

We recommend that BCBSM [redacted]

Plan Response

BCBSM acknowledges this recommendation. Under BCBSM's [redacted] plan, and as aligned with [redacted], BCBSM plans to issue revised [redacted]

[redacted]

[redacted] BCBSM will maintain compliance with the [redacted]

[redacted]

D. CONFIGURATION MANAGEMENT

1. [redacted] Standards

Recommendation 6

We recommend that BCBSM [redacted]

Plan Response

BCBSM acknowledges this recommendation. [redacted] plan, activities are identified and in progress [redacted] BCBSM will [redacted]

2. [redacted] Auditing

Recommendation 7

We recommend that BCBSM implement a process to [redacted]

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

Plan Response

BCBSM acknowledges this recommendation. BCBSM will formalize its current [redacted] program [redacted]

[redacted]

3. [redacted] Management

Recommendation 8

We recommend that BCBSM update its [redacted]

Plan Response

BCBSM acknowledges this recommendation. Under BCBSM's [redacted] plan, and as aligned with [redacted] BCBSM plans to [redacted]

BCBSM will provide pertinent [redacted] BCBSM will also [redacted] The plan will address other technical weaknesses identified in this audit's vulnerability scanning inquiry.

b) CONTINGENCY PLANNING

No recommendation noted.

c) Claims Adjudication

No recommendation noted.

BCBSM appreciates the opportunity to respond to each of the recommendations in the draft report. Moreover, BCBSM requests that its 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,

Kim King
Managing Director, FEP Program Assurance

cc: [redacted], OPM
[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