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 Rhode Island

Report Number 2022-ISAG-030
May 1, 2023

Executive Summary

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

Report No. 2022-ISAG-030 **May 1, 2023**

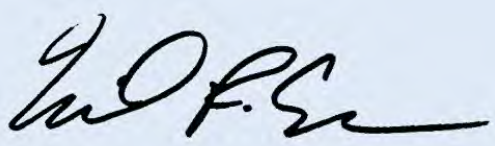
Why Did We Conduct the Audit?

Blue Cross and Blue Shield of Rhode Island (BCBSRI) 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 BCBSRI 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 BCBSRI information systems operating in the general control environment where FEHBP data is processed and stored as of December 2022.



Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of BCBSRI's information systems general and application controls determined that:

- BCBSRI has implemented adequate enterprise security controls.
- BCBSRI [redacted].
- BCBSRI has implemented adequate physical access controls.
- BCBSRI has implemented adequate data center controls.
- BCBSRI has implemented adequate network security controls.
- BCBSRI has implemented adequate security event monitoring and incident response controls.
- BCBSRI had not documented a system component inventory that accurately reflected systems by documenting relationships between systems and all components within the system. In response to the draft audit report, BCBSRI provided evidence demonstrating that the finding was remediated.
- BCBSRI has [redacted]
- BCBSRI has [redacted]
- BCBSRI has implemented adequate system development lifecycle controls.

Acronyms

BCBSRI	**Blue Cross and Blue Shield of Rhode Island**
CFR	**Code of Federal Regulations**
CMDB	**Configuration Management Database**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information Systems Controls Audit Manual**
GAGAS	**Generally Accepted Government Auditing Standards**
GAO	**U.S. Government Accountability Office**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
OIG	**Office of the Inspector General**
OPM	**U.S. Office of Personnel Management**
SP	**Special Publication**

Table of Contents

Report Fraud, Waste, and Mismanagement

I. Background

This final report details the findings, conclusions, and recommendations resulting from the audit of Blue Cross and Blue Shield of Rhode Island's (BCBSRI) general and application controls for its information systems operating in the general information technology (IT) control environment where Federal Employees Health Benefits Program (FEHBP) data related to the following health insurance plan codes are processed and stored, as of December 2022:

- Blue Cross and Blue Shield Service Benefit Plan Standard Option – 10;
- Blue Cross and Blue Shield Service Benefit Plan Basic Option – 11; and
- Blue Cross and Blue Shield Service Benefit Plan FEP Blue Focus – 13.

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 Officer 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) for information systems that directly process FEHBP data and all other information systems in the same general IT environment.

This audit was conducted pursuant to BCBSRI'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.

This was our initial audit of the information systems general and application controls at BCBSRI. All BCBSRI 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 BCBSRI has implemented adequate general and application controls to protect the confidentiality, integrity, and availability of FEHBP data processed and stored by its information systems.

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 BCBSRI information systems operating in the general IT control environment where FEHBP data is processed and stored as of December 2022.

Due to resource limitations, we were not able to assess BCBSRI's entire 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 BCBSRI's information systems environment and applications during the planning phase of the audit to develop an understanding of BCBSRI's controls. Using this risk assessment, additional audit steps were developed, as appropriate, to verify that the controls were properly designed, placed in operation, and effective.

Our audit program was based on procedures and controls contained in the 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 over-all 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 BCBSRI's controls. This included 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.

Due to social distancing guidance related to COVID-19, 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 BCBSRI's information systems. The business processes reviewed are primarily located in Providence, Rhode Island.

The findings, recommendations, and conclusions outlined in this report are based on the status of information systems general and application controls in place at BCBSRI as of December 2022.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether BCBSRI'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 BCBSRI's control structure. These criteria included, but were not limited to, the following publications:

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

While generally compliant with respect to the items tested, BCBSRI 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 BCBSRI's overall IT security program. We evaluated BCBSRI'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
- Plans of action are developed for identified risks.

Nothing came to our attention to indicate that BCBSRI has not implemented adequate enterprise security controls.

B. Logical Access

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 BCBSRI's network environment and applications supporting the FEHBP claims processing business function.

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

- Multi-factor authentication is implemented for access to privileged accounts;
- Limits for consecutive invalid logon attempts are enforced; and
- Access is granted using the principle of least privilege.

[redacted]

1. Authenticator Management

[redacted]

[redacted]

NIST SP 800-53, Revision 5, control IA-5 Authenticator Management, states that the organization change or refresh authenticators at organization-defined time intervals or when organization-defined events occur.

BCBSRI's *Access Control Policy* states that "IT should utilize password aging such that passwords are required to be changed at regularly scheduled intervals."

[redacted]

Recommendation 1:

We recommend that BCBSRI [redacted]

BCBSRI's Response:

"BCBSRI acknowledges the recommendation and took immediate steps to begin implementing it during fieldwork. This recommendation should be fully implemented by [redacted]; BCBSRI will work with the OPM Audit Compliance and Resolution team to close this recommendation after the final report is issued."

OPM OIG Comment:

As part of the audit resolution process, BCBSRI should provide OPM's Internal Oversight and Compliance office with evidence that this recommendation has been implemented. This statement also applies to all subsequent recommendations in this audit report that BCBSRI agrees to implement.

2. Account Management

BCBSRI has not assigned account managers for [redacted] system accounts. Additionally, BCBSRI does not have a procedure to assign a manager to all accounts. In response to this finding, BCBSRI has reduced the number of affected accounts to [redacted]. BCBSRI has also started developing a procedure to capture manager information in the future. BCBSRI continues to evaluate and address the remaining accounts that do not have a manager assigned.

NIST SP 800-53, Revision 5, control AC-2 Account Management, states that the organization assign account managers. NIST defines account types to include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service.

NIST SP 800-53, Revision 5, control AC-1 Policy and Procedures, states that the organization develop, document, and disseminate procedures to facilitate the implementation of access controls. This includes AC-2 control requirements.

Failure to assign account managers increases the risk that BCBSRI is unable to provide accountability and oversight for its system accounts.

Recommendation 2:

We recommend that BCBSRI develop, document, and disseminate a procedure which includes account manager assignment.

BCBSRI's Response:

"BCBSRI acknowledges the recommendation and is in the process of implementing it. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation after the final report is issued."

Recommendation 3:

We recommend that BCBSRI assign account managers to all accounts in accordance with the procedure described in Recommendation 2.

BCBSRI's Response:

"BCBSRI acknowledges the recommendation and is in the process of implementing it. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation after the final report is issued."

3. Disabling and Removing Accounts

[redacted]. The BCBSRI *Access Control Policy* states that accounts shall be disabled after 30 days of inactivity. However, our testing indicated that [redacted]. In response to this finding, BCBSRI has attested that [redacted] BCBSRI continues to evaluate and address the [redacted]. Further, BCBSRI is reportedly working to automate the response to disable accounts in the future.

NIST SP 800-53, Revision 5, control AC-2 Account Management, states that the organization disable and remove accounts in accordance with organizational policies and procedures, which BCBSRI defines as 30 days of inactivity. NIST defines account types to include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service.

Failure to disable and remove unutilized accounts increases the risk that accounts could be compromised.

Recommendation 4:

We recommend that BCBSRI [redacted]

BCBSRI's Response:

"BCBSRI acknowledges the recommendation and is in the process of implementing it, with completion expected by [redacted]. BCBSRI will work with OPM Audit Resolution and Compliance to close this recommendation."

4. Account Compliance Review

BCBSRI [redacted] In response to this finding, BCBSRI has started an effort to [redacted]. Further, BCBSRI provided evidence of [redacted] in the future.

NIST SP 800-53, Revision 5, control AC-2 Account Management, states that the organization review accounts for compliance with account management requirements at an organization-defined frequency. NIST defines account types to include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service.

NIST SP 800-53, Revision 5, control AC-1 Policy and Procedures, states that the organization develop, document, and disseminate procedures to facilitate the implementation of access controls. This includes AC-2 control requirements.

Failure to review system accounts increases the risk that accounts are not compliant with BCBSRI's organizational requirements.

Recommendation 5:

We recommend that BCBSRI [redacted]

BCBSRI's Response:

"BCBSRI acknowledges the recommendation. BCBSRI will update existing procedures to include all system accounts into the existing process by [redacted]. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation."

Recommendation 6:

We recommend that BCBSRI routinely review [redacted] for compliance in accordance with the procedure described in Recommendation 5.

BCBSRI's Response:

"BCBSRI acknowledges the recommendation and is in the process of implementing it, with completed expected by [redacted]. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation."

C. Physical Access

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 BCBSRI's facilities and data centers.

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

- Monitoring and response capabilities for physical security incidents;
- Unnecessary physical access is removed in a timely manner; and
- Physical access to the headquarters facility is controlled using a badge access system.

Nothing came to our attention to indicate that BCBSRI 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 BCBSRI's primary and back-up data centers.

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

- Uninterruptable power supplies provide immediate power failover for systems;
- Environmental controls maintain temperature and humidity; and
- Alternate telecommunication services provide network redundancy.

Nothing came to our attention to indicate that BCBSRI 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 BCBSRI's controls related to network design, data protection, and systems monitoring.

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

- Perimeter controls secure connections to external networks;
- Network communications are denied by default and permitted by exception; and
- Network access controls prevent unauthorized devices from connecting to the internal network.

Nothing came to our attention to indicate that BCBSRI has not implemented adequate network security controls.

F. 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 BCBSRI'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:

- Monitoring capabilities throughout the network to collect security event logs;
- Security event documentation and tracking; and
- Documented incident response plan.

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

G. Configuration Monitoring

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

We also reviewed the results of several credentialed vulnerability and compliance scans performed by BCBSRI, on our behalf, for a sample of BCBSRI servers and workstations. We judgmentally selected a sample of [redacted] servers from a universe of [redacted] and [redacted] workstations from a universe of [redacted] The sample included a variety of system functionality and operating systems across production, test, and development environments. The sample was judgmentally selected from systems that store and/or process FEHBP 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]

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

- Documented change management procedures;
- Documented server configuration baselines; and
- Software installation policies are enforced using technical controls.

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

1. System Component Inventory

BCBSRI has not developed a system inventory that documents relationships between systems and all components within the system. NIST defines system components as "discrete, identifiable information technology assets that include hardware, software, and firmware." BCBSRI had previously identified this as an opportunity for improvement and has an ongoing project to document system component relationships in its configuration management database (CMDB). As a result of the ongoing project, BSBSRI has updated its CMDB to include system inventory records for 98% of hardware components and 92% of application components. BCBSRI's goal is to update at least 95% of the records for both.

NIST SP 800-53, Revision 5, control CM-8 System Component Inventory, states that the organization "Develop and document an inventory of system components that … Accurately reflects the system [and] Includes all components within the system … ."

Failure to document a system inventory that accurately reflects systems and includes all components within the systems increases the risk that BCBSRI will be unable to account for all system components with vulnerabilities.

Recommendation 7:

We recommend that BCBSRI develop and document a system inventory that accurately reflects the system by documenting all relationships between systems and all components within the system.

BCBSRI's Response:

"BCBSRI acknowledges the recommendation. BCBSRI self-identified this matter prior to the audit and worked towards implementing this recommendation throughout fieldwork."

OPM OIG Comment:

In response to the draft audit report, BCBSRI provided evidence demonstrating that it has achieved its goal to update its system inventory for [redacted]% of its hardware and application records. The intent of this recommendation has been addressed. No further action is required.

2. Unsecure Configurations

As a result of our vulnerability scanning exercise, we identified [redacted]. In response to this finding, BCBSRI attested that it had previously identified the [redacted] and either accepted or implemented a plan to remediate associated risks in accordance with its vulnerability management program. However, BCBSRI's scanning tool identified some of the [redacted] to have a severity categorization below the organization-defined threshold to be included in the vulnerability management program. The scanning tool we used to perform this audit testing considers the identified [redacted] to have a higher severity categorization than the tool routinely used by BCBSRI. It is our position that based on our scan results, the risks associated with the [redacted]

NIST SP 800-53, Revision 5, control RA-5 Vulnerability Monitoring and Scanning, states that the organization "Remediate legitimate vulnerabilities [within an organization-defined response time] in accordance with an organizational assessment of risk."

Failure to remediate legitimate vulnerabilities leaves systems susceptible to exploits which leverage those vulnerabilities.

Recommendation 8:

We recommend that BCBSRI perform an assessment of risk for the [redacted]

BCBSRI's Response:

"BCBSRI acknowledges this recommendation and is in the process of implementing it. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation after the final report is issued."

Recommendation 9:

We recommend that BCBSRI [redacted] identified during this audit, in accordance with the organization's assessment of risk described in Recommendation 8.

BCBSRI's Response:

"BCBSRI acknowledges this recommendation and is in the process of implementing it. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this

recommendation. This recommendation will be addressed in accordance with our existing program by [redacted]."

3. Unsupported Software

As a result of our vulnerability scanning exercise, we identified various instances of [redacted] on BCBSRI servers and workstations. In response to this finding, BCBSRI attested that it had previously identified [redacted] and has ongoing projects to [redacted]. Further, BCBSRI provided evidence of a global risk exception for all vulnerabilities that will not be patched or updated due to the imminent decommissioning of a system. This risk exception is updated with a list of associated vulnerabilities monthly.

NIST SP 800-53, Revision 5, control SA-22 Unsupported System Components, states that the organization "Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or … [acquire] alternative sources for continued support … ."

Failure to remove unsupported software from the IT environment increases the risk that components which are no longer receiving critical security patches will be compromised.

Recommendation 10:

We recommend that BCBSRI [redacted] identified during this audit which is [redacted]

BCBSRI's Response:

"BCBSRI acknowledges this recommendation and is in the process of implementing it. This recommendation will be implemented by [redacted]. BCBSRI will work with the OPM Audit Compliance and Resolution team to close the recommendation."

4. Missing Security Patches

As a result of our vulnerability scanning exercise, we identified various [redacted]. In response to this finding, BCBSRI attested that it had previously identified [redacted].

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

Failure to install security-relevant software updates within the organization-defined period of time after their release, increases the risk that vulnerable systems will be compromised.

Recommendation 11:

We recommend that BCBSRI install [redacted] identified during this audit.

BCBSRI's Response:

"BCBSRI acknowledges the recommendation. This recommendation will be implemented by [redacted]. BCBSRI will work with the OPM Audit Compliance and Resolution team to close it."

5. System Configuration Review

As a result of our compliance scanning exercise, we identified various [redacted] that are [redacted]. In response to this finding, BCBSRI stated that while [redacted]

NIST SP 800-53, Revision 5, control CM-6, enhancement 2 Respond to Unauthorized Changes, states that the organization take organization-defined actions in response to unauthorized changes to configuration settings.

NIST SP 800-53, Revision 5, control CM-1 Policy and Procedures, states that the organization develop, document, and disseminate procedures to facilitate the implementation of configuration management controls. This includes CM-6 enhancement 2 control requirements.

Failure to appropriately respond to unauthorized system changes increases the risk that systems will not be securely configured.

Recommendation 12:

We recommend that BCBSRI develop, document, and disseminate [redacted]

BCBSRI's Response:

"BCBSRI acknowledges the recommendation is in the process of implementing it. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation after the final report is issued."

Recommendation 13:

We recommend that BCBSRI respond to the [redacted] identified during this audit in accordance with the procedures described in Recommendation 12.

BCBSRI's Response:

"BCBSRI acknowledges the recommendation. This recommendation will be implemented by [redacted]. BCBSRI will work with the OPM Audit Compliance and Resolution team to close the recommendation."

H. Contingency Planning

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 BCBSRI'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.

However, we noted the following opportunity for improvement related to BCBSRI's contingency planning controls.

1. Disaster Recovery Plan

BCBSRI has not [redacted] Specifically, the disaster recovery

plan does [redacted] BCBSRI has contracted with third parties to perform many of its claims processing business functions. However, BCBSRI still manages many systems related to claims processing which were included in BCBSRI's migration to the cloud. BCBSRI has demonstrated that disaster recovery planning and testing is implemented for all systems hosted by its contracted third parties. However, disaster recovery plans for BCBSRI's internally managed systems [redacted]. BCBSRI has demonstrated that these plans are in the process of being updated.

NIST SP 800-53, Revision 5, control CP-2 Contingency Plan states that the organization "Update the [disaster recovery plan] to address changes to the organization, system, or environment of operation....."

[redacted]

Recommendation 14:

We recommend that BCBSRI [redacted]

BCBSRI's Response:

"BCBSRI acknowledges the recommendation and is in the process of implementing it. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation after the final report is issued."

I. System Development Lifecycle

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 BCBSRI'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 BCBSRI 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

March 15, 2023

Stephen Sala, 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 Response
Blue Cross Blue Shield of Rhode Island (BCBSRI)
Audit Report Number 2022-ISAG-0030
(Dated January 12, 2023)

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

A. Enterprise Security

No recommendations noted.

B. Logical Access

Authenticator Management

Recommendation 1:

We recommend that BCBSRI [redacted]

Plan Response:

BCBSRI acknowledges the recommendation and took immediate steps to begin implementing it during fieldwork. This recommendation should be fully implemented by [redacted]; BCBSRI will work with the OPM Audit Compliance and Resolution team to close this recommendation after the final report is issued.

Account Management

Recommendation 2:

We recommend that BCBSRI develop, document, and disseminate a procedure which includes account manager assignment.

Plan Response:

BCBSRI acknowledges the recommendation and is in the process of implementing it. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation after the final report is issued.

Recommendation 3:

We recommend that BCBSRI assign account managers to all accounts in accordance with the procedure described in Recommendation 2.

Plan Response:

BCBSRI acknowledges the recommendation and is in the process of implementing it. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation after the final report is issued.

Disabling and Removing Accounts

Recommendation 4:

We recommend that BCBSRI [redacted]

Plan Response:

BCBSRI acknowledges the recommendation and is in the process of implementing it, with completion expected by [redacted]. BCBSRI will work with OPM Audit Resolution and Compliance to close this recommendation.

Account Compliance Review

Recommendation 5:

We recommend that BCBSRI [redacted]

Plan Response:

BCBSRI acknowledges the recommendation. BCBSRI will update existing procedures to include all system accounts into the existing process by [redacted]. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation.

Recommendation 6:

We recommend that BCBSRI routinely review [redacted] for compliance in accordance with the procedure described in Recommendation 5.

Plan Response:

BCBSRI acknowledges the recommendation and is in the process of implementing it, with completed expected by [redacted]. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation..

C. Physical Access

No recommendations noted.

D. Data Center

No recommendations noted.

E. Network Security

No recommendations noted.

F. Security Event Monitoring and Incident Response

No recommendation noted.

G. Configuration Management

System Component Inventory

Recommendation 7:

We recommend that BCBSRI [redacted]

Plan Response:

BCBSRI acknowledges the recommendation. BCBSRI self-identified this matter prior to the audit and worked towards implementing this recommendation throughout fieldwork. Refer to **Attachment 1** for evidence of remediation.

Unsecure Configuration

Recommendation 8:

We recommend that BCBSRI perform an assessment of risk for the [redacted] identified during this audit.

Plan Response:

BCBSRI acknowledges this recommendation and is in the process of implementing it. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation after the final report is issued.

Recommendation 9:

We recommend that BCBSRI [redacted] identified during this audit, in accordance with the organization's assessment of risk described in Recommendation 8.

Plan Response:

BCBSRI acknowledges this recommendation and is in the process of implementing it. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation. This recommendation will be addressed in accordance with our existing program by [redacted].

Unsupported Software

Recommendation 10:

We recommend that BCBSRI [redacted] identified during this audit which is [redacted]

Plan Response:

BCBSRI acknowledges this recommendation and is in the process of implementing it. This recommendation will be implemented by [redacted]. BCBSRI will work with the OPM Audit Compliance and Resolution team to close the recommendation.

Missing Security Patches

Recommendation 11:

We recommend that BCBSRI install [redacted] identified during this audit.

Plan Response:

BCBSRI acknowledges the recommendation. This recommendation will be implemented by [redacted]. BCBSRI will work with the OPM Audit Compliance and Resolution team to close it.

System Configuration Review

Recommendation 12:

We recommend that BCBSRI develop, document, and disseminate [redacted]

Plan Response:

BCBSRI acknowledges the recommendation is in the process of implementing it. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation after the final report is issued.

Recommendation 13:

We recommend that BCBSRI respond to the [redacted] identified during this audit in accordance with the procedures described in Recommendation 12.

Plan Response:

BCBSRI acknowledges the recommendation. This recommendation will be implemented by [redacted]. BCBSRI will work with the OPM Audit Compliance and Resolution team to close the recommendation.

H. Contingency Planning

Disaster Recovery Plan

Recommendation 14:

We recommend that BCBSRI [redacted]

Plan Response:

BCBSRI acknowledges the recommendation and is in the process of implementing it. BCBSRI will work with the OPM Audit Resolution and Compliance team to close this recommendation after the final report is issued.

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]) [redacted] or [redacted] 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

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