Fairfax County Internal Audit Office

Department of Information Technology
Information Security Office
FOCUS Audit Log Configuration Audit
Final Report

October 2015

THIS AUDIT REPORT IS NOT TO BE RELEASED TO THE PUBLIC AND IS NOT SUBJECT TO FOIA (VA CODE 2.2-3705.2(3)) DUE TO CERTAIN SECURITY RELATED AND CONFIDENTIAL INFORMATION THAT MAY JEOPARDIZE COUNTY SECURITY.

"promoting efficient & effective local government"

Introduction

Fairfax County Unified System (FOCUS) audit log configuration plays an important part in ensuring the overall integrity and security of the system. FOCUS audit log keeps a daily record of user activities for each application server in an audit file on the SAP system. The FOCUS audit log configuration records event information based on organizational requirements while the audit log helps ensure audit records are stored and adequate detail is maintained for an appropriate period. By properly configuring the audit log, we receive a detailed look at critical events that occur in the SAP system. Furthermore, FOCUS audit log provides the ability to identify the events that are considered high risk, critical and require monitoring. When adequately configured, the audit log is a powerful tool used to keep track of users' activities and the transaction codes executed by those users. Additionally, the audit log provides important details of each transaction initiated; who initiated it; when it was initiated (date/time stamp); where the transaction occurred; and the final results, among other things.

FOCUS audit logs are a key component in effective information technology security. By activating the audit logs, important activities available in the SAP system will be recorded. Properly configuring the audit log provides a means to help accomplish several objectives such as accountability of user actions, intrusion detection, and notification of system errors and failures. Audit log parameters provide the capability to selectively configure critical events to capture information relating to user, system, and application performance. Additionally, it is important that audit log parameters are properly configured with adequate details, as omissions in configuration may result in improper capture of critical event information. Furthermore, it is essential for SAP systems to capture audit logs that contain sufficient information to support audits and investigations, as well as compliance with applicable laws, county policies, and regulations.

Executive Summary

The FOCUS system is comprised of core business functions which support the overall processing of human resources, payroll, vendor payments, budgets, procurements, and accounting. Our audit focused on determining whether FOCUS audit log configuration had the necessary controls in place to ensure critical events were captured, stored, and maintained securely for an appropriate length of time. We reviewed the process to ensure policies and procedures were in place to support the overall structure of audit log configuration. During our audit, we noted adequate policies and procedures existed to support the audit log configuration which were in compliance with the county's Information Security Policy 70-05. Additionally, we found that strong controls existed for configuring, reviewing, and monitoring audit logs. The audit log information was structured in a text delimited format that was readily usable for reviewing and processing. Overall, the FOCUS system controls accurately captured and recorded audit log information and adequate controls were in place regarding user access to audit information within the SAP system environment. A review of access and execution of sensitive transactions for standard users occurred daily to uncover suspicious activity. Approved users were contained in groups called "Roles" which gave them read only access with the ability to

view audit log information. The Security Team reviewed and monitored audit logs daily to prevent unauthorized users from creating, modifying, or deleting information. However, we noted the following areas where internal controls could be strengthened:

- At the time of FOCUS implementation in November 2011, both the Department of Information Technology (DIT), Information Security Office (ISO) and the Internal Audit Office (IAO) agreed to configure the audit log to capture all events until further analysis could be conducted. During our review, through discussions with DIT ISO, we both agreed that a standard baseline to capture only certain events that were critical and required monitoring should be developed. The baseline should capture sufficient information to support critical business functions and streamline the review processes.

- A formal documented procedure for audit log management, data retention and disposal had not been developed to provide guidelines on implementing and maintaining audit log data. This procedure should include information specific to audit log management processes to adequately reflect the current SAP network environment for the overall controls over management, maintenance, and disposal of audit log information within the FOCUS system.

- The current FOCUS environment would be significantly enhanced by an automated audit log management tool to strengthen controls to assist the Security Team in performing their job functions effectively and efficiently. The absence of an automated tool may cause a delay in reviewing and analyzing audit logs. As a result, the Security Team may not be able to identify and respond to critical events in a timely manner.

Scope and Objectives

This audit was performed as part of our fiscal year 2015 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. Those standards require 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This audit covered the period of October 1, 2013, through September 30, 2014. The objectives of the audit were to determine that FOCUS had:

- Adequate policies and procedures developed and in compliance with the County's Information Security Policy 70-05;
- Adequate controls over the complete and proper configuration of audit logs and parameter settings;
- Audit log information captured and retained in a manner readily usable for effective monitoring and within an adequate period of time;
- Adequate controls to protect audit logs from unauthorized access, modification, and deletion;

- Audit configurations that were consistent across the county to support the Department of Information Technology's policy outlined security objectives;
- Adequate controls over time source synchronization to ensure the time associated with logged events was correct.

Methodology

Our audit approach included interviewing appropriate staff in the DIT ISO Team to obtain an understanding of the FOCUS audit log configuration process, specifically audit log parameter settings, configuration, and analysis. We evaluated those processes for compliance with sound internal controls and the county/department policies and procedures. We observed the Security Team's daily work functions; and determined if controls were in place to prevent audit log data from unauthorized access, creation, modification, or deletion. In addition, we obtained/reviewed the procedures to configure and process audit logs to determine whether adequate controls were in place and capturing sufficient information to detect and respond to potential fraud, policy violations, unauthorized access or transactions.

IAO is free from organizational impairments to independence in our reporting as defined by Government Auditing Standards. We report directly and are accountable to the County Executive. Organizationally, we are outside the staff or line management function of the units that we audit. We report the results of our audits to the County Executive and the Board of Supervisors, and IAO audit reports are available to the public.

Findings, Recommendations, and Management Response

1. Audit Log Configuration Baseline

When the FOCUS system was first implemented in November 2011, DIT ISO developed a baseline that captured all audit events that occurred within the FOCUS system. To ensure that we did not miss critical information since it was a new system. IAO was given a copy of the methodology and agreed with the approach. As a result, large amounts of audit log information were captured and retained. After further experience with the system and analysis, we agreed that the standard baseline needed to be refined to only capture specific audit information and adequately reflect the criticality of high risks and important events. The proposed baseline for audit log configuration should provide consistency in configuring audit log parameters and settings to ensure the overall consistency across the enterprise. The audit log configuration baseline contains recommended settings that provides the Security team with relevant information to configure audit logs in a uniform manner.

Recommendation: We recommend DIT ISO develop a more stringent audit log configuration baseline to capture more specific events that are critical to business processes. These events should provide sufficient information to establish

accountability for transactions processed and any important changes made in FOCUS. Once completed, the audit log configuration baseline should be reviewed by IAO to ensure it is in compliance with County requirements.

Note: *IAO learned that the FOCUS system will be upgraded in November 2016. We recommend DIT ISO work with SAP to ensure changes being made to the FOCUS system are compatible with the new upgrade.*

Management Response: ISO has made contact with the appropriate parties in SAP/ASUG to talk about known best practices for making changes to the logs (SM20). DIT has designed a new baseline that will be reviewed for possible implementation. Prior to any changes the baseline will also be reviewed with IAO. Management has anticipated completing this action by December 15, 2015.

2. Documented Procedures

DIT had some written procedures in place; however, we found a number of areas that did not provide a clear guideline to the Security team. These areas include:

a. Audit log management procedures had not been developed to consistently provide a guideline and controls over the overall management and maintenance of the audit log. During our audit, DIT ISO developed Audit log management procedures to provide guidelines and controls over the management and maintenance of the audit log.

b. There was no formal data retention procedure for FOCUS audit logs. However, during our audit we learned that, DIT ISO was already taking steps to develop a procedure specifying the retention period for maintaining audit log data. This will reduce the storage space while complying with applicable laws, county policies, and regulations.

c. A disposal procedure had not been developed to provide all the necessary guidelines in order to ensure appropriate steps were performed during the audit log removal/deletion process.

Recommendation: We recommend DIT ISO develop and implement, written procedures for the audit log management, data retention, and disposal of audit logs to provide guidance and support of the overall audit log management processes that comply with applicable laws, county policies, and regulations. It is important that the Security team establishes formal procedures related to all aspects of audit log management. These procedures will provide a documentation of the baseline to ensure proper configuration and administration of audit logs are adhered to by all Security staff in a consistent manner.

Management Response: ISO will develop an ISO operating procedure for security log management based on COVA and GASB financial system management guidelines. Management has anticipated completing this action by March 2016.

NOTE: *This is an on-going DIT process. The SAP security audit logs will be part of a bigger discussion of archiving and disposal all SAP logs based on retention requirements. This activity usually occurs within years 5 or 6 of a SAP implementation. We are currently in year 5 for FILO and year 3 for HCM. Ownership of certain logs (including information captured in SM20) includes the Business Process Owners. Once ownership is determined the responsible staff will be adjusted to reflect the area and owner. Currently, all data is within the guidelines for archiving and disposal as outlined in VITA, HIPAA and PII codes. A responsive solution for business process needs is not available.*

3. Audit Log Management Tool

During our audit, we found that DIT ISO utilized a manual process to review, detect, and respond to potential fraud, policy violations, or unauthorized access or transactions. Audit logs were reviewed daily to determine if there was suspicious activity. However, the process was time and resource intensive and automated controls would strengthened the process to provide the Security team with more timely notification when critical events occurred requiring immediate attention. The lack of an automated audit log management tool can result in the inability to promptly identify and respond to critical security incidents.

Recommendation: We recommend DIT ISO implement an automated tool to assist the Security team in detecting, monitoring, and responding to critical events in a more timely manner. This will strengthen controls in place to provide monitoring and alerting notifications of critical events. Additionally, controls should have an automated trigger or alert such as an email/text generated in the event of a critical transaction to be sent to the Security team for their review if further investigation is required. The tool should identify certain unauthorized or high risk activity where possible to improve monitoring and reviewing processes.

Management Response: DIT is researching possible Audit Log Management tools for SAP. As indicated in #1, we are working through ASUG in our discovery process. So far, known capabilities are custom built by the customer. Once a feasible solution is determined a formal request for funding will be submitted. A cost benefit analysis will be completed before moving forward with funding or purchasing of such software. IAO will be informed of the decision to move to the tool once all aspects of review are completed as a part of audit follow-up work. Management has anticipated completing this action by June 2017.