County of San Diego

Auditor and Controller

OFFICE OF AUDITS & ADVISORY SERVICES

SHAREPOINT SECURITY AUDIT

FINAL REPORT

Chief of Audits: Juan R. Perez
Senior Audit Manager: Lynne Prizzia, CISA, CRISC
Senior Auditor: Franco D. Lopez, CPA, CIA, CISA
Auditor I: Wasim M. Akand

Report No. A13-019

January • 2014

Intentionally Left Blank

TRACY M. SANDOVAL
GENERAL MANAGER/
AUDITOR & CONTROLLER
(619) 531-5413
FAX: (619) 531-5219

County of San Diego

FINANCE & GENERAL GOVERNMENT GROUP
1600 PACIFIC HIGHWAY, SUITE 166, SAN DIEGO, CA 92101-2422

ASSESSOR/RECORDER/COUNTY CLERK
AUDITOR AND CONTROLLER
CHIEF ADMINISTRATIVE OFFICE
CIVIL SERVICE COMMISSION
CLERK OF THE BOARD
COUNTY COMMUNICATIONS OFFICE
COUNTY COUNSEL
COUNTY TECHNOLOGY OFFICE
GRAND JURY
HUMAN RESOURCES
RETIREMENT ASSOCIATION
TREASURER-TAX COLLECTOR

January 6, 2014

TO: Nick Macchione, Director
Health and Human Services Agency

Mikel D. Haas, Chief Information Officer
County Technology Office

FROM: Juan R. Perez
Chief of Audits

FINAL REPORT: SHAREPOINT SECURITY AUDIT

Enclosed is our report on SharePoint Security Audit. We have reviewed your response to our recommendations and have attached them to the audit report.

The actions taken and/or planned, in general, are responsive to the recommendations in the report. As required under Board of Supervisors Policy B-44, we respectfully request that you provide quarterly status reports on the implementation progress of the recommendations. The Office of Audits & Advisory Services will contact you or your designee near the end of each quarter to request your response.

Also attached is an example of the quarterly report that is required until all actions have been implemented. To obtain an electronic copy of this template, please contact Franco Lopez at (858) 505-6436.

If you have any questions, please contact me at (858) 495-5661.

JUAN R. PEREZ
Chief of Audits

AUD:FDL:aps

Enclosure

c: Tracy M. Sandoval, Deputy Chief Administrative Officer/Auditor & Controller
Brian M. Hagerty, Group Finance Director, Finance and General Government Group
Andrew McDonald, Group IT Manager, Finance and General Government Group
Andrew Pease, Executive Finance Director, Health and Human Services Agency
Richard McWilliams, Group IT Manager, Health and Human Services Agency

Printed on recycled paper

INTRODUCTION

Audit Objective

The Office of Audits & Advisory Services (OAAS) completed an audit of SharePoint Security. The objective of the audit was to assess the design and operating effectiveness of SharePoint security controls in areas including, but not limited to Health and Human Services Agency's (HHSA):

- Governance & Management Oversight
- Monitoring
- Configuration & Content Management

Background

SharePoint is a Microsoft platform that allows organizations to provide sharing and retention of data in various forms. The SharePoint platform provides users an environment to:

- Manage content and business processes.
- Discuss ideas and review documents or proposals.
- Coordinate projects, calendars, and schedules.
- Find and share information across business boundaries.
- Enable informed decisions.

In the County, SharePoint implementations are decentralized by department. Using the Insite, Collaboration or Application modules, departments can create, manage, and build sites within SharePoint to meet their business needs. Departments are responsible for ensuring their SharePoint environments are maintained in accordance with the SharePoint Management Plan and relevant County policies. HP Enterprise Services (HP) maintains the SharePoint infrastructure, while the County Technology Office (CTO) is the technical owner of the environment.

Group Leads are assigned to each County Group and act as a liaison between the CTO and County departments. Within HHSA, Group Leads also take on the role of Site Administrator for all sites within the Agency, assigning Site Owner account privileges to sites and sub-sites as appropriate. Site Owner privileges allow users to create sites and maintain appropriate user access. According to ISACA, decentralized implementation provides more challenges to the effective and secure controls over content; requiring a focus on governance practices, policy and guideline communications with the users, and a managerial monitoring activity to assure compliance with governance requirements.[1]

Audit Scope & Limitations

The scope of the audit focused on evaluating the adequacy of HHSA's SharePoint security controls from April to June 2013. This included reviewing technical configurations and the application of Countywide standards that affect SharePoint security for all County users. OAAS

[1] ISACA Microsoft SharePoint 2010 Audit/Assurance Program

also based their assessment on recommended IT controls from the IT Governance Institute's Control Objectives for Information and related Technology 4.1 (COBIT).

This audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing prescribed by the Institute of Internal Auditors as required by California Government Code, Section 1236.

Methodology

OAAS performed the audit using the following methods:

- Reviewed SharePoint enterprise objectives and guiding principles.
- Reviewed HHSA policies and interviewed stakeholders.
- Reviewed site monitoring and content controls of sampled sites.
- Reviewed if privileged accounts are appropriately configured and assigned to minimize unauthorized access.
- Ensured site security controls are established to protect the integrity of SharePoint site content.

AUDIT RESULTS

Summary

Within the scope of the audit, the design and operating effectiveness of SharePoint security controls were generally adequate as applied in the HHSA SharePoint environment. Specific issues were identified in the areas of SharePoint training and privileged account management.

To further strengthen current SharePoint security controls and improve control effectiveness, OAAS offers the following findings and related recommendations.

Finding I: **SharePoint Training Requirements Should be Enforced**

Out of 18 HHSA Collaboration sites identified, OAAS sampled 6 sites to evaluate the effectiveness of monitoring controls. Site Administrator and Site Owner monitoring efforts of the SharePoint Collaboration environment were adequate in areas outlined within the HHSA SharePoint policy. However, specific issues were identified in the area of training that highlight security controls which should be improved.

Site Owners of the six sampled sites had not completed HHSA SharePoint required training at the time of audit. While all site owners in the sample have started taking preliminary training, none had completed all SharePoint courses required by HHSA SharePoint policy (HHSA-F-11). Additionally, four of five sub-sites tested had managers with Site Owner privileges that also had not completed required SharePoint training.

Recommendation: To comply with policy and improve security controls, HHSA should ensure SharePoint users comply with training as outlined in policy (HHSA-F-11, Appendix C). Additionally, HHSA managers should obtain direction on the appropriate level of access they need within SharePoint.

Finding II: **SharePoint Privileged Accounts Security Needs Improvement**

The SharePoint environment has local Structured Query Language (SQL) accounts with excessive elevated privileges which need to be reduced. All other SharePoint administrative accounts have gone through a role based access (RBAC) review which restricts privileged account access to the least required per HP's standard. However, at the time of review local SQL accounts had not gone through an RBAC review. HP indicated they are working on identifying individuals associated with local SQL accounts where appropriate. This effort will include determining employee role and reducing privileges to the least required for that role.

The T424 Security Management Plan and COBIT[2] outline access should be granted to the users on a need-to-know basis for their job duties. Roles and responsibilities should be divided to reduce the risk of an individual having the ability to compromise a critical process. Currently, local SQL accounts have a high risk of providing account holders with the ability to compromise the SharePoint database. A compromise would not be automatically identified because monitoring of administrative accounts is not an activity currently conducted by HP.

[2] Standard PO 4.11, Segregation of Duties

DEPARTMENT'S RESPONSE (COUNTY TECHNOLOGY OFFICE)

County of San Diego

1600 PACIFIC HIGHWAY, ROOM 306, SAN DIEGO, CA 92101-2472

County Technology Office
MIKEL HAAS

Office of the CIO
Business Advisory Services
Communications
Enterprise Architecture & Technology
Financial & Contract Mgmt Services
Risk Management
Service Management

RECEIVED

DEC 17 2013

OFFICE OF AUDITS & ADVISORY SERVICES

12/16/2013
Ref: 13-IA-351

TO: Juan Perez
Chief of Audits

FROM: Mikel Haas, CIO
County Technology Office

DEPARTMENT RESPONSE TO AUDIT RECOMMENDATIONS: SHAREPOINT SECURITY AUDIT

Finding II: SharePoint Privileged Accounts Security Needs Improvement

OAAS Recommendation: The CTO should ensure that HP develops and executes a plan to reduce the administrative privileges of local SQL accounts to the least required as outlined in the T425 Security Management plan.

Action Plan: The CTO will task HP with determining and reducing the SharePoint local SQL accounts permissions to an appropriate level as required by the Security Management Plan (T424)

☐ Implemented ☐ In Progress ☒ Pending-Not Started

Planned Completion Date: June 30, 2014

Contact Information for Implementation: Valerie Kohls, Technology Manager (619) 515-4336

If you have any questions, please contact Mike Teays at (619) 316-5208 or myself at (619) 685-2397.

Regards,

Mikel Haas
Chief Information Officer

CC:Mike Teays
Susan Green

DEPARTMENT'S RESPONSE (HEALTH AND HUMAN SERVICES AGENCY)

NICK MACCHIONE, FACHE
DIRECTOR

RICHARD McWILLIAMS
GROUP IT MANAGER

County of San Diego
HEALTH AND HUMAN SERVICES AGENCY
INFORMATION TECHNOLOGY DIVISION
1255 IMPERIAL AVENUE, SUITE 818, SAN DIEGO, CA 92101
(619) 338-2818 • FAX (858) 715-6448

December 30, 2013

TO: Juan R. Perez, Chief of Audits
Office of Audits and Advisory Services

FROM: Richard McWilliams, Group IT Manager
Information Technology Division

VIA: Nick Macchione, Director
Health and Human Services Agency

RECEIVED
DEC 30 2013
OFFICE OF AUDITS & ADVISORY SERVICES

RESPONSE TO AUDIT RECOMMENDATIONS: SHAREPOINT SECURITY

Finding I: SharePoint Training Requirements Should be Enforced

OAAS Recommendation: To comply with policy and improve security controls, HHSA should ensure SharePoint users comply with training as outlined in policy (HHSA-F-11, Appendix C). Additionally, HHSA managers should obtain direction on the appropriate level of access they need within SharePoint.

Action Plan:

1. As of July 30, 2013, each SharePoint Group Lead within HHSA is enforcing all training requirements outlined in HHSA-F-11, Appendix C. Moreover, each site collection owner receives a weekly Learning Management System (LMS) report which is used to verify that every user with full control has completed all required training. If any user without the required training is found to have full control, that individual will lose full control permissions and the policy violation will be referred to the HHSA SharePoint Lead.

2. The HHSA SharePoint policy is being revised such that only site collection owners may be granted full control permissions. These site collection owners, who are appointed by their division's senior executive, must sign a memorandum document their understanding that they must comply with all information security and web development policies, and must not grant full control permissions to any other user.

3. The HHSA SharePoint Lead is creating a custom permission level, to be called "Site Administrator," which site collection owners can assign to individual site owners instead of full control. The Site Administrator permission level differs from full control in that the following actions are not allowed: manage permissions levels, create groups, and apply style sheets.

4. Finally, the IT outsource contractor is developing a SharePoint report to detect all users with Full Control permissions. The HHSA SharePoint Group Leads will monitor this report to ensure the effectiveness of the policy changes mentioned above.

Completion Date: January 15, 2013

Contact Information for Implementation: Derek Britt, Dept. Technology Systems Specialist, (619) 338-2603.

If you have any questions, please contact me at (619) 338-2818.

RICHARD MCWILLIAMS, Group IT Manager
Information Technology Division

RM/DB/ag