OBM | Office of Internal Audit

Department of Administrative Services
Patch Management Audit

Audit Period: November 2017 through October 2018

Results Summary:

Objective	Conclusion
Workstations Patch Management Process	**Major Improvement Needed**
Servers Patch Management Process	**Well-Controlled with Improvement Needed**

* Refer to Appendix A for classification of audit objective conclusions.

Report number: 2019-DAS-22 **Issuance date: December 13, 2018**

Executive Summary

Background

The Ohio Department of Administrative Services' (DAS) mission is to improve the effectiveness and efficiency of Ohio government by providing statewide leadership, oversight, products and services for activities related to information technology. Its goals are to:

- Deliver more effective and efficient government by optimizing the return on information technology investment, finding and delivering on opportunities for technology-enhanced business processes, leading appropriate consolidation and unification of technology solutions, and fostering the creation of collaborative applications across agencies.

- Be the provider of choice for Ohio governmental information technology by identifying, procuring, providing and supporting (where appropriate) reliable, secure, optimally performing products, services and infrastructure that encourage the use of common technology.

- Build a customer responsive organization that inspires confidence, is helpful, and actively collaborates to find enterprise-wide solutions while providing leadership in IT.

- Strengthen the OIT organization by successfully collaborating with central service agencies; developing leaders and strengthening our technical skills; improving procurement, customer relationship management and strategic planning processes; and building a first class service support organization.

DAS performs patch management for systems that are hosted and controlled at the State of Ohio Computer Center, as well as workstations used internally. As part of the FY 2019 audit plan, OIA was engaged to perform a review of system controls for patch management.

During the audit, OIA identified opportunities for DAS to strengthen internal controls and improve business operations. A summary, along with detailed observations, has been provided. OIA would like to thank DAS staff and management for their cooperation and time in support of this audit.

This report is solely intended for the information and use of agency management and the State Audit Committee. It is not intended for anyone other than these specified parties.

Scope and Objectives

OIA staff was engaged to perform an assurance audit related to the controls over the agency's patch management process. This work was completed October through December 2018.

The objectives of this audit are as follows:

- To evaluate the design and effectiveness of controls around the patch management process for workstations managed by DAS.
- To evaluate the design of controls around the patch management process for Windows servers managed by DAS.

The detailed scope of the engagement is as follows:

- For the workstations
  - Policies and procedures
  - Identification, prioritization, and communication
  - Change management process for patching (standard and emergency)
  - Testing, deployment, and validation
  - Exception process (if a patch cannot be installed)
- For the server patch management process
  - Policies and procedures
  - Identification, prioritization, and communication
  - Exception process

The audit period for this engagement is November 2017 through October 2018.

* Please refer to Appendix A for classification of audit objective conclusions.

Detailed Observations and Recommendations

The Observations and Recommendations include only those risks which were deemed high or moderate. Low risk observations were discussed with individual agency management and are not part of this report. However, the low risk observations were considered as part of the audit objective conclusions.

Observation 1 – Inadequate Procedures for Patching Workstations

Policies and procedures help ensure the actions initiated by management to address risks are achieved. Procedures define roles, designate responsibilities, and detail actions necessary to achieve management's objectives and help ensure compliance with applicable laws and regulations. In addition, detailed procedures help ensure the continuity of the process in the event of personnel turnover. Section 5.1.2.1 of DAS Policy, "System and Information Integrity Policy," indicates that "security vulnerabilities, as specified by DAS OISP, shall be remediated by system owners and/or application owners through the application of patches, configuration changes, replacing or removing software, and/or coding changes, or other compensating controls within 30 days of reporting."

During our review, we noted that:

- The workstation patch procedure document provided was not formally approved with an effective date or name of the approver.
- Roles and responsibilities for the workstation patching process are not adequately defined. In discussion with the ITS Desktop Support Team and OISP Vulnerability team, conflicting information was provided on which team makes the decision to deploy patches for specific third party software and zero day vulnerabilities.
- Policies and procedures for change management and communication for workstation patching do not exist.
- Process and procedures for testing and validation of workstation patches are not documented.

A lack of formally documented workstation patching policies and procedures may lead to ineffective and inconsistent implementation and monitoring practices, leaving the agency open to compromise via exploitable vulnerabilities. In addition, individuals with roles in the patching process may not be fully aware of their responsibilities and communication may not be occurring to all individuals.

Recommendation
Management should develop procedures for the workstation patching process. Policy and procedures should include the following: · The name(s) of the approvers and the approval date · Information on when the policy/procedure was last revised (and a summary of changes) · List individuals' roles and responsibilities in the process (i.e. for applying patches, testing patches, making the decision to apply patches, etc.) · Describe the change management process for workstation patching, including communication · The process for testing patches prior to deployment · Describe in detail the process for validation of workstation patch installations and who is informed of these · Define standard metrics, such as timeframe needed for patch installation · Work to complete remediation of vulnerabilities in the 30-day time period in section 5.1.2.1 of DAS Policy, "System and Information Integrity Policy." Alternatively, determine if a need exists to revise the timeframe for mitigating vulnerabilities via patch.
Management Response
DAS will develop procedures for the workstation patching process that documents the requirements for maintaining up-to-date operating system security patches and software version levels on all DAS supported desktops. This will include names of approvers, revision history, and individual roles and responsibilities. The Change management process is discussed in Observation 2., which includes the process of patching, testing and validation.

Risk*	Remediation Owner	Estimated Completion Date
High	CIO	January 31, 2019

Observation 2 – Inadequate change management for patching workstations

DAS Policy ITS-SEC-02 states NIST Special Publication 800-53 is the framework for information security control implementation for the State. NIST 800-53r4 control CM-3 requires that an organization review proposed changes to information systems with a consideration for security impact analyses.
OIA noted that change management tickets are not submitted when patches for workstations are deployed. However, it was indicated that DAS OIT staff (including the Service Desk) are aware of the timeframes when patches are deployed.

Since change requests are not created, workstation patches are applied to systems without formal communication, review, and approval. Further, potential issues can occur after applying a patch that may lead to additional research to determine the underlying cause of a workstation issue. If a clear history of patch deployments is not available for review via change requests, it may be more difficult to troubleshoot.

Recommendation

Management should ensure that change management tickets are created when workstation patches are deployed, using the DAS-established change management process using ServiceNow. These tickets should provide information on the specific patches being applied, systems receiving them, the date the ticket was opened, name of the person deploying them, and an estimated close date for deployment.

When change tickets are closed, the ticket should include details on the number of workstations that were affected and the number of workstations where the patch was successfully or not successfully applied.

Management Response

DAS will modify our procedure to ensure that change management tickets are created when workstation patches are deployed, using the DAS-established change management process, ServiceNow. Per this recommendation, we will list affected workstations and percentage completed upon closure of change ticket.

Risk*	Remediation Owner	Estimated Completion Date
High	CIO	January 31, 2019

Observation 3 – A formal validation process is not in place to ensure that all workstation patches are installed

DAS Policy ITS-SEC-02 states that NIST 800-53 is the framework for information security control implementation for the State of Ohio. It also states that the CIS Controls complement the security controls in NIST SP 800-53 and that the CIS Controls address the highest threat areas for the enterprise environment. According to Center for Internet Security (CIS) Control 3, back-to-back vulnerability scans should be compared to verify that vulnerabilities have been mitigated in a timely manner. Validation helps ensure that vulnerabilities have been mitigated.

OIA noted that the Desktop Support team does not perform a formal validation to ensure that all workstations have been successfully patched; however, some informal activity occurs. Qualys creates reports on the status of patch installations and these are available to the Desktop Support team. In addition, the OISP Vulnerability team e-mails monthly Qualys reports on the status of patch installations to the Desktop Support team.

Unless validation is performed to ensure that patches have been successfully applied to all systems, vulnerabilities can still be exploited on systems where patch installations were not completed.

Recommendation

Management should create a formal validation process for ensuring that workstation patches have been successfully installed. Potentially, this process could utilize Qualys reports that show open vulnerabilities in order to validate successful patch installation. The process should identify individuals responsible for validation, how often validation occurs, describe activities undertaken for validation, and define key individuals that receive reports on the status and results of patch deployments.

Management Response

DAS will create a formal validation process for ensuring that workstation patches have been successfully installed. The process will include leveraging Qualys reporting capabilities and Microsoft SCCM to verify that security patches were properly installed.

Risk*	Remediation Owner	Estimated Completion Date
High	CIO	March 31, 2019

Observation 4 – Inadequate patching of workstation vulnerabilities

According to Center for Internet Security (CIS) Control 3, vulnerabilities should be identified, remediated and minimize the window of opportunity for attackers. It also indicates that third party software on all systems should be running the most recent security updates provided by vendors. This will help ensure that vulnerabilities for third party software have been mitigated. Section 5.1.2.1 of DAS Policy, "System and Information Integrity Policy," indicates that "security vulnerabilities, as specified by DAS OISP, shall be remediated by system owners and/or application owners through the application of patches, configuration changes, replacing or removing software, and/or coding changes, or other compensating controls within 30 days of reporting."

OIA noted that not all patches are applied to all workstations consistently. The software affected was identified for DAS. As such, the timeframe for mitigating vulnerabilities is not met. Per the ITS Desktop Support Team, OISP informs them about specific critical third party patches that need to be applied to application software via Qualys report and security bulletins. However, the OISP Vulnerability team expects that all third-party software will be patched.

Unless all patches are applied, vulnerabilities will remain present on workstations that could be exploited by attackers. Further, potentially unclear roles and responsibilities can lead to confusion in the patching process.

Recommendation

Management should ensure that all patches are applied on a regular, established schedule on a prioritized basis to meet established metrics. Prioritization should be performed based on risk level. Any exceptions to applying patches should be documented with a rationale for the reason of not applying specific patches and the acceptance of risk that this presents. Further, roles and responsibilities for making the decision to apply patches should be formally documented.

Management Response

DAS will create a formal process for prioritizing patches based upon the potential risk, along with testing requirements to ensure that the patches work without causing system problems or hampering performance. The process will cover critical updates, non-critical updates, and any regularly scheduled maintenance periods. The majority of these discoveries will be through Qualys reports. This step of process will occur after first month of Change request.

Risk*	Remediation Owner	Estimated Completion Date
High	CIO	February 28, 2019

Observation 5 – Inadequate workstation patch testing documentation

DAS Policy ITS-SEC-02 states NIST Special Publication 800-53 is the framework for information security control implementation for the State. NIST 800-53r4 control CM-3 indicates that an organization needs to test, validate and document changes to information systems before implementation.

During our review, we noted that:

- Patches to resolve zero day vulnerabilities are not tested.
- The list of business test users' systems used for workstation testing may be out of date.
- Testers are not informed when patches are being applied.
- A process for testing, including specific application functionality tests, is not formally defined.
- Results of testing are not documented.

If test systems are not appropriately identified, the testing population will not be accurate and patches may not be tested by the appropriate testers. Unless the process for testing and results are documented, the scope and outcome of testing will not be appropriately recorded to reference if a problem occurs.

Recommendation

Management should determine if the current list of business test users is accurate. Further, a periodic review of business test users should be established in order to ensure that the appropriate users are acting as testers. Procedures for testing should describe how the list will be reviewed, how replacement testers will be identified when needed, and how often reviews will occur.

Further, management should define the testing process for workstation patches, including zero day patches, and track the results of testing prior to deployment on an ongoing basis. The standard testing process should describe key baseline tasks that are required for all applications whenever a patch is applied (i.e. applications should be able to be successfully executed and key critical functions should be able to be performed after a patch is installed). In addition, key functionality tasks to test for critical applications should also be defined. Key tasks to perform for testing should be defined when zero day patches need to be applied. The results of testing should be stored in a repository and be available to review on request.

The method and frequency used for communicating to defined testers should be defined. Roles and responsibilities for communication, testing, documentation of results need to be identified and documented.		
Management Response		
DAS will formally document patch testing procedures to include; patch distribution process, receiving notification of patches, assessing and prioritizing patches, and testing and deployment of patches.		
Risk*	**Remediation Owner**	**Estimated Completion Date**
Moderate	CIO	February 28, 2019

Due to the limited nature of our audit, we have not fully assessed the cost-benefit relationship of implementing the observations and recommendations suggested above. However, these observations reflect our continuing desire to assist your department in achieving improvements in internal controls, compliance, and operational efficiencies.

* Refer to Appendix A for classification of audit observations.

Appendix A – Classification of Conclusions and Observations

Classification of Audit Objective Conclusions

Conclusion	Description of Factors
Well-Controlled	The processes are appropriately designed and/or are operating effectively to manage risks. Control issues may exist, but are minor.
Well-Controlled with Improvement Needed	The processes have design or operating effectiveness deficiencies but do not compromise achievement of important control objectives.
Improvement Needed	Weaknesses are present that compromise achievement of one or more control objectives but do not prevent the process from achieving its overall purpose. While important weaknesses exist, their impact is not widespread.
Major Improvement Needed	Weaknesses are present that could potentially compromise achievement of its overall purpose. The impact of weaknesses on management of risks is widespread due to the number or nature of the weaknesses.

Classification of Audit Observations

Rating	Description of Factors	Reporting Level
Low	Observation poses relatively minor exposure to an agency under review. Represents a process improvement opportunity.	Agency Management; State Audit Committee (Not reported)
Moderate	Observation has moderate impact to the agency. Exposure may be significant to unit within an agency, but not to the agency as a whole. Compensating controls may exist but are not operating as designed. Requires near-term agency attention.	Agency Management and State Audit Committee
High	Observation has broad (state or agency wide) impact and possible or existing material exposure requiring immediate agency attention and remediation.	Agency Management and State Audit Committee