The University of Texas Rio Grande Valley™

Patch Management Audit

Report No. 23-AEN-10

May 31, 2023

Office of Audits & Consulting Services

EXECUTIVE SUMMARY

Overall Assessment:

The University has adequate controls over patch management. Policies and procedures are adequate to properly manage software patches, patches are applied timely, and systems tested are patched. However, an opportunity exists to improve patch testing documentation.

Background: Patches are small changes to a system's software designed to fix errors, improve functionality, improve performance, and minimize vulnerabilities. The University uses a diverse group of resources to manage software patches. Software vendors offer available patches, system owners decide which need to be applied, business analysts test them, and technical administrators apply them. Throughout the whole implementation process TeamDynamix, a ticketing system, is used to manage and document individual patches. To protect valuable University information, all changes need to meet TAC 202 requirements.

Objective: Review controls over timely patching of workstations, servers, and other IT infrastructure equipment.

Scope/Period: All current policies and procedures pertaining to patch management. All patches from 9/1/21 to 8/31/22.

Risk Levels
Appendix I

Priority
High
Medium
Low

Risk		Observation Summary
Medium	1.	No explanation for the "No" response provided in testing section of the TeamDynamix questionnaire that is used to document all software changes.
Medium	2.	Documentation provided to support successful testing had screenshots with wrong version and dates.
Medium	3.	Documentation reviewed did not have evidence that changes were accurately deployed into production.

We appreciate the courtesy and cooperation from the Information Technology department.

Observation Detail	Recommendation	Management Action Plan
Explanation for Not Testing 1. ***(Condition)*** We tested 20 software changes applied to different systems. All changes reviewed were documented in TeamDynamix. 16 out of the 20 software changes indicated "No" for the only question that refers to testing, "Is your completed test plan attached and successful?". No explanation for the "No" responses was provided. ***(Criteria)*** Texas Administrative Code §202.74, Subsection (a), "Each institution of higher education shall develop, document, and implement an institution of higher education-wide information security program, approved by the agency head or delegate, that includes protections based on risk for all information and information resources owned, leased, or under the custodianship of any department, operating unit, or employee of the institution of higher education including outsourced resources to another institution of higher education, contractor, or other source. The program shall include policies, controls, standards, and procedures that are based on the risk assessments required and cost-effectively reduce information security risks to a level acceptable to the institution head." ***(Cause)*** TeamDynamix questionnaire does not require explanations when changes are not tested. ***(Effect)*** Unable to verify that the test plan was successful before applying changes to production.	1. The Chief Information Officer should ensure that the testing section in TeamDynamix questionnaire is expanded to include explanations for any "No" responses related to test plans.	1. Change Request form will be modified to have a mandatory text field as to why not tested if "no test plan" is checked and what validation will be done in lieu of testing. Will also modify the work instruction to explain the No Test Plan explanation field. **Action Plan Owner**: Chief Information Officer **Implementation Date:** Service request (#22694918) to make the form changes submitted with design and validation done by June 1, 2023.

Observation Detail	Recommendation	Management Action Plan
Evidence of Testing 2. ***(Condition)*** Two systems were tested to ensure that they were up to date on their patches. One did not have proper testing documentation. Documentation provided had screenshots with wrong version and dates. ***(Criteria)*** Texas Administrative Code §202.74, Subsection (a), "Each institution of higher education shall develop, document, and implement an institution of higher education-wide information security program, approved by the agency head or delegate, that includes protections based on risk for all information and information resources owned, leased, or under the custodianship of any department, operating unit, or employee of the institution of higher education including outsourced resources to another institution of higher education, contractor, or other source. The program shall include policies, controls, standards, and procedures that are based on the risk assessments required and cost-effectively reduce information security risks to a level acceptable to the institution head." ***(Cause)*** Attached incorrect testing documentation. ***(Effect)*** Unable to verify that the test plan was successful before applying changes to production.	2. The Chief Information Officer should ensure that patch management processes include documented evidence of test plan results such as screenshots, system files, etc. for changes that were tested prior to deployment.	2. *Standard Change*: Supervisor is responsible for reviewing and approving the change and supporting documentation. That includes is it up to date. Will reinstruct supervisors of their responsibilities. Will implement a monthly audit by the Change Management Coordinator of change documentation. *Normal Change*: Are reviewed by Change Management Coordinator before going to in the Change Advisory Board that the documentation is correct and up to date. Note: This finding was on a Standard change. **Action Plan Owner**: Chief Information Officer **Implementation Date:** Reinstruct supervisor, June 1, 2023. Monthly Audit starts in May 2023.

Observation Detail	Recommendation	Management Action Plan
Evidence of Implementation 3. ***(Condition)*** Documentation reviewed did not have evidence that changes were accurately deployed into production. ***(Criteria)*** Texas Administrative Code §202.74, Subsection (a), "Each institution of higher education shall develop, document, and implement an institution of higher education-wide information security program, approved by the agency head or delegate, that includes protections based on risk for all information and information resources owned, leased, or under the custodianship of any department, operating unit, or employee of the institution of higher education including outsourced resources to another institution of higher education, contractor, or other source. The program shall include policies, controls, standards, and procedures that are based on the risk assessments required and cost-effectively reduce information security risks to a level acceptable to the institution head." ***(Cause)*** TeamDynamix questionnaire does not require evidence of implementation. ***(Effect)*** Unable to verify that the changes were accurately deployed into production.	3. The Chief Information Officer should ensure that patch management processes include documented evidence such as screenshots, system files, etc. that the changes were accurately deployed into production.	3. Will review the change management documentation and clarify the responsibilities of the person validating the change in production and what documentation is needed to document the results. Will resend Change Management training to all IT employees. **Action Plan Owner**: Chief Information Officer **Implementation Date:** July 1, 2023

APPENDIX I

Risk Classifications and Definitions

Priority	High probability of occurrence that would significantly impact UT System and/or UT Rio Grande Valley. Reported to UT System Audit, Compliance, and Risk Management Committee (ACRMC). Priority findings reported to the ACRMC are defined as "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*"
High	Risks are considered substantially undesirable and pose a significant level of exposure to UT Rio Grande Valley operations. Without appropriate controls, the risk will happen on a consistent basis. Immediate action is required by management in order to address the noted concern and reduce exposure to the organization.
Medium	Risks are considered undesirable and could moderately expose UT Rio Grande Valley. Without appropriate controls, the risk will occur some of the time. Action is needed by management in order to address the noted concern and reduce the risk exposure to a more desirable level.
Low	Low probability of various risk factors occurring. Even with no controls, the exposure to UT Rio Grande Valley will be minimal. Action should be taken by management to address the noted concern and reduce risk exposure to the organization.

APPENDIX II

Criteria & Methodology

Criteria

- Texas Administrative Code (TAC) 202 - Information Security Standards.
- UTRGV's Computer Security Standard

Methodology

We conducted this audit in conformance with the Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing. Additionally, we conducted this audit 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 findings and conclusions based on our audit objectives. The Office of Audits and Consulting Services is independent per both standards for internal auditors. These standards are also required by the Texas Internal Auditing Act.

To achieve our objective, we performed the following:

1. Reviewed policies and procedures related to patch management.
2. Reviewed patch documentation.
3. Reviewed existing systems to ensure they were up to date on their updates and patches.
4. Reviewed Change Advisory Board meeting minutes.

APPENDIX III

Report Distribution & Audit Team

Report Distribution

Dr. Jeff Graham, Chief Information Officer
UTRGV Internal Audit Committee
UT System Audit Office
Governor's Office - Budget and Policy
State Auditor's Office
Legislative Budget Board

Audit Team

Eloy R. Alaniz, Jr., Chief Audit Officer
Norma Ramos, Director of Audits
Isabel Benavides, Assistant Director of Audits
Joe Gomez, Senior Information Technology Auditor