UTHealth
The University of Texas
Health Science Center at Houston

Office of Auditing & Advisory Services

21-208 Coupa Integrated

EXECUTIVE SUMMARY

We have completed our audit of the Coupa Procure-to-Pay (Coupa) application. This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing.*

Background

Coupa was implemented in May 2021 and provides UTHealth with a comprehensive platform to manage the end-to-end procurement process. It includes functionality for searching online catalogs, creating requisitions, issuing purchase orders, and approving invoices for payment. The application also interfaces with PeopleSoft to verify budget information and facilitate financial reporting.

Audit Objectives

Our objective was to determine whether controls around Coupa are adequate and functioning as intended. Specifically, we wanted to determine if:

- Agreements with the vendor have been properly executed.
- Findings from security reviews have been adequately addressed.
- Security controls are adequate and functioning as intended.
- Financial/operational controls are adequate and functioning as intended.

Scope

- Transactions in Coupa between May 1, 2021 and July 31, 2021
- Users access list from Coupa as of August 12, 2021
- Configuration set-up between PeopleSoft and Coupa as of August 13, 2021
- UTHealth current employees list from PeopleSoft HCM as of August 16, 2021
- UTHealth terminated employees from PeopleSoft HCM between January 1, 2019 and August 16, 2021
- Outstanding credits as of August 17, 2021
- Requisitions approval chain as of September 1, 2021

Conclusion

Overall, controls around Coupa are adequate and functioning as intended. We noted the following opportunities for improvement:

#	Audit Observation Summary	Risk	Risk Rating
1	Application event logs are not actively monitored and reviewed for security incidents.	Failure to monitor application event logs could result in security	**Medium**

		incidents going undetected.	
2	External (i.e., non-UTHealth) users can access the Coupa web application without appropriate authentication controls.	Failure to implement authentication controls could lead to inappropriate access.	**Medium**
3	Users with inappropriate levels of access were noted and quarterly access reviews are not being conducted.	Failure to conduct periodic user access reviews could result in inappropriate access.	**Medium**
4	Coupa has not been configured to require approval from authorized individuals for IT related purchases and policies and procedures have not been updated to reflect changes in school IT approvers.	Failure to obtain approval from authorized individuals could result in inappropriate purchases.	**Medium**

AUDIT OBSERVATIONS & MANAGEMENT RESPONSES

#1 Application Event Log Monitoring

Cause

A process for monitoring application event logs has not been developed and implemented.

Risk

Failure to monitor application event logs could result in security incidents going undetected.

Condition

Management informed us application event logs for Coupa are not actively monitored and only reviewed in cases of a known issue.

Criteria

ITPOL-026 Application Logging and Monitoring Policy requires all mission critical applications and all applications that contain confidential information to generate event logs. The application event logs should be reviewed periodically and monitored for security incidents.

Coupa has been designated a critical application per the application/services inventory.

Recommendation

We recommend Supply Chain management develop and implement a process to periodically review and monitor application event logs for security incidents.

Rating

Medium

UT System Priority Findings Matrix Mapping (see Appendix A)

Information Security: Low probability of data breach

Management Response

Supply Chain will approach Coupa and IT Security to determine if any existing Coupa reports identify and document suspicious activity in an event log. Based on the information gathered, Supply Chain will develop and implement a process to periodically review and monitor the event logs.

Responsible Party

Eric Williams, Assistant Vice President, Supply Chain Management

Implementation Date

February 1, 2022

#2 User Authentication

Cause

System access was granted to external (i.e., non-UTHealth) users without requiring appropriate authentication controls.

Risk

Failure to implement authentication controls could lead to inappropriate access.

Condition

We obtained the user access listing as of August 12, 2021 and noted 14 users who can access the Coupa web application without being subject to authentication controls (e.g., two-factor authentication).

Criteria

HOOP 175 Roles and Responsibility for University Information Resources and University Data outlines various responsibilities for a system owner such as:

- Implement required security controls and procedures.
- Ensure that the system is in compliance with applicable federal, state, and local laws and regulations, UT System policies, and university policies, procedures and guidance.
- Determine appropriate access for system users based on the minimum necessary access required to perform their assigned job responsibilities. Approve new access assignments and review all assigned access for appropriateness on a regular basis.

IT Security performed an initial vendor security risk assessment of Coupa on November 9, 2019 and recommended Coupa be integrated with UTHealth's Security Assertion Markup Language (SAML) to grant staff federated access to the web application.

Recommendation

We recommend all Coupa web application users be subject to authentication controls.

Rating

Medium

UT System Priority Findings Matrix Mapping (see Appendix A)

Information Security: Low probability of data breach

Management Response

This has been resolved since SAML access is required for access to Coupa. For any new non-employees that are added to Coupa, we require a DMO or department manager's approval and set them up with Single Sign On instead of Coupa Credentials. If an employee leaves, their status will change from active to inactive in Coupa via a feed from HCM (addressed in Observation #3).

Responsible Party

Eric Williams, Assistant Vice President, Supply Chain Management

Implementation Date

Implemented as of October 25, 2021 (to be verified by A&AS)

#3 User Access

Cause

A quarterly access review has not been conducted while awaiting IT Security's approval of the exception to policy request.

Risk

Failure to conduct periodic user access reviews could result in inappropriate access.

Condition

We requested a list of active users in Coupa as of August 12, 2021 and noted a total of 2,473 users. At the time of our review, the following issues were noted:

- 99 user accounts belonged to terminated employees - network access was disabled; however, access was not disabled within the Coupa application.
- Of the 18 user accounts assigned to one or more administrator roles, 4 (22%) were determined to be inappropriate and subsequently deactivated.
- One user role was a duplicate of another user role.

Coupa was implemented on May 1, 2021 and an exception request (for an annual review instead of quarterly) was submitted to IT Security on May 17, 2021, which was still outstanding as of September 1, 2021. In the meantime, a quarterly access review has not been conducted.

Criteria

ITPOL-004 Access Control Policy, Section 6.2.6 states: "Owners or their designees must review access at least quarterly to ensure access privileges, including administrative and special access accounts, are appropriate. A user's access authorization shall be appropriately modified or remove when the user's employment or job responsibilities within the agency change."

ITGD-008 Administrative Privilege Appropriate User Guidelines, Section 5.4 requires system owners to review all assigned administrative access for appropriateness on a regular basis.

The Coupa Administrator team is responsible for ensuring periodic user access reviews are conducted. Reviews are conducted by confirming the appropriateness of assigned roles with department managers and responses are retained as evidence of the reviews.

Recommendation

We recommend Supply Chain management work with IT Security to resolve the outstanding exception request. In the interim, we recommend our outstanding exceptions be addressed and user access reviews be performed quarterly as required by ITPOL-004.

Rating

Medium

UT System Priority Findings Matrix Mapping (see Appendix A)

Information Security: Low probability of data breach

Management Response

Supply Chain will complete the exception request with IT Security – which will differentiate those roles requiring quarterly vs. annual reviews.

Regarding the 99 users referenced above, we believe there was an issue with a feed from HCM that did not deactivate some terminated employees in Coupa. We have since manually inactivated these users. We now receive a weekly report of terminated employees and review these users to ensure they are inactive in Coupa.

Responsible Party
Eric Williams, Assistant Vice President, Supply Chain Management

Implementation Date
January 1, 2022

#4 Requisition Approvers

Cause

Coupa has not been configured to require approval from authorized individuals for IT related purchases and policies and procedures have not been updated to reflect changes in school IT approvers.

Risk

Failure to obtain approval from authorized individuals could result in inappropriate purchases.

Condition

We selected a sample of 25 requisitions, verified approval was obtained from authorized individuals, and noted the following issues:

- In three cases, the SOD IT approver did not approve the requisition. Management informed us Coupa was not configured to require approval from the SOD IT approver designated in ITPOL-022 *Procuring Information Technology* (ITPOL-022).
- In one case, the SPH IT approver designated in ITPOL-022 was no longer employed by UTHealth at the time the requisition was submitted. Management informed us a new SPH IT Approver was appointed (and did ultimately approve the requisition); however, ITPOL-022 was not updated to reflect the new SPH IT approver.

Criteria

ITPOL-022 requires all procurement of information technology (including medical and scientific devices that store data) and information technology services in excess of $25,000 to be reviewed and approved by both the school IT approver and the Vice President and Chief Information Officer (CIO). The applicable school IT approver is specifically identified in ITPOL-022.

Recommendation

We recommend:

- IT management update ITPOL-022 to reflect changes in school IT approvers and communicate the changes to Supply Chain management.
- Supply Chain management configure the changes in Coupa.

Rating

Medium

UT System Priority Findings Matrix Mapping (see Appendix A)

Effectiveness and Efficiency: Low probability of a mission critical activity failing with major regulatory, reporting consequences.

Management Response

Supply Chain will obtain the IT approval workflows (by business unit) from Coupa and forward them to IT for review. Changes will be incorporated into ITPOL-022 and configured in Coupa.

Responsible Party

Eric Williams, Assistant Vice President, Supply Chain Management
Amar Yousif, Vice President and Chief Information Officer

Implementation Date

February 1, 2022

We would like to thank Supply Chain, IT, and IT Security staff and management who assisted us during our review.

Daniel G. Sherman, MBA, CPA, CIA
Associate Vice President & Chief Audit Officer

NUMBER OF PRIORITY FINDINGS REPORTED TO UT SYSTEM

None

MAPPING TO AUDITING & ADVISORY SERVICES FY 2022 RISK ASSESSMENT

Reference	Risk	Risk Rating
FIN 5	Tasks/Assignments may not be routed to the correct area in the Coupa System.	Low
FIN 6	Records may be removed in Coupa when rejected in the system.	Medium
FIN 7	There may not be sufficient audit trails in Coupa to retrieve pertinent information.	Medium
FIN 8	Coupa training may not align with function or duties.	Medium
FIN 25	Encumbrances may not be released/budget checks may not occur in Coupa.	Low
FIN 125	Coupa does not meet user expectations.	Medium
FIN 134	Travel expenditure module of Coupa is not implemented timely or effectively.	Medium

DATA ANALYTICS UTILIZED

Using Microsoft Excel, calculated and compared requisition approval cycle time, invoice approval cycle time, and payment cycle time to measure against Procurement's 6-month KPI metrics and averages.

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

AVP/CAO – Daniel G. Sherman, MBA, CPA, CIA
Audit Manager – Brook Syers, CPA, CIA, CISA, CFE
Auditor Assigned – Kathy Tran, CIA, CISA, CFE, CGAP

END OF FIELDWORK DATE

October 7, 2021

ISSUE DATE

October 28, 2021

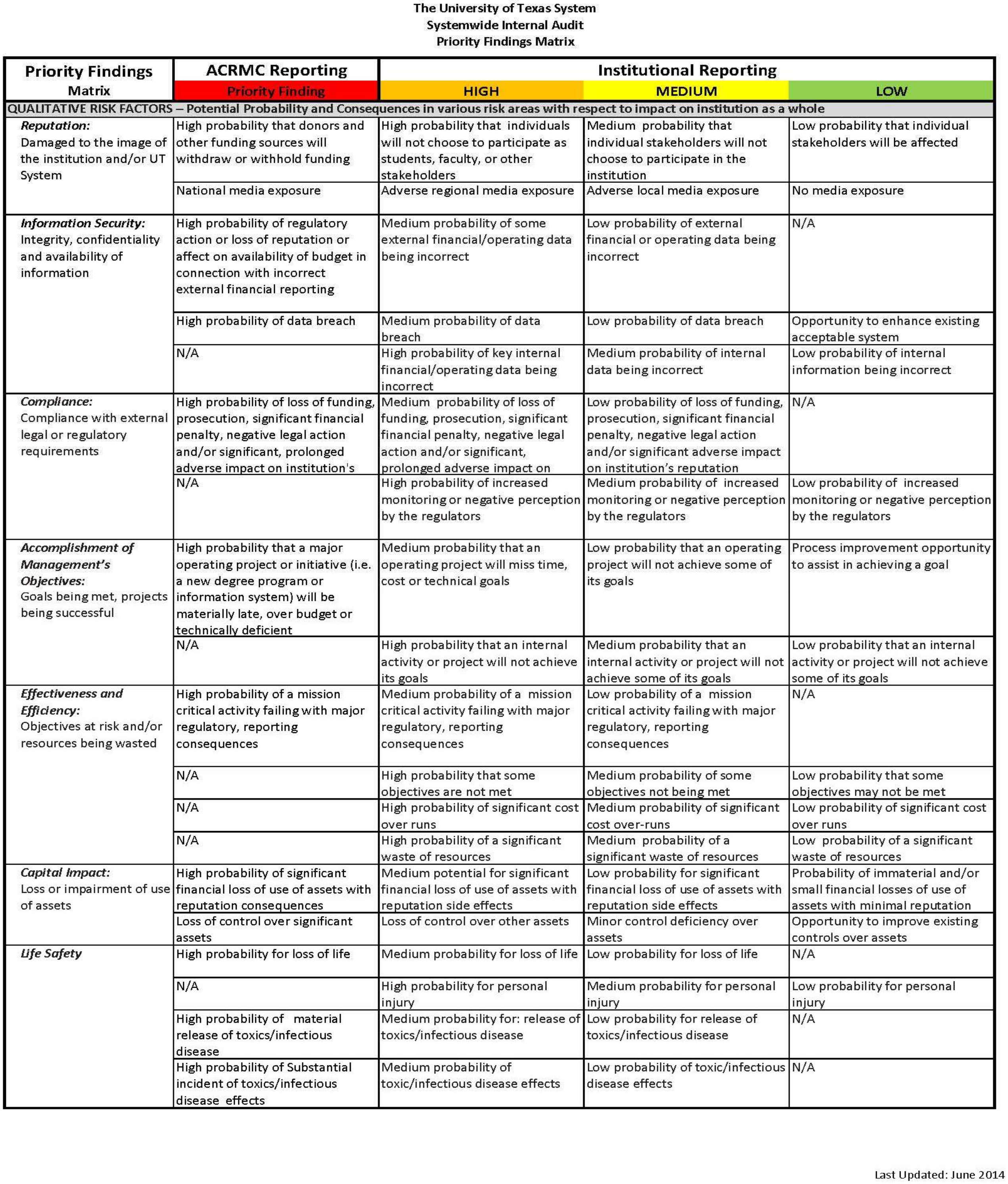
REPORT DISTRIBUTION

Audit Committee
Kevin Dillon

21-208 Coupa Integrated

Beverly Moore
Ana Touchstone
Michael Tramonte
Eric Williams
Amar Yousif

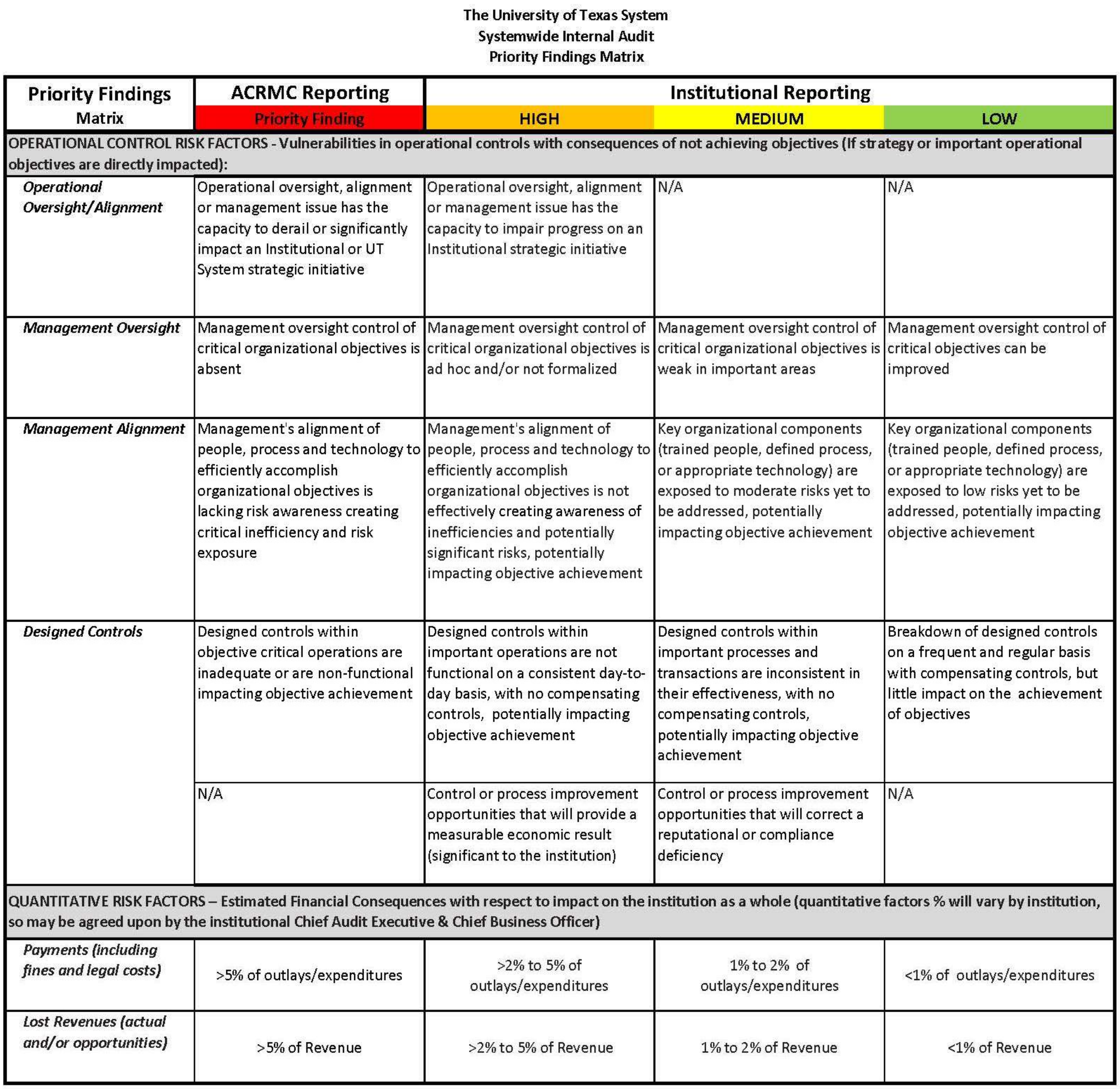
APPENDIX A
UT SYSTEM PRIORITY FINDINGS MATRIX



The University of Texas System
Systemwide Internal Audit
Priority Findings Matrix

Priority Findings	ACRMC Reporting	Institutional Reporting		
Matrix	Priority Finding	HIGH	MEDIUM	LOW
QUALITATIVE RISK FACTORS – Potential Probability and Consequences in various risk areas with respect to impact on institution as a whole				
Reputation: Damaged to the image of the institution and/or UT System	High probability that donors and other funding sources will withdraw or withhold funding	High probability that individuals will not choose to participate as students, faculty, or other stakeholders	Medium probability that individual stakeholders will not choose to participate in the institution	Low probability that individual stakeholders will be affected
	National media exposure	Adverse regional media exposure	Adverse local media exposure	No media exposure
Information Security: Integrity, confidentiality and availability of information	High probability of regulatory action or loss of reputation or affect on availability of budget in connection with incorrect external financial reporting	Medium probability of some external financial/operating data being incorrect	Low probability of external financial or operating data being incorrect	N/A
	High probability of data breach	Medium probability of data breach	Low probability of data breach	Opportunity to enhance existing acceptable system
	N/A	High probability of key internal financial/operating data being incorrect	Medium probability of internal data being incorrect	Low probability of internal information being incorrect
Compliance: Compliance with external legal or regulatory requirements	High probability of loss of funding, prosecution, significant financial penalty, negative legal action and/or significant, prolonged adverse impact on institution's	Medium probability of loss of funding, prosecution, significant financial penalty, negative legal action and/or significant, prolonged adverse impact on	Low probability of loss of funding, prosecution, significant financial penalty, negative legal action and/or significant adverse impact on institution's reputation	N/A
	N/A	High probability of increased monitoring or negative perception by the regulators	Medium probability of increased monitoring or negative perception by the regulators	Low probability of increased monitoring or negative perception by the regulators
Accomplishment of Management's Objectives: Goals being met, projects being successful	High probability that a major operating project or initiative (i.e. a new degree program or information system) will be materially late, over budget or technically deficient	Medium probability that an operating project will miss time, cost or technical goals	Low probability that an operating project will not achieve some of its goals	Process improvement opportunity to assist in achieving a goal
	N/A	High probability that an internal activity or project will not achieve its goals	Medium probability that an internal activity or project will not achieve some of its goals	Low probability that an internal activity or project will not achieve some of its goals
Effectiveness and Efficiency: Objectives at risk and/or resources being wasted	High probability of a mission critical activity failing with major regulatory, reporting consequences	Medium probability of a mission critical activity failing with major regulatory, reporting consequences	Low probability of a mission critical activity failing with major regulatory, reporting consequences	N/A
	N/A	High probability that some objectives are not met	Medium probability of some objectives not being met	Low probability that some objectives may not be met
	N/A	High probability of significant cost over runs	Medium probability of significant cost over-runs	Low probability of significant cost over runs
	N/A	High probability of a significant waste of resources	Medium probability of a significant waste of resources	Low probability of a significant waste of resources
Capital Impact: Loss or impairment of use of assets	High probability of significant financial loss of use of assets with reputation consequences	Medium potential for significant financial loss of use of assets with reputation side effects	Low probability for significant financial loss of use of assets with reputation side effects	Probability of immaterial and/or small financial losses of use of assets with minimal reputation
	Loss of control over significant assets	Loss of control over other assets	Minor control deficiency over assets	Opportunity to improve existing controls over assets
Life Safety	High probability for loss of life	Medium probability for loss of life	Low probability for loss of life	N/A
	N/A	High probability for personal injury	Medium probability for personal injury	Low probability for personal injury
	High probability of material release of toxics/infectious disease	Medium probability for: release of toxics/infectious disease	Low probability for release of toxics/infectious disease	N/A
	High probability of Substantial incident of toxics/infectious disease effects	Medium probability of toxic/infectious disease effects	Low probability of toxic/infectious disease effects	N/A

Last Updated: June 2014



The University of Texas System
Systemwide Internal Audit
Priority Findings Matrix

Priority Findings Matrix	ACRMC Reporting	Institutional Reporting		
	Priority Finding	HIGH	MEDIUM	LOW
OPERATIONAL CONTROL RISK FACTORS - Vulnerabilities in operational controls with consequences of not achieving objectives (If strategy or important operational objectives are directly impacted):				
Operational Oversight/Alignment	Operational oversight, alignment or management issue has the capacity to derail or significantly impact an Institutional or UT System strategic initiative	Operational oversight, alignment or management issue has the capacity to impair progress on an Institutional strategic initiative	N/A	N/A
Management Oversight	Management oversight control of critical organizational objectives is absent	Management oversight control of critical organizational objectives is ad hoc and/or not formalized	Management oversight control of critical organizational objectives is weak in important areas	Management oversight control of critical objectives can be improved
Management Alignment	Management's alignment of people, process and technology to efficiently accomplish organizational objectives is lacking risk awareness creating critical inefficiency and risk exposure	Management's alignment of people, process and technology to efficiently accomplish organizational objectives is not effectively creating awareness of inefficiencies and potentially significant risks, potentially impacting objective achievement	Key organizational components (trained people, defined process, or appropriate technology) are exposed to moderate risks yet to be addressed, potentially impacting objective achievement	Key organizational components (trained people, defined process, or appropriate technology) are exposed to low risks yet to be addressed, potentially impacting objective achievement
Designed Controls	Designed controls within objective critical operations are inadequate or are non-functional impacting objective achievement	Designed controls within important operations are not functional on a consistent day-to-day basis, with no compensating controls, potentially impacting objective achievement	Designed controls within important processes and transactions are inconsistent in their effectiveness, with no compensating controls, potentially impacting objective achievement	Breakdown of designed controls on a frequent and regular basis with compensating controls, but little impact on the achievement of objectives
	N/A	Control or process improvement opportunities that will provide a measurable economic result (significant to the institution)	Control or process improvement opportunities that will correct a reputational or compliance deficiency	N/A
QUANTITATIVE RISK FACTORS – Estimated Financial Consequences with respect to impact on the institution as a whole (quantitative factors % will vary by institution, so may be agreed upon by the institutional Chief Audit Executive & Chief Business Officer)				
Payments (including fines and legal costs)	>5% of outlays/expenditures	>2% to 5% of outlays/expenditures	1% to 2% of outlays/expenditures	<1% of outlays/expenditures
Lost Revenues (actual and/or opportunities)	>5% of Revenue	>2% to 5% of Revenue	1% to 2% of Revenue	<1% of Revenue

Last Updated: June 2014