UTSA The University of Texas at San Antonio™
OFFICE OF INSTITUTIONAL
COMPLIANCE AND RISK SERVICES

Date: FY XX-XX

To: Department Manager Name, Title

From: Leticia Vega, Compliance Management Analyst, Office of Institutional Compliance and Risk Services

CC: Department Manager's immediate supervisor

Subject: Quality Assurance Review

Attached is the final report from the Quality Assurance Review (QAR) we recently completed in your area. We appreciate your time and effort during the review.

QARs are conducted under the authority of UT System policy – UTS 142, UTSA Financial Guidelines and provide assurance to Financial Affairs in the Fiscal Management Sub-Certification process. The review of the controls and processes in this department is not an audit and does not substitute for an audit. The purpose of this review is to provide, in a consultative manner, an objective evaluation of internal controls in your area, which are essential in the prevention of potential fraud.

Although it is not possible to determine with certainty whether fraud will occur, based on the information available at the time of the review, the Office of Institutional Compliance and Risk Services has assessed your department as having a **low** risk.

If you have any questions, please contact me at leticia.vega@utsa.edu.

SAMPLE

Department/Area	Overall Risk Level
Department Name	**G**

SUMMARY OF FINDINGS

At the time of the QAR, the department should be commended as it was meeting or exceeding the minimum expectations toward achieving an overall **LOW** risk. Proper segregation of duties, managerial review and oversight contribute to the department establishing effective internal controls to mitigate the risk of fraud.

The following is an assessment of risk for each major area reviewed as part of the QAR, any issues of concern, including associated **RECOMMENDATIONS** (if applicable), which can serve to further strengthen and/or maintain effective internal controls.

Level of risk assigned

R	Significant departure from university policy, procedures and/or best practices
Y	Moderate departure from university policy, procedures and/or best practices
G	Low, compliant with or non-significant departure from university policy, procedures and/or best practices

RISK LEVEL ASSESSMENT, ISSUES OF CONCERN AND RECOMMENDATIONS

Fiscal Management – Monthly Reconciliation	**Risk Level**	**G**
No findings noted		

Fiscal Management – Purchasing (One Card and Travel)	**Risk Level**	**G**
No findings noted		

Fiscal Management – Cash Handling	**Risk Level**	**Y**
Approval to Accept Payments – At the time of our review The Departmental Cash Handling Request Form and Departmental Cash Handling Security Policy had not been updated and delivered to the Financial Services and University Bursar Office. **Recommendation:** If the Department Manager or any authorized cash handlers change, updates must be promptly submitted to the Office of Financial Services and University Bursar. Changes to authorized cash handlers may be submitted via e-mail, but changes to the Department Manager must be evidenced by resubmission of the Department Cash Handling Request and Departmental Cash Handling Security Policy forms.		

Fiscal Management – Gifts	**Risk Level**	**N/A**
No findings noted		

Capital Asset Management	**Risk Level**	**G**
No findings noted		

Information Security	**Risk Level**	**G**
No findings noted		

Information Security
As a reminder, ensure sensitive information is handled according to established guidelines allowing access only to those employees who need the information to perform their job responsibilities. In addition, identify those within your office or department who might use confidential information and be sure they have been trained in the rules regarding privacy/FERPA. Training available https://www.utsa.edu/enrollment/sissecurity/access/ferpa-compliance.html

Ensure all users of UTSA information resources in your area are aware of and comply with the requirements of the UTSA Standard for Passphrase and Password which include selecting a strong passphrase, never disclosing, writing down, or sharing account passphrases and enabling a passphrase protected locked screen (or logging off) when computing devices are left unattended.

- Be sure that backup files and computers with confidential information are not available to those who are not approved to handle such records.
- Do not transmit personally identifiable information (PII) via e-mail or through other electronic means not approved.
- Category 1 data should only be stored on the department shared (I: Drive) or on a secured server.

Hiring process
As a reminder, for hiring process, there should not be any documents kept that have social security numbers. Please see the Record Retention Checklist that shows what departments keep and what Office of People Excellence keeps.

As far as what documents the departments are allowed to keep outside of the recruitment process, this would depend on the purpose of the document. When in doubt is recommended to contact the Records Retention (https://www.utsa.edu/openrecords/retention.html) or the Office of People Excellence depending on the type of document.

People Excellence	Risk Level	R
Conflict of Interest disclosure - At the time of our review not all employees had completed the annual Conflict of Interest disclosure. **Recommendation:** Department Managers should ensure all employees have completed required annual Conflict of Interest disclosure, and request prior approval for outside activities in accordance with HOP 1.33. This disclosure is mandatory for all UTSA employees and can be completed utilizing the UTSA Conflict of Interest Portal.		