

Best Business Practices

To support your department in strengthening internal controls, improving operational efficiency, and ensuring compliance with university policies and regulations, we've compiled a list of best practices for your consideration:

1. Establish Strong Internal Controls

- **Segregation of Duties:** Ensure that key financial and operational duties (e.g., approving transactions, recording transactions, and handling cash) are assigned to different individuals to reduce the risk of fraud or errors.
- **Access Controls:** Implement role-based access to sensitive data and systems, ensuring that only authorized personnel have access to certain information or functions.
- **Reconciliation Procedures:** Regularly reconcile financial and operational records to detect discrepancies and correct them in a timely manner.

2. Maintain Accurate Documentation and Records

- **Document Retention:** Follow university guidelines for document retention, ensuring important records (e.g., contracts, financial transactions, and correspondence) are kept for the required period.
- **Record Keeping Consistency:** Ensure that all records are consistently organized, easily accessible, and accurately reflect activities, transactions, and decisions.
- **Electronic Records:** Use secure electronic systems to store records and ensure backup and disaster recovery processes are in place.

3. Conduct Regular Risk Assessments

- **Risk Identification:** Regularly assess the risks facing your department, including financial, operational, compliance, and reputational risks.
- **Risk Mitigation Plans:** For high-risk areas, develop and implement risk mitigation strategies, including preventive measures and contingency plans.
- **Continuous Monitoring:** Continuously monitor key risk indicators and internal controls to ensure that risks are managed effectively.

4. Foster a Culture of Ethical Conduct

- **Code of Ethics:** Ensure that all staff are aware of and adhere to the university's code of ethics and integrity.
- **Conflict of Interest:** Require disclosure of potential conflicts of interest and implement processes to address them appropriately.
- **Whistleblower Protections:** Encourage employees to report unethical behavior or concerns without fear of retaliation, and ensure that there are clear reporting channels.

5. Ensure Compliance with Policies and Regulations

- **Policy Adherence:** Ensure that all department activities comply with university policies, state and federal regulations, and any applicable industry standards (e.g., FERPA, Title IX, HIPAA).

- **Training and Awareness:** Provide regular training for department staff on compliance requirements, university policies, and best practices for ethical conduct.
- **Regulatory Changes:** Stay informed about changes in laws and regulations that may impact the department, and adjust policies and procedures accordingly.

6. Implement Effective Financial Management Practices

- **Budget Oversight:** Ensure that departmental budgets are reviewed and approved regularly, and that spending aligns with budgeted allocations.
- **Expense Approvals:** Establish clear processes for reviewing and approving expenses, ensuring that they are legitimate, necessary, and in compliance with university policies.
- **Grant Compliance:** For departments managing grants, ensure compliance with specific grant requirements, including proper allocation of funds, reporting, and documentation.

7. Promote Transparency and Accountability

- **Clear Reporting:** Ensure that all financial and operational reports are accurate, clear, and transparent to university leadership and stakeholders.
- **Audit Trails:** Maintain clear, traceable records of decisions and transactions, ensuring that all actions can be easily reviewed and audited.
- **Response to Audit Findings:** Act promptly and transparently to address audit findings or concerns, and implement corrective actions where necessary.

8. Engage in Continuous Process Improvement

- **Process Evaluation:** Regularly evaluate department processes for efficiency and effectiveness. Look for areas of improvement to reduce waste and improve performance.
- **Feedback Mechanism:** Implement a system for collecting feedback from staff and stakeholders on processes, and use it to inform improvements.
- **Advisory Support:** Work with the internal audit department for advice on best practices for process improvements or new initiatives.

9. Leverage Technology for Efficiency and Security

- **Automated Systems:** Use technology to automate repetitive tasks (e.g., invoicing, procurement) to reduce human error and improve efficiency.
- **Cybersecurity Best Practices:** Ensure the protection of sensitive data by implementing strong cybersecurity measures, including encryption, multi-factor authentication, and regular security audits.
- **Data Integrity:** Regularly review data management systems to ensure the accuracy, integrity, and security of information being used for decision-making.

10. Create an Audit-Ready Environment

- **Prepare for Audits:** Regularly review key documentation and processes to ensure that the department is audit-ready at any time. Ensure records are up-to-date and that audit trails are complete and accessible.
- **Audit Cooperation:** Work collaboratively with internal and external auditors during the audit process, providing requested documentation and answering questions in a timely and accurate manner.
- **Audit Action Plans:** After an audit, take ownership of findings and develop clear action plans with timelines to address any identified weaknesses or recommendations.

11. Develop a Strong Vendor Management Program

- **Vendor Selection and Evaluation:** Ensure that vendor contracts and agreements are carefully evaluated for compliance with university policies, cost-effectiveness, and quality of service.
- **Monitoring Performance:** Regularly assess vendor performance and compliance with contractual terms, including service level agreements (SLAs).
- **Conflict of Interest:** Ensure that all vendor relationships are reviewed for potential conflicts of interest and that appropriate disclosures are made.

12. Plan for Business Continuity

- **Contingency Planning:** Develop and maintain business continuity and disaster recovery plans to ensure that departmental operations can continue in the event of an emergency (e.g., natural disaster, cybersecurity incident).
- **Crisis Communication:** Ensure clear communication strategies are in place for handling crises, keeping staff, stakeholders, and the public informed as necessary.

13. Foster Collaboration with Internal Audit

- **Engage Early:** Collaborate with the internal audit department during the planning and development of new projects or initiatives, especially when there may be a need for advisory support on controls or risk mitigation.
- **Ongoing Communication:** Keep an open line of communication with the internal audit team to address emerging risks, challenges, or areas where audits might be beneficial.

14. Performance Metrics and Accountability

- **Set Clear Goals:** Establish measurable objectives for department operations and regularly assess performance against these goals.
- **Key Performance Indicators (KPIs):** Develop KPIs to monitor the success of programs, ensuring that goals are being met, and resources are being used efficiently.
- **Continuous Improvement:** Regularly review departmental performance and adjust goals, processes, and practices as needed to align with strategic objectives and improve outcomes.