Common Audit Findings: Quick Reference

For additional guidance on audit projects and how to prepare for an audit, refer to the Internal Audit FAQs.

1

Duties that are not properly segregated

Strong internal controls require the segregation of three main responsibilities: authorizing transactions, maintaining custody of assets (like equipment, cash, and p-cards), and making accounting entries or recording transactions. For example: one individual should not have the ability to order, receive, and approve payment for goods or services.

2

Lack of written procedures

The lack of complete written procedures increases the risk of disruption to operations, loss of funds, theft, and that current and new employees do not become properly trained. Procedures should include sufficient information to permit an individual who is unfamiliar with the function to quickly learn the relevant tasks for that job role.

3

Missing supporting documentation

All transactions should be supported by adequate documentation. Documentation should include proper authorization and enough detail to provide a trail for a future reviewer to follow.

4

Missing reconciliations and oversight

A reconciliation process is essentially a close-out review process whereby a manager or person outside of the normal line of business reviews the activities that occurred within a period (often the preceding month) to identify abnormalities or errors, and ensure the related documentation is accurate and complete.

5

Non-compliance with policies and procedures

All employees should be familiar with policies and procedures and should strive to conduct ATP business in accordance with them. When employees do not know what our policies are or do not comply with established policies, there is greater risk that we do not operate as intended and we do not achieve our objectives.

6

Not documenting approvals

Most people have a hard time identifying errors in their own work and successful organizations create cultures where the accuracy of work is paramount. Transactions that have an impact to operations should be approved by a second reviewer. Workgroups should maintain evidence of these approvals to document a second review and approval occurred.

7

Not properly safeguarding resources

It is critical to recognize that all ATP does, and all ATP owns, is in service to the public and that our assets (which includes our employees and employee's work time) is a public commodity paid for using taxpayer money. Therefore, all employees are responsible for securing ATP resources.

8

Inappropriate Information Security Access

Critical or sensitive information should be appropriately restricted based on job duties. Examples of sensitive information are personally identifiable information (PII) and confidential or proprietary information. A good way to protect ATP information is to only log on to secure networks, to lock your computer when you leave your workstation, and to shred documents containing PII or other confidential information.

If you think you've witnessed misconduct or unethical behavior relating to ATP, please report it at https://atp.ipm.starcompliance.com/ or by calling the ethics hotline at 888-57-ATPTX (28789).