

2016 Fraud Risk Survey

A. Introduction

Like any company, MTS Systems Corporation (MTS) may be a target for fraudulent acts perpetrated through both internal and external sources. In recent years, unethical and fraudulent activities have been identified resulting in disciplinary action up to and including employee terminations. Regulations require MTS to take reasonable steps to prevent fraudulent activity that could harm our employees, customers, suppliers, or shareholders.

This Fraud Risk Assessment Survey is one of many tools MTS uses to help reduce the potential for fraud. It is a reminder that you play a lead role in fraud prevention. This survey asks you to think about fraud risks in your business function and to independently assess if controls exist to reasonably protect MTS from those risks.

This survey should be answered based on your area and level of expertise. For example, Directors and Managers should answer from a management level perspective, and other MTS professionals should answer from their functional level perspective.

Please complete this survey by Friday, August 5, 2016. If you have any questions, please contact Internal Assurance at internal.assurance@mts.com

Please check your business function:

- Americas – Accounting and Finance
- Europe – Accounting and Finance
- Asia – Accounting and Finance
- Operations
- Legal
- Information Technology
- Service
- Sales and Marketing
- Engineering
- Logistics
- Other (please specify)

What is Fraud?

Wrongful or criminal deception intended to result in financial or personal gain.

The five major types of occupational fraud are:

- a. **Asset Misappropriation** – The taking or use of goods, services, money, or benefits by any person, either internal or external to the victim organization, without due payment.
- b. **Third-Party Fraud** – Any fraud committed solely by a third party or committed by a third party in collusion with another party who may be internal or external to the victim organization.
- c. **Conflicts of Interest** – Situations where employee decisions and actions are influenced by personal interests.
- d. **Information Security and Cyber Fraud** – Any fraud involving the misappropriation of information, systems access, or the unauthorized use or manipulation of information networks for personal gain or financial – or other – loss of the victim organization.
- e. **Corruption and Bribery** – The use or offer of the use of money or power to influence another party's actions to perform unauthorized tasks in some unauthorized manner to benefit personal or organizational interests.

What is NOT Fraud? (examples)

- a. An error in the calculation of inventory reserve or payroll accrual.
- b. Not reviewing account reconciliations in a timely manner.

Please complete the Survey to receive full credit for completion of the course.