

# Internal Controls, Segregation of Duties and Fraud

Prepared by:  
Karen McMurray, CPA, CFE, CICA, CGMA  
*Blackburn, Childers & Steagall, PLC*

**LORMAN**<sup>®</sup>

Published on [www.lorman.com](http://www.lorman.com) - October 2020

Internal Controls, Segregation of Duties and Fraud, ©2020 Lorman Education Services. All Rights Reserved.





Lorman Education Services is a leading provider of online professional learning, serving individuals and teams seeking training and CE credits. Whether you're looking for professional continuing education or an enterprise-wide learning and development solution, you will find what you need in Lorman's growing library of resources.

Lorman helps professionals meet their needs with more than 100 live training sessions each month and a growing collection of over 13,000 ondemand courses and resources developed by noted industry experts and professionals.

Learn more about Lorman's individual programs, economical All-Access Pass, and Enterprise Packages:

[www.lorman.com](http://www.lorman.com)

# **Internal Controls, Segregation of Duties and Fraud**

*Written by Karen McMurray, CPA, CFE, CICA, CGMA-Partner in the firm of Blackburn, Childers and Steagall, PLC with offices in Johnson City, Kingsport and Greeneville, Tennessee and in Boone, North Carolina.*

There is a link between good internal controls and the prevention of fraud. It will not prevent all fraud from occurring, but will serve to deter fraud and will likely lessen the loss and the length of the fraud.

## **2018 Report to the Nations**

According to the Association of Certified Fraud Examiners' 2018 Report to the Nations, internal control weaknesses were directly responsible for half the fraud cases. Of the 2,700 fraud cases studied, the organizations typically believed they had controls in place.

Almost 80% of the companies had a dedicated fraud department and a code of conduct. Over 70% thought their controls included management review and management certifications. However, often controls were not actually present, or were not operating effectively, and thus did not timely identify and correct fraud.

We all think it will not happen to us. But that attitude actually makes you more at risk of becoming a fraud victim.

The one leg of the fraud triangle we can impact is Opportunity. Don't set people up for failure by making it easy to commit fraud.

The primary control weaknesses that contribute to fraud include: Absence of internal controls 30%; overriding existing controls and lack of management review contributed to about 20% each; poor tone at the top and incompetent personnel in oversight roles about 10% each; other areas included: lack of independent audits, minimal employee fraud education, and lack of a formal reporting mechanism.

Fraud is an intentional deception. It usually implies deceit or bad faith. Typically fraud can be lumped into three categories: asset misappropriation, intentional financial statement misstatement, and corruption. Asset misappropriation was the largest type of fraud by far, according to the 2018 Report, accounting for nearly 89% of the cases studied. This is also the area most affected by small organizations/businesses.

Intentional Financial Statement fraud may be hard to prove-it is hard to know "intent".

Corruption (such as conflicts of interest, bribes, extortion) is present about 38% of the fraud cases with a median loss of \$250,000.

How is fraud caught?-Tips do make up 40% of the detections of fraud cases and internal audit makes up 15% and Management reviews make up 13%. An external audit is not the most effective way to detect fraud. Employees account for over half

of the tips. The number of cases detected by tips increased to 46% for organizations with hotlines, versus the 30% tip detection rate for organizations without hotlines. Frauds that are not detected internally tend to be much more costly. Hotline reporting can be through a variety of methods: phone, email, web-based form, mailed letter, or fax.

Small businesses with employees less than 100 lost about twice as much per scheme to fraud, with a median loss per case of \$200,000, largely due to the lack of functioning internal controls. Collusion greatly increases the median loss amount. The median loss for a sole person committing the fraud was approximately \$74,000, while the median doubled to \$150,000 with two individuals and quadrupled to \$339,000 with three or more fraudsters.

The more victims lose, the less likely they are to make a full recovery.

It is nearly impossible to measure the amount of fraud prevented by a specific control, but in the study done by the 2018 Report to the Nations, the presence of every control analyzed was correlated with lower fraud losses, often substantially. Similarly, duration of the fraud was also impacted by the presence of controls. Again, the presence of each control analyzed was correlated with lower fraud duration, often reduced in half.

Active Detection Methods are crucial. Typically the more active your detection method is (such as internal account



reconciliations, management review, and surprise audits), the lower the fraud's duration and loss impact.

In companies that had these in place the loss was less and was caught sooner than those that did not have strong controls.

What do you have in place to prevent something from going wrong and what do you have in place to catch it timely if it does?

### **Internal Controls-COSO**

5 components:

- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring Activities

Each of the 5 components also applies to each of the three objectives of operations, reporting and compliance. A good internal control system should keep these objectives in mind when addressing each of the five components. There are also four levels within each of these for the overall entity, division, operating unit and function. Depending on the size of the organization, the internal control system may need to have several steps at each of the levels. For smaller organizations, there may not be separate divisions or that many operating units.

#### **Control Environment**

- Demonstrates commitment to integrity & ethical values
- Exercises oversight responsibility

- Establishes structure, authority and responsibility
- Demonstrates commitment to competence
- Enforces accountability

#### Risk Assessment

- Specifies suitable objectives
- Identifies & analyzes risk
- Assesses fraud risk

A good risk assessment must also address the issue of technology and computer security

#### Control Activities

- Selects & develops control activities
- Selects & develops general controls over technology
- Deploys through policies & procedures

#### Information & Communication

- Uses relevant information
- Communicates internally
- Communicates externally

#### Monitoring Activities

- Conducts ongoing &/or separate evaluations
- Evaluates & communicates deficiencies

An effective integrated framework, one that has effective internal controls-has each component and each relevant principle present and functioning and all five of the components are operating together.

Employees need compelling reasons to care about security. Security controls can be modified, depending on the organization's security stance, inbound threats, and employee training scores.

Prevention, not remediation, is key to cyber security and to financial fraud.

## **SUMMARY**

- Establish strong control environment and tone at the top.
- Remove opportunity by establishing effective internal controls, updating technology, and segregate functions.
- Continuously monitor, review, and modify and tighten your internal controls to adapt to changing technology and companies' environmental shifts.
- Work with all of your departments, finance, IT, and others.
- Educate all levels of employees and owners. Develop and use tools to evaluate customers.
- Initiate monitoring examinations across departments and levels.
- Repeat – continuously review and refine your perspective and actions.



The material appearing in this website is for informational purposes only and is not legal advice. Transmission of this information is not intended to create, and receipt does not constitute, an attorney-client relationship. The information provided herein is intended only as general information which may or may not reflect the most current developments. Although these materials may be prepared by professionals, they should not be used as a substitute for professional services. If legal or other professional advice is required, the services of a professional should be sought.

The opinions or viewpoints expressed herein do not necessarily reflect those of Lorman Education Services. All materials and content were prepared by persons and/or entities other than Lorman Education Services, and said other persons and/or entities are solely responsible for their content.

Any links to other websites are not intended to be referrals or endorsements of these sites. The links provided are maintained by the respective organizations, and they are solely responsible for the content of their own sites.