

# Risk Insights

## Fraud Prevention: Segregation of Duties

### Sustaining a focus on fraud prevention

**THE LONG-TIME TRUSTED CONTROLLER** handles virtually every step of every financial process, never takes a sick day, never takes vacation, never asks for help and often takes work home. Then one day, the company owner comes across a bank letter regarding an account he did not know existed. A few days later, he hears from a long-time customer wanting to know why the controller's signature also appeared on several cancelled checks.

The owner is concerned, puzzled. He comes back on the weekend and rifles through the controller's office and files. The evidence he discovers is wrenching, overwhelming: his controller, someone he trusted completely, has been committing fraud for years. The owner's company is in worse financial shape than he ever imagined.

Amidst his feelings of anger, betrayal and despair, the owner wonders how differently things might have been if he had hired an accounting manager under the controller to oversee the transactional responsibilities handled by other employees or if he had taken it upon himself to review bank statements, invoices and other financial documents.

That owner's plight illustrates all too well why the concept of segregation of duties – dividing conflicting or incompatible responsibilities among more than one individual – is a vital fraud prevention tool for organizations of all sizes, within all industries and sectors. Implementing segregated duties is a foundational element of effective internal controls.

Segregation of duties and other fraud prevention measures function as a form of insurance, an insurance that keeps organizations from having to assess the known financial damages and profound losses in confidence and trust that accompany fraud detection. It is a form of insurance that spares organizations the prolonged business disruption associated with a fraud investigation. It is a form of insurance that requires ethical leadership and the willingness to acknowledge that the potential for fraud exists everywhere.

### Emphasizing Fraud Prevention and Incorporating Segregation of Duties

**PREVENTING FRAUD REQUIRES** acknowledging that improper behavior can happen in any organization. Management's "tone at the top" provides a foundation and fundamental control for fraud prevention practices. By continually emphasizing ethical behavior, management creates a culture in which individuals value safeguarding assets and feel compelled to report any suspected improper activity. That culture serves as a foundation for implementing segregation of duties and other fraud prevention concepts.

## Fraud Prevention: Segregation of Duties

Fraud schemes vary immensely in nature, manner of execution, size, scope and other factors. In addressing an organization's specific vulnerabilities, managers must recognize that the following five elements surround all fraudulent activities:

1. Intent
2. Motive
3. Opportunity
4. Concealment
5. Repetitive acts

There is also a newly recognized sixth element that contributes to fraud at an increasing rate – competency. With the increase in technology reliance and usage, competency is currently seen as the element to defend against, and segregation of duties enforced through system access restrictions is the most powerful defense. Actually, segregation of duties combats all of these fraud-related elements.

For example, a company sales representative might entertain thoughts of attaining reimbursements for personal or nonexistent business travel expenses to sustain a lifestyle he cannot afford. Needing prior travel expense approval from a supervisor means the sales representative must explain to someone else why that travel is necessary or related to company business, which dispels perceptions that an easy opportunity to commit fraud exists. Additionally, a policy requiring that such expenses be paid for with a company-issued credit or debit card assures that third-party documentation – a detailed credit or debit card statement – will be obtained and reviewed by an accounts payable staff

member, and not the sales representative. That policy then eliminates the ability to conceal questionable expenses. Having an accounts payable person reviewing that documentation also diminishes the possibility that the sales representative could repeatedly incur improper expenses without facing scrutiny.

On at least a biennial basis, management should perform a fraud risk assessment to identify the specific activities for each organization that create exposure to fraud, and segregation of duties should then be incorporated into all of those activities. In addition to deterring fraud, that concept helps to more clearly define work roles and establishes a means for detecting honest mistakes that could get overlooked by a single individual.

For various transaction cycles, segregating duties means that one person does not address all of the authorization, custody of assets, record keeping, control activity or reconciliation functions associated with any specific cycle. Within a sales-related transaction cycle, one employee should not have authorization responsibilities for approving credit and credit terms, approving access to credit-related data files, approving deviations from standard prices and authorizing write-offs of uncollectible accounts. That situation could lead to an act of corruption, such as granting a customer lower prices in exchange for kickback payments. Properly segregating authorization duties provides a deterrent against that and other fraudulent schemes.



Fraudulent behavior usually targets money, but it can also focus on fixed assets, merchandise, raw materials, supplies, finished products, or various combinations of cash and physical items. These situations can arise within the sales returns and allowances cycle.

Credits or refunds, for example, may be issued for products that were never actually returned. A returned product requiring only minor repairs may be written off as scrap and then refurbished and sold off the books. Preventing such fraud requires segregation of duties so that one person is not responsible for authorizing credits and returns, issuing receipts for returned items and taking custody of returned goods.

Defining and documenting processes throughout the organization helps managers recognize where conflicting or incompatible duties may exist. For further understanding, those processes can be displayed in a spreadsheet or matrix format that visually illustrates processes requiring segregation of duties.

### Integrating Segregation of Duties and IT Access Privileges

**PROPERLY SEGREGATING DUTIES** also requires establishing IT access restrictions that correspond with work boundaries defined in job descriptions. Those restrictions deter individuals from executing fraud through various IT components. IT access controls also provide a preventative, automated means of enforcing defined segregations of duties for critical financial and operational processes. Those controls operate in a preventative manner and assure that individuals can only access the various applications, application functions, data sets and files needed to perform authorized work responsibilities.

“Aligning IT access restrictions with **defined segregated duties** requires establishing individual employee **roles, rights and duties**”

Aligning IT access restrictions with defined segregated duties requires establishing individual employee *roles, rights* and *duties*. Those roles, or work responsibilities, determine which IT access rights or privileges that person needs. Duties define particular individual tasks or activities, including functions performed within an application, database or other IT component.

*User provisioning* provides a profile to each employee, based on that person's roles, rights, duties and IT access needs. The concept of *least privilege*, which limits access to only the IT systems required by work duties, is incorporated into the user provision. Access attempts are then granted or denied based on the password, login and network active directory information.

Such IT access policies and restrictions ensure that segregated duties remain separated. An individual, for example, may plot to enter personnel records for nonexistent employees with direct deposit payroll funds for those ghost workers routing to his personal bank account. Not having access to all of the required human resources and payroll applications, modules and databases, however, keeps that individual from launching such a scheme. Aligning access restrictions with segregated duties throughout the organization creates an automated, entity-wide system of preventative controls.

### Maintaining Segregation of Duties

**INDIVIDUALS GO ON VACATIONS**, take extended leaves or take on new roles within the organization. New employees are hired to meet expanding business needs or to replace departing employees. Existing processes evolve or expand. New processes are established to meet unfolding needs, and IT components are continually upgraded, replaced or supplemented with additional applications or systems.

Properly maintaining segregation of duties within dynamic internal environments requires continual attention and monitoring. Whenever a work role evolves or a personnel change occurs, affected responsibilities must be examined to ensure that conflicting or incompatible sets of duties do not develop. Changing or newly-established processes require similar examination.

Related IT access restrictions require sustained attention, too. Whenever any new IT component is introduced, access rights and related automated controls must be implemented. IT access directories must continually be updated to reflect personnel changes and evolving work roles. Such diligence needs to include immediately deleting all individual access rights whenever someone leaves the organization.

## Fraud Prevention: Segregation of Duties

### Implementing Other Monitoring Controls when Needed

**DUE TO STAFFING LIMITATIONS**, remote location of a company facility, slim time constraints required for completing a particular process or other factors, situations arise in which implementing segregation of duties is just not practical.

In such cases, various means of monitoring are needed to deter or detect fraud. Those measures may include reviewing detailed activity reports and external documentation for classes of transactions that have been determined to have a high risk of fraud, such as cash, payroll and inventory accounts. The monitoring controls, which are detective in nature, should be aligned with the risk of fraud associated with a particular activity or account balance in order to ensure that the organization is utilizing its limited resources efficiently and effectively. Periodic checks of various processes provide oversight. That oversight should include confirmations with vendors and customers that transactions actually occurred as documented.

### The Full Benefits of Implementing Segregation of Duties to Prevent Fraud

**THE TOTAL KNOWN FINANCIAL LOSSES** in a detected and investigated fraud scheme are seldom recovered. Recovering stolen intangible qualities, qualities such as credibility, goodwill and trust, is even more difficult.

Segregation of duties establishes a system of workplace checks and balances, a system of preventative controls that function continuously, a system of controls that sustain the organization and constantly mitigate fraud risks. Appropriately segregating incompatible responsibilities protects the company and the individual employee. Segregation of duties helps keep the organization from having to address the aftermath of fraud detection.

## CONTACT US

**Alyssa G. Martin, CPA, MBA**

Partner-in-Charge

Risk Advisory Services

alyssa.martin@weaver.com

Weaver's risk advisory services are strategic, executable and measurable—and our nimble process is designed to help companies remain optimally functional as they identify and manage risk. We work closely with our clients to customize services that fit their existing staff structure and operations. Integral to this sensitive work, we believe our communication skills are as valuable as our technical knowledge and professional insight. You will experience thoughtful, purposeful communication throughout the process. Specific services we provide include:

- Business continuity planning
- Business process improvement
- Contract monitoring and compliance
- Enterprise risk management
- Internal audit
- Internal control evaluation
- Integrated financial and IT audit
- Performance audit and measurement
- Regulatory compliance
- Risk assessment
- Sarbanes-Oxley compliance

*Disclaimer: This content is general in nature and is not intended to serve as accounting, legal or other professional services advice. Weaver assumes no responsibility for the reader's reliance on this information. Before implementing any of the ideas contained in this publication, readers should consult with a professional advisor to determine whether the ideas apply to their unique circumstances.*

© Copyright 2014, Weaver and Tidwell, L.L.P.

**weaver**  
Assurance • Tax • Advisory