Fighting Business Fraud with CRIME

9 min read

Key Takeaways

- Reconciliation of accounts reduces risk, identifies fraud, assists in the case of an audit, and protects your company if one of your vendors is ever audited.
- Once you have implemented your control activities, run risk assessments, and optimized your information and communication systems – you need to make sure that your internal control system is running properly.
- When you take the time to objectively and comprehensively perform the assessment, you'll gain many valuable insights into your company's strengths, and whether you like it or not, its vulnerabilities.

While the title of this article may lead you to believe we're recommending criminal activities to combat fraud, in reality, we've got a much more effective, and legal, strategy to protect your business and reduce your risk of fraud. In this example, C.R.I.M.E. stands for the five components of a system of internal controls.

C.R.I.M.E.

The five components of a successful system of Internal Controls:

Control Activities

Risk Assessment

Information Systems and Communication

Monitoring

Environmental Control

Internal controls should be used to limit risk within an organization and to help prevent business fraud. In this blog, we explore in detail what each component of CRIME stands for and how implementing a systematic internal control system within your business can help mitigate risk and reduce your chances of falling victim to business fraud.

Control Activities

Control Activities are actions that companies take to minimize risk. Some activities are preventative measures, while others are used to monitor and identify undesirable events; thus allowing management to take corrective steps to fix the situation. Ideally,

management will integrate control activities into day-to-day business processes and systems. Here are some common control activities:

Reconciling Financial Records

Reconciliation of accounts reduces risk, identifies fraud, assists in the case of an audit, and protects your company if one of your vendors is ever audited. When reconciling accounts, you review all deposits, checks, transfers, and other transactions against the general ledger ad, as well as the bank records. Business fraud can occur through creating bogus vendors, erroneous deposits, or fake checks. Reconciliation follows the paper trail of your money to make sure that it's either in the bank, or paid to the correct payee.

Review and Approval

Within a larger organization, it's the internal controller's job to review all financial records for validity. Small and medium-sized businesses may not have enough resources to have an internal controller; so utilizing an outsourced bookkeeping provider or an outsourced controller is one way growing organizations can ensure that an authorized financial personnel is able to review all transactions to keep the books error-free.

Authorization

Setting authorized users for specific financial processes reduces risk by allowing management to know and control who has access and to what systems. For example, only certain members of staff should be authorized to manage the general ledger. This can be accomplished through setting user permissions in a bookkeeping software system such as QuickBooks. With proper user policies management can easily track who logged into the ledger and when, and keeps lower-level employees from making errors in the ledger. Conversely, if everyone is accessing the file using the shared administrator role, then you have no login history or paper trail to identify the guilty party should fraud occur.

Separation of Duties

Business fraud can occur when duties aren't separated and delegated to selected individuals. This is especially true for the accounts receivable position - when a single employee is in control over billing, collections, and balancing the books. The person who cuts the check should never, ever be the same person who signs the checks and records the transaction in the ledger. Creating a chain of command for processes by separating duties among employees reduces risk and ensures that multiple eyes remain on your books and your account. If you can't achieve this level of separation within your business, it's time to get creative or considering outsourcing.

After reviewing and implementing control activities, businesses need to run a risk assessment on their organization. A risk assessment identifies and analyzes both external and internal risk factors. Additionally, a risk assessment establishes objectives and baselines to follow to make sure your business is staying on track.

How does a risk assessment, and communication & information systems work to reduce business fraud?

Risk Assessments

There are so many factors that contribute to a business's success or failure. This is why running a risk assessment is so important for an organization. Knowing what specific internal or external factors pose a risk to the company, and allows management to implement risk management strategies that keep the business on track while reducing risk across the organization.

- **Internal Risk Factors** – Internal risk factors include all the events taking place inside an organization. These risks are usually related to operations and can involve human factors (turn-over, human error, etc.), technological risks (IT system failure), physical risks (fire, failure of equipment, theft), and financial factors (access to credit).
- **External Risk Factors** – External risk factors are things that happen outside of an organization that are usually outside of anyone's control. There are economic factors (change in markets, competition, fluctuations in demand), governmental

factors (changes in regulation or taxes), and natural factors (hurricanes, earthquakes, natural disasters).

Knowing these risks in advance helps a business prepare for whatever may come their way. In relation to business fraud, risk assessments paint a clear picture of all internal risk factors that may contribute to fraudulent activities and allow management to create systems and processes to keep the risks from happening.

Information and Communication Systems

In order to keep the system of controls in place, information and communication are essential to the controls' success. Internal information including business objectives, contingency plans, the control environment, and policies and procedures need to be clearly communicated across the organization. This information cannot live with executive-level management but needs to be distributed among all employees.

Both information and communication systems may be formal or informal. Formal systems may include databases, official documentation, or even regular staff meetings. Informal forms of information and communication include conversations with employees and those outside of the organization including customers and vendors. **Information and communication both play a key role in reducing business fraud.** Without clear communication of business objectives as well as internal regulations and applicable law, it is easy for faulty transactions and other unsavory business practices to arise in some area of a company.

Having systems in place for disseminating information as well as encouraging communication among employees as well as between employees and upper management help to keep everyone on track. **Businesses should adopt a "see something, say something" attitude and encourage staff to communicate any sort of activity that may not seem completely legitimate** as well as making sure to provide staff with training and documentation to become aware of said activities.

Once you have implemented your control activities, run risk assessments, and optimized your information and communication systems – you need to make sure that your internal control system is running properly.

The last two components of a complete system of internal controls involve monitoring and reviewing environmental controls.

Monitoring

Once you've put the effort into building a system of controls, it's only natural that you'll want to see how it is performing, right? Unfortunately with controls, it's very easy to overlook the need to review the rules and processes regularly. Many times, a review is only done in reaction to an instance of fraud, in which the company loses a significant amount of money. While monitoring is an important task that needs to be done with consistency, it can be simplified by utilizing tools for review and establishing protocols for the review process.

Reconciliation of accounts is one way to check the books for fraudulent transactions. Ideally, businesses should reconcile accounts at the end of each day, but at the very least, companies need to make it a weekly or monthly occurrence. There are numerous tools that can be used to help identify fraud within your accounting system. For instance, audit trail reports can be run within many popular bookkeeping systems. Some banks offer fraud monitoring as part of being their customer. For example, corporate credit cards will alert you if frivolous or uncharacteristic spending happens on your account.

Moving past the books - other systems also need to be reviewed; ones that don't directly involve transactions. Businesses need to run reviews of which employees have access to which systems. Passwords should be changed on a regular basis (in some states, it is required by law to do so), and there needs to be a system in place in regards to changing information when an employee leaves the company to make sure proprietary information such as passwords and trade information doesn't leak outside of the organization.

Environmental Control

Stretching across departments so that it is incorporated into every aspect of the business, the control environment sets the tone for the entire organization. From human resources, to finance, and even to marketing and sales, setting up the environment to reflect the internal controls ensures that no one individual or process within your company is exempt from the system of controls. **Establishing the control environment is made easier once you have established and optimized the information and communications systems.**

Whether it is through internal documentation, digital information, staff training, one-on-one discussions between employees and their supervisors, or better yet, all of the above – educating the entire organization on the controls and procedures is what establishes the control environment. All of your staff should be aware of the consequences for fraudulent activity as well as ways to report fraud or reduce the risk of occurrence.

The CRIME Assessment

Before doing anything else, you need to gain an understanding of how your company's structure, policies and procedures impact your level of risk. You can do this using the C.R.I.M.E. Assessment[11].

When you take the time to objectively and comprehensively perform the assessment, you'll gain many valuable insights into your company's strengths, and whether you like it or not, its vulnerabilities. Although the results can be disappointing, you absolutely need to study them and create a strategy to eliminate any weaknesses. At the same time, you should establish a system that facilitates oversight and promotes transparency.

Control Activities

Is there proper separation of duties? Is there a review and approval process for invoices, estimates, purchases, etc? Is the computer safeguarded? Do you have a backup if the system fails?

Risk Assessment

Do you know what your risk tolerances are and what areas have the highest risk arising from both internal and external sources?

Information Systems & Communication

Are there proper controls over computer processing? Have you established clear lines of communication with vendors and customers regarding policies for billing and collections?

Monitoring

Is there a review of your internal control activities to ensure they are being set up as specified? Is there documentation of the internal controls to allow for independent review?

Environmental Control

Is there a code of conduct? Do conflict of interest, acceptance of gift, and other related policies exist? What is the tone from the top? Does management encourage compliance with control activities?

For more information, download The CEO's Guide to Reducing Fraud, which includes recent statistics on business fraud, the financial impact of employee theft as well as efforts that growing businesses can take to help reduce their risk for fraud.

For further information, learn how GrowthForce protects businesses from fraud, or schedule a free consultation to learn if your business is ready for outsourced bookkeeping.

The C.R.I.M.E. Assessment was developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)