

Does theft prompt change?

Highlights

- Do not wait for a theft or fraud to prompt necessary improvements to your internal control systems.
- Implementing and maintaining basic internal control activities can help avoid serious consequences.
- Conducting risk assessments is a proactive way to identify control weaknesses.

Recently, Frisch's Restaurants Inc. filed a civil lawsuit against its former assistant treasurer, charging that he embezzled \$3.3 million from the company over several years. The company claims that the employee, Michael Hudson, forged payroll documents and created false credit card transactions to support his gambling habit.

The theft itself is not that unusual. The news is continually sprinkled with articles about employees who steal or commit fraud against their employers. What is significant in this case are the comments made by the Frisch chief executive officer (CEO), Craig Maier, after the theft was uncovered. He made the following statements to the press:

"We took swift action as soon as we discovered the fraud."

"As a precautionary measure, the Company is implementing an additional layer of checks and balances in our accounting systems to protect against this type of fraudulent behavior in the future."

The CEO's reactionary stance is not that unusual. We are all busy, and spending time analyzing things that we do not see as broken does not necessarily seem like a good use of our time. We also do not like to think about our coworkers being capable of fraud or theft. As the Frisch CEO stated: "We were saddened to learn of these unlawful and fraudulent acts carried out ... by a trusted and long-time employee..."

According to a recent *Internal Auditor* article, the absence of three internal controls contributed to the Frisch theft:

- Lack of ethics and financial management policies with clear expectations for employee behavior.

- Lack of appropriate segregation of authorities and duties.
- Lack of accounting systems that routinely flag unusual and large transactions.

None of these controls are strange or mysterious. They are basic internal control activities which should be familiar and already in place. So do we really need to experience a theft or fraud in our agency to prompt us to take action to shore up our internal controls?

The Frisch example shows that the absence of basic internal controls can have serious consequences. None of us wants to stand before the legislature or the press and explain, as the Frisch CEO did, how and why a fraud or theft occurred. Promising to "fix the problem" after the fact makes the agency look bad and puts management on the defensive. It also generally takes substantial time and energy to remediate a bad situation. Instead, a proactive approach is always best.

Conducting formal risk assessments to evaluate internal controls is a proactive way to identify control weaknesses and could stop a fraud or theft before it happens. Agency employees are in the best position to identify and mitigate weaknesses and vulnerabilities in their business processes. Let's not wait until something bad happens, but take action now to ensure strong internal control systems within our agencies.

Suggested action steps: Take time to think about your agency's internal control culture. Is there a sense of urgency to conduct risk assessments and to fix identified weaknesses? Make a commitment now to take proactive steps to evaluate and improve your agency's controls before something bad happens.

If you have questions, please contact [Jeanine Kuwik](mailto:Jeanine.Kuwik@state.mn.us) at Jeanine.Kuwik@state.mn.us or (651) 201-8148.