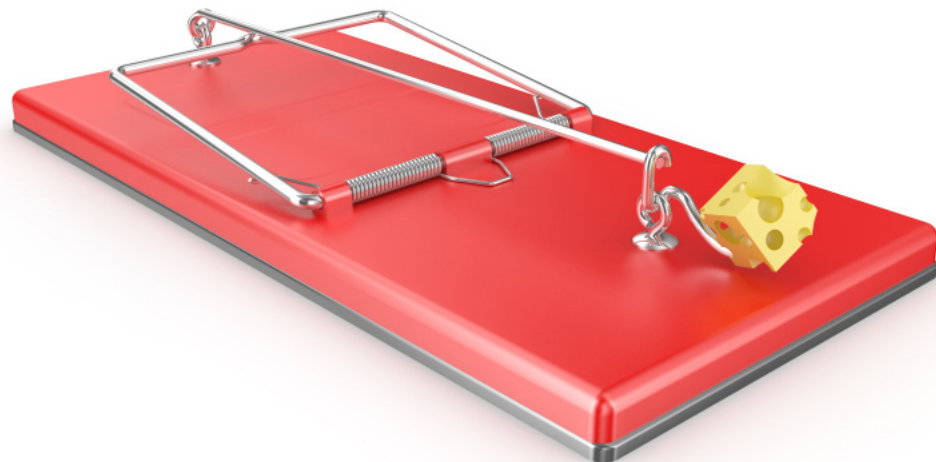


## Ten things to improve your next internal investigation Investigators share experiences



# Ten things to improve your next internal investigation

1. A little preparation
2. Know your team
3. A prompt and prudent response
4. Investigations are different from internal audits
5. Diligent but efficient
6. Loose lips...
7. Navigating global differences
8. Anticipating the unexpected
9. It's not only what they say but also how they say it
10. Creating more value

---

## Resolving concerns about inappropriate activity is a critical responsibility of those charged with governance; in particular, board members, general counsel and internal audit directors. Regulatory changes are expected to escalate this responsibility to new heights.

Increasing regulatory and government enforcement activity has become a fact of life on a global level and in the U.S. in particular. The worldwide tightening can be traced to both economic and political roots. The Dodd–Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) of 2010, which instructs the U.S. Securities and Exchange Commission (SEC) and the U.S. Commodity Futures Trading Commission (CFTC) to pay whistleblowers monetary awards for information leading to successful securities law enforcement action, quickly had an impact.

In February 2011, Tom Sporkin, chief of the SEC’s Office of Market Intelligence, spoke of an “onslaught” of tips since Dodd-Frank was enacted. He said the volume of “high-value” tips had increased from about two dozen each year to one or two each day, often presented by lawyers representing whistleblowers and with supporting documentation, enabling the SEC to follow up quickly.<sup>1</sup>

The SEC’s proposed implementation rules permit a whistleblower to make a report to the company in question, file a report with the SEC within 90 days, and still be eligible for a monetary award. While the final rule due in April 2011 may provide more time, this gives companies a limited period to investigate and report back to the whistleblower in time to avoid a report to the SEC and an SEC investigation if the allegation can be shown to be without merit. This, combined with the possibility of other whistleblowers reporting directly to the government, may put increased pressure on companies to conduct more investigations and do so more quickly than in the past.

---

<sup>1</sup> The SEC Speaks in 2011, PLI, February 4, 2011.

In addition, the increasingly global nature of corporate operations and the relatively high whistleblower awards that could arise, particularly from violations of the U.S. Foreign Corrupt Practices Act (FPCA), may increase investigations in remote parts of the world. Such probes present added challenges relating to differences in language, culture, and legal systems.

All of these factors highlight the need for prompt and efficient conduct of investigations.

### Enhancing investigation speed and efficiency

This paper explores 10 ways companies may be able to enhance the speed and efficiency of their investigation processes.

The goal of this paper is to provide you with practical ideas to help you respond to issues promptly and efficiently, which can help mitigate the potentially greater financial and reputational risks your company may now face.

### Acknowledgements

We would like to thank Juniper Networks, Inc., its executive vice president, general counsel and secretary, Mitchell Gaynor and its vice president, internal audit, Joseph Cooney, for providing valuable observations and insights from their many years of experience.

# 1. A little preparation



Senior management at a multinational's European subsidiary received a tip alleging that the operation's purchasing director was receiving kickbacks from certain suppliers. The company had no personnel identified or protocols for conducting investigations.

The subsidiary's management hired a local investigator to research the suspected employee's lifestyle. The investigator obtained copies of the employee's personal bank statements, which showed several incriminating deposits. The employee was terminated for cause, but subsequently filed a wrongful termination lawsuit. Obtaining the bank records without his consent violated local privacy laws. The evidence supporting the termination could not be offered in court without admitting to having

acquired it unlawfully. So the company had to settle the lawsuit with the employee and pay a very substantial severance.

Such incidents highlight the importance of developing an allegation response process to avoid potentially costly missteps.

Measures your company can take include establishing key roles and responsibilities with respect to potential investigations — specifically, how the legal, compliance, security, human resources (HR), and internal audit functions will coordinate to respond to alleged or suspected fraud and other wrongdoing as it arises. Developing investigative protocols in advance can help to keep investigation teams operating within appropriate bounds, reducing the risk of financial and reputational damage.

Investigation protocols may cover such matters as the criteria for invoking attorney-client privilege; methods for collecting and preserving hard copy and electronic records so they may be admissible in court; communication protocols; and retention of specialists needed to assist with aspects of the investigation such as lawyers, forensic accountants, and computer forensics and data analytics specialists.

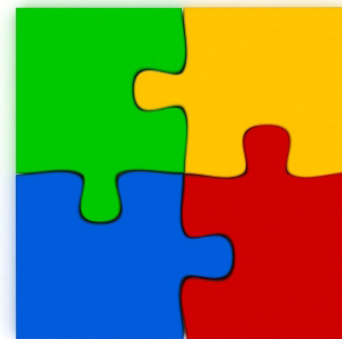
Other key considerations include establishing a case management system to facilitate tracking reports of wrongdoing received from any source, as well as procedures to evaluate allegations, assign them to appropriate parties for investigation, and track their resolution.

---

“It's important for whoever is chosen to lead the investigation to have a process, be able to explain the process, know the next steps, and provide management with a strong sense of confidence. Otherwise, executives may feel the need to take actions on their own that ultimately can be counterproductive and unintentionally undermine the investigation.”

— Mitchell Gaynor  
EVP, General Counsel and Secretary  
Juniper Networks, Inc.

## 2. Know your team



The size of the investigation team and the skill sets needed will likely vary based on the nature of the matter, its potential impact, and the parties possibly involved. A small embezzlement by a junior employee might be handled by someone in internal audit trained in investigation techniques. He or she might report to corporate legal counsel, HR leadership, or another member of management.

In matters that have significant potential impact, involve someone in senior management, or relate to financial or regulatory reporting, a more sophisticated investigation team will likely be expected by those charged with governance, by prosecutors, or regulators.

Members of a sophisticated team may include:

- **Internal investigations lawyers** — Corporate or regular outside counsel may be comfortable handling minor investigations. But when allegations involve major fraud or senior executives, lawyers skilled in leading internal investigations are typically brought in due to the complexities involved.

- **Forensic accountants** — When you're trying to find a smoking-gun entry in financial records, accountants with experience spotting trails of numbers that betray financial manipulation and cover-up can help you get the facts faster.
- **Computer forensic specialists** — Today, incriminating documents and the perpetrators' "fingerprints" are more likely to be found in electronic records. Retrieving deleted, hidden, and password-protected files and other electronic evidence normally requires prompt action and adherence to a highly disciplined technical process. Computer forensic specialists are now a key part of most investigation teams.
- **Industry specialists.** People with deep industry knowledge can help to develop the investigation plan, evaluate technical records, and identify potential misstatements by interviewees.
- **Data analytics specialists.** As the volume of electronic records has mushroomed, data analytics can be vital in controlling cost by screening large volumes of data and ferreting out a subset of records that merit human scrutiny. Sophisticated data analytics skills play an increasingly important role in larger and more complex investigations.
- **Skilled interviewers.** Lying is an inherent part of fraud, so perpetrators will likely lie to investigators just as they have to others. An investigator skilled in the fine art of persuading people to admit their wrongdoing can be invaluable for interviewing alleged or suspected fraudsters. Often these skills will be provided by lawyers and forensic accountants on the team, but on occasion individuals with specialist skills in this area may be brought in for particularly challenging interviews.

---

“Often you can’t use your usual resources for internal investigations, yet you have very little time to initiate the process. It’s good to have a backup team ready — one that can help you right out of the chute.”

— Mitchell Gaynor

# 3. A prompt and prudent response



An anonymous whistleblower letter sent to an HR department detailing multiple allegations about a senior executive. HR questioned the motivation of the writer and did not take action. Incidents over the next several months caused HR to believe the anonymous letter was possibly valid. Ultimately, the company conducted an investigation that supported nearly every allegation and revealed other misconduct as well.

Companies may not respond to whistleblower reports consistently. Their reluctance to investigate appears to increase when the tip is anonymous. An academic experiment involving 83 experienced audit committee members found that whistleblower reports received through an anonymous channel were given less credibility and allocated fewer investigative resources than those coming from an identified source.<sup>2</sup>

---

<sup>2</sup> Hunton, J. E. and Rose, J. M. (2011), Effects of Anonymous Whistle-Blowing and Perceived Reputation Threats on Investigations of Whistle-Blowing Allegations by Audit Committee Members, *Journal of Management Studies*, 48: 75–98

---

“Investigations can take months. The immediate reaction by most people is disbelief. It’s very important when dealing with a whistleblower — and with your own company — that your response is timely and that you set expectations for how long it will take.”

— Mitchell Gaynor

According to a recent benchmarking report, half of all whistleblower calls are anonymous.<sup>3</sup> Under-investigating half of all allegations could leave directors, senior executives, and their companies exposed to legal, regulatory, and financial consequences.

The Dodd-Frank Act’s whistleblower awards make it more important than ever to evaluate tips diligently, including anonymous ones. Employees who believe whistleblower reports are not acted upon appropriately may be motivated to report directly to regulators or law enforcement, potentially increasing the cost and management distraction arising from an investigation.

It is important to have a culture that encourages people to report potential wrongdoing internally, giving the company the opportunity to investigate the matter quickly and with the least impact. Many whistleblower systems can be improved to encourage employees and others to speak up and to provide more tips.

Submitted tips should be responded to promptly and thoughtfully and documented carefully. Whistleblowers need to feel that their concern is being addressed, so it can be helpful to convey that message back to the whistleblower within a few days of the report being filed using appropriate arrangements to maintain anonymity. Whistleblowers should be informed that the investigation could take some time. And, they can be encouraged to keep in contact so they can provide further assistance to the investigation team if needed.

---

<sup>3</sup> 2010 Corporate Governance and Compliance Hotline Benchmarking Report,” The Network, Inc. and BDO Consulting.

# 4. Investigations are different from internal audits



Internal audits are important for evaluating internal controls and enhancing operational efficiency. Investigations have a different purpose, use a different methodology, and present significantly different risks, all factors that highlight the need for experienced investigators. These investigators may be specially trained internal auditors, former law enforcement detectives in the company's security function, or external specialists.

The importance of a diligent, focused investigation can be seen in the example of a company that received an allegation that its procurement manager was getting supplier kickbacks in exchange for contracts. The company believed a standard internal procurement audit would be sufficient to investigate the matter. Internal auditors sampled competitive bids, tested them for compliance with established policies and procedures, but found nothing unusual.

A year later the allegations resurfaced and the company retained investigators. Instead of sampling bids, they performed data analysis on all bids and found patterns suggesting preference may have been given to a small group of suppliers. Analysis of the procurement manager's company e-mails and forensic analysis of his company-issued computer found evidence that he had a social

relationship with these suppliers. The e-mails also indicated he was living beyond his employment income. Documents found on his PC showed he had been creating false bid documents from suppliers who, when interviewed, claimed that they had never been invited to submit bids. These findings led to further investigative procedures, which resulted in the purchasing manager admitting to the kickback scheme (which had grown in the year since the earlier tests were performed).

This example illustrates that investigative procedures are typically performed on a complete data set, or one more extensive than in a typical internal audit. Investigations may use technology more widely to identify suspicious data patterns. Investigations tend to use techniques such as forensic imaging and analysis of computers, which are unlikely to be cost-effective for internal audits. Also, investigations tend to place greater emphasis on internal and external interviews and study of public records. Because they are unpredictable and may need to stand up to legal scrutiny, investigations can take longer than internal audits.

Generally, investigative objectives and results are not shared broadly in the company. Accumulated information and evidence is typically kept privileged and confidential until lawyers determine what to disclose, to whom, and when. So communications are generally controlled more tightly in an investigation.

Investigations may lead to interviews seeking admissions from suspects. Investigators generally conduct their work with the expectation that the matter may ultimately be litigated or disclosed to external parties. Because of this, there is greater emphasis on documentation and preservation of evidentiary material, as the manner in which evidence is obtained and retained can affect its admissibility in court.

---

“The closer an investigation gets to the top of the company, the more an internal audit executive needs to think about handing it over to the audit committee to ensure objectivity.”

— Joseph Cooney  
Vice president, internal audit  
Juniper Networks, Inc.

# 5. Diligent but efficient



Investigations require balancing speed with quality, thoroughness, and completeness. Approaching an investigation in thoughtful phases and remaining focused on specific issues or allegations can help to manage costs. It helps to start with a set of preliminary investigative steps to identify supporting evidence that would help the company to determine the need to probe further.

In one instance, investigators were assisting a company by looking into allegations of employee collusion with a third-party at the company's European regional office. Using an early case assessment tool, the investigators were able to focus on the key individuals, the time period, and the issues identified in the allegations. As a result, they were able to locate key e-mails quickly. These e-mails provided the company with enough evidence of misconduct to take immediate action to deal with the wrongdoers and investigate the matter quickly.

Another important consideration is to distinguish between data and documents that need to be collected and preserved, and those that also need to be reviewed. Depending on the allegations, it may be wise to secure electronic data on a broader basis, thereby limiting the

opportunity for individuals to delete or destroy e-mails or files. You may not need to review all of the collected data, but if you decide later that analysis is warranted and you haven't secured it upfront, you may have missed your chance to obtain that data, or to be sure that it hasn't been altered.

It is important to proceed with urgency, but not so fast that it may compromise the investigation's scope and quality. Examples of this include confronting subjects prematurely or rushing the investigation to completion to meet internal or external deadlines. In one instance, investigators were conducting an inquiry into embezzlement allegations by several employees. The company, feeling pressure to resolve the allegations quickly, rushed to confront the suspects before a diligent analysis of accounting and electronic documents had been performed. As a result, the investigators were unable to obtain valuable information as the employees were terminated after the interviews. Although well intentioned, this rush to confront the suspects likely increased investigative costs for the company.

Performing investigative activities in a certain order can help to control costs. For example, if you start the electronic document review and simultaneously commence interviews, a second round of interviews may be needed. And, if you confront a suspect without strong evidence, valuable information may not be obtained.

It's important to focus on the allegations rather than peripheral issues. As other potential misconduct is discovered, you can determine the priority in which it should be addressed while maintaining focus on the original allegations and issues.

---

“Try to remember what it is you're investigating — understand, define, and keep the scope focused.”

— Mitchell Gaynor

# 6. Loose lips...



Compromised confidentiality can have major consequences including waiver of legal privileges, premature and selective disclosure, or damaged employee morale. In one case, investigators were asked to help legal counsel study company e-mails for evidence that senior regional managers initiated or knew about improper accounting practices at a subsidiary under their control. Some evidence was identified and an initial attorney-client privileged report was issued, which led to a full investigation into practices at the regional headquarters.

As the investigative team continued its investigation at the regional headquarters, they didn't know that the privileged report had been circulated and obtained by the key suspects. As a result, attorney-client privilege was waived and the investigation was compromised. Forewarned, subsidiary managers knew what the investigators had found, what they were looking for, and the nature of evidence obtained as of the report date. They had the opportunity to destroy or alter evidence, influence others to keep quiet, and craft consistent explanations.

To avoid such issues it helps to determine in advance who should receive information about the investigation and reevaluate that as the investigation proceeds. Limiting information to key parties can help prevent:

- *Impairing the relationship with the suspect should the allegations prove unsupported.* Investigators looking into alleged bribery of government officials by the Asian regional head of a multinational company found

the allegations unsupported. Had the company not controlled the investigation's circle of knowledge, the manager's reputation might have been irreparably damaged, exposing the company to potential litigation and the loss of a highly valued employee.

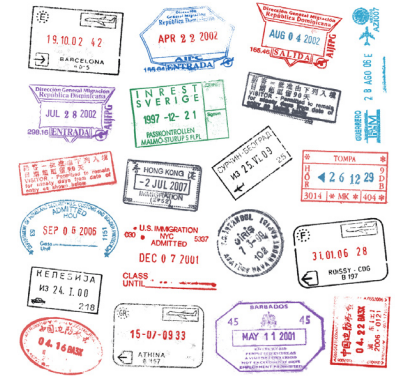
- *Negatively affecting employee morale in the office or region.* A company was investigating allegations that employees had entered into side agreements with customers at a regional office. Through various channels employees in the office became aware of the investigation. The leaks deeply affected office morale as employees feared for their jobs and the fate of their boss at the center of the allegations.
- *Inadvertently alerting perpetrators to destroy evidence, potentially increasing regulatory scrutiny and legal exposures while likely slowing the investigation's progress and potentially increasing investigation costs.* Investigators were looking into allegations that management had intentionally misled key stakeholders about the company's financial condition. A senior executive learned of the investigation though leaked information. Forensic analysis of the executive's company-issued computer showed that relevant e-mails had apparently been deleted. However, investigators still found e-mails containing evidence of misconduct by the executive, who was subsequently terminated.
- *Prematurely disclosing the investigation to outside parties.* Investigators were gathering information at a company when an interviewee revealed having already discussed the investigation with an outside stakeholder, without permission. The company quickly determined that communication protocols could help to prevent premature disclosure of inside information.
- *Making employees or third parties reluctant to report future misconduct for fear of disclosure due to lack of confidentiality.* With passage of the Dodd-Frank Act, employees may decide to report suspicious activity to regulators rather than internally if they believe internal reporting confidentiality is weak.

---

“Getting people to not talk about an investigation is tough because it is counter to a lot of corporate cultures to tell someone they can't talk about something, especially with their manager, or that they can only communicate within an attorney-client privilege framework.”

— Mitchell Gaynor

# 7. Navigating global differences



Conducting investigations internationally presents additional hazards. Following local laws and customs is paramount so the investigator doesn't become the investigated! You will likely not want to conduct searches or terminate employees, for example, without understanding and adhering to the jurisdiction's privacy and employment laws.

It is generally true that employees are hesitant to speak negatively about their superiors; however in some cultures the reluctance is particularly intense. Investigators conducting an investigation in Asia found that employees had strong loyalty to their boss at the center of allegations. Even after being shown evidence of wrongdoing, they were reluctant to provide information beyond what the investigation team already knew.

Interviews during the process demonstrated the importance of using local words or phrases. For instance, "side letters" wasn't how the local employees thought about the agreements made outside of the primary

contract. To the employees these arrangements were legitimate contracts between the company and the third party.

Ultimately, gaining trust from witnesses will require different approaches in different cultures. Using investigators from the region can help you navigate the culture and customs. Also, having investigators who speak the local language is a distinct advantage. Hiring translators is a second-best option, as much can be lost in translation and sensitive information could be revealed to third parties. Having an interviewee speak in her second language, for the convenience of the investigator, can reduce the value of the information provided as use of a more limited vocabulary can change meanings.

Data privacy laws vary from country to country. Understanding where electronic information is stored for your company is critical as it may affect your ability to remove data legally. For example, investigators were conducting an investigation into an alleged revenue acceleration scheme at a European subsidiary of a U.S. company. Because of privacy laws in the European Union, the investigators could not collect the data and bring it to the United States for analysis. Conveniently, the suspected employee traveled to the United States on business during the investigation, where the company was able to forensically image his company-issued laptop.

Unfortunately, navigating privacy laws isn't always this simple. If your data is stored in an offshore location, it would be helpful to establish protocols for obtaining the data legally. Once you know where your data is housed, your lawyers might recommend switching to a facility in a jurisdiction that will facilitate future investigations and compliance with legal and regulatory requirements.

---

**“After the investigation has revealed what happened and before thought turns to what to do with the employees, you need to understand the applicable rules for making disciplinary decisions or you can limit your options.”**

— Mitchell Gaynor

# 8. Anticipating the unexpected



Conducting investigations a certain way can help reduce the risk of adverse events. For example, encouraging management not to fire an employee until solid evidence of wrongdoing has been gathered can help to reduce allegations of wrongful termination — charges often made simply to put management on the defensive and extract a costly settlement. Avoiding making adverse public statements about individuals under investigation can help prevent charges of slander. Even choosing interview seating arrangements carefully can help avoid accusations of false imprisonment.

Some events can be anticipated. Others can surprise and disrupt an investigation. Relevant employees may resign during the investigation. Witnesses may request legal representation during interviews. Evidence of other misconduct may arise, potentially involving people higher up. To the extent possible, investigators may consider what could go awry during the investigation and, where feasible, put mitigation procedures in place.

---

“Your investigation needs to be integrated with your corporate incident response plan and coordinated by legal counsel with the people responsible for external communications. You might need to respond quickly to something, and you want to make sure the team that’s going to craft that response is up to speed on the facts.”

— Joseph Cooney

One company undertook an investigation into allegations of a corrupt senior management team in Eastern Europe. In an effort to derail the investigation, the local top executive called the police and falsely accused the senior investigative manager of breaking into the chief accountant’s office and removing company documents. The police took the manager into custody and interrogated her into the night. Wisely, the investigative team had previously lined up a local lawyer, who was immediately brought in to help. The lawyer stayed at the manager’s side during the interrogation and was able to gain her release the next morning.

At the start of an investigation of alleged manipulation of a company’s share ownership, the chief operating officer welcomed the investigation team warmly, offered to get them whatever information they needed, and even recommended local restaurants. He was not thought to be involved in the alleged wrongdoing, but by the time the investigation ended it was clear he had full knowledge of it. His friendliness was just an attempt to find out what the investigators were looking at and had found. They had anticipated he could possibly be involved and were careful not to reveal anything when obtaining documents or in conversations, even over dinner (where one night they found the executive seated within earshot, just around a corner)!

At another company, suspects in alleged financial misconduct were interviewed with legal representation and then terminated. Later, the company found it needed certain financial information. Had it anticipated that need, it could have engaged forensic accountants earlier and involved them in the interviews to obtain that information. Once employees have been terminated, it can be time consuming and more costly to obtain information in other ways.

# 9. It's not only what they say but also how they say it



Some people should never play poker because their body language communicates the strength of their hand. Similarly, interview specialists believe nonverbal cues and their timing during an interview can be as revealing as verbal ones. As with speech patterns, the issue is not so much the particular movement or phrasing, but how it differs from an interview subject's actions when not under stress.

While nonverbal cues have no utility as evidence and would not be introduced as such in court, they can help investigators identify situations in which an interview subject appears to be acting abnormally. This can alert the interviewer to explore certain areas more deeply and to adjust the flow of interview questions.

In one case, investigators conducted an FCPA risk assessment in Russia. When one individual was asked if he had done anything that would make his coworkers

uncomfortable, he said no and he exhibited no verbal or nonverbal cues to suggest potential deception. But when asked if he was aware of coworker conduct that would make him uncomfortable, he demonstrated cues of potential deception by fidgeting and not answering the question. Based on these cues, the investigators continued their questioning and discovered that the witness suspected potential coworker misconduct.

Red flags investigators often look for in evaluating the truthfulness of interviewees include refusing to answer a question, frequently repeating the question (which can be a stalling tactic to buy more time to think up a plausible answer), or responding to the question with another question. Others include providing qualified answers such as, "I didn't steal any money on Thursday" (it was Friday), unusually frequent or emphatic use of oaths, cutting off the interviewer's question or taking unnaturally long pauses.

In one case, investigators asked a financial controller about some journal entries that affected the reported profitability of one accounting period versus the next one. She answered each question without hesitation. But when asked who determined the final amount of a particular journal entry, her response was, "Good question." She then took a long pause, laughed, and provided a response that danced around the issue without naming any individuals. The investigators asked follow-up questions during which the controller identified the other parties involved.

---

**“To me, the most important thing is getting the truth and understanding what happened in your company.”**

— Mitchell Gaynor

# 10. Creating more value



Some companies with sophisticated antifraud strategies place a high value on leveraging their learning from each investigation, applying it to improve business processes in their operating units worldwide. By doing this, they help prevent perpetration of similar frauds in other locations, and they continuously improve their business processes. This increases the value created by investigations, helping to offset the costs incurred.

Each investigation is an opportunity to identify and remediate vulnerabilities in your business processes and weaknesses in your internal controls that a perpetrator may have exploited. It is a chance to learn about new schemes. Key indicators observed during the investigation that ultimately led to the discovery of wrongdoing can be

communicated to employees, building their awareness and supporting development of proactive detective procedures.

For example, investigators uncovered a large fictitious vendor invoicing scheme involving the procurement of spare parts for a manufacturing company. The investigators identified the items purchased from the suspected vendor. They then compared purchasing volume for each item to related usage and the ending quantity on hand recorded in the company's parts system.

The investigators discovered that hundreds of items had been purchased for which there was zero usage and the quantity remaining was illogically low. For example, 100 units of a particular part were purchased during the course of a year, yet no usage of that part was recorded during the year and only three items were found on the shelf. This analysis became a standard procedure for future internal audits.

Decisions about the cost-effectiveness of remediation options are the responsibility of management, overseen by those charged with governance. A diligent investigation team can often suggest a range of options, some of which may have little or no cost involved. Changing business processes to reduce opportunities for fraud may be more cost-effective than layering on more internal controls.

Finally, it is valuable to consider what the investigation tells you about your company's ethical culture and what steps might be prudent to drive it to measurably higher performance. This is a topic that may be of keen interest to both management and those charged with governance.

---

“The general counsel can contribute value simply by helping to calm people, giving them confidence that the process is going appropriately, and assuring that the right resources are engaged so the investigation will be completed as effectively and rapidly as possible.”

— Mitchell Gaynor

# Deloitte Forensic Center

The following material is available on the Deloitte Forensic Center Web site [www.deloitte.com/forensiccenter](http://www.deloitte.com/forensiccenter) or from [dfc@deloitte.com](mailto:dfc@deloitte.com).

## Deloitte Forensic Center book:

- *Corporate Resiliency: Managing the Growing Risk of Fraud and Corruption*
  - Chapter 1 available for download

## Deloitte Forensic Center

### ForThoughts newsletters and videos:

- Sustainability Reporting: Managing Risks and Opportunities
- The Inside Story: The Changing Role of Internal Audit in Dealing with Financial Fraud
- Major Embezzlements: How Can they Get So Big?
- Whistleblowing and the New Race to Report: The Impact of the Dodd-Frank Act and 2010's Changes to the U.S. Federal Sentencing Guidelines
- Technology Fraud: The Lure of Private Companies
- E-discovery: Mitigating Risk Through Better Communication
- White-Collar Crime: Preparing for Enhanced Enforcement
- The Cost of Fraud: Strategies for Managing a Growing Expense
- Compliance and Integrity Risk: Getting M&A Pricing Right
- Procurement Fraud and Corruption: Sourcing from Asia
- Ten Things about Financial Statement Fraud — Third edition
- The Expanded False Claims Act: FERA Creates New Risks
- Avoiding Fraud: It's Not Always Easy Being Green
- Foreign Corrupt Practices Act (FCPA) Due Diligence in M&A
- The Fraud Enforcement and Recovery Act "FERA"
- Ten Things About Bankruptcy and Fraud
- Applying Six Degrees of Separation to Preventing Fraud
- India and the FCPA
- Helping to Prevent University Fraud

- Avoiding FCPA Risk While Doing Business in China
- The Shifting Landscape of Health Care Fraud and Regulatory Compliance
- Some of the Leading Practices in FCPA Compliance
- Monitoring Hospital — Physician Contractual Arrangements to Comply with Changing Regulations
- Managing Fraud Risk: Being Prepared
- Ten Things about Fraud Control

### Notable material in other publications:

- Where There's Smoke, There's Fraud, *CFO* magazine, March 2011
- Will New Regulations Deter Corporate Fraud? *Financial Executive*, January 2011
- The Countdown to a Whistleblower Bounty Begins, *Compliance Week*, November 9, 2010
- Deploying Countermeasures to the SEC's Dodd-Frank Whistleblower Awards, *Business Crimes Bulletin*, October 2010
- Temptation to Defraud, *Internal Auditor*, October 2010
- Shop Talk: Compliance Risks in New Data Technologies, *Compliance Week*, July 2010
- Many Companies Ill-Equipped to Handle Social Media e-discovery, *BoardMember.com*, June 2010
- Many Companies Expect to Face Difficulties in Assessing Financial Statement Fraud Risks, *BNA Corporate Accountability Report*, May 2010
- Who's Allegedly 'Cooking the Books' and Where?, *Business Crimes Bulletin*, January 2010
- Being Ready for the Worst, *Fraud Magazine*, November/December 2009
- Mapping Your Fraud Risks, *Harvard Business Review*, October 2009
- Listen to Your Whistleblowers, *Corporate Board Member*, Third Quarter, 2009
- Use Heat Maps to Expose Rare but Dangerous Frauds, *HBR NOW*, June 2009

This article is published as part of *ForThoughts*, the Deloitte Forensic Center's newsletter series, which is edited by Toby Bishop, director of the Deloitte Forensic Center. *ForThoughts* highlights trends and issues in fraud, corruption, and other complex business issues. To subscribe to *ForThoughts*, visit [www.deloitte.com/forensiccenter](http://www.deloitte.com/forensiccenter) or send an e-mail to [dfc@deloitte.com](mailto:dfc@deloitte.com).

### Authors

**Jim Lombardo** is a director in the Forensic & Dispute Services practice of Deloitte Financial Advisory Services LLP. Mr. Lombardo may be reached at [jimlombardo@deloitte.com](mailto:jimlombardo@deloitte.com).

**Colleen Gately** is a manager in the Forensic & Dispute Services practice of Deloitte Financial Advisory Services LLP. Ms. Gately may be reached at [cgately@deloitte.com](mailto:cgately@deloitte.com).

### Commentators

**Mitchell Gaynor** is executive vice president, general counsel and secretary of Juniper Networks, Inc.

**Joseph Cooney** is vice president, internal audit, for Juniper Networks, Inc.

### Deloitte Forensic Center

The Deloitte Forensic Center is a think tank aimed at exploring new approaches for mitigating the costs, risks and effects of fraud, corruption, and other issues facing the global business community.

The Center aims to advance the state of thinking in areas such as fraud and corruption by exploring issues from the perspective of forensic accountants, corporate leaders, and other professionals involved in forensic matters.

The Deloitte Forensic Center is sponsored by Deloitte Financial Advisory Services LLP. For more information, visit [www.deloitte.com/forensiccenter](http://www.deloitte.com/forensiccenter).

This publication contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this publication, rendering accounting, auditing, business, financial, investment, legal, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

### About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.