

In this issue...



### Effective anti-fraud and anti-corruption programs

## Mitigating the threat of fraud and corruption

Fraud and corruption are significant threats to all organizations in every jurisdiction. Each year, the typical organization loses five percent of its revenues as a result of fraud<sup>1</sup> through activities such as the misappropriation of company assets, corruption and bribery, financial reporting fraud, theft of physical assets or intellectual property, and more.

Regulators are becoming increasingly focused on fraud with the expectation that organizations have established robust anti-fraud programs. In September 2015, US Deputy Attorney General Sally Quillian Yates issued a memorandum to US federal prosecutors that emphasized the importance of holding individuals accountable for their crimes, including management and directors with responsibility for the environment in which the crimes took place. The US Securities and Exchange Commission places a high priority on enforcing the Foreign Corrupt Practices Act, with settlements in the first five months of 2016 approaching \$900 million.<sup>2</sup> Similar regulation applies in many countries, and there is a continued trend of increased cooperation among the regulators enforcing anti-corruption laws.

Directors may be personally liable if a fraud or corrupt practices occur and the board is found to have been less than diligent in carrying out its responsibilities for ensuring that management put in place effective anti-fraud and anti-corruption programs and controls.

.....

Directors may be personally liable if they are found to have been less than diligent in carrying out their responsibilities for ensuring that management puts in place effective anti-fraud and anti-corruption programs.

.....

### Understanding the risks

The risks facing organizations continue to grow in number and complexity. With their 2013 update to the Internal Control – Integrated Framework, the Committee of Sponsoring Organizations (COSO) acknowledged that “business and operating environments have changed dramatically, becoming increasingly complex, technologically driven, and global.”<sup>3</sup> The globalized business environment exposes organizations to increased fraud and corruption risks, which are further heightened when supply chains extend to countries with a high Corruption Perception Index rating.<sup>4</sup>

<sup>1</sup>Association of Certified Fraud Examiners, *Report to the Nations on Occupational Fraud and Abuse, 2016 Global Fraud Study*

<sup>2</sup><http://www.sec.gov/spotlight/fcpa/fcpa-cases.shtml>

<sup>3</sup>COSO: Internal Control – Integrated Framework; Executive Summary

<sup>4</sup>See On the Board's Agenda “Understanding third-party risk,” April 2016 for further information on third-party risk

Boards of directors need to have an effective, up-to-date understanding of their organizations' fraud and corruption risks. Directors need to understand the issues well enough to be able to ask the right questions of management and know whether or not they are receiving the right answers. To do so, the board should not rely solely on management to keep it informed of the risk environment. Obtaining independent, third-party viewpoints will help directors validate what management has told them, gain insights into leading practices, and understand how their organizations compare to others—especially those within the same industry.

## Assessing and mitigating the risks

Although regulators in many jurisdictions require management and/or directors to see that the organization designs and implements effective anti-fraud controls, many organizations still continue to be victims of fraud or corruption. Often this is because, while the organization has developed anti-fraud and anti-corruption policies and procedures, these procedures may not be effectively integrated into the organization's day-to-day operations. Management and boards should therefore obtain an independent assessment of the effectiveness of their anti-fraud and anti-corruption programs and confirm that their policies and principles are being followed throughout the organization.

The whistleblower "hotline" or "speak-up" program, which is typically overseen by the audit committee is an important element of an effective anti-fraud control program.<sup>5</sup> (The ACFE's 2016 Global Fraud Study found that frauds are most commonly detected through tips, especially in organizations that have reporting hotlines.)

Because hotlines and other anti-fraud controls can potentially generate reports on a wide range of activities, audit committees need to determine the level of information to be reported to them. While some audit committees may want to be informed of every reported incident, most would find that level of reporting to be overwhelming. Instead, the audit committee may wish to set a few guiding principles around the type of matters that should be reported to them. Audit committees will likely want to be informed of allegations or instances of:

- Corruption, bribery, and insider trading
- Significant deficiencies in internal control
- Senior management malfeasance
- Accounting irregularities
- Theft and financial losses
- Broad deviations from the organization's anti-fraud policies

The Sarbanes-Oxley Act of 2002 was enacted in response to a prevalence of financial reporting frauds and a growing mistrust of the capital markets. The act requires organizations to evaluate the design and effectiveness of their internal control programs and provide external

certifications. Recently, attention has returned to internal control certification with the release of the 2013 COSO framework and stricter oversight of auditors by regulatory bodies, such as the Public Companies Accounting Oversight Board (PCAOB). Both COSO and the PCAOB have emphasized the importance of establishing robust risk assessment procedures, increasing the consideration of fraud risks and examining activities performed on the companies' behalf by suppliers and service providers.

As part of the scoping of the internal control certification program, management must assess the likely sources of material financial reporting risks and advocate the use of a "top down, risk-based" approach, while also considering exposure to fraud. While internal control certification programs are intended to strengthen the control environment, these programs do not provide absolute assurance that fraudulent acts will not occur.

## Investigating incidents of fraud and corruption

When fraud or corrupt practices do occur, the financial damage to the organization is often far surpassed by the damage the wrongdoing causes to the organization's brand and reputation. It is not surprising, then, that organizations prefer to see events investigated as quickly as possible to contain the financial and reputational damage and enable the organization to move on.

For this reason, organizations are often tempted to investigate actual or alleged incidents of fraud or corruption using in-house resources, although the effectiveness of these investigations may be limited. For example, not all organizations have a sufficient investigation methodology or the experienced resources to execute an in-depth and rigorous investigation. Further, the level of investigative scrutiny may be less stringent when an in-house team investigates and questions its own colleagues. Pressure from management to close the investigation as quickly as possible to limit damage may also cause incomplete results and a bias towards concluding that incidents are isolated events rather than part of a broader issue.

When fraud or corruption is suspected, audit committees should ensure that the appropriate investigative team is consulted and engaged early in the process. Many organizations wait to call in outside advisers, such as forensic investigators, legal counsel, and external auditors, until after the organization has completed its own in-house investigation, with the expectation that the external advisers will review the procedures performed and conclude that the incident had been resolved appropriately. More often, however, the organization's internal investigation may compromise evidence and complicate the post-investigative review, particularly when it uncovers gaps in the in-house investigation, resulting in additional time and cost to the organization to remediate such issues.

<sup>5</sup>A further discussion of whistleblower programs is provided on page 4



**Anthony Campanelli**  
Partner, Deloitte Advisory  
Regulatory, Forensics, & Compliance  
Deloitte Financial Advisory Services LLP

*“Fraud and corruption-related issues can arise from and potentially involve all parts of an organization. An effectively designed, implemented, and managed compliance program needs to be tailored to the organization’s specific risk areas. Audit committees need to confirm that the program is regularly assessed to verify that its principles and procedures are being followed appropriately, and that the audit committee is notified when suspected incidents occur or are reported so it can ensure they are investigated.”*

## Key components of an effective anti-fraud and anti-corruption program

The audit committee should evaluate:

- The overall compliance structure, including the roles, resources, and responsibilities of the compliance, legal, and internal audit functions.
- The thoroughness of the anti-fraud and anti-corruption risk assessment, including the criteria used to determine high-risk accounts, activities, and operations.
- Policies and procedures covering risky accounts and activities, such as revenue recognition, reserves, and activities of third-parties acting on the company’s behalf, particularly with government officials.
- Training protocols, including how training is monitored and assessed as well as its method of delivery, frequency, and content. This could include training for new hires, managers, and employees with responsibility for business functions such as third-party due diligence or the approval of charitable contributions, as well as train-the-trainer activities.
- Protocols for third-party due diligence, including the assessment of the sufficiency and quality of due diligence reports and how red flags are addressed.
- The substance and frequency of senior management and regional compliance officer anti-fraud and anti-corruption communications.
- The nature of the whistleblower reporting systems for employees and third parties, including communications and training, anonymity, ease of use, frequency of use, whistleblower protections, and language capability.
- Ongoing monitoring and review processes, including internal audit programs and protocols for investigation and reporting.
- Policies regarding disciplinary and incentive procedures for violations of anti-fraud and anti-corruption policies and procedures.
- Anti-fraud and anti-corruption merger and acquisition due diligence procedures including both pre- and post-closing acquisition due diligence.

# A compliance officer's perspective



David Doyle is the chief compliance officer for Starwood Hotels & Resorts Worldwide Ltd., which owns, manages, or franchises more

than 1,300 hotels in 100 countries under renowned brands such as The Luxury Collection, Westin, W Hotels, St. Regis, Le Méridien, and Sheraton. Mr. Doyle is responsible for developing and overseeing Starwood's global ethics and compliance program, administered through a team of US and international legal professionals.

*A whistleblower program is an important tool to help identify wrongdoing within the organization. David Doyle discusses the characteristics of an effective whistleblower program.*

## **What are the key considerations for the audit committee when setting up a whistleblower program?**

For US companies, the audit committee's first consideration should be to ensure that their whistleblower program complies with the Sarbanes-Oxley requirement that the audit committee make a whistleblower program available to employees. Audit committees of organizations based in other jurisdictions would similarly want to ensure that their program complies with their local requirements.

Having said that, the regulations do not provide a great deal of guidance as to what a whistleblower program should look like. It's largely left to the audit committee to determine what is appropriate for the organization and, generally, that includes allowing reporting through different mechanisms—telephone hotlines, websites, etc.—which usually should be available on a 24/7 basis for larger, more complex organizations. In the United States, Sarbanes-Oxley also requires that the whistleblower program must provide a mechanism for anonymous reporting.

When a whistleblower program is to be extended to other jurisdictions, things become more complex. For example, it may be cost prohibitive to make the platform available in every language favored by employees. There are also different laws to comply with; in some parts of the European Union, for example, anonymous reporting is prohibited, which runs counter to Sarbanes-Oxley requirements in the United States, so those differences need to be reconciled.

Another important consideration for the audit committee is ensuring that a truly independent function is set up within the organization to vet the allegations and concerns that come in and follow them up appropriately. It is important that the people conducting the investigations and recommending the responses are not implicated and are without any conflicts of interest. At Starwood, this vetting responsibility is shared among groups including legal, internal audit, and human resources, which helps add accountability and redundancy to the function.

One also needs to consider the socialization of the various reporting mechanisms. A successful compliance program must communicate with and educate its employees, including through sharing information about hotlines and other reporting avenues. While there is no one-size-fits-all methodology, providing information on the company's Internet page and notifying employees through various training programs may generally satisfy this requirement.

## **This sounds like a complex task. Where can the organization go for help?**

There are many vendors and service providers that offer predesigned or customizable whistleblower products, and they can cover a range of services, including the provision of the hotline or reporting mechanism, translation services for programs in multiple languages, monitoring the calls that come into the hotline, and even investigating the issues that are raised.

A common practice among larger organizations is to utilize a vendor to provide the reporting mechanism, such as the website, and to staff the reporting phone lines because it's important to have skilled people taking the calls, especially when they may come in different languages. Having an outside vendor handle the hotline can also help assure employees that the people taking their calls won't themselves be implicated in the problem, and provides additional comfort that their reports may remain anonymous. Utilizing an external vendor for such services can also free up internal compliance resources for other matters, without foreclosing the possibility of, or discouraging the reporting of, issues or concerns through internal channels too.

Once the vendor reports back to the organization about the incidents reported on the hotline, most organizations will use an in-house team to assess the complaints, and if necessary, respond to them and mitigate the problems.

**These programs can generate a range of complaints. What steps can be taken to guard against missing something significant among a lot of trivial concerns?**

Whistleblower programs in large organizations generate both significant and relatively trivial issues across a range of bases—human resource complaints, financial concerns or ethical issues—and it isn't uncommon for a single call to raise multiple issues.

The best way to protect against important matters being obscured is to make sure an appropriate team of people is reviewing the complaints. The team needs to be trained to identify what is truly important and know where to refer the complaints for follow-up. Given that the calls will generate complaints across a variety of areas, it's also helpful to have people with different areas of expertise on the team. In our organization, for example, the team includes people from internal audit with specialized financial training as well as members of our ethics and compliance group to ensure that the necessary specialized skills and knowledge are brought to bear to evaluate every allegation and that there is agreement among the group about the appropriate follow-up.

Another important consideration is building redundancy into the team and the process. You must have more than one set of eyes reviewing the complaints because it's only natural that the people who read the complaints day after day can become a bit jaded after a while and may miss something.

**What should happen when complaints are raised?**

The board of directors and the audit committee need to make sure that the proper escalation procedures are put in place to address complaints about significant matters. Often this will require the involvement of different functions and members of senior management, including finance, the general counsel, and others.

If the organization is appropriately staffed to conduct its own internal investigation, then complaints can certainly be handled internally. However, there are certain thresholds beyond which it would be risky and perhaps even improper for an internal investigation to be the sole response. Empowering the internal investigation team and providing sufficient resources to balance these often competing considerations is a critical management function of the board and audit committee, and should be continually reassessed to ensure a robust investigative function that is capable of responding to the company's needs.

If senior management is potentially implicated, there needs to be a proper show of independence from the investigators, and that certainly argues in favor of having external investigators who are engaged by a group other than management, such as the audit committee. Therefore, the audit committee needs to put in place protocols for removing management from the oversight and responsibility for investigating and remediating a problem and transferring that role to the audit committee or

another designated committee of the board to engage their own external representation to conduct an independent and thorough investigation.

**What information should be publicly disclosed about an allegation?**

If a complaint suggests a potential significant risk to the company, such as a material financial risk, then the question of disclosure becomes significant. In the case of a public company, for example, the board will need to consider what to communicate to shareholders and when—for example, will it report to shareholders when issues have been identified, or only when an investigation is underway? The timeliness of the communication is also important because the organization may need to make a disclosure before it's even been able to determine whether the allegations are credible and have substance. These are difficult decisions that are best done in consultation with the organization's external counsel and outside auditors.

**What matters should be reported to the audit committee?**

The audit committee should be informed of any allegations that may be material to the organization so the committee can ensure that they are being dealt with appropriately. It's also important that the company's external auditors be kept apprised of these developments.

What's important is the definition of materiality. To that point, the audit committee needs to set out clear guidelines with respect to the issues it wishes to be informed about, the degree of frequency of those reports, and the means of those reports. The committee should also set out the issues that it is comfortable delegating to management to resolve. In certain instances, it may be appropriate to inform the audit committee of allegations or concerns involving senior management to ensure sufficient independence of the investigative function, and to reaffirm the proper "tone at the top" of the organization. Such communication is easiest when the compliance function has a direct or dotted line reporting relationship to the board or audit committee, which is why this structure is increasingly viewed as a best practice.

**What should be reported internally about the whistleblower program and the way complaints are handled?**

That will depend on the audience. The audit committee and management need to know how well the ethics and compliance program is responding to whistleblower complaints. In this new era, with a tremendous focus on accountability, compliance program metrics have become an increasingly popular method of evaluating the efficacy of a compliance program. In this regard, it is helpful to have statistics on the number of complaints that have been raised, including those that were substantiated or unsubstantiated, and those that required follow-up and those that did not. There should also be statistics about the turnaround time to respond to complaints and complete investigations.

It's helpful to benchmark the organization and its whistleblower program against others in its industry or more broadly. Many of the third-party vendors that provide hotline services collect those statistics across the population of their customer base and make them available for organizations to use to compare and assess their performance.

### **What about reporting back to employees?**

That can be difficult. The people who use the hotline need to have confidence that their complaints have been heard and some action has been taken in response to them. Therefore, it's important to notify the reporters that their complaints have been received and they are being given appropriate consideration; that's something our organization does for every complaint it receives.

However, often what you cannot do—and what the hotline users want—is to give an indication a priori that the allegation is being treated as true. Usually, it isn't possible to provide details of how the company has responded to a complaint, especially with more significant allegations or concerns since they may be confidential, privileged or involve a conflict of interest.

One of the best ways to generate buy-in and enthusiasm for a hotline is for the employees to see there is an impact when they make a complaint, especially if it is a well-founded concern that the company takes steps to address. So after an investigation is closed and when some action is deemed appropriate, there needs to be some thought given to how to appropriately educate employees about the steps that were taken and the reasons for them. It certainly helps to reinforce the profile of the whistleblower program and build that confidence in it.

Organizations should also be cognizant of any labor and employment implications, along with privacy implications in foreign jurisdictions, in reporting back information to employees, particularly after an investigation has been completed. Moreover, they should be very careful in the substance reported back, as they should always expect these disclosures may become public. When in doubt, consult with outside counsel.

### **Given the limitations on reporting back to users, what else can be done to build confidence in the whistleblower program?**

A whistleblower hotline won't do the organization any good if it isn't supported with a culture that encourages people to pick up the phone or log on to report any concerns they may have. That's the reason for making a hotline available on an anonymous basis: to give employees some measure of comfort in using it without fear of retaliation. But people's level of confidence in the hotline will vary widely by jurisdiction; we've seen different cultural microclimates regarding people's degree of comfort of using even an anonymous hotline when it's available.

There needs to be the proper tone at the top—the board and management must be seen to be committed to the program and, whenever possible, be seen to be acting on the information that comes in. That includes taking steps to continually raise the profile of the hotline within the organization and give employees continuing reassurance that their reports will be dealt with appropriately without retaliation. Employees should be encouraged to view the hotline as one way they can communicate their concerns to management. Doing that requires careful communication to employees, and I think it's essential that the audit committee and compliance team make sure there is a true culture of accountability with management that starts with the whistleblower hotline.

### **What training should be provided to employees about the whistleblower program?**

Some organizations may wish to pair training content for their whistleblower program with anti-retaliation awareness or other human resource subjects. Most often, however, training to refresh employees' awareness of the whistleblower program can and should simply be incorporated into broader training modules relating to code of conduct, anti-harassment, anti-corruption, or other specialized compliance subjects. Periodic communications to keep the program top of mind can also be disseminated through whatever media the organization uses to keep in touch with its employees and promote initiatives.

### **Some regulators, such as the SEC, have introduced their own programs that compensate whistleblowers who report to them. How has this impacted your whistleblower program?**

The compliance literature confirms that overall whistleblowing activity is on the rise, and surely some of this must be a result of the bounty programs that the SEC is promoting, together with years of messaging about the importance of good corporate citizenship. I have seen no clear correlation between these messages and our own activity level at Starwood. However, I do think it is usually a positive sign in any organization—particularly one putting resources into promoting or developing its whistleblowing program—for there to be stable or even modestly increased usage over time. Barring some spike in related reports (of which one must always take careful note), this can signal both growing faith in the system and a more vigilant culture. By extension, a well-used and well-run program helps to foster more positive and productive "mood at the middle" and "buzz at the bottom," and that's really what it's all about.

• **Dan Konigsburg**

• Managing Director  
• Global Center for Corporate Governance  
• Deloitte Touche Tohmatsu Limited  
• [dkonigsburg@deloitte.com](mailto:dkonigsburg@deloitte.com)

• **Michael Rossen**

• Managing Director  
• Global Center for Corporate Governance  
• Deloitte Touche Tohmatsu Limited  
• [mrossen@deloitte.com](mailto:mrossen@deloitte.com)

• **Anthony Campanelli**

• Partner, Deloitte Advisory  
• Regulatory, Forensics, & Compliance  
• Deloitte Financial Advisory Services LLP  
• [acampanelli@deloitte.com](mailto:acampanelli@deloitte.com)

---

[www.global.corpgov.deloitte.com](http://www.global.corpgov.deloitte.com)

Visit our [Global Center for Corporate Governance website](http://www.global.corpgov.deloitte.com) to find relevant resources to support your board's needs.

---

## Acknowledgements

The Deloitte Global Center for Corporate Governance would like to thank all of the professionals who assisted with drafting, editing, and reviewing this publication, including those listed below:

Co-authors: Chantal Rassart (Canada) and Hugh Miller (Hugh Miller Communications).

Technical Reviewers: Michael Rossen (United States), Kevin Tracey (United States), and Kris Wentzel (Canada).

## [www.deloitte.com](http://www.deloitte.com)

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 220,000 professionals are committed to making an impact that matters.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

© 2016. For information, contact Deloitte Touche Tohmatsu Limited.