Take the Conflict of Interest Challenge

This illustration is part of the OCEG GRC Illustrated Series. You can download it and earlier installments at www.oceg.org/illustrations or by selecting "Topics," then "GRC Illustrated," from the News pull-down menu at www.complianceweek.com.

by Carole Switzer

I recently read a very interesting interview with Dave Smith, EVP of Sales for the GRC software company, Convercent, discussing the damage a company can suffer from conflicts of interest (COIs). Dave cites two studies that highlight the problem, which can be summed up like this:

FACT: COIs are observed often, but reported rarely - COIs are the third most commonly observed type of misconduct, according to the *2013 National Business Ethics Survey* (NBES), but only 49 percent of workers who observe COI misconduct are reporting what they see.

FACT: Companies aren't effectively managing COIs despite technology being available to help - a combined 74 percent of companies use internal/desktop tools, or none at all, to manage COIs, according to the *2015 Compliance Trends Survey* from Deloitte and *Compliance Week*, which reveals the lack of sophistication around managing this risk area.

Dave goes on to discuss how COI has become a big risk area for companies of all sizes, in all industries and any country, but especially for those that are large and widespread. Indeed, if you spend an hour on the web, you'll find many examples of COI causing financial losses for companies or their customers, questionable outcomes in scientific and medical research, and facilitation of fraud, bribery, and corruption; not to mention loss of stakeholder trust. You'll also find numerous guidance documents from industry oversight bodies and public sector entities.

Switzer

What you won't find is any clear pattern of change or maturing in COI management.

So why have companies not taken conflict of interest management more seriously? Why haven't more applied available technology to make identification and assessment of COI risks and the submission and resolution of disclosures easier and more effective? I have a few theories about the reasons for this shortcoming.

Reason 1 – lack of knowledge

Maybe it's because the company costs from realized COI risks haven't been easy to ascertain. When conflicts aren't managed in a unified system that allows for full analysis as changes in circumstances arise, it's virtually impossible to identify and quantify related losses. So here you have the proverbial chicken and egg problem. We don't have the information management and analysis in place to ascertain the amount of damage being done due to COI. Therefore, we don't recognize the damage and don't think it's worth investing in a better management system.

Reason 2 – lack of motivation

Maybe it's because companies that engage in conduct that harms their customers based on conflicted interests haven't felt the pain. Take the case of JPMorgan, which agreed to $300,000,000 in settlements with the Securities and Exchange Commission and the Commodity Futures Trading Commission a few months ago, for failing to tell its customers that it was making huge profits by putting their money into mutual funds and hedge funds that generated fees for the company, even though these might not be the best investment choices for the customers. Nearly a third of a billion dollars sounds like a big penalty, but according to Bloomberg News, it represents only about 1 percent of the company's annual operating profits or about a month of profits from its asset-management division. Maybe that's just not enough to motivate a change in behavior industry-wide.

Reason 3 – lack of strategic direction

Maybe, and most likely, it's because companies fail to apply the strategic goal of Principled Performance to managing COI risk. Principled Performance, as defined by the non-profit think tank, OCEG, is the ability to reliably achieve objectives while addressing uncertainty and acting with integrity. What we know as GRC is the integrated set of governance, risk management, and compliance capabilities that support and drive attainment of Principled Performance.

If your company has taken a weak approach to COI up until now, whatever the reason or reasons, it's time to take what I'll call the five step "Conflict of Interest Challenge."

Step One

Start by employing GRC capabilities to collect and analyze the information needed to determine past losses, and track future potential losses, from failing to properly manage COIs.

Step Two

Put in place a layered system of proactive controls including policies, training, and disclosure procedures to ensure COIs are identified and risk-based decisions about how to address them are applied.

Step Three

Establish processes for detecting actual and potential conflicts beyond what is disclosed, and for remediating any improper situations.

Step Four

Assess your COI management plan using the free, open source OCEG GRC Capability Model from oceg.org as a guide.

Step Five

Support your plan using modern technology systems that allow for oversight, analysis and reporting in real time.

By taking the challenge, your company will be one step closer to the goal of Principled Performance. ■

Carole Switzer is the co-founder and president of OCEG, a non-profit think tank that develops standards and guidance to help organizations achieve Principled Performance—the reliable achievement of objectives while addressing uncertainty and acting with integrity. www.oceg.org.

GRC Illustrated

GRC for Conflict of Interest Management

Employee Conflicts of Interest (COI) present a huge management challenge in today's widespread and complex organizations. Integrated governance, risk management and compliance (GRC) capabilities can enable full disclosure of potential conflicts by employees, and management of each COI according to risks presented. Strong COI compliance capabilities includes monitoring, risk assessment, policies, training, detective controls and systems of disclosure management that maintain up-to-date information and enable communication as changes arise.

Compliance Week and the Open Compliance and Ethics Group have teamed up to provide readers with this regular illustrated series on governance, risk, and compliance programs. For information on this series and a downloadable version of this illustration, please go to www.complianceweek.com, and select "GRC Illustrated" from the "Topics" pull-down menu on our toolbar.

DEVELOPED BY OCEG®

WITH CONTRIBUTIONS FROM convercent

Observe Environment to Identify Potential COIs

Verify regs or contracts that require COI management

Identify supplier and customer relationships

Understand ecosystem of third parties and all parts of the company

EXTERNAL

INTERNAL

Understand existing COI policies, procedures and controls

We've mapped all the disclosed and potential COIs

Next we analyze misconduct trends and risks

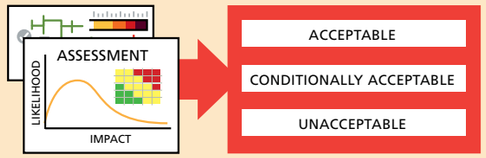
Analyze structured and unstructured data from disclosures, incidents, procurement, sales, HR and legal and third party sources

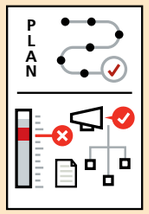
Evaluate current COIs and disclosures

Assess COI Risks and Design Controls

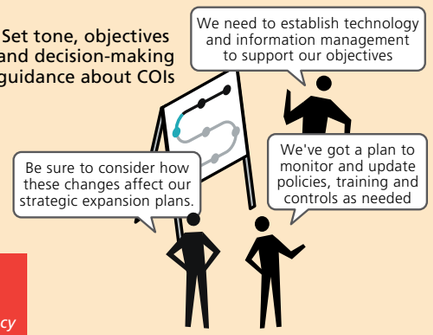
Assess COI risk, considering impact on different employee populations

Assess and rank potential threats and negative outcomes from various types of COIs in each employee population

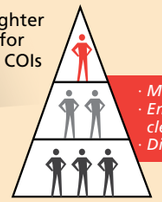




Set tone, objectives and decision-making guidance about COIs



Establish tighter controls for higher risk COIs



- *Multi-level approvals*
- *Employee attestation to clearance conditions*
- *Disclosure refresh frequency*

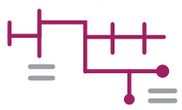
Define the strategic and tactical plans to address COIs based on risk ranking

Verify COI Management Capabilities

OTHER DATA SOURCES:
- Employee surveys
- Suspicion reports
- Gift records
- Incident trends
- HR data

DISCLOSURE REPORTS:
- ✓ Employee groups
- ✓ Business units
- ✓ Regions
- ✓ Dispositions
- ✓ Declination rates

DATA COLLECTION + AUDIT TRAIL ACTIVITY

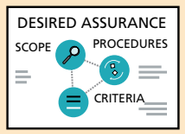


DISCLOSURE VERSIONING

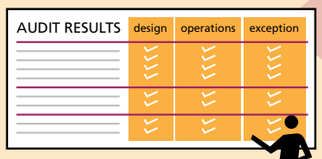
REPORTING & ANALYTICS

ESCALATION

Monitor the capabilities and improve them



Provide assurance to leadership and satisfy legal and external reporting requirements

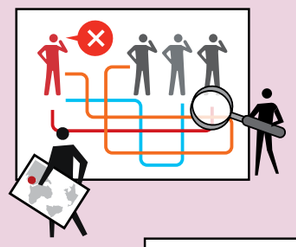


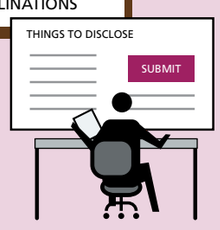
Evaluate all system capabilities

Perform COI Control and Monitoring

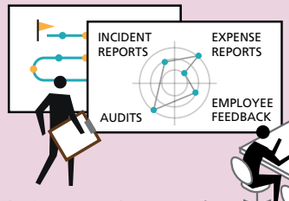
Run proactive controls

- POLICIES
- TRAINING
- DISCLOSURES + DECLARATIONS
- DECISION-MAKING RULES + GUIDANCE
- ENHANCED CONTROLS
- DISCLOSURE DECLINATIONS

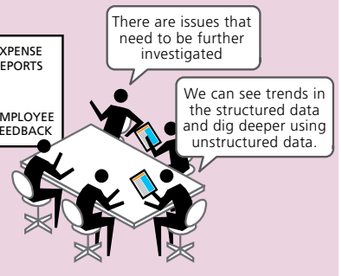




Maintain detective control monitoring



Activate responsive controls



EMPLOYEE DISCLOSURES ARE KEY

Disclosures are central to COI management. Conflicts can arise in many situations including:

- Serving on a board
- Running for or holding office
- Having personal relationships
  - *> in the company*
  - *> at a competitor*
  - *> at a third party*
- Holding financial interests
- Receiving gifts or entertainment
- Maintaining other jobs
- Publishing a book or teaching

COI RISKS ARE VARIED

COI risks go beyond employee self-interest. Conflicts can lead to losses from many angles, including:

- Antitrust violations
- Bribery, corruption or fraud
- Competition disadvantage
- Data breaches
- Insider trading
- IP leakage or theft
- Stakeholder litigation
- Unfair employment practices

[AN **OCEG ROUNDTABLE**]

Conflicts of Interest: An OCEG Conversation

SWITZER: The term "business conflict of interest" means different things to different people. Most commonly, we think about taking an action that benefits you but clearly hurts your company. Conflicts, however, aren't always that obvious. How do you define business conflicts of interest?

HASSAN: A business conflict of interest exists whenever an employee might be unable to make an unbiased and objective decision in the best interest of the company because of a competing personal goal or interest. In short, it occurs whenever the employee's interests are in competition with the company's. Potential conflicts of interest with dealers, distributors, and resellers are not always as obvious to many people. For example, suppose an employee has a family member who changes jobs and starts working for a dealer, distributor, or reseller of the company. The appearance of conflict can exist and call into question whether that dealer, distributor, or reseller is receiving some type of preferential pricing, rebate, or incentive as a result of their family relationship —the employee's family interest is potentially in competition with the company's best interest. This may not create any actual conflict of interest—but the potential for a perceived conflict is certainly there and should be disclosed, vetted, and cleared.

WINTERBURN: We look at conflicts of interest or COIs as anything that could compromise an employee's objectivity in doing his or her job. This might be something that they can personally benefit from, or that may be detrimental to the company—or might not. The challenge of COIs is that they don't need to actually exist to do harm: The mere perception of them can be corrosive. There is plenty of gray area where objectivity is harder to apply but consistency, transparency, and accountability are still critical. Disclosure not only of relationships but also of certain types of activities that an employee engages in is a key step. One example is that all of the data breaches and sensitivity around IP leaks and data protection has given rise to more focus on early COI detection and handling. Specifically, we're seeing that companies want to know about employees' outside activities like second jobs, pet projects, consulting activities, book publishing, public speaking, or teaching a course. Look at any situation where they might share sensitive information, even if it's not done maliciously.

SWITZER: What are some of the activities or changes that might give rise to new conflicts, and how do you go about tracking those?

HASSAN: Many times people think of conflict of interest risk arising in a transactional context. Has there been an acquisition or merger of some kind? Has the company entered into a new joint venture? I prefer to look at conflict of interest risk in the broader context of relationships. Relationship changes of any kind, whether company-based or personal, can create the potential for new conflicts of interest. Instead of only thinking about what corporate transactions are taking place, think about which of your relationships, both personal and professional, are changing. Has your sister recently gotten married? Who does your new brother-in-law work for? Is there a potential conflict there? Have you recently formed a new summer softball team with a bunch of your old college buddies? If so, who do they each work for and is there a potential conflict? If you focus your risk assessment for potential conflicts on relationships, you're casting a much wider net and capturing many more potential conflicts than you would with a focus only on transactions.

WINTERBURN: Any number of regular business activities could create new COIs, from hiring a new employee to competing for new business to acquiring another company. This is really where the future and power of conflict management lies—to be able to drive strategic business decisions based on better compliance information. Instead of sending out an annual disclosure form, and triaging those disclosures that contain conflicts once they're already in play, imagine if, when expanding your offices in China, you can place a higher level of scrutiny on any hiring process that involves a job candidate with ties to a government official. Or when you enter a procurement process, you alert employees in another division with an existing relationship to the potential customer about the blackout period.

SWITZER: What are the best ways to identify actual any potential conflicts? And then how do you keep track of them as changes occur?

HASSAN: In many respects, conflicts of interest really are in the "eye of the beholder"—you know one when you see one. But how can a company "see" into the lives of each of their thousands, or tens of thousands, of employees? One of the best ways to identify potential conflicts is to arm your employees with a thorough understanding of what a conflict of interest is and then ask them to tell you about theirs. Consistent training and education pieces about what a potential conflict of interest can look like, the context they are often found in, how to identify one, and how to report and clear one when you do, are key elements of conflict of interest prevention programs. There is also no substitute for simply asking employees about their relationships and potential conflicts. An annual outreach to employees asking them to identify and report potential conflicts is imperative.

WINTERBURN: I'd say consider asking for disclosure of some potential COIs as early as the recruitment process. During interviews ask your candidates to disclose any intellectual property, non-solicitation, or non-compete agreements that they may have. This helps avoid future litigation and IP infringement conflict with other companies. One of the best resources you'll have is a comprehensive history of all of your disclosures, no matter if and how it was cleared. It'll let you take an early look at previous disclosures that may present a new risk of a conflict given the business change.

Start by combining an evaluation of your current environment—legal requirements, contractual obligations, history of COI-driven issues, disclosure history, and ecosystem of third parties—with information from your risk assessment. Then go through the exercise of ranking them and deciding which are unacceptable, which are acceptable and which are only acceptable under certain conditions.

Relationships and business change daily, so it's important to consider the ongoing maintenance of your disclosures as carefully as your initial collection and clearance activities. Employees should know how (and be able) to make changes as needed without submitting an entirely new disclosure. Compliance should be able to request and receive updates to high-risk disclosures more frequently. And there should be auditable records kept of disclosure versions, even ones that have been archived.

A newer practice is to target and tier the collection and management of COI disclosures. First, solicit disclosures related only to a limited set of COI types for specific employee groups. This requires that you understand which types of COIs are most pervasive and present the most risk at different levels of your company. You might, for example, want your entire company to disclose any second jobs they have, but only ask your VPs, C-level executives, and directors about boards they sit on. Then, you calibrate your review and clearance processes by the potential risks COIs present. Perhaps you want every board membership disclosure to be cleared by your CCO and general counsel. Or require outside jobs to be cleared by the employee's supervisor before being sent to and cleared by HR. Going further, you can require employees attest to the conditions under which you're clearing a conflict and update the disclosure on a more frequent basis to ensure the conflict as you understand it—and have cleared it—hasn't changed or escalated past your comfort level or risk threshold.

SWITZER: Do you always just not allow any conflicts, or are there varying levels of control that you put in place? How do you risk assess them to make that determination?

HASSAN: It would be impossible to entirely eliminate every situation that creates a potential or even theoretical conflict. For situations that create only a theoretical risk of a conflict, it is reasonable to document the potential risk and put controls in place designed to prevent the development of an actual conflict. For example, if you have an employee working in purchasing whose father recently changed jobs and now works for a supplier, having the employee sign a recusal agreement promising to recuse themselves from any and all negotiations or transactions with that supplier is a reasonable control that can be audited against and confirmed annually. This is different, of course, from an actual and existing conflict of interest—for example, an employee who actually obtained preferential pricing or treatment for the company as a result of a family member working for a supplier. That type of actual conflict cannot be allowed.

WINTERBURN: The first element of an effective COI management program is to do away with conflict-shaming. It's an important myth to dispel that all conflicts are bad—which isn't true—and shouldn't be tolerated—which isn't necessary. Potential conflicts are going to exist in all companies, at all levels, to varying degrees. It's important, then, that organizations take the opportunity to thoughtfully approach how they find out about them and hold themselves accountable for transparency around why and how certain conflicts are tolerated or not. Begin this entire exercise by seeing conflict management as an opportunity to foster a dialogue—an important one—with your employees. Done right, you'll build a rapport and level of trust by making it clear that your goal isn't to stifle business by drawing a hard line. You simply want to point out where the line is and help them do their jobs by operating right up to that line, without stepping over. To do that, you need to understand the risks of the different COIs—preferably across different employee population segments, geographies, and business units. This is no different than how you assess and mitigate any other risk, but can be important in saving your employees from having to wade unnecessarily through communications and questionnaires about conflict types they're unlikely to have, and will save your reviewers from having to wade unnecessarily through conflicts that are unlikely to pose risk or create issues. ■

ROUNDTABLE PARTICIPANTS

MODERATOR
Carole Switzer
Co-Founder & President,
OCEG

Gwendolyn L. Hassan
Managing Counsel –
Global Compliance & Ethics
CNH Industrial N.V.

Philip Winterburn
Chief Product Officer
Convercent

[GRC ILLUSTRATED]