Steele

Five Ways Your Conflict of Interest Process is Creating Risk

One Sansome Street. Suite 3500, San Francisco, CA 94104
info@steeleglobal.com

THE STAGGERING COST OF NONCOMPLIANCE.

The risks associated with noncompliance are increasingly debilitating, and expensive. First, what do we mean
by noncompliance? Regulatory compliance describes the organizational goal to ensure awareness of and take steps to comply with relevant laws, polices, and regulations. Noncompliance, then, would be a failure to ensure awareness and take steps to comply with relevant laws, policies, and regulations. For both large companies and small, today's increasingly complex regulatory landscape and the associated costs are becoming harder than ever to ignore.

The cost of noncompliance rose 45% between 2011 and 2017, and that trend is poised to continue. In an analysis of 53 multinational companies located in the U.S. and a survey of executives, the average cost of noncompliance in 2017 was $14.8 million per company.[1] Examples of the items counted among the costs of noncompliance are fines, penalties, business disruption, loss of productivity, and settlement costs. With an increasingly complicated and demanding regulatory landscape, the cost of compliance is rising, as well. Particularly manual, paper-based or inefficient compliance programs. However, noncompliance costs are 2.71 times more expensive than the cost of maintaining or meeting compliance requirements.[2]

Beyond the financial costs, the reputational risks associated with noncompliance are of equally great importance in an increasingly socially conscious world of business. Negative press can harm a company's ability to acquire business, attain grants, retain existing business, and otherwise hurt the company's reputation for years to come.

It follows logically that ensuring organizational compliance is a key priority in risk mitigation. Staying informed, implementing impactful policies, and efficient processes are all key to avoiding risks associated with noncompliance. Conflict of interest (COI) management is no different. An outdated or inefficient process for tracking and dealing with conflicts of interest can be a major contributor to the risk of noncompliance. However, the contributors to risk are not always so clear.

> "
>
> The average cost of noncompliance in 2017 was $14.8 million per company. Noncompliance costs are 2.71 times more expensive than the cost of maintaining or meeting compliance requirements.
>
> PONEMON INSTITUTE LLC & GLOBALSCAPE
>
> "THE TRUE COST OF COMPLIANCE WITH DATA PROTECTION REGULATIONS"

1) LOW RESPONSE RATES

Low response rates and lengthy response times from employees who have a requirement to complete forms are not uncommon. Unfortunately, this is a contributor to an increased rate of organizational noncompliance and the associated risks. Is it the fault of the employee? Not necessarily. The greatest contributor to poor response rates and lengthy response times is an ineffective process for gathering, evaluating, and following up on responses.

WAYS TO NAVIGATE RISK

Great improvements can be made in both response rate and time by creating a direct and effective process with which to gather, evaluate, and follow up on responses. Some of the common mistakes that lead to low response rates are preventable:

- Failure to solicit enough information or the right information on disclosure form
- Failure to ask the correct follow-up questions in a timely manner
- Not pursuing 100% completion, due to logistical difficulty, or any other complications

The most cost-effective and painless way to avoid these issues is by leveraging technology to establish an automated and dynamic process for distributing and evaluating forms, and following up with employees. Dynamic forms that adjust questions automatically and prefilling forms based on past responses are simple steps with a major impact on efficiency. The correct process will lead to considerably less manual work, and lower risk.

2) MISSED CONFLICTS

A primary purpose of any conflict of interest process is the detection of conflicts. Unfortunately, it's not always that simple. Missing potential conflicts is another large contributor to conflict of interest related risk. There are various ways in which a conflict can be missed, and the most obvious of is a failure to disclose properly. However, conflicts can also be missed even if they are properly disclosed. A few common ways in which conflicts can be missed are:

- A paper process does not notify the appropriate parties of conflicts, often leaving conflicts idle in a stack of papers, instead of being properly acted upon
- Blank entries on forms
- Conflict is difficult to track throughout cumbersome escalation and resolution process

While appearing minor, these examples undermine the effectiveness of a COI process and are unnecessary contributors to risk.

WAYS TO NAVIGATE RISK

As with low response rates, the issue of missed conflicts is another risk that is best prevented by establishing an effective, transparent, and automated conflict of interest process. A few very simple process improvements include:

- Send automatic notifications anytime a conflict is disclosed
- Use an electronic process that requires each field to be filled
- Use a process that makes tracking conflicts fast, transparent, and easy
- Set thresholds and rules that allow technology to identify conflicts
- Change surveys from year to year as your business landscape evolves

The above adjustments are simple, but they can prevent the serious risks of noncompliance.

3) INEFFECTIVE FOLLOW-UP

By maximizing response rates and minimizing missed conflicts, a great deal has been accomplished in ensuring that a conflict of interest process is obtaining the correct information. But now that all of the information is gathered, what's next? Naturally, next in line is mitigation, or effective follow-up. As already mentioned, having the correct information is not enough to absolve an organization of risk. Without timely escalation to the appropriate parties and swift plan of action, a company remains at risk. A few common mistakes that lead to ineffective follow-up are:

- Lack of defined (step-by-step) process for handling conflicts
- Slow escalation of conflict
- Lack of clarity as to who should be notified of the conflict

All of the above lead to confusion, and general ineffectiveness in addressing conflicts of interest.

WAYS TO NAVIGATE RISK

Streamlining the follow-up process and enabling the right individuals to simply and effectively address conflicts are the easiest ways to prevent risk, here. Simple solutions include:

[1] Ponemon Institute LLC & Globalscape, "The True Cost of Compliance with Data Protection Regulations", December 2017
[2] Ponemon Institute LLC & Globalscape, "The True Cost of Compliance with Data Protection Regulations", December 2017

- Establish and define a clear process for conflict follow-up, and ensure that process is used by automating the process
- Customize the process so that the correct individuals are notified of a conflict automatically, so that they may respond in a timely manner
- Regularly track conflicts throughout their escalation to check on progress

The same trends continue to prevail: transparency, automation, and efficient processes are applied to the issue of ineffective follow-up to minimize risk.

4) LACK OF AUDIT TRAIL

Considering the steep costs of noncompliance, audit can be a scary word. But that is precisely why having a strong audit trail is extremely important. An audit trail will provide record of processes and behavior that could save millions of dollars in the event of an audit. Manually, creating an audit trail can be strenuous, time consuming, and expensive. For these reasons, the most cost-effective way to maintain a strong audit trail is to do so automatically.

WAYS TO NAVIGATE RISK

It's been established so far that a manual conflict of interest process, or an inferior software solution, complicates the COI process and often adds unforeseen risk. An audit trail is inherently risky and difficult to maintain using outdated processes, but the same strengths that make an ideal COI process effective also make it simple to build an audit trail: transparency, automation, and efficient processes. With good policy, established process, and automation an electronic conflict of interest process will generate its own audit trail. Examples of this in action may include:

> "Infractions of compliance standards can lead to all sorts of negative business outcomes like lost contracts, penalties, and even fines. Audit trails can help to avoid these infractions."
>
> ADAM BLUEMNER, "CATASTROPHIES A GOOD AUDIT TRAIL CAN HELP YOU AVOID",
>
> SOFTWARE CONNECT, AUGUST 2014

- Having a process that tracks the time of a conflict, and any changes in status, is a means of ensuring that all details are tracked and that the decisions made are based on the best information available.
- Automated systems can track key dates that disclosures were made, as well as provide an opportunity to update compliance documents in real-time as their situations change
- Automated systems store information year-over-year. This ensures that users can update existing responses, rather than relying on memory of what they entered previously. This ensures no details are lost over time.
- Automated systems also keep track of which person within a company took action on submitted forms, or determined the management plan for a potential conflict. This allows for better follow up with all related parties as time goes on

Assurance that you have an audit trail in place will pay dividends in the future.

5) LACK OF SECURITY

To many, information security looks to be governed by an ever-changing plethora of laws, policies and regulations; each somewhat relevant and apparently originating in a different jurisdiction. If it appears complex, that's because it is."[3] The news is never short of data breach horror stories, and the protection of data has reached a regulatory landmark with GDPR. It's never been more important to ensure that the compliance process protects delicate information. And it's never been more costly to ignore information security.

WAYS TO NAVIGATE RISK

Compliance protocols and the conflict of interest process are by nature subject to exposure to sensitive information. It is extremely important for the conflict of interest process in place to adhere to current information security regulation. And, as evidenced by GDPR, it's extremely important for the COI process to be prepared to protect data adherent to new regulation. A basic checklist of data security might include the following questions:

- Is information secure?
- Is information encrypted?
- Is the hosting facility ISO certified?
- Is the current process ready for GDPR?

If any answers to the above questions are unclear, the likelihood of risk is increased. Performing the due diligence to guarantee that every step has been taken to protect data is no longer a business luxury; it is a necessity.

COI RiskManager™ - MITIGATING THE COST OF NONCOMPLIANCE.

In the five examples above, we have looked at five common ways in which an outdated or inefficient process for tracking and dealing with conflicts of interest can be a major contributor to the risk of noncompliance. With the costs of noncompliance rising so dramatically (45% between 2011 and 2017[4]) it has never been more important that those responsible for managing risk and ensuring compliance stay ahead of the curve. And while satisfactorily maintaining compliance across an entire organization can be tricky in a constantly evolving regulatory landscape, your conflict of interest process should not be an area of concern. Although manual-based and outdated software solutions will only serve to increase risk and lead to time lost, a powerful, simple, and comprehensive conflict of interest solution will greatly mitigate risk while also saving considerable time and headache. ensuring the highest degree of mitigation for costly COI related risks.

COI RiskManager™ is a powerful web-based solution that efficiently captures disclosures, automatically identifies potential conflicts, and provides reviewer workflows to quickly mitigate issues for any size organization, across many industries. By using COI RiskManager™, organizations obtain the highest compliance levels from their users while fulfilling industry regulations through auditable best practices. Click here for more information about COI RIskManager™.

Click Here For More Information About COI RiskManager™

[3] Infosec Institute, "A Look at Data Security Compliance and Regulations by Industry", January 2018
[4] Ponemon Institute LLC & Globalscape, "The True Cost of Compliance with Data Protection Regulations", December 2017

ABOUT STEELE COMPLIANCE SOLUTIONS, INC.

Steele is the global leader in Ethics & Compliance Management. We partner with the world's largest, most respected companies to deliver compliance products and services that help organizations embrace a culture of compliance while protecting their brand.

Steele

Steele
Worldwide Headquarters
One Sansome Street
Suite 3500
San Francisco, CA
94104 USA

+1 (415) 692-5000
info@steeleglobal.com
www.steeleglobal.com