SCCE
corporatecompliance.org

Compliance & Ethics PROFESSIONAL®

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

FEBRUARY 2018

The Red Flag Group

The Red Flag Group raises the bar with support from the Academies

see page **18**

by Leigh Faugust, Esq., CCEP

An enforcer's view of compliance

» A robust compliance program is one that not only identifies issues but also addresses the nature, extent, cause, duration, and mitigating activities that must be completed to prevent recurrence.
» Strong internal controls reduce the risk of non-compliance.
» Compliance programs must emphasize finding issues and reporting them quickly and accurately.
» A company can only solve a problem if it understands what caused it.
» Mitigation should address these questions: How did this happen? How can it be prevented from happening again?

Leigh Faugust *(lafaugust@gmail.com) is Enforcement Counsel at a not-for-profit international regulatory authority in Washington DC.*

Finding a problem, assessing the risk and cause of that problem, and addressing and preventing recurrence of that problem are key factors in establishing an effective compliance program. I have had a unique perspective on internal controls related to compliance at the end of the life cycle of non-compliance. Although I have personally reviewed thousands of instances of non-compliance, few of these have posed a serious risk. Companies with robust internal controls find problems early, address those problems, and prevent repeat issues, thereby — most importantly — reducing the risk those problems may pose.

Faugust

Identifying non-compliance

"Sense and deal with problems in their smallest state, before they grow bigger and become fatal."

— Pearl Zhu

When considering an internal compliance program, the first question I ask is always, "How did the company discover there was an issue?" If an entity's internal compliance program cannot find a problem, then how good of a program is it? Compliance programs must put an emphasis on finding issues and encourage company employees to report non-compliance quickly and accurately. If a culture does not encourage identifying issues, or inadvertently incentivizes hiding non-compliance to protect financial gain or for other reasons, there can be only bad results.

A company that truly wants to create a culture of compliance will encourage its employees to proactively identify potential issues. A program could include a variety of methods of detection. These may include regular internal reviews, hiring external compliance professionals, or performing spot checks of records and procedural documents to identify areas of concern. Many companies perform internal reviews when they know a regulator audit is approaching, but the companies that review on a regular basis, regardless of audit schedule, receive the greatest benefit — both in improving culture and, potentially, from reduction or elimination of regulator sanctions.

When a company identifies a problem, a robust compliance program must determine the full scope of that problem. If investigating and determining the extent of the condition would prevent notifying its regulator in a timely manner, then the entity could perform this step later as part of mitigation. No matter if the company determines the extent of condition at the time of discovery or through mitigation, reviewing the following helps ensure a full picture:

- Other facilities across the corporate structure;
- Procedures, assets, facilities, or personnel that could be affected as part of the non-compliance;
- Whether other regulations were violated based on the facts of the identified issue;
- Prior compliance history; and
- Additional instances discovered during mitigation.

Assessing non-compliance

"We must accept human error as inevitable — and design around that fact."

— Donald Berwick

Once a company knows there is a problem, it should begin the process of ensuring a prompt mitigation and prevention of recurrence. To do this, it should identify the scope of the issue and consider all procedures, assets, facilities, or personnel affected by the issue. The best way I have seen to make sure a problem is properly contained and recurrence is prevented is to perform a root cause analysis. Focusing on the identification and correction of the root cause of a problem, instead of simply addressing its symptoms, helps prevent that problem from recurring. A root cause analysis should first clearly articulate what happened, when it happened, and why it happened; then it should examine investigation files for clues on how the issue developed. Finally, it should determine the cause of the non-compliance. Companies should consider at a minimum the following:

1. What was the sequence of events that led up to the issue?
2. Why did the issue develop as it did?
3. Is the identified sequence of events logical, and does it represent an accurate picture of what happened?
4. Is this issue just a symptom of a potentially larger problem?
5. With respect to the cause of the issue, were there extenuating circumstances?
    a. Was it the result of intentional, negligent, or inadvertent behavior or action?
    b. Was the company trying to comply in good faith?

In my experience reviewing companies' identified root causes, many conclude with the same thing: human error. The problem with stopping at the individuals involved is that it does not prevent similar mistakes in the future. Therefore, a fundamental part of a compliance program is designing controls that accept that humans will make mistakes. Then, the causes of non-compliance can be better identified as, what allowed a person to make this mistake? Addressing that question would then prevent recurrence of the issue in the future, regardless of the staff involved.

Preventing recurrence of non-compliance

"An ounce of prevention is worth a pound of cure."

— Benjamin Franklin

Once a company has found and assessed the risk and cause of an issue, it is in the position to prevent the issue from occurring again. The best method I have seen for ensuring mitigation and remediation of a problem is to create a mitigation plan. The plan could be a formal written document that includes milestones and dates for completion,

or it could be a relatively informal list of how to address the causes for the violation the company has identified. Either way, a company should design its mitigation plan to address the risk posed by non-compliance, as well as identify controls and corrective actions to reduce the likelihood of a future occurrence.

A company should design its corrective actions to mitigate non-compliance and restore compliance as quickly as possible. Corrective actions should directly address the root causes. For example, if the entity determines the root cause is human error because personnel were unaware of some policy or procedure, it should ensure that procedures are documented and training on updated procedures is provided. During mitigation, a company should address any risks of the cause and violation until mitigation is completed.

The last step in assessing the violation is to determine the likelihood of recurring non-compliance. Evaluating its own compliance history will provide an understanding of whether prior mitigation was deficient. When a company evaluates mitigating factors for non-compliance, it should consider:

1. Whether the cause of the problem is the same or similar as prior problems.
2. Whether the circumstances surrounding the issue are rare or common.
3. What steps are already in place to address the issue?
4. What steps should be put into place to prevent it from happening again?

Putting it all together

"Checklists remind us of the minimum necessary steps and make them explicit. They not only offer the possibility of verification but also instill a kind of discipline of higher performance."

— Atul Gawande

A robust compliance program is one that not only identifies issues but also addresses the nature, extent, cause, duration, and mitigating activities that must be completed to prevent recurrence. The following are some of the considerations I go through when reviewing actions taken to identify, assess, and correct non-compliance.

- Did the compliance program find a problem that otherwise I would not have found (i.e., through either a scheduled or random identification outside of preparation for a regulator audit or other compliance monitoring activity)?
- Did the compliance program include an extent of condition review to find out the scope of the problem?
- Did the compliance program include a root cause(s) analysis and find any other contributing factors?
- Was there a thorough assessment of the risk of not only the problem at hand but also of the root causes and contributing factors? Was that assessment of the risk accurate, and does it take a holistic view of the entity and the circumstances of the violation?
- Is there a mitigation plan to address the problem?
- Does the plan include correction, detection, and prevention?
- Do the actions included in the plan address cause and risk?
- Has any interim risk of the cause been identified and addressed during mitigation?
- Has any future risk of recurrence been described and addressed? ✳

The views and opinions expressed in this article are mine alone and do not reflect the official or unofficial policy or position of my employer. Any examples discussed are hypothetical in nature, and any similarity to specific non-compliance is unintentional.