NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS Currents June 2018

# How to Master the Annual Review and Promote a Culture of Compliance

*By Elizabeth Cope*

## A 3-Part Guide for CCOs

Being the Chief Compliance Officer ("CCO") is tough. You are the "NO" person; the "You did that wrong" person; the "You have to report everything to me" person. Your job is critical…and full of liability.

You are one of the people expected to lead the firm with a strong culture of compliance and collaborated to ensure written policies and procedures are in place. You are also responsible for assessing the adequacy and effectiveness of those policies, at least annually, in the form of an annual review.

How to Master the Annual Review and Promote a Culture of Compliance is Part 1 of a 3-part series in which you will learn how to develop an annual review to work for you instead of against you, how to make it realistic to implement and manage, and how to make it support the operations and ever-changing needs of your firm, as opposed to being just another thing you have to do to meet regulatory requirements. This series will cover, step by step, how to develop your risk assessment, how to decide what needs to be tested, how to schedule when the testing occurs, how to document your testing, and how to present that documentation to the regulators.

## The Joy of the Annual Review

I know it's a requirement, but the annual review is actually a great tool. If set up correctly, it not only serves as your compass to make sure your firm is in compliance, it can help your firm:

1. promote a culture of compliance,
2. create operational efficiencies,
3. bring to light areas where practices among employees are inconsistent,
4. identify where you may benefit from elaborating more on your policies or refining your procedures, or
5. identify where you may benefit from providing additional compliance training to your employees.

The annual review, in essence, is a big project. It requires all elements of project management, including initiation, planning, execution, monitoring, and closing. The process and the underlying requirements are the same from firm-to-firm, but the application, organization, and specific tasks involved in an annual review differ, depending on the nature and size of the firm. Therefore, it is essential that your annual review be "customized," and it is vital that it be "practical."

This three-part guide will help you develop an effective annual review program, tailored to your firm.

## The Importance of "Customized" & "Practical"

First things first. It is crucial that your annual review process be practical. By **practical**, I mean simple, effective, functional, and useful. The key is to develop a system that…not only meets the expectation of the regulators and third parties…but also **works for your firm and increases buy-in from your personnel**. It needs to be a **customized** system that not only you, as the CCO understand, but that personnel at the firm—especially the principals who are guiding the compass of the firm—understand and adopt. When people know "WHY" something is the way it is, they are more likely to get on board and stay on board, which will actually make your job much easier.

You like simplicity, right? Another way to improve buy-in is through **simplicity**. The system you develop for your annual review doesn't have to be overcomplicated. In fact, *I* **urge you** not to overcomplicate your processes. Less is often more, and SIMPLE is often better!

***About the Author***
**Elizabeth Cope** is Managing Member with SEC Compliance Solutions, LLC. She can be reached at liz@seccsllc.com.

Now that you understand "why" a *customized, practical* annual review is indispensable, let's get started on the "how!" We've tried to make it simple for you…

## Part 1: Create a Risk Assessment.

The Risk Assessment will drive the entire annual review process. To make this easy for you, I have attached a template in Microsoft Excel. You don't have to use Excel but if you're starting from scratch, you may consider it as it's easy, almost everyone has it, and you can do quite a bit with it. If not, you can certainly use other tools or technology to develop your risk assessment, but the same principles should be considered. Remember, keep it "practical." Just use a system and method that makes sense to you and your firm.

### Step 1: Identify the Risks

Identify the potential risks your firm may incur as a result of the services being offered. If you are unsure of the risks, sit down with the people doing the work, talking to clients, and making the trades. Ask them where they think the risks are. Document this.

In the template provided, this step is in Column A. You will see we have already identified examples of potential risks advisers may incur. You may take these into consideration as you develop your own risk assessment. I suggest only including risks applicable to your firm. For example, if you do not engage in soft dollars, you do not need to address those items as potential risks. (Keep it simple.)

| RISK ASSESSMENT |
|---|
| **Risks** |
| **Compliance Oversight** |
| (Example: Compliance officer and compliance staff are not aware of rules and regulations) |
| (Example: General staff is not aware of rules and regulations) |
| (Example: Roles and responsibilities of Firm personnel not clearly defined) |
| (Example: Staff has disciplinary history that has not been disclosed) |
| (Example: Outside Business Activities are not properly disclosed) |
| (Example: emails violate with firm policies) |

At the very bottom of this template (starting on Row 161), you will see a section to identify the potential conflicts of interest. These will be identified as a result of the overall risk assessment. The key is to make sure any identified conflicts are disclosed fully and fairly to clients. I suggest taking a moment and putting yourself in the shoes of your clients or potential clients. What kinds of conflicts would you be concerned about? What would you want to know if you were investing your money? The SEC has made it clear that advisers don't have to avoid all conflicts, but they do have to make full and fair disclosures so that investors can make sound decisions.

### Step 2: Assess Risk Level

It is not a requirement to identify the level of risk associated with the risks you identified in Step 1. However, doing so, provides guidance for the type and frequency of testing you conduct for your annual review. An item that is of high risk will most likely require a higher priority level of review (i.e., perhaps conducted more frequently, or using a larger sample size, or a deeper, more in-depth review). You will see in Columns B and C of the provided template, we suggested two methods for assessing the risk level. We suggest rating risks in two categories a) the likelihood of this risk actually occurring, which can be based on past experiences and b) the impact should this risk occur. This can be rated as high, medium, low or 1, 2, 3, etc.

| **Probability** that the risk will occur (High, Medium, Low or 1 = Low, 5 = High) | **Effect** the risk would have on Firm's business (High, Medium, Low or 1 = Low, 5 = High) |
|---|---|
| | |
| H | M |

When you are first starting out, go with your initial gut feeling, following discussions with the team. Then let the results of the annual review guide your updates for the coming year (i.e., if you find a significant amount of violations, then that area would most likely be high risk for the likelihood of occurring).

### Step 3: Document the Controls and Map the Controls to Your Policies

A very common fault that advisers have in their exams is having policies and procedures in place that are not consistent with the firms actual practice or that are not "reasonably" designed to mitigate the risks at the firm. That is why I have broken this up into two areas (1) document the controls and (2) map the controls to your policies and procedures.

**Document the Controls**

This is Column D of the template. For each risk, document the control in place to mitigate that risk. How? Talk to your people and document what they actually do; get their input and involvement. This is another opportunity for you to get them on board with compliance and to explain the "why." This is where they have the opportunity to let you know what is practical and what is not, understanding that there are items (such a personal trade reporting) where there is not a lot of flexibility. Together, you can compromise on procedures that not only satisfy the regulators' expectations and rules but are also practical for your employees. Getting personnel involved in developing compliance processes and keeping them practical helps ensure that the policies and procedures can and will be followed.

**Map the Controls to Your Policies and Procedures**

This is Column E in the template. The purpose of this field is to reference the location and title of the identified policy. For example, for the first risk identified in the template, "Compliance officer and compliance staff are not aware of rules and regulations," I would reference the section of your manual that discusses ongoing training and responsibility to stay current with federal securities laws.

This is a great exercise to identify any gaps in your manuals and make updates where necessary. If you do not have controls and policies and procedures in place to mitigate the identified risk…develop them!

**Step 5: Identify Responsible Persons/Departments**

Identify the individual(s) and/or departments responsible for overseeing and adhering the identified controls and policies and procedures. In many cases, there may be more than one. This will help streamline accountability in the firm. This is Column F.

**Step 6: Changes to Risk**

Review your risk assessment no less than annually. If violations occur or when new rules are implemented, systems change, or people change, this is the time to assess changes to the overall risk, which trickle down to the controls, policies, procedures, and personnel. This is noted in Column G of the template. We suggest noting why a specific area was change. For example, an adviser might assess "Compliance officer and compliance staff not aware of rules and regulations" as High for both probability and effect because the firm is newly registered. After a year of being registered, administering the annual review, and undergoing training, they could assess this to a lower risk level and then document why the change.

**Step 7: Comments**

This column, Column H, is an optional field. Only update it if it adds information you feel is relevant to your overall assessment.

## Summary

Even though the annual review is a regulatory requirement, it has a lot of benefits that can serve your firm in a positive way and make YOUR job as the CCO much easier. If implemented and reviewed with firm personnel, it can also serve as a tool for promoting a culture of compliance and getting your team onboard with consistently carrying out the practices that adhere to your firm's compliance-related policies. Therefore, it is essential that you customize your annual review to your firm's unique operations and make your annual review as simple and practical as possible.

The first step in tailoring your annual review to your firm is to (1) thoughtfully consider your firm's risks, (2) estimate the likelihood of each risk occurring as well as how serious the effect would be if it did, (3) document the controls your firm has in place to mitigate those risks, (4) map the risks to your written policies and procedures, (5) identify the individuals or departments responsible, and (6) review your risk assessment at least annually, but also after any material change in your firms operations, personnel, or products/services, as well as whenever rules or guidance are implemented or amended.

**You have the power to master the annual review!**

We hope you join us for Part 2 of How to Master the Annual Review and Promote a Culture of Compliance, which will be published in the July 2018 issue of NSCP Currents. Part 2 is all about testing and reviews. You will learn how to (1) set the testing schedule, (2) define the scope of the testing, and (3) document the results. See you in July!

DOWNLOAD EXCEL FILE