

# COSO and the GAO Green Book are the same thing

JANUARY 18, 2019

## Objectives

- **Identify the purpose of the GAO's Green Book**
  - **Identify the standard setting bodies that are involved in the creation of the GAO Green Book**
  - **Identify reasons why most organizations do not achieve the ideal internal control structure described in the GAO Green Book**
- 

GAO Green Book, GAO Yellow Book ... will the Government Accountability Office (GAO) never cease creating books with colored covers? Next thing you know, it will come out with a Purple Book!

The GAO Green Book's formal title is *Standards for Internal Controls in the Federal Government*. The Yellow Book is also known as *Generally Accepted Government Auditing Standards*. Are you sleepy after reading those long titles? If you are like me, you are grateful for the simpler, color-oriented monikers of these important pieces of professional government literature.

The GAO Green Book presents a comprehensive model that professionals can use to both create and audit controls. The latest GAO Green Book was published in 2014 and is available online here: <http://www.gao.gov/greenbook/overview>.

In this text, we will use the GAO Green Book's model to design controls over the use of credit cards in a government entity. In early chapters, I occasionally will mention the auditor's perspective on controls. But we will learn more about controls if we endeavor not just to *evaluate* controls as auditors do but, instead, to *create* them from scratch as managers must do.

At the end of the book, we will switch gears and look at controls from the auditor's perspective and design tests of controls.

But before we get too far along with our case study, let's look at how the GAO Green Book came into being and find out whether your organization should be using it. As we will see, the Government Accountability Office (GAO) bases the

Green Book on a model of internal control created by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

**The GAO pushed for better controls in 1983.**

The GAO is the legislative auditor for the federal government. In addition to auditing federal agencies and reporting the results back to Congress, it also advises executive agencies on how to make government more efficient and effective. The Federal Managers Financial Integrity Act of 1982 requires the Government Accountability Office (GAO) to establish standards for internal controls. The GAO made its first efforts toward creating a standard for internal controls in 1983.

In the opening letter to this first version of the GAO Green Book, the Comptroller General of the GAO said:

*In the past decade, numerous situations came to light that dramatically demonstrated the need for controls as the Government experienced a rash of illegal, unauthorized, and questionable acts which were characterized as fraud, waste, and abuse. It is generally recognized that good internal controls would have made the commission of such wrongful acts more difficult. Consequently, increased attention is being directed toward strengthening internal controls to help restore confidence in Government and to improve its operations.*

I wonder what the Comptroller General would think of the hijinks in the government realm in the past 30 years!?!

**Congress pushed for better controls in 1977, and the Treadway Commission was formed.**

Only six years before the Financial Managers Financial Integrity Act, corporate fraud was getting the attention of Congress. In 1977, Congress enacted the Foreign Corrupt Practices Act (FCPA) as a result of 400 US corporations admitting that they had made questionable or illegal payments to foreign officials as part of conducting business in other countries. In response, the Treadway Commission, a private-sector initiative, was formed in 1985 to inspect, analyze, and make recommendations on fraudulent corporate financial reporting.

### **The COSO Report was issued in 1992.**

As a result of the Treadway Commission's initial report, the Committee of Sponsoring Organizations (COSO) was formed. COSO retained Coopers & Lybrand, a major CPA firm, to study the issues and create a report on controls. This report was titled Internal Control – Integrated Framework and was issued in 1992.

And for the first time, we were introduced to the COSO cube that many of us use in our work today.

Over time, the COSO model, as it came to be called, was integrated into various auditing standards including the American Institute of CPAs auditing standards, the GAO's *Generally Accepted Government Auditing Standards* (the aforementioned Yellow Book), and the Institute of Internal Auditor's professional literature.

### **The COSO model evolved.**

The Institute of Internal Auditors (IIA) didn't just accept the COSO model as is: in 2004, they added to and enhanced the model and renamed it the Enterprise Risk Model. We will look at the Enterprise Risk Model in more detail later because it has some features that will help us understand the risk assessment portion of the Green Book.

### **SOX renewed interest in the COSO model in 2002.**

After a parade of corporate financial scandals (Enron, WorldCom, etc.) at the turn of the century, Congress passed the Sarbanes-Oxley Act (frequently referred to as SOX) in 2002. The Sarbanes-Oxley Act requires that publicly traded companies in the United States certify that their internal controls over financial reporting are effective. Most corporations used the COSO model as the framework to guide this assessment.

### **The COSO model and report were revised in 2013.**

The COSO model was revised in 2013, more than 20 years after its initial creation. The 2013 revision didn't alter the cube very much; the side of the cube now uses the term "division" instead of "unit," and a few titles were changed on the face of

the cube: "financial reporting" on the top of the original cube was changed to the more broad "reporting," and "monitoring" was changed to "monitoring activities." The side of the cube now uses the term "division" instead of "unit."

These changes are minor compared to what COSO did to the text of the report. The original 1992 COSO report was presented in narrative form using lengthy complex paragraphs. The 2013 version breaks each of the five elements on the face of the cube into 17 principles, and then these principles are further broken into 81 points of focus. Breaking down the narrative into smaller, more digestible concepts makes the document much easier to scan and, thus, to use.

The 2013 version of the COSO model is available online for \$99-270, depending on whether you want a piece of the document or the entire set of literature.

### **The GAO published the Green Book in 2014.**

In September 2014, the GAO revised the Green Book. The 2014 version replicates the 2013 version of the COSO model but changes some terminology to customize the model for the government environment.

### **Is the GAO Green Book required?**

So now that you know the history of the GAO Green Book, we can address whether you have to use it. And to understand that, we need to know whom you work for.

If you work for a federal executive agency, your agency is required by the Financial Manager's Financial Integrity Act to report each year on the status of internal controls. And the GAO Green Book is the benchmark that your agency is likely to use in this evaluation. However, federal agencies are not required to ensure that their controls meet every internal control standard described in the GAO Green Book.

If you are a grantee, you should consider the following paragraph from the *Uniform Administrative Rules, Cost Principles, and Audit Requirements for Federal Grants* issued in 2014 (bolded print added):

### *200.303 Internal Controls*

*The non-Federal entity must:*

*(a) establish and maintain effective internal control over the Federal award that provides reasonable assurance that the non-Federal entity is managing the Federal Award in compliance with federal statutes, regulations, and the terms and conditions of the federal award. These internal controls should be in compliance with guidance in "Standards for Internal Control in the Federal Government" issued by the Comptroller General of the United States and the "Internal Control Integrated Framework" issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).*

Notice that the introductory clause to that paragraph says "must," and then, within section (a), it says the non-federal entity (read that as grantee) "should" be in compliance with the Green Book. Now the combo of this "must" and "should" statements may make you think, as I did when I first read it, that grantees *must* apply the Green Book in designing and implementing their internal controls.

But per a question and answer document from COFAR (Council on Financial Assistance Reform, who are the creators of the Uniform Administrative Rules, Cost Principles, and Audit Requirements for Federal Awards), the word "must" does not apply to that sentence about the Green Book. Only the word "should" does. And to the federal government, "should" is not mandatory but, instead, simply a best practice.

Are you confused? Join the club! Often it seems like the federal government's job is to prevent intelligent humans from comprehending their writing. The bottom line is that in the government realm, the Green Book is used as a benchmark for controls, not a mandatory requirement for controls.

**COSO is a little stricter.**

I feel I should repeat a few things before I show you a bold statement from the COSO organization. First of all, please remember that COSO is not the same entity as the GAO. And the GAO borrows the COSO model to create the Green Book but does not go along with everything COSO says.

Secondly, it is very unlikely that COSO has any authority over you. For it to apply, your organization, or the standard-setting body to which your organization adheres, must adopt the COSO internal control model.

For instance, if you are a publically traded corporation and subject to the Sarbanes Oxley Act, you might have adopted COSO as your control model. But a publically traded corporation may have easily adopted another control model, like COBIT (Control Objectives for Information and Related Technology).

Or, if you are an audit organization following the AICPA auditing standards, you are required to use the COSO model to evaluate internal controls. But this does not mean that the audit client is required to apply it in the creation of their internal controls.

Now that I have made it clear that this is a statement from COSO and not the GAO and that COSO likely has no authority over your controls, here is that high and mighty sentence from the 2013 COSO Executive Summary:

*When a major deficiency exists with respect to the presence and functioning of a component or relevant principle, or with respect to the components operating together in an integrated manner, the organization cannot conclude that it has met the requirements for an effective system of internal control.*

My mouth fell open when I read that sentence! (And yes, it is one sentence if you thought about checking it again.) That long sentence sets a very high bar as you will see when you travel through this book.

If you are like most people, the internal controls described in the Green Book are more than a little overwhelming and years away from being a reality in your organization. As you read the rest of this text, I suggest that you imagine the day when the Green Book makes a similarly bold statement and think about whether you could meet that expectation.

### **The Green Book describes control nirvana.**

The GAO Green Book lays out an ideal control structure – a nirvana for internal controls, if you will. And I have never encountered any entity that has achieved this ideal. Yes, I've seen some entities achieve control nirvana in some part or aspect of their business. But I have never seen an entire entity under complete

control, and I doubt I ever will. In my experience, implementing the COSO model/Green Book for just one piece of an entity's operation is rare. And I think that is a reasonable state of affairs.

So before we start dissecting the Green Book and seeking to meet its ideals, I want to take a few minutes to ground us in reality. I have a few stories that should do the trick. One is about Paco's Tacos and McDonalds and one is about controls in my similarly tiny little business. First, let's talk about Paco's Taco's and compare it to a few restaurants I've patronized.

### **McDonald's**

If you have been to Austin in the past 10 years, you realize how crowded my hometown has become. Over the years, my commute to downtown at 8 a.m. has increased by 45 minutes. The Austin economy is great; the traffic is horrific.

In order to avoid the ridiculous traffic when teaching at the University of Texas or a state agency downtown, I leave the house an hour early and have breakfast and put on my makeup at a restaurant on MLK Boulevard. MLK Boulevard divides the UT campus from the state capital and offers a variety of breakfast options including McDonald's, Taco Cabana, and a little locally owned Mexican restaurant I will call Paco's Tacos. (Paco's Tacos is not the real name of the restaurant, and you will see why I changed the name in just a bit).

On mornings that I am emotionally fragile and tired, I head straight to McDonald's in order to minimize upset and frustration. I eat at McDonald's quite a bit when I am on the road because I can count on their consistency and speed. I am pretty sure I ate the exact same biscuit with bacon in Alaska that I ate a few weeks later in Manhattan. The exact same biscuit! (Of course, I cannot prove that.) No matter where I am (and I have visited 48 states), my McDonald's breakfast is always in my hand and correct within five minutes of my order. This is an absolutely amazing feat!

How does McDonald's make my experience of their restaurants, nationwide, so consistent and, therefore, so comforting? Did I hear you say, "internal controls?" Yes, McDonald's is one of the most controlled businesses I have ever encountered.

And that recurrent biscuit is not the only proof I have of their strong controls. My husband is a Diet Coke fanatic, drinking two liters a day, easy. Yes, I have expressed my concern for his health over this choice. But after years of resisting his habit, I have now become an enabler.

I sometimes stop at McDonald's on the way home and get him two large Diet Cokes. And as a true soda addict, he wants more soda than ice in his cup. Once I asked through the drive-thru speaker whether I could get less ice and more soda, and the answer was, "No. Your total is \$2.16. Pay at the first window." It turns out that the soda cup travels along a conveyer belt, and a measured amount of ice and soda is automatically put into each cup. The attendant only has to place the lid on the cup. Wow. That is controlled.

Because I am an accountant, I know that this means that someone in the McDonald's corporate offices has created an Excel spreadsheet analyzing the most profitable and customer-pleasing ratio of ice to soda. Does their entire organization suffer from OCD? (I saw a t-shirt recently that said, "I am CDO. It is like OCD, except the letters are in the proper alphabetical order!")

### **Paco's Tacos**

Now contrast McDonald's to a neighboring restaurant, Paco's Tacos. I tried Paco's Tacos a few times because our weekly arts and entertainment paper, The Austin Chronicle, gave it a good rating and mentioned the fabulous refried beans. Any refried bean aficionado will tell you that good refried beans are cooked with pork lard. No vegetarian, low-fat refried beans will suit this Austinite!

So I went to Paco's for breakfast one morning, and indeed their beans were good – really good. But nothing else was. My huevos rancheros came out all wrong, and it took them a half-hour to get my order to me.

But because the beans were so delicious, I went back a second time. But this was also my last visit because my order was wrong, it was late, and it was served by a man who had been sleeping on the street only an hour earlier. I might have been able to tolerate his smell and disheveled clothes, but what I couldn't tolerate was the deep gash on his nose that needed stitches. I paid my bill without touching my meal and ran through the drive-thru at McDonald's to grab that same old biscuit.



Plotting McDonald's and Paco's Tacos on a scale rating their internal controls that spanned from 0 to 5, McDonald's is a 5 and Paco's is a 0 or a 1!

### **The internal control rating scale 0-5**

- 0** – nonexistent: internal controls are not applied at all
- 1** – initial: controls are ad hoc and disorganized
- 2** – repeatable: controls follow a regular pattern
- 3** – defined: controls are documented and communicated
- 4** – managed: controls are monitored and measured
- 5** – optimized: good control practices are followed and automated

### **The case of Taco Cabana**

If you have never experienced Taco Cabana, then you are missing out. Think of it as a Taco Bell with margaritas and beer.

Because breakfast at Taco Cabana is tasty and interesting, I am willing to tolerate flaws in their internal controls system here and there. One morning, my huevos rancheros were topped with a cold pico de gallo instead of a warm ranchero sauce, they were out of napkins another morning, and I once drove away with coffee in my iced teacup. I could go on. It isn't just the food that gets messed up; they have money issues as well. The corporate office would probably like to know that the beautiful lady that works the cash register might give you an \$8 meal for \$3 if you chat with her about her kids.

Taco Cabana is a 3 on the internal control scale. They have written policies and procedures, and everyone knows what they are supposed to do, but it doesn't get done all the time, for one reason or another.

Personally, I don't think there is anything wrong with being a 3. I wish I were a 3 in more areas of my business.

### **An embarrassing story about me**

I would like to be able to brag and say that I have never messed up or harmed any of my clients due to weak internal controls. But I can't. As a matter of fact, a few years ago, I experienced a failure of epic proportions. OK, I didn't threaten the welfare of humanity, but it felt epic to me!

I was sitting in the Austin airport on a Monday morning preparing to board the airplane when I got a call from my client in Kentucky. I was traveling to see them because my calendar said that I was to teach two full-day seminars for them on Tuesday and Wednesday. My client had called to ask me if I was lost! My heart sunk, and I felt sick to my stomach. For over 17 years, I had never missed a seminar. But I was missing this one because I messed up the dates on my calendar.

I was getting busier than I could handle alone, and I was making little errors here and there that should have clued me in that I was headed for big trouble. And big trouble was in the form of 100 people waiting for me to show up to teach a seminar in a city over 1000 miles away.

After bowing and scraping and making it as right as I could with my client in Kentucky, I immediately started putting controls in place. One control was to hire an assistant to review all of my booking and sync them up with my travel reservations. Her suggestion to use the Triplt app has changed my life, by the way.

So, as you can see, I am not a 5! I can confidently rate myself a 3 in some areas of internal controls in my business, and I am a solid 1 in other areas. And I worked hard to get there, thank you very much!

### **Two main reasons we can't reach control nirvana**

And those stories allow me to make a few points about the reality of controls. When you combine the facts that most organizations are more reactive than proactive when it comes to controls and that controls are expensive, you can see why most control systems are pretty patchy and weak.

### **Controls are created because someone messed up**

Just like laws, controls are created when someone does something stupid. Most of us don't have the foresight to think ahead about consider the consequences of our actions or inactions. Most often, we wait until something goes wrong before putting controls in place. Think bike helmets, banking regulations, and the like. I wish I had thought ahead and put controls in place before I missed that gig in Kentucky.

## **Controls are expensive**

Why isn't Taco Cabana more like McDonald's when it comes to controls? And why isn't Paco's Tacos as strong as Taco Cabana when it comes to controls? It's not a matter of will or culture. Much of it ultimately boils down to money.

Although I could really use the help, my assistant doesn't help me pack my clothes when I travel. Recently, I taught a CPE seminar in Beaumont in casual sandals that were only one step up from flip-flops because I forgot my dress shoes!

As wonderful as being perfect in all of our business activities would be, Paco and I can't put controls over everything because we simply can't afford it!

## **Therefore, controls are patchy.**

I am afraid that most controls are applied in a willy-nilly, patchy fashion without any regard to risk. Most organizations' internal controls instead barely hold everything together.

We all know that sometimes putting patches on things doesn't really resolve issues. Issues that are approached systematically and methodically often hold better.

As we will see, looking through the Green Book, the GAO recommends a comprehensive, systematic approach to controls and, thereby, rejects quick fixes and patches. Patches seem cheaper and faster in the short run but, in the long run, you end up with an unwieldy, ineffective bureaucracy that halts operations and progress. Maybe you work in one of those?

## **Where are you on the scale?**

Enough talk about me and Paco. Where is your organization on the internal control rating scale? Where is your specific function on the scale? Maybe you'd give your fellow departments a 2, but award yourself a 4. You are reading this book, which could indicate a higher level of consciousness about controls than the average bear.

No matter what you think you are, the Green Book is here to help you be a 5!