SOX 404: COSO Guidance on Monitoring Internal Control

Webcast Presentation

Presented by:
Trent Gazzaway,
Managing Partner, Corporate Governance
Grant Thornton LLP

About Trent Gazzaway

Trent is an audit partner and the partner-in-charge of corporate governance for Grant Thornton LLP. Trent's experience includes auditing public and private companies and assisting an array of companies in the improvement and documentation of effective systems of internal control. He has also assisted large public companies in the development and execution of plans to restate their financial statements in the wake of internal control failures.

In addition to managing the Firm's corporate governance practice, Trent serves as a key resource in training Grant Thornton personnel to audit internal controls over financial reporting in accordance with newly established auditing standards. He is one of four steering committee chairmen assisting in the development of the Open Compliance and Ethics Group's framework for integrating governance, compliance, risk management and integrity into all business processes (www.oceg.org). Trent is also a member of the advisory board of the Enterprise Risk Management Initiative (www.mgt.ncsu.edu/erm) at NC State University's College of Management.

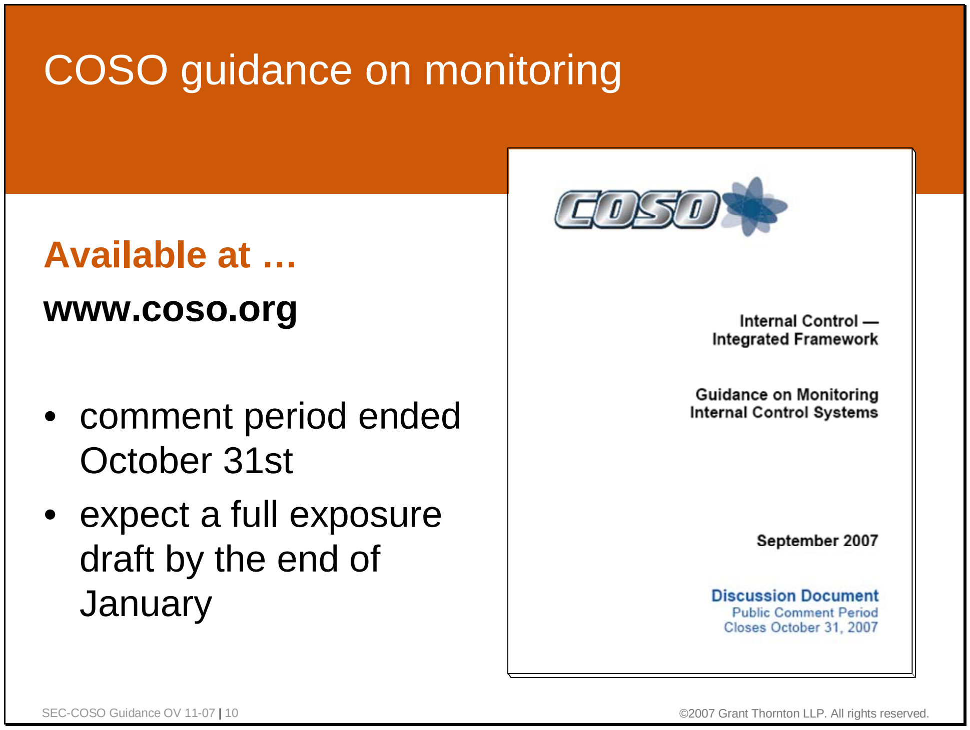
Most recently, Trent was appointed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) board to lead a project to develop guidance regarding the effective monitoring of internal control in accordance with COSO's Internal Control—Integrated Framework.

Trent is a frequent speaker at seminars, has authored several nationally and internationally published articles related to Sarbanes-Oxley and corporate governance, and publishes Grant Thornton's award-winning quarterly Corporate Governor newsletter.

Education
Trent has a Bachelor of Science in Business Administration and a Masters of Accounting from the University of North Carolina at Chapel Hill.

Table of Contents

COSO Guidance on Monitoring Internal Control



We published the COSO guidance in the middle of September as a discussion document for public comment. It wasn't a full-blown exposure draft. This is really a two-phase project. And I'll talk about the two phases in a second, but the discussion document is the first phase. And the comment period for that discussion document ended October 31st. We received a lot of comments. I was pleased with the results of the comment process. There were mostly positive comments, a lot of good, constructive comments, and we're going to go back and make some changes. But the vast majority of the comments didn't result in wholesale changes to our thinking process. A lot of the comments had to do with the structure of the document, and the way we presented it, and wanted us to clarify some points. But I think what you see in the discussion document now — the fundamental thought process — is going to remain true in the final document, based on the comments that we received on the exposure draft. The full Exposure Draft is due to be published in late March or early April.

Primary Goals

COSO guidance on monitoring (cont'd)

Two primary goals …

- help companies recognize effective monitoring when it is already present and "take credit" for it
- help companies identify places where effective monitoring is lacking and provide guidance regarding possible improvements

SEC-COSO Guidance OV 11-07 | 11

There were two primary goals of this project when COSO started it towards the end of 2006. One, there was a recognition on COSO's part that we really needed to improve the understanding of the monitoring component of internal controls. If you know the COSO framework, you know it consists of five individual components, one of which is monitoring. All five components work together to form an effective internal control system. You can't really strip any one of them out and say, ok, this is really the key to an effective internal control system. But COSO did perceive, and I agreed with this, that there really was a lack of understanding of what effective monitoring looks like. In some cases, effective monitoring was taking place in a lot of but companies were not taking credit for it. Instead, they were layering additional, often unnecessary monitoring on top of it. So one of the goals is to help companies recognize effective monitoring where it already exists, take credit for it, and use that effective monitoring in support of their 404 assertions.

The second goal is to help companies identify where effective monitoring may be lacking, and provide guidance to help them correct that, so they can have effective monitoring not only for 404 purposes, but really just for good business purposes. As I mentioned, this was a two-phase project. The first was a proof-of-concept stage, which resulted in the discussion document which was downloaded almost 11,000 times. I don't know how many of you had an opportunity to read through it. I will tell you — and we knew this when we published it — that the first draft was very theoretical, with some practical guidance baked in. What we're going to do in the exposure draft is to visually separate the theory from the practical application concepts. That way readers can quickly read through the practical material, and yet still have the theoretical backing there to support it. We will also have a separate volume of application techniques that demonstrates how some real companies are applying these concepts today.

That's what we're working on in phase two. We're interviewing companies to come up with some practical examples, case studies, tools that companies can use to monitor internal controls, to support, ultimately, their assertions about ICFR.

Ongoing Development

COSO guidance on monitoring (cont'd)

The SEC **encouraged the further development** of control frameworks and evaluation methodologies as technology, control systems and financial reporting evolve.

> "As we have previously stated, the Commission supports and encourages the further development of control frameworks and related implementation guidance."
>
> Source: The SEC's Interpretive Guidance for Management

SEC-COSO Guidance OV 11-07 | 13

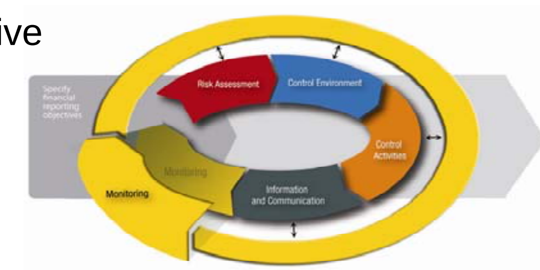
Again, as I mentioned earlier, the SEC encouraged the further development of control frameworks within its interpretive guidance. This is a quote out of that guidance.

Effective Monitoring – Value Proposition

COSO guidance on monitoring (cont'd)

Effective monitoring — value proposition:

- provides management with most of the evidence it needs about ICFR effectiveness to support its assertion
- encourages effective control operation
- helps manage and/or mitigate risk



SEC-COSO Guidance OV 11-07 | 14

The value proposition here in the COSO guidance is that good monitoring can provide management with the evidence it needs to support its assertions and is also just a good business practice of knowing that you have effective internal controls in place. It encourages effective control operation. Then, of course, effective monitoring helps the organization make sure that it's managing or mitigating risk appropriately.

Control Evaluation - Examples

COSO guidance on monitoring (cont'd)

Let's look at a simple example of the concept …

- assume:
  - a reconciliation control is deemed important to financial reporting
  - the supervisor of the area performs an appropriately detailed review of the reconciliation each time it is prepared

SEC-COSO Guidance OV 11-07 | 15

So let's look at a simple example that I think will really highlight what we hope people can get out of the COSO guidance.

Let's assume for a second that an organization has a reconciliation control that is deemed important to the financial report. Assume further that a supervisor of the area performs an appropriately detailed review of that reconciliation each time it is prepared.

COSO guidance on monitoring (cont'd)

Let's look at a simple example of the concept (cont'd) …

- the supervisor's review (if it is effective) accomplishes two things:
  - tells him or her whether the control is working
  - encourages continued effective operation of the control

SEC-COSO Guidance OV 11-07 | 16

Now that review — the monitoring of that reconciliation — really accomplishes two things. The first thing it does is tell the supervisor whether the control is working. That's what monitoring is supposed to do first: tell you whether the control is working the way it was designed to work.

Now, as I mentioned earlier, you ought to read that and say, "Well, that's exactly what 404 suggested, that you need to know that those key controls are working." So the monitoring — the review of that reconciliation as it relates to the risks that that reconciliation addresses — tells him or her whether the control is working.

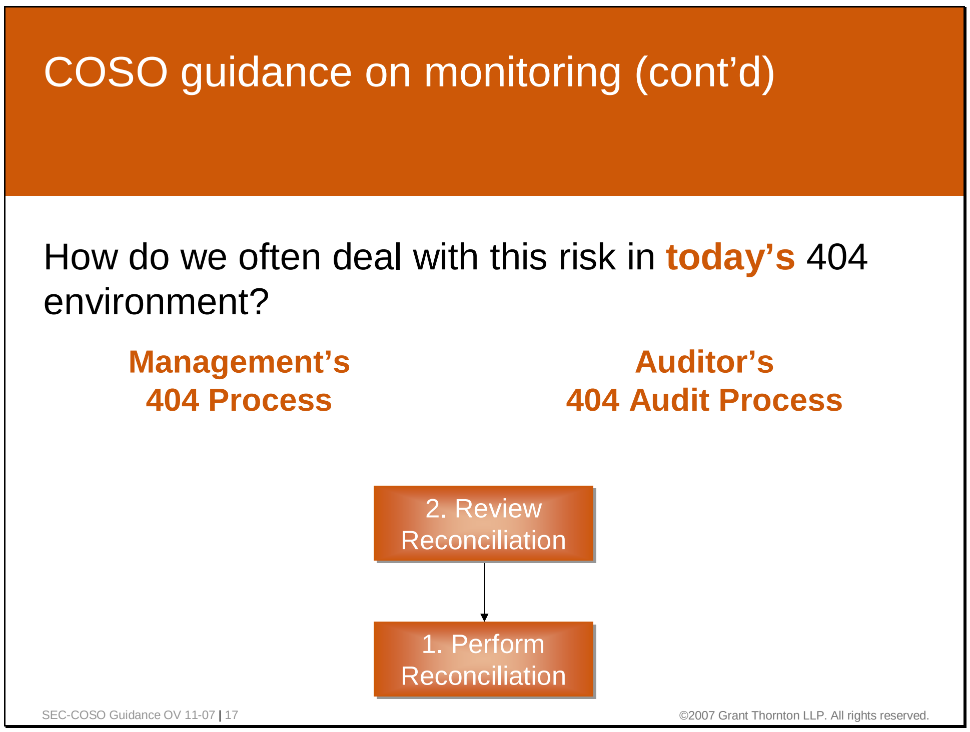
But there is another element that is almost, in my mind, more important. It is at least equally important. And that is that the monitoring actually encourages the continued effective operation of controls. That's because the people performing the reconciliation know that somebody above them is going to be reviewing that reconciliation, and if they don't do it right, there will be some consequence. I'm not talking about people getting fired, but when people know that other people are going to be reviewing their work, they tend to do a better job. So it encourages that continued effective operation.

I have seen, again and again, reconciliations that were not properly reviewed deteriorate over time. This deterioration happens because people get to the end of a month and say,"I'm busy this month. I haven't had a problem with this reconciliation in the past, so I'll skip it this month and pick it up next month." Or "I'll complete the reconciliation and put the reconciling items in an expense account." And lo and behold, that becomes a habit, and those reconciling items build up.

I've seen more restatements than I care to count because of simple nuts-and-bolts-type things that really should have happened, but didn't. And they these problems didn't get corrected in time because the controls weren't effectively monitored.

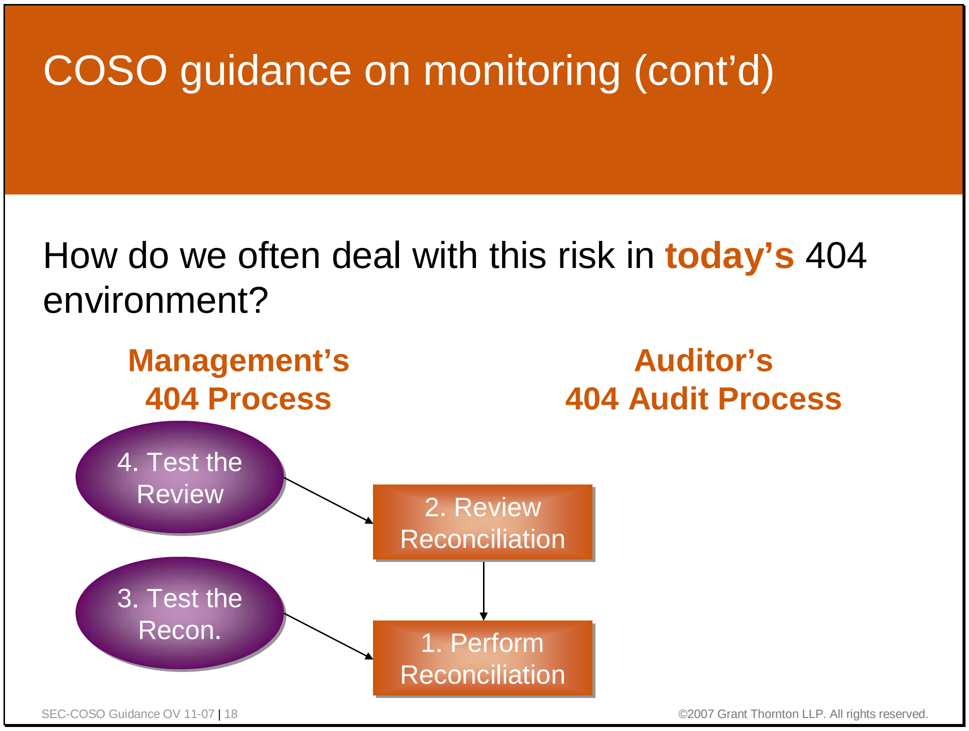
So if you think about it from a control perspective, whether you are a CEO, CFO, on the audit committee, or the independent auditor of a company, when you look at these two controls — the reconciliation control or the monitoring control — you almost could look at that monitoring control and say, “You know, that’s actually the key control in my mind;” first, because it tells you whether the underlying control is working, and two, because it actually encourages the effective operation of the underlying control.

Now, it goes without saying that the reconciliation is what prevents or detects the error. But that monitoring control accomplishes a tremendous amount. It tells you that the control is working. And it encourages effective operation of the control. Of course, this is only true if the monitoring is effective. If it's just checking initials at the top of a page, then it's not really an effective review. It doesn't tell you that the reconciliation is working effectively. So part of the COSO guidance is designed to help you identify if that supervisory review — or that monitoring — is effective. And if it is effective, then what should be the result?



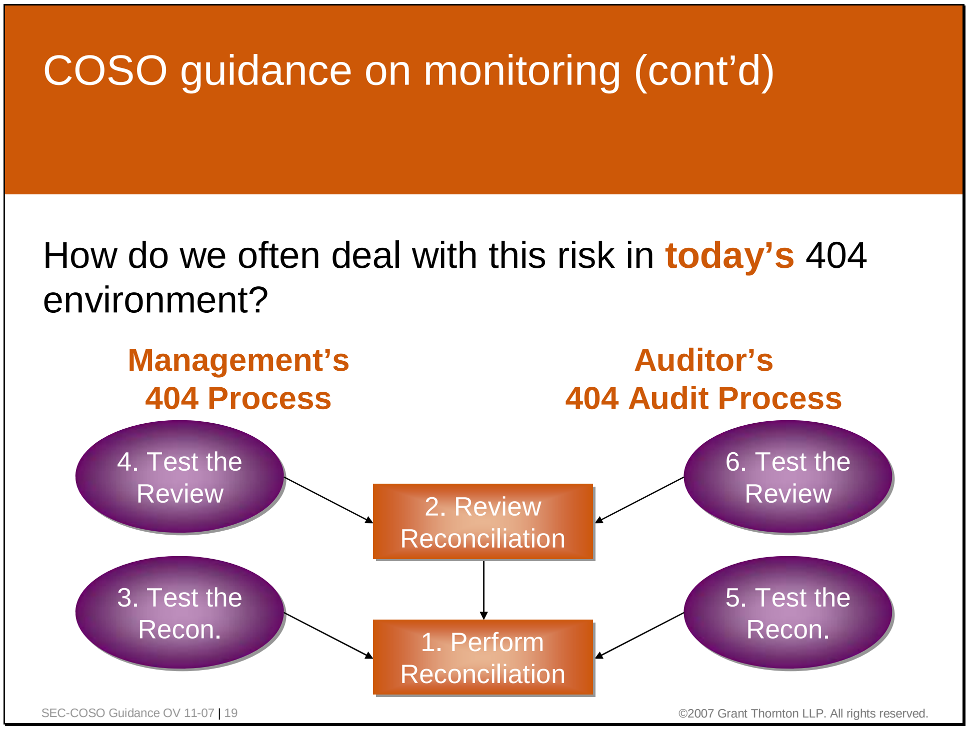
So let's look at a quick example here, and see how we often deal with this risk in today's environment. On this slide we have the reconciliation control at the bottom of the page, and the review of the reconciliation is above it.

Control Evaluation – Management's Process



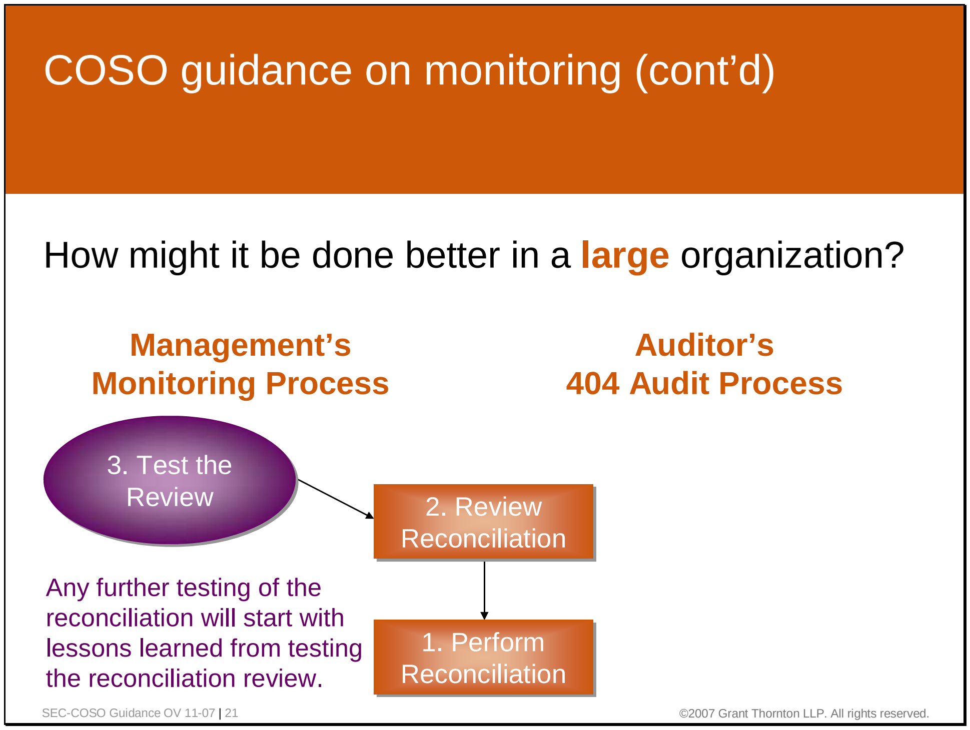
What often happens today is that management tests the reconciliation, and it also has somebody come in and test the review of the reconciliation. So there's a multi-layered process where four different things are going on to address this single control.

Control Evaluation – Auditor's Process



Then the auditor comes behind them, and they test the reconciliation and also test the review of the reconciliation. So we've got six different things that are happening to address the same risk.

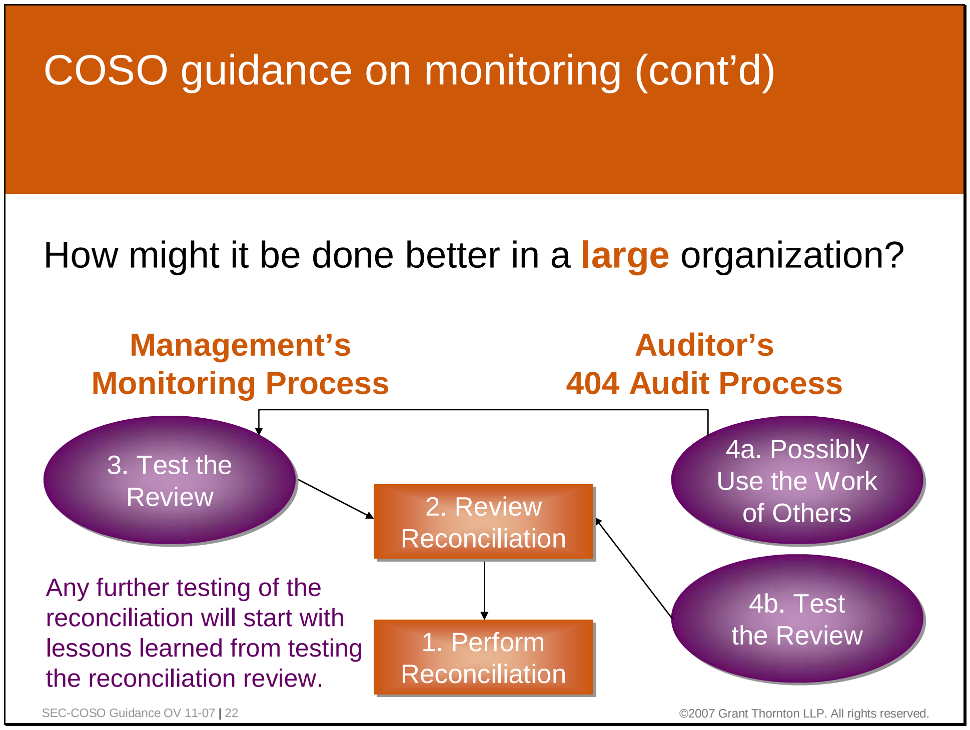
Monitoring in a Large Organization



Now let's see how this might work if the reconciliation review (i.e., the monitoring) is effective. We will look at it in the context of both a large and small organization, and see how the two scenarios might differ.

In a large organization, we start with the same reconciliation, and the same review of that reconciliation. But then we might say that, for senior-management to be confident that the reconciliation is working, it is going to focus on whether the *reconciliation review* is working correctly, because that review is already telling the supervisor that the control is working. If senior-management can conclude that the reconciliation review is working effectively, then they have a reasonable basis for concluding that the reconciliation is working. That's not to suggest that senior-management would *never* look at the reconciliation itself, but certainly, any further testing of the actual reconciliation would be influenced by the results of evaluating the monitoring control.

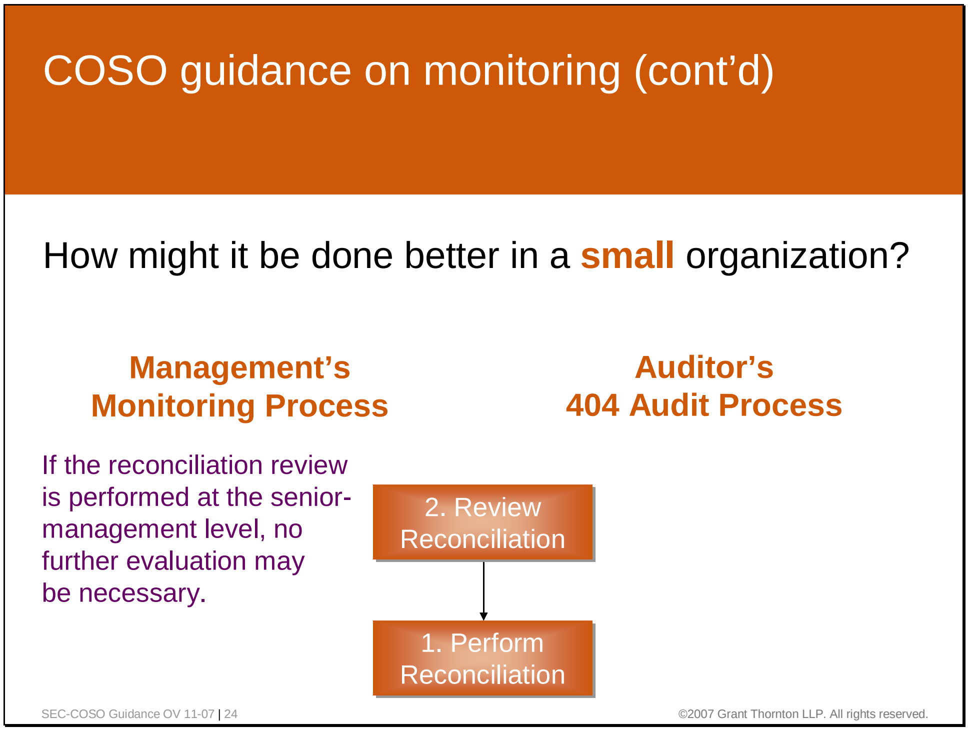
So automatically, from a management perspective, in a large organization, we've weeded out one of the tests that are burdening the organization at the end of the year.



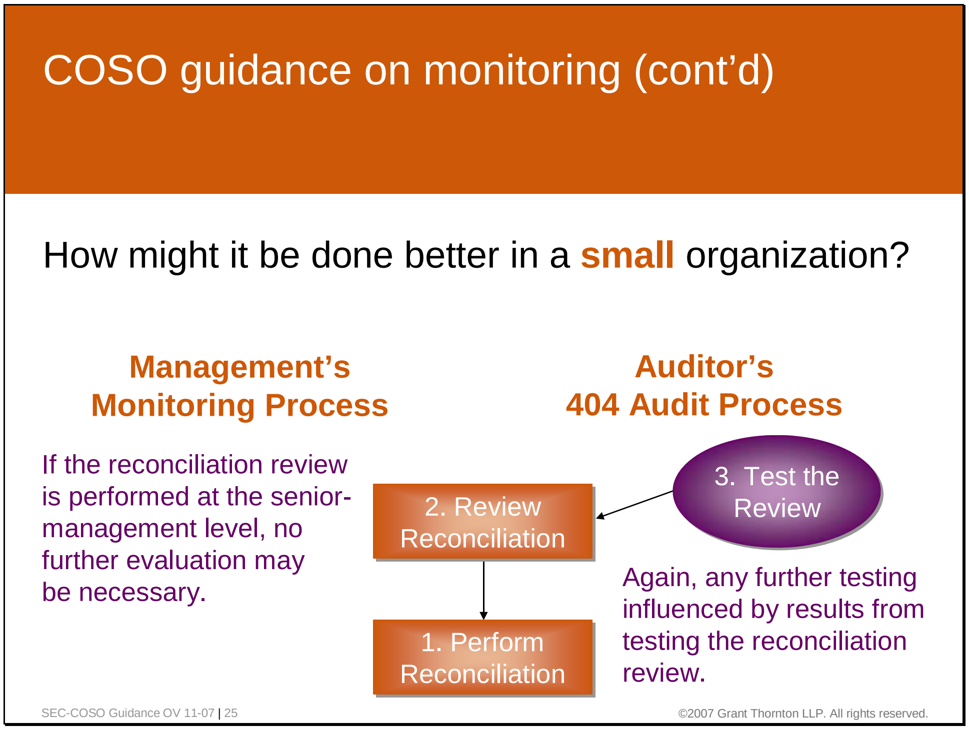
Now, from the auditors' perspective, they might do one of two things. Like senior-management, the auditor might also test the review. Or they might use the work of others and look to see what senior-management did to test the review of the reconciliation.

Note that, in this large company example, the reason we have management testing the review of the reconciliation is because senior management is removed from the monitoring control. Since senior management is not in close proximity to the monitoring, it needs to make sure that monitoring is actually taking place. Now let's look at a similar example, but in a small organization.

Monitoring in a Small Organization

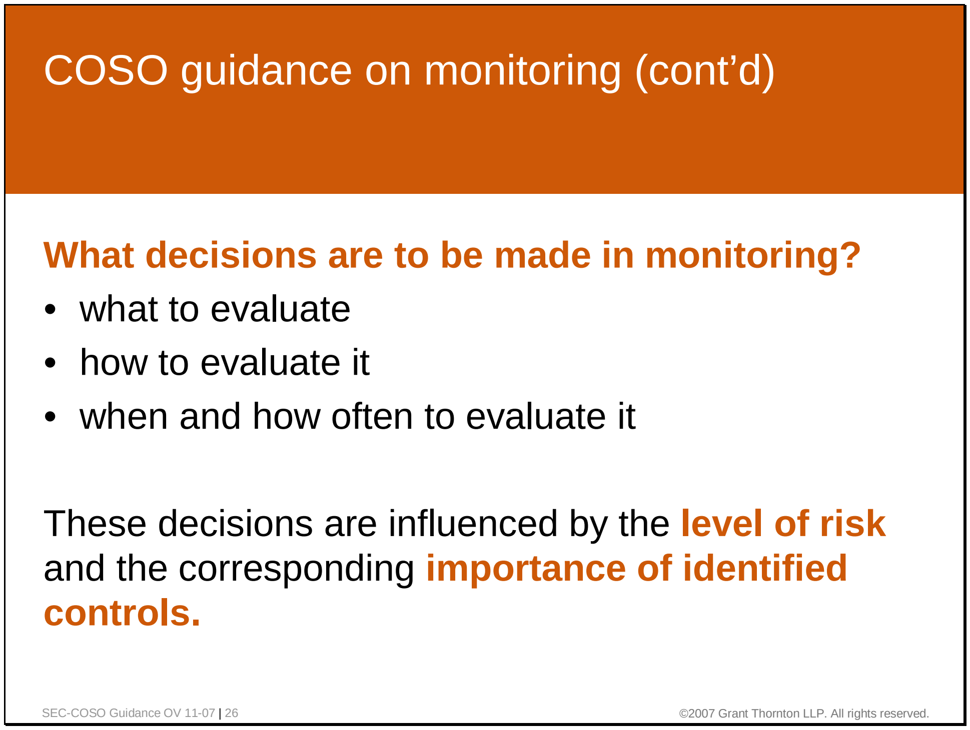


In this example, the same reconciliation is being performed, and that reconciliation is reviewed. But here, senior management might be the CFO performing the review of that reconciliation. Since senior-management in a small organization might be very close to the review of that reconciliation, it may not need to do anything more than what it's already done to review the reconciliation. In other words, by performing the monitoring at the senior–management level, they already have the support they need to conclude whether the control is working.



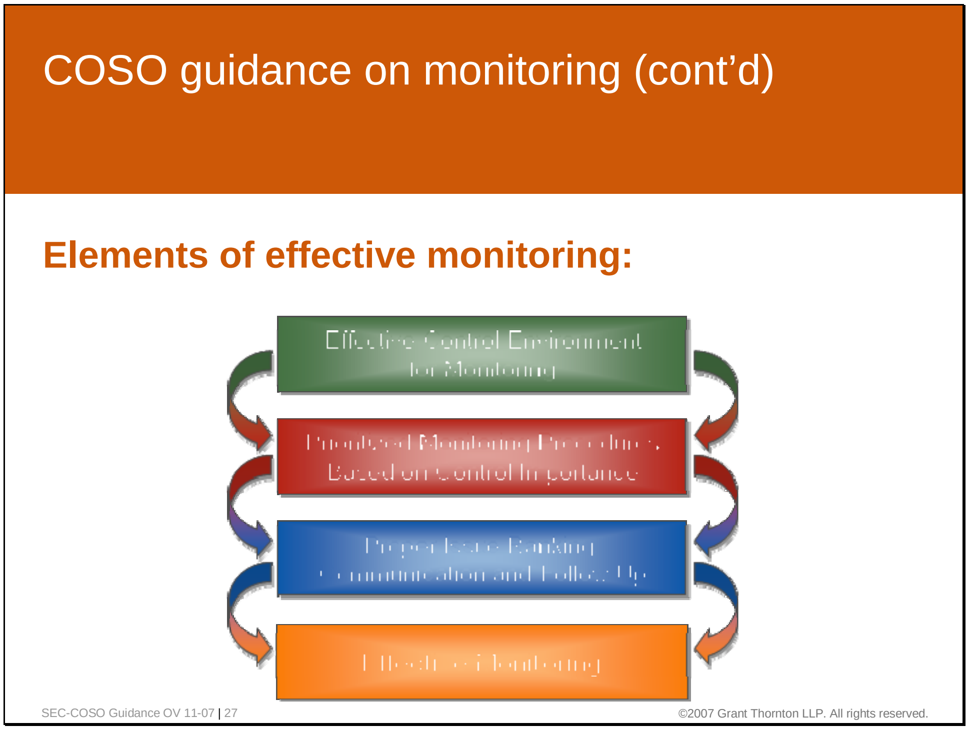
The auditor might come in and just test the review of the reconciliation. Again, any further testing that either management or the auditor does is going to be influenced by the results from the testing of the review itself. So you see, if we have effective monitoring in place, we can weed out a lot of this duplicative testing, both on management's side and on the auditor's side. And that's really what we want to accomplish in the COSO guidance: help people to know whether that review of the reconciliation is effective, and then be able to take credit for it when it is.

Monitoring Decisions

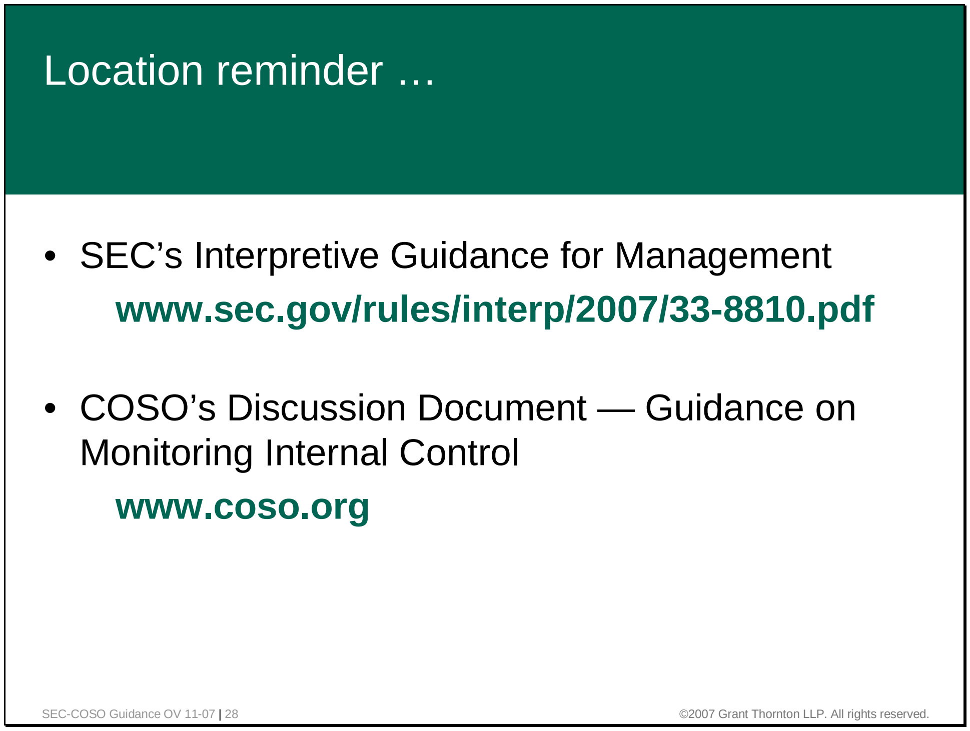


So what decisions are to be made in monitoring? We have to decide what to evaluate, how to evaluate, and when and how often to evaluate. All of that is influenced by the level of risk and the importance of the related controls in mitigating that risk. The COSO guidance seeks to help companies answer those questions for themselves, in their own unique risk context. It is not intended to be prescriptive – telling organizations what risks to be concerned about and what controls to monitor in relation to those risks. No guidance could properly cover the range of options that are available to companies of all different sizes, complexities, organizational structures, industries, etc. The goal is to help companies understand the underpinnings of monitoring so they can build it into their normal business processes.

Elements of Effective Monitoring



The first thing companies need is what I call an effective control environment for monitoring. Now, we are going to change the wording a little in this graphic in the final document, because people confuse the control environment for monitoring with the overall control environment for the organization. But all we’re saying is that, in order to have effective monitoring, you have to have the right attitude about monitoring, and you have to have the right people responsible for monitoring — people with the appropriate skills and authority in those key risk areas that are responsible for making sure that the internal controls are operating effectively. So you start with the control environment for monitoring itself. Then you prioritize monitoring procedures based on risk and the importance of the controls in mitigating that risk. And then you have proper issues ranking, communication and follow-up to make sure that issues are being resolved. We try to cover all of this in the COSO monitoring guidance, and the end result is, hopefully, effective monitoring, which you can take credit for.



So that's the end of my overall presentation. I do want to point out that the SEC's interpretive guidance is available on the SEC's Web site. It's under the interpretive guidance section, so you've got to do a couple of clicks to get to it, but that information is up on the screen. And then, regarding the discussion document — although the comment period for the discussion document has ended, you can still download the document free of charge at COSO's Web site, at www.coso.org.

About Grant Thornton

Grant Thornton LLP is the U.S. member firm of Grant Thornton International, one of the six global accounting, tax and business advisory organizations. Through member firms in more than 110 countries, including 50 offices in the United States, the partners and employees of Grant Thornton member firms provide personalized attention and the highest quality service to public and private clients around the globe. Visit Grant Thornton LLP at www.GrantThornton.com.

About Softrax

Softrax Corporation is a leading provider of enterprise revenue management and billing software solutions that fundamentally change the way companies manage, analyze, report and forecast their revenue. Softrax solutions automate the entire revenue cycle, from revenue recognition, reporting and forecasting, through complex billing and contract renewals. Hundreds of corporations benefit from using Softrax to optimize their revenue, reduce operating expenses, comply with revenue recognition regulations and Sarbanes-Oxley requirements, and gain unprecedented visibility into their business performance. Softrax Corporation, headquartered in Canton, MA is privately held. More information can be found at www.softrax.com, www.revenuerecognition.com, and by calling 1.888.4.SOFTRAX.

SOFTRAX

SOFTRAX CORPORATION
45 SHAWMUT ROAD
CANTON, MA 02021
1 888 4SOFTRAX