Compliance for Boards:

Is your program designed to work?

Four Big Questions to Ask Your Compliance Officer

BROADCAT

Is your company's compliance program designed to work?

That is, does it actually try to prevent compliance issues, or is it just an expensive exercise in corporate busywork?

Because some programs are designed to prevent issues, and some are just compliance-for-the-sake-of-compliance.

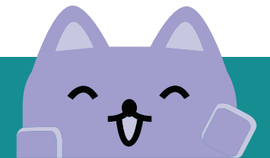
And that doesn't mean minimum effort; in fact, busywork compliance programs often exert a huge amount of effort, dumping mountains of paperwork on their boards each quarter to show how much they are doing.

These programs can win awards and their compliance officers can go on the speaking circuit—but do they actually prevent anything from happening?

That's what you want to know. And it's easy to end up with a busywork program that costs a lot of money and generates a lot of activity but can't answer that question.

To get that answer, you need a compliance program that views its mandate as preventing misconduct and focuses its efforts on identifying, controlling, and monitoring risky business processes.

That's because a focus on business process produces measurable results and lets you know what employees are actually doing—and "what employees are actually doing" is what determines if you are compliant.



Avoid scandal, not just liability.

Now, to be clear: getting this right isn't "duty of oversight" stuff. That's not what this is about.

Because in all honesty, the average director's obligation for compliance oversight is pretty light.

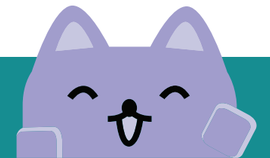
That is, assuming you're operating under Delaware law and have at least *some* kind of compliance program, the likelihood of you having legal liability is almost nil.

So having the right kind of compliance program is not about legal liability; it's about keeping your name out of the paper by avoiding scandal in the first place.

Because realistically, you'll probably win a shareholder suit about a compliance issue; they're almost impossible for shareholders to win. But at the same time, the compliance issues that trigger shareholder suits are usually ugly, painful, and embarrassing events that most directors want to avoid in the first place.

And while it's impossible to prevent every issue, you can get comfortable that your company's compliance program is at least *trying* to prevent issues—instead of just generating a lot of paperwork.

That's what this guide is about.



How this guide works.

In the **“Four Big Questions”** section, you get simple risk questions to ask your compliance officer, and guidance on what type of answer you want to hear (and what type should act as a big red flag).

That’s because pretty much any compliance program can answer these questions. So the distinction isn’t *whether* there’s an answer; it’s *what kind* of answer you get.

Does the answer give you the sense that the compliance team is focused on mitigating risk in a measurable way, or does it sound more like they’re doing a lot of compliance-flavored busywork?

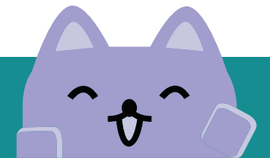
We’ll give you some tips on what this looks like for each question so you can make the call.

Then, in the **“More on Monitoring”** section, we go a little deeper into compliance monitoring.

Monitoring is the part of a compliance program that lets you know what employees are doing and whether your policies, controls, and training actually work.

It’s also the part of a compliance program that busywork-style programs gloss over—even though it’s part of the Federal Sentencing Guidelines—because it might tell them that their award-winning initiatives don’t really work.

You’ll hear us mention monitoring a lot in the “Four Big Questions” section, and so we give you a little more here to help you drive the conversation with your management.



(And of course, none of this is legal advice.)

Wouldn't it be amazing if you could download free legal advice off of the internet?

You could just download a little guide like this and get an attorney-client relationship that you could rely on for practical advice, without having to hire lawyers to understand your unique circumstances—all for free.

That would be amazing.

But it'd also be amazing if we all got ponies, and that isn't happening either.

So, no. This isn't legal advice, and we don't have an attorney-client relationship with you. Sorry.

Four Big Questions

Big Question #1: What are our biggest risks right now?

What you should expect to hear:

A discussion framed around your company's current operations and initiatives, what risks apply to them, and how that's changed since the last report.

The "framed around your current operations and initiatives" part is key. Because it's fine to know your abstract legal risks (antitrust, privacy, etc.) and regulatory developments, but it shouldn't be the focus of the discussion; that's an academic exercise.

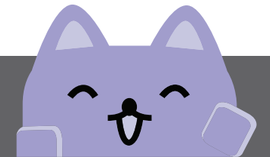
The value add of a compliance program here is understanding what risk looks like in the unique context of your company's active operations and strategy—and so the answer should reflect that this understanding exists.

Red flag:

You get a list of abstract risks and a description of recent court cases and regulatory developments, but no connection to how those risks impact active business operations or corporate strategy.

This is a sign that your compliance program exists in a silo: it issues policies and gives training on risks, and then it hopes the business will figure out how all of that abstract risk information applies to their jobs.

This approach can generate a lot of records of compliance activities, but it can't prevent compliance issues in the business—because it's not even thinking about risk in the context of what the business actually does.



Big Question #2: How is our compliance program structured—and why have we structured it this way?

What you should expect to hear:

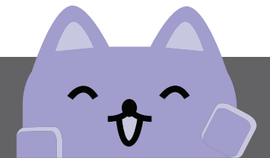
An explanation of your company's compliance structure and how your compliance monitoring has validated that this structure actually works.

You should expect to hear that your company uses standard compliance program tools (a Code of Conduct, processes, a hotline, etc.), but the focus should be on the results the company has achieved from those tools, not just that those tools exist. You should get specific outputs from core risky processes, with evidence that those outputs have become measurably less risky as a result of the compliance program.

Red flag:

You get a review of the basic elements of a compliance program—policies, training, a Code of Conduct, a hotline, etc.—and an explanation that they are best because of benchmark data about what other companies do. There is no explanation of how they have been validated other than the fact that other companies do the same things.

This is a sign that your compliance program is a bolt-on, busywork exercise, because the choices that have been made are simply based on what other compliance programs do—instead of any validation that they are appropriate and functional at your company.



Big Question #3: What type of compliance issue will get reported to us?

What you should expect to hear:

A description of: (1) what gets immediately escalated to you, and (2) what gets reported to you in normal updates.

For each category, you should understand what *type* of issue gets escalated to you, as well as *at what point* it gets escalated—that is, when it is first discovered or after some initial vetting (and if the latter, what that means).

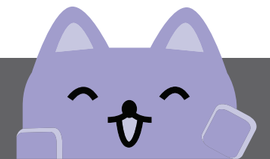
You should feel comfortable that the compliance program has a clear-eyed view of risk and knows what is worth immediately raising to your attention, what is worth aggregating into dashboards for regular reporting, and what never needs to cross your desk.

Red flag:

There is no clear threshold and information is reported randomly. Or, alternatively, you get a line-by-line review of every hotline case each quarter.

Either circumstance is a sign that the compliance team is unsure of what merits your attention. This might mean that they simply do not understand board duties, but it might also mean that they do not understand risk.

If this is the case, you might be dealing with a busywork-style compliance program: your compliance team isn't sure what's risky enough to raise to you because they're not really thinking in terms of risk in the first place.



Big Question #4: Does our compliance program have the resources it needs?

What you should expect to hear:

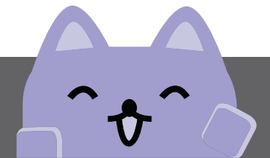
A discussion of the results of your company's compliance monitoring program and audits, and where those results indicate things are good—and where you need to allocate more resources.

That is, a prevention-focused program is not always going to give you good news: sometimes it is going to tell you that your monitoring shows you need to give an area more attention. And that's a good thing; it's a meaningful, rational way to be confident where your processes are solid, and to be aware of where they need work.

Red flag:

You get benchmarking data on compliance activities and features: the company's compliance budget, time spent training employees, compliance headcount, employee culture surveys, etc.—but no data from monitoring and auditing business processes that create or control risk.

This is a sign that you have a busywork program; it compares its work to other programs, but not whether its work creates results. You cannot be confident that this type of program is adequately resourced because you do not know if any of its components actually work.



More on Monitoring

“Monitoring” is just checking on things.

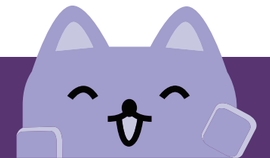
We’ve mentioned compliance monitoring repeatedly in this guide, so here’s a practical definition of what that means: it’s regularly looking at your risky business processes to check if you’re compliant.

Monitoring matters because it’s how you know whether your compliance program is actually accomplishing anything. It forces you to break down “risk” into specific behaviors employees do that create or control that risk—approve invoices, sign contracts, hire consultants, whatever—so that you can write meaningful policies, create useful training, and implement controls that address those behaviors. And then you use monitoring to check if those policies, trainings, and controls are working.

Now, don’t get distracted by advice on AI and automation and other tech stuff here; you’ll find a ton of that, but that’s just a way to monitor, not monitoring itself. Your compliance team can monitor manually at first, and some things will probably always need to be monitored through manual spot-checks. Of course, you’ll want to automate what you can as your program matures, but don’t fall into the trap of letting tech limitations be an excuse for not doing it in the first place.

And here’s the good news: you probably already do a lot of this in other areas of the business. Checking to see if your initiatives work is pretty basic business stuff.

So the trick here isn’t doing something radically new; it’s just encouraging your compliance program to be more businesslike in how it does its work.



The company's hotline is not monitoring.

Your company probably has a hotline already, and that does something that seems similar, so it's fair to ask whether your hotline is basically monitoring.

And . . . no. It's a hotline. It's important, but different.

Here's an analogy to explain.

Imagine that your management is thinking about buying a new piece of equipment that could transform your business operations.

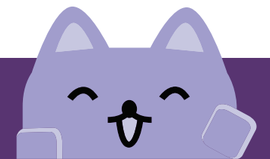
But it also has some safety concerns: the manufacturing process it improves requires using a bunch of combustible materials, and the machine could cause fatalities if it malfunctions.

So you ask for a report on the manufacturer's safety record. And you learn that the manufacturer does not do any quality assurance or safety testing on any of its products, but it does have a very slick hotline you can call in case the equipment blows up.

You probably do not buy that piece of equipment.

Relying on your hotline as your primary way to know about compliance issues is kind of the same thing.

It's a good thing to have a hotline, you want employees to use it, and you should want to see that data—but it is not a substitute for proactive monitoring. Don't let anyone tell you that it is.



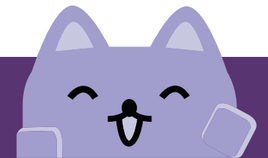
Monitoring is how you measure if your program works.

We're harping on this because there are a surprising number of people who believe that compliance is somehow the one thing in the world that can't be measured. They will tell you that compliance is essentially proving a negative, and the best way to measure it is by benchmarking how much busywork your compliance team is doing.

If your compliance officer says this type of thing, watch out. It should worry you if the person in charge of mitigating compliance risk for your company thinks it is impossible to measure compliance risk.

In most cases, the reason people believe this is that they're thinking too high-level. You ask them for results from your anti-corruption program, and they fret about how difficult it would be to measure a lack of bribes and fines—instead of how they could monitor red flags in purchase orders and payments and contracts to catch early indicators of corruption risk, and then track that over time to measure if their initiatives work. They simply need to break down your risks into the behaviors that matter; monitoring (and by extension, measurement) then becomes achievable.

(And of course, that's a lot of work, which is why "compliance officer" is a full-time job. If your compliance officer is being asked to do compliance *and* litigation *and* safety *and* whatever, you're going to get a high-level busywork program, because that's all they have time to do, and it's unreasonable to expect otherwise.)



Further reading

Here's some more reading (for you compliance all-stars).

1. For a simple analogy explaining why compliance should produce measurable results (and how to do it):

   Want to measure corporate compliance? Look for the dirty socks. Broadcat Blog, available here.

2. For a step-by-step guide to practical training and measurement on a finance process, complete with all of the math for reducing employee behavior to dollars:

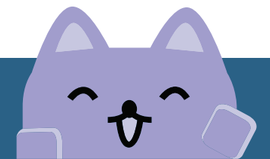
   Why most compliance training fails—and how to fix it. Broadcat, can be ordered here.

3. For an analogy of what "operationalized compliance" means, using safety teams and the zombie apocalypse:

   What "operationalizing compliance" actually means—and why it matters. Broadcat Blog, available here.

4. For validation that your company's annual compliance training really is a lot of counterproductive busywork, just like you always suspected:

   You don't need annual compliance training, but we made some anyway. Here's why. Broadcat Blog, available here.



This guide was made by Broadcat.

We're a compliance startup that takes a simple, operational approach to compliance—and we wrote this guide. We make training and tools and do advisory work for folks who want to stop busywork and get practical.

If your compliance officer has ever shown you a visualized summary of Department of Justice guidance that they "downloaded from the internet," we probably made it.

You can learn more about us, and how to get a free copy of our book on compliance training and measurement, by clicking this button.

Order the book!