Keeping Compliance Simple.



BROADCAT

Get back to basics.

This material is based on a conference session I (Ricardo Pellafone, Broadcat's founder and former CEO) led with John Partridge of Gibson Dunn. After the session, we received a bunch of feedback from people that this was next-level, cutting-edge stuff.

And that's flattering, but this is not next-level stuff.

This is what compliance actually is.

The training "best practices" you've been taught simply obscure what the government has told us to do for over 20 years: make sure your stuff works. This just applies social science, design, and business principles to help accomplish that.

That said, this is "cutting edge" in the sense that not everyone will be ready for this. Holding yourself to results is risky and scary, because you can't control everything—and you might fail.

But that's the standard your sales, marketing, engineering, and executive teams hold themselves to. And if you want a seat at the table, that needs to be your standard, too.

You might not be ready for it, but you need to get there as soon as you can—or change careers. Corporate compliance is too important to play around with squishy metrics and participation awards.

And don't worry: I made every mistake I mention here when I was in-house. Because when you're in-house, you're trying to do ten million different things.

But now I'm a vendor, and vendors have the luxury of single-issue focus. You're supposed to rely on us to think deeply about this stuff, because that's our value. And that's what we're doing for you here.

First, forget “best practices.”

The first step in recovery is admitting you have a problem. And in corporate compliance, our problem is that we are addicted to best practices.

It’s a problem because best practices only measure what you are doing, not whether any of it works.

And since you can always be doing more stuff, holding yourself to a “best practices” standard means that you’re stuck in an eternal arms race of who can have the most complex, flashy program.

That is not the right standard.

It is not what the government wants, it is not what your executives want, and it is absolutely not what your employees want.

You can use best practices surveys and benchmarking to get ideas. But achieving a “best practices” program just means that you have spent a lot of money and time; it doesn’t mean that any of it works.

This is the only question that matters: what works for my company, and how can I prove it?

That’s what this covers. Not “best practices,” but “effective practices.”

And we break that down into a few big topics.

1. What does the government really require?
2. How do you design effective training?
3. How do you implement it?
4. How do you measure it?

Let’s get started by talking about the real standard.

What does the government really require?

You need to be “effective.”

The Federal Sentencing Guidelines have a pretty basic standard for training—**it should be “effective.”**

That’s it.

They also have some stuff about training being “periodic,” “practical,” and “appropriate to . . . roles and responsibilities,” but those don’t help much.

Because if you were to ask “how periodic? how practical? how role-specific?”—the answer is going to be “enough to be effective.”

This seems obvious, but it isn’t. Because if you talk to anyone in compliance training, you will hear people rattle off a laundry list of “requirements” about Code of Conduct training refreshers, completion rates, seat time, auditability, and a whole bunch of other nonsense.

None of that has any basis in the Guidelines.

Folks have probably gleaned some of these things from Non- or Deferred-Prosecution Agreements, or from Corporate Integrity Agreements, but basing your training program on those things is a mistake.

That’s like trying to avoid committing a crime by buying an ankle monitor. Instead of focusing on prevention, you’re preemptively punishing yourself.

The goal of training is not to minimize a penalty; it’s to avoid misconduct in the first place.

When you confuse those things, you end up doing stuff that looks like compliance, but is actually just paper-pushing. And then you wonder why employees aren’t into it, but that’s obvious: because you’re acting like you assume it won’t work. Aim higher.

And “effective” is good.

The “effective” standard seems annoyingly vague and lawyerly, but it isn’t. It’s actually great.

Because it’s the same standard everyone else in your business operates under.

> How many calls are your salespeople supposed to make? Enough to make sales.
>
> How long should your engineers spend on that new project? Enough to meet the requirements.
>
> How many developers do you need to assign to that new upgrade? Enough to meet the deadline.

Business is about results, not how hard you try or how much money you spend. The less time and money you spend on something to get the same results, the better you are at business.

So, the problem with the government’s standard isn’t that it’s vague; it’s that a lot of us come from professional services backgrounds where we had the mantra of “trying hard and spending time on something = value.” That’s how billable hours work.

That is not how business works. In business, “value = value.” There are no participation awards in business.

So the government’s standard is actually good. Hard, but good. “Effectiveness” is far more business-friendly than an arbitrary requirement or some best-practices nonsense.

Of course, it requires a shift in mindset. It’ll force you to think in terms of investment, return, and even occasionally open up Excel to do some math. But it’ll get you a seat at the table, secure your budget, and protect your headcount even in lean years.

How do you design effective training?

Target “transfer.”

If you want to design effective training, you need to leverage how people learn. This will help keep you focused on the right goal.

And people learn like this, wildly simplified:

(1) Engage: they pay attention to something
(2) Retain: they remember it
(3) Transfer: they apply it in the real world

You need to be focused on that last step, because the point of compliance is real-world application. **Anything that does not promote transfer is a waste of time and money.**

The problem, however, is that most compliance training does not even attempt to do this. Instead, it focuses on the first two steps.

When you focus on “engagement,” you end up doing a bunch of useless flashy stuff because you think your problem is that people aren’t paying attention. Your training is still useless; it just costs more because now it’s in 3-D and has lasers.

Likewise, when you focus on “retention” you just end up torturing your employees with quizzes and tests. Don’t do that. Compliance is an open-book test; there is no extra credit for memorization. Your goal is to require your employees to remember as little as possible to get the job done.

Both “engagement” and “retention” are necessary, but they are not your focus. **Your focus is transfer, because that’s the only thing that actually prevents improper conduct.** Everything else is just entertainment or academic.

Stop training on risks.

To promote transfer, you need to minimize the gap between learning and the real world.

So, stop training people on risks.

That is how you learned. Your job is to apply risks to new situations, so you needed that broad skill.

But that is not anyone else's job. Their job is to sell stuff and build stuff and so on. You need them to do their jobs compliantly, not learn how to do your job.

If you want people to do their jobs compliantly—which is the entire point of compliance—then you need to meet them on their terms.

Figure out how risks apply to what they do, and then integrate that into their job training.

Risk-focused training doesn't work because it pushes all of the "transfer" work to the employee, which practically means that it doesn't happen.

And that's because your employees do not know how to apply risks to what they do. That is your skill set, not theirs. It's not "common sense;" it just feels that way to you because you've been doing it for so long.

But here's the good news: that's why you have a job. If your employees could magically apply risks to their job tasks just by hearing about them, there would be no in-house compliance. Your legal team would just forward Gibson Dunn client alerts to everyone and call it a day.

That doesn't happen, and that's why you have a job to do. And that job is meeting employees on their terms.

(But someday, get to risks.)

Quick caveat: at some point, it will be a good idea to train very selected audiences on risks.

You are not there yet.

You might be years away from it.

But eventually, you will get your high-risk tasks nailed down, and then you'll want to empower certain folks—like Legal and Audit—with a deeper risk knowledge so they can apply your guidance in situations that you can't anticipate.

The problem is that virtually every compliance program jumped straight to this stage, which doesn't work. You need to handle the easy, knowable, high-risk tasks first—and then, and only then, should you be screwing around with telling people what anti-corruption or antitrust is.

Here's an analogy.

In an ideal world, all restaurant workers would have medical-grade knowledge of how bacteria is transmitted.

But when you eat at a restaurant, you don't really want the line cooks to be trained with little animated videos and newsletters talking about disease vectors. You know that wouldn't work.

You want a sign next to the bathroom sink that says "wash hands before returning to work."

You need to totally own the easy, repeatable stuff before getting fancy. Too many programs fail because the compliance team is focused on creating a *Jetsons*-style program when they don't have *Flintstones*-level compliance.

Instead, train on tasks.

Compliance happens at the job-task level.

To be clear: compliance does not happen at the program level, the risk level, or the job-function level. It happens when an employee does a specific, risky job task the right or wrong way.

So, if your goal is to get people to perform specific, risky job tasks the right way, you need to frame your training around those specific, risky job tasks.

This seems daunting, but it isn't. The number of tasks that actually impact the vast majority of your compliance efforts is surprisingly small, and they're generally consistent across companies and industries.

Your duty is to identify them, get your people better at them, and then measure their performance on them routinely.

And you are going to accomplish this by tackling them one at a time, staying lean and nimble and not creating a bunch of unnecessary process.

We'll get into how to do that in the next section, when we discuss implementation. But first, let's walk through what this looks like in practice.

Example: the China trip.

Let's pretend that one of your company's salespeople is going on a 2-day business trip to China. They will spend one day at a conference and another day holding meetings with customers and prospects.

What risks apply to that?

The short answer is "all of them, more or less." Anti-corruption, antitrust, fraud, cybersecurity, privacy, intellectual property, trade compliance, and so on.

What do you think the odds are of any salesperson at your company correctly identifying all of those risks?

Zero.

Because remember: that's your skill set, not theirs.

And even if they did identify them, do you think they'd go read through all of your applicable policies for a refresher before the trip? Or your entire Code? Or re-watch a bunch of video modules in your LMS?

For a two-day trip?

Nope. Because no one would do that.

All of your carefully orchestrated risk-based training is going to fail—and yet, "going on a business trip overseas" is a really common, knowable, high-risk thing that your employees do.

So, frame your training around going on a trip. Let's see what that looks like.



GOING OVERSEAS ON A BUSINESS TRIP?

HERE'S YOUR TO-DO LIST

GET PRE-APPROVALS

- ☐ Planned business gifts and entertainment
  If giving to a government official or more than $150, you need pre-approval
- ☐ Product samples you have to carry with you
  It's easier to ship in advance—if you can't, email TradeControl@Company.com for help

PACK SMART

- ☐ Take a Safe Laptop instead of your regular computer
  Avoid problems at customs—email [safelaptop@Company.com] to get a travel-safe machine
- ☐ Understand how to rotate your SIM card if necessary
  If this applies, IT will inform you when you get the Safe Laptop
- ☐ Only take work files you need for this specific trip
- ☐ Know how to disable WiFi and find secure networks
  Need a reminder? [It'll appear when you boot up your Safe Laptop]
- ☐ Bring a privacy screen for your laptop to use in public areas

BE IN THE KNOW ON THE GO

- ☐ Review what to do if you get asked for a bribe on the spot
  Need a reminder? Check out the [RESOURCE (Intranet, call Helpline)]
- ☐ Save the Ethics Helpline and 24/7 Travel Desk in your phone
  Ethics Helpline: [NUMBER] — Travel Desk: [NUMBER]
- ☐ Keep your Emergency Card on you at all times, just in case
- ☐ Hold all business and travel documents until you return
  Do not discard confidential information at the hotel, in a public place, or another company's office

© Broadcat

This is a checklist. It integrates gifts, trade compliance, cybersecurity, confidentiality, privacy, anti-corruption, hotline awareness, and physical safety into one page.

And then it further breaks down those risks around the order in which someone goes on a trip: pre-approvals, packing, and being on the trip itself.

It accomplishes transfer by being framed exactly around what you want people to do.

And it takes care of retention by being in a format that can be made available to the employee when they need it. **All the employee needs to remember is "I'm going on a trip. There's a checklist for that."**

This checklist handles everything except attending the conference; you could integrate that in here, but it's not really a neat overlap because those two things don't always go together. So let's look at that next.



This is the same guidance that's in your antitrust policy; it's just framed around what people actually do instead of an abstract legal category.

No one has to remember "conference = antitrust = no discussing pricing, territory, or other agreements with competitors."

They just need to remember "conference = that thing on what to do at a conference."

If you're fancy, you can have your finance system spit these things out when someone applies for an overseas trip or conference spend. But don't worry about that right now—start with email and print and then eventually work your way to automation.

Now, could a bad employee delete an email with one of these in it, or throw away a printout? Of course.

But so what? **Training is for good employees, not bad ones.**

All of your training should fundamentally assume that your audience wants to do the right thing—because those are the only people who will listen to you.

You handle bad apples through controls and auditing; don't worry about them when you're training.

How do you implement it?

First, stay calm.

You are going to face one of two temptations when implementing this.

The first is to look at your HR data and give up because you don't know what everyone at the company does. But guess what: you don't need to know that. You know enough right now to get started.

The second is to try to map every single thing at the company and address it all at once. That is also a mistake. Even if you have the willpower and budget to do so, you will get overwhelmed and fail. Miserably.

And you'll lose all kinds of credibility with your business, because they'll be annoyed you put them through some massive project without testing if it'd work first. That's amateurish.

So, don't do either of those things. Instead, here's what you're going to do: **tackle these high-risk tasks one at a time.**

That's right: one at a time.

And don't worry about planning two years into the future with the next 20 high-risk tasks mapped out, either. That's just an excuse to sit in your office color-coding things instead of actually getting stuff done.

Just worry about tackling the very first task.

If that's all you ever accomplish, you're still better off than a person who spends 12 months mapping out every single task, because by the time they finish all the tasks will be different anyway. So don't worry about two years from now: worry about today.

Next, pick your task.

Here's how: start with a risk. Let's say you choose anti-corruption, because you'll probably choose that.

Then, choose a process implicated by that risk. For example, under anti-corruption you might have "getting permits," "lobbying local governments," "selling to state-owned enterprises," and so on. Just choose one of those things.

So far, you should have spent like 90 seconds on this. If not, you're overdoing it.

Next, you're going to map out the tasks that people do in that process, remembering that virtually all processes end with someone getting paid. If you need help, your auditors should know this stuff already; go sit with them.

Finally, pick one of the high-risk tasks in the process. It'll be a either a front-line task that creates the risk (like "engaging a third-party agent"), or a gatekeeper task that controls the risk (like "approving a third-party invoice").

If you spent more than 30 minutes on this, something went wrong.

You should be starting with the most obvious, easy-to-fix stuff, because that's the stuff that will make your program look especially bad if you screw it up.

Keep it simple.

(And start with Finance.)

Here's a recommendation that will make your life infinitely easier: start with a task someone in Finance does. Like Accounts Payable or Accounts Receivable.

Here's why:

(1) They generate a lot of data
(2) They're easy to audit
(3) If you're going to get in big trouble, it almost always involves someone getting paid

A lot of people will want to start with their front-line folks (the people who create the risk), but I really encourage you to start with gatekeepers like Finance, Legal, and the front-line folks' managers.

A bad actor in your front-line isn't going to be stopped by training—but they can be caught by a well-trained gatekeeper. And your gatekeepers need to be trained.

Here's why: imagine that tomorrow your CEO comes in and tells you that you've been doing such a great job on your stuff that you now own SOX, too. Would you be confident that what you're already doing addresses SOX?

No, because that's a totally different area. And it's the same with gatekeepers—yes, they're looking for stuff, but it's not your stuff. You need to train them on what to look for and make that part of their workflow.

When your gatekeepers are trained, they catch bad employees early in the process of misconduct. But when they don't know what to do, you end up with what you'll tell the media is a "rogue employee" but is really just a weak compliance program.

Get your gatekeepers on point first, and then worry about the front-line.

Finally, measure & train.

Once you've picked the task, get a baseline reading on how good your people are at it—we'll talk more about how to do that in the next section—and then train them on it.

You can train your people however you want, because the only standard is that it should work, and you'll find out soon enough if it does.

Whatever method you like, do it. The specifics of designing that training on a granular level are beyond the scope of what we're doing here.

All I want you to remember is that **no matter what you do, you need to give them something to read while they are actually doing the task.**

Because again, this is an open-book test. You do not get extra credit for memorization.

The employee who works through a checklist when they are doing a high-risk task and the employee who has the red flags memorized are equally compliant—the first one is just more likely to actually exist.

How do you measure it?

Auditing is your metric.

Auditing tasks is the only way to measure if your training actually increases compliance—it's the only thing that measures what people *do* (versus what they *remember* or *think*). And you need to use it if you want to be taken seriously.

Here's why. Imagine that you roll out a new Code of Conduct. You train 100,000 employees on it with a 1-hour course, and you get 100% completion. You proudly report this to your C-suite.

Here's what they hear: "We spent 100,000 hours on this but don't know if it made a difference. High five!"

And then they'll realize that since there are 2,000 work-hours in a year, you basically had 50 employees who did nothing but take that training all year.

And then they'll think about how each employee costs the company around $50,000 a year in comp and benefits and overhead, so your training cost the company $2.5 million in real money, and you have no idea if it was valuable or not.

And then they will think about what they'd say to any other leader who burned through $2.5 million without being able to articulate why that spend was valuable.

They won't say it to you, though, because they won't want to be viewed as anti-compliance. So they'll just say "great job!" and then quietly exclude you from important decisions because they'll think you don't understand business at all.

If you want a seat at the table, you need to audit what is really going on so you can articulate why your work matters in terms your leaders will appreciate.

And auditing is easy.

Because you don't have to do it. Your audit team should do it for you.

Auditing tasks like "catching red flags in an invoice" and "monitoring incoming payments for sanctioned countries" is what your auditors do all day. So you're going to recruit them to do exactly that for you.

And this is where you could run into one of two roadblocks.

First, your auditors might say no. And then you need to go to your CEO and tell them that auditing is one of the elements of a compliance program under the Federal Sentencing Guidelines.

And beyond the legal requirement, it's the only way to make sure you can measure return on investment on your compliance program. So you need your CEO to tell your auditors to get a new attitude.

If that doesn't fix the problem, quit and find a new job. If audit and compliance are not working together, you are just throwing stuff at the wall and have no hope of being effective. Something is deeply wrong with that company's culture—get out.

Second, you might get bogged down in trying to figure out how to audit some kind of offline task. If so, you picked the wrong task to start with. You tried to get fancy and picked something hard.

Start with something easy that generates records. Because, again, if it's easy for you to fix, it's also easy for the government to blast you on if it's broken. If the way to audit the task isn't obvious, pick a different task.

Here's how to do it.

Step One: Get a baseline reading.

After you've picked your task, talk to your auditors and find out how good people are at it right now—before you do any training.

If you're lucky, they've audited it recently. If not, ask them to pull the paperwork on the task. If you took my advice and started with a Finance task, that will be easy and fast.

Once you have the paperwork, audit it. Check the invoices for red flags. Check the incoming wires for country of origin. Check the T&E reports to make sure they sync up with your gifts & entertainment approval thresholds. Whatever.

This can be done by a junior employee, and it is not a big task. You are just counting how many things had red flags (or whatever) and weren't flagged for further review. Ask for a few hundred invoices or PO's or whatever you are reviewing; if your people know what to look for, they can knock out several per minute. It should take a few hours at most, and you don't need a fancy report. A PowerPoint slide is fine.

Step Two: Train.

Train the people that do the task and make sure they have a takeaway that they can look at real-time.

Step Three: Audit again.

Wait a few months for new data to be generated—again, easiest if you're working with Finance—and repeat Step 1. If the people got better at it, your training works. If not, dig into why, fine-tune, and try it again.

(Advanced: measure ROI.)

The final step in this process is to do some basic business math that calculates, in dollars, the impact of increased compliance.

I am not doing that here.

Here's why: if you've never built a financial model or written a business plan, walking through it here is going to be too overwhelming. Get through the first iteration of baseline/train/audit on a task, and then reach out to me. I will explain to you how to do it.

If you do have that experience, figuring out the cost of training is pretty straightforward, and here's a tip for calculating one of the benefits: look at saved investigations spend. Because every time you achieve proactive compliance on a high-risk task, you're saving a potential investigation.

And the truth is that investigations have low ROI—you're addressing a single issue in the most reactive, expensive way possible.

For example, you can easily drop $10,000 on an international business-class airplane ticket, and all that does is put an investigator in the air.

And while you'll always need to do investigations, you shouldn't be wasting resources investigating stuff that could have been prevented with a checklist.

So with some basic assumptions about in-house and external spend, it's pretty easy to demonstrate how proactively catching just a few more red flags each quarter can result in dramatic savings.

But either way, worry about this when you get to it. Execute a small, single-task iteration, then evaluate.

(Advanced: incentives.)

Super bonus, not really discussed at the conference: this is how you incentivize compliance, too. Because remember, "incentives and discipline" are another one of the seven elements of a program under the Federal Sentencing Guidelines.

While most people grasp "discipline" intuitively, "incentives" are often executed as some kind of award given out to a handful of employees for calling the hotline, or as a requirement that everyone take training in order to get their bonus.

There's nothing wrong with that stuff, but I don't think that's really what "incentives" means.

The reason people struggle with incentives is that they get stuck thinking about them too high-level. You cannot incentivize "compliance" in the abstract.

You can, however, incentivize people to catch red flags in invoices, and make sure all their business gifts are approved, and only bring clean laptops when they go on trips to countries with high cybersecurity risk.

Those are all measurable, auditable things. And they can be integrated into performance management, so that people get held accountable to them as part of regular performance reviews. And that means that incentives like promotions and bonuses are tied to the proper performance of high-risk tasks in a way that actually impacts your company's compliance.

So as you integrate your training and auditing into operational tasks, involving HR for the "incentives" element of the Guidelines becomes a lot more achievable, too.

Troubleshooting

What about offline tasks?

Don't worry about them right now.

Start with the stuff that does leave a record. That is the stuff that will get you in real trouble—stuff where your lawyers signed it and your finance people paid it and no one noticed.

Stuff that leaves a record is low-hanging fruit for you to train on, your auditors to audit, and the government to blast you on if you drop the ball.

So start there.

Once you have that reasonably under control, worry about figuring out how to audit the offline stuff. That will take you at least a year, probably several.

When you get there, you'll find you can still audit what people do offline by working backwards from what they submit for approval and signature.

For example, if your salespeople keep submitting third-party invoices for payment that are riddled with red flags, your salespeople are not managing their third parties very well.

And if your marketers keep writing POs for marketing agents that aren't tied to a contract, they're making commitments without going through vendor due diligence.

And so on.

And at some point, you'll decide that you're good with the offline stuff, because you'll be hitting diminishing returns. But that is literally years down the road. Start with the easy stuff first, and worry about the hard stuff if and when you get to it.

This didn’t work for me.

Now, we come back to engagement.

Framing stuff around real-life activities is not going to fix your problems overnight. You might legitimately have an engagement problem if your employees have learned to ignore you because either (1) your program has a history of being too high-level or complex or (2) you don’t have the support of your senior people.

If that’s the case, here is my advice to you.

First, get tactical. If the problem is how you’ve operated in the past, you have a reputation problem. That is not going to be fixed simply by giving better training and auditing; you need to go on a charm offensive.

You need to think of your team like a company that has had a product recall; the problem isn’t just fixing the product, it’s rebuilding customer trust. You have a damaged brand, and that won’t be fixed overnight.

Get your training fixed, and then—before you roll it out—you need to go sit with your business leaders, explain what you’re trying to accomplish, and ask for their support.

One at a time. In person, not by email.

Yes, this is hard and a time suck, but it is literally your entire job. Let me be clear on that: **if you are in-house compliance, managing relationships is your entire job.**

And that is a very good thing, because only you can do that. Investigations, audits, risk assessment, training, legal expertise—all of that can be outsourced

or handled by software, and often much cheaper than having a full-time employee do it. The real value of an in-house team is not that they know how to do investigations or give training, but that their VP of Sales respects and listens to them.

Any compliance initiative you handle is 10% doing the stuff and 90% getting buy-in. So go read Kristy Grant-Hart's book ("How to Be a Wildly Effective Compliance Officer"), hone your sales skills, and then execute.

And when you roll it out, be persistent—keeping in mind that most sales efforts result in a rejection, and the ones that succeed require one million follow-ups with the customer (give or take).

That's the standard your business-side people have in mind when they think about what persistence means. If you send something out once or twice and then give up, don't expect your business leaders to feel sorry for you. Get aggressive.

Second, if that doesn't fix the problem, the problem isn't you or your team. It's the company.

So quit and find another job.

Seriously. There are definitely workplaces where compliance is devalued and leadership does not support it, and you work at one. Although you might be able to turn it around in the long term, life is short.

Do step 1 first, because even if you're 100% sure the problem isn't you, running through step 1 will help you develop critical stakeholder-engagement skills, ensure you leave the company on good terms, and make your resignation serve as a more potent wake-up call to the organization.

But if things don't change, there are many other workplaces that do want your skill set and want to do the right thing. Find one of them and go work there.

Being in-house compliance can be a difficult, lonely job in the best of circumstances. Do not waste your life on a company that doesn't want it.

What about Code training?

Good question. Because that "your Code training cost $2.5 million" statistic we gave earlier is brutal, but doesn't tell you how to fix it—mainly because Code-level training doesn't get at tasks and so isn't easily audited.

The reality is that your Code training is not going to be worth $2.5 million in risk reduction; it's too high-level. No one is learning to do anything specific from your Code training.

I am not 100% sure how we got to a place where everyone does these monster Code trainings, but they're divorced from the reality of your risk assessment and what the government is actually asking you to do and the fact that employees violently hate them.

At the same time, I get change management and political capital. So I know you're going to run into some static if you come back from a conference and say "hey, this [35-year-old] kid with a shaved head and tattoos said Code training doesn't work because of math and science, so let's not do it anymore."

Nor do I think that stopping Code training is necessarily the solution—it just needs to be done in a way that reflects what the real value is.

So here's what I recommend: make it as short as possible and focus on what people really need to know. And only they need to know four things.

(1) We have a Code
(2) It applies to everything you do*
(3) Here's how to find it
(4) Here's when you should go read it

You can give a few examples for #2, but anything else is too much. Your goal is to make sure they know how to find the Code when they need it, not memorize it right then.

The whole thing should take less than 10 minutes for someone to complete. And to be clear on the stakes: if you can get it down to 10 minutes from 1 hour, congratulations: under our hypothetical, you just saved your company over $2 million in real money.

And no, you do not need a video or a quiz or a game for this. Just do it on well-designed, minimal slides—they can be 100% text if your copywriting is on point.

And let your employees read the slides at their own pace, without being forced to listen to a slow-as-molasses voiceover or for the text to appear super slowly on each click.

Employees hate that stuff, because they're adults.

Remember, training is to help good employees, not catch bad ones. Someone who is committed to ignoring compliance is going to find a way to get around any stupid LMS trick you build—don't lose the good employees by treating everyone like children.

If you're seriously worried about bad apples, making training an expensive and painful experience for everyone is not the solution. It just alienates good employees without getting any closer to handling the bad ones.

Remember that training is one part of a compliance program, not the whole thing—it can't do the job of controls, auditing, and investigations. Instead of trying to win over bad apples with your training, use the other parts of your program: audit your high-risk tasks, investigate to track down the bad apples, and use discipline to get rid of them.

*I get that Codes do not specifically cover every possible situation, but I also guarantee you have a decision tree in your Code that you tell people to follow when that's the case. So it's still accurate to tell them in your Code training that it covers everything, because it does.

In conclusion:

You can do this.

Right now.

With the resources you have. The budget, the people, the buy-in, the experience, whatever. You can do it.

It doesn't matter what you've done in the past, or what you've already bought or licensed or rolled out. Those are all sunk costs; they exist whether you keep on the same path or do something different.

Whatever your situation is, it's the best it can be.

You can start this today.

Your biggest hurdle will be, honestly, fear. You will be afraid that you are not training people using risk modules loaded up into a LMS with little videos and games where they have to spend at least two minutes per slide, and that's different from what everyone else is doing, and that is a little scary.

Because even though you know that none of that junk works, at least everyone's doing it, so you can point to that if something goes wrong.

Which, of course, it will. Because you don't seriously believe that type of training makes a difference—that's why you're more concerned with completion rates and record-keeping than auditing for a real test, because you already know what auditing will tell you.

But you got into this field to make a difference.

So go do it. Pick the one place where you want to start and don't worry about the end of the journey—just take pride that you started it.

Get in touch:
hihi@thebroadcat.com

