Ethikos Volume 37, Number 4. October 01, 2023

Three low-cost ways to test if your compliance program is REALLY working

by Rupert Evill

Rupert Evill (rupert@ethicsinsight.co, linkedin.com/in/rupert-evill/) is founding director at Ethics Insight in Lewes, England, United Kingdom. Evill is also the author of Bootstrapping Ethics.

It's easy to get stuck doing *busywork*. This morning, I caught myself trying to change a bank card on a subscription I won't renew. Why? Because I'd received an email with legal language warning about the card's expiry. I was complying without thinking.

Risk and compliance can get like that. We have so many forms, boxes, tracking tools, and so on. All this busywork can distract us from focusing on 20% of our organization's work activities, creating 80% of risk. But how do we identify where to spend precious time without expensive and exhausting "assessments?"

Phone-a-friend

Could you commit to two to three 30-minute weekly calls for a year? You already do. Some of those calls may be staggeringly unproductive as you and others draft emails, "doomscroll" social media, and contemplate running away to open a pet-themed beach bar. One of the best excuses to avoid these calls is to have a legitimate excuse: "I've got to drop for another call." Take that option. Schedule two or three calls with people randomly selected from within your organization.

That's what a head of ethics and compliance for a 29-country multinational did. He'd had enough of creating content in a void and trying to understand why a robust *best practice* compliance framework was spluttering. He set a target for 100 conversations in a year. The agenda was kept loose. He wanted to understand the other person's compliance experience, challenges in their role, and support they needed (from him). At the end of the year, he had the following observations:

- He understood the business, risks, and pressures people face much more deeply.
- He built connections with people across the organization who continue to share information that helps us do better.
- He had a better handle on what people needed and wanted from him.

The elegance of this approach is its simplicity. One-on-one chats—with no bosses or peers eavesdropping—allow a more honest and personal conversation. Functions at the center in (regional) headquarters can seem aloof, removed, and irrelevant. When we emerge from "The Death Star" (a former colleague's name for HQ), we humanize our risk and compliance work. Unfortunately, our other appearances are often as enforcers (monitoring, investigation, risk assessment) or educators (training, communications, workshops). I'm not suggesting those can't be collaborative and constructive. But we're transmitting. There's nothing quite like listening!

Some of you may wonder about skewed data. I would, too. The trick is not to extrapolate based on location, function, seniority, etc. It's to look for trends that occur across the board. For more thematic and aggregated data, we need numbers—enter user experience surveys and speak-up data.

User experience

User experience (UX) makes you like the apps and sites you return to. It's about engaging and minimizing *friction* (the clunkiness that makes you hate most government websites). UX is not a strong focus in much risk content, alas. Understandably, we build content to meet regulatory requirements, like teaching school kids using the penal code as a textbook. Not incredibly inspiring and accessible.

We need lots of opinions to understand better where UX might need tweaking. Enter the 80/20 rule.

80% there in 20% of the time

I love the Pareto Principle—the 80/20 rule. In this instance, we used cleverly designed surveys to get us 80% of the risk assessment value 20% of the time (of workshops, interviews, etc.). The benefits don't stop there—these surveys usually help us triage a massive data set (I'll call it "human risk factors") down. With the insights we gain, we can go deep into 20% of activities or areas causing 80% of the risk.

First, let's step back and consider a good risk assessment. I'd argue that it starts with an understanding of the external context. What, who, how, where, and when do we encounter pressures that could create risks? For instance, on a recent project related to healthcare infrastructure, we identified licenses, land zoning, inspections, local community opposition, and access *could* be pressure points. That was before the facility was even operational. The extent to which those interactions represent risk depends on the who, how, where, and when (urgency, criticality, reliance).

Armed with a risk blueprint of what we do, we can consider what controls are appropriate—a "best practice benchmark." But we're missing the HUGE bit: Our people (not us) must uphold those standards when they meet external and internal pressures. What do they know, think, feel, and want? How is the risk and compliance UX for them?

Let's ask them. I use four domains to analyze the data:

1. Knowledge
2. Access
3. Accountability
4. Trust

Before getting to each, if you do use a survey tool, please:

- Vary the response options (we get bored, and not all questions need to exist on a Likert scale).
- Keep it anonymous—if you ask for location, function, length of service (or other valuable data), make sure that no one group is smaller than five people.
- Measure our answers and how we respond (drop-off rates, time taken to answer specific questions, etc.).

Knowing me, knowing you, aha!

When we do something for a while, we get cursed—the curse of knowledge. We can forget what it was like not to know. The goal is not to test the *what* of risk and compliance but the *how*. Do people know what's expected of them, where risk meets their roles, how to report a concern, the values and guiding principles, how to manage third parties, and so on?

It might not come as a huge surprise, but the data I've gathered suggests knowledge falls over the further you get from the author, working language familiarity, and a desk. For example, operational folks—usually connected to you only by their smartphone—don't always absorb the one-and-done induction training—especially if not delivered by a native speaker.

Access all areas

Following the knowledge gaps, we must also test local-level access. Do people know where to find support (policies to ethical dilemmas)? Does the speak-up framework work for them? Was the training relevant to their roles (accessible)?

UX requires that people can access timely and useable information. Again, this will differ across organizations, but I've noticed that access can be weakest in support functions. Many organizations purpose supportive resources to the rainmakers, developers, engineers, or whoever's targets most closely align with board-level rewards.

Accountable to everyone

Accountability is both personal and collective. Are incentives ethically realistic? Are team members held accountable? Is the risk and compliance framework realistic? What happens if something goes wrong? We must understand one of the significant drivers of pressure (and thereby risk)—what happens at the line-manager level.

The responses to these questions vary significantly. If I had to pick a theme, it would be that middle management is often most cynical about this. That's a problem when they're setting the tone and targets.

Trust and verify

Psychological safety is its own specialism, and books are written on it. To try and keep the scope tight, I'd focus here on comfort speaking up, taking risks, making mistakes, and trusting in the investigative (and nonretaliation) framework. Trust has been weakest (usually) in HQ functions. Returning to the Pareto Principle, that tells me the 20% I need to focus on with chats, workshops, or more assessments. The reasons for the breakdown in trust will differ, but a big one tends to be the groupthink and politics that can swirl around the seat of power. On a recent project, someone said, "Whenever I go to HQ, I'm having hushed conversations in quiet corridors." It's easier to speak truth to power when that power isn't omnipresent and directly impacting your daily life.

Some of you may be thinking, that's not us. You'd be right. Few organizations flunk all four UX areas. But even the ones with great ethical cultures typically have one topic needing some tender loving care. Isn't it better to know that and direct 80% of your time to the 20% (okay, 25%) needing attention?

(Not) speaking-up data

As we examine the user experience data, it's always fascinating to pair it with speak-up data (if you have it). You'll see some juxtapositions. For example, in a recent project, the brave people in one subsidiary kept speaking up against fraud and corruption. The whistleblowers often faced retaliation but kept going, incensed by a malaise that tormented their country, work, and personal lives. A fear of retaliation (from the user experience survey) paired oddly with a well-above-average speak-up rate.

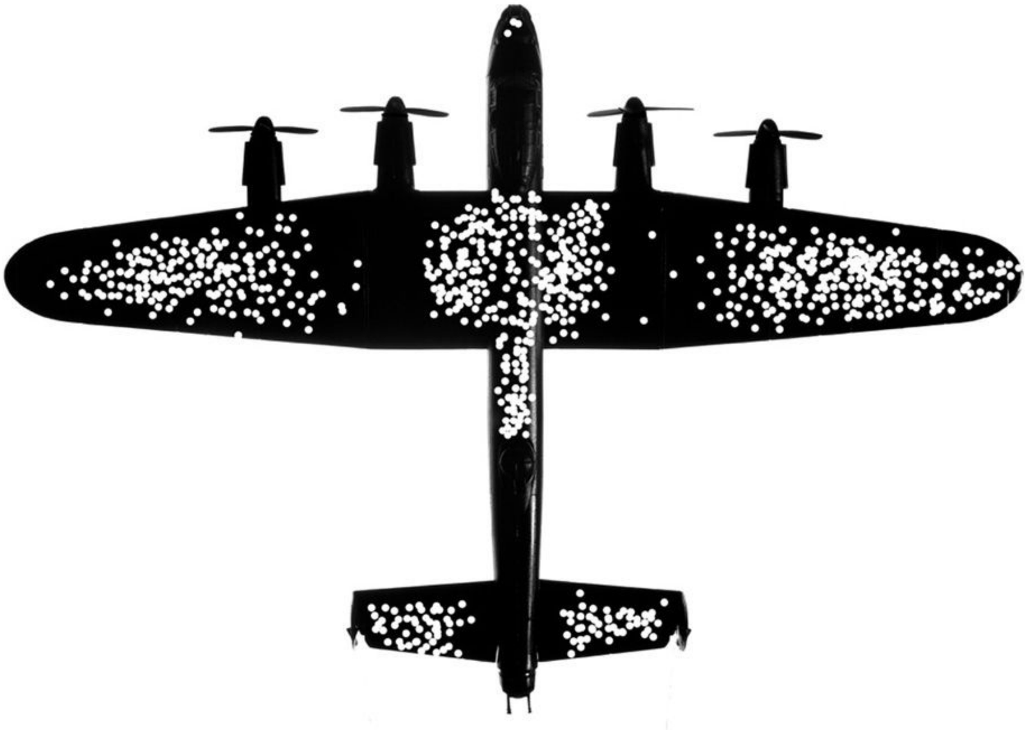
But what about where people are silent?

Aviation safety briefing

Many of you will have heard about the World War II airplane study.[1] A high number of Allied bombers were being downed on raids over Germany. Researchers at the Center for Naval Analysis started reviewing returning bombers, analyzing (in meticulous detail) the bullet and flak holes (see Figure 1). The thesis went something like, "Let's strengthen the bits of the plane [the wings and body] most peppered with holes." But that's not very helpful data.

These bombers had made it back. Those (presumably) with holes in the cockpit, engine, and parts of the tail had not returned. It was the absence of data that identified the risk. Acting on the flipped insight, those surviving the raids rose.

Figure 1



Source: https://www.trevorbragdon.com/p/when-data-gives-the-wrong-solution. Used with permission.

How do we find our risk and compliance cockpit, engine, and tail? By looking at what we do have. While clumsy, we can assume that the same functions and activities confer similar risk levels—especially if the operating environment is similar. I remember in the early 2000s, as Goldman Sachs coined the term BRICs (the term for a grouping of the economies of Brazil, Russia, India, China, and South Africa), a symposium where the heads of risk for Russia and Brazil agreed that their climate, politics, and culture might differ widely, but corruption manifested nearly identically. Much has changed since, but you get the picture—you will have some comparable data. Start there.

Focus on bridging gaps

Of course, there are good reasons that may explain discrepancies. But identifying them often unearths risk and compliance gold. I remember looking at two comparable Southeast Asian archipelago countries, where the risk data seemed widely different. In one, there was an excellent leadership team, a robust speak-up culture, and, therefore, seemingly more problems.

When we visited the silenced region, we were met with a leadership culture of apathy, fear, and blame shifting. Within a day, we'd identified that they paid bribes weekly to keep operating, but no one had ever dared air that pretty problematic (and universally known) nugget. That was the bad news. The good news was that we had a pretty good template from the functional leadership team, including how they'd worked through seemingly intractable and bleedingly vicious extortive bribe requests from critical stakeholders.

Time and cost

There are undoubtedly time commitments to these low-cost risk and compliance program efficacy tests. But how much time are you currently spending developing content in a void or stuff few people will ever read? That's not a criticism; every role has boxes to be ticked.

A friend recently explained how they'd been asked to provide a diversity and inclusion policy as part of a requirement on a request for proposal. This friend is the sole employee, a solopreneur. They ticked the box, sending a quickly compiled policy they were sure no one read. That's compliance.

As a solopreneur, it helps to think about your suppliers, partners, and behaviors in the context of diversity and inclusion. If everyone you work with looks like you, that might not be good. The request for the policy sparked that analysis. That's assessing risk.

Tick boxes quietly and quickly and assess risk thoughtfully and through engagement.

Takeaways

- If we consider our colleagues as customers, we start to build frameworks and content with them in mind. This increases knowledge, access, and trust.
- We must listen to maintain accountability. When we do, and we examine the missing speak-up data, we can start to protect the organization from previously hidden risks.

[1] Trevor Bragdon, "When data gives the wrong solution," September 7, 2017, https://www.trevorbragdon.com/when-data-gives-the-wrong-solution.