COSMOS
Navigate the Compliance Universe

Ethikos Volume 36, Number 3. July 02, 2022
Three Cs: Counterterrorism, counterespionage, and crisis management-Lessons for compliance

By Rupert Evill

Rupert Evill (rupert@ethicsinsight.co) is the founding director at Ethics Insight in Singapore and London.

Whatever area of risk and ethics and compliance (E&C) one is focused on, we all are broadly concerned with prevention, detection, and response. Counterterrorism requires precision in assessment, analysis, and communication that can help those of us working on preventive E&C measures. Counterespionage, by definition, fixates on detection and monitoring, posing some great questions and quandaries for us in E&C. Crisis management is the art of proportionate and effective response.

Having worked in each area in the past few decades, I'm starting to see where the different disciplines can help each other.

Counterterrorism class

Effective counterterrorism (CT) is multidimensional. We must consider several additional Cs: context, culture, capacity, and crown jewels.

Context

What is the operating context? In E&C, I sometimes see myopia around specific risk issues. We look to indexes to assess country-level corruption, money laundering, modern slavery, and sanctions. I would avoid such extractions at the national level. Your exposure is a function of what you do, where precisely in the country, whom you do it with, and how you do it.

For instance, a Texas-based biotech disruptor in the fertility space faces starkly different risks from a cryptocurrency platform in Manhattan. In CT, we're concerned with a broader basket of contextual indicators of risk. Political capacity, the rule of law, the efficacy of security forces, local-level demographics (including social issues), history, and conflict are all factors. I'm not suggesting that E&C professionals become country analysts for every single location of operation. This knowledge sits in the heads of your people—using around 20 E&C–specific country context questions (typically taking around four minutes to complete), we gather infinitely more insightful data than we do from indexes.

Culture

Next, we must understand the local culture. Whether your position is oppositional (looking for baddies) or capacity-building (hearts and minds), it's near impossible if you don't understand the societal, religious, cultural, and political dynamics at play.

For E&C culture analysis, we're most interested in knowledge, access, and trust. Are the compliance constructs understood by our audience? Conflicts of interests, gifts, hospitality and entertainment, and anti-competitive practices travel particularly poorly. Next, we should look at access to support (including leadership) and

resources. Many E&C failures occur when employees don't feel they can ask for help, admit they don't know what to do, or access advice quickly. Finally, we need to know whether people trust the leadership—and E&C. Trust is often more about perception than anything else. Do people feel leaders *walk the talk*, is everyone held equally accountable, and do employees feel leaders in faraway headquarters understand their frontline realities? Do they feel safe (nonretaliation, confidentiality, and anonymity) if they speak up?

I spent much of my career developing assets (i.e., human sources of information and intelligence). Asking people to tell you secrets or actively gathering intelligence in places where it can have severe consequences for life and liberty is a sobering endeavor. I sometimes see Northern European and North American E&C and leadership teams struggle to conceptualize that the *speaking truth to power* they hold sacred in their flat (and safer) hierarchies is almost entirely alien to others.

Finally, when we assess vulnerability in CT, we consider both security (controls) and predictability (culture). If terrorists know you go to the gym after dropping your kids off at school using the same route, your home fortress is rendered obsolete, and you're now an easy target for kidnapping. Similarly, in E&C, there can be a tendency to obsess about controls rather than the predictable (nonthinking and nonconscious) application of those steps. Where are you on autopilot?

Capacity and intent

When considering terrorist threats, we're concerned about capacity (capability) and intent. Not all threats are created equal. In E&C, we can assume that all threats are created equal. For example, corrupt demands are uniform.

An environmental inspector might cite (possibly spurious) violations in your facility that they're willing to overlook "for a small fee," or they'll hit you with a hefty fine (leveraging opaque regulations to their favor). A deputy minister furiously scrambling to buy votes for an impending election who threatens to cancel your operating license unless you pay millions is a different proposition. In this case, the minister's capacity is weak and their intent broad. Even in a very dysfunctional country, it's tricky taking a proposal to cancel a license generating massive revenue to your cabinet without a solid (quasi-)legal basis. My client was one of many targets for similar shotgun strategy shakedowns.

Again, there will be people in (and sometimes outside) your company who will know the unethical runners and riders. Qualifying the threat posed by external stakeholders—including (fair or capricious) regulators—will save time in the long term as you won't be doing the CT equivalent of assuming angry trolls pose similar risks as battle-trained insurgents.

Crown jewels

What do terrorists want? The answer depends on the terrorists' intent. If we know more about the intentions of external stakeholders, we have two tactical advantages: we know what to defend and how to negotiate. In the deputy minister example, the license cancellation required the approval of a local transport authority. Initially, the authority went along with the threats (bullets in the mail and alike). Still, if they canceled the license, it would significantly harm their reelection chances (in midterm equivalents). They'd previously campaigned on a go-green initiative and done nothing about it. My client implemented a raft of more sustainable changes (diesel to electric, renewable energy sources, and more). We then invited the local authority down to the unveiling of an upgraded facility, telling them they could take the photo opportunity and credit if they left us alone; they agreed.

As you map your security and predictability, spend the most time on your crown jewels. Next, consider what your higher-risk stakeholders consider your crown jewels—yes, cash will often be king, but not always. We can

often find ethical ways to appease challenging stakeholders.

Counterespionage

Spy-hunting is an issue in most strategic sectors. What is strategic will depend on the threat actor's intent. It's very tough, because it poses numerous ethical and tactical questions. For example, if we know that state-sponsored espionage efforts focus on our sector, do we view employees from that nation as a potential threat? Profiling, privacy, permitted technology, acceptable monitoring, and proportionate controls are also recurrent challenges in E&C detection.

If you've done the risk assessment piece, including establishing intent, capacity, and crown jewels, it becomes easier to categorize both threat actors and your vulnerabilities tightly. This exercise helps justify proportionate monitoring controls. For example, a manufacturer of rail equipment working on new technology for its domestic national railways might legitimately restrict access to the research and development to those who've undergone security clearance. Such controls are more palatable than profiling citizens from (ancestrally or by birth) hostile foreign state actors.

Behavioral analysis

We now also face questions about privacy and surveillance. In counterespionage, we use the same technical tools that E&C teams increasingly have. However, we're more concerned with humans and behavior. Behavioral analysis is not about Pinocchio's nose—there is no universal indicator of deception (or broader ill intent)—it's about clusters of behavior. Once we understand this, we can focus on analyzing behaviors in higher-risk areas.

In the E&C context, mapping your crown jewels against potential stakeholder threats provides the monitoring blueprint. For instance, let's say you make high-end electronic equipment in an emerging market run by a single-party state with aggressive growth plans. You have intellectual property of value to domestic competition (and potentially the authorities). Your products will likely have a high black or gray market value. You'll often need materials quickly, making you vulnerable to extortive shakedown attempts from customs. The components might include gold, rare earth metals, and other items with considerable scrap value. That's just for starters, but now we know what areas might merit monitoring and what behaviors to consider, and we can start to choose appropriate detection tools.

Blue on blue

If you're struggling to know where to start, the risk assessment process should help, but so will asking your people to play baddy. It's a surprisingly fun exercise to ask people, "If you were to defraud [or another undesirable act] us, how would you do it?"

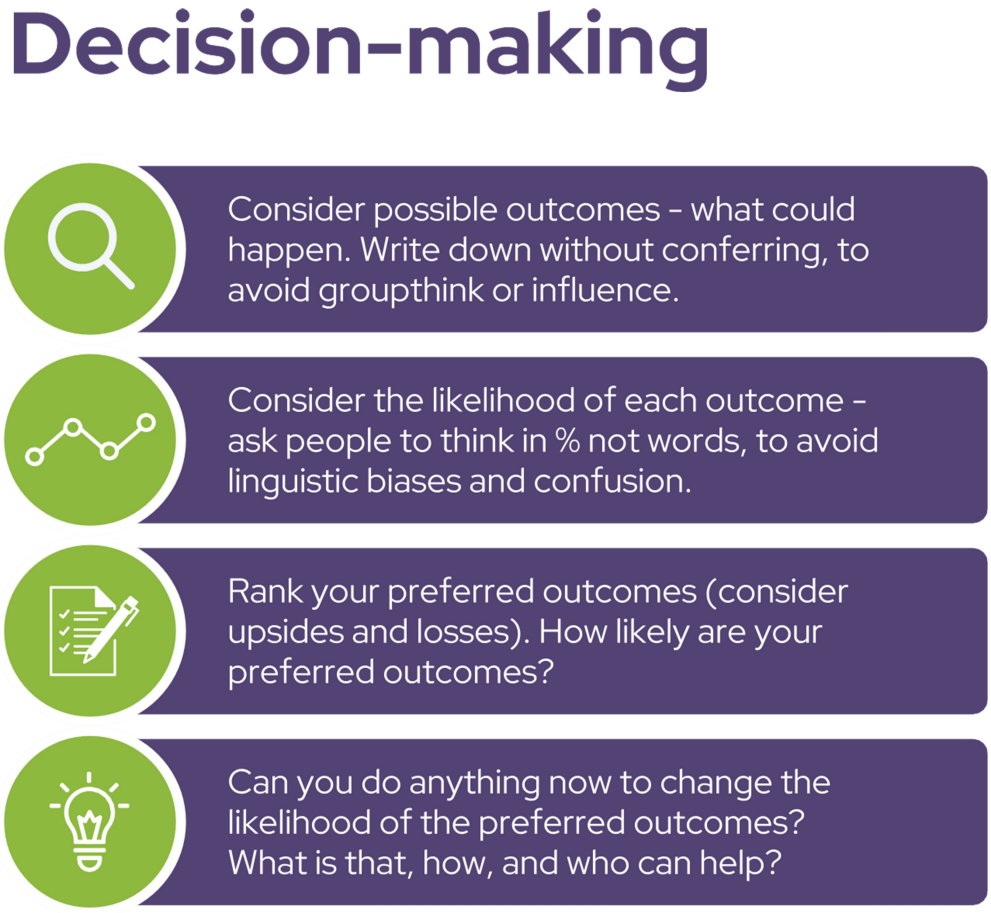
Finally, go back to your data on employee trust (and other contextual factors that may inhibit speaking up). Tips remain a primary counterespionage and E&C tool. I cannot emphasize enough how important it is to earn your people's trust. Even in markets where the geopolitical forces may be hostile, your employees don't wake up wanting to be the bad guy.

Crisis management

Making sense of chaos and responding, not reacting, have helped in every facet of my life. You don't have time for long policies or complex controls when everything has gone to hell. Crisis management forces simplicity in decisions, communication clarity, and opinion diversity.

I've used the model in Figure 1 in cases spanning the topics covered in this article. It works in all settings, so we're now repurposing it to help make better ethical decisions.

Figure 1: Decision-making model



Facts and assumptions

The first step is to distill assumptions into facts. We leap to conclusions, especially when facing threats, discomfort, or conflict. A country manager of a large infrastructure firm recently explained how his firm had won a large contract in a middle-income market. He knew his sales team was taking the client out to dinner and decided to gate-crash. Upon arrival, he was horrified to see the client ordering a spread that even Nero or the Romanovs might have felt a touch opulent; the wine bill alone was heading toward GDP per annum territory. It wasn't that his sales team encouraged the client; they'd been railroaded and didn't know how to refuse an influential stakeholder. The team needed the manager to play a strict senior foreigner who was there to keep things by the book to help them save face in front of the client—and avoid picking up the entire tab. Responding to (mini or major) crises requires us to step back and check facts before acting.

Often, in E&C issues, the facts might be sparse. Many reporting-line allegations or complaints are light on detail.

We must avoid the temptation to leap to action and instead check assumptions. Having identified the most significant assumptions—often that the allegation is credible and material or the stakeholder has both capacity and intent—we should test them. In the deputy minister's example, this was relatively easy. We found out very quickly that they'd be running around town shaking down anyone and everyone rich. This clarification of assumptions can make all the difference between a proportionate or preposterous response.

Outcomes and scenarios

If we're dealing with a (potentially) significant issue, we need to consider outcomes. When we do this as groups, it's a disaster. If you ask people for a show of hands, you'll be swayed by the majority. If you ask us to write down our decision, you'll get a much greater plurality of opinions. In E&C, we want different perspectives to calibrate outcomes (impact especially). Similarly, we assess likelihood differently, especially when the semantics of the language are involved (use percentage probability to hack that challenge).

I appreciate that you may not have time for committee meetings and voting on every issue, but if you can get more than one view, it helps. With an idea of facts, assumptions, and outcomes (impact and likelihood), we can consider what we'd *like* to happen. In many E&C cases, this can seem like a quick decision, but pause for a second. I've worked on many cases where people have made the right decision too hastily—for example, terminating suppliers for fraud before considering blowback that ended in violent assaults with machetes. In more cases than you might think, the guilty parties will retaliate. This response can range from irksome to lethal.

Focus on the goal

Taking a recovery-led approach to crises, investigations, and complaints makes sense wherever you operate. Our core focus is to preserve life, assets, and business continuity. We're not solely fixated on innocence or guilt, as can happen in E&C cases.

For this reason, we're always considering how we can influence and change outcomes. Whatever strategies you develop should include contingencies. This mental exercise of triggers and responses forces and creates a better decision-making discipline.

Change is the only constant

I like to use an ABC model shown in Figure 2 to bring these strands together—Assess, Build, and Change are the core components in E&C, whether you're preventing, detecting, or responding.

- If we train our assessment muscles to go beyond surface-level data, we can better**prevent** issues, as a CT specialist would. Next, we need to build content, capacity, and trust in our preventive framework, adapting and changing (culture, controls, leadership) as necessary.
- We're doing what counterespionage specialists do in **detect** mode by looking for models. Focus on what matters: assessing risks to your crown jewels, building content to reduce vulnerabilities, and monitoring changes in behaviors.
- To **respond** appropriately, we assess the issue, build scenarios, change how we approach problems, consider outcomes, and respond with recovery as your focus.

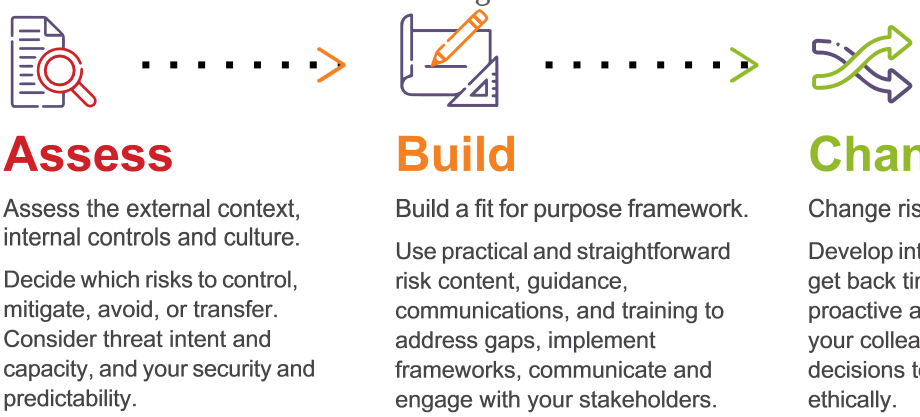
If you want a hack to make your leadership take these lessons seriously, run a simulated crisis exercise. I remember one occasion when we split the leadership team into four groups. Each was given the same initial E&C allegation as their starting point, and we'd anticipated where they might go (like Choose Your Own Adventure books). After one hour:

- Group one had panicked and exited the country in question, leaving staff stranded and millions of dollars of equipment confiscated.
- The second group disparaged local politicians to the press and faced a dawn raid.
- The third group was alive and well, which was a win!
- When asked to present back to the general counsel, who was heading into an emergency board meeting, the final group had hired paramilitary goons to protect the facility after a riot involving the local community. They told the general counsel, "It was only a little bit of violence."

Better to make mistakes in a safe environment and train those decision-making muscles!

Don't be daunted; we're constantly assessing, building content and systems, and changing our responses accordingly. Sometimes it just helps to have a structure and framework to practice with.

Figure 2: An ABC model



Takeaways

- You can better prevent, detect, and respond to issues by qualifying threats (considering capacity and intent), monitoring compliance using behavioral indicators, and responding to problems with a recovery mindset.
- Step back from your compliance program and ask what needs assessing, building, and changing across those prevention, detection, and response categories.