ethicsinsight

# Making Risk Relevant Whitepaper


ETHICSINSIGHT.CO

# Introduction

This document may be titled a white paper, but it's not – the (virtual) paper is colourful. Less facetiously, when I think of white papers, I imagine well-researched and footnoted academic literature. Not here. For better or worse, the contents represent my experiences and observations working with many different organisations (large and small, for-profit, government, or not-for-profit) across various countries. I've seen more similarities than differences – more common pain points than unique problems.

This document attempts to bring together varied experiences into what I hope is helpful, examining the challenges and offering solutions. Within the scope of this paper, you will not find every answer, but I doubt you expected to. I hope it provides food for thought and starts discussions. If you'd like to expand on any topic, you know where to find me!

The eagle-eyed amongst you – all of you – will see that the order of topics does not match regulatory guidance. That is intentional. The structure reflects where I hope you can create the most impact.

**Rupert Evill**
**Founder - Ethics Insight**

ethicsinsight

# Contents

# Executive Summary

Risk, Ethics & Compliance (E&C) is much like medicine, only we've gone from leeches and animal bile enemas to keyhole surgery in about fifteen years. The resourcing has not kept pace – most E&C teams I meet are on the soothsayer end of the budgetary spectrum, less Los Angeles plastic surgeons. E&C, when I started in 2001, was fraud prevention, money laundering, and a smattering of corruption in "the third world". I'm very relieved it's changed.

E&C's remit in most instances extends to overlap with other functions, including human resources, legal, information technology, physical security, communications, finance, and procurement. This expanded scope correlates with increased enforcement, more stringent regulations, and society in change. Yes, there are exceptions, but as a rule, I see more similarity in employee, customer, and stakeholder expectations than differences. Organisations can no longer sit on the sidelines during societal, social, and political movements. Faced with complexity, we have two options: get lost in the maze or elevate and simplify.

The latter option seems more palatable, which is why if you drew a Venn diagram of every area covered by E&C, that central circle, where all areas overlap, would be packed.

Effective E&C is a function of a few common-sense rules:

1. Clear communication with all stakeholders: You're not doing it right if you can't explain it to a 10-year-old.
2. Knowledge, access and trust: The consumers of your E&C content must understand it, have access to support, and trust you (speak up to enforcement).
3. Plagiarism is good: If other functions have changed behaviours and decreased risk, what did they do?
4. Timing matters: Understand when your people face pressures or decision-fatigue.
5. Behaviour leads and tech follows: E&C is a human discipline, which requires an understanding of why we behave as we do; technology is a tool, not a guide.

Now, it's time to operationalise those rules.

# Risk Assessment

Risk assessment is the kryptonite to risk and E&C professionals' superhero status. It is the origin but also a process of self-harm for many organisations. Why?

## Problems – one dimensional, one and done

Risk assessment is frequently an internal exercise focused on examining controls, not external context and internal culture, creating issues, including:

1. Analysing what is written, not what is implemented.
2. Using binary (Y/N) scoring, rather than reflecting that controls efficacy is a scale from ineffective to effective.
3. Focusing on a snapshot in time, not considering if the control is improving or deteriorating.
4. The assessment is intermittent, not a living and breathing part of risk management.
5. A failure to consider the external context (where your good intentions meet risk realities and unethical pressures).
6. Not matching controls and broader risk analysis with purpose, values, and risk appetite.
7. No meaningful study of culture.

**Consider where good intentions meet risk realities and unethical pressures.**

If you're looking at that third point and wondering how a control might worsen, consider confidentiality clauses, rights to audit, and social media policies. The hashtag era of leaked internal memos, videos, and communications suggests that confidentiality clauses no longer cover the heft they once did. Audit rights are tough to enforce in many situations, especially in a divided world. Social media policies that don't evolve quickly risk being obsolete as soon as they're uploaded.

Mapping internal controls without considering external risks (point 5) is like testing a sunscreen's efficacy in the dark. We must understand what happens when our internal defences meet the great big world.

Purpose, values and risk appetite (should) dictate what matters to your organisation. For instance, in Singapore, some domestic banks appear to be more frequently mentioned in connection with scams targeting their consumers. Maybe that reflects their resources, but I don't think so. I get the sense consumer protection is not prioritised evenly across the banks. Risk and E&C folks can sometimes see all controls as equals. They are not. For example, data breaches, product recalls, and workplace accidents (among many other areas) are often viewed very differently by firms operating in the same space.

Analysis of risk culture – by which I mean knowledge of, access to, and trust in the risk and E&C framework – strikes the fear into many. Why? There's no rejection like hundreds (or maybe thousands) of colleagues telling us our training stinks. I've sifted through thousands of feedback forms for content I've developed or training given. It is natural to gravitate toward the negative (for me, at least), but it's hard to improve without it.

## Possible solutions – three dimensional and living

What are the antidotes to the malaise above? I'd argue the structure should look something like the steps below.

### A) Risk appetite

An assessment without understanding our organisation's appetite and tolerance of risk is doomed to a life of irrelevance and abstraction. Sometimes risk appetite is very simple, don't break the law. What can we do for the rest of us with slightly more progressive morals? An internet search for risk tolerance (the more granular cousin of appetite) will lead you down a rabbit hole littered with confusing numerical droppings – share price percentage drops between X and Y, or operational delays of between A and B days. Maybe this is risk charlatanism, but in E&C especially, I find most of the estimations are inaccurate and unhelpful.

I'd opt for something a bit simpler. What is it you value as an organisation? For some of us, brand, reputation, customer loyalty, and other less tangible elements might lead. Or it could be assets (people and physical or intellectual property). This exercise requires examination of both your values (the real ones, not any performative ones on websites) and an inventory of what makes your organisation survive or thrive.

Next, you'll have to think of what could go wrong. Your code of conduct (or business ethics) will generally summarise the key things you don't want to happen; bribery, fraud, human rights violations, etc. In most sectors, you will be able to find an example of a code violation befalling others in your location or sector. Then it's time to think laterally about events with impacts that are sector (and sometimes even site) agnostic – imagining a pandemic, for example. For example, we might argue that Facebook can weather successive legal and regulatory storms, but how would it survive a world with less energy and electricity?


'That's it agreed then - the company's new motto is going to be *"We didn't do anything illegal"*.'

The questions I've summarised in the subsequent sections – while not exhaustive – may help spur ideas. Once you have your scenarios and ideas of what could go wrong, put them to your leadership, and ask them on a sliding scale (tolerable to intolerable) what they could live with if the worst happened.

## B) External risk analysis

Now we can approach our analysis of the external operating environment with a little more nuance (and relevance). The questions will vary depending on what you do, but this list is a simple starter pack (asked on an agree-disagree scale).

Who should you ask? Typically, a selection with frontline experience from within your organisation. Isn't that a lot of work? The first time it can be, yes. After that, it gets easier. Or, if you'd like to try out this assessment (and get a free report and analysis) for yourself, we've set up a tool HERE.

| | AREA | QUESTION |
|---|---|---|
| 1 | COUNTRY RISK | I trust the legal system |
| 2 | COUNTRY RISK | Government and public institutions are not a source of corruption |
| 3 | COUNTRY RISK | Human rights are respected and protected |
| 4 | COUNTRY RISK | Civil unrest, strikes, riots and other disturbances are rare |
| 5 | COUNTRY RISK | Crime - including violent crime - is not generally an issue |
| 6 | SECTOR RISK | Our sector is not exposed to human rights or labour issues |
| 7 | SECTOR RISK | We don't collaborate or communicate with competitors |
| 8 | SECTOR RISK | The potential environmental impacts of our activities are limited |
| 9 | SECTOR RISK | Our sector is diverse, with different groups represented in leadership positions |
| 10 | SECTOR RISK | We are not the target of campaigns, boycotts or protests |
| 11 | BUSINESS MODEL | We are not involved in any government contracts |
| 12 | BUSINESS MODEL | We do not make political donations or lobby political bodies |
| 13 | BUSINESS MODEL | Giving or receiving gifts, hospitality, or entertainment is rare |
| 14 | BUSINESS MODEL | We do not use intermediaries to win business or handle customers |
| 15 | BUSINESS MODEL | We have clear visibility of our supply chain (inputs, people, processes) |

Can't I just use one of the indexes? You can, but most will sit at the country (and sometimes a smattering on the sector) level, so you miss many details depending on where exactly you operate, with whom, and how. If that's a bit abstract, imagine trying to arrive at "country risk" alone for two firms in the United States, a tech start-up in Silicon Valley and a port operator in New Jersey.

You can go as deep with this process as you like. I've seen and worked on risk assessments that map stakeholders (by group typically), events, and interactions with probability and impact. If you're operating in high-risk markets, this level of detail can be the difference between success and failure.

### C) Internal risk and culture analysis

For internal controls, the simple step of moving from (often binary) having assessments to doing (implementation) analysis can be transformative. Rather than asking, "Do you have XYZ policy?" we can ask questions about what's included, how it's implemented and whether it is trusted. We put together a a Compliance Maturity Scorecard HERE to demonstrate.

This blending of control and culture questions typically gives much deeper insight into where we should deploy risk and E&C resources. Some of the questions I like to use for this work are below (or you can try our Reduce Integrity Risk Scorecard HERE).

> *My manager trusts me*
> *I am confident speaking up*
> *My opinions are valued*
> *I feel safe to make decisions*
> *I feel safe making mistakes*
> *I can ask team members for help*
> *I am treated fairly*
> *I am held accountable for my actions*

I'd prefer to use surveys, polls, or anything with some anonymity. To ensure the data is useable, group people, but the minimum group size should be five people. It helps to know the finance team in Country A are struggling to understand the gifts, entertainment, and hospitality expenses system. Without data on that team, it's hard to contextualise and develop a solution.

Technology has a role to play here and in the external assessment. Tech can help with analysis, reaching people, and speeding up the process, but we must choose the questions carefully. When we built the minimum viable product of our platform, benchmarking risk, our questions were perfect for seasoned E&C professionals but too complex for the users of their content. There is a tendency to want tech to solve issues for us, but I feel its job is to get us 80% of the way there in 20% of the time (and cost). We still need to follow up with people to contextualise specific findings. If you bear this in mind when creating questions (that you do not need to cover 100% of the issues), it will likely be more effective and better received by your colleagues.


**To ensure the data is useable, group people, but the minimum group size should be five people.**

# Policies & Procedures

Nothing elicits a yawn quite like a policy, and that's the best case. The more likely scenario sees the person skimming the document (if at all) and signing. If you're thinking, that's not me, you may be right, as many of you reading will come from legal backgrounds. However, do you remember the last time you updated that little habit-forming snitch next to you (your phone)? Did you read the terms & conditions?

## The problem – sleep aids

Nothing elicits a yawn quite like a policy, and that's the best case. The more likely scenario sees the person skimming the document (if at all) and signing. If you're thinking, that's not me, you may be right, as many of you reading will come from legal backgrounds. However, do you remember the last time you updated that little habit-forming snitch next to you (your phone)? Did you read the terms & conditions?

> *"Ah, thank you for printing out those policies; I needed some fire-starting materials."*

### Who?

Who is the intended audience? That may seem like a daft question but bear with me. When we write policies and procedures, often it's a tightrope act balancing regulator demands and the business realities. The good news is that some regulators are now waking up to realise that if written content isn't simple to understand, it's unlikely to work
.

### What?

What knowledge are we assuming? When you're an expert on a given topic, it can sometimes be tricky to step back. What is intuitive and a given for you isn't for most others. Furthermore, have we checked what is feasible? It's all well and good to create mandates and frameworks, but good luck if they jar with operational realities or existing systems and knowledge.

Add a few layers of cultural differences, and we soon start writing content that doesn't travel well. For example, if you live in a country where small bribes to get officials to do pretty much anything are commonplace, the term "zero tolerance of facilitation payments" might not work. Firstly, it's impractical and fails to recognise the enormous challenges. It also makes little sense if the reader does not speak UK Bribery Act.

### How much?

How much detail is enough? The answer will depend on your organisation, the audience, and other demographic data. If your long policies aren't getting read, a move toward brevity may seem logical, but how exactly? Simply cutting out or editing down may not help if the content still doesn't speak to the audience and reflect their reality.

## Possible solutions - plain speak

There are many solutions to writing better policies and procedures, but these three rules are a start.

### A) Listen

Have you asked your colleagues what they need? We need to listen to the experts to move a policy into practice. Say you're talking about supply chain transparency and understanding the environmental and social impacts. You could start with the (frequently) nonsensical lists your local stock exchange issued. Or you could ask folks in procurement and operations who understand both the inputs and the supplier selection process. Armed with their advice, you can share what (you think) the regulators are seeking to achieve.

Crowdsourcing policies may seem like a recipe for death by committee. The simple hack is to tell those involved that whatever you co-create, they will need to operationalise, which tends to sharpen the focus.

## B) The roll eye test

Borrow a pre-teen if you don't have one of your own (lucky you!). Read the first few lines of the policy and if they're pulling this face, work harder.

Pre-teens will typically have a solid vocabulary that might serve as a sensible benchmark in your organisation. If they understand each of the words but not the phrasing or intention, the concept isn't clear enough. Furthermore, younger folks have much less restrictive imaginations than most of us fake adults. Asking them how you might better present the concept can be illuminating.

If you can't access a pre-teen, read your policy aloud in a monotone. I like to channel my 'David Beckham reads the phonebook voice', and if you fall asleep or confuse yourself, back to the drawing board.

## C) Borrow or steal

Can you steal or borrow? The content should be your own, but the delivery method is often replicable. Health and safety content has been a happy hunting ground for me. There's little room for ambiguity when trying to prevent harm, which forces clarity of message often missing from other guidance.

Other disciplines often don't feel burdened with preambles, context, and legal background. For example, cyber policies don't spend a long time discussing how malware infects a computer. Health and safety experts don't need us to understand the chemical reactions creating combustible mixes. Maybe we could learn from this. Does everyone in the organisation need to understand the intricacies of placement, layering and integration in money laundering? Or do they need to know that we must understand the identity of a customer and the origins of their wealth to ensure the funds are not illicit?

**Keep it simple, steal from creative types who've gone before you..**

# Training & Communication

> *""More compliance training,"*
> *No one, ever.*

## The problem – struggling actors, once a year

A common question around training & communication goes something like, "We're thinking of maybe an amination or a video, something engaging." The intention is a noble one – to improve on PowerPoint – but the medium is not the message. If you think of a book that confused you, transposing that book into a film, podcast, or cartoon may not help much.

Now, let's say we watch that film annually or sporadically. How confident are you that you'd be able to recall the key elements? Some of us (not me) have great memories, and perhaps we'd be able to regurgitate the key features. But could you apply that data in a real-world setting? Let's say the book was about vehicle mechanics, and it's now a video of someone fixing up cars. Would you feel confident driving in something you'd fixed after watching a video a year ago?

In this analogy, a lot of training & communication goes further than purely showing vehicle repair. The video might start with a long preamble about the combustion engine and its importance to society.

The only difference between a mechanic video and much of the E&C training content I've seen is the use of struggling actors. Much of the training we (in the industry), like giving ourselves awards for (because it uses struggling actors and a pensive and taught soundtrack), is not working. Middle school production quality videos or freelancer animations only work if the message is relevant, concise, applicable, and implementable. The message is not the medium!

## Possible solutions – relevant, adaptable, repeated

What could we try instead?

### A) User-focused

Does everyone need to know everything? Nope. If I pick a favourite topic, anti-corruption and anti-bribery as an example. Do your business development people need to know about facilitation payments made to customs officials in your supply chain? Probably not in that detail. Do your finance people (assuming, like most such teams, they don't get out much) need guidance on appropriate client hospitality? Function-specific training is increasingly the norm, but it often follows "high-level training". If you have your values and purpose squared away, could you improve that generic training, which is usually a long dirge about how corporate failures are bad, with scary data around fines, harm and jail time?

What I'm driving at here is the ten-year-old test. Can you condense the messages in that high-level training down to the core behaviours (not the mechanics or consequences)? Can you explain that we never pay to get something we have no right to? A couple of examples tailored to the user could then drive the point home. For example, the senior leaders might see a scenario around tender manipulation, whereas the factory manager will get one around paying off an inspector for a favourable environmental review. Most organisations have enough data classification (by job function) to make this work.

### B) Different channels

Training offers measurable data (attendance and completion rates). However, it's the comprehension that matters. Yes, training should ideally utilise different channels (in-person, virtual, online, etc.), but start with the intention. What does that look like in practice?

| GOAL | TRAINING OPTION | LEARNING CONSIDERATIONS | TEST OF SUCCESS |
|---|---|---|---|
| Raise awareness | Yes, here visuals and conceptual content might work but keep it short. | Is the concept common sense (e.g., anti-fraud – don't steal), or does it require technical know-how (e.g., data privacy or environmental compliance)? For simpler training, link back to values and behaviours. For more complex training, direct the user to where they can find resources, support, and contacts of people with answers. | If a ten-year-old doesn't understand the call to action, it fails. |
| Gather information or find solutions | A facilitated session with x3 of them talking to x1 of you. | Come prepared with samples, examples, and scenarios. To understand what's happening (e.g., a risk assessment workshop), we must talk in specifics, not the abstract. Use scenarios to stimulate discussion. Use polls and surveys (anonymous) to let quieter/fearful people speak. | Useable output (as people raise issues, don't be shy to say, "I don't understand"). |
| Implement a system or process | Online modules, user-paced (as we learn differently), follow up with facilitated clinics. | Have a look at demo videos for other products and see what you like. Break down learning into steps (no one wants to sit through 20mins of video). Test knowledge after each step (not at the end). Embed cheat sheets and guides throughout. Provide contact details and clinic options to allow discursive learners their chance to engage. | User acceptance, pass rates on tests, downloads of materials. |
| Change behaviours | All of the above. | Start with the concept (where we want to get to), discuss the issue (gather feedback) and barriers to success, find solutions to those challenges, and crowdsource approaches that work (better). | Psychological safety metrics (confused? Ask me). |

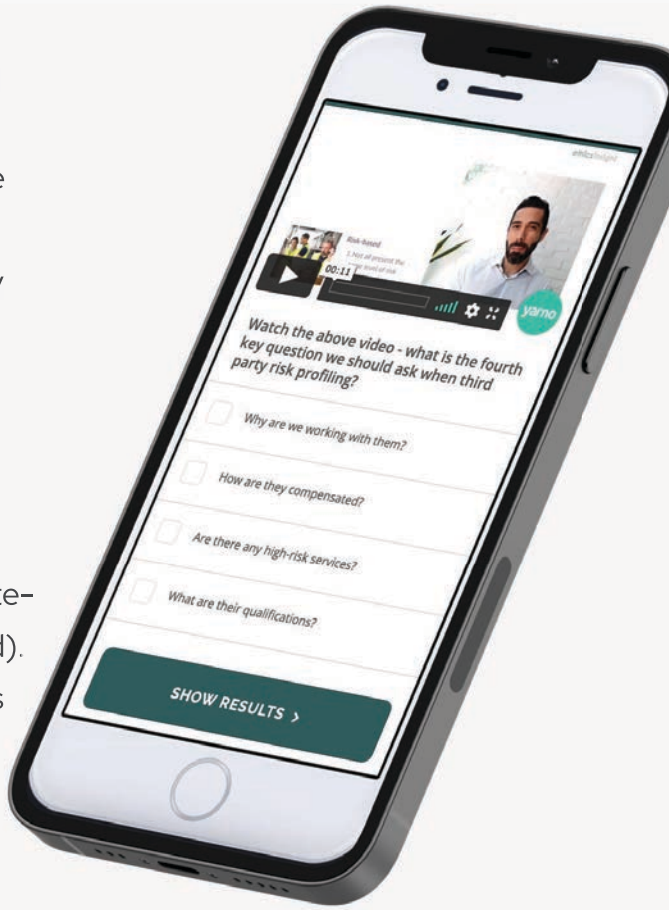
The table is not exhaustive, but it does demonstrate that we need different tools depending on the task.

## C) Spaced repetition and microlearning

Think back to learning a language. We had vocab lists to learn at school, lessons focused on grammar and structure, with aural comprehension and the odd bit of clumsy role-play. Is it any wonder I herald from a nation of people who are utterly hopeless at speaking other languages! The vocab was abstract; the grammar unrelatable; the Dupont family's shenanigans in La Rochelle were about as interesting as the character development in Paw Patrol.

Apps like Duolingo have worked out that we learn by doing (the shock!), much as we learned our native tongue. So is it true of any new skill or behaviour? Microlearning gets a confusing press. Some see it as a solution to their crappy content – simply parse it into smaller chunks. Others see it as lacking the immersive element of intentional practice. I see it as a tool. If you're introducing new topics, break them down into bite-sized components, and let people learn by doing (answering questions and navigating scenarios, making mistakes). We're increasingly time-poor, so you're not going to hold attention for two hours, and knowledge will not be retained unless practised.

You'll have read research about how quickly we forget (if not, google Herman Ebbinghaus). To help, use spaced repetition, a fancy term for reminders (usually three to four times in the two weeks after the initial training). I'm not suggesting you ask people to endure the same content repeatedly. Ideally, your systems should be able to learn and refresh the user's memory with variations of the theme (and targeted reminders around areas they struggled with). If this sounds fanciful, it's not. It's already here, we use it.




While downloading apps can cause issues in organisations (security, personal devices, etc.), remote-enabled platforms don't require apps (browser-based). Reaching your user on the device they use the most is essential. It's critical if many of your people are not deskbound (e.g., construction) or not on company email (e.g., contract staff in retail).

# Ethics & Compliance Function

Who is going to do all of this work? You! What do you need?

## The problem – all things to all people

Risk management and medicine overlap in their core functions, prevention, detection, and response. However, doctors have specialised, with general practitioners (GPs, or your local equivalent) serving a local constituency and referring more complex cases to a specialist. Except for some huge multinationals – staffed with a blend of specialists and generalists – internal risk teams often try to practice modern medicine with the same resources as a rural GP's clinic.

Fraud, corruption, and money laundering may have enough overlap for this model to work. But what of discrimination, harassment, modern slavery, data privacy, sanctions, anti-competitive practices, and the amorphous global mess that is ESG (environmental, social, and corporate governance). In this tortured analogy, the health minister (at the board level) has as much understanding of medicine as your average health minister or as much budget as the Department for Repatriating Lost Migratory Birds. How many global organisations have a dedicated risk or E&C representative on the board?

Finally, the brave souls staffing risk and E&C teams typically herald from legal (and sometimes law enforcement) backgrounds, with a smattering of finance, human resources, CSR and business alumni. As we move from models built around controls to culture, systems to psychological safety, and policies to practical application, will this blend meet stakeholder demands?

## Possible solutions – put your money where your mission is

If you care about ethics, you need to incentivise ethical behaviour.

## A) Training and fresh ideas

Few immediate quick fixes don't require a budget, time and resources. However, training does not need to cost the earth. The number of remote, part-time, and flexible training courses has exploded, bringing price competition. If you're struggling to articulate the value, the average cost of a meeting in North America was $650.[1] How many pointless meetings have you sat through this week that could have been better addressed in another format? Within a month, you should have enough for an MBA, well, almost.

More expensive courses, like that I undertook in Behavioural Analysis and Forensic Emotional Awareness (a.k.a. spotting emotions, truth, and deception), pay dividends for years, decades. So what sorts of courses could risk and E&C professionals benefit from? It depends on existing skills, but common areas include:

[1] https://www.beenote.io/calculate-cost-meetings/

- Psychological safety – we've all seen the fraud triangle with pressure, opportunity, and rationalisation on each side. Yet most of us focus predominantly on the opportunity (where someone can subvert controls). Psychological safety assessments offer some missing pieces, such as pressure (which can correlate with rationalisation).
- Behavioural analysis and investigative interviewing – the applications extend well beyond investigations into any area requiring an understanding of what people are feeling (everything!).
- Design thinking, graphic design and user experience (UX) – everyone is selling something, or so the cliché goes. For us, risk and E&C comrades, the potency and importance of our message is not enough. We must engage if we want our consumers (your colleagues) to act.
- Environmental risk management – a simple one, we can't possibly expect to make a good fist of ESG with little experience in the E bit. Don't wait for advisors to save you here; the good ones are in serious demand – by good, I mean those who focus on knowledge transfer and systems you can manage alone.

- Blockchain and data analytics – lumping these two together is clumsy, but there is method here. Both of these areas – if done correctly – leverage data to provide further insight than is possible using existing methods, often with a fraction of the effort. For instance, imagine if supply chain inputs were structured using blockchain, giving insight into every 'packet' (input) in your supply chain. How might that turn due diligence upside down!?
- Philosophy and (organisational) psychology – our job is to understand why people do what they do in an organisational context. A retreat into the whys of human behaviour might be considerably more helpful than whatever the latest management guru tells us.

There are other areas, but I think we have enough to start! The alternative is to hire people with these backgrounds with a deliberate plan to learn from each other.


**"An investment in knowledge pays the best interest."**

**Benjamin Franklin**

### B) Reward and recognition

E&C needs a seat at the top table if you're serious about ethics. Saying you care about ethics and values (blah blah) is hollow if not discussed by someone with authority, teeth, and influence at every board meeting. Too often, E&C sits at the legal team's table, brought it for the data dump of active allegations and investigations as a board meeting line item. I know you know this, but it merits repeating just in case this document ends up in the hands of the executive function.

# Confidential reporting

We don't speak up and out the same.

## The problem – preferences and retaliation

How comfortable are you speaking up? Let's pick some hypotheticals:

- Your best friend says something hurtful.
- The server in a mid-range restaurant is rude to you.
- An elderly relative utters offensive remarks.
- Your CEO belittles a colleague publicly, and no one says anything.
- You discover your neighbour is having an affair; you like their partner.

Do you react the same way in each instance? I'm guessing not. The context, our culture, relationships to and with the parties involved, and the actions of others can impact our decisions. Now let's add in the complexities of our organisational culture and fear of repercussions (for speaking up). Why might we remain silent?

1. Fear.
2. It won't make a difference.
3. The bystander effect.

There are many reasons to fear raising your voice. Many of us are conditioned not to be a snitch or teacher's pet from a young age. We can risk excommunication from social and professional groups. That's the best case. For many folks making reports, their lives are made a misery – they lose their job and income with the associated financial, physical, and mental health challenges. Most (sizeable) organisations will have a no retaliation policy, but how is that administered and enforced? How do you link subtle slights, demotion, exclusion, reallocation, threats, intimidation, social isolation, or acts of sabotage and frustration to retaliation? It's not as simple as it may appear.

The bystander effect is similarly complex, where we hope someone else steps in. Why does it have to be us, with all the fear and perils that may follow?

## Possible solutions – psychological safety, simplicity, training

It's hard to know where to start until we understand what people think. If they spot a (potential) issue, do they know what to do? Can they access the speak up channel easily? Do they trust you (to protect them, investigate properly, keep it confidential)?

### A) Ask, and then listen

Start by asking some questions. We're going deeper than an employee engagement survey but with fewer questions. Look back at the risk assessment section for some inspiration around culture questions.

I like to ask questions on a Likert scale (disagree-to-agree). It may be a semantic point, but I prefer sliding scales rather than numbered scales (e.g., 1-5). You want the engagement to be kinetic and natural, not burdened with too many variables. If your surveying functionality only allows for numbers, consider choosing an even-numbered scale. With odd numbers, we can fence-sit and pick the middle option (3 out of 5, 2 out of 3, etc.). By removing that option, you're forcing people to take a position. If you need any help or inspiration, we have some free surveys HERE, giving you some guidance on what to do with the results.

## B) Psychological safety

If you're on either end of this spectrum, "we don't do fluffy here – we do care, no, really", go big. Psychological safety assessments can now be paired with KPIs. This analysis will show where the fearful and disengaged folks are and, more importantly, where that intersects with performance. For leadership teams that don't care about being nice (come on, we all know they exist!), sell this to improve performance and reduce costly attrition, mistakes, and problems. I want to keep a little powder dry on this topic, as it's one worth talking through in person. We work with a partner who specialises in nothing else but these assessments, and it's revelatory (for culture and performance). Curious? Just ask.


## C) Non-retaliation assurances

Most organisations will wrap in a "we do not tolerate any form of retaliation" into their code (or similar policies). This statement might include references to consequences and who to contact, but how can this be enforced appropriately. Firstly, we'd need to describe non-retaliation and give examples. A non-exhaustive list might include some of the topics on the next page.

# EXAMPLES OF RETALIATION


Retaliation isn't always immediate or overt. Giving examples and scenarios can help to explain. For non-retaliation to stick, it will need a dedicated training and communication campaign. I would also suggest (if you have the resources) appointing a case officer. This person should sit outside the reporter's team and any teams implicated in the allegation or incident. Someone with experience in line managing or mentoring would be ideal. The case officer is the primary point of contact for the reporter if they have any questions or concerns, specifically relating to the consequences of speaking up. We want to avoid a situation where someone takes that courageous step to come forward, and they get an automated reply and are left hanging.

Suppose you don't have the size or capacity to make the case officer model viable. In that case, someone very senior (executive committee or board-level) should call the reporter (assuming they have not requested their identity be kept confidential). Showing respect and face, let alone senior support and gratitude for those speaking up, goes a long way. But it needs to be intentional and backed up with real action against anyone retaliating.

# Confidential investigation

We all like to think we're super sleuths, not Keystone Cops.

## The problem – too deep, too wide

Conducting investigations was never easy, but it's become more challenging. We can't get around like we once did, and compelling someone to cooperate over Teams or Zoom is tricky. Then there are emerging technologies, which are double-edged swords. Yes, data analytics and forensic discovery have advanced markedly but so too have tools of deception and evasion (encryptions, masking, scrubbing, etc.).

We were already taking work home before Covid, but the blurring of the personal and professional complicates matters further. The location of information is a significant headache for investigators – compounded by increased use of personal devices for work and vice versa. For example, suppose a suspect in an investigation uses a messenger platform (like WhatsApp) on their personal smartphone to communicate with co-conspirators. In that case, you have little recourse to access that device. Even if you get past all these hurdles (and encryptions on many messaging platforms), you may not even be able to transfer the data across borders (as data protection and privacy laws ramp up their scale and scope).

Okay, so what about talking to people? We won't be remote working forever, surely? It depends. But even if you're able to speak to witnesses and suspects, how many E&C professionals feel they've had adequate training in investigative techniques?

Finally, what is considered E&C is expanding and will continue to do so. Yet, as discussed elsewhere in this document, the resources have not grown for most. If you're consistently messaging and promoting your speak up and confidential reporting channels, you will also increase the volume of cases you need to respond to.

## Possible solutions – triaging, training, fixing

For different organisations and individuals, the priorities will differ. However, as a rule, you can never be over-trained as an investigator. Similarly, processes are essential in this area, maybe more than any other – as Jack Reacher says, "Details matter!".

### A) Intake and exhale

Starting at the top, we need to triage allegations, complaints, and any other issues uncovered during monitoring, audits, etc. Not all possible investigations are created equal. You need a system to filter and prioritise (like that below).

Getting your intake set up can be the difference between drowning or delivering results.

| 1 STEPS | 2 TASKS | 3 OBJECTIVES |
|---|---|---|
| Allegation received / issue uncovered | 1. Acknowledge<br>2. Gather data<br>3. Establish communication protocols<br>4. Confirm a time to follow up / get back to the reporter | 1. Establish rapport<br>2. Build trust<br>3. Gain information |
| Review information / reallocate | 1. Immediate conversion to investigation (seriousness)<br>2. More info needed? Create a list, test assumptions. Who has it?<br>3. Closure - for out of scope issues<br>4. Reallocation - relevant but not to you (e.g., client complaint) | 1. Act of facts<br>2. Test assumptions<br>3. Develop a plan<br>4. Remove out of scope |
| Risk owner & categorisation | 1. Who has the technical knowledge?<br>2. Who has the investigative experience?<br>3. Availability & timeframes<br>4. Confidentiality (& privilege), who needs to know? | 1. Establish lead<br>2. How & when to communicate to stakeholders |
| Assess initial risk & complexity | 1. Credibility: Is the allegation credible? Have there been similar issues/near misses in the past?<br>2. Verifiability: What do we need to verify? Do we have access?<br>3. Impact: People, planet, reputation, regulatory, profit, etc.<br>4. Could response create further harm (e.g., political aspect)? | 1. Qualify complexity and verifiability<br>2. Preliminary impact rating<br>3. Contingency planning |

## B) Behavioural science for everyone

The years I spent studying behavioural analysis, investigative interviewing and deception detection were the best investment in my career, not just because they helped me with investigations. It has helped in most areas, especially risk assessments, monitoring, training, and investigations. If full-scale courses are not possible, the following books – ranked in order of their accessibility and ease of reading – might help:

- Rapport: The Four Ways To Read People, Laurence and Emily Alison
- Spy the Lie, Susan Carnicero, Michael Floyd, Don Tennant
- Telling Lies, Paul Ekman
- Investigative Interviewing, Shepherd, Griffiths

## C) Root cause & remediation

After every allegation, near-miss, or investigation, there are usually lessons. A close-out process can help prevent a recurrence, ultimately the goal. The framework should be practical and tangible, providing a summary of the findings (or lessons), the case status, the recommended corrective actions, who owns that, a timeline for implementation and a prioritisation (not all enhancements are immediately feasible).

**"The only real mistake is the one from which we learn nothing."**

**John Powell**

# Monitoring & Reporting

Isn't that what internal audit do?

## The problem – never enough time or resources

Risk management is prevention, detection, and response. When resourcing E&C, the detection bit –monitoring – normally comes in last. It's challenging to know what to look for, when, and how often, especially if you lack meaningful data. Most organisations (outside of the mega-corporations) don't have sophisticated surveillance, and some don't want to (concerned about morale and data privacy, among other things).

Even if you have the technological capacity (and stomach) for mass-monitoring, where will you focus, and who will oversee? It's like installing CCTV; you still need to decide where to stick the cameras and who will sit in front of the screens eating Pringles.

There might also be a feeling that paying for internal (and external) audits should cover the monitoring bit. Audits are not universally welcomed (perhaps an understatement). Having generated that much ill-will with frontline colleagues, some E&C teams are reticent about adding to the disruption.

## Possible solutions – making tech work & understanding people

A watchful guardian.

### A) Legitimate tech

Most of us accept that surveillance increases in specific locations – like airports, major railway stations, places with high-value items. The rationale for monitoring is either self-evident or explained. Data, including that produced each year in the Association of Certified Fraud Examiner (ACFE) 's Report to the Nations [1] – indicates that if people feel the chances of detection are higher, it acts as a deterrent, not a huge surprise.

[1] https://acfe.com/fraud-resources/reports-and-statistics

We, in E&C, need to learn to tell people where their activities are monitored. If you're thinking, "But won't they just commit crimes elsewhere?" Maybe, but that's why you don't need to tell them everything you monitor! It's a balance and requires explanation. For instance, it's not unreasonable to expect that expense claims will be monitored, whereas announcing you screen all internet activity is possibly less reasonable (even if you scan for inappropriate content).

The graphic below clearly indicates that monitoring, IT controls, account reconciliation and internal audit are all effective methods of reducing fraud (defined broadly to include most E&C integrity violations).

Data analytics has come on leaps in recent years, and the pricing is now more accessible. If you're coupling your high-risk areas with creative (machine learning) questions, you can also really start to focus your monitoring efforts. For example, a Japanese insurer experienced a jump in automotive claims in one country. Using renewal date, address and named driver questions, the data analysis revealed that a suspiciously high number of claims were made a few days before the policy was due for renewal. The designated driver did not renew the policy, which would typically confer an increased premium. Instead, the accident-prone driver would mysteriously appear as the second named driver on a new policy (often registered to the same address). Conducting this analysis long-form would have been time-consuming and expensive, but we leveraged technology by looking at the high-risk variables (driver, address, date of claim).

### B) Intelligence-led monitoring

The second essential component to whatever technological solutions you can muster is using human intelligence, including:

1. Speak up data – what trends (where, what, when, who) do you observe?
2. Investigative data – are certain activities or functions more prone to problems?
3. Turnover data – where you have bad bosses and crappy morale, astonishingly, you have E&C problems.
4. Risk assessment data – if it's been identified as high-risk, monitor.
5. Blue on blue training – when I run training, I like to play the "how would we defraud our employer" game if I'm allowed. You'd be amazed at the gold that comes from this.

With monitoring, it's a bit like parenting. When the risks are very high – as they are during infancy – you monitor everything and waste money on night-vision cameras to record someone who is never more than a few feet away. As the child gets older and explores the world, you look for sharp, toxic, and generally big hazards. Then comes general idiocy, which for boys seems to last until around senility and for girls until the first meeting with consequences. During pre-teen and teenage years, your threat analysis shifts to focus increasingly on other humans (peers and predators). The point is that your monitoring must adapt depending on the maturity of different functions of your business and the risks they face. If you do this, it's not easy, but it's manageable.

# Third-party management

"I love our third-party management systems," said no E&C officer I've ever met.

## The problem – death by a thousand ticked boxes

One of life's delicious little ironies, I now get to fill out vendor onboarding forms. There's nothing the client's procurement team, and I love more than a three-month process with lots of repetitious data entry. What's going on here?

The reasons vary, but perhaps a significant driver is a case law curse. Much E&C guidance originates from common law jurisdictions where we build as we go. When this model is used for operational frameworks, it can confuse. As regulation and risk evolve, we add questions (and sub-questions and qualifications for questions). Layer on a bit of CYA (cover your ass) – where we ensure we've made the third-party tick three pages of boxes listing every possible violation we seek to prohibit – and it's a proper mess.

When we're faced with unintelligible, hefty forms, we acknowledge and move on. There are only so many hours in a lifetime. Alternatively, we try and understand the document, fail because it's written in legalese with sixteen compound clauses per paragraph, and question our sanity. We then send it back to some hapless sole on the client side – who's forgotten the reason for asking half of the questions. We occasionally innovate this process, migrating it from Excel to something claiming to be technologically superior; Windows 3.1 bangs angrily on the door, asking to have its software back.

Recently we've made this process much better by focusing on supply chain transparency – including the UK and Australian Modern Slavery Acts. We can now use our deep understanding of third-party risk to ask ever more confused (and usually smaller) organisations further down the supply chain about their speak up line and business continuity framework. Using this method of carpet-bombing confusion, we will somehow eliminate human suffering, corruption, money laundering and various other ills. Third-party management is like Martin Luther King Jnr, only a bit different – we're aiming for equality of confusion, dismay, and cataloguing pointless data.

## Possible solutions – the 80/20 rule

Maybe we should focus instead on identifying risk in our third-party relationships.

### A) Risk assessments that consider risk!

Standard third-party risk criteria include:

1. Location
2. Sector
3. Watchlist research (sanctions, political exposure, debarment)
4. Media check
5. Conflicts of interest
6. Payment terms or structure (e.g., commissions)
7. Ultimate beneficial ownership
8. Reliance risk (e.g., your sole distributor in a large market)
9. Compliance maturity (e.g., confirming they have a Code of Conduct)


Some of this data is hard to access or identify (in many cases and markets). For example, confirming ultimate beneficial ownership in countries without reliable or public registries. Other questions require insight that the person in procurement may lack the training to determine (questions 8 and 9). Most organisations rely on indexes – especially Transparency International's Corruption Perception Index – to rank location (country) risk.

**"The art of knowing is knowing what to ignore."**

**Rumi**

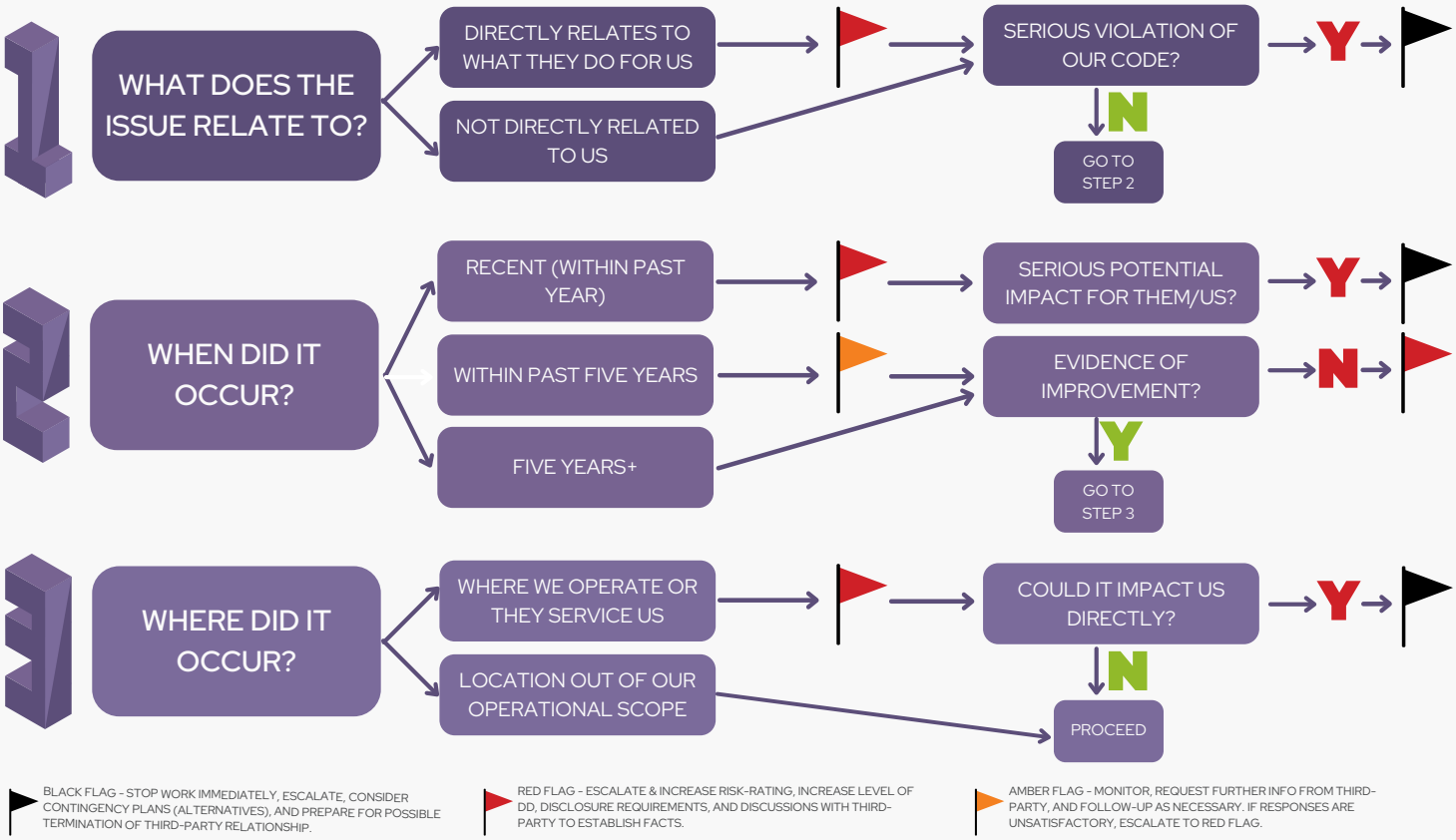
As an experiment, in 2020, we aggregated lists including those related to press freedom, human capital, corruption, money laundering, sustainability, and ease of doing business. Belarus averaged 59th place (out of 182 countries), outscoring China (77th) and India (95th). China and India do present many challenges, but where (precisely) within the country you operate and what you do, I would argue, are essential contexts. For example, in any sensible universe, graphic designers in Bangalore cannot be considered higher risk than any endeavour in Belarus. Haven't I already brought in sector risk? Yes, that's the point. Country risk alone (when derived from indexes) is problematic. You either rank three-quarters of the world as high-risk or add nuance.

The trick is to take as much pain out of the process as possible. That might look something like this:

1. Location and sector – simple dropdowns, ideally with (meta) search capabilities (so you don't have to scroll down to spare the pain for folks dealing with wholesalers in Zimbabwe or utilities providers in Uzbekistan). These selections create a composite score using logic, so we capture that vital insight into sector impact on country risk.
2. Watchlists, ownership and media results need context too. The image on the next page was one attempt to help an organisation contextualise any scandals they identified relating to their third-parties. Simple cheat sheets like this make the lives of procurement folks easier.
3. Conflict checks, payment terms, and reliance risk are ideally automated, but you'll often still need a few binary questions with risk weighting attached. For conflicts, that might include:
    a. Are we aware of any close personal relationships between the third-party and our employees?
    b. Are any of the third-party's key personnel former employees?
    c. Was the third-party introduced to us by a current or former employee?
    d. Did a government official introduce the third-party?
4. Maturity risk is, in my view, a real headache. Let's say the third-party shares their Code. So what? Enron had a Code. If you're not able (time, resources, access) to look under the bonnet and assess how the compliance engine runs, being sent a photo of the vehicle doesn't help you decide about whether it's a reliable proposition or a liability. Better not to ask, unless you're ticking a box, in which case, why!?

If you get a simple ranking process, the human inputs should sit at decision points (i.e., when you find a risk issue). The trick is striking that balance between caution and not flooding decision-makers with false positives. Tweak and adapt any rating weightings as you go; the process should not be static.

## THIRD PARTIES - WHEN YOU FIND AN ISSUE




BLACK FLAG - STOP WORK IMMEDIATELY, ESCALATE, CONSIDER CONTINGENCY PLANS (ALTERNATIVES), AND PREPARE FOR POSSIBLE TERMINATION OF THIRD-PARTY RELATIONSHIP.

RED FLAG - ESCALATE & INCREASE RISK-RATING, INCREASE LEVEL OF DD, DISCLOSURE REQUIREMENTS, AND DISCUSSIONS WITH THIRD-PARTY TO ESTABLISH FACTS.

AMBER FLAG - MONITOR, REQUEST FURTHER INFO FROM THIRD-PARTY, AND FOLLOW-UP AS NECESSARY. IF RESPONSES ARE UNSATISFACTORY, ESCALATE TO RED FLAG.

## B) Why are we here?

The decision-making framework above (when you identify a third-party issue) illustrates that people need to know why we ask what we do. Have you heard the saying, misery loves company? Well, so do risks. It can help to take a step back from all the different categories of risk – fraud, bribery, conflicts of interest, money laundering, sanctions, environmental degradation, human rights, etc. – and recognise that they look similar from a detection point of view. I picked on ABAC (anti-bribery & anti-corruption), AML/CTF (anti-money laundering and counter-terrorism financing), trade sanctions, and human rights and looked at potential third-party red flags. There is more similarity than dissonance.

How would you explain that these issues are risks to a ten-year-old? Let's pick a couple.

| Compliance question | Ten-year-old question |
|---|---|
| **Unable or unwilling to disclose origins of wealth** | **If someone can't tell you where they got their money, would you trust them?** |
| **Lack of experience, resources or staff for proposed engagement** | **If you were picking a team, would you choose someone with no experience first?** |
| **It appears 'intangible' (little website/physical presence)** | **Would you meet someone you don't know, alone?** |

I appreciate you may not wish to speak to your employees like kids (!), but the point remains, we need to communicate the basic why here. Don't get involved with people who you don't know anything about, don't trust, aren't qualified, and don't cooperate.

It can help to anchor third-party risk back to your values. You may not always be aligned ethically with your partners, but it should be considered.

## C) Tech that works

Some excellent technological solutions take a lot of the heavy lifting out of onboarding, screening, and monitoring. That's the good news. The bad news comes when you get a quote.

Therefore, I'd rather not do an advertorial for companies that don't need it. Maybe, instead, we could focus on emerging technologies and ideas with the power to disrupt the status quo.

| TOOL | WHAT IS IT | HOW IT HELPS | LIMITATIONS |
|---|---|---|---|
| Data analytics | Looking through the universe of your data for patterns that are hard for us mere mortals to spot. | Flags possible fraud, conflicts of interest, corruption, money laundering (e.g., duplicate invoices, unusual payments, etc.). | Only as good as the data you have, the questions you ask (machine learning needs to be taught) require expertise to extract and assess. |
| Blockchain | This is tricky, but it's a data packet with a unique identifier. If altered, the chain is broken, and multiple decentralised people oversee chain integrity. | If you want insight into the integrity of your supply chain (understanding the inputs) or payment that is harder to manipulate, this may work. It's already being used for food chain integrity. | It's not entirely here yet, at least not in the form of third-party management. But it is coming. |
| Artificial intelligence | We're talking about trawling and gathering data, looking for connections in this context. | Distinct from analytics, we're more interested in the connections, origins, ultimate owners, and track record of third-parties. | Data is wildly uneven globally, transliterations and naming conventions complicate matters, and it can throw up a lot of false positives. |
| Corporate passports | Like the vaccine passports many of us have learned to carry, companies could put their corporate data into a virtual passport. | It would save time establishing basic information that any good faith third-party should be happy sharing (owners, directors, locations, etc.). | Not here yet. It would rely on reliable registries and corporate data (not the case in many markets). It depends on self-disclosure. |

I appreciate this is a whistle-stop tour of some deep areas, but you'll see that no technology (yet) offers the solve-all for third-party transparency. Blockchain, for my money, is the most compelling bet for improving due diligence and supply chain insights, with data analytics deployed mainly in a monitoring capacity.

# Leadership & Management

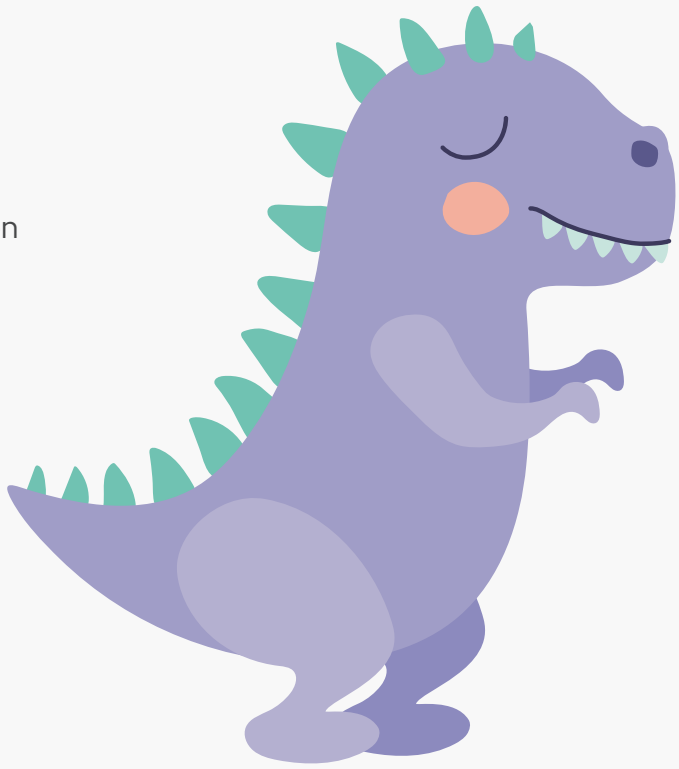
Not a week goes by without an article pointing to the importance of the tone from the top or bemoaning leadership failures which led to another ethical disaster. Rinse, repeat, rinse, repeat. What's happening here, and what can we do better?

## The problem – dinosaur thinking

"Do as I say, not as I do" has never been an effective mantra. Parenting is a relentless and unforgiving reminder of the perils of not walking the talk. It's hard to extoll the virtues of attention to detail as you pour expired and sour milk onto your child's beloved cereal. I am not, therefore, wholly unsympathetic to the plight of leaders who may lack the time, energy, and capacity to lead from the front – striding forward purposefully and vanquishing all ethical demons.

Leading by example is conventional wisdom, but maybe that's the problem. As an organisation scales – especially in times of remote working – how do you make the model visible without it seeming trite and performative?

Then there are those pesky stakeholders – from shareholders to employees and communities – who want more. More transparency, accountability, and equity. Yikes! Senior executives make these expectations even more challenging when they decide to pay themselves progressively more obscene amounts, often contrary to performance. How can they get away with this? If everyone else (in those upper echelons) is in on it, we end up with a bloated game theory.



## Possible solutions – evolutionary thinking

If we're not evolving, we're stagnating.

### A) Get perspective

There's a much-shared image of a large wolf pack, where the caption claims that the weak and old wolves lead the group, so they are not left behind, the strongest wolves follow (to protect them), and then pack leaders are at the back, guarding, protecting, like noble sentinels. Okay, I may have taken some creative license here, but it's total rubbish. Wolves don't form into a consistent social-physical marching hierarchy. But just because it's another embellished inspirational leadership meme doesn't mean we can't learn something. Perhaps, instead of leading from the front, leaders should get to the bottom of their organisations and see life in the trenches.

If you're a leader, thinking, "I'd rather not, let them eat cake", use a survey. Simple questions like "Corruption is a regular challenge in {location}" on a sliding scale from strongly disagree to strongly agree can reveal so much. Even more illuminating is asking questions you might be scared about, "Discrimination is common in {organisation}". The survey must be anonymous, using location, department, and seniority classifiers only if they don't make any group smaller than five people.

Armed with the views from the frontline, own them, own up, and plan to do better. We don't expect our leaders to be infallible, but we're used to them being dishonest. Listening openly and being honest about the journey ahead is always a better go-to than platitudinous waffle.

## B) Diversity

Try diversity – you'd be amazed how stakeholders might respond if they're met with someone that looks like them. Better still, the cognitive diversity and differing perspectives will help solve some of the knottier ethical challenges (which may even have a cultural dimension missing from the boardroom).

## C) Risk as strategy

Give risk a seat at the strategic table – When market sizing, forecasting, acquiring, or doing anything strategic, ensure you're factoring in the downsides BEFORE you decide. I see risk used routinely as an afterthought once a plan is rolling. The unfortunate risk, ethics or compliance team are then placed in the unenviable position of "deal blocking" or whitewashing, should their due diligence find anything unsavoury or troubling.

Risk data should be part of board meetings. What you can report on will depend on reliable information, but at a minimum live issues or investigations, regulatory changes or challenges, and speak-up trends are a must.

**"If the rate of change on the outside exceeds the rate of change on the inside, the end is near."**

**Jack Welch**

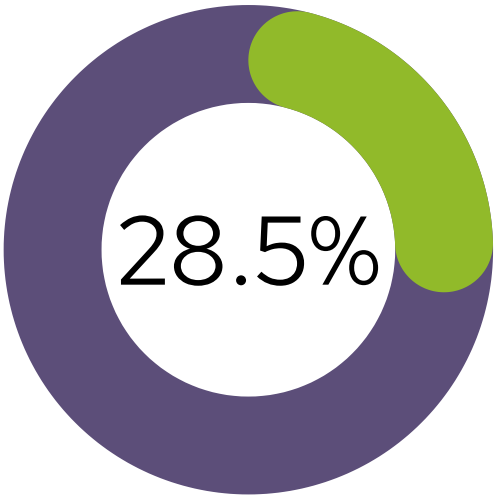
### D) Develop tools

Without information and tools, managers cannot be expected to make great risk decisions. Use the outputs from strategic meetings, turning them into actionable instructions. If you're wondering what the hell that might look like, a simple example that almost every organisation needs: "Things not to say if someone raises a possible compliance issue with you".

Those reporting to the managers will also need similarly pithy but salient guidance. Taking the example above, "Things to speak up about" would be a good poster, campaign or cheat sheet.

What you need to do as a leader will be influenced by your organisation's risk appetite, nature of business, locations, and structure. However, honesty, transparency, and listening are agnostic of those variables. If you're sick of what you feel is acerbic of preachy guidance – like this – telling you how to do what is a tough job, okay, but what's the alternative? Rumours, cynicism, mistrust, problems, underperformance, and being ignored.

## Goodwill sits on balance sheets, ethics underpins goodwill.
## S&P 500 assets = $9.3tn / Goodwill = $3.7tn




Source: Bloomberg

# Incentives & Disciplinary Measures

In the regulatory guidance, watch how incentives usually lead (in the title) and then, poof, vaporises in the body text

## Problems – reward and punishments mismatched

How do we incentivise people to do the right thing? It's a tricky question, so most folks seem to put it in the same place I put stuff like tax self-assessment on my to-do list NTNT (near the top, never touched). What is doing the right thing? In an organisational setting, that is an existential question. For example, it can mean inflicting self-harm, not accepting a high-net-worth client who might have derived their wealth from a criminal enterprise. If your targets are linked to bringing in clients, and you're having a tough time, turning that client away is potentially harmful. What about speaking up? Should we reward people for that, or will it spark a callout culture? These are common questions when organisations dodge the incentives issue.

Disciplinary measures are a nightmare in globalised organisations. In some countries, it's near impossible to fire people unless they commit a serious crime. In others, you have the opposite problem, where bosses wield too much power and can fire employees (often those challenging their tyranny or daring to speak up) at will. However, these extremes appear to be crutch arguments for a general inequity between the haves and the have nots. The haves (credit cards, corner offices, cars) don't get fired enough. How many of you have worked in an environment where someone senior and successful has created a toxic mist that corroded morale, creativity, and integrity? Yes, all of you. Why were they not fired? Because they were a key employee (or some variation of that trope)?

It's hard to trust and respect an unjust system.

## Possible solutions – celebrate and reward integrity, tell tales, cut out cancers to preserve life

This section is the hardest for me to write because it's the area where I've seen the least change, but let's try.

### A) Integrity champions

Integrity KPIs aren't easy, I agree. But we still need to try, so how's this for starters?

#### Senior leaders

- A reduction in incidents*.
- E&C training and certification pass rates across the organization
- E&C input included in strategy (e.g. addressable market, business partner selection and new market entry includes E&C input and risk mitigation planning)
- Anomyous employee survey results measuring trust in the leaderships adherence, support, and engagement with integrity risk
- All transparency objectives and obligations met (e.g. public reporting on supply chain slavery risks and measures taken to reduce them)

#### Managers

- E&C training and certification pass rates across the area you manage
- All direct reports have E&C component in their objectives/KPIs
- Decreased E&C incidents in the team you manage*
- Risk assessment completed for your functional area(s), with defined actions and ownership for each risk
- 100% compliance with relevant procedures (e.g., expenses, supplier vetting, etc.) in your team
- Exit interview data for employees leaving your team includes no evidence that subopimtal E&C culture was a factor

#### Employees

- Complete and pass E&C training and certification
- Ensure, in discussion with your manager, than you have an E&C objective/KPI
- Come up with at least one suggestion to improve E&C in the organization; this should be properly explained with a clear goal and timeline
- Uphold and promote the culture of E&C by speaking-up when you see possible or actual E&C issues
- Demonstrate clear adherence to the E&C areas relevant to your role (e.g. if in procurement, ensure third-party management measures are followed properly)

*** I HESITATE TO INCLUDE THIS, AS IT COULD DISINCENTIVISE HONEST REPORTING OR NATURAL CYCLES WHERE ISSUES SPIKE (E.G., ACQUIRING A NEW BUSINESS WITH SOME KINKS THAT NEED IRONING OUT OR LAUNCHING A NEW SPEAK UP LINE THAT INCREASES TRUST AND THEREBY CREATES A SPIKE IN REPORTS).**

These KPIs I wrote three years ago and reading them now, they're dated. I kept them in because they're surely now easily implementable. If I were more ambitious, I'd want to add proper psychological safety metrics. We could add targets informed by analytics (e.g., false expense claims to decrease from X% to Y%). Finally, some genuine diversity, equity & inclusion (DE&I) targets (again, very measurable, with numerous tech options).

If you're wondering about the link between DE&I and risk, it's pretty simple, groupthink. When we're in homogenous packs, it's easier for tribalism and fear of standing out to prevent people from challenging destructive behaviours. As soon as we allow in cognitive diversity, we have a more pluralistic perspective (and more creativity), less prone to myopia that can deteriorate into ethical blindness. To prove the point, if you're a risk or E&C professional (I'm guessing most of you are), then imagine all the fantastic ideas you could implement if your team had a behavioural analyst, a graphic designer, a developer, and a marketing professional.

### B) Telling tales

We seek feedback at the end of every training session I've run. One of the questions relates to which part was most helpful. When the organisation we're working with allows retelling of integrity and ethical near-misses, mistakes, problems, or successes, those stories are ALWAYS ranked as the most valuable part of the session. It's not surprising; they resonate and bring the theory to life.

Some organisations are reluctant to share, citing confidentiality or sensitivity. If the issue relates to something deeply personal – like harassment or discrimination – and any aggrieved employee(s) has not consented, don't share. But in most cases, people will already be gossiping about what happened. Being straightforward and transparent about it helps diffuse potential misinformation. In the context of incentives & disciplinary measures, this provides an opportunity to celebrate those championing integrity (including those speaking up, if they consent) and shine a light on the consequences of violations.

For disciplinary case studies, you can anonymise and remove any overly-sensitive information. The key is to communicate what did go (or could have gone) wrong, the consequences, and the lessons (how you improved). It's not about shaming – Person X was wrong and got fired – it is creating teachable moments.

### C) Champion the committed, toss the toxic

If you use ethics champions or equivalent, think of ways to make it an appealing and rewarding role. If you're just adding workload, it's a big ask. You don't always have to make the incentive monetary. Still, transferable training, face-time with senior leaders, increased internal visibility, international networking opportunities, and fast-tracking might be worth considering (among any other creative ideas you can muster).

If someone dares to speak up (and disclose their identity) but does not wish to go public, give them a call. Or better still, ask the CEO to do it. Often the person speaking up will face nervousness (or worse, retaliation). Having a very senior employee take time to personally thank them and give them assurances that they are there to support the reporter shows the right level of commitment.

Finally, fire people you know need firing. I'm not being glib here. No matter how much money they make, toxic and bullying people lose you more in the long run. I won't say more than that, as I know you know this and often have little influence in such matters, but it has to happen for cultures of integrity to thrive.

**"Toxic people with pollute everything around them. Don't hesitate, fumigate,"**

**Mandy Hale**

# Thank you for reading!

ethicsinsight

## Get in touch

ethicsinsight.co

hello@ethicsinsight.co

Click to book a time to talk

+44 7480 800435