rupert evill

bootstrapping ethics

Integrity risk management for real-world application

WILEY

BOOTSTRAPPING ETHICS

BOOTSTRAPPING ETHICS

INTEGRITY RISK MANAGEMENT FOR REAL-WORLD APPLICATION

RUPERT EVILL

WILEY

This edition first published 2023

Registered Offices
John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

Editorial Office

The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK
For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Library of Congress Cataloging-in-Publication Data is Available:

ISBN 9781119874904 (Hardback)
ISBN 9781119874928 (ePDF)
ISBN 9781119874911 (ePub)

Cover Design: Wiley
Cover Image: © Jakub Krechowicz/Shutterstock

Set in 13/16 pt Minion Pro by Straive, Chennai, India

CONTENTS

PREFACE

I spent most of my life in the shadows. In 2015, when I met my wife, she did her background check on me and became very concerned. I had no (public) profile, and many questions followed. I'd spent my career in the grey world of risk. I'd been a counter-terrorism analyst (much less glamorous than it sounds), an investigator, an intelligence gatherer, a political risk wonk, a crisis responder, a behavioural analyst, and an integrity risk advisor. I travelled this path by volunteering for every exciting project, job, and opportunity – by taking risks. I am and was happy being the clueless newbie learning from masters. I've been blessed with mentors like Dr Cliff Lansley and Dane Chamorro, who taught me the arts of deception detection and tradecraft. I've also learned from dozens of genius colleagues and clients – too many to mention; the people I still speak to regularly.

In retrospect, and I take no credit for planning this, the path gives me a rounded understanding of risk. Terrorists, corrupt politicians, fraudsters, hackers, harassers, and general baddies are not that different. They're humans; we need to know how the motives, means, and methods differ. Integrity risks – by which I mean most things that cause scandals – are a further unifier. All the baddies want money (or power). Whether you're smuggling ivory, building bombs, stealing state secrets, or ripping off your employer, if we're managing integrity risks, we reduce your chances of success.

I don't see integrity risks as figures – I am numerically useless. I see how caustic and vicious this corruption and abuse of power are. These risks gravely threaten our planet, wildlife, human existence, and hope. If we don't take them seriously, we're in trouble. We do our bit if you and I cut off the funding, increase accountability, and respond honestly to risk. The small bribe you pay isn't a drop in the ocean; as Rumi said, "You are the ocean in a drop."

In 2019, I started Ethics Insight. I was woefully unprepared to be a business owner. I made many mistakes, especially around marketing and sales – two areas I'd barely had to contend with previously. I was bewildered by the options – channels, funnels, adverts, email campaigns, cold leads, warm leads, it was all gibberish. It was a wonderful lesson. Risk had become implicit knowledge to me, just as marketing know-how was for all the people I read and spoke to. I realised why most people didn't understand what I did – I was speaking gibberish.

The pandemic necessitated a massive transformation as my traditional investigative work (and behavioural analysis training gigs) disappeared – 51 investigations in 2019 became three in 2020. A good friend (James Ritchie) told me as I prevaricated about entering the LinkedIn world of self-promotion, public speaking, and authoring, "Get over yourself." So I did. I used my followers and connections as a laboratory – assessing which risk simplification ideas worked (or not). I learned that if risk is ever to be relevant, it must start with more personal and human constructs (our values, ethics, and beliefs).

As I found my voice, the publisher Wiley found me. They asked me to write a book making risk relevant to you, a broader audience.

We all make risk-based decisions daily. We all face integrity and ethical challenges. If you'd like to improve, I hope this book will help you.

I can't and won't cover every facet of risk. You will be disappointed if you're looking for environmental, social, and governance (ESG) risk coverage. Corruption, dishonesty (inauthenticity, if I'm being kind), and abuse of power facilitate most ills ESG is concerned with, but I think ESG in its current form is useless. Not the concept, but the metric-driven performative crap peddled by charlatan advisors and cynical institutions. No one person can cogently explain plastic effluents, noise pollution, indigenous land rights, board composition, reporting best practice and sanctions. Again, I focus on integrity risk as it's the currency in which most organisational ills are transacted. My focus is on the root causes of rot, not treating every risk malaise.

This book will borrow statistics and survey data here and there, but, for better or worse, I based it on my experiences managing thousands of projects in more than 50 countries. I look for patterns, overlap, and consistency. Clarity. Enough gibberish, I hope!

INTRODUCTION

I don't like compliance. The very word is jarring, implying control of someone over another. I remember when I first came across the organisational structure and function of compliance. I have worked in some exciting areas, including crisis response, counter-terrorism, and political risk. I loved that work. I didn't realise it then, but it's all about people and why we do what we do. I moved from that job to one in investigations, which included conducting due diligence on the prospective clients of prominent investment banks. Due diligence – know your customer – is snooping into someone's background. Our job was to ensure the bank wasn't onboarding clients with more skeletons in their closet than a medical training aid factory.

When we delivered our reports, it became apparent that the focus was another acronym: CYA = cover your ass/arse. All too often, organisations term this butt-bashfulness, compliance. I remember sitting on a call with a few bankers and my Russia analyst colleague. We'd found strong evidence that a serving public official almost certainly owned a prospective business they wished to finance through offshore holdings. Officials should not hold non-disclosed commercial interests, generally. The bankers asked if we had documentary proof of the shareholding. The complex ownership structure quickly left Russia for sunny offshore jurisdictions

with ironclad secrecy. We did not. Our evidence followed testimony from former and existing employees. They confirmed that the official owned the business; he had an office with a dialysis machine (to cleanse his blood of all the cocaine). This official also had significant alcohol and drug abuse issues, which had resulted in his killing or maiming people (multiple occasions) while driving under the influence. The bankers asked us if the deaths had led to prosecutions. We confirmed they had not, as he'd bribed the police and judiciary. They countered by requesting documentary evidence of that bribery (our evidence was circumstantial but corroborated by multiple sources). Obtaining physical proof of corruption is incredibly challenging, as you require access to (often offshore) accounts and surveillance, among other methods. The call concluded with the bankers saying, "Well, then, as we see it, you don't have physical proof of wrongdoing, so I think we can proceed."

Compliance is often obeying clearly defined rules or pretending to. In this example, it is legal if it's not proven criminal. Compliance can be the base level of morality in many situations.

Why, therefore, am I writing a book covering topics that would be classed (by many) as compliance? Because I care about risk, and more specifically, helping people make ethically minded and risk-based decisions. I want to make integrity risk-relevant – all risks an organisation might face with ethical components. This broad church – from corruption to human rights to discrimination – overlaps more than it digresses.

In 1973, Donald R. Cressey devised what is now known as Cressey's Fraud Triangle.[1] Fraud, in this case, is defined so broadly

as to cover most crimes that will occur in an organisation. The model posited that fraudulent acts were a function of opportunity, rationalisation, and pressure. Compliance, for many years, focused principally on the opportunity part, where systems and processes do not exist or are insufficient. For example, stealing from the cash register because there is no CCTV monitoring and balance checks are irregular or sloppy. It makes sense to focus on opportunity; it is a variable we (think we) can control.

In my experience over the past 20 (or so) years, an opportunity is seldom the main reason. This hunch is borne out in the survey data that the Association of Certified Fraud Examiners (ACFE) gather yearly in their Report to the Nations.[2] Their report, surveying some of their 90,000 (and growing) members, who are focused on investigations, typically indicates that controls failure is the primary reason for violations in roughly a third of cases.

What's happening in the majority of cases? Well, that would be where pressure and rationalisation come into play. This human element is where I live and work. Pressure is a massive area we will unpack in some detail, but another word for it that may resonate more is *motive*. That's what makes us cut corners, do things we should not, and often compromise our ethics for the benefit of our employer. Understanding why we make the decisions we do and the cultural, situational, and psychological reasons for ethical and compliance failures is, I believe, the key to better organisational ethics and behaviour.

It is that mission that keeps me motivated. Why? Because I've spent most of my career working in emerging markets. I don't see corruption theoretically; I see it as nineteenth-century illnesses

stemming from unsafe water. The contractor who built the water pipes was unqualified (bribed to win the bid), and the subsequent pipe-laying overlapped with sewage systems. I don't see the money laundering pithily portrayed in high-budget TV series. I see North Korea funding brutal oppression, using banks in barely regulated nations to wash gambling and criminally acquired cash. I don't see human rights issues; I see logistics drivers in Myanmar forced to act as minesweepers at gunpoint. I don't see environmental violations; I see death after shoddily constructed hydropower projects collapse.

I am labouring the point intentionally. I don't relate to violations on paper; I see them experientially – and I haven't even got into human and wildlife trafficking. Compliance violations are not financial, white-collar, economic crime, or any other distancing language. They are crimes, infecting entire nations and robbing billions of people of fundamental rights. Corruption is the common denominator in almost all these issues – it is the *how* enabling almost all violations and deserves particular attention.

Maybe, therefore, we need to rethink integrity risk and compliance. That starts with honesty.

Why Now?

Organisational ethics is getting better, isn't it? Looking at whatever feeds you rely on for information will reveal the latest corporate, organisational, or governmental misdeed headlines. We could debate whether that is a function of unethical activity levels or increased societal and journalistic vigilance, but that

misses the point. It happens a lot, and we claim we want that to change.

I recently typed "business ethics" into Google and got 380,000,000 results. "Business corruption", a much clunkier phrase, generated 294,000,000 results. Acknowledging that Google – and its results – are not an academic analysis of all public discourse on the topics, that's a rough 56/44% split. If I said to you that 44% of businesses were corrupt, would you agree? Possibly not. So how many are? 30%, 20%, or 5%?

In more relatable terms, 5% of global Gross Domestic Product (GDP) represents an economy the size of Japan or Germany. Big.

I am not guesstimating that a certain percentage of organisations are all bad; I am saying the issue is significant. Any group is an aggregation of people with our collective flaws and limitations. We evolve (hopefully) and learn from our mistakes, creating more tolerant, transparent, and equitable societies. The entities and agencies who employ, serve, and supply us are also learning, but it's not easy. Where do you start?

I don't mind where you start; the journey and destination matter more. We are at an inflection point in many post-industrial economies, where environmental, social, and integrity concerns impact consumer, stakeholder, and employee actions and decisions. In the past few decades, I've seen a trickle (of genuine concern about ethics) turn into a steady stream. The natural inclination for many is to write more policies and create more controls. I prefer to treat people like adults and empower them to make better decisions.

Who Is This Book For?

This book is for those trying to do the right thing, usually with insufficient data, limited resources, and often with recalcitrant or hostile stakeholders. Just because you say no to corruption doesn't mean the local politician won't stick their hand out. It's where honest intention meets risk reality that I focus. I've spent most of my career operating in places where the demand side of risk remains pervasive and robust. It's hard to do the right thing when the decks are stacked; the political framework is inept or corrupt, the judiciary biased and bribed; and competitors don't share your values. That's the bad news. The good news is you're not alone.

I remember the turning point in my career vividly. I was working with a construction and mining firm that had uncovered the potential bribing of public officials in one of their subsidiaries. I was part of a team tasked with interviewing, assessing the risk, and training other subsidiaries. We were running a workshop in Manila. On entering the conference room, I saw a depressingly familiar sight, many large, burly white men with thick gold bracelets and necklaces, arms folded, leaning back, looking hostile. We weren't five minutes into discussing corruption risks when we got the first, "It's *how things are done in The Philippines*." More came once the one person had opened the floodgates of sweeping national assumptions. Terms like "*these people*" and "*they*" – always an indicator of otherness – reverberated around the hot and drab conference room.

Luckily, after about 30 mins of bashing our heads against hairy-chested "I reckon . . .", *they* spoke. The local finance manager,

a Filipina, stood up, banged the table (gently, but enough to get attention), and said, "No, you don't get it. I have to bribe to get down my road to work. I have to pay the doctor for them to see my sick child and the teacher even to grade their papers. I've had enough. If you want to come here, benefit from our resources, the least you can do is bring better standards."

I have wondered about the ethnocentric implications of imposing Western standards of corporate governance on other cultures. In Southeast Asia, where I lived for 12 years, there is a complex history and relationship between former colonisers, now investors and partners. The message is consistent; don't screw us up (again). I have worked with clients from numerous cultures – Japan to Brazil to Israel – and there is broad agreement on the vast majority of what *should* be done. The *how* may differ, but more ethical business practices are not one nation's or one culture's cause.

There is a danger that I talk too much about emerging market risk. In ten years covering the EMEA region, I saw more fraud, human trafficking, and money laundering in London and the United Arab Emirates than in any other country. There is a sort of hierarchy of douchebaggery. Corrupt elites in poorer nations supply resources (including people) that more prosperous nations exploit. The ill-gotten gains and shady deals are concealed offshore and washed in glitzy financial centres. Therefore, the job of ethical culture building is arguably more critical in the established markets, with our distance from the downstream impacts of our (in)actions.

My audience, you, I hope, are organisations and people who want to do the right thing, wherever you are, whatever the

circumstances and starting base. You might be working in a large organisation, fighting the good fight, where changing behaviours might feel like trying to turn a battleship in a bathtub. Or maybe you're in a start-up or purpose-driven social business, deciding how to build up your ethical culture and systems to navigate the uncertain seas. It doesn't matter your organisational type or size. I've worked with all sorts; the issues are – to quote South-east Asia's favourite saying – "Same, but different." The consistent factor: you care about doing the right thing because it is the right thing.

My job is to try and make the risk landscape (and regulation) navigable. So let's begin!

Endnotes

1. Donald R. Cressey, *Other People's Money* (Montclair, NJ: Patterson Smith, 1973), p. 30.
2. https://www.acfe.com/fraud-resources

1
WHO DO YOU WANT TO BE?

If you run an image search for "organisational values wordcloud", you will see similar words. I do this periodically to see what's changed; very little usually. Integrity, ethics, and innovation – or variations thereof – will typically be in most clouds, as will respect, excellence, and inclusion. The similarity in phrasing hollows out the words, leaving them more performative than purpose. I call bullshit, or "Purpass" ("Purparse" for us Brits), the term I coined to denote fake corporate purpose.

Another internet search for average employee satisfaction will produce results that generally herald an engagement rate above 50% as meriting praise. Break out the bunting; only half our employees care. I appreciate I'm taking a leap of logic and faith here, but if significant portions of our workforce are not engaged, they're probably not on board with the mission and values mantra. Fixing this disjoint between what your organisation says and what people feel it does is the first step to effective risk and compliance management.

If you'd told me that five years ago, I'd probably have said, "Hmm, interesting", which is my native British for, "Rubbish, not

interesting." I used to be quite sceptical about values, missions, and visions. Too many brand refreshes, replete with swooshes, fonts, and colours, chosen by people in functions that never saw operational realities, made me feel it was all rather cosmetic. Then I got out into the world of small and medium enterprises (SMEs). Talking to people and getting their input is easier when you're smaller. A friend who started a now-booming compliance business providing reporting lines described how his organisation had created their values: they'd asked people! Revelatory.

It's pretty easy to find a list of values, and asking people to vote for their favourites (top 5, for example), takes no time. But are the values all a bit the same? Yes, they are. To illustrate my cynicism, here is a Corporate Values Bingo game (Figure 1.1).

Many of these words have become meaningless and patronising. Are you saying to people, "You're not welcome unless you

Figure 1.1 Corporate Values Bingo.

are. . ." or saying we ascribe to grand pronouncements without any roadmap to explain *how*? Is it any wonder so many employees are disengaged?

You must demonstrate how you want things done; this should not be a FIFO approach (fit in or F-off). It is more akin to house rules. Are you a shoes on inside, or shoes left at the door kind of organisation? I've lived in Asia most of my working life, and if I had issues with shoes off at the door, I'd not have had much of a social life. It is okay to explain how you want things to be done broadly.

Depending on your organisational size, you may then be able to come together physically or virtually to start that discussion. If you're concerned that stronger personalities – or those in positions of authority – might dominate or stifle the voices of others, good, you should be. Technology can be a democratiser here, even in person. For example, suppose you're trying to compile a list of words that might describe *how* you behave as an organisation. In that case, you can ask people to group them into overlapping or similar concepts. Voting integrity, ethics, respect, transparency, honesty, and honour into a distinct *bucket* will make the next step easier.

At this stage, however, the words are still meaningless. What do these words mean in action? You can ask people to create "doing" sentences. The bucket above might become, "We do the right thing, even when no one is watching." Is that integrity or ethics? Yes. Is it honest? Yes. Is it respect or transparency? Maybe, maybe not. These finer points will stimulate discussion, forcing you all to define actions rather than demonstrate respectful or transparent behaviour. Or perhaps you'll decide transparency isn't your

schtick, as might be sensible in some professions where discretion is the currency of credibility.

If you hit an impasse, vote or shelve that topic and move on to the next bucket. After a while, the values start to sort themselves, or more precisely, the lived definition and actions associated with them. Every organisation is seeking to achieve something. Align the values to that. If you're in retail, I'd imagine a customer focus might be primary, whereas, for logistics, it'll be speed and security.

If you're now thinking, "we already have values", good, check back in with your people to see if they all (still) resonate. Your *how* and *what* are not immutable and unchangeable. As societal and political progress, albeit often glacial, moves and changes opinions and challenges perspectives, so should your organisational purpose. You will also need to make sure your ideas translate across cultures. The head of compliance for a large manufacturing company recently told me he had sent a survey about diversity, equity. and inclusion to colleagues in China. They had replied, "This is Western ideals, not relevant here." The Singaporean team at a large UK-listed financial institution also told me that my referencing #MeToo in a training session about ethics was "A Western topic that we don't recognise."

In both instances, and after some digging, the issues were more to do with the medium than the message.

Ideas need to be localised. Every culture I have experienced has its own stories, belief systems, and values. These ethical frameworks overlap more than they ever contradict. If a fan of the Greek and

Roman Stoics read Confucianist or Daoist texts, they'd likely find more that complements than contradicts. What went wrong in the situations above? Do Chinese people not care about inclusion? Are women free of harassment in Singapore? No.

My friend and I had not adapted the message for the local audience. Adapting is as much about finding the right words as allowing people agency. When I asked the Singaporean team what would work better than #MeToo, they replied, "Fairness." Fair enough!

I can already feel some of you squirming. You may be thinking of a decentralised mess where we mangle every message into something locally acceptable, thereby losing meaning or, worse, conflicting with the intention. Moral relativists will point out that we do not understand ethics similarly. You are right, but what's the alternative, misfiring missives with oblique aspirational words greeted with cynicism and rolled eyes?

Having tried to arrive at communal values in the most hostile environments – parents to two terrors – I can assure you it is possible. I've even included how we did it here (Figure 1.2).

We started with a long list of values (the internet is full of such lists). Each member of the family got to choose the five that resonated most. We whittled those choices down to seven words we wanted to turn into sentences. Yes, this involved compromise, but if you allow people to pick five, most of us will cede a couple without too much drama. Then came the significant bit, turning somewhat abstract words that sounded pretentious into lived action, as illustrated by one of the values in Figure 1.3.

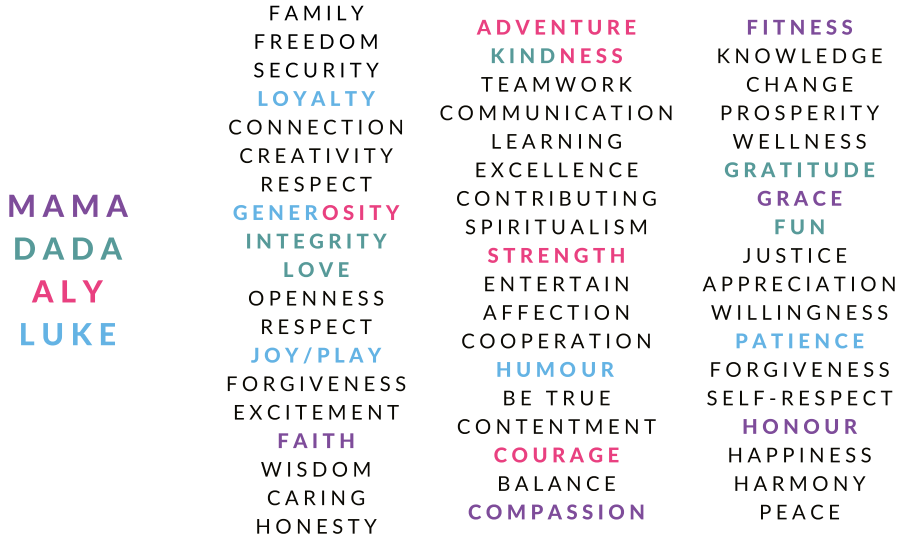

Figure 1.2 Possible family values.

We wanted to use the active (not passive) voice to give positive meaning and personal ownership. This process stimulated debate and discussion about how we wished to conduct ourselves collectively and individually (and hold each other accountable). Crucially, this was a democratic process. The parents did not get a more significant vote, and the kids hold us accountable (repeatedly!) when our behaviours fall short.

Why did we feel the need to embark on this exercise? Because rule-setting was unwieldy. As parents, we'd seldom remember what rules we'd set, let alone the associated punishment and reward tariffs. The kids probably forgot – or acted as they had – and chaos ensued. We could have codified every expected behaviour, but as an employee of an organisation with a weighty Employee Handbook (or equivalent door-stop) will testify, no one reads rules. Adequately articulated, agreed, and tangible

Figure 1.3 Example family value.

statements serve as the first line of defence against unethical behaviours.

Rules, policies, and procedures have their place, but they are the safety net when values have faltered. A moral code at a familial, organisational, or team level provides a framework around which you can hang your rules. For example, if your value is "We deal fairly and honestly with all stakeholders," that is the hook for specificity around fair competition, honest financial reporting, transparent data policies, etc. Without the framework, you have a shopping list of rules that few will read; adherence becomes about an individual's judgement in the absence of guidance, which frequently ends poorly.

If my friend and I had first consulted our colleagues and clients about the intention behind diversity, equity, and inclusion, we might have found an agreed framework. Few people object to broadly held human language around ethics; we tend to want to be good. We want to feel like we have some choice. Give that choice early in your organisational journey and regularly check back in.

Why not write your statements on the front page of a brief document you send out a month or two after people join, with a blank text underneath, and ask your employees to write down how they plan to demonstrate them in their work?

There are several reasons why this might help. Most of us like feeling some agency over our lives and work. For example, a study of just under 1,400 healthcare workers in Taiwan revealed that increased autonomy led to greater job satisfaction and a lower likelihood of leaving their positions.[1] Another study involving 20,000 people, in 2017, by the University of Birmingham, added that autonomy enhanced general well-being and job satisfaction.[2] Asking people to take ownership of their ethics may be more palatable than telling them how to behave.

Furthermore, if we have to author content, we might read it!

Start with Purpose

If deciding what organisation you are (or want to be) is challenging, fear not. That's a good thing. It's like job interviews, where hiring teams ask us to list our best traits or characteristics. There's often dishonesty to that process. The organisation pretends they want "out-of-the-box thinkers" for a role that is

mainly spreadsheet jockeying. The candidate plays along, feigning a passionate commitment to and admiration for an organisation they have yet to experience or understand. It's like a mating ritual – not with birds of paradise doing exotic and captivating dances, more like spiders deciding who will eat who. Dispensing with this performance requires courage and honest examination. The employer should, I feel, be straightforward about what the role *actually* entails. The employee should be honest about their expectations and competencies.

This recruiting ritual bears an uncanny resemblance to the disjoint between values and reality at the organisational level. Lofty pronouncements about putting customers at the centre of all we do can quickly become the stuff of ridicule when your frontline customer service representatives hate their boss. Similarly, pledges of integrity and valuing diversity are easily unpicked when tokenism and dodgy dealings are exposed. Employers must expect that employees (and other stakeholders) will not respect the contractual boundaries set unilaterally and (perceived) unfairly. Your average employment contract forbids you from any freedom of genuine expression and opinion about your employer. Poorly done and clumsily, such edicts will not be respected by inhabitants of an ever-more connected and discursive (if also divisive) world. Values set with the hopes of outwardly projecting a culture that does not exist internally are corporate catfishing. Not the bottom-dwelling fish beloved of niche reality TV shows, the process whereby a person creates a fictional persona or fake identity on a social networking or dating service.

If your organisation is a low-cost airline that charges people to relieve themselves, maybe dial back *we care* rhetoric. Instead, it

might make more sense to focus on cost, efficiencies, and reliability if they are the currencies of your competition and part of the corporate DNA. At least people (inside and out) will know what to expect. Similarly, if you're an investment bank routinely fined for financing terrorists, criminals, environmental degradation, and other ills, terms like *sustainability* will seem trite. Not everyone will like you if you're authentic, but there's a much greater chance they'll respect you.

Existential questions about your organisational existence extend beyond the realm of risk. For those in risk, legal, or compliance roles, your ability to influence stated values may seem limited. It is still worth raising the point – and the need for a constant examination of purpose – with the powers that be. It's often easier to let employees tell you what they think. Many organisations will use employee engagement (or similar) surveys to help here. Be careful. Some of the common pitfalls include:

1. Asking for too many personal details, rendering assurances of anonymity hollow.
2. Not asking the tough questions.
3. Not sharing the (complete) results.
4. Not doing anything with the results.

I remember one such survey, where the salary band, location, and department disclosure requirements meant I would have been instantly identifiable. I tried to be honest, but I held back a little. The questions are often directed at the organisation, not the person completing the survey. For example, "Do managers uphold

standards of excellence?" may seem a good question if excellence is one of your values and critical to what you do. However, it's asking the respondent to make personal judgements about managers they see (including their own). Instead, you may consider asking questions about their experience. You are trying to establish what they feel and think, after all. For example, you might ask for agreement or disagreement to the following statements:

1. I can discuss challenges with my manager.
2. I can speak openly with my manager.
3. My manager helps me.
4. I can ask my team for support.
5. I understand what my manager expects of me.

This non-exhaustive list of statements examines how a manager can create an environment where excellence might be possible. Many other important questions – not least around how valued someone feels – will impact their ability to strive for and attain excellence. The literature on psychological safety is constructive here – and when creating potential surveys. In the context of teams, Amy Edmonson defined psychological safety as "a shared belief held by members of a team that the team is safe for interpersonal risk taking".[3] Psychological safety is an expansive area, but it should be prerequisite reading for anyone managing risk.

To illustrate, we need only consider some reasons for ethical failures. In surveys – including those conducted by the ACFE and the Nordic Business Ethics Network[4] – I read the answers to two questions: (1) why did you not speak up (when you saw

wrongdoing)?, and (2) why did you break your ethical principles? I have also asked these questions in risk assessment and training work. Themes emerge, which I might summarise as "I didn't speak up because":

1. I didn't think it would make a difference.
2. I was scared.
3. I didn't think it was my problem (I didn't want to make it my problem).

The responses to questions about compromising our ethics reveal causes including:

1. I was told to (by my manager or someone senior).
2. I feared not hitting targets (time or financial metrics, typically).
3. Everyone else does it.

A theme in all these responses is a lack of psychological safety. We will discuss in detail the speak-up culture later. Still, these statements suggest that when people don't feel they can (safely) raise concerns, have an impact, or admit mistakes, they will be unlikely to uphold whatever values or missions you ascribe. To build a strong risk culture, you need people to take risks! The first such risk is telling you what they feel about your values. Without alignment of values and behaviour, your risk infrastructure has no foundation.

Be purposeful, ambitious, and honest with your values and goals. Those goals should extend to your strategic and financial targets.

Building a culture of integrity is impossible if you're simultaneously setting objectives that require corner-cutting and unethical dealings. If you take nothing else away from this book, set realistic targets if you want to reduce your risk exposure RADICALLY. Most bad ethical decisions stem from fear (of leaders or not hitting targets).

Be Authentic

Why is it such a big deal to have values conflict with reality? Doesn't everyone? Aren't they a statement of what we aspire to? You can manage risk without such alignment, in much the same way an oppressive state rules its citizens – through surveillance and fear. I wouldn't recommend that unless you have deep pockets and a stomach for attrition. Let me give you two examples to illustrate the point.

Unrealistic Targets

A US-headquartered healthcare firm had built a culture of compliance. They had compliance officers and champions, many rules, a glossy code, and practical financial monitoring frameworks.

The regional head of legal & compliance asked me to speak to their Vietnamese subsidiaries' management team. HQ had first tightened rules around gifts given to healthcare professionals (HCPs, doctors mostly), and the local team responded by taking them out to nice dinners and lunches. When that was banned, they moved to pay HCPs to speak at conferences. The iron fist of compliance squelched that ruse.

Next, an expensive claim came across my client's desk for thousands of dollars to "rent a room for an hour". Upon enquiry, the legal & compliance head realised that HCPs, so indignant at "compliance" clamping down on gifts and entertainment, demanded a steep "rental fee" to use a theatre in the hospital to demo the products.

You've probably realised that influencing HCPs through such payments and entertainment is slightly off. The local management team retorted, "Well, you didn't have a policy banning it [exorbitant 'rental' agreements]."

The issue was clear; no one thought of values or ethics, "How might this be perceived? What is our intention here? Is this the right thing to do?" Policing organisations that require you to prohibit every possible misdeed in some policy or missive is exhausting and ineffective. We will cover some situations where specificity and well-documented rules are necessary; for example, the right thing is not immediately obvious (like complex anti-competition or data privacy regulations). However, understanding or estimating intention (or motive) is essential in most risk areas. What did we, or the source of threat (adversary), hope to achieve? In this example, when pressed, the local management team struggled to explain how renting a room for a couple of hours could or should cost thousands of dollars. What was the intention of the HCPs? Presumably to get money where once were gifts, lavish dinners, and handsome speaking engagement fees. What was the goal of the sales representatives? To get the HCPs to buy, even if that meant paying them off. Did anyone need rules to see this was wrong?

Realistic Targets

A few years prior, just as Myanmar opened to the world (2011 or thereabouts), I met a Japanese heavy equipment manufacturer's APAC management team. We were running a workshop on ethics and compliance.

They had very little by way of a policy or monitoring framework. We asked them how they assessed and managed risk as they'd had remarkable success at avoiding the challenges that befall many others in their sector. Their leading salesperson described a prospect in Myanmar who had recently asked them to provide excavators and bulldozers. The salesperson had flown to Myanmar and "kicked the tyres." He told his regional CEO, "We shouldn't bid; these guys are cowboys." They didn't respond to the tender. A few weeks later, the prospective client bulldozed monks protesting environmental degradation at the mine site. The media carried photos of my client's competitor's vehicle, the weapon in the multiple murders. I asked the CEO how he'd agreed to the salesperson's recommendation and passed up on what would have been a lucrative contract. His reply was telling, "I trust my people to do the right thing."

You can manage risk well with limited infrastructure if you have clear and consistent values, hire the right people, empower them, and back them up.

The Japanese firm did, of course, have procedures to document business decisions. They also informally discussed risk when discussing what projects to (not) pursue. The difference with the

HCP example was that values and ethics led to decisions, not the ticking of boxes in compliance with rules.

Most organisations sit between these two examples. The trick is striking the balance of autonomy and control that works for you. This balance may be further complicated by workforce composition and demographic differences in larger organisations. Attitudes to instruction, hierarchy and critical feedback may vary widely across globalised firms. The analogy that makes sense is the equaliser on digital stereos (I know, I'm giving away my age). You can alter the frequency and timbre, but you must play the same song.

How do you choose the right song? You could try the experiment we did as a family. Doing so may not be as difficult as it first seems. Logic-based and advanced surveying tools, or even interactive feedback tools like Mentimeter,[5] help assess our thoughts and feelings at scale quickly. As ever, the devil is in the detail. We must allow space for nuance. Asking people if integrity is essential as a binary (yes/no) question will generally elicit an overwhelming response in the affirmative. However, it may not be their first choice if you ask them to rank a list of values – one of which is integrity.

Furthermore, you might see more qualified responses if you ask, "How important is integrity?" on a Likert scale (from unimportant to essential). As I said, authenticity is vital. For example, have you ever been to a mechanic or called out a repairperson for a broken home appliance and heard the ominous *sharp-intake-of-breath-through-pursed-lips*? This phenomenon is usually followed by obfuscating or deliberately complex language – interspersed

with jargon or the names of obscure widgets – and then a hefty quote. What about the adverts that say, "Hurry, limited stock"? Or the real estate agent who claims another buyer is putting together an offer for that dream home just outside your intended budget. Of course, there are artisans, mechanics, salespeople, and realtors with impeccable integrity and honesty. Not every positive word – like integrity, honesty, transparency, kindness – may authentically resonate with your organisation, so don't fake it.

We respond to genuine much better than we react to performative. Choose authenticity, but recognise this is just the start of the journey towards ethically and appropriately managing risk.

Where Does Risk Fit In?

Let's also consider risk when deciding what kind of organisation you want to be. It is everywhere, and most good opportunities live on the other side of fear and risk. We must, therefore, define our risk appetite.

Risk appetite and risk tolerance can confuse people at first. The former is typically more qualitative, and the latter is given the veneer of quantitative (even if that is an estimation). Let me explain with a scenario. Your company, Startup Sensation, might decide certain risks are not worth taking as they could cause significant damage to the business. The operative word is significant, which varies depending on what you do and with whom.

Let's say Startup Sensation sells ethically sourced vegan products. Significant damage might stem from links to animal (or human) rights violations. Startup Sensation's leadership team may deploy

risk management resources to supply chain transparency and ethical sourcing. Startup Sensation could elect to expend fewer resources on fraud risk management; perhaps they feel purpose-driven people are less likely to defraud them. The leadership might qualify the risk tolerance as near-zero per cent for animal rights violations in the supply chain and decide they won't accept fraud risks above 3% of revenue.

If you think this doesn't make much sense, I'd agree. Risk appetite and tolerance are very useful when you're a mega-corporation with data and resources to model and estimate most things. It's handy if your business lends itself to qualitative analysis, for example, a financial services business where fines, fraud, and human error can be qualified and quantified (within reason).

Now, if Startup Sensation sold discounted (factory outlet priced) goods online, relying on warehouses in low-cost locations with lower-cost workers, the tolerances might be flipped. In this scenario, they may care less about ethical purchasing and more about fraud impacting tight margins. Maybe the leadership team would spend no time vetting suppliers and much more time monitoring employees, packaging areas, returns, refunds, suspicious purchasing patterns, and more.

To deal with the confusion, you can go one of two ways: (1) get all ISO; or (2) keep it simple. The ISO path (in particular ISO 31000 – Risk Management[6]) defines risk appetite as "the amount and type of risk that an organization is prepared to pursue, retain or take". Risk tolerance sets the parameters and variation (often in percentage terms) within each risk (e.g., returns of faulty goods of

less than 1% of revenue). If your eyes are glazing over, maybe this model is more straightforward:

1. **Risk appetite**: What kind of organisation are we?
2. **Risk tolerance**: How will we know if we're on track?

If you've established your organisational purpose and values, it should be more straightforward than considering the entire risk universe in abstraction. For the vegan products, trust (in the origin of the products), treatment of your employees, and customer service should probably be areas of low-risk appetite. The risk tolerance will become the flipside of your promises; for example, if you advertise your products as "100% cruelty-free", you'd better damn well have the risk controls to ensure 0% of that in your supply chain. Similarly, you could measure employee treatment with psychological safety assessments, engagement surveys, turnover rates, employment disputes (unfair dismissal, harassment, discrimination, etc.), and exit interview data, to name a few.

I am covering a lot of ground very quickly here, intentionally. My experience of risk appetite and tolerance is that they're pointless unless you understand the frontline risks your organisation experiences, the focus of much of this book. You may wish to return to these areas once your risk universe is clearer.

Be Purposeful

Just because many organisations fail to live up to their values and mission statements have become a joke (in many cases) doesn't mean they're worthless. In my mind, they are not some

brainwashed mantra to be uttered by subjugated drones; they are your purpose. If that is to make as much money as possible, screw those pesky customers and employees, then keep values focused on profit, efficiencies, and cost reduction. Be authentic, get opinions from within, and make sure you have the right building blocks for the cultural, governance, and strategic infrastructure you will build around them.

Endnotes

1. Blossom Yen-Ju Lin, Yung-Kai Lin, Cheng-Chieh Lin, and Tien-Tse Lin, Job Autonomy, Its Predispositions and Its Relation to Work Outcomes in Community Health Centers in Taiwan, *Health Promotion International*, 28(2) (2013), 166–177. https://doi.org/10.1093/heapro/dar091.
2. D. Wheatley, Autonomy in Paid Work and Employee Subjective Well-Being, *Work and Occupations*, 44(3) (2017), 296–328. https://doi.org/10.1177/0730888417697232.
3. Amy Edmondson, Psychological Safety and Learning Behavior in Work Teams. *Administrative Science Quarterly*, 44(2) (1999), 350–383. https://doi.org/10.2307/2666999.
4. https://www.nordicbusinessethics.com/survey/
5. https://www.mentimeter.com/
6. https://www.iso.org/iso-31000-risk-management.html

2
LIVING UP TO YOUR PROMISES

The real work begins, turning your purpose into practical (and concise) guidance. We learn and relate to information differently. There is no perfect solution to communicating your expectations across the organisation. There are a few hacks, however.

Don't be too shy (or proud) to beg, steal, and borrow from other parts of your organisation. For example, if health, safety, and environment (HSE) is a more mature part of the risk function, look at how they communicated messages, socialised expectations, and set frameworks. HSE content and culture are borrowable because (typically) they are straightforward. That level of "wear a hard hat at all times while on-site" may seem simplistic for ethics and compliance issues (which can get complex), but my rule is if I can't explain it to a 10-year-old child, so they understand it, I'm not explaining it clearly enough. HSE does clear guidance pretty well, usually.

Other teams with lessons to teach might include information security, quality assurance, and marketing. Good information security guidance doesn't waste time explaining how a computer

works or the intricacies of firewall breaches; they focus on behaviours. The message might be "don't stick thumb drives into your laptop" or "only click links to legitimate and known sites". In ethics and compliance especially, many feel the need to explain their workings; few of us care. Have you ever sat through a compliance training session where the various violations under a given law were poured over in gruesome and unflinchingly dull detail? Most of us have. Understanding the adequate procedures defence to the UK's Bribery Act 2010 may be helpful knowledge for the board (and select other senior leaders). If your objective is to tell salespeople to stop wining and dining clients to win business, talk through those scenarios instead. Focus on the behaviours that drive the issues, not the legal ramifications. Making training stick we will cover later, but remember, the medium is the message.

Quality assurance for many organisations is essential. Contamination, failure, liability, injury, and death are words no one wants to hear. How do you ensure those words don't materialise with respect to your organisation? I imagine it's not through lengthy policies written in legalese or interminable training videos featuring out-of-work actors walking at diagonals across the screen as they talk confidently to the camera. Typically, one might assure quality through a blend of simple frameworks, concise, and user-relevant training, with supervision and testing. Look at these systems and processes and see what you can borrow.

Finally, marketing (or the equivalent function) will have much to teach about relatability. These folks will speak the language of impressions, reactions, click-through, and engagement rates. Marketing will know how long people linger on certain intranet pages, what types of emails get read, whether people click links

or prefer embedded content, etc. Beyond your organisation, what resonates with customers? There is no shame in using attention-grabbing, pithy, or witty content to get across your (serious) points; generally, it's preferable.

A friend of mine, currently the Chief Compliance Officer for a large logistics firm, described the best compliance officer he'd ever met. The organisation was in disarray (from a compliance perspective), and they took the unusual decision to appoint someone with a marketing background as the new officer. He embarked on a world tour of the various global subsidiary companies with a simple presentation about compliance; one slide, with his mobile phone number. The message was clear; before the organisation could resolve issues, they needed to understand why they kept occurring. The simplest way was to build trust; a senior executive giving you their direct line seemed a quick way to generate that. My friend, Charles, explained how this taught him a second vital lesson: brevity. Charles explained that with every new regulation, he made it his mission to ensure that little of the legal language from the guidance made it into any of his policies or communications. Why is this excellent advice? Google anti-competition law, wherever you are, and then try and read the legislation to the nearest 10-year-old. Let me know how you get on.

Or, you could explain to that same precocious (I've yet to meet a 10-year-old that isn't!) primary-schooler the concepts using classroom dynamics. It might work better. For example, would it be fair if a small group of students blocked access to the swings during break-time? In legal speak, this might be the denial of market access. If those same students copied each other's answers during

tests, your 10-year-old advisor might say that was unfair (or collusion, in grown-up speak). I'm not suggesting you distil complex law into child-centric examples, more that you communicate the core of the message succinctly and in a format people can follow. In other words, a call to action – a central component of most marketing campaigns.

In later chapters, we'll cover communication and training strategies (that work), but first, you need to set realistic expectations around living up to your promises.

Zero Tolerance = Zero Clue

I am sure you have heard the phrase "zero tolerance". It is used in numerous settings, from law enforcement to school bullying to compliance. In all cases, it's at best unwise and at worst highly damaging. I am not suggesting we tolerate unpleasant and potential criminal behaviour. I'm arguing that zero tolerance loses trust and prevents people from coming forward.

I have worked on many investigations but have responded to more allegations and reports (often channelled through a whistleblower or speak-up line). When you interview someone brave enough to make a report, you often realise many others chose to stay silent; why? It's hard to know precisely, but my anecdotal experience suggests the most common reasons are:

1. I was scared.
2. I didn't think it would make a difference.
3. It didn't seem that important.

Fear as a deterrent to speaking up we will unpack in due course. The other reasons often link to zero tolerance if you talk to witnesses (who chose not to come forward). You have set an incredibly high bar if you claim that you will respond with full force to every violation and not tolerate infractions. Imagine if law enforcers said they had a 100% conviction record; would that fill you with confidence? Or would you think this sounds like North Korea? It is impossible to secure confessions (or sufficient evidence) on every case and allegation. Let me give you a few examples of issues I've seen.

A manufacturing company fired a senior employee for harassment. So enraged at his treatment, he threatened to go to the competition authorities with evidence he claimed to possess of "significant violations" involving his erstwhile employer. He made this allegation, having been ejected from the office and his laptop confiscated. The overzealous IT team wiped the computer immediately, readying it for the next person through the door. What should you now do if you have a policy claiming zero tolerance for anti-competitive practices? Fire him twice? With what evidence? He claims to have plenty, but you wiped his computer. To complicate matters, in that country (South Korea), the authorities offer witnesses and whistleblowers on anti-competition issues immunity from prosecution. Your chances of securing access and interviews with the subject (outside of a courtroom) are limited.

What about a female contractor (a security guard) alleging that an employee exposed himself to her repeatedly? What if the female contractor did not consent to an interview? Supplementary research suggested that the employee implicated had been the subject of other inappropriate allegations, but the lack of witnesses

hampered the investigation. What does zero tolerance tell you to do here? Fire the employee without evidence or due process?

These examples are necessarily simplified, and we looked at the logical investigative avenues (IT forensics, CCTV review, interviewing proximate witnesses). However, you will lose people's trust if you set your prosecutorial bar at a zero failure rate.

Harsh-sounding non-compliance rhetoric may force people to downplay the seriousness of an issue. Let's choose another example; let's say a new joiner, who is black, is not invited to team building nights out. The new employee challenges his supervisor, who replies, "We go to country and western bars; we didn't think it would be your thing." You would probably want more data to arrive at a prognosis and establish the subtext and intent of the supervisor's statement.

Now put yourself in the new employee's position; would you speak up? Let me qualify that. Would you come forward if the company has a zero-tolerance policy for racism? What if the supervisor is otherwise supportive and friendly, albeit emotional and culturally challenged? If you fear the supervisor might be fired, you may decide "it's not that important". But it is. These things make workplaces toxic. You need to have appropriate (and flexible) frameworks that allow escalation of concerns without the imminent threat of stiff penalties and enforcement.

Finally, zero tolerance can be and has been misused. We all make mistakes. I have seen instances where over-zealous or politicised punishment of non-compliance has destroyed trust in the risk and compliance function.

A few years back, an oil and gas equipment manufacturer invited a client for a factory site visit. The client arrived in Indonesia (from Singapore) and applied for a visa. Indonesian permits, especially related to technical work visits, can be complicated. The immigration official, sensing an opportunity to extract a corrupt payment, claimed she needed a different visa and detained the client in a cell. Understandably panicked, she called the manufacturer's country manager requesting help. He duly spoke to the officials who requested a "fee" to settle the issue and allow his client safe passage. He paid, which was the wrong thing to do from a compliance standpoint, but an understandable human decision as he was dealing with a distressed and angry client.

An internal investigation followed, and the zero tolerance for bribery was used as a pretext to fire the country manager. When I visited the facility – with a brief to understand how other similarly risky interactions might be better managed – the whole office was terrified. Extortive requests from officials are the norm in some parts of Indonesia's bureaucracy. Without the safe space to admit as much, no one wanted to make any decisions, paralysing the business.

In the Indonesian case, the clumsy and ill-conceived application of non-compliance penalties was not malicious. In other instances, it is. I have seen managers use technicalities of non-compliance to force people out of jobs. Often those targeted are speaking out against unethical conduct. For instance, a project engineer observed how bribes to win bids had seen woefully unqualified contractors appointed to an infrastructure project. The region was reeling from an earthquake that had left citizens without safe water. So bad was the work that the water was contaminated, and

the engineer estimated the tunnels would soon collapse, possibly causing fatalities and landslides. He raised these concerns. His employers threatened him with dismissal (they were in on the corrupt plot), but he continued. Eventually, his superiors used a minor instance of timesheet non-compliance as grounds for firing him.

The water project case is not an outlier. A simple internet search, especially with keywords including "tech sector" and "employee harassment", reveals that performative or ineffectual zero-tolerance frameworks are common.

In summary, recognise that committing to zero tolerance – or another similarly sweeping and all-encompassing phrase – will not work because:

1. It is unrealistic and sets you up for failure.
2. Violations are not binary; they're on a sliding scale.
3. It allows little space for restorative justice.
4. It can be a deterrent to people coming forward.
5. All too often, it's performative (showing off to regulators and investors).

What's the alternative? Be honest and explain you do your best, which is an evolving process and be open to feedback. Then be as transparent as you can be about the process and findings. That notion can make people fidgety and nervous (lawyers especially), but the best lessons and learnings come from actual events, not fictitious scenarios.

To be clear, I am not advocating leniency for the more severe violations. I suggest realism and honesty with your people around the consequences of failing to live up to your values.

Managing Reasonable Expectations

Now the real work begins: reasonableness. For the legally minded among you, this will be a very familiar concept. The reasonableness test is a staple of various laws and statutes; it is also subjective. For lovers of specificity, this may be frustrating, but it's your friend.

Early in my career, I sat through a surprisingly non-torturous presentation by the Financial Conduct Authority (FCA), a UK financial services regulatory body. It was the early 2000s, and other attendees raised objections about the lack of clarity in specific regulations. The speaker, whose name sadly escapes me, replied, "We didn't want to draw a straight line in the sand; we wanted a wiggly one. If you've ever tried to trace a wiggly line, it's not easy. Our decision was intentional; stay well on the right side of the line."

The concept was a sound one, ignoring the FCA's abject failures related to the flows of corrupt and dirty money into the UK. It's one I've used frequently since. For example, if two countries have laws on the same topic – let's say, bribery – and one prohibits private and public bribery, and the other only public corruption, which do you pick? Do you adhere to different laws in different markets? Or do you decide that bribery is generally not a great foundation to build a business and choose the higher watermark (farther from the wiggly line)?

Your colleagues want to be reasonable. Few of us set out to be the baddie in the documentary movie of our life in which we are the star. Managing reasonable expectations is explaining that lines can sometimes be hard to trace and err on the side of caution. This approach is sometimes called a culture of ethics (distinct from a culture of compliance). We will unpack some ethical decision-making frameworks in due course, but you want to encourage people to ask questions for now.

The first step to walking your values and building a culture of genuine (not performative) integrity is to discuss what that looks like in daily decisions. If you think this sounds cumbersome and like it will slow down decision-making, it's not really. You probably already have meetings to discuss what to do (about almost everything). A "Have we discussed the risks or potential consequences?" question is not a massive task. You're already doing it, maybe not all the time or for the risks we'll discuss in this book.

At this stage, it may help to define reasonable expectations of employees (and other stakeholders). Typically, this might take the form of a Code of Conduct, Code of Business Ethics, or something else with the word Code in it.

Your Code

Ah, the Code. Never in the writing field has so much time been spent, by so many, on something so few read. Ask most people what's in their organisation's Code, and they'll probably say, "Rules 'n' stuff", before shrugging their shoulders and pushing up their lower lip to make a feigned confused frowny face.

They might reference the introduction from a CEO (or equivalent) they have never met, usually a grey dude in a dark suit. You're thinking, why would they not read something I am selling so well?

Because it's usually dull boilerplate rubbish, a recent experiment – to try and find clear decision-making frameworks – in various Codes of large organisations confirmed the issue. Most decision-making frameworks start with "We always obey the law" – oh, yeah, slow clap. The basis of your ethics is avoiding criminality; please stop it. You're dreaming too big. The next step might read, "We always follow the Code and our policies [which no one reads]." Now, where's my prize?

Codes are desperately dull and lack any thought of their audience. Most of your colleagues are not experts on the law. Saying that you expect people to follow the law leaves a lot to be interpreted (often wrongly). Most folks will recognise that stealing is against the law. Still, they'll have a more challenging time determining the legal framework on data privacy, anti-competition, appropriate waste disposal, cybersecurity, or numerous other areas that most organisations must contend with. Secondly, the law is a safety net, not a moral benchmark. We need to aim higher than what we *could* do to consider what we *should* do.

A good Code talks to the reader. What is it we do (as an organisation)? How do we treat one another? Where might we face unethical, legal, or other pressures? What do we ask you to do about that? Who can you speak to if you're aware of a possible issue? Throughout these questions, succinct scenarios from within your organisation can bring the Code to life.

I wanted to spell out what a good Code should look like, but that's tricky when it has to be bespoke to your organisation. The best I can do is this:

1. Introduce the issue in a line or two. For example, a conflict of interest is where your interests might compromise your decisions or judgement in the workplace.
2. Explain the common areas (of confusion): How and what (possible conflicts of interest) to disclose.
3. Explain what you want people to do.
4. Give an example or two.
5. Direct them to any further resources.
6. Have a simple key to explain who needs to know (not all Code issues are relevant to all employees).
7. Tell them where to go if they have a question, comment, or concern.

If you think this will make documents epic, potentially, in this long form, it will. Using the miracle of graphic design and imagery, you can fit anywhere from two to four areas of your Code on a landscape-oriented PDF page.

Taking a step back, you might wonder what sage has the answers to points 2 and 4. Yes, the team(s) responding to possible issues can help, but so will employees working in frontline roles. My best anecdotes always come from frontline stories. I'll tell you the one I heard this afternoon. An insurance assessor visited a policyholder who claimed a $200,000 excavator had gone missing;

"poof" just vanished. This visit was not the assessor's first rodeo; they researched the make and model. Upon arriving, the assessor's first question was, "What colour is it?" An interesting opener. The policyholder replied, "Yellow, I think." A fair guess, given many excavators are yellow or orange. Unfortunately, this model only came in white, a less common colour. The policyholder withdrew the claim shortly afterwards. This story won't add much to a Code, but it demonstrates that case studies and actual situations are better teachers than pages of theory; in this case, preparing for investigative interviews is essential. These accounts can also inject a modicum of humour, which tends to be more memorable.

Crowdsource your content; it will be more relatable and actionable for your readers. Then have a clear "Call To Action" (CTA). I will repeatedly return to this concept, as risk and compliance doctrine is often couched in the pastime of fence-sitting. Give an opinion, and give your colleagues a CTA.

There can be an understandable temptation to get the Code together quickly. Typically, this might include researching a few competitors' or sector-relevant versions and picking and choosing what you like. That makes a lot of sense, but be careful. When I was about 12 years old, my school, to make us less feral and more valuable members of society, decided it would be a great idea if we learned the basics of garment-making. I believed my dad would appreciate silk boxer shorts (he didn't). One fabric was not enough for this endeavour. Best to choose about seven different patterns, a riot of colour, in my mind at least. Other materials also react differently to different stitching techniques. The lopsided and scratchy result lasted one

round in the washing machine, emerging as a slew of soon-to-be dusting cloths. Don't make your Code like my dad's boxer shorts.

If you want to draw inspiration from the work of others, and why not, treat it more like an interior designer might. Sketch out how each room in your house – each area of the Code – looks for you. Where are there lights (additional content and training support), the doors (where to go for help), and who lives in each room? Now take those snippets from others' Codes and work out how you'll need to adapt them for your home. I've seen this done well by a select few. They all had a plan – a framework or floorplan – where they needed to place fixtures, fittings, and furnishings.

I have created template Codes in the past, and they have their place. Typically that place is when trying to tick a box – often as part of a tender or a client onboarding process – where you don't have weeks or months to draft your organisation-specific version. Even in these situations, the template Codes are built with adaptation – to reflect those issues that matter to you. Whether your Code is a work of art or a template needing refining, the good news is you've taken your first step, and it's probably better than the vast majority of legalese dirges out there!

Who Follows the Code?

Now you have a Code (or something similar). Who needs to know? This question may seem obvious, and you might be thinking, "Our people, duh!" True, but that is a big assumption. In many organisations, Codes are not universally accepted or recognised.

The senior leadership team might view the Code as the framework for employees (an autocratic but not uncommon view). Those subject to that yoke will likely view the Code as performative rubbish. Laws – and a Code is your internal legal system – are unpopular when they are enforced unevenly (or worse, politically and selectively).

Your first task, which can be challenging, is to explain that even venerable and lofty boards are subject to the Code's provisions. A less aggressive way to do this might be to ask members of the board (or your version) to own sections of the Code and communicate what it means to them. Senior leaders talking through their challenges and dilemmas humanises "them" to the "us" and enhances understanding. Teaching others has been proven to be one of the most effective ways to internalise knowledge – infinitely better than reading![1]

One of the better examples I saw in a giant telecommunications company involved simple self-shot videos by executive committee members talking about an "ethics moment" they had faced and how the Code had helped them. These approaches may also help frontline employees recognise that (most) senior leaders once met the same risks they now manage. Conversely, if you have leaders who have no clue about the frontline – which remains a depressingly familiar situation – keep them away from such initiatives, as they will do more harm than good.

With your internal Code coverage a bit clearer, you may now wish to decide how far the framework should extend. For instance, will you ask contractors, temporary workers, or consultants to comply? What about third-party providers? By third parties,

I mean any organisation with whom you have contractual or commercial relationships. If this sounds daunting or shocking, it isn't. I run a small business, and I am surprised when we are *not* asked to sign documents with Code in the title. Often these frameworks are a variation of the original – condensed and catered for the exposure we pose to our client or partner. It should be logical which elements of the Code are relevant to external parties, but we will explain how to manage external stakeholders later.

If you extend your Code to others, you also make it clear how and where (and to whom) they can ask questions or report concerns.

The Mood in the Middle

If you've encountered ethics and compliance language before, you may have heard the phrase "the tone from the top" or something along those lines. If leaders don't walk the talk, then you can't expect others to. It's a very sound principle, and myriad idioms point to the downside (where this doesn't happen), notably, the Chinese proverb "the fish rots from the head".

We talked about getting those leaders on board in the previous section, but we also need to consider the mood in the middle; how the managers (or similar operational leadership functions) feel about your Code, values, and organisation. You've probably heard the maxim, "people don't leave companies; they leave managers". While such a simplistic analysis of multifaceted choices is misleading, there is some truth in it. Rubbish managers pollute cultures. In various surveys and my anecdotal experience, one of the top three reasons for ethical

failures is, "I was following the instructions from my manager." It should be no surprise that the person with the most influence over your day-to-day can also have the most significant negative impact.

Therefore, understanding how your middle management feels about the Code (and your values) is an essential step to functional integrity. We discussed starting your values with purpose, and I offered a few questions that might help you understand how your people feel. Those questions again:

1. I can discuss challenges with my manager.
2. I can speak openly with my manager.
3. My manager helps me.
4. I can ask my team for support.
5. I understand what my manager expects of me.

If you're asking these questions, some possible additions or variations might include:

1. I understand what is expected of me.
2. My team knows what is expected of us.
3. My manager trusts me.
4. I feel safe making decisions.
5. I feel safe making a mistake.
6. I can ask my team for help.

7. In my team, we are all accountable for our actions.
8. Work is allocated fairly.
9. My team accepts different people.
10. My work is valued.

This list is by no means exhaustive, and you will need to adapt it to your organisation. The objective is simple, to understand how your people feel. Feelings get a bad rap in many business circles where rationality must prevail, right? Nope! Think back to the last time you bought insurance, was it a sanguine and analytical process or were emotions driving you? We can kid ourselves with our thinking, but our feelings are harder to manufacture. If you've ever tried to feel a contrary emotion to what you're experiencing, you'll know how challenging it can be. These more personally phrased questions are designed to understand the respondent's lived experience. Asking us to psychologically profile our manager – with the usual "my manager is . . ." statements – forces us to estimate the person's state and intentions. It's much simpler to just ask us how *we* feel.

Be careful about the identifiers you ask if you decide to go down some form of surveying or canvassing route. You must allow people the anonymity that encourages honesty. Once you have your results, you may find a few things. Some teams will be toxic but seemingly performing well – look for burnout here and losing some of your best talent. Other groups will be contented underachievers – maybe the managers are too much friendly and too little pace-setting. There will be bright spots of happy and high-achieving folks, as there will be the reverse.

As a risk or ethics and compliance professional, your role is to recognise where managers might be abusing their positions and where employees feel disengaged or angry. Abusive managers seldom stop at making lives miserable; they might feel empowered to take other liberties (here you find corruption, anti-competitive behaviours, discrimination, and harassment). Fed-up employees will often feel little loyalty to your cause. In these conditions, fraud (including petty theft) and conflicts of interest (especially side-hustles) sprout like mushrooms in a damp and dingy forest.

If my simplified prognosis sounds bleak, don't worry; knowing where to start your work is a gift. As one friend – then the compliance officer for Asia-Pacific for a healthcare company – put it, "I just want a system that tells me, 'This is what you need to work on today, start here', because there's so much I could do, it's overwhelming." Knowing where to start is a blessing.

Risk Assessments

I wouldn't call analysis of the tone at the top or the mood in the middle a risk assessment, as it's much more than that; it's a cultural roadmap to reach the consumers of your risk and compliance content. The analogy that makes sense to me is a culture MRI – helping us understand if there are any underlying (and not always visible) issues and where we're nice and healthy. The risk assessment is like the health check and lifestyle questions before the MRI.

Turning from this metaphor to your organisation, we start by considering the risk factors seemingly outside your control

(country and sector) before considering those we might have some agency over:

1. **Country risks** include the rule of law, the security situation, the government commitment to integrity, public sector corruption, attitudes towards business (and foreign investment), respect for human rights, geopolitical disputes, and freedoms (personal, media, and of association).
2. **Sector risks** overlap with country risks and may include industry-specific exposures (e.g., financial services to money laundering or manufacturing to modern slavery). Other stakeholders (including industry bodies, competitors, and regulators) will further impact your operations in areas including intellectual property protection, data privacy, and environmental protections.
3. **Operational risks** consider the day-to-day issues, including environmental and social impact, ease of doing business, security (cyber and physical), licensing and permitting.
4. **Routes to market risks** consider the extent to which you rely on public procurement, your customers' expectations (gifts, entertainment, offshore structures, donations, etc.), your reliance and use of intermediaries (agents, distributors, and alike), business partners, and funders.

These lists are far from exhaustive, but they get you started. We're mapping what you do, where you do it, how you do it, with whom, when, and why.

Listing all these stakeholders and interactions may seem onerous – and it's not easy – but you can get 80% of the way there in a couple

of hours of focused (group) work. If you need help, ask me. These initial hours invested will be invaluable as you build a right-sized program, matching your operational realities. If I go back to the MRI analogy, imagine trying to live a life where you protect yourself from all risks without considering how your environment, lifestyle, and genetics might impact your well-being.

I've used a whiteboard, or the fancier online and interactive tools, to facilitate this exercise by starting with those simple questions. Write a "Who you deal with" column and ask your colleagues to list all those stakeholders and interactions. Next, you can ask "Why?"; this is an excellent question as it should be easy to answer; for instance, we deal with this joint venture as it is mandatory in that country to have a local content partner. If it's harder to answer a *why*, dig deeper, some of these interactions may indicate legacy redundancies, but they can also suggest collusive, corrupt, or otherwise problematic dependencies.

When questions help us understand a few things, including dependence, leverage, and criticality. Do not assume infrequent means less critical – maybe you deal with the agency that licenses your products once a year, but you can't do business without their approval. "When" questions help us determine what interactions sit on our critical path and could derail operations if they go south.

What you do may seem self-explanatory, but it significantly impacts risk. If you hold reams of sensitive government data, you're likely of greater interest to hackers than if you are a garments wholesaler. But the wholesaler likely has more downstream risk exposure to human rights (including modern slavery) abuses in their supply base.

The way you phrase questions here will be essential. My experience – and I understand it's also the subject of many studies – suggests that we struggle with terminology. Many risk assessments are built on a matrix with probability/likelihood on one axis and impact/consequences on the other. Then you will see words like "almost certain" to "rare" and "severe" to "negligible". It will be no surprise that we get perplexed picking the correct ranking. The data you discover will also confuse you, as you'll wonder if people's perception of risk differs on a given issue or if their perception of word meaning differs.

A safer approach, always, is to use simple language. For example, "Demands for bribes are common during tenders", with a 5-point Likert sliding scale from "strongly disagree" to "strongly agree". If you get varied responses here, you know it's about the perception of the risk issue (which is a helpful indicator; are we too cautious or too cavalier about this risk?), not people struggling with terminology. I like numbers. Estimating in percentage terms avoids all linguistic subjectivity and is universally translatable. We also tend to be more accurate at the median numerical point. What about impact?

Impact is the Pandora's box of risk. Let's stay with the tender bribery risk to illustrate the challenge. What impact are we assessing? The impact of paying the bribe? The impact of paying the bribe and an employee raising this internally? The impact of the media uncovering your dodgy deal? What is the impact of a regulator finding out (if so, which one)? The impact of not paying the bribe and losing the bid? You get the point. Those questions lead to more, including investigative costs, fines, jail time, lost business, lost revenue, cancelled contracts, debarments, low

employee morale, business disruption, no client retention, etc. Many organisations try to quantify these risks in terms of lost revenue, remediation costs, share price, and other metrics. It's a bit like trying to estimate the impact of a fire in your home – it depends.

A better way to think of impact, for me at least, is to consider harm to people and the planet. For those integrity risks that may not be immediately evident, the next question should be, "Is the process impacted by the risk critical?" For example, if we establish a high(er) probability of bribe requests during tenders, ask if such tenders are essential to your business. If so, that's a high-risk event, and you'll need to plan ways to win work cleanly. Don't overcomplicate it; you will already have a good sense of impact from the when, why, and what questions; listen for words like "frequent", "critical path", "mandatory", "fundamental", "essential", etc. Low, medium, and high work perfectly well if you're trying to think of a scale to measure impact.

Test out your framework on unsuspecting friends and family. We manage risk daily (driving a car, personal security, swiping right, ordering late-night kebabs, asking elderly relatives about immigration), so pick an example and roll with it.

If you're considering external data sources, there are loads of resources ranking country and sector risks; they are a bellwether, at best. Trying to aggregate the perception of corruption, money laundering risk, or sustainability is like aggregating crime across a large country. Your exposure is impacted by where precisely in the country, your attractiveness as a target,

and your predictability. Do the bad guys know that you have excellent security and are not worth the hassle of hacking, or is your security framework implemented unevenly, with gaps vulnerable to exploitation?

Still confused? Don't worry. Risk assessment is the area – along with managing third parties – which baffles most people. Find me on LinkedIn; there are plenty more resources on my page, head to the Ethics Insight site for free risk assessment tools, or ask me a question.

These questions about your defences take us into the following assessment process, benchmarking your controls against the identified (potential) risks.

Benchmarking

Comparing yourself to others seldom ends well – we don't need to feel inferior or superior about our risk; we must feel cool-headed, with our eyes open, present, and paying attention. There is a lot of guidance – from those enforcing regulations – telling you what you should have in place. That's a good start, but it can be a bit overwhelming. Having done the hard work of assessing your internal culture and calibrating the external risk environment, now consider what you have in place to mitigate, manage, resist, or avoid those risks. If this is getting a bit technical, maybe Figure 2.1 will help.

We want to know your ability to prevent, detect, and respond to possible issues. Let's break that down.

Figure 2.1 Risk assessment workflow.

Prevent

Prevention is better than cure, they say. The trick here is to strike a balance between *having* and *doing*. Most organisations above a certain size will have policies, such as your website privacy policy. I'm more interested in what you do to make policies, frameworks, and rules jump from the screen into reality. Much of the remainder of this book will delve into specific risk issues, looking at how we can move stated intention into practical application. For now, though, look at your risk and compliance policies and procedures and ask a few questions, including:

1. Do we have any!?
2. Are they easy to access?

3. Are they easy to understand?
4. Do people refer to them?
5. Are they up to date?
6. Do we provide training on these topics?
7. Does this training involve testing (comprehension)?
8. Do we get feedback on our frameworks and continuously improve them?

This small sample of questions will get you started, but we would typically be more specific to make them more targeted and relevant. For instance, I like to include issue-specific questions – to understand how we address risk issues identified (in earlier steps) as appropriate to the organisation. For areas including corruption, sanctions, and human rights, it's imperative to assess the risk posed by people acting on our behalf. If you're using third parties, then you should include questions about any vendor (or equivalent) management processes, systems, and training you provide.

If you're stuck, head to our website – ethicsinsight.co – where we have various assessment tools.

Detect

Detection is straightforward – we want to know about your systems and processes to identify potential risk issues. What you do will have a significant impact here. For example, monitoring for potentially fraudulent (or otherwise suspicious) transactions should be part of the existing framework if you're a payments

platform. If you're wondering what else to consider, break it down into what I might call transactional monitoring, people data, and security systems.

Transactions include the obvious financial ones, but we're also interested in the flow of anything of value through your business (people, counterparties, products, raw materials, waste, etc.). Using the output from your risk assessment will sharpen your focus. For instance, if you manufacture items using metals, monitoring the origin (for human rights and conflict issues) will hopefully be coupled with proper disposal and scrapping (a typical hotspot of fraud and organised criminal activity).

Do you know what your people think, feel, and do? That may seem strange, but if you're not capturing data from your colleagues – including where they perceive risk – you're driving your risk program without a map. You will likely already have employee surveys, exit interview processes, and appraisal data, but are you doing anything with that? If people are leaving a particular team, that might merit closer inspection. Conversely, if you never hear a peep from another department, is that a sign that all is okay, or are people fearful of speaking up? We will unpack speak up and monitoring in more detail, but please monitor whatever channels you use to listen to your people.

Information and physical security will invariably involve monitoring. Check if this extends beyond those two areas to include other possible risk issues. For example, do you conduct audits focused on these risk issues and monitor employee links with third parties? I am not suggesting Orwellian surveillance, but a data analytics query looking at employee and supplier bank

accounts and address detail may uncover duplicates, meriting further scrutiny. It is a balance, but you have a right to some level of transparent and fair surveillance in your organisational home.

Respond

Response is not simply how you deal with potential violations; it's how you continue to operate, learn lessons, and improve. Yes, we want to know if you have an investigations framework, speak-up channels, and non-retaliation provisions. But we also want to know about business continuity and crisis management. If you're thinking, "What the hell is that?" don't worry. It's your Plan B. For example, if you suffer a data breach, where is data backed up and stored? How do you continue to operate? Or, how might you respond if you found a fraud involving your largest supplier (do you have a back-up)?

When you identify an issue, that is often just the start. Going back to our MRI analogy, you now know you must conduct further tests, including establishing the spread or impact on other organisational functions.

To benchmark your response framework, ask the following questions:

1. How do people raise concerns?
2. What is our investigative capacity?
3. How do we keep operating and minimise disruption?
4. How do we deal with uncooperative or hostile stakeholders?

If that last question sounds concerning, it's a reality. If you get hacked, don't count on large IT providers to prioritise helping you. Don't expect the police to bend over backwards to support you if you uncover a fraud. Suppose you receive a corrupt demand in a country where the rule of law cannot be relied on. Good luck getting the local authorities to investigate. These are all worst-case situations; hopefully, none will come to pass. You will need to be ready to continue operating without much support, so check if and how you can do that.

Getting the right blend of prevention (education and support) and detection (monitoring) may seem daunting, but it isn't once you have a right-sized framework to test *doing,* not just *having*. It will also help you work out what needs improving (hopefully) ahead of an issue.

Speaking Up, Non-Retaliation, and Consequences of Violations

Organisations with an effective speak-up culture typically detect issues more quickly, reducing financial, human, and operational costs. Having a speak-up framework is one of the simplest and most effective risk-reduction tools you can employ. To demonstrate the point, I built a speak-up channel on a surveying platform in an afternoon and confirmed that you do not need a 24/7 multilingual call centre to get started.

The Association of Certified Fraud Examiners' (ACFE) *Report to the Nations* includes detailed information, suggesting that median losses from fraud were typically doubled in organisations without hotlines. The average detection time was 12 months with and

18 months without a hotline.[2] The term hotline is a broad catchall for mechanisms whereby employees (and other stakeholders) can raise concerns (often anonymously).

If you're considering developing a speak-up framework, please check local regulations as they may include provisions on preserving anonymity, preventing retaliation, and statutory reporting requirements for certain offences. Once you're clear on what you must do, you may have a few decisions, including those summarised in Table 2.1.

Your next decision will determine who is covered by the reporting framework. Full-time employees, but what about contractors, temporary workers, business partners, third parties, customers, the local community, and whomever else might be impacted by your activities? The answer to this question will inform the choice of channel and tools. I would advocate for the more, the merrier – some estimates suggest up to half of the *tips* about wrongdoing emanate from outside your organisation.

Before communicating the reporting framework, anticipate one of the first questions, "What should we report?" Many reporting lines are misused, usually more misinformed than malicious. You will still get some "My boss is a douchebag" and "I didn't get the promotion I deserve" messages; that's pretty normal. It can help to have some sort of classification framework. You may not wish to publicise the entirety to all stakeholders, but it will help in subsequent phases, including investigations. A common catchall is "workplace misconduct", but I'm not a fan of that, as it's not immediately apparent to me (or most employees) what

Table 2.1 Questions to ask when you build a reporting framework

Question	Positive considerations	Possible downsides
Should we allow anonymous reports?	If people can report anonymously, you will get more reports and a potentially more accurate risk picture	Few reports include sufficient detail at the start, so having a mechanism to follow up with the reporter helps You will also have to filter out disgruntled or malicious allegations, increasing your workload
Which platform is best?	You know your organisation; choose the platform(s) that people use most. Ideally, provide options	Simple is best. It will be less effective if you have too many options or require too many steps for someone to make a report
In-house or outsourced?	Consider the capacity and resources you have. Can you respond to reports promptly internally? Do you have people manning the reporting channel 24/7 (allegations seldom happen at 9 a.m. on a Monday)?	Outsourced can sometimes mean requests to download apps or generate logins. Make sure the provider focuses on user experience. Consider how well you need and want the provider to know your business; do you need them just to record and pass on, or do some sort of analysis and triage?

constitutes misconduct (or why it needs to happen in a workplace to merit reporting)!

Your Code will help you identify the issues you encourage people to report. Be intentional, purposeful, and clear about the scope of the reporting framework; it will save a lot of time in the long run.

Once you're ready to socialise the reporting line, look at what else has worked. How do you communicate product or service updates (internally and externally)? Have you been through any particularly effective change programs or job-specific training? It is always easier to piggyback on initiatives that have worked rather than reinvent the wheel. As a tip, keep visuals simple. You will want a clear call to action (what, where, and how to report).

Test the reporting line periodically, ask people for feedback (and test knowledge during training and surveys), and monitor usage. Dig deeper if you see anomalies (e.g., two proximate departments with very different average reporting data). The reporting framework is not the sole or most reliable indicator of organisational health but can be a tremendous top-line indicator of high-risk areas within the organisation.

Investigations: What Do People Need to Know?

A robust speak-up culture is fundamental whether you use a speak-up line or not. Encouraging the lovely and intelligent people you work with to bring their best selves is a no-brainer. If you want your people to innovate, create, and make, you must allow them to um, err, and stumble. Earlier, we discussed questions to better calibrate the mood in the middle, including safety making mistakes, asking for help, and accountability. These areas are critical in a speak-up culture, distinct from call-out culture.

Publicly castigating others for perceived or actual violations is seldom constructive. Speak-up culture is different; it's more objective and grounded in the shared values, codes, and rules you collectively (as an organisation) agree to respect. For that to work, people need to trust your investigations framework. We must, therefore, work backwards to create a functioning and healthy culture where we can raise issues safely.

Let's start at the end of an investigation, where you decide what to do and to whom. Was the allegation proven accurate? Who is guilty, and to what extent (primary or accessory)? What is a fitting punishment? If you get this wrong, you lose trust, and people will stop speaking up. Let's use a case example.

Employees in a small manufacturer in a fast-growing emerging market (with a weak rule of law) are terrified of the boss. This leader has little appetite for opposition to her power. If anyone dares challenge her authority, she will invite them into her office and make various lurid threats (sometimes involving family and often with the pistol she keeps in her desk drawer, for emphasis). A brave soul has had enough and contacts the global head office one day. Guns and threats to family require sudden flapping and busy responses (with little forethought). A team of investigators flies in, but the boss knows they're coming (it's her factory, and no visitors get past without her approval). At the factory, the overseas team discover laptops wiped, sparkling and empty desks (free of sidearms), and serried ranks of cowed employees with little to say. Miraculously, and with some help, the investigative team find enough evidence to confirm the allegations. But the boss is also a director, and a significant local shareholder in the venture, with political connections that may thwart any attempted ouster.

For those of you tut-tutting that this wouldn't happen in your country (with a supposed strict rule of law), you're wrong. Baddies frequently get away with it. Sometimes on a technicality, sometimes investigative screw-up, in other cases, because they have leverage.

What's the moral of the story here? No one in your organisation can or should be irreplaceable if you have solid values and a healthy speak-up culture. In practice, this can be hugely challenging. The briefest glance at various Silicon Valley start-up scandals indicates that a powerful cabal (usually controlling most of the shares) at the top can spread toxicity throughout. Simply removing a majority shareholder is not simple at all! Still, it doesn't mean you shouldn't try just because it's hard.

What your stakeholders want from an investigative process is simple: trust. They want assurances that they will be protected and not subjected to retaliation if they speak up. Stakeholders want to feel the process is fair and transparent. I've seen many firms trip over that last bit, fearful about how much transparency is necessary. My view, as much as possible. Why? Three reasons; people talk, and if you think you can keep an investigation secret in this age of leaks and social media, you're in the minority. Get ahead of the story before it becomes the usual blend of stinky half-truths that squelch out of firmly clasped corporate cheeks. The second reason, you're robbing everyone of your best material. Failure is a much more faithful teacher than success; investigations must become case studies, training material, and honest discussions. Yes, we need to balance shame and disclosure, so for sensitive interpersonal issues (especially harassment and bullying), always seek consent and

err on the side of less is more. But stories resonate for problems you will encounter again – unethical demands from external stakeholders to misuse of assets and property. I have trained thousands of people and always asked what was most helpful. The case studies within that organisation (sector or group) are the clear winner; a story paints hundreds of words of methodology and theory.

The third reason? Trust. By sharing (suitably shame-filtered) updates with your stakeholders, you trust them to handle the truth. Much like, as parents, we are told to discuss our failings and mistakes with our kids – including apologising – this trust removes some of the "them and us" piety in hierarchies.

So, what do employees need to know about the mechanics of your investigations? Not much. They don't need to know the intricacies of chains of custody (unless it's their belongings) or forensic imaging (unless it interrupts IT coverage). What stakeholders will want to know is:

1. Is it fair (justice for all)?
2. Will it be thorough (many investigations are not)?
3. Is it transparent?
4. Will you protect me if I come forward?
5. What do you need from and expect of me?

Communicate your position, and remember to avoid the dreaded *zero tolerance*. Explain that you will do your best, and then do it. Some investigations are inconclusive, especially when it is one

person's word against another's. Your stakeholders will be unhappy in these cases, but they will respect the effort if you communicate transparently, deal fairly, and protect all those involved.

Investigations: How to (Not) Do Them

All those involved include the accused. The first mistake, especially in the social media age, is to forget the concept of innocent until proven otherwise. Everyone has the right to a fair trial and restorative justice (wherever possible). The second thing that happens when an allegation is made, or issue uncovered, is to assume that binge-watching crime drama transforms you into an (effective) detective by osmosis.

I was called to a meeting by an engineering firm in Singapore. They were involved in building infrastructure and would rotate hundreds of engineers in and out of the island. The company asked the head of Facilities Management to organise the serviced apartments for this conveyor belt of project workers. Some time later, the client identified payment anomalies in the invoices for these apartments; inflated payments, transfers during periods of no occupancy, duplicate invoices, etc. The facilities manager had his fingers in the till, with real estate agents in cahoots. The head of HR leapt into furious action.

She called the manager in for a meeting, seized his personal phone, recorded the session, and told him he'd brought shame to his family and, as the eldest, "Who will care for your parents now you're going to jail?" Shortly after leaving the meeting, the manager headed home, grabbed a hastily stuffed bag and fled the country.

Well, that went well. I wish this were an extreme example, but it isn't. Here's what your average person knows about investigations (Figure 2.2).

Seizing private property was not enough for our budding Jack Bauer; the HR manager proceeded to head to a dodgy phone shop and had the device jailbroken so she could read the messages.

Do not take private property and access personal data illegally; aside from the inadmissibility issue, breaking the law is generally not a sound investigative tactic. Don't record without checking it is legal and requiring the appropriate consent. Even then, ask, "Why are we recording? Does this further the cause and help

Figure 2.2 What most people know about investigations.

us secure our objective?" Recording can contaminate interviews (people's behaviour changes when recorded).

Avoid the temptation to shame. Your role as an interviewer (not interrogator) is to build rapport. When we feel empathy from the other person and connection, that might help us unburden our guilt. Guilt is directed at the act, and shame is directed at the self. Most people clam up when shamed. Even the most heinous offences may necessitate rapport and words like, "It was a mistake many others in your situation might have made." And, please, do not go in for the kill without a follow-up plan. What do you intend to do if you find guilt? Disciplinary action, dismissal, report them to the authorities? Understanding the objective will help plan when, how, and where to organise an interview.

Mind the Gaps

While I am confident you're not using the lousy cop, worse cop tactics, some of the less egregious pitfalls can still trip us up. A proper investigation could be (and is) the subject of many books in their entirety. I have much ground to cover and limited space. The first step is to step back. Don't get caught turning assumptions into *facts* and missing simple truths. Ask first, what do you *know* has happened? That might be a concise list, "Someone made an allegation that our CEO is misleading investors." Then list the assumptions and determine how you might test them. I like to use a *value* and *effort* matrix. Let's start with effort (or complexity), which is a constituent of:

1. **Context:** Local legal, political, and cultural dynamics (e.g., an allegation involving an influential stakeholder is more complex than one about a non-critical supplier).

2. **Access:** Can we obtain information? Can we speak to the reporter? Are those involved internal or external?
3. **Understanding:** Is this a familiar topic (e.g., theft of IT equipment vs ransomware from unknown threat actors)?
4. **Trust:** Do we have the reporter's trust? Can we consider their credibility (sadly, some allegations will be malicious)?
5. **Control:** If we find wrongdoing, can we do something about it (links to context, relationship dynamics, and leverage)?

It's not that you should discount assumptions if they're hard to prove. It's more about prioritising quick wins. Back in the mid-2000s, I was in China. At that time, most foreign firms needed a local partner. Occasionally that partner would steal the intellectual property and set up a parallel (counterfeit, close imitation) business. One of our clients feared this was the case. Determining ownership (on paper) of a nearby factory and gaining access to verify if they were (as suspected) producing rip-off products would have been challenging. Instead, we asked a potential client to call the factory and arrange a meeting. The client's business partner greeted our asset, handed over a business card, and explained he was the owner of the competing factory; assumption no more. There are usually a few ways to test a hypothesis.

What about the value? Taking a business card to the Chinese courts wouldn't have helped, especially without evidence that their business partner had handed it over and confirmed he owned the factory. This evidence had little value from a legal perspective. However, our client did not need that as they had

little faith in the local legal system and wanted time to line up a replacement partner before terminating the relationship. The goal was to prove the suspicion with minimal fuss and limited risk of detection (snooping around records and factories is high risk). Therefore, in this case, the value and effort blend worked. In other cases, the value and effort thresholds can be much higher.

Consider what level of evidence you require to prove or disprove the allegation. If in doubt, get legal advice. Legal privilege and counsel are essential in some investigative situations, especially where you have to report regulatory infractions.

What Is Evidence?

Maybe it might help to place evidence on a scale, from the least robust to the more easily provable. We can't be exhaustive here, but let's focus on the evidence you'll most likely encounter.

First is anecdotal evidence, which cannot (typically) be used in court. Anecdotes are stories, and even if widely held, the danger is relying on *evidence* that may be hearsay, rumour, or confirmation bias. The saying, "No smoke without fire", fails to qualify that some tiny fires can create acrid and toxic smoke. Anecdotal evidence's best friend is character testimony. We now move from stories to what people feel about each other. Statements about someone's character can help if you're trying to understand the pressures people are under (that often precipitate ethical lapses) but be careful to sift out rumour, grudges, bias, and conspiracy.

Circumstantial evidence will be familiar to most, but let's ensure we're on the same page. Direct evidence is a witness confirming they saw John access the storeroom at 7 a.m. when we know that items were stolen from that location at precisely that time. Circumstantial evidence is a witness saying they saw John near the storeroom at 6.50 a.m. It's smokier and fierier than anecdotal but still treat it with the same rigour as when moving assumption to a fact.

Physical, material, or demonstrative evidence is what it says. For instance, CCTV recordings show John entering the stockroom at 7 a.m. Digital evidence might record John's biometric thumbprint entering the stockroom at 7 a.m. Digital evidence is frequently the organisational investigator's best friend – emails, messages, files, data, transactions, and anything else you can extract from digital devices. The overlap between physical and digital often occurs during the collection of publicly available data. For example, if you access corporate filings to show that John holds a competing business selling the same products as those stolen from your stockroom. Accessing that data may be digital, but the file may be a scan of a physically signed document (sometimes termed documentary evidence).

Don't worry about the differences; the critical point is to ensure that you appropriately record, preserve, account for, and record any movements (physical or electronic) of evidence. Deleting digital evidence is also (often) easier, so be careful there too. Do your research around the chain of custody considerations.

Digital evidence bleeds into forensics – specifically, and unsurprisingly, digital forensics! Other types of forensic evidence

(fingerprints, blood, ballistics, and like) are rare in your common or garden variety of organisational investigation.

Phew! Let's assume you've gathered the evidence you might reasonably be required to. What now!?

Before You Start

When starting an investigation, resist the temptation to jump in. By now, you've hopefully got a clear idea about the objective and the limitations of data and evidence retrieval (for most of us). Let's instead focus on how you'll talk to people.

I know you've watched the TV shows and cannot wait to bust out your steely cop stare. No judgement. We've all been there. Maybe you even have a bright lamp and spent the day before yelling to rock classics, just so your voice has the right amount of rasp and gravitas. You get in early, set up the room with the jug of water and paper cups – you know that's a prop cops use when they need a dramatic pause in proceedings. The first suspect arrives. They ask you if you've got a cold and why there's an unplugged lamp on the conference room table (the cord didn't reach, did it?). Slightly rattled, you head for the dramatic pause water station and pour it on your crotch. Well, that didn't go as planned.

We get ahead of ourselves sometimes, and investigations get most people excitable. That's why we need PEACE. I'm not yelling; PEACE is an acronym for a model developed in the UK to reduce false confessions stemming from more aggressive interviewing techniques. PEACE is perfect for organisations where a

non-confrontational conversation management process is always preferable. The five stages are:

P = planning and preparation
E = engage and explain
A = account
C = clarification and challenge
E = evaluation and closure.

Planning and Preparation

Fail to prepare, prepare to fail. When planning, ensure you've reviewed the case, the interviewees (suspects and witnesses), points to clarify or prove, the objective, and the evidence you have (and need). Now it's time to strategise. Some of the variables to consider might include the interview(s) location, recording protocols, interviewers' roles, and other considerations (e.g., translations, technology). We will also need to prepare both physically and mentally. Think about the presentation of materials – will you share evidence, and in what order? Check your own biases, get focused, calm, and ready to pay attention. Being fully present during an interview is draining, and there are plenty of distractions. I like breathing exercises beforehand to get centred and ready to pay deliberate attention. If I'm doing an in-person interview, I also like to have a few things in my investigator's grab bag (Figure 2.3).

Engage and Explain

Once the interview starts, that also has a timbre and tempo. Introduce the process – who is involved, housekeeping, timing, and like.

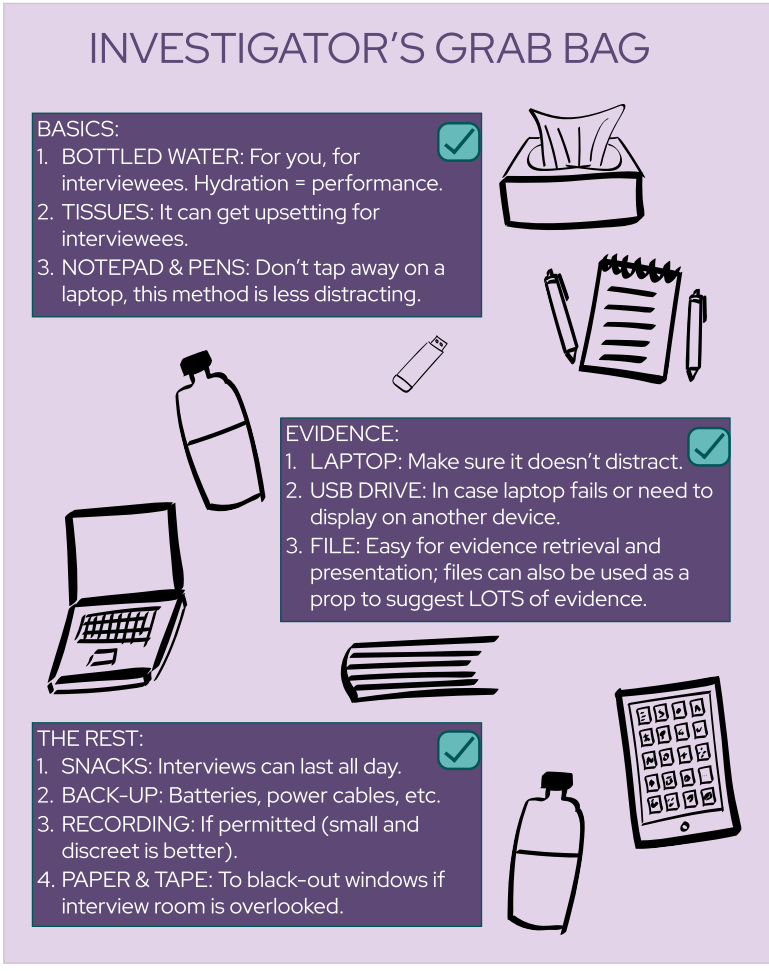

Figure 2.3 Contents of an investigator's grab bag.

Explain the purpose of the interviewee and who will be doing what. While you're doing this, observe the interviewee and establish their baseline. Now, the baseline may be tricky from the start, as few people walk into an investigation with a skip in their step. But your role is to try and put them at ease. Baseline is how we usually interact with others, mainly when dealing with questions

or topics that aren't emotionally charged – name, job role, small talk. You want to use background details that aren't core to the event or issue to continue this calibration and rapport-building.

Check regularly to confirm the interviewee understands those ground rules. For example, "if anything is unclear, please ask", "don't leave anything out, but it is okay to forget". This process is good practice and allows you to check how the interviewee responds in the affirmative and negative.

Be honest to the extent you can. Yes, you may need to keep a few things up your sleeve, and you may need to use some deceptive lines of questioning. But, on the general purpose of the interviewee and the parameters, be honest. For example, don't make bad choices seem like a choice. You may antagonise the interviewee. If the guilty party likely faces some form of sanction – disciplinary, criminal, or something else – don't claim you can give them options when all roads lead to punishment.

The Account

Do you know someone who interrupts you frequently before explaining your points? How does that feel? Yeah, pretty crappy. Don't be that person.

Let the interviewee speak freely – sometimes called free recall. They may need some context to get started. Usually, it helps to take their memory to where you want them to start. Ask them to recall everything. Sometimes we filter out what we feel is irrelevant, but it may be salient for your investigation. Additionally, it's another behavioural cue.

Generally, true accounts are a bit messy. We jump around in timelines, correct ourselves, include superfluous details, describe interactions, and if you tried to draw the narrative, it would look like a spider on psychoactive substances. However, it is typically a linear progression when we manufacture a lie – like a straight train track. Lies often lack the details.

Your role as the interviewee gives their account is simple: listen and observe. Yes, one of you may be taking notes, but learn to do that while looking at the interviewee. You don't want to be glued to your notepad and missing crucial details. Please don't type unless it's a video call and you've muted your mic; it's frickin' distracting!

Once you have the first iteration of the account, ask the interviewee to expand on areas of interest. Use phrases like, "Could you go over the . . . again?" You are trying to gather a more fulsome picture, but this is also your chance to see if any non-verbal (or verbal) slips you spotted in round one occur again. Summarise to the interviewee to confirm you understand correctly and see how they react (sometimes we don't realise what we let slip). Let them correct, qualify, or emphasise topics you may not have understood. The simplest way to do this is reflecting and paraphrasing language – a potent tool to get people to open up, but you need to mirror the good bits!

Clarification and Challenge

There are no stupid questions, so the saying goes. There are, in fact, plenty of stupid questions. A brief tour of the YouTube rabbit hole confirms this. But, in an investigative setting, the only

stupid questions demonstrate you didn't listen or prepare. That's why reflecting is so important – it encourages listening and creates rapport. Now is your chance to probe and clarify before closing the interview. Beware, however, that our memories like to fill in blanks, which can often be unhelpful in an interview setting.

During postgraduate studies in behavioural analysis and investigative interviewing, they asked for volunteers for a memory experiment. I put my hand up and soon had a blindfold and earphones as instructors led us around a conference venue and subjected us to disorientation, stress, and sensory overload tactics. The trainers warned us that the experience might not be pleasant. Our handlers bumped us around, screamed, and ran past us before shoving us into a room where they played bizarre sequences of sounds and music. The soundtrack was less whale song and spa muzak, more grenades and voodoo chants. The instructors handed us objects (still blindfolded) and gave us a few seconds to decipher what they were.

The purpose of this experiment was twofold – other students were able to quiz us (testing their interviewing skills), and we would compare recollections. It was sobering. Even data points as simple as the duration of sensory assault varied from 25 minutes to hours. The facilitators asked us to draw the route on a map; I was elated to get this bit right. I'd received training about counting steps and turns (right/left) in case of kidnap or detention. But that cognitive processing had seriously impacted other recollections. I thought a motorcycle air filter was a nasty 1970s lamp. A group of people, all primed and prepared for a mildly traumatic simulation, studying memory and behavioural analysis, were shockingly unreliable witnesses!

Were we an anomaly? No, our brain fills in the gaps, we assume, make logic leaps, and are not very good at remembering sequences or timelines. So many investigations rely on timelines, details, and descriptions. How should you manage this challenge? Gently take the interviewee back to the periods in their account that you need to clarify (for further details or inconsistencies). Ask them to set the scene, give them time, and jog their memory with any (non-revealing) evidence you might have. Be very careful if the event might be traumatic.

Don't just rely on a discussion. You can also ask people to demonstrate or illustrate if it clarifies the point (acknowledging some limits on remote communication). For example, ask the interviewee to draw or use items to mark where people and objects were. Think laterally; your role is to facilitate the interviewee's communication. Now is the time for empathy and rapport – yes, even if you think what the interviewee might have done is repulsive. You need to tap into their feelings, not their logical brain (busy filling in gaps). Why? Because we remember feelings better. Furthermore, we're much worse at faking feelings than we think – just recall the last present you gave someone that bombed!

If I asked you to recall a time when you (nearly) had a serious accident, would you accurately recount timelines, colours, and objects? Or would you remember sensations and feelings? Our emotions are (usually) a better vehicle to get us back to the location (and the truth).

We are sprinting through a topic that is more maze than a memo. Please don't rush to close and make sure you focus on the facts when summarising (not assumptions or sentiment). Closing is

critical if recording the interview or gathering a written statement. Stick to the facts!

Once you close, explain to the interviewee what happens next (to the extent possible). Direct them to further support, especially in cases where a witness or victim (may have) experienced trauma.

Misbehaviour Analysis

"You missed a bit", the razor-brained among you might now be thinking. You glossed over clarifying inconsistencies. Yes, because it deserves its mini-section, although I could (and would love to write a whole book on this alone).

I am a behavioural analyst – I went back to study mid-way through my career as I recognised the importance of non-verbal cues and different investigative interviewing techniques. Teaching you about reading non-verbal cues is not for now, but questions or elements of an account that cause a deviation from a person's baseline are worth summarising. We must consider:

1. **The context:** Is the interviewee a suspect? Has the interviewee (possibly) suffered trauma? Are they speaking up against someone powerful? We must consider any contextual factor that might impact their emotional state.
2. **Consistency:** Are the emotional cues consistent with the story? Be careful here of *me theory*, where we think about how we might respond in each situation. The consistency we're looking for is a congruence between the substance of the account and the emotions conveyed. For example, if someone is saying how disgusted they were that anyone would steal

while smirking, that is interesting, and we might need to probe further.

3. **Baseline deviation:** We all have a natural way of communicating. Some of us are demonstrative and speak with our hands and body. Others are more monotone and reserved. Yes, the context can alter this baseline, but it's our job to calibrate the interviewee's *typical* behaviour and look for deviation from that. We do this with the standard questions you'd expect at the beginning of an interview (name, the purpose of the meeting, what their role encompasses, etc.). These introductions (and small talk, if appropriate) allow us to see how the interviewee responds to questions without a significant stake. A noticeable deviation might be a calm and collected type suddenly fidgeting, shifting in their seat, or seeming distracted and flustered.

4. **Spontaneity:** Is the account spontaneous and the responses similarly so? Don't confuse this with speed. Some of us might ponder questions and take our time making our points (our baseline), but we should still be coherent and spontaneous. A lack of spontaneity could be a fluent, confident, loud, and animated natural communicator suddenly stumbling, stuttering, going quiet, and repeating simple questions (to buy time to think of a reply).

5. **Cognition:** You know that moment when you ask a question and can almost see the other person's brain whirring, thinking? That's cognition, and we'd expect to see cognitive load (the amount of information the working memory can hold) if we're asking difficult questions. However, if you're asking simple questions (often recounting a supposedly lived

experience), that should not cause a significant burden on our working memory. We're looking for: (a) have we confused the person with any of our questions?; and (b) why they might need lots of brain processing power to ask this question. If there's no apparent reason, maybe brainpower is being deployed to fabricate a lie?

In other words, there is no one universal indicator of deception (or truth). Still, if we see significant changes in behaviour in particular parts of an account, that merits more examination. We're not concerned by one or two flickers. Deceptive indicators come in clusters across multiple channels in a short space of time.

What channels and what are the behavioural cues we're hoping to elicit? There are six:

1. **Face:** In particular, micro-expressions, and I strongly suggest you look into the work of Dr Paul Ekman[3] to learn more and practise your ability to spot them. I love micro-expressions and am forever indebted to my mentor Cliff Lansley and the team at The Emotional Intelligence Academy[4] in the UK, who took me under their wing and trained me to spot them. Micros are fantastic because they are impossible to fake (they occur in a fraction of a second), giving clues to our underlying and subconscious emotional state. They are universal (all humans, and some primates, exhibit micros). Micros occur across seven emotions – surprise, fear, anger, disgust, contempt, sadness, and happiness – and for an interviewer, they help you build rapport, be sensitive to the emotional stage of interviewees, and spot dissonance between what is

said and what the face tells us. Study them; it will be time well spent for every facet of your life.

2. **Body language:** Most written about, yet least universally reliable (so far). Much body language is culturally specific, for example, the head shake or nod. We're looking for inconsistency, a lack of spontaneity, body language occurring outside our presenting area (our upper torso and face), and deviations from baseline. Much is written about eyes looking this way or that and liars holding your gaze, but it's more about variation. For example, one of my kids usually is very animated, and their head bobs around as they speak, but when they're lying, the body is statue-like, and they fix you with a steely (hopefully convincing) stare!

3. **Pitch, tone, and volume:** Our voice also betrays our emotions. You will have heard phrases like "a curt tone" or "a depressed tone", which you'll associate with an emotional state. Watch to see how the music of our voice sings a different song. For example, does the pitch go down and quieten during sad elements of a story?

4. **Interaction style:** How does what the person says flow? Are they evasive or unclear? Do you feel like they're trying to manage your impression of them? Again, we all have our preferences and natural styles – and they will alter depending on the topic, our ego, and the context. Remember that a true story is lived and relayed as such. A lie is a fabrication which can impact clarity, flow, and impression.

5. **Verbal content:** Does what they say match the other behavioural cues and the context? Truthful accounts often resemble a plate of spaghetti. We jump around in the story, relate

elements that are not core, describe interactions between people, and self-correct, but there is a natural flow. Deceptive accounts are often linear – departing from point A and getting to point B quickly. In a truthful statement, you can ask us to jump back into the story wherever you like, and it's a lived experience, so we can. When we're asked to recount a fabrication, you might start to hear verbal slips (e.g., the wrong verb tense), stalling, and a drop in spontaneity and coherence. Watch out for distancing language – if it's something with negative implications (and we did it), we often want to put distance between us and the act or subject.

6. **Psychophysiology:** No, not the name of an experimental late-90s British electronic music band. Sweating, blushing, increased heart rate, hairs standing on end, and increased temperatures in legs (flight) or arms (fight) can all indicate changes in emotional states. However, it will be hard to detect with certainty in your average interview. So let's leave this one here unless you want to geek out – in which case, get in touch, and I can point you to some supercool research in this area, including evidence that most people in airports are angry (makes sense, right?!).

To elicit any of these behavioural clues, we must have good questions. There are many schools of thought on this topic. However, if it helps, I prefer to think of questions like a funnel. You start wide at the top, where the funnel is broadest, then narrow down as you need specificity and clarity. Something like this:

1. Tell me more about. . .
2. Take me back. . .

3. Walk me through. . .
4. Could you outline. . .?
5. Can you clarify. . .?
6. If I understood correctly. . .
7. What did you mean by. . .?
8. How. . . [explanation about the circumstances in which something occurred]?
9. What. . . [to get specificity about an occurrence, detail, or fact]?
10. Where. . .?
11. When. . .?
12. Why. . . [often accusatory and requires an opinion, justification, or explanation]?

You may wish to use tricky questions to try and catch someone if you think they're being deceitful, but be careful. Use these questions sparingly and only if you have a secure grounding (e.g., evidence the interviewee does not know you have). For example, a mind virus question is where you suggest you have information the interviewee does not know about. A mind virus question might start, "So there's no reason that someone saw you at that location?" Now the virus starts in their head, "What else do they know?"

Another common tricky question is a presumptive question, where you assume something and hope that exaggerating will prompt the interviewee to counter with a more reasonable confession. For instance, "We know you stole from petty cash on at

least five occasions . . ." Here, you hope the person will confess to their lesser crime.

Be careful, if you're dealing with someone smart, they'll see you coming, and you'll have lost all the rapport and trust. I'd only use tricky questions if you have substantial evidence and are willing to have your bluff called.

The best advice I can give you to succeed in investigations is to use your ears and mouth in the ratio they were given to you. We all face that urge to jump in with that fascinating question, challenge or insight, but it's not about us. Our job as investigators is to gather data. It's hard to receive when you're on transmit.

Evaluate

Evaluating the interview is crucial. There is a tendency to rush or even overlook this stage. Sometimes, there is a bit of a cringe factor, especially if we must listen (or worse, watch) our performance. Have you ever heard a recording of your voice and said, "Oh, no, that's not how I sound, is it?" It's like that, but worse, because you'll inevitably realise you could've, would've, should've, asked better questions, or . . . shut up more! Just remember two things, no one cares as much as you do, and however badly it went, it will still be better than the "improv" my 15-year-old self put on at a school parents' day. As I typed that, my ears went red, my mouth pursed, and I inhaled sharply while groaning. No excuses then for not evaluating performance.

We're trying to understand what went well, how the roles worked, which interview objectives we met, and what needs improvement

(including any corrective actions required). Self-critique first before seeking input from any co-interviewer (we're usually much meaner to ourselves; unless your co-interviewer is Dutch).

Once you've finished the self-flagellation – or putting your shoulder out patting yourself on the back – get back to the case! Review the information obtained (did you get what you needed?). Did you miss anything? If you receive further evidence, what will you do with it? Are there new avenues of enquiry?

I remember one particularly woeful internal investigation. High-value items (smartphones mainly) were disappearing at an alarming rate from a major online retailer's facility. The elite investigative team had spent the first week staring at the top of people's heads. They'd found CCTV footage, then assumed that the thefts occurred during packing for dispatch. The only problem with this foolproof assumption – assume, usually makes an ass of u and me – was that all packers wore disposable white caps and face masks. Team Clouseau had whittled down the suspect list from everybody who worked in packing to everybody who had a white hat or came near the packing station. Genius. It was revelatory when we elected to speak to a human (an oft-forgotten art in the era of screening pointless data). Each item has a code, and the code is scanned as the objects pass through the facility (arrival, quality control, storage, sorting, packing, dispatch). Each employee rotates through different parts of the plant, usually requiring swipe access to various locations and logins on the scanners. At this stage, data became useful, as we could look to see where coded items were dropping off the internal ether and who was on shift at those times. A pattern and small suspect list quickly emerged. Gathering evidence changes investigations.

Speaking to people – when you're prepared – changes investigations. Just make sure you properly evaluate and coordinate the next steps.

Learning from Failure

The excellent week-long hairnet CCTV staring meditation fiasco is a great lesson. You will fail in investigations. They are unforgiving as we deal with those pesky and unpredictable things: humans. Assuming the failure wasn't catastrophic (and it rarely is), see it for the lesson it is.

I told you about your ears and mouth ratio, and now I'll share the other great tip I received from a seasoned interviewer and investigator. Have hypotheses, as many as possible. I recently worked on an insurance claim – I know you're on the edge of your seat at the mention of the world's sexiest topic. A person had reportedly committed suicide in the States. The deceased's body had remained undiscovered for three months (until a welfare call from the building owner after neighbours complained of the stench). A registered firearm lay next to the body and an unregistered ammunition casing. Shortly after their death, a gentleman purporting to be a relative put in a claim for a huge life insurance policy, which had been upped by millions of dollars in the previous years, with no named beneficiary. The policy was issued in a country halfway around the world, and the relative was in a different country. What might have happened here? The possibilities and hypotheses are many. Who died? Was that their policy? Is the relative genuine? Why was there no-named beneficiary despite repeatedly upping the policy's value by $1 million? What was the relationship if they were a relative (given the body

lay undisturbed for months)? Why buy a registered weapon and then seek illicit ammo? That's just for starters.

It's easy to make assumptions and leap to conclusions. But that's not our job. Our job is to seek the truth, discover the facts, and consider all the possibilities. Then, when we fail, to learn and come back better.

Endnotes

1. Cohen, P.A., Kulik, J.A., and Kulik, C.-L.C. Educational Outcomes of Tutoring: A Meta-analysis of Findings. *American Educational Research Journal*, 19(2) (1982): 237–248. doi:10.3102/00028312019002237.
2. https://www.acfe.com/rttn-archive.aspx
3. https://www.paulekman.com/
4. https://www.eiagroup.com/

INDEX

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.