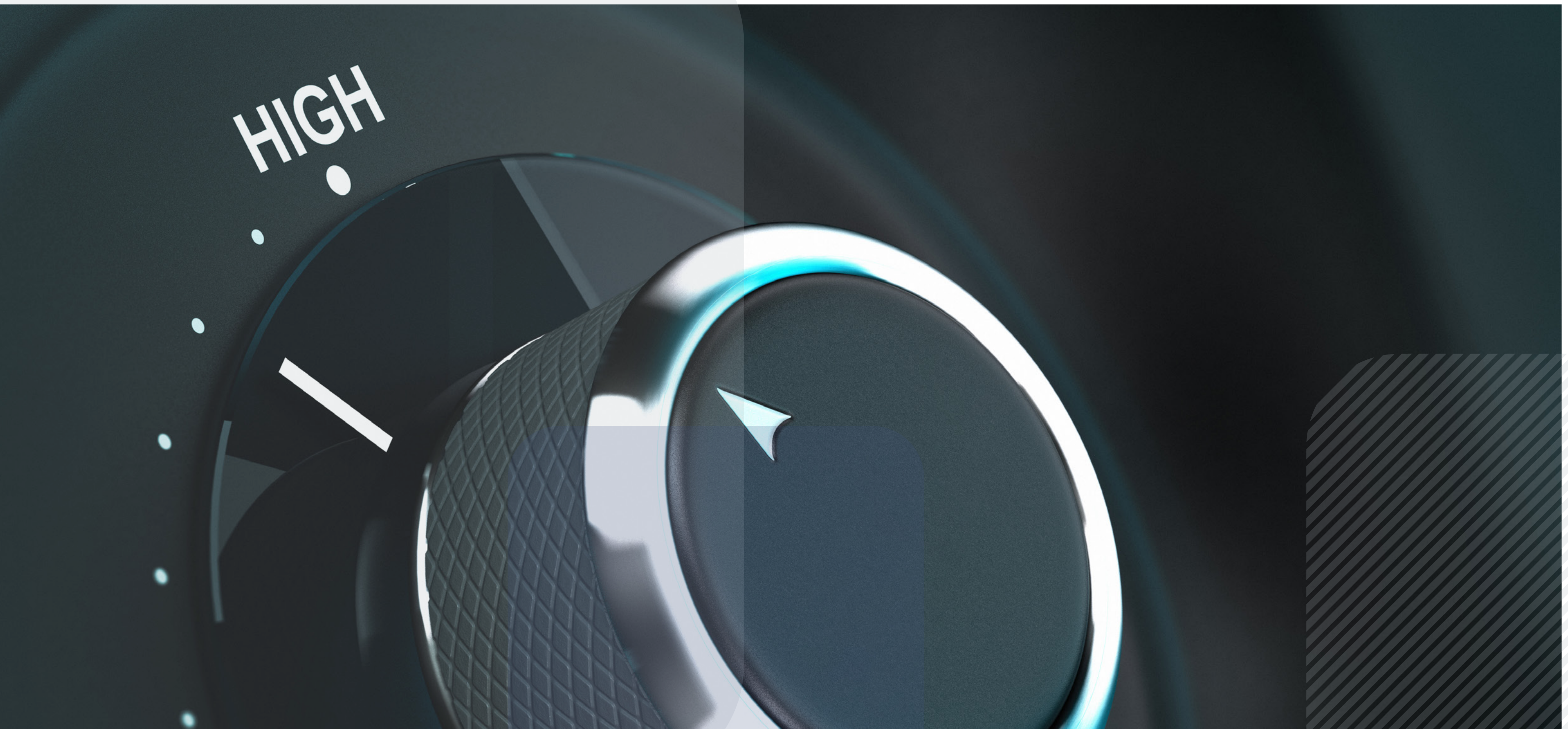
vault.

MANAGING RISK & DETECTION



Managing Risk and Detection

Risk is a fundamental element of any organisation's day-to-day operation. Risk can never be entirely eliminated - and, in fact, without risk businesses would never thrive.

But detecting and managing risk should be key priorities for any business leader. Risk comes in many forms, and affects every function of an organisation, from finance to compliance to HR.

Employee misconduct is just one factor that can cause problems for an organisation, and for its people. But it is also one of the most prominent types of risk that should be mitigated - and the implications for organisations that do not do so can be very significant.

CONTENTS

Misconduct is bad for business, but more importantly, it's bad for people. And, from corporate to behavioural misconduct, the risks have never been greater. One of the highest-profile examples of this can be seen at Uber, which is reported to have lost in excess of $10 billion as a result of the now-public sexual misconduct scandal that shook the organisation.

Elsewhere, 21st Century Fox paid out $135 million in legal settlements for workplace misconduct in just one year. And it's not just interpersonal behaviour that costs businesses - it's also corporate and operational infractions. Volkswagen, for example, recently lost over $25 billion as a result of unreported supply chain fraud, while Toshiba lost $6 billion thanks to unreported accounting mispractice.

Cultural changes are also increasing the importance of risk management, particularly in relation to employee misconduct. Employees are demanding changes within their workplace in new and concerted ways, and corporate exposure has never been higher. Even away from the headlines, the costs of ignoring workplace misconduct are severe: 46% of those experiencing workplace harassment will quit their job as a result, while companies with the highest incidences of sexual misconduct underperform US stock markets by an average of 19.9%.

01.

Understanding Risk Profiles

Every organisation has its own unique risk profile and, as such, there is no such thing as a ‘catch-all’ risk management strategy. The risks facing an organisation will depend on a huge variety of factors, including geographic location, regulatory environment, employee headcount, the nature of the business being carried out, partnerships and suppliers, and more.

In addition, the world of work is undergoing a dramatic upheaval, catalysed in great part by the pandemic. New developments such as the explosion in remote working, as well as new communication methods such as Slack and their concomitant behavioural changes, mean that businesses around the world now operate in fundamentally different ways - and this is the case for organisations of every size. The ‘future of work’ already looks radically different to what’s gone before, and this has important knock-on effects for every business’s risk management strategies.

It’s also crucial to understand the enormous shifts brought about by social movements such as #MeToo. There is a greater understanding of the importance of workplace safety today than perhaps at any time in history, and employees, customers, and lawmakers all now quite legitimately demand that employers do more to ensure a safe, supportive, and compliant working environment.

Strategic Risk

Finally, strategic risks are those that are accepted and taken in order to achieve a greater strategic goal. Strategic risks and their impacts should still be mitigated, and this can be achieved through tools such as the Key Risk Indicator (KRI) model. As with preventable and external risks, strategic risk management requires the development of a full suite of mitigation processes, and the resources necessary to build and run them.

02.

Categorising Risk

As we've seen, each organisation's risk profile is unique. However, we can broadly assign different risks to one of three categories:

Preventable Risk

This describes risks that arise from within an organisation, and that have no associated strategic benefits. Preventable risks can be managed through monitoring, control, and compliance processes, and the theoretical aim is to eliminate them when it is practicable and cost-effective to do so. For the risk-management function, preventable risk involves the development of a comprehensive Ethics and Compliance culture, along with the establishment of controls and audits.

External Risk

External risks are those that arise from outside the organisation, and that cannot be prevented. However, they can generally be mitigated, and are tackled through impact reduction. The risk-management function within an organisation responds to or prepares for external risk through scenario planning and, of course, risk assessment. 'Stress testing' is also important when preparing for external risk.

03.

Risk Management Strategies

There are three elements to a comprehensive risk management strategy. These different strands of action are all crucial when dealing with organisational risk

Identifying Risk

In order to manage risk, you first need to know what you're looking for. Identifying potential risk should be a fundamental part of any business planning activity, and should remain front and centre as an organisation grows. Risk identification should happen early and often - that is, it should be baked into planning and strategy, and should be treated as an ongoing process, not a one-time exercise. It should be performed regularly, and the schedule of its performance should be fully codified. Additional risks should also be identified and evaluated at key points in a business journey, or when material circumstances change.

It's also important that risk identification is not treated as a 'top-down' exercise. With the best will in the world, senior business leadership will not have a comprehensive understanding of the day-to-day operational risks their organisation faces. Risk identification needs to happen in partnership with rank-and-file employees, guided by management. Similarly, the practice should be incorporated into everyday project planning, with risk management a fundamental element of any team or employee's activity.

Evaluating Risk

Once risks have been identified, they need to be evaluated. There is a range of different risk evaluation frameworks, and each of these may work more or less effectively in individual organisations. For example, the CARVER framework, borrowed from World War II military planning, aims to help organisations assess the criticality of threats or risks to specific assets. There are many other such frameworks, each of which has its own specific focuses and practices. Many organisations use 'risk event cards' to help stakeholders understand the implications of individual identified risks. Risk event cards set out the nature of the risk event, and the strategic goal that it relates to. They will detail the potential outcomes of a risk event, and the likelihood of such an event occurring. Often, likelihood and consequence are mapped on a graph showing their relative severity. Crucially, risk event cards also set out the management controls associated with the risk, and the manager accountable for their implementation.

Prioritising Risk

Once risks have been identified and evaluated, they must also be prioritised. In the evaluation stage, management should establish the relative severity and likelihood of individual risk events, and their potential outcomes. These assessments will provide a structure by which prioritisation can take place. Risk prioritisation should take place at every level of an organisation. Top-level strategic risks are only part of the picture - and, in fact, they may well not be the risks that have the biggest potential impact. Teams should be given the power to and responsibility for prioritising risk on a project or departmental level, while the overall risk-management function within the organisation should ensure that managers are given the resources and training required to do so.

04.

Improving Detection

First, as we explored earlier, it's important to understand that the nature of work is changing. Businesses are increasingly digital-first, from the services they provide right through to the way their people interact. This digital transformation has important implications for risk detection, especially in the new remote working paradigm.

With fewer (or no) employees in a physical office, detection and reporting procedures must change. For an organisation to successfully respond to misbehaviour and misconduct, it must first be aware that such events are occurring. In the battle for detection, employees and partners are the most important weapon in a business's arsenal. People must be empowered to speak up, and they must have confidence that their reports will be taken seriously.

There are three key ways in which this process can be supported. The first is through culture. The importance of corporate culture is now widely understood, but all too often it remains a tick-box exercise that amounts to little more than the establishment of nebulous 'values'. In fact, in order to be sustainable, organisations must focus on developing a culture of compliance that percolates throughout its entire structure, with accountability at every level. Employees are more likely to speak up when they are confident that misconduct is not tolerated. In contrast, when minor rule-breaking or a culture of turning a blind eye are taken for granted, reporting and disclosure is stifled.

This can be disastrous for any organisation - as we saw earlier with Uber, Toshiba, and others.

The second way in which organisations can aid detection is through the full integration of the risk management function at every level of the organisation. This is, clearly, closely connected with company culture, and it requires leaders to understand risk management as an important and ongoing business process. MORE

Finally, the third form of support for detection comes from the efficient use of technology. In a digital-first world, carefully considered technological solutions are absolutely crucial for detection efforts. Even today, many organisations still rely on 'hotline'-type reporting solutions. But these are cumbersome, limited in scope, and chronically underused by employees. Indeed, according to, only 25% of corporate misconduct is reported at all. Technology-enabled reporting solutions such as Vault Platform can dramatically increase this figure.

05.

Modern Detection Systems

So what does a modern misconduct detection system look like?

First, efficient misconduct systems will focus on delivering simple, intuitive, low-impact reporting processes. Vault Platform, for example, uses advanced, mobile-first technology, combined with a people-first understanding of the realities of workplace relations, to provide safe and reliable routes through which employees can speak up. The innovative GoTogether function, for example, enables employees to report misconduct as part of a group, with the feeling of 'strength in numbers' encouraging higher reporting rates. Modern misconduct platforms also provide bulletproof protection for whistleblowers, giving organisations the tools they require in order to comply with whistleblowing and reporting regulations such as the EU Whistleblower Protection Directive or the FCA's reporting rules.

But detection alone isn't enough. Modern platforms such as Vault provide an integrated reporting and resolution system geared towards the modern workforce. As well as providing employees with the tools they need to speak up, Vault is built around a suite of tools that enable leaders to respond to misconduct and reduce its frequency. This often begins with the creation and dissemination of codes of conduct and associated policies. In the past, codes of conduct have all too frequently been treated as another box-tick, distributed to employees as part of the onboarding process and never touched again.

By contrast, modern misconduct platforms allow leaders to create living, breathing policy portfolios that are accessible to employees in intuitive, digital-first ways. They also provide tools to ensure those policies are deeply integrated within employees' day-to-day working lives, and that performance and behaviour can be measured against them.

Once reports have been made, the case management stage begins. Here, Vault Platform creates a simple and direct line of communication between the case manager and the employee or employees making the report - even in cases where the report is made anonymously. Managers are then empowered to close the loop on reports, demonstrating to the reporting party and to the organisation at large that remedial action is being taken. By taking a digital-first approach, organisations can reduce friction between employees and case managers. Ease of reporting, along with the transparency gains delivered by platforms such as Vault, have been shown to increase reporting rates by 19%.

05.

Prevention is better than cure

Clearly, in an ideal world there would be no misconduct to report. In reality, it is impossible to eliminate misconduct, especially across large organisations. However, the priority for any risk-management function should be the reduction of misconduct to the lowest level possible.

Robust detection and resolution practices are an absolutely fundamental element of this effort. The provision of simple reporting tools, along with comprehensive and transparent resolution and remedial action programs, help to foster the all-important culture of compliance. The more actively and visibly an organisation deals with misconduct, the more empowered its people will feel to speak up. In this way, a virtuous circle is developed.

Visibility of key ethics, compliance, and behaviour data is also crucial. Vault Platform provides leaders with extremely granular information, including 'heat map' reporting to enable the identification of patterns of behaviour within specific departments or functions. It also encourages the location of 'blind spots' within organisations, helping managers to be proactive in combating misconduct.

Looking Forward

Finally, it bears repeating that risk management and misconduct detection and resolution are not one-time exercises. These are living business processes that require constant input and constant revision. The importance of this process-driven approach is underscored by the speed with which the regulatory landscape is evolving. Organisations must be agile in their response to new regulatory obligations, and misconduct and risk management are at the forefront of this.

In order to be successful, risk management and detection must be both reactive and proactive. Misconduct, along with any other risk event, should be dealt with quickly and transparently - at the same time as leaders take action to prepare for changing regulatory obligations and the fundamental shifts brought about by the new world of work.