Deloitte.

The Misconduct Resilient Organisation

The Misconduct Resilient Organisation

The Association of Certified Fraud Examiners estimates that financial crime – including bribery, corruption, misappropriation of assets, tax evasion, and cyber-crime – costs organisations five percent or more of their revenues per annum. That amounts to roughly €15 billion in the Netherlands alone, so besides reputational losses, there is significant value to be recovered by managing the risk of fraud and misconduct.[1]

1 Association of Certified Fraud Examiners, ACFE's 2016 Global Fraud Study, Report to the Nations on Occupational Fraud and Abuse (2016)

The Internal Control Paradox

Many organisations protect themselves against misconduct by way of their internal control frameworks. This approach focuses on prevention, for example, policies and procedures, training and due diligence. Financial crimes are detected in various ways (e.g., hotline reports, internal and external audit activities, and other forms of monitoring).

In 2016, fraud was two times more likely to be detected by a whistle-blower than internal audit activities.[2]

Layer upon layer of internal controls have been compounded by new regulations from national governments, the European Commission and the OECD which impose additional compliance burdens on organisations and increase internal bureaucracy. When an incident is identified, the typical response is to understand what has gone wrong and implement more controls to mitigate the newly identified risks one by one.

Herewith creating an inextricable web of rules, procedures and audits. The results are threefold. First, employees are finding it more difficult to conduct their work, due to the complexity of the process, mistakes occur more frequently. Second, the more creative employees are finding ways to circumvent the web because detection decreases as the layers of the web grow.

Finally, more rules, procedures and audits have a negative impact on the rationalization of employees. The web indicates that the organisation is full of unethical employees. This may push a law-abiding employee over the tipping point to become a fraudulent employee.

The approach of prevent, detect and respond, has its limitations in terms of cost and effectiveness. The question arises whether 100% prevention is possible. An organisation will assume that the existence of controls absolves them of the need to be alert to the risk of misconduct. A smart and more balanced approach will make the organisation more resilient and better equipped to protect itself against misconduct. A new approach is imperative.

2 Association of Certified Fraud Examiners, ACFE's 2016 Global Fraud Study, Report to the Nations on Occupational Fraud and Abuse (2016)

The Future of Financial Crime

Recognising this administrative burden and the cost thereof, and that the existing approach of responding to control failures with more controls is limited in its effectiveness, there is an increasing urgency to adopt a different approach. The legislative pressures, the hyper-connected world we live in and the focus on reputation, requires companies to change the way they manage the risk of fraud and misconduct. To understand these new requirements, one should understand the future of fraud:

New technologies

provides opportunities and results in new fraud schemes. Technology also allows outsiders, like hackers and criminal organisations, to realise financial gain or disrupt organisations.

Modern financial systems

combined with hyper-connectivity change the nature of financial transactions. Financial transactions will increase in volume while the average value will decrease.

Financial crime fraud schemes

will increasingly become facilitated through collusion with people inside the organisation to circumvent the internal control environment. Internal fraudsters, on the other hand, will also **seek to cooperate** with other third parties to circumvent internal controls.

Reputational risk

will be heightened and accelerated due to regulatory requirements, public pressure, and the connectivity between organisations.

Regulation is driving individual accountability

for corporate wrongdoing forcing management and those charged with governance to provide all relevant facts about individuals involved in corporate misconduct. Therefore, analytical procedures, as well as investigative procedures, need to be defined to determine this information.

The Response: the Misconduct Resilient Organisation

As the prevalence of technology is increasing; the risks of fraud and misconduct to organisations is increasing, by placing powerful tools in the hands of potential fraudsters. However, technology also allows organisations to take action in advance to reduce the threat of misconduct and its impact on the business. With advances in technology, efforts can switch from preventative controls, which are limited in their effectiveness, to real-time monitoring and (pro) active intervention. By creating misconduct awareness capabilities and methodologies to rapidly respond to risk events, organisations are better equipped to manage the risk of fraud and misconduct.

We refer to these organisations as Misconduct Resilient Organisations (MRO).

MROs use this insight supported by technology to become vigilant to risks and breaches, and become resilient when they occur. To create a Misconduct Resilient Organisation companies must also rethink policies and procedures that cater to the needs of the business process instead of trying to change employees into ‘paralegals’. Employees can then focus on daily business instead of continuously taking into account the legal consequences of their actions.

The Response: the Misconduct Resilient Organisation

Vigilance is a combination of systems, processes and cultures which allows organisations to detect misconduct before it has affected the business and to respond timely to limit the impact. But this is only effective if an organisation looks at the right data and applies analyses to detect patterns and possible fraudulent behaviour. Vigilance involves being on constant alert, focusing on behaviours and the digital footprint of potential wrongdoers and acting before any misconduct can occur.

In addition to the regular observations, it is possible to use pattern recognition and advanced analytics to predict or identify unusual activity. The outcomes are combined with other signals to create insights into fraud schemes. Ideally these fraud schemes are shared across industries to increase fraud prediction capabilities.

Initially, organisations may engage an external provider to help them run analytics on their data, but as soon as possible – given the need for constant vigilance – the solutions need to be embedded into the organisations own systems, processes and cultures, and such solutions need to flex over time. As organisations adopt the tools and techniques required to be vigilant, they also need to build and maintain the response capabilities, otherwise they will lack the ability to address the problems that arise.

For example, while people understand what a bribe is they don't necessarily understand, or have the ability to understand, its journey through the organisation's processes and financial systems. Bribes can occur in many forms and emerge from various places within the organisation. Furthermore, bribe schemes evolve over time and in their nature are usually hidden within the organisation's (financial) systems. Ongoing monitoring is essential which means embedding tools within the organisation's systems in such a way that they can be rapidly flexed to recognise that organisations change and new identifiers may emerge.

When investigating misconduct the starting point has often been to look at documents as the first source of evidence before examining financial systems, but with the power of analytics this can be reversed.

The Response: the Misconduct Resilient Organisation

Predictive analytics can be used to analyse large volumes of transactions in real time to identify behaviours that may be characteristics of fraud. This is possible because of the volume of data available from multiple sources (e.g., e-mails, invoices, contracts, payments, chronology of payments, destination of funds, amounts charged to expenses, and evidence (or lack of it) that goods or services have been received in respect of payments made).

To take advantage of analytics for vigilance, the organisation needs a set of examples or fraud scenarios to feed into the algorithm. This set is used in an iterative learning cycle to remove false positives and false negatives. Whilst third party providers can run analyses on the organisation's data, it is better if the tooling is built into their own systems so that monitoring can be ongoing.

Within the context of data privacy and security regulations, organisations need to rethink how they can work with the data they hold, looking across systems and databases. Approaches should be designed to avoid burdening the non-fraudulent with more controls. By combining data from different sources it is possible to build a clearer and more sophisticated picture that allows for better risk assessment – as the Dutch Tax Authority puts it, "Everyone gets the level of attention they deserve."

The Response: the Misconduct Resilient Organisation

Resilience: MROs accept that in our highly regulated and connected world, compliance breaches and misconduct will happen. Therefore, they need to be resilient which involves fixing breaches when they occur, communicating quickly and convincingly with their stakeholders and constantly learning from experiences. Speed and effectiveness are the key measures of resilience.

To become resilient, organisations need to understand their data and build response capabilities.

This involves hypothesising various scenarios (including preparedness for black swan risks) and then identifying what data is needed in order to identify that a scenario is imminent or in progress. This drives the solutions implemented for the purpose of vigilance. For each likely scenario the organisation should establish a standard operating procedure which dictates who, what and when to engage – this will include those responsible for minimizing the effect of the breach and those responsible for communication and any other components of crisis management.

For effective resilience a person or team needs the mandate to immediately implement a rigorous response proportional to the effect of the incident. Without this when a breach occurs, the organisation can quickly lose control of the incident.

It is important for those with the mandate to deal with breaches to scenarios, plan, and ‘war game’ so that the response is both planned and agreed and so that all those involved understand their roles and responsibilities. Having this framework allows the MRO to deal with an incident proactively in contrast to the organisations which opt for crisis management – an invariably reactive approach.

What's Stopping Organisations from Becoming a Misconduct Resilient Organisation?

In our experience there are a variety of barriers organisations face as they embark on the journey to becoming a MRO including:

Natural resistance to change
A misguided faith in the effectiveness of preventive controls (the inextricable web) or fear of setting the organisation free (reducing the preventive controls to the minimum necessary).

Cost vs. reward
This can be complicated especially when the impact of misconduct is felt in one part of a business, but the cost of rectifying it lies elsewhere.

Data quality
Data privacy and security regulations which limit the ability to access personal data or data in databases sitting in different parts of the business.

Technology lock in
Insistence on quality rather than accepting mistakes and learning from them.

None of these barriers are insurmountable, indeed some of the characteristics of the future of fraud may help organisations to overcome them.

It seems unlikely that those charged with governance will allow cost considerations to take precedence when competing against their individual accountability and exposure to prosecution.

It is certainly the case that privacy and security need to be taken into account, by encouraging internal departments to work together to determine what is possible within the boundaries of the regulations can enable organisations to remain compliant and become misconduct resilient.

Issues of data quality abound and whilst it would be wrong to trivialise the value of high quality data, in many cases data quality as a reason for not adopting the technology solutions, which are a key component of vigilance, is little more than prevarication. In others it arises from a misunderstanding that without high quality data analytics is impossible. Or that the volume of data under the organisations control is so extensive it is impossible to know where to start.

In reality, no organisation has perfect data quality or has tried to implement vigilance solutions across the whole organisation in one go. For those who have embarked on the MRO journey, pragmatism prevails. Like start-ups, they start small and evolve: vigilance solutions are susceptible to the "minimal viable product" model.

The biggest challenge however is changing the organisation's culture.

The Paradigm Shift

Moving from prevent, detect, and respond to vigilance and resilience requires a cultural change. From the top down the organisation has to accept and make sure their employees understand that:

- They are all responsible for vigilance;
- They should speak up if they observe patterns of behaviour that suggest misconduct; and
- They should apply professional scepticism rather than assuming that the control framework or someone else is alert so they don't need to be.

The paradigm shift starts with the notion that all transactions are basically truthful and only a small percentage are dishonest. Mechanisms must be put in place to find (only) these exceptions.

There is an uncomfortable message for "Theory X" command and control managers in this, because they have to give up their article of faith that no one can be trusted which underpins the call for a tightly controlled organisation. MROs recognise the limitations of "prevention" as a head office function and seek to decentralise responsibility throughout the organisation. This requires trust in those to whom control is ceded.

This change might also involve difficult adaptation where the culture has previously been one in which people assume that the control framework absolves them from the need to be alert, ignoring the obvious and repeatedly demonstrated truth that there is always a way around controls so they are only as strong (or weak) as the people responsible for applying them. To make this change managers need to overcome their perception that implementing preventive controls is seductively easy and it is easy to train people in applying them. Training and key performance indicators are more difficult in an MRO because it requires an intangible change of mind-set rather than a documented new set of routines.

Taking a Step Back…

To achieve the cultural change that is fundamental to a MRO, it helps to understand what we mean by organisation and misconduct.

An organisation is a combination of individuals who have come together for a common purpose. Without a common purpose there is no organisation. With a common purpose, it is possible to define misconduct. Left to their own devices, these individuals may set about achieving the organisation's objectives in a variety of ways ranging from the ineffective to the undesirable. Just as societies – themselves organisations – codify standards of acceptable behaviour, businesses implement policies and frameworks that draw the line between what is appropriate and misconduct.

Organisations operate at two levels – external and internal. The external rules are designed to protect the organisation from the risk of non-compliance with the laws and regulations of the jurisdictions in which they operate, such as the forthcoming General Data Protection Regulation. While internal rules elaborate policies and standards of behaviour designed to achieve the organisation's purpose, which is the definition from an organisational perspective of who we are and what we do.

Misconduct takes a variety of forms:

Internal – where an employee is not compliant with the organisation's policies or the obligations it is under by law or regulation.

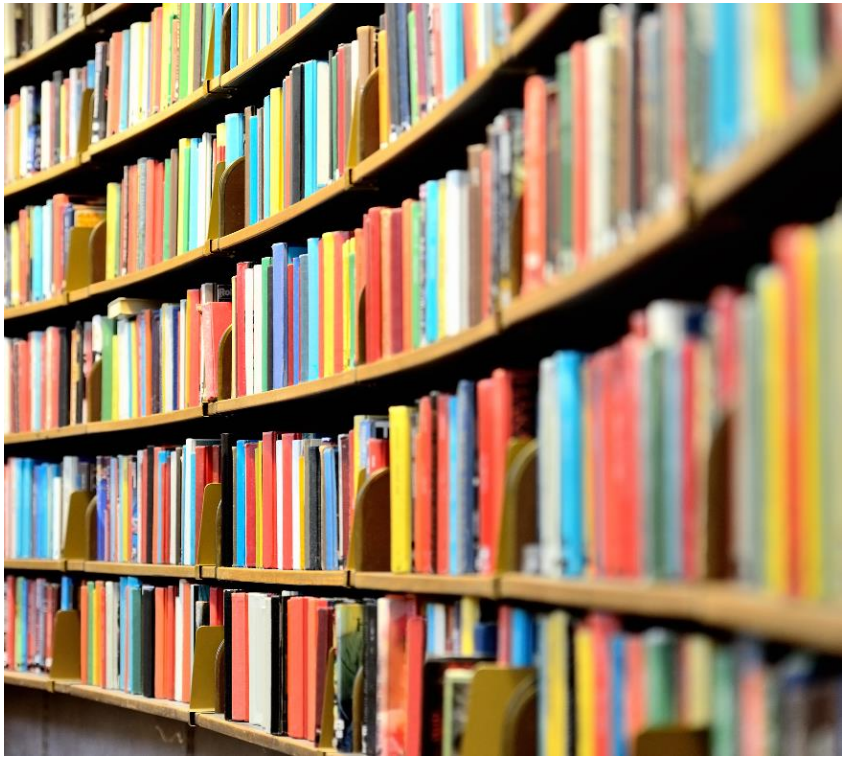
- Consumers – those clients who misuse financial processes and (lack of) controls for personal gain.
- Third parties – business relations using interconnected systems and or processes.
- Unknowns – those who have no direct relation with the organisation beyond the desire to harm it, using existing vulnerabilities with either employees, consumers or third parties for illicit gains.

With these multiple threats, the organisation needs to protect itself with barriers and boundaries to be legally compliant without disrupting the business. There needs to be policies and well-articulated general expectations so that employees, customers and third parties act in a way that is aligned with all other stakeholders.

Taking a Step Back…

The actions of third parties and consumers are ensconced by legal protections. Organisations need to be alert to the risk and take resilient actions by way of contract termination or legal action.

Despite the impression given by lurid news stories such as the recent DDoS attack on internet service provider Dyn and the experience of Tesco Bank's 9,000 customers, threats from these "Unknowns" are uncommon (compared to frauds committed by individuals alone or in collusion) and not the most difficult to counter. Organisations can prepare themselves for disruptive actions using approaches such as ethical hacks which allow them to identify gaps in their protective skin and protect themselves by fixing them. However, this does require organisations to be proactive. It is too late to be vigilant after the event when the opportunities for being resilient are already weakened. So in addition to proactive use of ethical hacks organisations should have stringent procedures to help prevent disruption from outsiders. This means being aware of potential problems and the preventive measures that need to be taken to minimise them. This allows the organisation to withstand and respond to blows in a robust way rather than "falling over."



Taking a Step Back…

Far more insidious is the threat posed by people within the organisation which is more difficult to tackle because the sort of protections that can be deployed against external threats are not available within “the wall.” This is why trusting everyone in the organisation and sharing the responsibility to be vigilant is so important.

The integrity of an organisation and its behaviour is not the sum of the individual members, employees or citizens. It is secured through buy-in to shared objectives, the common purpose, and the organisation’s “why”. Unfortunately, both internal and external pressures can undermine the why with a focus on what and how. Without the guiding principle of the common purpose, people within the organisation can succumb to pressure by cutting corners. Sooner or later, a line is crossed and this can have a profound, even existential impact on the organisation.

If this responsibility is not communicated properly or the environment in which it operates is misunderstood, there is a risk that everyone within the organisation will distrust each other.

This can be overcome with another component of trust, namely full transparency: there is nothing to spy on if everything is out in the open. To take an everyday example, compliance with corporate expenses is traditionally addressed through a series of controls, checks and balances. If every employee’s expense claims were available to everyone else in the organisation, peer pressure would achieve more than controls ever could, and allow a real time response – a hallmark of a resilient organisation – to deal with wrongdoing.

Such transparency can extend beyond the organisation. As regulations continue to increase they bring with them reputational risk to the organisation and individual liability for breaches, MROs are accepting the importance of opening a dialogue with regulators. In the tax arena, Dutch corporates who provide the Tax Authorities with analytics-based insights into their operations beyond what is required for compliance purposes are minimising their exposure to tax audit and the loss of time and expense that involves.

Meet Our Team

Would you like to know more on Misconduct Resilient Organisations or the other services we have to offer? Please do not hesitate to contact one of us directly:

Laura Klapwijk
Senior Manager
Deloitte Risk Advisory
+31882886049
lklapwijk@Deloitte.nl

Frank Cederhout
Manager
Deloitte Risk Advisory
+31882887283
fcederhout@Deloitte.nl

Deloitte.