January 2023

Restoring trust through enhanced fraud risk management

www.pwc.nl

Fraud and economic crime are on the rise, with new working practices arising out of the pandemic, market and supply chain disruption and global instability, all increasing the motivation, rationalisation and opportunity to commit fraud resulting in significant damage for organisations and society.

Despite this, fraud risk management at organisations is not getting the attention it deserves, with many organisations not dedicating enough resources to fraud risk assessment, governance and effective fraud prevention and detection controls.

For financial years ending on or after 15 December 2022, auditors in the Netherlands are required to explicitly report on fraud in their auditor's report. Not in general terms but specifically concerning the identified fraud risks and the work performed by the auditor on these fraud risks and, potentially, the results of the work. This reporting requirement is one of the measures implemented to create more transparency and improve the results of the auditor's work around fraud. We note that an organisation's steps to prevent and detect fraud should be the starting point for the auditor's work on fraud.

We believe that a robust fraud risk management framework is critical to an organisation's overall risk management structure and the success of its business. Drawing on our experience of advising organisations in the area of fraud risk management, as well as helping to investigate and respond to actual and alleged fraud incidents, we can offer a view of what a good fraud risk management framework would look like and how it could contribute to increasing the trust your stakeholders have in your organisation.

In this paper, we not only provide our views on what the key elements are of a fraud risk management framework, we also outline a number of practical considerations to help organisations consider fraud risks and what evidence would be useful to support their framework.

Why enhanced fraud risk management is important

- Trust and confidence in business is critical in creating a flourishing business environment. Robust fraud risk management is crucial in protecting value, detecting possible issues and enabling trust in businesses.
- Capital markets require trust and transparency to operate effectively. Corporate conduct and reporting that robustly counters fraud and financial crime are crucial in building trust.
- Financial fraud is on the increase and the pandemic has served to accelerate the rise. Our 2022 PwC Global Economic Survey shows a pandemic-related increase: 70% of those encountering fraud experienced new incidents of fraud as a result of disruption caused by COVID-19.
- Enhanced fraud risk management is an opportunity to rethink and refresh an organisation's approach in performing a fraud risk assessment and implementing a more formal internal controls regime. This way, improving the prevention and detection of fraud.

Contents

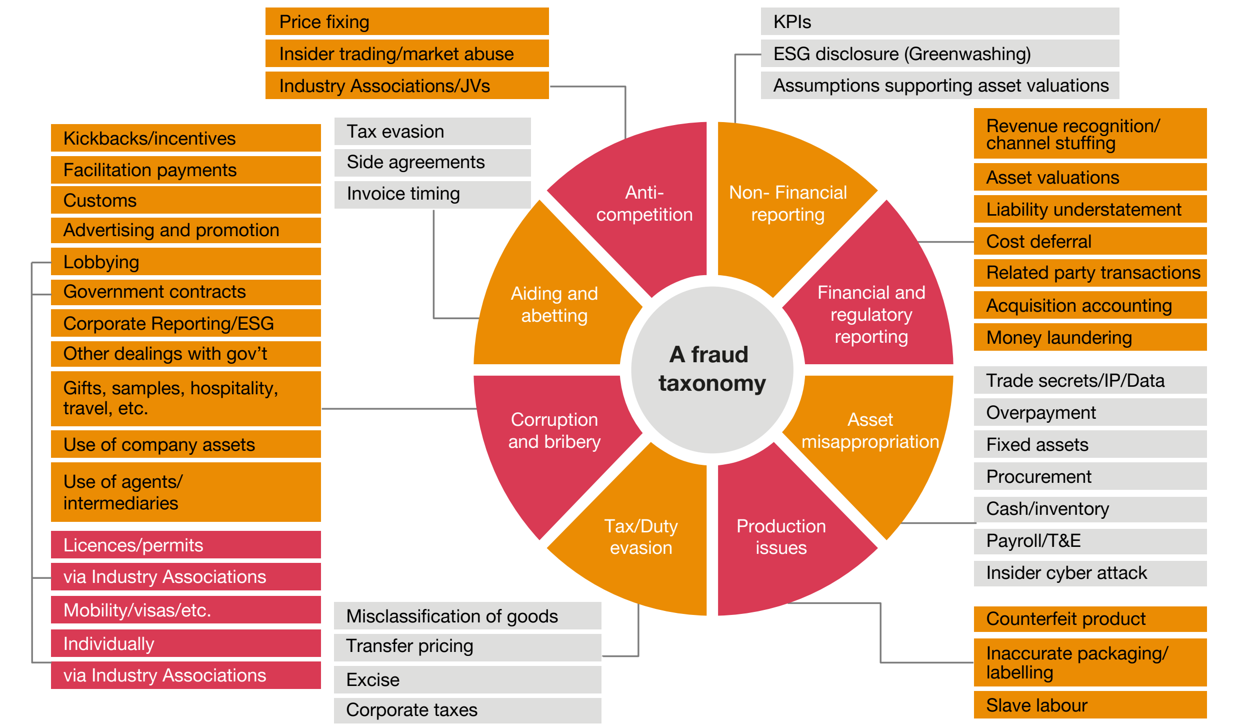
1. What does fraud mean to you?

In establishing and maintaining an effective fraud risk management framework, it will be necessary to first determine what fraud means to you and your organisation. There is no single, global definition of fraud. Per ISA 240.11 definition "Fraud is an intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage".

Legal definitions can vary by territory, and therefore consideration should be given to what other definitions there could be in group structures and whether there are any significant differences to the definition used in the fraud risk management framework and whether these differences are required to be reflected within the risk management policies.

There is also a wide range of activities that could be classified as fraud. Here is an example, although not exhaustive, of a number of possible fraud types which an organisation might need to consider depending upon their individual structure, industry and business.

The organisation's fraud risk management framework should be designed to consider all fraud risks, whether or not the impact could be material. However, in order to ensure the process is focussed on the most significant fraud risks, it will be important to determine what constitutes a material fraud for your organisation, considering both the financial definition of materiality in the financial statements and also which qualitative factors (e.g. internal perpetrators such as management and other employees and/or external perpetrators such as agents and suppliers) or non-financial factors (e.g. media exposure, brand or reputational damage etc) may be material to stakeholders and the organisation.



2. Key elements of a fraud risk management framework

With careful design and implementation, a robust fraud risk management framework (the ‘framework’) could have a powerful impact on understanding and reducing the risk of fraud.

We believe the COSO principles, which are designed to help organisations understand the key elements needed for an effective internal control framework, are a good basis for a fraud risk management framework as these help with understanding and improving the processes and controls in place to prevent and detect fraud. At the core of any fraud risk management framework is a robust fraud risk assessment. In our observation, less than half of the organisations have such a fraud risk assessment in place. In addition, whilst many organisations have considered in detail specific Bribery & Corruption fraud risks, the identification and assessment of the broader fraud risks relevant to the organisation are not being documented beyond a generic ‘fraud’ risk in their enterprise risk assessments.

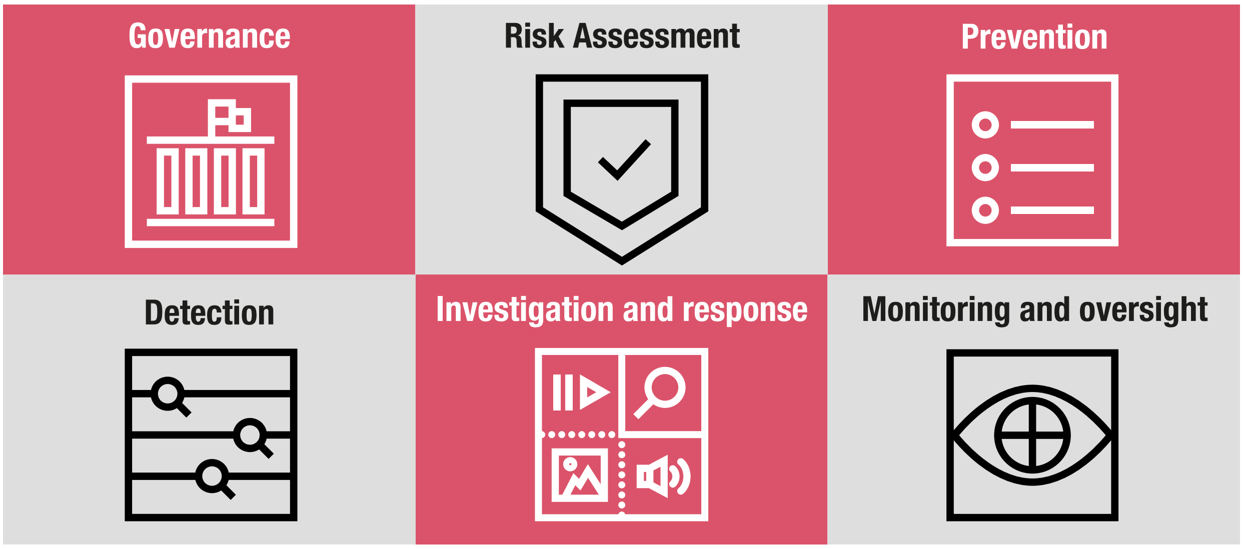
Further, whilst policies may be in place to address certain aspects of the fraud risk (i.e. whistleblowing, ethics policies etc.) many organisations have not yet captured the key elements of their fraud risk management framework within formal policies and standards.

As a consequence, organisations are now having to make decisions about who is responsible for managing and addressing fraud risk in the organisation, how comfortable they are that they have identified all of the relevant fraud risks and what management information they need to get themselves comfortable that sufficient steps have been taken to prevent and detect fraud.

A fraud risk management framework

Using the COSO principles, we have developed a fraud risk management framework that consists of six components. Our fraud risk management framework is summarised below along with some practical considerations for each of the elements that organisations should take into account when developing their framework.

We note that the design of a fraud risk management framework depends on the organisation’s size and complexity. It is important that a fraud risk management framework is tailored to the specific situation of an organisation. The fraud risk management framework below is scalable and can also be used for smaller organisations. We stress that a fraud risk management framework is relevant for each organisation, small or big.



Element	Practical considerations
Governance	Corporate governance failures are behind many high-profile corporate frauds. Protected organisations have a strong governance and reporting structure, set within a culture that reinforces ‘doing the right thing’ and embeds counter fraud behaviours throughout the organisation. Whilst all directors have a responsibility to ensure sufficient steps are in place to prevent and detect fraud, how the board is structured to govern these processes will vary from one organisation to another and certain directors may have specific responsibilities. When establishing governance around the fraud risk management framework, consider: • Which member(s) of the board will be directly responsible for the management and reporting of fraud risk? • Does this director(s) have the necessary capabilities and experience to perform this role? • How does the organisation ensure that fraud risks are effectively identified, monitored, discussed and reported at director level? This may include the formation of a specific working group, e.g. under supervision of the Audit & Risk Committee. • Where there are material operations in various territories or segments, which, if any, of the board’s responsibilities should be delegated to the respective management who have oversight of these operations? How does the board ensure that it sufficiently supervises/monitors these activities? • Where the organisation has a combined Risk Management and Internal Audit function, what steps are taken to ensure that the audit function remains independent (and has direct access to the Audit & Risk Committee). • There might be separate risk management exercises going on within an organisation to address fraud risks, for example, around the risk of tax evasion, cybersecurity threats and Anti-Bribery & Corruption. These might not all need to be pulled into one overall fraud risk management framework, but we would recommend a reconciliation process to ensure all relevant risks are covered.

Element	Practical considerations
Risk Assessment	A comprehensive risk assessment is fundamental to capturing key fraud risks, assessing the impact they have on the organisation and the key controls in place to prevent and detect instances of fraud. In developing a fraud risk assessment, consider: • What the fraud risk assessment will comprise. We would recommend that the key elements of a comprehensive fraud risk assessment include: - Identification of key areas of fraud risk within the organisation; - A detailed description of the fraud scheme, relevant to the risk identified; - Identification of relevant processes and process owners; - The likelihood and impact (financial and non-financial) to the organisation were the fraud risk to manifest itself; - Identification and mapping of key controls, including an assessment of their design and operational effectiveness; - The residual risk level, including commentary on the organisation’s response to the remaining level of risk; - Whether there are any more macro or internal factors that need to be considered, which could indicate a higher overall risk environment. Such factors might include: • The industry and/or territory in which the organisation operates • The extent to which management holds shares of the organisation • Specific targets that management hold and it’s feasibility • Recent changes in the organisation’s management/governance structure • Imminent potential deal activity. • We would suggest that the board representative responsible for fraud risks is also responsible for the risk assessment process. • We would say the fraud risk assessment should be reviewed on at least an annual basis. In case there is a significant change in circumstances, e.g. a major transaction, change in strategy, changes in internal controls and procedures, changes in the organisational structure, external events such as COVID-19, the risk assessment may need revisiting in a shorter timeframe. • Different functions or departments within the organisation might perform their own ‘fraud’ risk assessments, even if not called as such. For example, IT may perform a cybersecurity risk assessment, Legal might perform a risk assessment over compliance with laws and regulations. At a minimum, organisations should take into account the output of these other assessments, but they might want to consolidate this process to some extent under the umbrella of an overall fraud risk assessment. Some organisations also organise fraud workshops, not only to create awareness amongst employees, but also to use the views and experience of the participants as input for the fraud risk assessment. • Group companies might also be split across multiple territories with different risk environments and regulations. It should be clear how this has been reflected in performing the fraud risk assessment, including how the views of the different territories about local fraud risks have been taken into account.

Element	Practical considerations
Prevention	Well-designed and operationally effective controls help protect an organisation from internal and external fraud. When establishing/maintaining preventative controls around fraud, consider: • Is there a complete understanding of the existing controls in place across the organisation (also at group level) that are specifically designed to address the risk of fraud? Is it clear what fraud risk these controls are addressing. Is it clear who owns the operation and review of such controls? • How regularly are the controls reviewed for design effectiveness (not just operating effectiveness)? Is there a formal testing programme that ensures targeted testing of key controls, using appropriate sample sizes and at an appropriate frequency? Are such reviews coordinated centrally, or delegated to the management of respective divisions, and if delegated, is there enough independence from the control owner? Who reviews the results of the testing and determines any remediation plans? • Does the control environment include a balance of manual and automated controls? Is this balance appropriate for the relevant risks and size of the organisation? • Have controls failed in the past? Was the root cause of the failure identified? Have they been appropriately remediated and retested? • Are 'hard controls' (e.g. policies and procedures, systems and structure) supported by 'soft controls' (e.g. values, communication, openness, expectations)? What impact do deficiencies in soft controls have on hard controls? Refer to section 3 for more information on the organisational culture and fraud risk management.
Detection	Controls, processes and systems that actively look for fraud in key risk areas, enabled by innovative technology. When establishing/maintaining your detective controls around fraud, many of the points to consider for the preventative controls above will also be important. Also consider what detective processes the organisation has in place to actively hunt for fraudulent transactions? In our experience, organisations are not making sufficient use of the advances in technology to detect fraud, which include data analytics and/or data visualisation tools. As technology advances, also fraud becomes more sophisticated and difficult to detect. While no universal solution for protecting the organisation from all types of fraud may exist, the organisation could focus on fraud prevention and detection tools most relevant for its operations. There are tools available that typically proactively monitor data to identify potential fraudulent activities or potential fraudulent counterparties, such as: • Payment analysis tooling; • Continuous monitoring platform; • Entity News Due Diligence tooling.

Element	Practical considerations
Investigation and response	The organisation's ability to rapidly and effectively investigate indications or suspicions of fraud and trace assets, individuals and networked relationships. Consider: • Are there clear processes and communication channels in place for reporting potential instances of fraud within the organisation (e.g. a whistleblower hotline)? Are these safe, transparent and available to all staff? • What management information is available within the organisation regarding the number of instances of potential fraud that have been reported? How regularly are such activities monitored and reported on and by whom? Is there an appropriate triage process to address all reported issues including responsibility inside the organisation and a decision-making process for potential use of parties outside of the organisation? Is this appropriately disseminated? • Are the necessary skills and experience available within the organisation to investigate the key fraud risk areas? Where appropriate, what services might be required from third-party providers (i.e. legal counsel, e-discovery, forensic accountants, HR consultants, cyber experts)? • Does the organisation have a recovery plan when confronted with fraud (including: how is the fraud stopped, what measures are taken to prevent the fraud from happening again, recovery of damages, filing a report to the police)?
Monitoring and oversight	Regular effective monitoring and oversight is key to ensure that the fraud risk management framework has been correctly implemented and that any weaknesses are resolved in a timely manner. Consider: • Is there an internal audit function to provide a third line of defence, including the testing of preventative and detective fraud controls? Does the internal audit function have sufficient experience and knowledge of fraud and fraud risk management? Are they independent of management and other lines of defence (i.e. risk management, compliance, legal)? • Are key elements of the fraud risk management programme included in the annual internal audit plan? Where key controls are identified that address the key fraud risks, are these tested at an appropriate frequency and sample size? • Does management and other relevant compliance functions understand their role in relation to the monitoring of fraud risks? Are these clearly stated in their job descriptions and built into annual objectives? • How are the various monitoring activities reported? Where deficiencies are identified, especially in relation to key fraud risks, how are these escalated and resolved? • How does management report about the fraud risk management framework to those charged with governance? And how does the organisation report about fraud to its stakeholders (e.g. what is included in the annual statements about the fraud risk assessment and measures to prevent fraud)?

Example of a fraud risk assessment

A fraud risk assessment can be documented in a risk register, an example of such a risk register is included below:

Risk	Proces	"Risk manifestation (how the risk can manifest itself)"	Impact (1)	Opportunity (2)	Risk (3)	Measures/controls already in place	Risk coverage	"Remaining risk (net risk) (3)"	Additional measure
Fraudulent payments	Purchasing and payments	Employee changes creditor's IBAN in payment batch and inserts its own IBAN	1	10	10	Authorization of payment run by CEO, without IBAN check	Partial	6	4-eyes principle on IBAN - modifications
		Employee sends fake invoices	4	3	10	..	Whole	1	N/A
		Employee increases existing invoices	..	..	..	..	..	..	..
		..	..	..	..	..	..	..	..

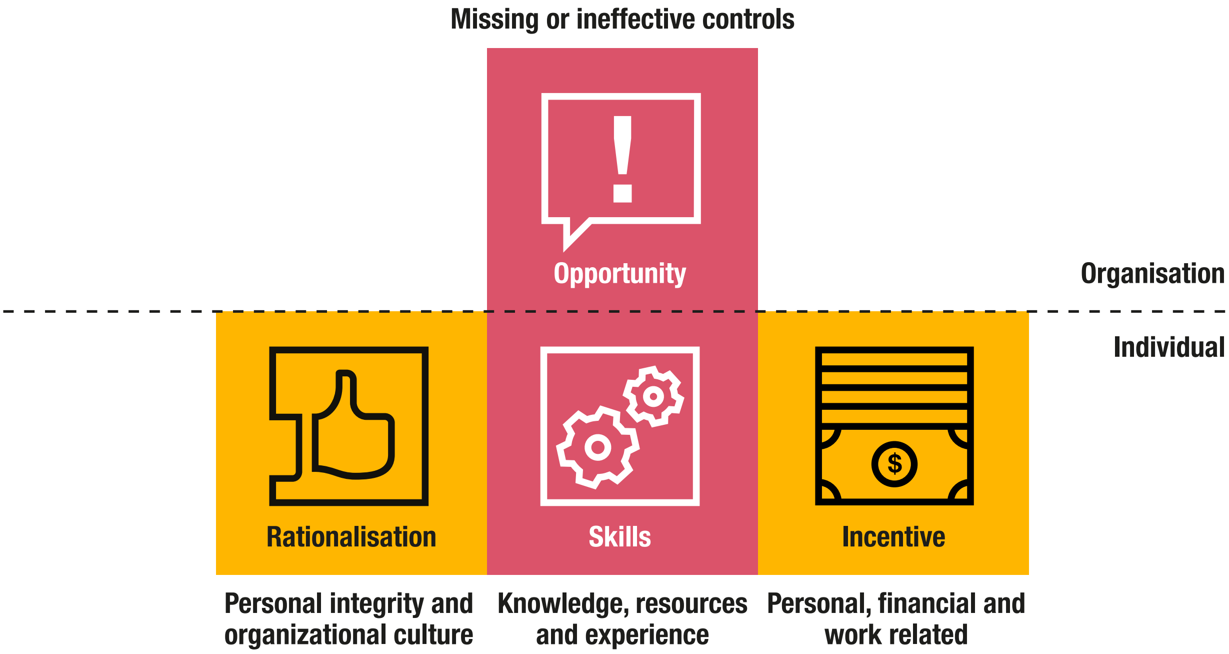
(1) The impact scores indicate: 1 - lowest impact for the organisation if the risk manifests itself to 10 - highest impact for the organisation if the risk manifests itself
(2) The opportunity scores indicate: 1 - lowest opportunity for the risk to manifest itself to 10 - highest opportunity for the risk to manifest itself
(3) The risk scores indicate: 1 - lowest probability for the risk to manifest itself to 10 - highest probability for the risk to manifest itsefl

We recommend considering the following aspects when performing a fraud risk assessment:

- Involve the entire organisation in identifying the fraud risks: The more complete the risk register, the better the organisation is able to consider which risks are acceptable and which are not. Control activities can be designed only when risks are known. But, how does the organisation ensure that the risk register is as complete as possible? This requires creativity and knowledge of the organisation. Therefore, it is crucial to conduct the risk assessment with a broad group of disciplines within the organisation (e.g. the purchasing, sales and management departments).
- Learn from past frauds: frauds observed in the industry are indicators that the risk also applies to your own organisation.
- Always view risks as inherent risks: the risk without taking into consideration the control measures in place.
- Look at risks from different perspectives: what are the risks related to security, commerce, fraud and/or cyber risks?
- Look at the impact of the developments on the risk assessment. For example: COVID-19 leads to more remote working and therefore the cyber risk might increase.
- There are various studies that look at fraud risks of a specific industry, these can be used as inspiration.
- Apply the fraud triangle (opportunity, pressure, rationalisation) when identifying fraud risks and include gaps in internal controls as reported by the internal or external auditor in the fraud risk analysis. More information about the fraud triangle is included below.

The fraud triangle

A useful way to frame the problem of fraud is a construct called the fraud triangle (see the picture below), incorporating three key factors that induce people to commit fraud: incentive (pressure), opportunity, and rationalisation. The genesis of a fraudulent act usually follows a standard trajectory. It starts with pressure, generally related to a personal issue. Then, if an opportunity presents itself, the person will wrestle with it emotionally. The final driver, which enables them to move from thought to action, is rationalisation. All three drivers must be present for an act of fraud to occur.


Missing or ineffective controls
Opportunity
Organisation
Individual
Rationalisation
Skills
Incentive
$
Personal integrity and organizational culture
Knowledge, resources and experience
Personal, financial and work related

Evidence to support the fraud risk management framework

From a good governance perspective it is important that the activities within the fraud risk management framework are appropriately evidenced, for example, the effective operation and testing of internal controls that prevent and detect fraud. This will enable a proper assessment to be made over the effectiveness of the framework.The type of evidence can depend on the activity, but could be in the form of meeting minutes, testing plans, testing results and reports to the board.

Fraud and internal controls over financial reporting

The fraud risk management framework outlined in this paper is focused on the prevention and detection of all types of fraud, including those over fraudulent financial reporting. In our experience, when management fulfils their broader responsibility to implement robust internal controls that support an appropriate tone and culture of honesty, the opportunities to commit fraudulent financial reporting can also be reduced significantly. This is supported by a number of external studies on the impact of the internal control requirements of the US Sarbanes-Oxley Act (US SOx), including:

- The CAQ paper 'Financial Restatements Trends in the United States 2003-2012' notes that at the start of the decade studied (2003) 5% of the identified restatements involved fraud. By the end of the decade studied (2012) it was 1%. While this cannot necessarily be attributed only to the introduction of US SOx, it is believed it has played a key role as it requires awareness of an organisation's key fraud risks, and whether mitigating controls are in place to address those risks.
- The paper 'SOx after 10 years: a multi disciplined review' also noted that a FERF 2005 study found that 33% of large company CFOs agreed that US SOx had reduced fraud. It also conjectured that the heightened awareness of corporate frauds revealed in the economic downturn in early 2000s drove adoption of new laws to deter fraud. The governance template provided by US SOx made it easier for countries to copy the law.
- One of the higher risk areas for fraud is the processing of manual journal entries, which can be open to fraudulent manipulation. In a Harvard Business Review article in 2006 'Unexpected benefits of Sarbanes-Oxley', the writers provide a specific company example of how US SOx helped reduce the fraud risk around journal entries.

3. Organisational culture and fraud risk management

In addition to a well-designed fraud risk management framework, we believe that the organisational culture, behavioural aspects and also other elements that define the way of doing business within the organisation, are some key factors that may impact the understanding and reduce the fraud risks within the organisation. These factors are visible in the way people interact within the organisation, in how employees perform their tasks, in how the organisation is managed and the perception from the outside world.

The organisational culture consists of the combined behaviours, beliefs, mental models and explicit and implicit rules of its people. Culture and behaviour within the organisation is achieving an increased role as fraud and misconduct are attributed more and more to cultural gap and misalignment. Accordingly, the "intended culture" - what the organisation wants (vision, purpose and values), should be in agreement with the "actual culture" - the behaviour displayed by its employees. Risks may arise when the "actual culture" does not keep up with the organisation's goals.

The culture influences the results of the organisation and the controls the organisation has in place, both soft controls and hard controls. Soft controls are non-tangible factors that influence behaviour and along with "hard controls" (e.g. policies and procedures) constitute the internal control environment of an organisation. As noted in our proposed fraud risk management framework and as included in the COSO framework on which it is based, culture is considered a starting point in defining risk management. Hence, it is important for the organisation to assess and measure its culture and the so-called "soft controls" to determine and mitigate risks. It is important for the organisation to understand what the main drivers of behaviour for its employees are.

These can include but are not limited to the following elements:

- Governance and tone at the top - pointing the direction to employees and leading by example by reinforcing the behaviours that are expected from the rest of the team.
- Incentive - what are the behaviours and achievements that get praised within the organisation and how?
- Diversity and inclusion – do leaders see the employees' perspective/point of view? Are employees listened to and do they participate in the course of the business?
- Psychological safety - do employees feel comfortable when sharing suggestions or challenging the management without fear of social consequences?

"A healthy culture is purposeful, psychologically safe, diverse and inclusive"[1] Examples of behaviours that define a healthy culture include but are not limited to:

- Collaboration spirit and holistic thinking;
- Openness and humility - willingness to learn from others and from honest mistakes;
- Accountability and willingness to accept personal responsibility on actions;
- Transparency – instead of masking or avoiding to share negative news, these are communicated in a constructive way to employees;
- Recognising employee contribution - this can boost organisation-wide morale and encourage a culture of proactivity and healthy competition
- Make employees feel comfortable and stimulate them to share their points of view, suggestions and to challenge management.

[1] Culture audit in financial services, reporting on behaviour to conduct regulators. Roger Miles, 2021

There are several studies and models available that an organisation can use to understand culture and behaviour, but the but there are two main approaches:

1. Measuring culture from surveys and interviews to employees; and
2. Measuring culture from naturally occurring data such as observation of behaviour and internal sources such as i) sickness rate; ii) strategy documents; iii) culture-related KPIs.

In order to have a holistic view and a more accurate output, both methods should be alternated during the culture assessment/ measurement.

Considering the culture and soft controls for fraud risk management, allows the organisation to have a more accurate understanding of its control environment and the effectiveness of the framework in preventing, detecting and mitigating fraud risks. Furthermore, assessing the actual culture and existing soft control environment, gives insight in the risk profile and in areas that the organisation should focus on in order to bridge the gap between the intended and the actual culture.

4. Suggested elements for further disclosure over the prevention and detection of fraud in the management's board report

Current requirements

Pursuant to the Dutch Civil Code (Article 2:391[1]) and the Dutch accounting standards (RJ 400), a legal entity should describe in its management report the main risks and uncertainties that it faces during its business activities. This analysis should be in line with the size and complexity of the legal entity and group companies. As per RJ 400.110b, the main risks and uncertainties include the identification of, among others, the operational activities, which include the risk of fraud and corruption.

Based upon RJ 400.110c the legal entity should provide a broad description of its inclination to cover risk and uncertainties, the so-called "risk appetite" (the amount of risk an organisation is willing to take in pursuit of objectives it deems have value). In addition, the entity must provide the following information:

- Description of the measures taken to manage the main risks and uncertainties;
- Description of the expected "impact" on the results and/or the financial position;
- Description of the risks and uncertainties that had a significant "impact" on the entity in the past financial year along with their consequences; and
- Which improvements have been or will be made to the legal entity's risk management system.

Based on the current Dutch Corporate Governance Code, the organisation should have adequate internal risk management and control systems in place. The management board is responsible for identifying and managing the risks related to the strategy and activities of the company and its affiliates and also for determining the risk appetite and measures in place to face the risks. Based on the risk assessment, the management board should implement and maintain adequate internal risk management and control systems.
This includes monitoring the design and effectiveness of the internal controls and risk management at least once a year. The Dutch Corporate Governance Code specifies that special attention should be given to observed instances of misconduct and irregularities.
The management board should establish a procedure for reporting actual or suspicion of misconduct or irregularities within its company and affiliated enterprises. This procedure should be published on the company's home page. Furthermore, it should ensure that the employees have the opportunity to file a report without any consequences to their legal position.
The supervisory board should monitor the management board on the process, and any instances of actual or suspected misconduct or irregularities should immediately be reported to the supervisory board.

Pursuant to the Dutch Corporate Governance Code, the management board should include the following information in the management report:

- The execution of the risk assessment, with a description of the principal risks the company is facing in relation to its risk appetite, including strategic, operational, compliance and reporting risks;
- The design and operation of the internal risk management and control systems during the past financial year;
- Any major failings in the internal risk management and control systems that have been observed in the financial year, any significant changes made to these systems and any major improvements planned, along with a confirmation that these issues have been discussed with the audit committee and the supervisory board.

The management board should clearly state in the management report, that the report provides sufficient information on any deficiencies in the risk management and internal controls system and that the system provides reasonable assurance that the financial reporting does not contain any material inaccuracies, that it is justified that the financial reporting is prepared on a going concern basis and that the report states those material risks and uncertainties that are relevant to the expectation of the company's continuity for a period of twelve months after the preparation of the report.

Suggested elements for further disclosure

On 2 February 2022, a consultation document "Proposal to Update the Dutch Corporate Governance Code 2022" was issued by the Corporate Governance Code Monitoring Committee. As part of the consultation of the 2022 Dutch Corporate Governance Code, (among others) The Royal Netherlands Institute of Chartered Accountants and the Minister of Finance suggest that the scope of the in-control statement should be expanded from solely financial reporting risks to also include operational and compliance risks.

PwC Netherlands prepared a response to the consultation document, indicating primarily that it is important for the code to stay ahead of societal developments. These developments include the climate crisis, the COVID-19 pandemic, the war in Europe and growing social inequality. One of the topics that PwC proposed as deserving a "more explicit" place in the updated code is including the responsibility of the management board and the supervisory board members on three topics: fraud, going concern and in-control. These themes are currently discussed in the code only in retrospect, when misconduct and irregularities are found. Users of financial statements need better information and accountability by companies on risks and safeguards to prevent fraud and violation of laws and regulations.

Therefore, PwC advocates that the code should include as "best practice" the disclosure of information about guarantees for fraud prevention and compliance with legislation and regulations in the management board report and in the report of the supervisory board.

We consider that a proper disclosure of the organisation's fraud risk assessment could contribute to enhancing the trust in the organisation, by providing stakeholders and market participants a better understanding of the organisation's exposure to risk of fraud and the controls implemented.

We would highly recommend organisations to disclose in their management report the following main aspects (but not limited to):

- Types of fraud risk, deriving from the industry, the business and the organisational structure, and other factors, specifying where in the business they could occur and why, followed by the specific actions taken to mitigate those risks.
- Details of suspicion of fraud, identified fraud(s) or fraud(s) identified in the past along with the improvements and remediation plans implemented by the organisation, should also be included to the extent they are appropriate.
- Descriptions of the main procedures and processes in place related to the fraud risk assessment, or the description of the fraud risk management within the organisation. These could include a description of the steps the organisation has taken to prevent and detect fraud such as undertaking an appropriate fraud risk assessment and responding appropriately to identified risks, promoting an appropriate corporate culture and corporate values, and ensuring appropriate controls are in place and operating effectively.

For questions on this guide, please contact
one of our fraud specialists:

Sander Kranenburg
Partner, Forensics
sander.kranenburg@pwc.com

Rian Mes
Senior manager, Forensics
rian.mes@pwc.com

Jan-Kees Janse
Partner, Assurance
jan-kees.janse@pwc.com

Lenda Pacaj
Manager, Assurance
lenda.p.pacaj@pwc.com

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC NL, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.