

# Restoring trust through enhanced fraud risk management



## Fraud is on the rise, with new working practices emerging out of the pandemic, market and supply chain disruption and global instability all increasing the motivation, rationalisation and opportunity to commit fraud.

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

In July 2023, the Government's Department for Business & Trade (DBT) laid before Parliament new draft legislation which will require that companies that have over 750 employees and over £750m annual turnover include in their Directors' Report in the Annual Report a 'Material Fraud Statement'. This statement will summarise the directors' assessment of the risk of material fraud to the company's business operations, including how the directors have assessed the company's susceptibility to material fraud and the types of material fraud considered. It will also describe the main measures which are in place to prevent and detect the occurrence of material fraud including any new measures which are in place or proposed to be put in place during the relevant financial year or the next financial year. The new disclosure looks likely to be applicable for companies who meet this threshold and whose equity share capital is admitted to trading on a UK regulated market, from 1 January 2025 and for all other companies that meet the threshold, from 1 January 2026.

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 support the future reporting requirements. In this paper, as well as providing our views on what are the key elements of a fraud risk management framework, we outline a number of practical considerations to help companies consider fraud risk and what evidence would be useful to support their framework. We also suggest what the key elements of the directors' disclosure could be around the prevention and detection of fraud.

**The UK's fight against economic crime is a key focus area for the Government as it seeks to strengthen the UK's whole system response in this area; the Covid-19 pandemic has also generated new opportunities for fraudsters, economic criminals and other hostile actors to exploit, highlighting the threats our financial system and our wider institutions face.**

**In addition to the draft Statutory Instrument, the Government is currently proposing a failure to prevent fraud offence in the 'Economic Crime and Corporate Transparency Bill'. Under the new offence, an organisation will be liable where a specified fraud offence is committed by an employee or agent, for the organisation's benefit, and the organisation did not have reasonable fraud prevention procedures in place. The bill is in the final stages of passing through Parliament. This is discussed in further detail later on in this document.**

For questions on this guide, please contact:

**Jayne Kerr**  
Director, Public Policy  
[jayne.l.kerr@pwc.com](mailto:jayne.l.kerr@pwc.com)

**Sotiris Kroustis**  
Partner, UK Head of Public Policy  
[sotiris.kroustis@pwc.com](mailto:sotiris.kroustis@pwc.com)

**Jonathan Holmes**  
Partner, Forensics  
[jonathan.holmes@pwc.com](mailto:jonathan.holmes@pwc.com)

**Steve Bewick**  
Partner, Forensics  
[steven.j.bewick@pwc.com](mailto:steven.j.bewick@pwc.com)

**Oliver Delve**  
Director, Forensics  
[oliver.m.delve@pwc.com](mailto:oliver.m.delve@pwc.com)

### Why enhanced fraud risk management is important

- Trust and confidence in business is critical to creating a flourishing business environment and helping make the UK an attractive destination for foreign investment and world leading as a capital market. Robust fraud risk management is crucial in both protecting value and enabling trust in businesses.
- As a global centre for trade and investment, the UK economy has built a reputation based on adherence to a strong and independent rule of law. Capital markets require trust and transparency to operate effectively. Corporate conduct and reporting that robustly counters fraud and financial crime is crucial in building trust.
- Financial fraud is on the increase and the pandemic has served to accelerate the rise. Our 2022 PwC Global Economic Crime Survey<sup>1</sup> saw 64% of UK respondents reporting having experienced a fraud in the previous two years, compared to 56% in the UK results of our 2020 survey.
- This is an opportunity to rethink and refresh a company's holistic approach to fraud risk management. It is likely many companies will need an extensive refresh of their approach to performing a fraud risk assessment and implement a more formal internal controls regime for the prevention and detection of fraud.

### Why should you act now

- Being in a position to confidently disclose the steps taken to prevent and detect material fraud, and possibly have it assured to some extent, will for many companies require a significant enhancement of their current fraud risk management framework.

<sup>1</sup> <https://www.pwc.co.uk/services/forensic-services/insights/global-economic-crime-survey-2022-uk-findings>

# Contents

1	What does fraud mean to you?	02
2	Key elements of a fraud risk management framework	03
3	Future reporting requirements over the prevention and detection of material fraud	07
4	Suggested elements of directors' disclosure on the steps taken to prevent and detect material fraud	08



## What does fraud mean to you?

In establishing and maintaining an effective fraud risk management framework, and in support of the 'Material Fraud Statement' disclosure proposed in the draft Statutory Instrument, it is first necessary to determine what fraud means to you and your company. The draft Statutory Instrument that has been laid before Parliament notes "fraud" as meaning behaviour falling into sections 2 to 4 of the UK Fraud Act 2006 ('Fraud Act'). This includes:

- fraud by false representation;
- fraud by failing to disclose information; or
- fraud by abuse of power.

Fraud is interpreted by the Fraud Act as a deliberate act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception or dishonesty, to obtain an unjust or illegal advantage to make a personal gain for oneself and/or create a loss for another.

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 that a company might need to consider depending upon their individual structure, industry and business.



The fraud risk management framework should be designed to consider all fraud risks, whether or not the impact could be material. However, as part of the assessment process, the organisation will need to ensure the process identifies those risks which will need to be described in the Material Fraud Statement.

The draft Statutory Instrument has defined material, for the purposes of this disclosure, as "fraud of a nature or magnitude that could reasonably be expected to influence the decisions which a reasonable shareholder would make in connection with their shareholding in the company". Applying this definition in practice will require consideration of financial, qualitative (e.g. internal perpetrator or third party) and non-financial factors (e.g. media exposure, brand or reputational damage etc.).

## 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.

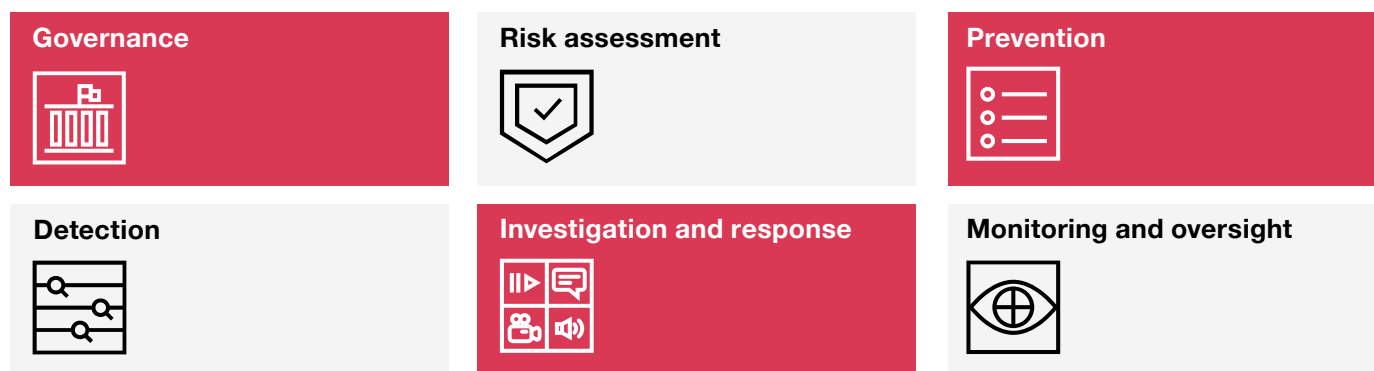
We believe the COSO principles, which are designed to help companies understand the key elements needed for an effective internal control framework, are a good basis for a fraud risk management framework and help with understanding and improving the processes and controls in place to prevent and detect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


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

As a consequence companies 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

Our fraud risk management framework has six elements, developed using the COSO principles, which we have summarised below and followed with some practical considerations for each of the elements when companies are developing their framework.



Element	Practical considerations
<b>Governance</b> 	<p>Corporate governance failures are behind many high profile corporate frauds. Protected companies 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 will 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 organisation by organisation and certain directors may have specific responsibilities. When establishing governance around the fraud risk management framework, consider:</p> <ul style="list-style-type: none"> <li>• Which members of the board will be directly responsible for the management and reporting of fraud risk?</li> <li>• Does this director(s) have the necessary capabilities and experience to perform this role?</li> <li>• How does the company ensure that fraud risk is effectively monitored, discussed and reported at director level? The committees and/or sub-committees that are needed will likely vary organisation by organisation, but may include the formation of a fraud risk steering group, which as appropriate, may be a sub-committee of the Audit &amp; Risk Committee (or similar) where such a Committee is already in place.</li> <li>• Where there are material operations in various territories or segments, what, if any, of the board's responsibilities should be delegated to the respective management who have oversight of these operations?</li> <li>• Where the company has a combined Risk Management and Internal Audit function, what steps are taken to ensure that the audit function remains independent?</li> <li>• There might be separate risk management exercises going on within a company to address fraud risk, for example, around the risk of tax evasion, cyber security threats and Anti-Bribery &amp; Corruption. These might not need to be all pulled into one overall fraud risk management framework but we would recommend a reconciliation process to ensure all the relevant risks are covered.</li> </ul>

## Risk Assessment



As noted above, the Material Fraud Statement will need to summarise the directors' assessment of the risk of material fraud to the company's business operations, including how the directors have assessed the company's susceptibility to material fraud and the types of material fraud considered.

A comprehensive risk assessment is fundamental to capturing key fraud risks, assessing the impact they have on the company, and key controls in place to prevent and detect instances of fraud. In developing a fraud risk assessment, consider:

- We would recommend the key elements of a comprehensive fraud risk assessment include:
  - A detailed description of the fraud scheme, relevant to the risk;
  - Identification of relevant processes and process owners;
  - The likelihood and impact (financial and non-financial) to the company were the fraud risk to manifest;
  - 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; and
  - Whether there are any more macro 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 company operates;
    - Level of share ownership by management;
    - Recent changes in the company management/governance structure; and
    - Imminent potential deal activity.
- We would suggest that the board representative responsible for fraud risk is also responsible for the risk assessment process.
- We would say the fraud risk assessment should be reviewed on at least an annual basis. Where there is a significant change in circumstances, e.g. a major transaction, change in strategy, or a significant geo-political or social event (e.g. pandemic), the risk assessment may need revisiting in a shorter timeframe.
- Different functions within the company might perform their own 'fraud' risk assessments, even if not called as such. For example, IT may perform a cyber security risk assessment, Legal might perform a risk assessment over compliance with laws and regulations. Whilst it may be appropriate to keep these risk assessments separate at the functional level, to inform the Material Fraud Statement a consolidation of these risks will need to occur, at a minimum, at the Board / Exec level of reporting.
- Groups 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 risk have been taken into account.

## Prevention



Well designed and operationally effective controls help protect a company 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 group 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 program 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 company?
- Have controls failed in the past? Was the root cause of the failure identified? Have they been appropriately remediated and retested?

## 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 preventative controls above will also be important. Also consider:

- What detective processes does the company have in place to actively hunt for fraudulent transactions?
- How is the company leveraging appropriate advances in technology to detect fraud? For example, data analytics or data visualisation tools?

## Investigation and response



The company's ability to rapidly and effectively investigate 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 company? Are these safe, transparent and available to all staff?
- What Management Information is available within the company 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 company and a decision making process for potential use of parties outside of the company? Is this appropriately disseminated?
- Are there the necessary skills and experience within the company 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 etc)?

## Monitoring and oversight



Regular effective monitoring and oversight is key to ensure that the 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 etc.)?
- 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?

As noted above, the Material Fraud Statement included in the directors' report will need to describe the measures proposed to be put in place to prevent and detect fraud during the relevant financial year or the next financial year. To inform any such disclosure organisations should consider the role of internal audit and risk management teams, and any recommendations or proposals made as a result of controls testing undertaken in the period.



## Evidence to support the fraud risk management framework and related disclosures

From a good governance perspective it will be 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 and support the directors' disclosures described in the next section. The type of evidence will 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 of the impact of the internal controls 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 where an organisation's key fraud risks are, 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 the 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.





## Future reporting requirements over the prevention and detection of material fraud

Currently there are no explicit requirements (either in law or in the regulations that apply to listed companies) for directors to take specific steps to prevent or detect fraud. However, the current regulatory landscape is taken and over the last two years, the UK Government has taken a number of steps, through proposed and actual regulatory or legislative changes, to ensure that directors of UK businesses are more accountable for the consequences of fraud. These changes are set out below.

### Draft Statutory Instrument

As described above, in July 2023, (DBT) laid before Parliament a draft Statutory Instrument, which includes legislative requirements for 'The Material Fraud Statement' proposed under the UK's Audit and Corporate Governance reforms.

The new disclosures will be required for UK companies that have 750 or more employees and £750m or more annual turnover. The new disclosures will be effective for those companies exceeding this threshold that have equity share capital on a UK regulated market, for reporting periods beginning on or after 1 January 2025, and for all other companies that exceed the threshold, from 1 January 2026.

The Statutory Instrument sets out the following key points in relation to the Material Fraud Statement:

- Definition of fraud: The Statutory Instrument includes the definition of "fraud" as meaning behaviour falling into sections 2 to 4 of the Fraud Act 2006.
- Fraud risk assessment: The Statutory instrument confirms that the directors would need to summarise "their assessment of the risk of material fraud to the company's business operations and how they have assessed this".
- A description of the main measures in place to prevent and detect material fraud. In addition, the Statutory Instrument states that measures proposed to be put in place during the relevant financial year or next financial year would also be disclosed.

As we outline above, any such disclosure should be supported by the company's fraud risk management framework.

### UK Failure to prevent fraud offence

The Government is currently proposing a failure to prevent fraud offence in the 'Economic Crime and Corporate Transparency Bill'. Under the new offence, an organisation will be liable where a specified fraud offence is committed without reasonable fraud prevention procedures in place that either directly, or indirectly, benefits the organisation. As currently envisaged, the new offence encompasses a number of fraud and false accounting offences, although excludes money laundering offences due to the current AML procedures required by law and requirement to be regulated by the FCA.

We expect that when this offence comes into force, further guidance will be published on what constitutes reasonable fraud prevention procedures.

When the UK Government introduced the "failure to prevent" legislation in respect to bribery (Bribery Act 2010) and the facilitation of tax evasion (Criminal Finances Act 2017), it meant that the directors of companies could be subject to a fine and/or imprisonment if insufficient actions were taken to prevent any instances of these financial crimes. The impact of these legislative changes were then realised through action taken against companies like Petrofac Limited, who pleaded guilty to seven separate counts of failing to prevent bribery, amongst others.

### Connection between the UK failure to prevent fraud and the draft Statutory Instrument

The scope of the UK failure to prevent fraud legislation is anticipated to be wider than the draft Statutory Instrument, it is expected to encompass large organisations, defined using the standard Companies Act 2006 definition as organisations meeting two out of three of the following criteria: more than 250 employees, more than £36 million turnover and more than £18 million in total assets.

While further guidance on what constitutes reasonable fraud procedures is still to come, we would encourage those companies that fall within the offence but outside of the draft Statutory Instrument to still be considering the draft Statutory Instrument guidance and documenting the measures in place to prevent and detect fraud.

For those companies that are in scope of both the failure to prevent fraud offence and the draft Statutory Instrument the two could work in parallel as the disclosures could support how the company may have had reasonable fraud prevention procedures in place.

In our view, considering these regulatory implications now is a no regret action. Good fraud risk management discipline makes good business sense and while many businesses will feel they know their risks, we can expect the changing implications of getting it wrong will demand management attention.

### Audit requirements

Although DBT is not proposing any new audit or reporting requirements for auditors, recent revisions to the auditing standard ISA (UK) 240 on the auditor's responsibilities in relation to fraud in the audit of financial statements, have increased the focus auditors place on the robustness of a company's fraud risk management framework. Auditors will also have to assess the consistency of the new directors' disclosures with their knowledge from the audit.



## Suggested elements of the Material Fraud Statement

The exact details of the new disclosure are not yet fully known, but we have assumed it would take the form of a narrative description of the steps taken in a report format. We have assumed that there will be a formal confirmation that the steps taken are regarded as appropriate by directors. The disclosure could cover all types of fraud, not just fraudulent financial reporting. In terms of content, while we can't be sure what would be required in the ultimate disclosures as that will be down to the final legislation, the following would be important whatever the precise scope and form of the reporting:

- The main focus should be on the specific types of fraud risk, where in the business they could occur and why, followed by the specific actions taken to mitigate those risks.
- Details of identified frauds and lessons learned should also be included to the extent it is appropriate.
- Descriptions of process and procedure will be necessary, for example when explaining the governance process over the fraud risk assessment, but should not be the main focus of the disclosures. Boilerplate language should be avoided and the reporting should be as informative and company specific as possible.

In terms of positioning within the annual report, it's important that fraud risk is integrated as far as possible with other parts of the annual report dealing with risk that companies and auditors need to respond to – potentially the principal risks and uncertainties and most likely in the reporting on risk management and internal control. The key is that there is an overall coherent and meaningful disclosure of risks in the annual report, including fraud risk. We've suggested potential elements of the disclosure below, along with thoughts on the details they might contain.

### No need to wait!

Where fraud risks are currently disclosed as (part of) principal risks in an annual report and/or where they are described as part of the corporate governance statement disclosures around risk management, the suggested elements of good disclosure described below would equally be relevant.



## Material Fraud Statement

### Our fraud risk management framework

- Brief summary of the key elements and responsibilities within the company's fraud risk management framework (for example, as suggested in our fraud risk management framework guidance above, these could be: Governance, Risk assessment, Preventive controls, Detective controls, Investigation and response and Monitoring and oversight).
- Explanation of how the 'tone at the top' and culture at the company influences behaviours and the roles played by the board, audit committee, management, Internal Audit and employees in the fraud risk management framework.

### Our fraud risk management framework

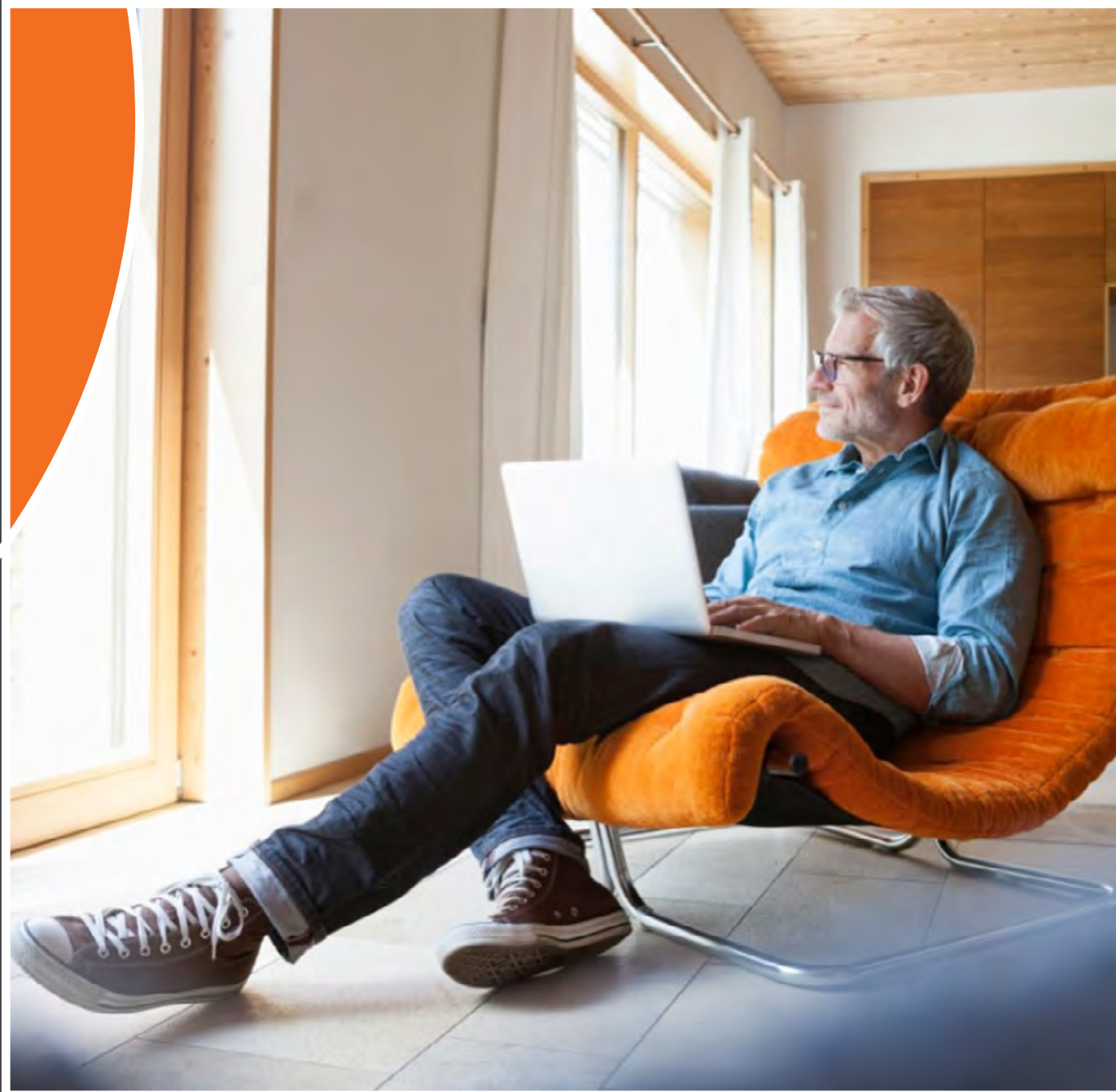
- Description of how fraud has been defined in the context of the business.
- If a multinational group, explanation of any territorial differences in the definition of fraud and how they have been reconciled to the definition actually used.
- Explanation of the basis for the determination of what is considered 'material' fraud.
- Describe the results of the directors' fraud risk assessment of the risk of material fraud to the company's business operations, including the directors' assessment of the company's susceptibility to material fraud.
- Description of the areas of the business most susceptible to fraud and the material types of fraud that could impact them and why (see section on 'What does fraud mean to you?' above for examples of different types of fraud that could be tailored by industry). Include what the consequences could be for the company for each type of fraud, for example:
  - Fines from law enforcement or regulatory breaches.
  - Loss of physical or financial assets.
  - Impact on reported information or reputation and values.
  - Undermining the trust of employees, people, customers, and suppliers.

### Steps we have taken to prevent and detect fraud

- Outline of how the specific areas of fraud risk identified above are mitigated by the company's fraud risk management framework.

### Our response to instances of suspected fraud

- Brief summary of the process for responding to instances of suspected fraud including reporting to the board/ audit committee.
- Outline of the number and type of instances investigated in the year, those that have been resolved, those that are still under investigation.
- Description of any changes made to the fraud risk management framework as a result of instances of fraud.



[pwc.co.uk](https://www.pwc.co.uk)

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, PricewaterhouseCoopers LLP, 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.

© 2023 PricewaterhouseCoopers LLP. All rights reserved. 'PwC' refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](https://www.pwc.com/structure) for further details.

RITM13489399