Dear Councillor

CORPORATE GOVERNANCE COMMITTEE - WEDNESDAY, 26 NOVEMBER 2025

I am now able to enclose for consideration at the above meeting the following reports that were unavailable when the agenda was printed.

Agenda Item No.

5. INTERNAL AUDIT UPDATE REPORT (Pages 3 - 16)

To receive two further appendices providing an update of the work of the Internal Audit Service since the last meeting.

This page is intentionally left blank

Emerging Risk Radar

Emerging risk considerations

Autumn 2025

Emerging risk radar – Autumn 2025

Given your strategic objectives, what do you see as the **emerging events or threats that could impact on your business,** either negatively or positively, and that you believe should be watched?

We received **201 survey responses** from board members & senior management across all industries/sectors as well as drawing on our current emerging risk knowledge.

Key emerging risks in summary

There are 26 emerging risks identified, an increase of 2 since the last publication. New emerging risks in the form of **misinformation spread via social media platforms and a loss of trust in institutions** – impacting private, public and not for profit sectors, both new risks being intrinsically linked. In addition, there have been updates in wording in many of the previous emerging risks.

6 emerging risks identified as more prevalent being 2 more since the last emerging risk radar publication, including **geo-political instability, cyber attacks increasing, artificial intelligence governance lag, threats to operational resilience of technology, continued economic slow down** and **affordability and cost pressures**.

Many of these emerging risks are already recognised and being tackled by businesses. These risks, however, are constantly changing and therefore their management should be kept under review by the Board or equivalent. Furthermore, these emerging risks rarely exist in isolation so it is important that a holistic view is taken to understand their connectivity and how best to tackle these emerging risks.

The top 3 most prevalent emerging risks

01

Geo-political instability
Geo-political change and instability, including potential for trade wars, fall-out from and expansion of armed conflicts and the impact on businesses and society.

02

Cyber attacks increasing
Cyber-attacks increasing in frequency and complexity. Unable to sufficiently invest in defence – attacks more disabling, coupled with loss of data in serious targeted attacks.

03

Artificial Intelligence (AI) governance lag
Increasing use of and reliance on AI without sufficient checks and balances to ensure strengths, weaknesses, threats and opportunities are understood.

Emerging risk – why and what?

Why?
The board should establish and keep under review the risk and internal control framework and determine the nature and extent of the emerging and principal risks it is willing to take to achieve its strategic objectives.

What?
An emerging risk might be defined as:
"a new or unforeseen level of uncertainty driven by external events – the risk may still be forming, and it may not be clear as to the implications for the business, be these negative or positive."

To be watchful of these emerging risks and how they might play through is an important element of preparedness and the business management of risk.

We have framed the emerging risks as:

Most prevalent: risk themes that were more regularly identified in responses and discussions.

Keep monitoring: to represent the risk themes that had a moderate prevalence in responses and discussions

Worth watching: those emerging risk themes that were less prevalent.

These risk themes are constantly evolving and shifting, so are all worthy of consideration.

Emerging risk considerations

What do you see as the emerging risks?

How far will these emerging risks affect your business?

How far will these emerging risks play through into your existing strategic risks?

How far will they change the way you currently manage your strategic risks?

How will you respond?

How will you continue to review the emerging risks?

Emerging areas of risk
Autumn 2025

Consistent
Increasing
Decreasing

Direction of travel since previous emerging risk radar publication.

	Most prevalent	
2.2	Geo-political change and instability, including potential for trade wars, fall-out from and expansion of armed conflicts and the impact on businesses and society e.g. trade and travel barriers.	→
4.1	Cyber-attacks increasing in frequency, complexity with greater levels of disruption, including targeted ransomware attacks across all sectors. Coupled with loss / theft of data. Businesses being unable to invest in defence or afford cost of recovery leading to business failure.	→
4.2	Artificial Intelligence (AI) governance lag – increasing use of and reliance on AI without sufficient checks and balances to ensure strengths, weaknesses, threats and opportunities are understood.	↑
4.3	Operational resilience of technology increasingly threatened e.g. power outage, IT infrastructure age, cost of maintenance / lack of investment, sabotage (be this physical or digital via cyber attack), as well as reliance on AI going un-checked.	↑
5.1	Continued economic slow-down. Persistent inflation. Reduced spending by consumers. Reduced and / or changes in spending by Government impacting all sectors.	→
6.1	Affordability and cost pressures e.g. employment costs, energy costs etc. Creating financial pressure impacting investment and discretionary spend. Impacting longer term plans.	→

Emerging areas of risk
Autumn 2025

Direction of travel since previous emerging risk radar publication.

	Keep monitoring	
1.1	Availability and effectiveness of public services are reduced due to under investment, lack of resources, strategic change e.g. devolution, local government review and police reform. Further, likely increased industrial action and increasing demand from the public.	^
1.3	Societal tensions created, stemming from, by example, racial, ethnicity, diversity, wealth, age, cultural differences as well as fall out from global geo-political tensions and instability, as well as social media. These can spill-over into the working environment.	^
2.1	Change in government priorities resulting in new or changes to laws, policies, regulations and consequences affecting businesses across all sectors.	v
2.3	Increasing level of regulation, compliance and inspection / enforcement. e.g. Economic Crime and Corporate Transparency Act etc.	>
3.1	Ability to effectively engage with and leverage off the sustainability agenda, including ability to meet green agenda targets (coupled with potential for Green Washing).	>
3.2	Increasing weather pattern shifts / extreme weather impacting all sectors – storms, floods, temperature changes impacting supply chains, productivity and continuity / recovery of operations.	>
5.2	Reduced investment in research and development - businesses take a short-term approach and focus on business as usual (reducing agility and innovation) due to macro-economic conditions including geo-political challenges.	>

Emerging areas of risk
Autumn 2025

Direction of travel since previous emerging risk radar publication.

	Keep monitoring	
6.2	Supply chain resilience across all ranges of goods and services, including having supply chain knowledge and visibility e.g. unknown child labour practices.	›
6.3	Access to and availability of finance and funding – impacting both private, public and not for profit sectors, including cost of finance, funding changes - including funding and grants provided by Government.	›
6.4	Increasing levels of fraudulent activity making use of technology as a tool for doing so including use of AI.	^
7.1	Loss of access to skills, knowledge and experience – reduced investment in staff development / apprenticeships, temporary contracts more frequent, reduced pool of skilled / experienced staff available with movement between employers coupled with changes in the working landscape. Increased use of AI / technologies in the workplace replacing human roles – likely impacting all sectors and professions in medium / longer term.	›
8.1	Loss of accountability and oversight - lip service to standards / codes, lack of transparency in decision making, conflicts of interest justified.	^
8.2	Developing the board member capacity and capability - fitness for future, including availability of non-executives for appointment and holding modern world insights.	›

Emerging areas of risk
Autumn 2025

Direction of travel since previous emerging risk radar publication.

	Worth watching	
1.2	Increasing awareness of mental health and physical well-being issues impacting individuals stemming from post pandemic fall-out e.g. remote working fatigue, expectation of business v individuals. Further, being increasing poverty etc. Also impacting on public services and employers (creating potential duty of care implications).	>
1.4	Access to affordable housing. Increasing homelessness and poor housing conditions. e.g. damp and mould hazards. Access to affordable housing and the impact on individuals, families, society more widely and business in the form of access to / availability of staff due to location or ill-health.	>
1.5	Epidemic / further pandemic (and lock down) impacting public health / productivity.	>
4.4	**NEW**: Misinformation spread via social media platforms impacting businesses.	New
5.3	Various factors leading to market changes impacting business e.g. access to materials and labour, global trade embargos, restrictions, tariffs, business re-location, competition, ownership / acquisition and merger.	>
8.3	Shifts in business culture due to external influence and attitudes creating conflicts and tensions amongst leadership in all sectors.	>
8.4	**NEW**: Loss of trust in institutions, both large businesses, government and public sector bodies.	New

Emerging risk radar
Autumn 2025

RSM

Societal and Community

1.1 – Availability and effectiveness of public services are reduced.

1.2 – Increasing awareness of mental health and physical well-being issues.

1.3 – Societal tensions stemming from, by example, racial, ethnicity, diversity, wealth, age, and cultural differences, spilling over into the work environment.

1.4 – Access to affordable housing, homelessness and poor housing conditions.

1.5 – Epidemic / further pandemic (and lock down) impacting productivity.

Governance

8.1 – Loss of accountability and oversight – lip service to standards / codes, lack of transparency in decision making, conflicts of interest justified.

8.2 – Developing the board capacity and capability – fitness for future, availability of NEDs and having real world insights.

8.3 – Shifts in business culture due to external influence and attitudes creating conflicts / tensions amongst leadership.

8.4 – **NEW** Loss of trust in institutions, both large businesses, government and public sector bodies.

Economic and Financial

6.1 – Affordability & cost pressures e.g. staff, energy etc.

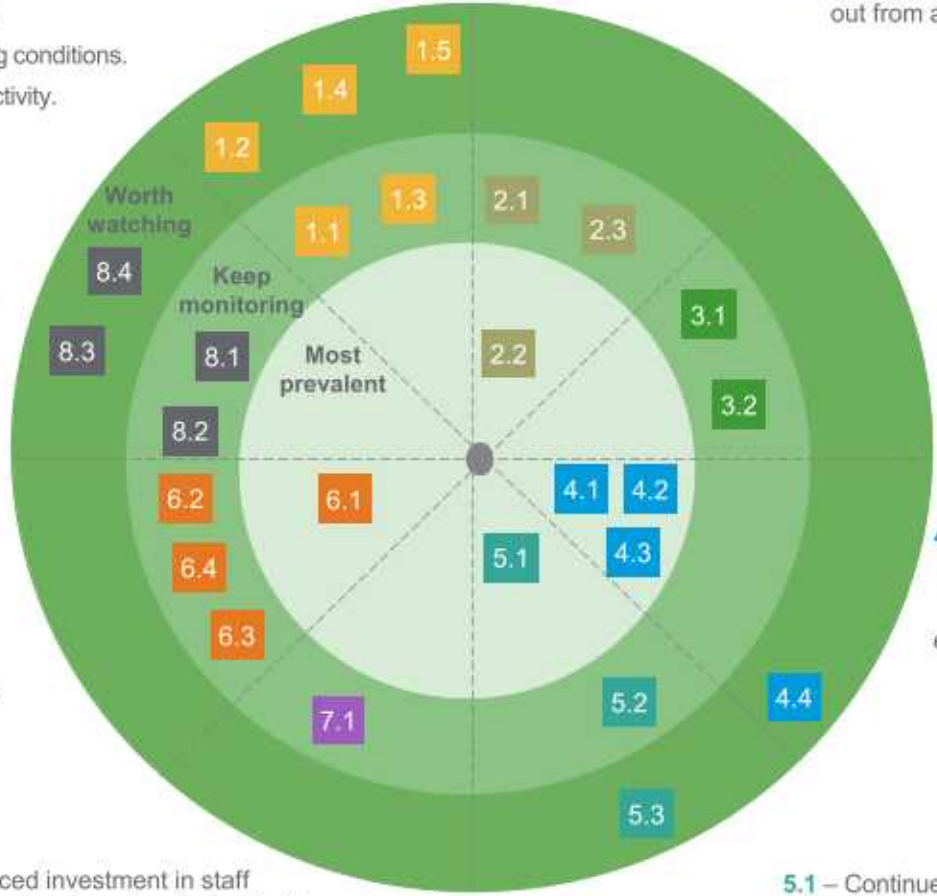
6.2 – Supply chain resilience across all ranges of goods and services, including supply chain visibility.

6.3 – Access to and availability of finance and funding including cost of finance and funding changes.

6.4 – Increasing levels of fraudulent activity making use of technology as a tool for doing so, including AI.

People Resources

7.1 – Loss of access to skills, knowledge and experience – reduced investment in staff development / apprenticeships, temporary contracts more frequent, reduced pool of skilled / experienced staff available with movement between employers and increased use of AI replacing human roles.



Political, Policy and Regulation

2.1 – Change in government priorities resulting in new or changes to laws, policies, regulations affecting businesses.

2.2 – Geo-political change and instability, including potential for trade wars, fall-out from and expansion of armed conflicts and the influence on society and business.

2.3 – Increasing level of regulation, compliance and inspection.

Environmental

3.1 – Ability to effectively engage with and leverage off the sustainability agenda.

3.2 – Increasing weather pattern shifts / extreme weather impacting businesses productivity and continuity / recovery of operations.

Technological

4.1 – Cyber-attacks increasing in frequency and complexity.

4.2 – Artificial Intelligence (AI) governance lag – increasing use of and reliance on AI without sufficient checks and balances.

4.3 – Operational resilience of technology increasingly threatened e.g. power outage, IT infrastructure age, cost of maintenance / lack of investment, sabotage etc.

4.4 – **NEW** Misinformation spread via social media platforms impacting businesses.

Commercial

5.1 – Continued economic slow-down. Persistent inflation. Reduced spending by consumers. Reduced / changes in spending by Government.

5.2 – Reduced investment in research and development, reducing agility and innovation due to macro-economic conditions.

5.3 – Various factors leading to market changes e.g. access to materials and labour, global trade restrictions, location, competition, ownership, acquisition & merger.

Emerging risk radar
Spring 2025

RSM

Societal and Community

1.1 – Availability and effectiveness of public services are reduced.

1.2 – Increasing awareness of mental health and physical well-being issues.

1.3 – Societal tensions stemming from, by example, racial, ethnicity, diversity, wealth, age, and cultural extremes.

1.4 – Access to affordable housing, homelessness and poor housing conditions.

1.5 – Epidemic / further pandemic impacting public health / productivity.

Governance

8.1 – Tick box governance – lip service to standards / codes, lack of transparency in decision making, conflicts of interest justified, and loss of accountability.

8.2 – Developing the board capacity and capability – fitness for future.

8.3 – Shifts in business culture due to external influence and attitudes.

Economic and Financial

6.1 – Shifts in employee costs, energy costs etc.

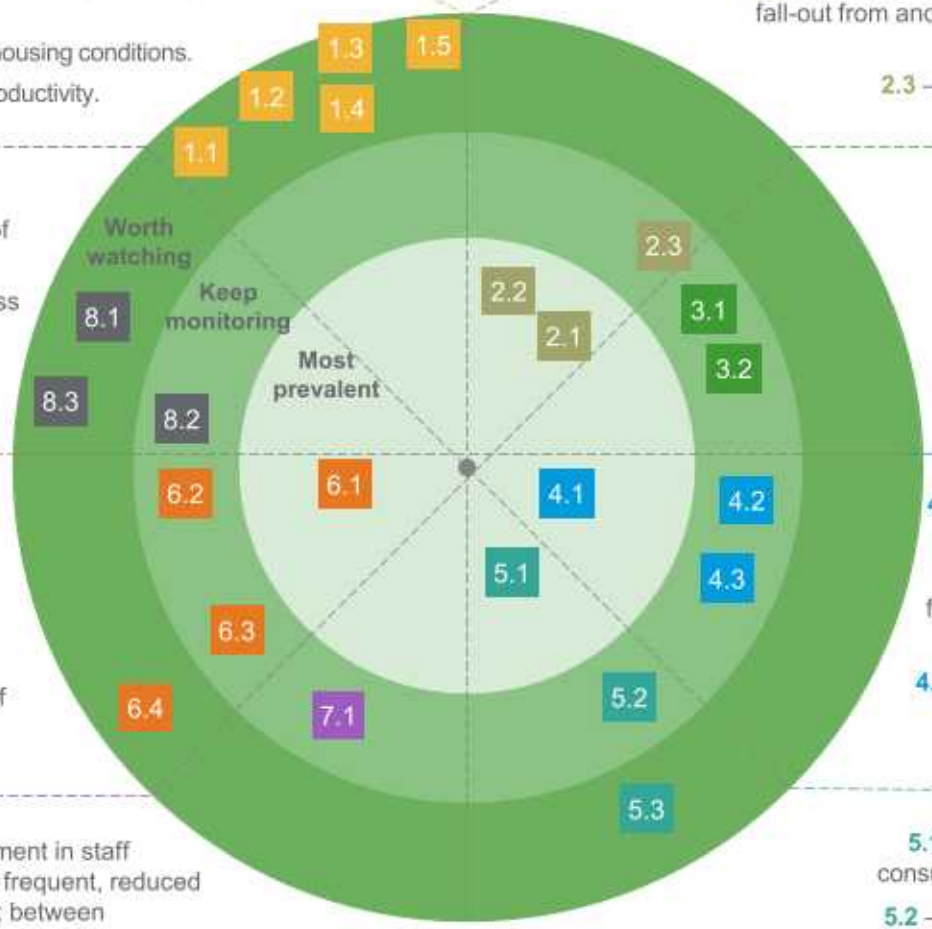
6.2 – Supply chain resilience across all ranges of goods and services.

6.3 – Access to and availability of finance and funding including cost of finance and funding changes.

6.4 – Increasing levels of fraudulent activity making use of technology as a tool for doing so.

People Resources

7.1 – Shortages in skills and experience – reduced investment in staff development / apprenticeships, temporary contracts more frequent, reduced pool of skilled / experienced staff available with movement between employers.



Political, Policy and Regulation

2.1 – Change in government priorities resulting in new or changes to laws, policies, regulations affecting businesses.

2.2 – Geo-political change and instability, including potential for trade wars, fall-out from and expansion of armed conflicts and the influence on society and business.

2.3 – Increasing level of regulation, compliance and inspection.

Environmental

3.1 – Ability to effectively engage with and leverage off the sustainability agenda.

3.2 – Increasing weather pattern shifts / extreme weather impacting businesses and supply chain (nationally and globally).

Technological

4.1 – Cyber-attacks increasing in frequency and complexity.

4.2 – Digital transformation including Impact of artificial intelligence on business – capacity, capabilities and funding available to understand, keep-up with, explore and develop digital.

4.3 – Operational resilience of technology e.g. power outage, IT infrastructure age, sabotage etc.

Commercial

5.1 – Continued economic slow-down. Reduced spending by consumers and reduced / changes in spending by Government.

5.2 – Reduced investment in research and development due to macro-economic conditions.

5.3 – Access to markets - global trade embargos, restrictions, tariffs and competition.

Further insights

Insight4GRC™
RSM's Governance, Risk Management and Compliance Digital Solution.
www.insight4grc.com

4risk: https://youtu.be/12NyJhSNK3o

4action: https://youtu.be/xEuFSwzbzvw

4policies: https://youtu.be/ufXYt1juwhA

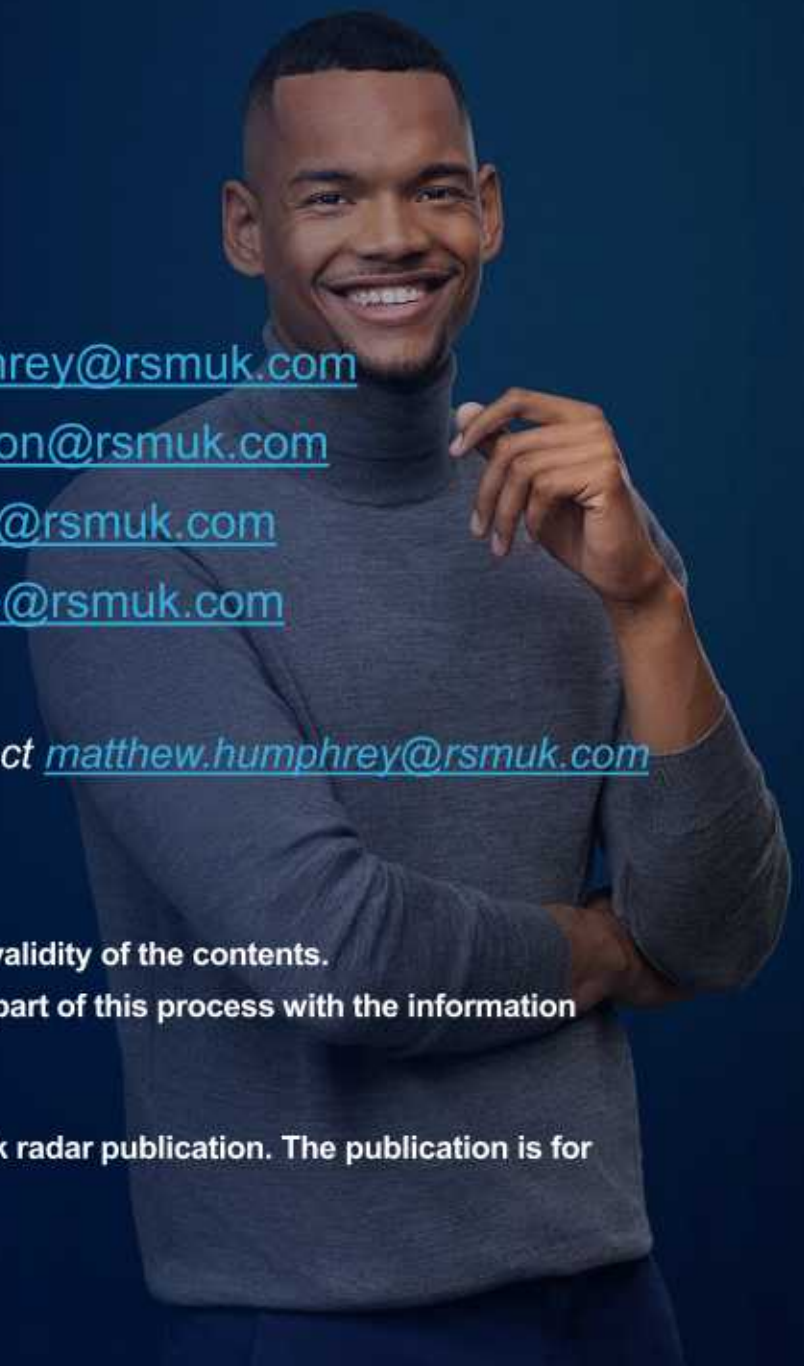
4questionnaires: https://youtu.be/NW17EoRJsjs

This is our 6th emerging risk radar publication. We know from feedback that this lands well with boards and management in all sectors, with the publication being used for comparison with existing risk information, as well as helping strengthen and improve controls and risk mitigation plans, with the publication often being used to stimulate board, committee and management discussion – including at away days as part of board and organisation development. We are now offering a facilitated emerging risk discussion / workshop so that individual businesses may get more from the emerging risk radar. If you would like to know more about this service then please make contact.

Contact

Matt Humphrey, Risk & Governance Consulting Partner Matthew.Humphrey@rsmuk.com
Howard Munson, Risk & Governance Consulting Director Howard.Munson@rsmuk.com
Adam Lickorish, Risk & Governance, Associate Director Adam.Lickorish@rsmuk.com
Richard Mackie, Risk & Governance, Associate Director Richard.Mackie@rsmuk.com

If you would like to participate in the next emerging risk radar survey, please contact matthew.humphrey@rsmuk.com



Note re contents of the emerging risk radar:

- **This is not subject to any form of validation. RSM cannot guarantee the completeness, accuracy or validity of the contents.**
- **The content is based on the views of board members and others with whom RSM have interacted as part of this process with the information gathered being collated, interpreted and summarised by RSM.**
- **The views are not necessarily representative of all sectors.**
- **There is no relationship of any kind created between RSM and the recipient / user of the emerging risk radar publication. The publication is for purposes of reference, compare, contrast and discussion as required by the recipient / user.**

Failure to Prevent Fraud

1 September 2025

The government issued guidance on the new corporate offence of failure to prevent fraud (under s199 of the Economic Crime and Corporate Transparency Act), on 6 November 2024.

Relevant organisations must implement fraud prevention procedures or risk an unlimited fine.

What organisations are in scope?

The offence applies to '**large organisations**', defined in the legislation as those meeting at least two of the following conditions, a turnover of more than £36m, more than £18m in total assets, or more than 250 employees. It also applies to their **subsidiaries** regardless of where the organisation is headquartered or where subsidiaries are located.

However, **smaller organisations** should be aware that they may fall under the definition of an 'associated person' (a person or entity whose actions, in effect, may lead to the prosecution of a large organisation) while they provide services for or on behalf of large organisations. In these circumstances, small organisations may be subject to contractual or other requirements imposed by large organisations in respect of the failure to prevent fraud offence.

Recap on the offence

A relevant organisation will be criminally liable where a specified fraud offence is committed by a person associated with the organisation (such as an employee or agent) with the **intention** of **benefiting** the organisation or its clients. If the organisation is a victim of the offence, it is not criminally liable.

It is a strict liability offence, meaning that there is no requirement to prove the organisation, or its senior managers had any prior knowledge of the fraud, for the offence to be committed.

The definition of a 'specified fraud offence' (or 'base fraud') captures the fraud and false accounting offences most relevant to large organisations, such as fraud by false representation, false accounting, false statements by company directors and cheating the public revenue.

How does a large organisation defend itself?

The only defence is that at the time of the offence, the organisation had reasonable fraud prevention procedures in place. Failure to implement a robust, proportionate fraud prevention framework may lead to dire consequences for a large organisation – the maximum penalty for a conviction under the offence is an unlimited fine.

Organisations need to act now

The focus on fraud committed for the intended **benefit** of the organisation is significant and may mean that existing fraud risk assessments and associated procedures are no longer sufficient to meet the requirements of the new legislation. Up until now, organisations have generally concentrated their attention and resources on fraud that could harm their businesses. The new legislation means that organisations should review their existing fraud prevention frameworks to ensure that they are fit for purpose and could protect them from potential prosecution.

The government guidance outlines **six principles** that organisations should implement, to prevent a specified fraud offence from being committed and to protect themselves from potential prosecution for the failure to prevent it. The principles are consistent with the prevention procedures already found in the other corporate 'failure to prevent' offences (bribery and the facilitation of tax evasion):

- Top level commitment.
- Risk assessment.
- Proportionate, risk-based prevention procedures.
- Due diligence.
- Communication (including training).
- Monitoring and review.

Organisations should act now to ensure that they have sufficient time to undertake the fraud risk assessment and make the appropriate changes, to rely on the defence by 1 September 2025.

Organisations may already have existing procedures for investigating frauds or attempted frauds against them. However, it is likely that they need to extend them to cover frauds that are intended to benefit the organisation.

Questions to consider:

- Could your organisation be in scope of this offence?
- Do you have a steering committee set up to drive this agenda?
- Have you commenced a risk assessment to consider fraud risks as a potential beneficiary of fraud?
- Is your organisation clear on the identity of its 'associated persons'?
- Have you updated policies, communicated the approach and updated controls?

Further details please contact:

Andrea Deegan
andrea.deegan@rsmuk.com
M | +44 (0)7817 002136