



HUNTINGDONSHIRE DISTRICT COUNCIL

Internal Audit Progress Report

Corporate Governance Committee – 25 March 2025

This report is solely for the use of the persons to whom it is addressed.

To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party.

CONTENTS

Key messages.....	3
1. Final reports	5

Appendices

Appendix A: Progress against the internal audit plan 2024/25.....	8
Appendix B: Other matters	10

KEY MESSAGES

The internal audit plan for 2024/25 was approved by the Corporate Governance Committee (CGC) on 29 May 2024. This report provides an update on progress against that plan and summarises the results of the work completed by the in-house internal audit team to date.

RSM have been appointed in an interim capacity from January 2025 to assist the in-house team in the production of a 2025/26 internal audit plan, the provision of management, support and oversight of the in-house team and to prepare an annual report for 2024/25.



Since the last CGC meeting in January 2025, we have finalised the following internal audit reports:

These are:

- **Code of Procurement (Limited Assurance)**
- **Green Bin Implementation – Transfer to BAU Operations (Reasonable Assurance)**
- **Key Financial Controls (Limited Assurance)**
- **One Leisure, Poor Operation Records (Limited Assurance) [to note]**

A summary of the outcome of these reviews, are included in this report at Section 1.1 below



The following report is currently at **draft** report stage:

- Commercial Estates Rent Review Processes and Invoicing.

This report has been discussed with Officers and needs further discussion at CLT ahead of being finalised. This will be presented in final at the next meeting. **[to note]**

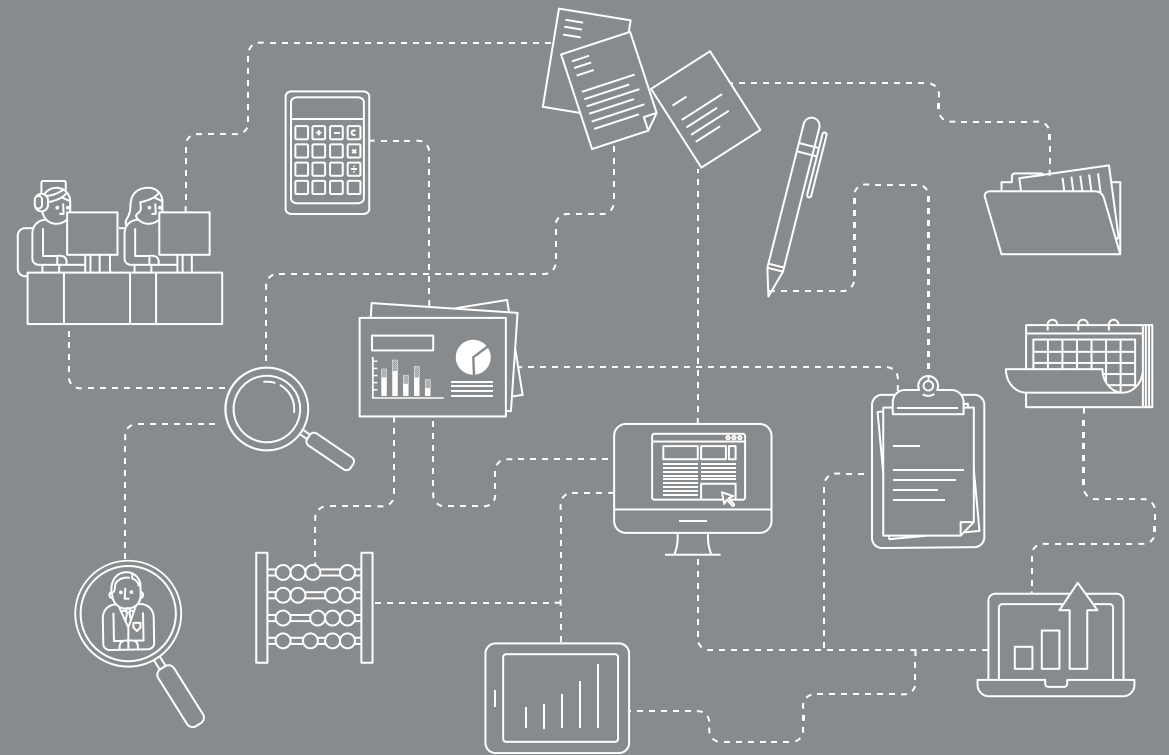


Details of the progress made against the 2024/25 internal audit plan are included at Appendix A. **[To note]**

We have completed the annual planning process for the 2025/26 internal audit plan and there is a separate paper on this item is on the agenda today. **[To note]**

Final Reports

01



1. FINAL REPORTS

1.1 Summary of the key issues arising from the final reports being presented to this Committee

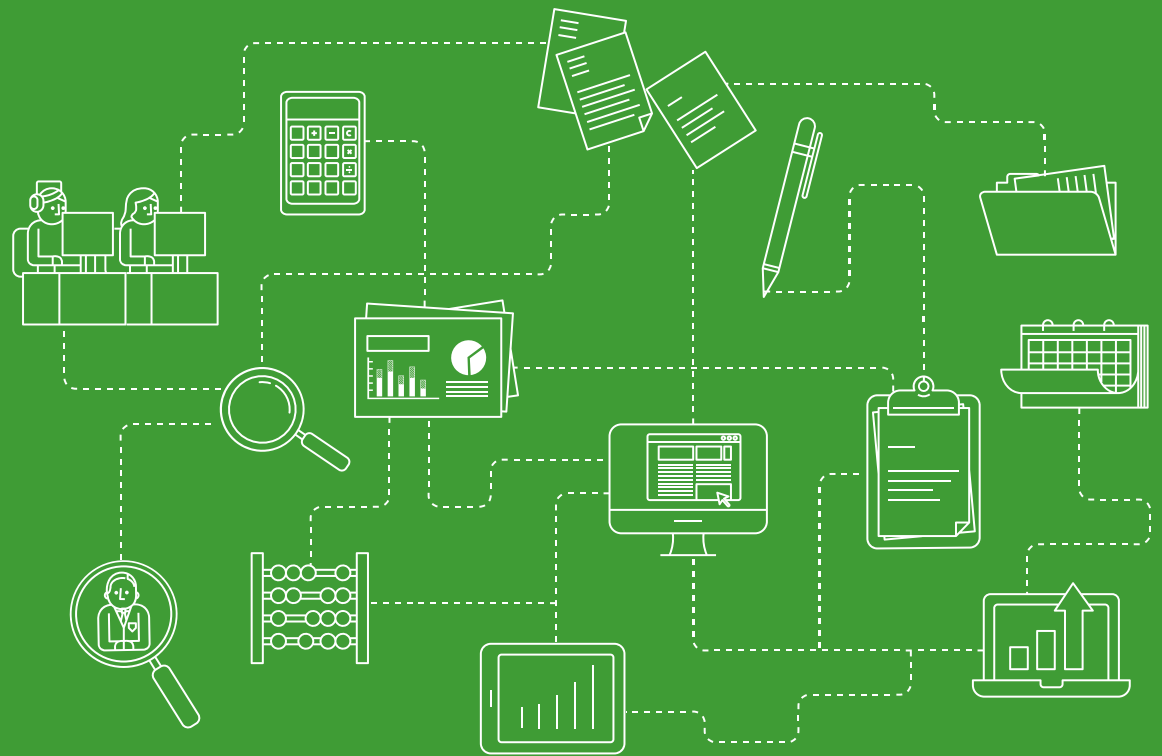
This section summarises the reports that have been finalised since the last meeting.

Assignment	Opinion issued	Actions agreed		
		L	M	H
<p>Code of Procurement</p> <p>The main issues identified from the audit are as follows:</p> <ul style="list-style-type: none"> Code of procurement and procurement procedures require review and updating in line with the new procurement act. Limited awareness of Code of procurement requirements and a lack of adequate interaction between the service teams and the procurement lead during the procurement and contract award process. Gaps in completeness of the internal contracts register. Sample checks are not periodically performed on purchases to check that sufficient written quotes have been obtained. We noted management plans to ensure all waivers and contracts let without sufficient quotes to be flagged as non-compliant for the attention of the Procurement Board. No centralised, periodic check by procurement team to review how contracts are managed post award. Formal PO approval, invitation to tender and contract award hierarchy document not evident. Procurement team is understaffed resulting in several key control activities not being performed. 	Limited Assurance	0	3	4
<p>Green Bin Implementation – Transfer to BAU Operations</p> <p>The main issues identified from the audit were as follows:</p> <ul style="list-style-type: none"> There are no process notes to cover the green bin subscription fee process from start to finish. There are no identified risks recorded on the risk register. Management we unable to locate all contracts in the contracts register. The Operations team are unaware of backup plan should the there be a break in the technology. Some specific examples of good practice we identified 	Reasonable Assurance	0	3	0

Assignment	Opinion issued	Actions agreed		
		L	M	H
<p>Key Financial Controls</p> <p>The main issues identified from the audit are as follows:</p> <ul style="list-style-type: none"> Accounts Receivable is not balancing, with discrepancies fluctuating between £54,000 to £86,000 each month. This is a known and ongoing issue. A significant portion of aged debt continues to increase, with debt over 90 days rising from £2.86m in April to £3.71m in August. This indicates that older debts are not being effectively managed or collected. The approval process for journals over £850k occurs at month-end after the journals have already been posted, allowing unapproved high-value journals to impact financial records before they are formally reviewed. 	Limited Assurance	4	7	2
<p>One Leisure Pool Operation Records</p> <p>Of 42 actions relating to pool and plant room health and safety, 25 were reported as implemented, 12 were reported as part-implemented and 2 were not implemented. 3 actions had no status update.</p> <ul style="list-style-type: none"> 8 actions were selected from the high priority actions included within the 2023/2024 health and safety audits which related to pool and plant room health and safety providing 27% coverage. Of the 8: 4 actions were reported on the action plan as 'complete', however evidence of completion could not be provided for 2 actions. 3 actions were reported as 'in progress' however 2 were verified as complete. 1 action remains underway despite an original due date for completion of 15/1/24. 1 action had no status update however this was confirmed 'complete'. The 2024/25 follow up health and safety audits reported the same findings for the 8 actions. <p>Whilst the 2024/25 follow up health and safety audits reported an overall improvement in scores across the One Leisure sites, 289 actions were recommended, of which 31 were rated major risk and 156 were rated high risk.</p> <p>There has been limited oversight and reporting over the implementation of the action plan, creating the risk that failures to address identified health and safety weaknesses are not promptly identified, escalated and remediated. During the audit, we were advised that the Business and Compliance Support Manager, who coordinated the action plan, is currently on secondment and there are no plans to fill this role.</p>	Limited Assurance	0	2	2

Appendices

02



APPENDIX A: PROGRESS AGAINST THE INTERNAL AUDIT PLAN 2024/25

Reviews shown in bold below have been finalised since the last CGC meeting.

No.	Assignment	Status / Opinion issued / Start date	Actions agreed			Original and Target CGC for final report	Actual CGC meeting
			Red	Amber	Green		
#1	Risk Management, implementation of strategy & follow up of previous actions	Deferral to 2025/26 *				-	-
#2	Minor works follow up - now Medium Term Civils Contract procurement	Final Report (No opinion) – Follow Up Assignment	0	3	0	July 2024	July 2024
#3	Budget Management; financial sustainability	Final Report - Reasonable Assurance	0	6	0	July 2024	July 2024
#4	Corp Gov Scheme of Delegations	Deferral to 2025/26 *				-	-
#5	Partnership Working	Deferral to 2025/26 *				-	-
#6	Development Management	Replaced and removed from the 2024/25 plan				-	-
#7	Home Improvement Agency	Deferral to 2025/26 *				-	-
#8	Operations Vehicle Maintenance Processes	Final Report – Reasonable Assurance	0	5	0	July 2024	July 2024
#9	All Services, Contract Management	Deferral to 2025/26 *				-	-
#10	Data Quality Standard Compliance	Deferral to 2025/26 *				-	-
#11	One Leisure, Pool Operation Records	Final Report – Limited Assurance	2	2	0	March 2025	March 2025
#12	Review of Asset Management Records, HDC properties	Replaced and removed from the 2024/25 plan				-	-
#13	Review of Commercial Estates rent review processes and invoicing	Draft Report – Discussion on findings required at CLT ahead of finalisation				March 2025	June 2025
#14	DFG Grant Verification	Final Report - No opinion as Grant Review (no report available)	0	0	0	n/a	n/a
#15	Green Bin Implementation and transfer to BAU operations	Final Report – Reasonable Assurance	0	3	0	March 2025	March 2025
#16	Green Credentials on projects already implemented	Audit removed from the plan				March 2025	-

No.	Assignment	Status / Opinion issued / Start date	Actions agreed			Original and Target CGC for final report	Actual CGC meeting
			Red	Amber	Green		
#17	Code of Procurement	Final Report – Limited Assurance	4	3	0	March 2025	March 2025
#18	Facilities Management and ICT	Not commenced **				-	-
#19	Key Financial Controls	Final Report – Limited Assurance	2	4	7	March 2025	March 2025
#20	Critical Application Security	Not commenced **				-	-
#21	Follow ups, previous ICT actions	Not commenced **				-	-
#22	Immutable Back ups	Not commenced **				-	-
#23	IT Governance and Strategy	Not commenced **				-	-
#24	Home and Hybrid Working	Fieldwork in progress				June 2025	-
#25	Committee Governance Structure	Fieldwork in progress				June 2025	-
#26	Follow Up	Fieldwork in progress				June 2025	-
#27	Cyber Essentials Readiness	Fieldwork in progress				June 2025	-

* These reviews have been deferred by the previous Internal Audit Manager (Head of Internal Audit) prior to RSM commencing our role. We understand that these changes have not been reported through to the CGC for information or approval.

** These IT reviews have not been completed during this financial year. RSM has been informed that historically IT reviews were completed by an outsourced provider, however for the current financial year they have not been delivered.

APPENDIX B: OTHER MATTERS

Detailed below are the changes to the 2024/25 internal audit plan since the previous meeting of the CGC in January 2025:

Note	Auditable area	Reason for change
1	Home and Hybrid Working Advisory Review (replaces the Development Management)	The CEO and Section 151 Officer requested we complete this review as it would add more value than the audit contained within the original 2024/25 IA plan.
2	Committee Governance Structure (replaces Asset Management Records, HDC properties)	The CEO and Section 151 Officer requested we complete this review as it would add more value than the audit contained within the original 2024/25 IA plan.

Detailed below are the changes to the 2024/25 internal audit plan reported to the previous meeting of the CGC in January 2025:

Note	Auditable area	Reason for change
1	Audits deferred from 2024/25 plan: <ul style="list-style-type: none"> Risk Management, implementation of strategy & follow up of previous actions Corp Gov Scheme of Delegations All Services, Contract Management Partnership Working All Services, Contract Management Data Quality Standard Compliance 	<p>RSM has been informed that six audits from 2024/25 have been (informally) deferred by the previous internal audit manager during the current financial year.</p> <p>Of these six reviews, four had previously been deferred from the 2023/24 internal audit plan.</p>
2	Audits not commissioned from external specialists from 2024/25 plan: <ul style="list-style-type: none"> Facilities Management and ICT Critical Application Security Follow Ups, previous ICT actions Immutable Backups IT Governance and Strategy 	<p>Five IT reviews previously planned have not yet been delivered during 2024/25. Historically HDC commissioned these reviews externally.</p> <p>RSM is currently in discussions with the Section 151 Officer with regards to provision of a technology risk assignment for the 2024/25 internal audit plan.</p>
3	Additional Audits to be delivered in Q4 2024/25: <ul style="list-style-type: none"> IT Key Control / Cyber Essentials Follow Up of previous actions / recommendations 	RSM have agreed with the Section 151 Officer to undertake two reviews in Q4 of 2024/25 to provide some assurance around the key IT / Cyber controls in place at the Council and to undertake an independent review of previously agreed management actions / recommendations and provide some assurance that these issues and risks identified are being mitigated.

Compliance with Public Sector Internal Audit Standards (PSIAS)

Previously reported to the January 2025 CGC meeting:

Each Local Authority (and the internal audit team) is required to comply with the PSIAS. Under the standards, internal audit services are required to have an external quality assessment (EQA) every five years. We understand from our enquiries and review of previous CGC papers that two different self-assessments were undertaken by previous in-house Heads of Internal Audit, and that the Local Government Association (LGA) also undertook a peer review of governance processes in 2023/24, assessed against CIPFA's "Unlocking Internal Audit Potential" report, to provide insight into the effectiveness of the Council's arrangements', including an independent review of the internal audit service. However, from our enquiries we do not believe that a formal EQA has been commissioned for at least seven years. The peer review was reported to the CGC in July 2024 and highlighted some important areas that have historically come under the responsibility of Internal Audit but should be considered for separation in order that Internal Audit is able to independently review and report (for example, Whistleblowing, AGS)).

We understand that the Council commissioned an independent EQA readiness review in 2024/25 (final report issued in August 2024). This identified a number of significant gaps with EQA readiness in key areas, raising four high and two medium actions. It also concluded that these improvement areas needed to be addressed in preparation for an EQA. We have been advised that a number of these actions and improvement areas remain outstanding.

We have already concluded, based on the EQA readiness assessment report produced by BDO and the gaps identified that the team have not fully met the Public Sector Internal Audit Standards (PSIAS) in 2024/25 (for example we are not aware that any of the 4 high and 2 medium recommendations have been implemented).

We have already flagged a clarification point we need to discuss and resolve with the S151 Officer in relation to compliance with the PSIAS in 2025/26 (and new Global Internal Audit Standards – effective 1 January 2025). RSM audits will be fully compliant with the new standards, but we need to hold further discussions in relation to the work delivered by the in-house team, and how to ensure compliance with the standards in 2025/26.

Please note that in relation to work delivered by RSM:

The RSM UK Risk Assurance service line commissioned an external independent review of our internal audit services in 2021, to provide assurance as to whether our approach continues to meet the requirements. The external review concluded that RSM 'generally conforms* to the requirements of the IIA Standards' and that 'RSM IA also generally conforms with the other Professional Standards and the IIA Code of Ethics. There were no instances of non-conformance with any of the Professional Standards'.

* The rating of 'generally conforms' is the highest rating that can be achieved, in line with the IIA's EQA assessment model.

Annual Report 2024/25

Previously reported to the January 2025 CGC meeting:

We understand from reviewing the previous three financial years annual reports that 'Limitations of Scope' have been applied to the Head of Internal Audit opinions and the annual reports. Some of these limitations of scope have been due to resourcing (ie a lack of resource to undertake enough work to provide an opinion on risk management and governance).

The above prior year limitation of scopes, combined with the limited amount of work delivered to date in relation to the 2024/25 internal audit plan, the number of reviews deferred to 2025/26 (some of which were deferred from 2023/24) and the likely non-compliance during 2024/25 with PSIAS has resulted in our advice to the S151 Officer and wider Executive Team that we will issue a limitation of scope position statement within the 2024/25 annual report across Risk Management, Governance and Internal Control.

We have developed a risk-based plan of work for 2025/26 that will commence in April 2025. It is submitted for approval by the committee at the March 2025 meeting.

Information and briefings

RSM has appended the following client briefings as information for members and officers:

- Emerging Risk Radar – Spring 2025
- Global Internal Audit Standards – January 2025 briefing
- Failure to Prevent Fraud Briefing

FOR FURTHER INFORMATION CONTACT



Dan Harris, Partner and Acting Head of Internal Audit

Email: Daniel.Harris@rsmuk.com

Telephone: 07792 948767



Alastair Foster, Managing Consultant

Email: Alastair.Foster@rsmuk.com

Telephone: 01908 687800

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of Huntingdonshire District Council, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM UK Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM UK Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.

Emerging Risk Radar

Emerging risk considerations

Spring 2025



Emerging Risk Radar – Spring 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 **129 survey responses** from board members across all industries/sectors as well as drawing on our current emerging risk knowledge.

Key emerging risks in summary

There are 24 emerging risks identified, an increase of 6 since the last publication. New emerging risks in the form of **increasing levels of regulation, technology resilience, access to markets, technology fraud, shifts in business culture and potential for an epidemic** – impacting both private, public and not for profit sectors. In addition, there have been updates in previous emerging risks.

5 emerging risks identified as more prevalent (4 less since the last emerging risk radar publication), with **geo-political instability, change in government priorities, cyber attacks, continued economic slow down** and **financial planning uncertainties**. No change in these emerging risks since the previous emerging risk publication.

The top 3 most prevalent emerging risks:

01

Changes in government priorities

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

02

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.

03

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.

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

01

What do you see as the emerging risks?

02

How far will these emerging risks affect your business?

03

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

04




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

05






How will you respond?
How will you continue to review the emerging risks?



Emerging areas of risk – Spring 2025

Consistent 
 Increasing 
 Decreasing 

Direction of travel since previous emerging risk radar publication.

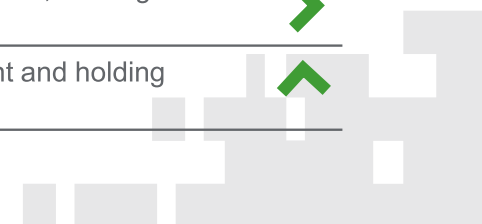
Most prevalent		
2.1	Change in government priorities resulting in new or changes to laws, policies, regulations affecting businesses.	
2.2	Geo-political change and instability, including potential for trade wars, fall-out from and expansion of armed conflicts and the impact on businesses and society.	
4.1	Cyber-attacks increasing in frequency and complexity. Unable to sufficiently invest in defence – attacks more disruptive and disabling, coupled with loss / theft of data in serious targeted attacks.	
5.1	Continued economic slow-down. Reduced spending by consumers and reduced / changes in spending by Government.	
6.1	Shifts in employee costs, energy costs etc. Creating financial pressure, forecasting and planning uncertainties	



Emerging areas of risk – Spring 2025

Direction of travel since previous emerging risk radar publication.

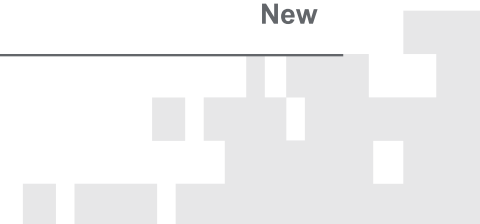
Keep monitoring		
2.3	NEW: Increasing level of regulation, compliance and inspection. e.g. Economic Crime and Corporate Transparency Act etc.	New
3.1	Ability to effectively engage with and leverage off the sustainability agenda, including ability to meet green agenda targets (coupled with potential for Green Washing).	✓
3.2	Increasing weather pattern shifts / extreme weather impacting the UK (and globally) – storms, floods, temperature changes impacting supply chains, productivity and continuity / recovery of operations.	➤
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	NEW: Operational resilience of technology e.g. power outage, IT infrastructure age, sabotage etc	New
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.	✓
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.	✓
6.2	Supply chain resilience across all ranges of goods and services.	➤
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.	➤
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 – Spring 2025

Direction of travel since previous emerging risk radar publication.

Worth watching		
1.1	Availability and effectiveness of public services are reduced due to under investment, lack of resources and increased demand from the public.	➤
1.2	Increasing awareness of mental health and physical well-being issues impacting individuals stemming from post pandemic fall-out, increasing poverty etc. Impacting on public services and employers (as well as having potential duty of care implications).	➤
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. 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.	➤
1.5	NEW: Epidemic / further pandemic impacting public health / productivity.	New
5.3	NEW: Access to markets - global trade embargos, restrictions, tariffs and competition.	New
6.4	NEW: Increasing levels of fraudulent activity making use of technology as a tool for doing so.	New
8.1	Tick box governance – lip service to standards / codes, lack of transparency in decision making, conflicts of interest justified, and loss of accountability creating a loss of trust.	▼
8.3	NEW: Shifts in business culture due to external influence and attitudes.	New



Emerging Risk Radar Spring 2025

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

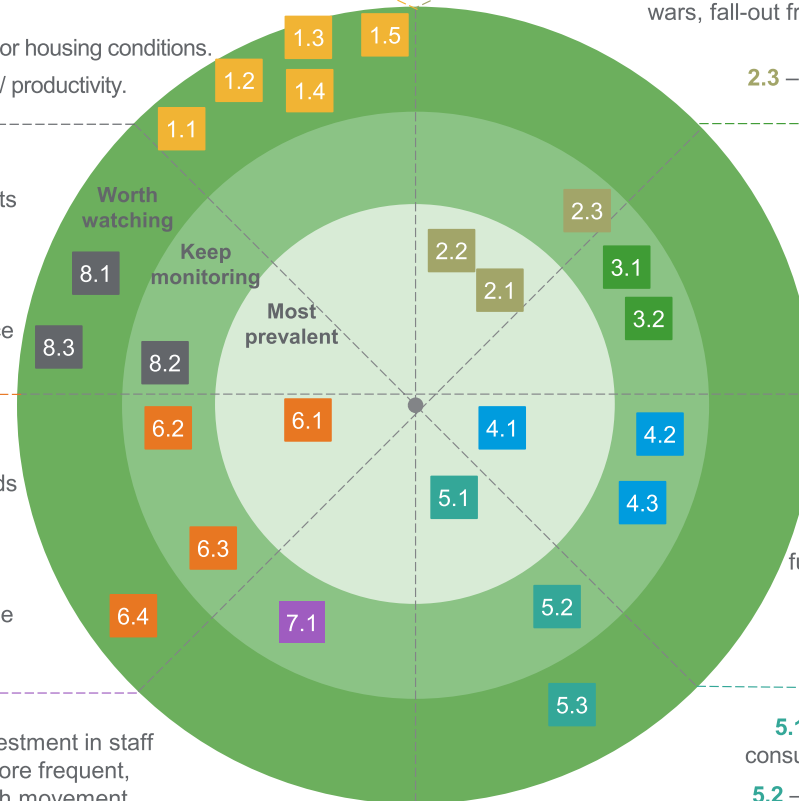
- 3.1 – Ability to effectively engage with and leverage off the sustainability agenda.
- 3.2 – Increasing weather pattern shifts / extreme weather impacting businesses and supply chain (nationally and globally).

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.



Previous Emerging Risk Radar Summer 2024

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 – Homelessness and poor housing conditions.

Governance

- 8.1 – Tick box governance. Lack of transparency in decision making, conflicts of interest justified, and loss of accountability and trust.
- 8.2 – Maintaining board member capacity and capability – fitness for future.

Economic and Financial

- 6.1 – Shifts in inflation, interest rates, salaries and wages, energy costs.
- 6.2 – Availability of supplies leading to increased costs across all ranges of materials.
- 6.3 – Access to and availability of finance and funding including cost of finance and funding changes

People Resources

- 7.1 – Shortages in skills and experience – reduced investment in staff development, temporary contracts more frequent, reduced pool of skilled staff with movement between employers and increasing lack of commitment to longer term career.

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 instability, including fall-out from and expansion of conflicts and the influence on society.

Environmental

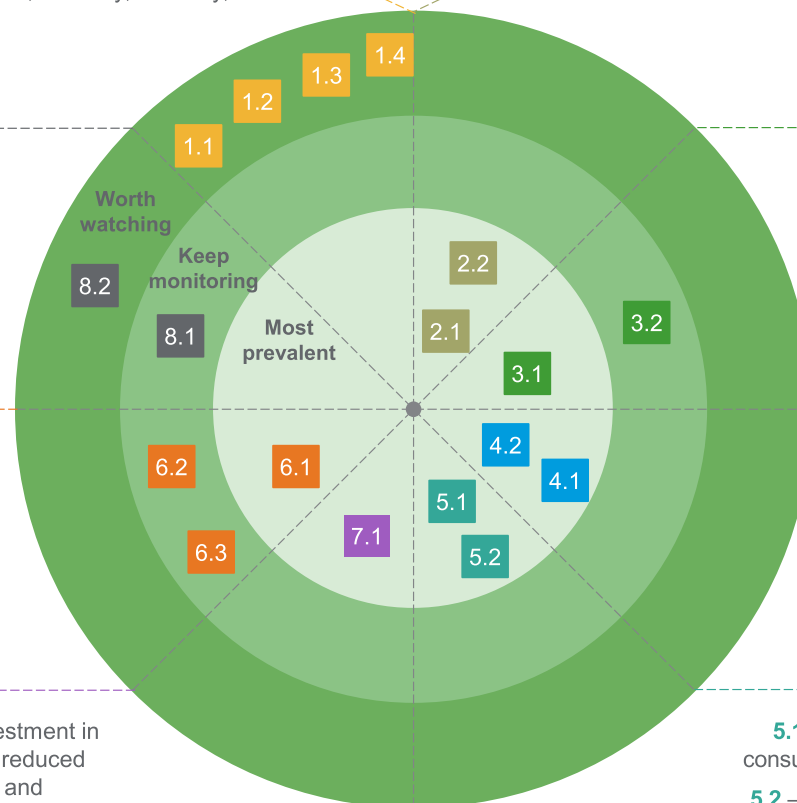
- 3.1 – Ability to effectively engage and leverage off the sustainability agenda.
- 3.2 – Increasing weather pattern shifts / extreme weather impacting the UK (and globally).

Technological

- 4.1 – Cyber-attacks increasing in frequency and complexity.
- 4.2 – Impact of artificial intelligence both positive and negative implications.

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.



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>

Contact

Matt Humphrey

Risk & Governance Consulting Partner

Matthew.Humphrey@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.

Application Note Global Internal Audit Standards in the UK Public Sector

January 2025

Global Internal Audit Standards in the UK Public Sector

The Application Note 'Global Internal Audit Standards in the UK Public Sector' is being adopted by the Relevant Internal Audit Standard Setters (RIASS) from 1 April 2025. It follows a period of consultation, and on the advice of the UK Public Sector Internal Audit Standards Advisory Board (IASAB), the Application Note should be applied in conjunction with the Global Internal Audit Standards published by the Institute of Internal Auditors. It includes key requirements and interpretations that are crucial for implementing the Standards within the practice of internal audit in the UK public sector.

Overview of the Standards

The RIASS have determined the Global Internal Audit Standards are 'a suitable basis for the practice of internal auditing', subject to interpretations and requirements. Whilst the section on 'Applying the Global Internal Audit Standards in the Public sector' is welcome, the Application Note provides UK public sector specific context and additional requirements.

Internal auditors must adhere to the requirements of the Global Internal Audit Standards and the International Professional Practices Framework. Throughout 2024, internal audit providers have been transitioning to the Standards, which became effective on 9 January 2025. The current Public Sector Internal Audit Standards have been in place since 2017. From 1 April 2025, auditors in the public sector must adhere to the Application Note, in addition to the requirements of the Global Internal Audit Standards.

The IASAB will periodically review the Application Note. This includes consideration of any Topical Requirements that are relevant to the public sector.

We have published several client briefings on the Global Internal Audit Standards and the requirements.

- Overview of the Global Internal Audit Standards.
- Quality Assurance and Improvement Programme.
- Key Stakeholder Requirements in Domain III.
- Assessing Readiness and Action Plans.

Please get in touch with your usual RSM contact to request a copy.

Global Internal Audit Standards in the UK Public Sector

Key interpretations and requirements

The Application Note includes several requirements and interpretations in the context of the UK public sector, summarised as follows.

- Alongside the requirements in the Global Internal Audit Standards in Domain II: Ethics and Professionalism, internal auditors must apply the Seven Principles of Public Life (the 'Nolan Principles').
- Auditors in the UK public sector need to understand when they are required to share or publish information. They should be familiar with their organisation's policies and procedures for publishing certain information, as well as any statutory obligations to do so.
- In meeting the requirements of Standard 9.1 Understanding Governance, Risk Management and Control Processes and Standard 13.4 Evaluation Criteria, auditors must recognise the importance of value for money.
- With the legal and regulatory structures across the public sector, where the chief audit executive is unable to co-ordinate with other assurance providers, the barriers must be set out to the board.
- Where a board does not have authority over budgets, this can hinder the chief audit executive's ability to seek additional funding due to other organisational priorities. To comply with Standard 8.2 Resources, the chief audit executive should develop a resource strategy that proposes practical solutions for the board's consideration.
- Where the chief audit executive is unable to develop a strategy to obtain sufficient resource to address shortfalls, there is no expectation to comply with Standards 10.1 to 10.3, Principle 10 Manage Resources. The chief audit executive must inform the board of the effect of insufficient resources and highlight any options to mitigate the impact. If internal audit's ability to fulfil its mandate is at risk, the board must also be informed.
- The chief audit executive must provide an overall conclusion on governance, risk management and control annually, with the conclusion informing internal audit planning in alignment with Standard 9.4.
- The results of internal quality assessments are to be reported annually and include any action plans to address non-conformance.
- The chief audit executive is to be qualified, holding a professional qualification such as CMIIA, CCAB or other equivalent qualification that includes training on the practice of internal audit. They should also have suitable experience.
- At least one individual within the external quality assessment (EQA) team should hold the skills and qualifications as that required of the chief audit executive. An EQA assessor is expected to understand the Global Internal Audit Standards in line with an individual with the Certified Internal Auditor designation, including how the standards are applied to the UK public sector.

Domain III Governing the Internal Audit Function sets out important 'essential conditions' for the board and senior management. When implemented they enable the internal audit function to be effective and fulfil its purpose. Given the unique governance and organisational structures in the public sector, internal audit functions may need to adapt some standards to achieve the same outcomes. These alternatives must be approved by the board or audit committee and, if permanent, must be explained in the Charter.

Global Internal Audit Standards in the UK Public Sector

Our internal audit services

In transitioning to the Global Internal Audit Standards, during 2024 we have updated our manuals, reports, charter and mandate, and trained our people. This ensured our preparedness and conformance with the new standards.

As a leading provider of internal audit services to the public sector we have carefully considered the requirements of the Application Note Global Internal Audit Standards in the UK Public Sector. With the Public Sector Internal Audit Standards being replaced, our charter and reports will be updated, applicable from 1 April 2025.

Having reviewed the interpretations and requirements, our internal audit services align with the intent of the Global Internal Audit Standards in the UK Public Sector.

Our last EQA concluded that RSM 'generally conforms to the requirements of the IIA Standards' and that 'RSM IA also generally conforms with the other Professional Standards and the IIA Code of Ethics. There were no instances of non-conformance with any of the Professional Standards'. The rating of 'generally conforms' is the highest rating that can be achieved, in line with the IIA's EQA assessment model. Our next EQA is due to take place in 2026 and will reflect the requirements of the Global Internal Audit Standards in the UK Public Sector.

Further information

Access the Application Note Global Internal Audit Standards in the UK Public Sector at: <https://www.iasab.org/standards>

Access the Global Internal Audit Standards at: <https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/>

Should you have any questions regarding the Global Internal Audit Standards in the UK Public Sector, what it might mean for you, or our adherence to the Standards, please get in touch via your usual RSM contact.

FURTHER INFORMATION

Mark Jones

RSM Head of Internal Audit

mark.jones@rsmuk.com

Shauna Mallinson

Head of Risk and Governance Technical

shauna.mallinson@rsmuk.com

rsmuk.com

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM UK Corporate Finance LLP, RSM UK Restructuring Advisory LLP, RSM UK Risk Assurance Services LLP, RSM UK Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP, and RSM UK Tax and Accounting Limited are not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services because we are licensed by the Institute of Chartered Accountants in England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide. RSM UK Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317, to undertake reserved and non-reserved legal activities. It is not authorised under the Financial Services and Markets Act 2000 but is able in certain circumstances to offer a limited range of investment services because it is authorised and regulated by the Solicitors Regulation Authority and may provide investment services if they are an incidental part of the professional services that it has been engaged to provide. Whilst every effort has been made to ensure accuracy, information contained in this communication may not be comprehensive and recipients should not act upon it without seeking professional advice.

Failure to Prevent Fraud

Countdown to 1 September 2025

RSM

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 prior to the offence coming into force on **1 September 2025** 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

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London, EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM UK Corporate Finance LLP, RSM UK Legal LLP, RSM UK Restructuring Advisory LLP, RSM UK Risk Assurance Services LLP, RSM UK Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP and RSM UK Creditor Solutions LLP are limited liability partnerships registered in England and Wales, with registered numbers OC325347, OC402439, OC325349, OC389499, OC325348, OC325350, OC397475 and OC390886 respectively. RSM UK Employer Services Limited, RSM UK Tax and Accounting Limited and RSM UK Management Limited are registered in England and Wales with numbers 6463594, 6677561 and 3077999 respectively. All limited companies and limited liability partnerships are registered at 6th Floor, 25 Farringdon Street, London, EC4A 4AB. The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm which practises in its own right. The RSM network is not itself a separate legal entity in any jurisdiction.

