

**FOR PUBLICATION**

**DERBYSHIRE COUNTY COUNCIL**

**AUDIT COMMITTEE**

**5 December 2023**

**Director of Finance & ICT**

**Overview of Finance & ICT Risks**

**1. Purpose**

- 1.1 Background information for the Audit Committee's review of Finance & ICT risks.

**2. Information and Analysis**

- 2.1 The Audit Committee is conducting a rolling programme to review risk management arrangements directly with Executive Directors.
- 2.2 This item offers the audit committee the opportunity for a deeper dive into one part of Corporate Services & Transformation (CST) – Finance & ICT - following the broad overview of CST risk management recently provided to the committee by Joe O'Sullivan (Executive Director, CST). Mark Kenyon (Director of Finance & ICT) will attend for this item. Mark will give a short overview of risk management in his department, followed by questions and discussion with the committee members.
- 2.3 Finance & ICT owns three risks on the current strategic risk register. The risks are listed below with full details (updated to 2023-24 Quarter 2) provided in Appendix 2:
- Impact of a prolonged recovery and a funding gap
  - Failure to manage contracts across the county council
  - Information governance and data security
- 2.4 The full Finance & ICT risk register (updated to 2023-24 Quarter 2) is provided for background information in Appendix 3. This is an abridged

version of the data held on APEX. A full version of the register with all data can be provided to the committee if required.

### **3. Alternative Options Considered**

- 3.1 This is a regular rolling review of departmental risk management by the Audit Committee.

### **4. Implications**

- 4.1 Implications are discussed in Appendix 1.

### **5. Consultation**

- 5.1 No formal consultation was undertaken in the preparation of this report. The risk register was prepared by the CST department.

### **6. Background Papers**

- 6.1 Electronic files held by Risk and Insurance, Finance & ICT Services, County Hall Complex.

### **7. Appendices**

- 7.1 Appendix 1 – Implications
- 7.2 Appendix 2 – Finance & ICT strategic risks (on strategic risk register)
- 7.3 Appendix 3 – Finance & ICT risk register 2023-24 (abridged version)

### **8. Recommendations**

That the Audit Committee:

- a) Reviews the information provided in this paper for discussion with Mark Kenyon.

### **9. Reasons for recommendations**

- 9.1 The Audit Committee is charged with providing risk management assurance within the Council.

#### **Report Author:**

**Tony Kearsey**

Finance Officer (Corporate Risk)

#### **Contact details:**

tony.kearsey@derbyshire.gov.uk

### **Implications**

#### **Financial**

- 1.1 Financial implications are noted in the strategic and departmental risks where applicable in Appendix 2 and Appendix 3.

#### **Legal**

- 2.1 Legal implications are noted in the strategic and departmental risks where applicable in Appendix 2 and Appendix 3.

#### **Human Resources**

- 3.1 Human resources implications are noted in the strategic and departmental risks where applicable in Appendix 2 and Appendix 3.

#### **Information Technology**

- 4.1 Information technology implications are noted in the strategic and departmental risks where applicable in Appendix 2 and Appendix 3.

#### **Equalities Impact**

- 5.1 Equalities impact implications are noted in the strategic and departmental risks where applicable in Appendix 2 and Appendix 3.

#### **Corporate objectives and priorities for change**

- 6.1 The strategic risk register, departmental risk registers and corporate risk management strategy underpin the successful delivery of the Council's objectives and deliverables set out in the Council Plan and service delivery plans.
- 6.2 The council's corporate risk management strategy is designed to strengthen risk management arrangements to underpin improved performance across the Council, and to deliver greater public value from its work.

#### **Other (for example, Health and Safety, Environmental Sustainability, Property and Asset Management, Risk Management and Safeguarding)**

- 7.1 All other implications are noted in the strategic and departmental risks where applicable.

## Strategic Risk Register

2023-24 Quarter 2 (30 September 2023)

## Extract – Finance &amp; ICT risks

## Impact of a prolonged recovery and a funding gap

In the event that the Authority does not develop sufficient and timely proposals to deal with the ongoing or further reductions in funding/resources, there is a risk that the need to close the funding gap may result in identifying measures for unplanned reductions in service spend leading to deterioration or interruption of front-line service delivery.

APEX Unique Risk Number (URN): 518

**Risk Owner:** Mark Kenyon, Director of Finance & ICT

## Assessment history:

Target	Likelihood: Probable (4)	2022-23 Q2	2023-23 Q3	2022-23 Q4	2023-24 Q1	2023-24 Q2	Likelihood: Almost certain (5)
Amber (12) by 20/09/23	Impact: Moderate (3)	Red (25)	Red (25)	Red (25)	Red (25)	Red (25)	Impact: Substantial (5)

**Reputation impact assessment:** Moderate

**Financial impact assessment:** Band 8 (Loss over £20 million)

## APEX quarterly commentaries:

Quarter ending	Progress commentary (by risk owner)
30 September 2023	The Revenue Outturn 2022-23 was reported to Cabinet on 27 July 2023 which showed a portfolio overspend of £15m, offset by underspends on corporate budgets to give an overall underspend of £4.7m. However, this is after substantial use of £55m of the Council's earmarked reserves. Inflation continues to remain at higher than anticipated levels, with Cpi at 6.8% in July. Current forecasts suggests that the Council will be seeking further savings in 2024-25. This being a combination of in-year savings identified and savings brought forward from previous years. Inflationary and demand pressures are adding pressure to the 2023-24 revenue budget. The quarter 1 position is being considered by Cabinet on the 21 September 2023.
30 June 2023	The Revenue Outturn 2022-23 will be reported to Cabinet on 26 July 2023. Preparation is underway to review the approach to budget setting for 2024-25 with a focus on service priorities.
31 March 2023	The Council has updated its Five-Year Financial Plan alongside the setting of the Revenue Budget 2023/24 in February 2023. The update reflects the outcomes of the Local Government Finance Settlement 2023/24. The revenue and capital budgets for 2023/24 were agreed at Council on 15 February. These continue to be constrained by the

	availability of funding and continue to rely upon the use of reserves to manage the achievement of the required budget reductions.
--	--

### Failure to manage contracts across the county council

Failure to manage contracts effectively could lead to unforeseen increased costs, risk of contracts collapsing and an increased carbon footprint.

APEX Unique Risk Number (URN): 520

**Risk Owner:** Mark Kenyon, Director of Finance & ICT

#### Assessment history:

<b>Target</b>	Likelihood: Unlikely (2)	<b>2022-23 Q2</b>	<b>2023-23 Q3</b>	<b>2022-23 Q4</b>	<b>2023-24 Q1</b>	<b>2023-24 Q2</b>	Likelihood: Possible (3)
<b>Green (8) by 31/03/23</b>	Impact: Significant (4)	Red (25)	Red (25)	Red (25)	Red (25)	Amber (12)	Impact: Significant (4)

**Reputation impact assessment:** High

**Financial impact assessment:** Band 8 (Loss over £20 million)

#### APEX quarterly commentaries:

Quarter ending	Progress commentary (by risk owner)
30 September 2023	Due to the lack of progress and problems with the recruitment off staff. We are proposing a new 'phased' approach to the roll out of contract management which will be subject to Change Board approval. The new approach will be looking to break the original project into more manageable work streams (while aligning to the original vision) to deliver the benefits associated with this project. The first work stream will be implementing Contract Management for Gold classified contracts (highest value, highest risk and complexity) . A Project Change Board report and Project Plan using RAAID approach is being produced for consideration. Staffing update: 3 x G8 and 1 x G6 recruited, with exemptions forms for 2 x G11 posts submitted for consideration/approval.
30 June 2023	Principal Procurement Officer has started in role who will lead on the initiative. Also, other posts are being recruited to the activity. A review of current contract management practices is being undertaken with departments. The results of this review will feed into the development of the Contract management framework. There are currently 2 x grade 11's and 1 x G6 roles vacant. Three strong candidates have been shortlisted for interview week commencing 11 September. A successful grade 8 candidate commenced her employment on Tuesday 29 August.
31 March 2023	The officer appointed as the Principal Procurement and Compliance Officer and leading on the deliver is initiative is now leaving the

	Council. Failure to recruit into the team continues to jeopardise the ability to successfully deliver the agreed strategy on contract & supply chain management.
--	--

## Information governance and data security

The Council's information governance policies, processes and systems insufficiently protect personal, commercial and other sensitive data, leading to potential harm to vulnerable persons, employees and commercial relationships, legal action, financial penalties and reputational damage.

APEX Unique Risk Number (URN): 521

**Risk Owner:** Mark Kenyon, Director of Finance & ICT

### Assessment history:

Target	Likelihood: Possible (3)	2022-23 Q2	2023-23 Q3	2022-23 Q4	2023-24 Q1	2023-24 Q2	Likelihood: Possible (3)
Amber (12) by tba	Impact: Significant (4)	n/r	n/r	Amber (15)	Amber (15)	Amber (12)	Impact: Significant (4)

**Reputation impact assessment:** High

**Financial impact assessment:** Band 3 (Loss between £100,000 and £1 million)

### APEX quarterly commentaries:

Quarter ending	Progress commentary (by risk owner)
30 September 2023	James Hodges is overseeing the working group which last met on the 1 September, a timeline is being produced for the Data Management Strategy.
30 June 2023	Working group has been established. Support has been provided through SoCITM Advisory in terms of good practice. Individual identified to lead on the review and development of the data management strategy over the next 8 weeks. Once the strategy is updated and drafted this will be shared through the data management group and other key boards for ratification.
31 March 2023	A working group has been established to develop and implement a data management strategy for the County Council. This will be based on best practice across local government and learning from similar organisations. The Council's arrangements in relation to cyber security are being reviewed and improved to ensure there is an appropriate resilience.

## Risk severity matrix and tables

## Risk severity matrix (from 18 September 2023)

<b>Impact Score</b>	Substantial	5	Blue	Green	Amber	Red	Red
	Significant	4	Blue	Green	Amber	Amber	Red
	Moderate	3	Blue	Green	Green	Amber	Amber
	Minimal	2	Blue	Blue	Green	Green	Green
	Negligible	1	Blue	Blue	Blue	Blue	Blue
			1	2	3	4	5
			Rare	Unlikely	Possible	Probable	Almost certain
			<b>Likelihood Score</b>				

## Impact scoring

The highest scoring area (the 'primary impact') used to assess risk severity.

	Impact grading	Public and employee health, safety and wellbeing	Community	Economy	Environment	Service Disruption	Skills capability	Legal	Contracts and Partnerships	Information Security
5	Extremely high	Substantial level of harm to the health, safety and wellbeing of the community, members of the public or employees	Substantial disadvantage to large parts of the community and/or many vulnerable residents	Substantial negative impact on the County's economy, including hard infrastructure	International and/or national environmental damage	Substantial external or internal disruption and/or loss of service (more than seven days)	Substantial under-performance from skills gaps and/or shortages	Substantial legal action, claims and/or penalties against or by the Council	Substantial impact on service delivery from a contract and/or partnership failure	Substantial breach; Information Commissioner Office (ICO) fine; loss of ISO 27001 certification
4	High	Significant level of harm to the health, safety and wellbeing of the community, members of the public or employees	Significant disadvantage to large parts of the community and/or some vulnerable residents	Significant negative impact on the County's economy, including hard infrastructure	Significant regional environmental damage and/or failure to meet all or most internal climate change targets	Significant external or internal disruption and/or loss of service (between three to seven days)	Significant under-performance from skills gaps and/or shortages	Significant legal action, claims and/or penalties against or by the Council	Significant impact on service delivery from a contract and/or partnership failure	Significant external breach with no loss of sensitive data; or minor external breach with loss of sensitive data



	<b>Impact grading</b>	<b>Public and employee health, safety and wellbeing</b>	<b>Community</b>	<b>Economy</b>	<b>Environment</b>	<b>Service Disruption</b>	<b>Skills capability</b>	<b>Legal</b>	<b>Contracts and Partnerships</b>	<b>Information Security</b>
<b>3</b>	<b>Moderate</b>	Moderate level of harm to the health, safety and wellbeing of the community, members of the public or employees	Moderate disadvantage to large parts of the community and/or some vulnerable residents	Moderate negative impact on the County's economy, including hard infrastructure	Moderate regional and/or major local environmental damage and/or failure to meet many internal climate change targets	Moderate external or internal disruption and/or loss of service (between 24 to 48 hours)	Moderate under-performance from skills gaps and/or shortages	Moderate legal action, claims and/or penalties against or by the Council	Moderate impact on service delivery from a contract and/or partnership failure	Significant internal breach with no loss of sensitive data; or minor internal breach with loss of sensitive data
<b>2</b>	<b>Low</b>	Minimal level of harm to the health, safety and wellbeing of the community, members of the public or employees	Minimal disadvantage to the community and/or some vulnerable residents	Minimal negative impact on the County's economy, including hard infrastructure	Minimal regional and/or local environmental damage and/or failure to meet some internal climate change targets	Minimal external or internal disruption and/or loss of service (less than 24 hours)	Minimal under-performance from skills gaps and/or shortages	Minimal legal action, claims and/or penalties against or by the Council	Minimal impact on service delivery from a contract and/or partnership failure	Minor external or internal breach with no loss of sensitive data
<b>1</b>	<b>None</b>	No impact	No impact	No impact	No impact	No impact	No impact	No impact	No impact	No impact

## Likelihood scoring

5	<b>Almost certain</b>	The event is expected to occur every year
4	<b>Probable</b>	The event could occur every year
3	<b>Possible</b>	The event could occur every two years
2	<b>Unlikely</b>	The event could occur every five years
1	<b>Rare</b>	The event could occur every 10 years or longer

## Reputation impact assessment

<b>Extremely High</b>	Lasting or permanent national/local brand damage resulting from adverse comments in national press and media. Members/Officers almost certainly forced to resign.
<b>High</b>	Temporary national/local brand damage lasting up to two years from coverage in national and/or regional press/media. Members/Officers potentially forced to resign.
<b>Moderate</b>	Temporary local brand damage lasting up to one year from extensive coverage in regional press/ media.
<b>Low</b>	Temporary local brand damage lasting up to a few weeks from minor adverse comments in regional press/social media.
<b>Extremely Low</b>	Negligible local brand damage from limited adverse comments with minimal press/social media.

## Financial impact assessment

Each risk is assessed for the potential range of capital and/or revenue loss to the Council if the risk materialised.

<b>Band 8</b>	Loss over £20 million
<b>Band 7</b>	Loss between £10 million and £20 million
<b>Band 6</b>	Loss between £5 million and £10 million
<b>Band 5</b>	Loss between £3 million and £5 million
<b>Band 4</b>	Loss between £1 million and £3 million
<b>Band 3</b>	Loss between £100,000 and £1 million
<b>Band 2</b>	Loss between £50,000 and £100,000
<b>Band 1</b>	Loss under £50,000
<b>Band 0</b>	No financial loss

**FINANCE & ICT RISK REGISTER 2023-24 (ABRIDGED VERSION)**

Risk	Statutory Duty	Reputational Impact Assessment	Financial Impact Assessment	Target Rating	Mar 2023 Rating	Jun 2023 Rating	Sep 2023 Rating
Funding Availability	Yes	Moderate	Band 8	Amber (12)	Red (25)	Red (25)	Red (25)
Impact of a prolonged recovery and a funding gap	Yes	Moderate	Band 8	Amber (12)	Red (25)	Red (25)	Red (25)
Pressure on Services	No	High	Band 4	Blue (4)	Red (20)	Red (25)	Red (25)
Claims and recoveries not processed efficiently and effectively within agreed/statutory timescales	Yes	Extremely Low	Band 4	Green (6)	Amber (16)	Red (20)	Red (20)
HR (Knowledge) - Key staff leaving resulting in skills gaps impacts ability to delivery priorities.	No	Moderate	Band 2	Green (6)	n/r	Red (20)	Red (20)
SAP - SAP project at risk of failure due to lack of direction, plan or design	No	High	Band 3	Blue (2)	n/r	Red (20)	Red (20)
Strategy & Policy - No cloud or data centre strategy restricting ability to make ICT decisions	No	Moderate	Band 3	Green (6)	n/r	Red (20)	Red (20)
Cyber Security - Systems or data breach as a result of a deliberate or accidental action	Yes	High	Band 4	Green (8)	n/r	Amber (15)	Amber (15)
Cyber Security - Systems or data breach due to outdated software or system firmware.	Yes	High	Band 4	Green (6)	n/r	Amber (15)	Amber (15)
Cyber Security (ERP) -Security breach of SAP system due to out-of-date unsupported databases	Yes	High	Band 4	Blue (3)	n/r	Amber (15)	Amber (15)

Risk	Statutory Duty	Reputational Impact Assessment	Financial Impact Assessment	Target Rating	Mar 2023 Rating	Jun 2023 Rating	Sep 2023 Rating
HR (Leadership) - No permanent ICT Team in place to provide long term ICT Leadership	No	Low	Band 1	Blue (4)	n/r	Amber (15)	Amber (15)
HR (Skills) - Lack of training and skills limiting ability to deliver ICT services	No	Moderate	Band 2	Green (8)	n/r	Amber (15)	Amber (15)
Provision of Financial Accounts	Yes	Moderate	Band 0	Blue (4)	Green (6)	Amber (12)	Amber (15)
SAP - Insufficient funding in place to support the SAP project	No	High	Band 3	Blue (2)	n/r	Amber (15)	Amber (15)
SAP - SAP system operates on an out-of-date database platform with known cybersecurity risks	No	High	Band 4	Blue (3)	n/r	Amber (15)	Amber (15)
Strategy & Policy - No agreed Property Strategy restricting ability to make ICT decisions	No	Moderate	Band 3	Blue (4)	n/r	Amber (15)	Amber (15)
Strategy & Policy - No current ICT Target Operating Model leads to an ineffective ICT service	No	Moderate	Band 3	Blue (3)	n/r	Amber (15)	Amber (15)
Unnecessary claims against the Council	Yes	Extremely Low	Band 3	Green (6)	Amber (12)	Amber (15)	Amber (15)
Upgrade of SAP core business system	No	High	Band 5	Green (6)	Red (20)	Amber (16)	Amber (16)
Budget & Financial - Insufficient ICT funding to support ICT service delivery of the next 3 years	No	Moderate	Band 3	Green (6)	n/r	Amber (12)	Amber (12)
Council does not address identified weaknesses in control environment	No	Moderate	Band 2	Green (8)	n/r	n/r	Amber (12)
Cyber Security - Inability to share data with 3rd party organisations	Yes	Moderate	Band 1	Amber (16)	n/r	Amber (12)	Amber (12)

Risk	Statutory Duty	Reputational Impact Assessment	Financial Impact Assessment	Target Rating	Mar 2023 Rating	Jun 2023 Rating	Sep 2023 Rating
Cyber Security (EDRM) - Out of date EDRM software creates heightened security threat	Yes	High	Band 4	Blue (4)	n/r	Amber (12)	Amber (12)
Failure to manage contracts across the county council	No	High	Band 8	Green (8)	Red (25)	Red (25)	Amber (12)
HR (Recruitment) - Recruiting difficulties impacting on the delivery of business priorities.	No	Extremely Low	Band 2	Green (6)	n/r	Amber (12)	Amber (12)
Inability to secure adequate insurance cover for Council risks or in a timely manner	No	Low	Band 4	Amber (12)	Amber (15)	Amber (15)	Amber (12)
Information governance and data security	Yes	High	Band 3	Amber (12)	Amber (15)	Amber (15)	Amber (12)
Infrastructure - ICT systems failure causing major disruption to Council Services	Yes	Moderate	Band 3	Green (8)	n/r	Green (8)	Amber (12)
Infrastructure - Unsupported software or hardware failure causing disruption to Council Services	Yes	Moderate	Band 3	Green (8)	n/r	Amber (16)	Amber (12)
Procurements - Contract Renewals & New Projects procurement are not delivered	Yes	Moderate	Band 7	Blue (3)	Red (20)	Red (20)	Amber (12)
Risk is not adequately understood or assessed in strategic and operational planning and delivery	No	Moderate	Band 4	Blue (2)	Amber (12)	Amber (12)	Amber (12)
Cyber Security (Resources) - Limited resource puts council at risk from cyber threats	Yes	High	Band 4	Blue (3)	n/r	Green (10)	Green (10)
Fraud	Yes	Moderate	Band 3	Green (9)	Green (9)	Green (9)	Green (9)
Audit Plan not delivered	Yes	Moderate	Band 2	Green (6)	Amber (16)	Green (8)	Green (8)

Risk	Statutory Duty	Reputational Impact Assessment	Financial Impact Assessment	Target Rating	Mar 2023 Rating	Jun 2023 Rating	Sep 2023 Rating
Contract Management - Poor contract management leading to delivery to procure systems and services	No	Moderate	Band 3	Blue (2)	n/r	Green (8)	Green (8)
Asset Management - No agreed ownership or management of Hybrid Rooms, restricts forward planning	No	Low	Band 1	Blue (3)	n/r	Green (6)	Green (6)
Asset Management - Software Licence non-compliance and potential financial penalties	Yes	Moderate	Band 3	Blue (4)	n/r	Green (9)	Green (6)
Corporate and departmental risks are not identified and/or managed effectively by risk owners	No	Low	Band 6	Blue (4)	Green (9)	Green (6)	Green (6)
HR (Out of Hours) - No formal arrangements for OoH support putting business ICT continuity at risk.	Yes	Low	Band 1	Blue (2)	n/r	Green (6)	Green (6)
ICT Disaster Recovery documentation and plans not current or workable	Yes	Moderate	Band 3	Green (6)	n/r	Green (8)	Green (6)
Ineffective audit coverage	Yes	Moderate	Band 3	Green (6)	Amber (12)	Green (6)	Green (6)
Use of Multi Factor Authentication (MFA) for accessing Caspar (Deputyship Money Management System)	No	Moderate	Band 2	Blue (1)	Green (6)	Green (6)	Green (6)
Council's assets not adequately protected	Yes	Low	Band 4	Blue (4)	n/r	Green (8)	Blue (4)
Infrastructure - Key facilities artefacts not pro-actively managed could fail	Yes	Extremely Low	Band 1	Blue (3)	n/r	Blue (4)	Blue (4)
Insurable risks not identified or undervalued	No	Moderate	Band 7	Blue (4)	Green (9)	Amber (12)	Blue (4)