Leicestershire County Council

CORPORATE GOVERNANCE COMMITTEE – 6 DECEMBER 2024

REPORT OF THE DIRECTOR OF CORPORATE RESOURCES

RISK MANAGEMENT UPDATE

Purpose of the Report

1. One of the roles of the Corporate Governance Committee is to ensure that the Council has effective risk management arrangements in place. This report assists the Committee in fulfilling that role by providing a regular overview of key risk areas and the measures being taken to address them. This is to enable the Committee to review or challenge progress, as necessary, as well as highlight risks that may need to be given further consideration. This report covers:

   - The Corporate Risk Register (CRR) – updates on risks
   - Emerging risks
   - Launch of the Cyber Assessment Framework for local government
   - Counter Fraud Updates

Corporate Risk Register (CRR)

2. Within the County Council's Constitution, Article 9.03 'Role and Function of the Corporate Governance Committee' states that the Committee shall have responsibility for the promotion and maintenance within the Authority of high standards in relation to the operation of the Council's Code of Corporate Governance with an emphasis on ensuring that an adequate risk management framework and associated control environment is in place.

3. The Council maintains Departmental Risk Registers and a Corporate Risk Register (CRR). These registers contain the most significant risks which the Council is managing, and which are 'owned' by Directors and Assistant Directors.

4. The CRR is designed to capture strategic risk that applies either corporately or to specific departments, which by its nature usually has a longer time span. The CRR is a working document and therefore assurance can be provided that, through timetabled review, high/red risks will be added to the CRR as necessary. Equally, as further mitigation actions come to fruition and current controls are embedded, the risk scores will be reassessed, and this will result in some risks being removed from the CRR and managed within the relevant departmental risk register.

5. Updates to the current risks on the CRR (last presented to the Committee on 16 September 2024), are shown in **Appendix A**. Following a recommendation by the Council's external auditor (Grant Thornton) in its Auditor's Annual Report 2022-23, column 2 shows that corporate risks are now aligned to the Council's Strategic Plan outcomes, i.e.: -
    a. Great Communities (GC)
    b. Clean and Green (C&G)
    c. Improved Opportunities (IO)
    d. Safe and Well (S&W)
    e. Strong Economy, Transport & Infrastructure (SE, T&I)
    f. All (A)

   Risks which have been removed in the last two years, and a brief reminder of the risk scoring process are at the end of the appendix.

   A more detailed update of the CRR (providing additional information on current and further controls/actions on how the risks are being mitigated), will be presented to a future meeting.

6. Movements since the CRR was last presented are detailed below: -

Risks added

9.6 – E&T

If we fail to comply with the Operator's Licence, then the licence could be revoked/curtailed

Risks removed.

7.6 – A&C

If A&C fail to provide robust evidence of good practice for the CQC inspectors, then this will result in a poor inspection outcome and incur reputational risk alongside extra resources and possible external governance to undertake any actions required to make the improvements necessary to fulfil statutory requirements.

Rationale – Several actions are in place to mitigate against the risk which will continue to be monitored at Department level.

Risks amended.

None this cycle

Presentation

7. A presentation will be provided on the risks relating to recruitment pressures and the costly use of agency.

Emerging risks

Adult Social Care – Government Policy Changes

8. There is an emerging risk in the delivery of the Council's adult social care duties which could lead to unsustainable costs to the County Council due to announced and pending government policy changes including: -
    a. Increases to the employer National insurance contributions which will need to be reflected in increased Council fee payments to providers
    b. A manifesto commitment to an adult social care sector pay agreement which would see pay increasing above national minimum wage levels
    c. A commitment to introduce a national care service framework with new standards and responsibilities for councils
    d. The introduction into parliament of the Mental Health Bill which has additional duties and responsibilities for local authorities

9. Impacts should become more apparent over the next 12 to 18 months.

NHS winter pressures

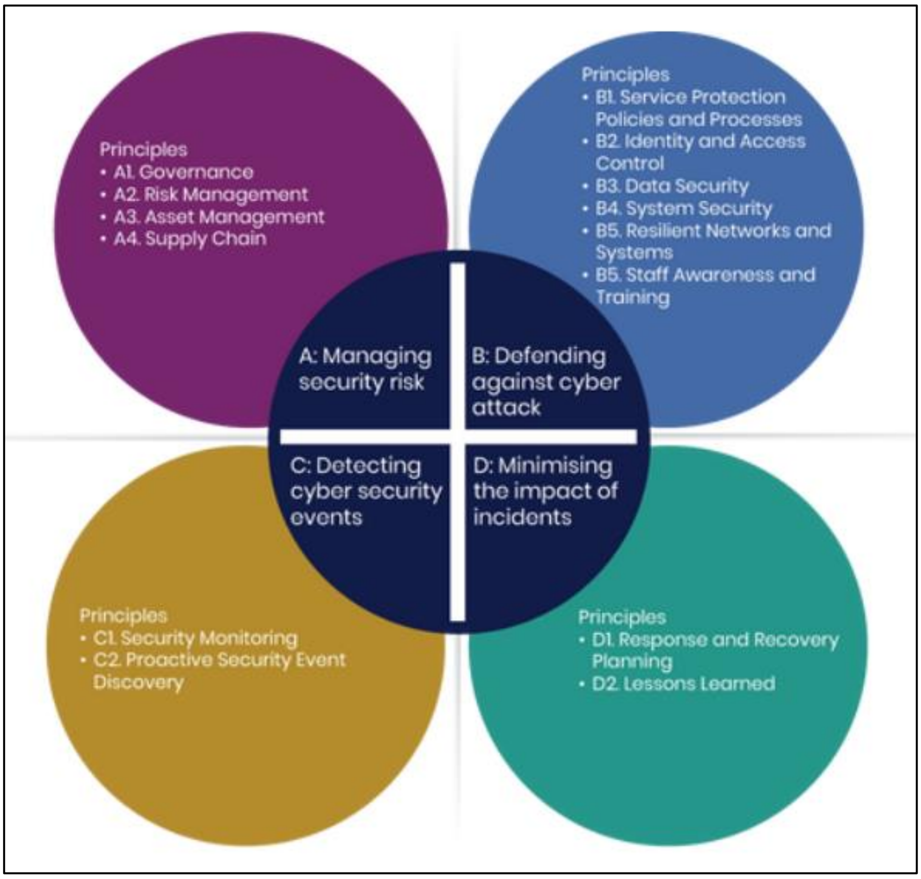
10. The NHS system locally is experiencing unprecedented demand, particularly in relation to activity at A&E. This situation is expected to remain throughout winter. This may lead to additional demand for care services provide by the Council. A productive and efficient winter plan will be needed, to be delivered by the NHS to mitigate additional seasonal pressures on the care system.

Launch of the Cyber Assessment Framework (CAF) for local government

11. The CAF is a cyber security framework developed by the National Cyber Security Centre (NCSC). Originally developed for organisations forming part of Critical National Infrastructure and organisations providing essential services as defined in The Network Information Systems (NIS) regulations.

12. The Government Cyber Security Strategy 2022-2030 states that the CAF will be adopted by central government as a recognised framework for assessing cyber resilience by providing a common reference to good practice. Sector specific profiles will be developed for other public sector organisations but this with be for lead government departments to adapt and apply an approach most appropriate for public sector organisations within their scope. The Ministry for Housing, Communities & Local Government (MHCLG) have developed a local government CAF profile.

13. What is the CAF


Principles
• A1. Governance
• A2. Risk Management
• A3. Asset Management
• A4. Supply Chain
Principles
• B1. Service Protection Policies and Processes
• B2. Identity and Access Control
• B3. Data Security
• B4. System Security
• B5. Resilient Networks and Systems
• B5. Staff Awareness and Training
A: Managing security risk
B: Defending against cyber attack
C: Detecting cyber security events
D: Minimising the impact of incidents
Principles
• C1. Security Monitoring
• C2. Proactive Security Event Discovery
Principles
• D1. Response and Recovery Planning
• D2. Lessons Learned

14. The CAF compromises 4 high level objectives and 14 individual principles. Assessment against the framework is based on 39 separate outcomes. Each outcome is assessed against a structured set of Indicators of Good Practice (Achieved, Partially Achieved, and Not Achieved).

15. The CAF is not a certification, it is a framework for organisations to assess their overall cyber resilience, and to enable identification of cyber security and resilience improvement activities. It is not a checklist exercise and requires councils to interpret the Indicators of Good Practice to determine the most appropriate approach to demonstrate each of the outcomes. There is a strong emphasis on governance, policy & procedures, utilising a top-down approach from senior leadership and cross-organisation involvement in completing the assessment.

CAF for Local Government

16. MHCLG have developed a CAF profile specific to local government. Although this was launched in November it is only the initial stages. The full CAF for Local Government is expected to be launched in spring 2025. At present the CAF is not mandatory and at this stage no indications have been given that it will be mandatory. However, MHCLG are encouraging councils to begin a self-assessment journey. Indicative timelines and resource requirements have

been provided which suggest several months duration and cross-organisational involvement to complete the self-assessment.

Other cyber security standards

17. The CAF differs from other security standards, such as Cyber Essentials and Public Service Network (PSN) Code of Compliance, in that is not prescriptive in terms of technical controls and does not include an IT Health Check assessment (currently the core element of PSN). Therefore, is not yet seen as a replacement for the Council's existing PSN activities. Nor is there any indication as to how the CAF with support/supplement the existing Cyber Essentials scheme or PSN Code of Compliance.

18. The proposed approach to the CAF for Local Government is to maintain a watching brief ahead of the full launch in spring 2025, and to continue the council's preparations for the PSN Code of Compliance submission due in April 2025.

Counter Fraud Updates

International Fraud Awareness Week (17-23 November 2024)

19. To coincide with International Fraud Awareness Week (IFAW), the Internal Audit Service (IAS) issued targeted comms to staff during the week via the Corporate Intranet and other means on a range of fraud risk areas. A strong and continuous process of raising awareness of fraud risk with staff remains a key defence against fraud and IFAW each year provides an ideal opportunity to convey important messages

National Fraud Initiative (NFI) 2024-26 Update

20. The biennial National Fraud Initiative (NFI) data matching exercise is under way and the Council has submitted each of its mandatory data sets to the Cabinet Office within the prescribed timescales. The NFI timescales expect to see 'matches' being returned to councils and other participating bodies for investigation from January 2025 onwards.

21. The NFI is a mandatory data-matching exercise coordinated by the Cabinet Office which seeks to identify potential anomalies and fraud through matching the Council's data sets, e.g. payroll, pensions, creditors, employee data (potential conflicts of interest), blue badges, concessionary travel, etc., with those of other mandatory participants, including the Department for Work and Pensions deceased persons data and director data held at Companies House.

22. A full update on NFI output and outcomes of investigations will be provided to this Committee during the 2025/26 financial year.

Revised Counter Fraud Policies and Procedures

23. The IAS has responsibility for the upkeep of four of the Council's counter fraud documents, namely the overarching Anti-Fraud and Corruption Policy, the Anti-Bribery Policy, the Anti-Money Laundering Policy and the Policy for the Prevention of Facilitation of Tax Evasion. These documents are revised on a biennial basis and have been updated during this last quarter. At its meeting in February 2015 the Corporate Governance Committee delegated authority to the Director of Corporate Resources to approve minor policy revisions without specific recourse to Committee

24. Changes this time are mostly cosmetic but should Members wish to read the four policy documents they can be found on the Council's website at: - https://www.leicestershire.gov.uk/about-the-council/council-spending/fraud

25. With specific regard to the Anti-Fraud and Corruption Policy the biennial revision coincides with the formulation of a new two-year action plan that sits behind the Policy, and which sets out a range of proposed actions moving forward, designed to strengthen the Council's resilience to fraud yet further.

Reporting Fraud

26. During the last quarter, the IAS has developed two new avenues for fraud suspicions and concerns to be reported through to the Council, either internally or externally: -
    a. A dedicated fraud-specific mailbox (fraud@leics.gov.uk)
    b. A web e-referral form

27. These new referral channels are commensurate with the approaches of many other councils and seek to complement existing referral channels, rather than replace them, such as staff reporting concerns to managers or staff making referrals via the Council's formal whistleblowing process.

Fraud Awareness Training

28. The Council's mandatory fraud awareness training module has been refreshed. As part of this refresh, all staff will be expected to undertake recertification within an initial six-month period. Historically, the training required 'one-off' completion only and this refresh will help to keep fraud risk at the forefront of everybody's mind and mitigate the risk of staff knowledge waning over time.

29. Furthermore, two-yearly refresher training on fraud awareness has been developed in an on-going effort to keep fraud risks prominent in the minds of staff. This refresher training will be mandatory for all staff.

30. Additional training exists specifically regarding procurement fraud risk and efforts continue to promote this training to those staff with elements of procurement activity within their job roles and responsibilities.

31. During the last quarter the Council's fraud resource page on the Corporate Intranet (SharePoint) has been refreshed.

Fraud Risk Assessment 2024/25

32. The CIPFA Code of Practice – Managing the Risk of Fraud & Corruption recommends that local authorities identify and assess the major risks of fraud and corruption to the organisation. The IAS performs a biennial fraud risk assessment and uses the results to direct counter fraud resources accordingly. The County Council does not provide some of the services that have historically been at high risk of fraud, such as revenue and benefits but that is not a reason for the Council to become complacent regarding the risk of fraud and its effect on the public purse.

33. National fraud intelligence received through networks such as the CIPFA Counter Fraud Centre and the National Anti-Fraud Network (NAFN), along with key publications such 'Fighting Fraud and Corruption Locally – The Local Government Counter Fraud and Corruption Strategy' helps to inform local authorities of key fraud risks for councils and of emerging frauds relevant to the sector. Such intelligence is used proactively to influence the fraud risk assessment. The IAS networks closely with other local authorities to share both fraud intelligence and strategies to manage fraud risks, including via the Midland Counties' Fraud Networking Group.

34. **Appendix B** contains a summary of the 2024/25 Fraud Risk Assessment, with a corresponding risk grading for each area, based on the Council's overall potential exposure and on national fraud intelligence received. Recognising fraud in this manner ensures there is a comprehensive understanding and knowledge about those areas where potential fraud risk is the highest.

35. The highest scoring areas include categories such as procurement (both pre-contract award stage and post-contract award stage), social care fraud, cybercrime, and insider fraud. These high-scoring areas are typically those reported nationally by other councils. The fraud risk assessment helps to direct the Council's overall strategy for countering fraud and enables the Council to direct its counter fraud resources accordingly. Consequently, this informs the internal audit annual planning process.

School Fraud Risk

36. The Corporate Resources Technical Accounting Team, with support from the IAS, has recently undertaken targeted work with schools within the LA-maintained sector regarding system configurations where schools make electronic payments, e.g. Bankline. The schools' sector has largely migrated away from traditional cheque payments with electronic payment solutions now very much the norm, e.g. Bankline, BACS. Targeted work has led to those schools noted to have weak segregation of duties in the electronic payment

process being given constructive advice how system controls can be better configured to prevent the risk of fraud, e.g. dual authorisation.

37. Cyber risk remains a major threat within the education sector, including ransomware attacks. The Education Effectiveness Team, C&FS, recently brokered a schools' training day facilitated by the Police's Cyber Crime Unit to reinforce key messages and fraud prevention strategies, e.g. multi-factor authentication, system security and off-site backups. The IAS Senior IT Auditor attended the training and (in conjunction with C&FS colleagues) will use the learning outcomes and materials gained to develop a self-assessment questionnaire; will embed some key basic cyber security controls within the existing programme of work that should be assessed during a school's audit and scope out a maintained schools themed audit.

38. The Education Effectiveness Team is progressing with plans to set up a School Business Managers forum, primarily aimed at LA-maintained schools. The IAS has expressed an interest in attending an early meeting of the forum in order to provide school-specific counter fraud advice on a range of current issues.

Recommendations

39. It is recommended that the Committee:

    a. Approves the status of the strategic risks facing the County Council.

    b. Makes recommendations on any areas which might benefit from further examination.

    c. Notes the emerging risks

    d. Notes the launch of the Cyber Assessment Framework (CAF) for local government

    e. Notes the updates regarding counter fraud.

Resources Implications

None.

Equality and Human Rights Implications

None.

Circulation under the Local Issues Alert Procedure

None.

Background Papers

Report of the Director of Corporate Resources – ‘Risk Management Update’ – Corporate Governance Committee, 21 November 2022, 26 January 2023, 16 March 2023, 26 May 2023, 22 September 2023, 17 November 2023, 26 January, 20 May and 16 September 2024.

http://politics.leics.gov.uk/ieListMeetings.aspx?CommitteeId=434

Officers to Contact

Declan Keegan, Director of Corporate Resources
Tel : 0116 305 6199
E-mail : declan.keegan@leics.gov.uk

Simone Hines, Assistant Director (Finance, Strategic Property and Commissioning), Corporate Resources Department,
☎0116 305 7066 E-mail Simone.Hines@leics.gov.uk

Neil Jones, Head of Internal Audit and Assurance Service
Tel: 0116 305 7629
Email: neil.jones@leics.gov.uk

Appendices

Appendix A - Corporate Risk Register Update (October/November 2024)

Appendix B - Leicestershire County Council - Fraud Risk Assessment 2024/25

This page is intentionally left blank