Governance, Risk and Best Value Committee

10.00am, Tuesday, 1 August 2017

Corporate Leadership Team Risk Update

Item number	7.5
Report number	
Executive/routine	
Wards	

Executive summary

The Council's risk management framework ensures that risks to the Council are reviewed and updated regularly through quarterly Risk Committees at Directorate and Corporate Leadership Team (CLT) level.

The information in this report reflects the Council's top risks and the key controls in place to mitigate them as at 8 June 2017. 'Capital asset management', 'ICT transformation and change programme', 'business continuity', 'budget management' and 'cyber security and data privacy' are currently the Council's top risks.

Actions have been developed to reduce the level of risk. These risks and controls have been discussed and challenged by the CLT and are presented to the GRBV Committee for information and review.

Links

Coalition Pledges

Council Priorities

Single Outcome Agreement

Report

Corporate Leadership Team Risk Update

1.   Recommendations

1.1   To note the information provided.

1.2   To invite appropriate officers to discuss key risks and mitigations as required.

2.   Background

2.1   The Governance, Risk and Best Value (GRBV) Committee is responsible for monitoring the effectiveness of the Council's risk management arrangements.

2.2   The Council has an Enterprise Risk Management Policy and Risk Management Procedure in place which describe why, when and how risk management should take place. These documents are reviewed and updated annually.

2.3   The purpose of this report is to provide a quarterly update to GRBV Committee on the key risks facing the Council and the work being undertaken to reduce the level of risk within the Council.

2.4   The CLT Risk Update was last presented to GRBV Committee on 9 March 2017.

3.   Main report

3.1   During the last quarter risks have been reviewed at Risk Management Groups, Senior Management Teams and Risk Committees within each Directorate. The top risks have been escalated to the CLT Risk Committee for challenge and discussion in accordance with the Council's risk management framework.

3.2   The information in this report reflects the Council's top risks and the key controls in place to mitigate them as at 8 June 2017. Appendices 1 and 2 reflect the current top risks to the Council and the key controls in place to reduce the level of risk.

3.3   'Capital asset management', 'ICT transformation and change programme', 'business continuity', 'budget management' and 'cyber security and data privacy' are currently the Council's top risks as scored using the current methodology on an inherent basis. This represents no change from the previous quarter.

3.4   Future CLT Risk Updates will present risks on a current basis which will factor in the likely timeframe to an event occurring, the effectiveness of controls in place and the level of control over which the Council may have over that event, and will present a more realistic view of the risk. Using this methodology it is likely

that 'business continuity' would be the top risk, and this is reflected in the residual risk scoring shown in the appendices.

3.5   Since the last risk update several high-profile events have occurred which have been considered in a risk management context. These events include the Grenfell Tower fire, ransomware attacks, terrorist attacks in London and Manchester and the raising (and subsequent reduction) of the threat level from international terrorism to Critical. After review these events have not altered the scoring of the relevant risks (part of the 'capital asset management' and 'business continuity' risks).

3.6   The Council is a Category 1 Responder as defined in the Civil Contingencies Act 2004, which brings legal duties to assess, plan and advise in relation to emergencies. The Council has an Emergency Plan and a Business Continuity Plan in place and ready for use in the event of a major incident occurring. These documents and the responsibility for associated arrangements are owned by the Resilience Team which sits within Strategy and Insight. The Resilience Team regularly liaise with multi-agency partners including Police Scotland and the Scottish Government. For security reasons the plans and information about our possible responses are not made public.

3.7   The new Chief Risk Officer, Duncan Harwood, started on 27 February 2017 replacing a secondee from PwC thereby achieving savings for the Council. The Corporate Risk Team is now wholly in-house and currently comprises 2.75 FTE.

3.8   The Council won the Resilience Award at the national 2017 Alarm Risk Awards in Manchester, recognising the coordinated and collaborative actions of several departments in response to the collapsed school wall at Oxgangs Primary School and subsequent school closures in April 2016.

3.9   Improvements to the risk management framework, based upon good practice in the public and private sector, will be introduced from July 2017. These are designed to refine and enhance several areas of the risk management framework and will be documented in the next update of the Policy and Procedure documents.

4.   Measures of success

4.1   Effective risk management aims to ensure that key risks to the Council are identified, managed and communicated appropriately and that suitable controls are put in place to mitigate risks to acceptable levels.

5.   Financial impact

5.1   There is no direct financial impact arising from this report.

5.2   Control measures to mitigate risk may have an associated cost which is to be funded from existing budgets in the first instance.

6.   Risk, policy, compliance and governance impact

6.1   Effective risk management aims to improve performance against objectives by contributing to more efficient use of resources, reduction in management time spent dealing with sudden shock events, and more focus internally on doing the right things properly.

6.2   By its very nature risk management cannot guarantee to protect against every possible negative consequence. Even with a perfectly-functioning risk management framework in place events considered extremely unlikely may still occur resulting in significant negative consequences.

7.   Equalities impact

7.1   There are no direct impacts upon equalities arising from this report.

8.   Sustainability impact

8.1   There are no direct impacts upon sustainability arising from this report.

9.   Consultation and engagement

9.1   As part of the Council's risk management framework the information in Appendices 1 and 2 has been discussed and challenged by the CLT.

10.   Background reading/external references

10.1   Corporate Leadership Team Risk Update: report to GRBV 9 March 2017

Stephen S. Moir

Executive Director of Resources

Contact: Duncan Harwood, Chief Risk Officer

E-mail: duncan.harwood@edinburgh.gov.uk Tel: 0131 469 3193

Links

Coalition pledges

Council outcomes

Single Outcome Agreement	
Appendices	Appendix 1 - Top Inherent Risks as at 8 June 2017
	Appendix 2 - Top Inherent Risks with Mitigating Actions
	Appendix 3 - Risk Scoring

Appendix 1 Top Inherent Risks as at 8 June 2017

1. **Capital asset management**
   With reduced resources and a heightened need for structural inspection and maintenance the current asset management plan may be insufficient to cover the immediate need for capital improvements (eg improvement of highways, post PPP1 structural reviews and other capital infrastructure) which could result in continued underinvestment and assets that are not fit for purpose or meet health and safety consequences now and in the future.

2. **ICT transformation and change program**
   Key deliverables, benefits & timescales for achieving IT transformation may not be achieved in line with business expectations, requirements & contractual agreements. This will result in adverse impacts on service delivery and the Council's ability to operate, its finances or its reputation.

3. **Business continuity**
   A sudden high impact event causes buildings, people, systems to be non-operational for an unacceptable period of time.

4. **Increased service with less resource**
   Funding reductions, legislative changes and increased demographic pressure, the requirements of the Local Development Plan and the anticipated need for further cost efficiencies will create an unexpected material pressure on our infrastructure, capital and revenue funding, the execution of our strategy and business plan with associated adverse reputational impact.

5. **Budget management**
   Material overspends on service budgets may impact upon the funding of other services

6. **Cyber security and data privacy**
   A significant cyber breach occurs resulting in sizeable loss of data integrity, confidentially or availability with adverse reputational impact.

7. **Customer expectations**
   Customer dissatisfaction around delivery of customer facing services (eg waste, roads, delayed discharge) may lead to increased complaints with consequential increased financial strain and reputational damage.

8. **Health and Social Care**
   Through either lack of CEC resource and/or provider capacity, the Council may be unable to secure appropriate contracts with its providers or deliver appropriate services as directed by the IJB. As a result we may be unable to deliver our own commitments and to delivery of the H&SC partnership's strategic plan.

9. **Health and Safety**
   Non-compliance with Council Health and Safety policies and procedures and legal and regulatory requirements could lead to avoidable employee or 3rd party injury or ill health and/or regulatory fines and liability claims, and associated reputational damage.
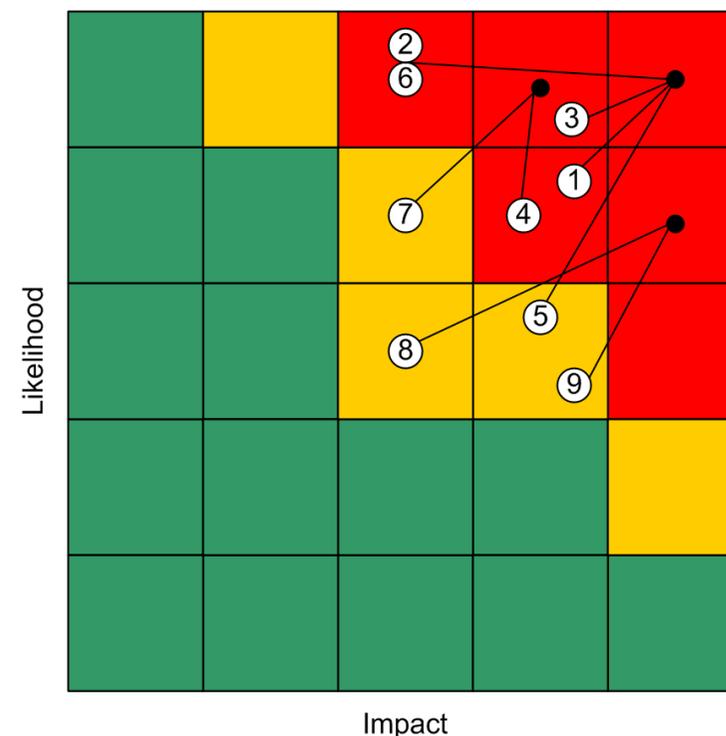
Inherent risk ● Residual risk ①

Appendix 2 Top Inherent Risks with Mitigating Actions

	Risk description	I	L	Current key mitigating controls	I	L	Further actions
1	**_Capital asset management_** With reduced resources and a heightened need for structural inspection and maintenance the current asset management plan may be insufficient to cover the immediate need for capital improvements (eg improvement of highways, post PPP1 structural reviews and other capital infrastructure) which could result in continued underinvestment and assets that are not fit for purpose or meet health and safety consequences now and in the future.	5	5	• Property Management (IPFM) report to CLT • Condition surveys performed routinely • Property Rationalisation work-stream • Asset registers in place with prioritised budget spend on those deemed of greatest risk to public safety. • General Inspections carried out annually as part of asset management programme	4	4	• Ensure asset management strategy clear, prioritised, affordable and deliverable • Ascertain extent of any gaps in recording and inspection of fixed assets • Produce North Bridge Improvement Plan • Procurement underway for contract to inspect all boundary walls. Complete by December 2018.
2	**_ICT transformation and change program_** Key deliverables, benefits & timescales for achieving IT transformation may not be achieved in line with business expectations, requirements & contractual agreements. This will result in adverse impacts on service delivery and the Council's ability to operate, its finances or its reputation.	5	5	• Improved project governance, risk and compliance arrangements between CGI and CEC • Plans for the key projects in terms of scoping and resources	3	5	• Robust plans with clear outcomes
3	**_Business continuity_** A sudden high impact event causes buildings, people, systems to be non-operational for an unacceptable period.	5	5	• Formal Business Continuity Plan in place • ICT Disaster Recovery (DR) arrangements • BCP and ITDR stress tested annually	4	5	• Rolling programme of DR tests on a per application basis • Audit actions being closed out
4	**_Increased service with less resource_** Funding reductions, legislative changes and increased demographic pressure, the requirements of the Local Development Plan and the anticipated need for further cost efficiencies will create an unexpected material pressure on our infrastructure, capital and revenue funding, the execution of our strategy and business plan with associated adverse reputational impact.	4	5	• Provision for demographics built into long term financial plans • Assumptions reviewed regularly and reported to F&R with mitigating actions • Regular review of funding gap with Members Core Group • Service Areas update assumptions half yearly	4	4	• As Transformation Programme rolls out this will include attention to service delivery priorities

#	Risk			Controls			Further Actions
5	**Budget management** Material overspends on service budgets may impact upon the funding of other services	5	5	• Monthly budget monitoring includes KPIs reported regularly • Quarterly reporting to Members Core Group • Regular reporting by Directors of budget pressures • Savings and implementation plans monitored	4	3	
6	**Cyber security and data privacy** A significant cyber breach may occur resulting in sizeable loss of data integrity, confidentially or availability with adverse reputational impact.	5	5	• Refreshed Information security policy introduced • Laptop and media encryption • Service automation controls in place • New IT Security managed Service procured with requirements to adopt CESG (Communications Electronics Security Group – now part of the National Cyber Security Centre) and ISO (international standards) best practice approaches and improve the security defences, monitoring and awareness of the security threat landscape. • Leavers process includes removal of access to IT applications	3	5	• Assess impact of delays in delivery of IT systems • ISMS (Information Security Management System) • Monthly MI demonstrating any threats
7	**Customer expectations** Customer dissatisfaction around delivery of customer facing services (eg waste, roads, delayed discharge) may lead to increased complaints with consequential increased financial strain and reputational damage.	4	5	• Waste improvement plan • New Roads Manager now in place • Roads Service Improvement Plan in place	3	4	
8	**Health and Social Care** Through either lack of CEC resource and/or provider capacity, the Council may be unable to secure appropriate contracts with its providers or deliver appropriate services as directed by the IJB. As a result we may be unable to deliver our own commitments, for example, to enable efficient discharge from hospital and consequently risk not fulfilling our duty of care to customers and to delivery of the H&SC partnership's strategic plan Separate H&SCP risk register to be incorporated where appropriate in next risk review cycle	5	4	• New structure for procurement designed to ensure appropriate skills • Access to external experts for capacity and capability and knowledge sharing • Partnership working with Service Areas and IJB (IJB Procurement Board) • Contract register includes end of contract action plans • Exceptional items escalated to CLT quarterly • The Chief Officer is a member of CEC CLT	3	3	• Consider co-production with voluntary sector • MI reporting to include RAG status on progression of contracts and exceptions • Comprehensive lessons learned review underway to inform enhanced provider failure protocol and contract management
9	**Health and Safety** Non-compliance with Council Health and Safety policies and procedures and legal and regulatory requirements could lead to avoidable employee or 3rd party injury or ill health and/or regulatory fines and liability claims, and associated reputational damage.	5	4	• Progress on Corporate H&S Strategic Plan is reported annually to CLT and Finance and Resources Committee • H&S performance measured and reported to CLT Risk Committee quarterly • Oversight of assurance programme to CLT Risk Committee quarterly • H&S risks and issues are reported to CLT each week. H&S is a standing agenda item • Corporate H&S Training prog available across all levels	4	3	

Appendix 3 Risk Scoring

Likelihood	1 – Rare	2 – Unlikely	3 – Possible	4 – Likely	5 – Almost Certain
Probability	0-15%	16-35%	36-60%	61-80%	81-100%
Chance of Occurrence	Hard to imagine, only in exceptional circumstances	Not expected to occur, unlikely to happen	May happen, reasonable chance of occurring	More likely to occur than not	Hard to imagine not happening
Timeframe	Greater than 10 years	Between 5-10 years	Likely between 3-5 years	Likely between 1-3 years	Likely within 1 year

Impact	1 – Negligible	2 – Minor	3 – Moderate	4 – Major	5 - Catastrophic
Effect on outcomes	Minimal effect	Minor short term effect	Part failure to achieve outcomes	Significant failure to achieve obligations	Unable to fulfil obligations
Financial effect	Corporate: up to £250k Services: up to £100k	Corporate: £250k - £750k Services: £100k - £300k	Corporate: £750k - £5m Services: £300k - £1m	Corporate: £5m - £20m Services: £1m - £5m	Corporate: £20m + Services: £5m +
Reputational damage	None	Minor	Moderate loss of confidence and embarrassment	Major loss of confidence and adverse publicity	Severe loss of confidence and public outcry

Likelihood	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
5 Almost Certain	Low	Medium	High	High	High
4 Likely	Low	Low	Medium	High	High
3 Possible	Low	Low	Medium	Medium	High
2 Unlikely	Low	Low	Low	Low	Medium
1 Rare	Low	Low	Low	Low	Low

Impact