

**Title of Report: Corporate Risk Management 2018/19
Quarterly Report to 31 March 2019**

Report of: Darren Collins, Strategic Director, Corporate Resources

Purpose of the Report

1. This report updates the Committee on developments in Corporate Risk Management during the period 1 January 2019 to 31 March 2019 in compliance with the requirements of good corporate governance.

Background

2. Quarterly reporting to those with the responsibility for the oversight of risk management issues complies with the principles of good corporate governance. It is also embodied in the Corporate Risk Management Policy, last approved by Council on 21 May 2013, which is kept under review, and whilst it has been amended to reflect changes in Senior Officer titles since that time, it remains relevant and fit for purpose.
3. The report covers progress against the Corporate Risk Management Developmental Objectives for 2018/19 as cited in the Corporate Risk Management Annual Report 2017/18 and any other risk management issues emerging within the quarter under consideration.

Development Objectives

4. The Action Plan for the delivery of the Developmental Objectives for 2018/19 incorporating progress to date is shown at Appendix 1, work is progressing as per the plan.

Strategic Risk Management

5. In November 2018 Cabinet and Council approved the revised Strategic Risk Register which had been presented to Audit and Standards Committee on 1 October 2018.
6. The Register has now been adopted and will be monitored and actions reported quarterly to Audit and Standards Committee with any significant amendments reported to Cabinet.
7. A new risk in relation to cyber attack has been documented which details how the Council could have its confidentiality, integrity and availability of information and systems effected by such an event. Work is ongoing to assess how cyber risks could be built into operational risk registers and on raising the awareness and general profile of the risk of a cyber security attack. Plans for maintaining service provision in the

event of such a business interruption will be considered as part of Business Continuity Planning.

8. A risk in relation to UK exit from the EU has also been documented to monitor the potential local impact of EU exit planning, considering the implications for Gateshead and assessing the Council's readiness to respond until a final agreement is known. The Council's Risk and Resilience Group has also been meeting on a more frequent basis to inform Council preparedness for EU exit.
9. The updated version of the Strategic Risk Register is attached in Appendix 2.

Operational Risk

10. To help to ensure operational risks are aligned with Service objectives and reduce the number of generic operational risks which are currently included within the Operational Risk Register, revised guidance has been circulated to Service Directors, supported where requested with Training from the Corporate Risk Management Team.
11. By aligning operational risk to Service priorities, it will help to focus risk management activity on key areas within a Service which can then be managed and used to support decision making and the achievement of key outcomes.

Business Continuity

12. The new Business Impact Assessment and Business Continuity templates have been used in the annual review of Business Continuity which commenced in February. All Services are now actively working on refreshing and updating their impact assessments and business continuity plans.
13. Once all the information has been received these plans will be collated to inform the Corporate Continuity Plan.

Critical IT systems

14. Corporate Management Team agreed to a review of all critical IT systems to enable the Council to corporately identify priority systems for recovery in the event of a system failure/disruption.
15. As part of this work, all Service Directors, in their capacity as Information Asset and Business System Owners were asked to complete a template to prioritise key systems and software applications within their Service. This included information regarding the length of time that the Service could operate without the systems being available and how frequently data would need to be backed-up.
16. Since then, colleagues within IT have worked across the Council to ensure all systems had been captured.
17. The critical systems list will be cross referenced against Business Continuity Plans to ensure consistency and to assist the prioritising of all critical systems onto a corporate priority list.

Risk and Resilience Group

18. The Risk and Resilience Group meeting in April discussed:
- the latest position in relation to UK exit from the EU
 - the issues, challenges and outcomes from the work which has taken place during the previous quarter, including the revised Risk Management and Business Continuity guidance.
 - Any lessons learned, or good practice identified from reviews of Operational Risk Registers to ensure consistent application across the Council.

Recommendation

19. It is recommended that the Committee note the report and consider the effectiveness of the Council's risk management arrangements.

CONTACT: Stephanie Humble extension: 3731