Annex B
Analysis of Key Corporate Risk 2 – Governance

Summary

1. This Annex provides a more detailed analysis of KCR2, Governance.

2. The description of this risk is as follows; Failure to ensure key governance frameworks are fit for purpose. With the current scale and pace of transformation taking place throughout the organisation it is now more important than ever that the council ensures that its key governance frameworks are strong particularly those around statutory compliance including information governance, transparency and health and safety.

Risk Detail

Increased interactions in relation to FOIA and transparency

3. The Freedom of Information Act (FOIA) 2000, which came into effect in January 2005, provides an enforceable right to access recorded information held by around 100,000 public sector organisations. The council has received the following volume of requests under FOIA.

2013/14	1384
2014/15	1864
2015/16	1670
2016/17	1719
2017/18 year to date – April 2017 to December 2017	1305

4. Whilst there is no significant and sustained uplift in volume of requests received, there has been an increase in the caseload. This is as a result of the improvements made in ensuring FOIA requesters understand their rights to seek a review and informing them of their rights to contact the Information Commissioner's Office. There has also been a rise in the complexity of FOIA requests.

Failure to comply with data protection and privacy legislation

5. Legally compliant and excellent information management covers both information governance and information security.

6. For information governance, the General Data Protection Regulation (GDPR) will take effect in the UK from 25 May 2018. It replaces the existing law on data protection (the Data Protection Act DPA 1998) and gives individuals more rights and protection regarding how their personal data is used by councils and we must comply with its requirements, just like any other organisation. It introduces increased monetary fines the regulator can impose for breaches of the data protection and privacy legislation as well as the right to compensation for damage (material or non-material) by individual(s) as a result of a breach.

Annex B
Analysis of Key Corporate Risk 2 – Governance

7. Whilst the GDPR's main concepts and principles are very similar to those contained in the current DPA, there are some changes and additions, as well as some things that we have to do for the first time or differently. This will impose new burdens on the council, including new reporting requirements, the risk of increased fines and penalties and the potential increased resource required for reduced timescales for responding to individuals who request access to their records.

8. The Information Commissioner's Office (ICO) is still the regulator in charge of data protection and privacy issues and as their audit of the council in 2015, included recommendations that had looked ahead at the implications of the GDPR; we have been better placed than many organisations to start to meet the new challenges.

9. We have been working to ensure arrangements are in place to prepare for and meet the requirements of the GDPR across all services. These include adapting our approaches, procedures, and policies as well as embedding strong controls around personal information and full accountability for these controls such as the introduction of a breach management procedure, the information asset register and maintaining external accreditations such as the Payment Card Industry (PCI).

<u>Serious breach of health and safety legislation or Failure to comply with statutory obligations in respect of public safety</u>

10. Responsibility for health and safety in the council extends to our role as employers, service providers and as major procurers and commissioners of goods and services. The legislation that sets out the duties and responsibilities of local authorities, including duties of care, is spread out over many different Acts of Parliament and other instruments of legislation.

Implications

11. The implications for the Council include;
    - Increases in cases held or fines levied by Information Commissioner
    - Failing to meet the legal timescales for responding to FOIA may lead to reduced confidence in the council's ability to deal with FOIA and in turn, its openness and transparency
    - Individuals will be at risk of committing criminal offences if they knowingly or recklessly breach the requirements of the GDPR legislation.
    - Potential increased costs to the council if there are successful individual claims for compensation as a result of a breach of GDPR legislation.
    - Impact on the end user/customer
    - Public and staff safety may be put at risk

Annex B
Analysis of Key Corporate Risk 2 – Governance

- Possible investigation by HSE
- Prohibition notices might be served preventing delivery of some services
- Prosecution with potential for imprisonment if Corporate Manslaughter
- Further incidents occur
- Adverse media/ social media coverage
- Reputational impact

Controls

12. The controls in place include;

Electronic Communication Policy

13. The Electronic Communications Policy (ECP) sets out how CYC employees must use information technology, computer systems and all electronic forms of communication appropriately in the workplace. The ECP applies to all information technology users, whether working within a CYC building or remotely, including staff, Elected Members and third parties. This policy must be communicated to all Information technology users and applies to all users of CYC's infrastructure whether accessed from within a CYC building or remotely. Managers have a key responsibility in ensuring adherence to this policy and must discuss the requirements with their staff to ensure compliance within their Directorate, department or team. The requirement to do so is included in the corporate induction obligation for all new staff members. This policy is reviewed on a biannual basis (or as required if a major change occurs) to take into account changes in legislation, instances of abuse or misuse and concerns from staff and unions.

IT security systems in place

14. This policy sets out how anyone using CYC Information Systems are to use the corporate ICT facilities provided to them, what responsibilities they have and what is acceptable and what is not acceptable when using these ICT facilities. This policy is in place to protect both CYC and its employees as inappropriate use exposes all parties to risks and can compromise the integrity and security of the corporate ICT systems, compromise the network systems and services and may have legal implications. This policy is reviewed every 12 months.

Annex B
Analysis of Key Corporate Risk 2 – Governance

Governance, Risk and Assurance Group (GRAG)

15. The Governance, Risk and Assurance Group (GRAG) monitors, reviews and manages the development of the council's corporate governance arrangements. The group includes the Section 151 Officer, the Monitoring Officer and the Head of Internal Audit as well as other key corporate officers and is responsible for drafting the Annual Governance Statement on behalf of the Chief Executive, Leader and Audit & Governance Committee.

16. The council has responsibility for conducting, at least annually, a review of the effectiveness of its governance framework including the systems of internal control. In preparation of the Annual Governance Statement a review of corporate governance arrangements and the effectiveness of the council's systems of internal control is undertaken and co-ordinated by GRAG. The review includes consideration of:

- the adequacy and effectiveness of key controls, both within individual directorates and across the council
- any control weaknesses or issues identified and included on the Disclosure Statements signed by the Section 151 Officer and Monitoring Officer
- disclosure Statements signed by Directors identifying control weaknesses or significant issues
- any control weaknesses or issues identified and included in the annual report of the Head of Internal Audit, presented to the council's Audit and Governance Committee
- significant issues and recommendations included in reports received from the external auditors, Mazars/ or other inspection agencies
- the results of internal audit and fraud investigation work undertaken during the period
- the views of those members and officers charged with responsibility for governance, together with managers who have responsibility for decision making, the delivery of services and ownership of risks
- the council's risk registers and any other issues highlighted through the council's risk management arrangements
- the outcomes of service improvement reviews and performance management processes
- progress in dealing with control issues identified in the previous year's Annual Governance Statement.
- the councils counter fraud strategy and the level of conformance to the CIPFA code of practice on managing the risk of fraud and corruption

17. The Annual Governance Statement is available on the Council's website.

Annex B
Analysis of Key Corporate Risk 2 – Governance

Information security checks and ongoing Internal Audit review of information security

18. Information security checks were undertaken at West Offices, Hazel Court and 30 Clarence Street in November 2017 by Internal Audit. The purpose of these checks is to assess the extent to which confidential, personal or sensitive data is stored securely and to ensure that data security is being given sufficient priority within council departments. The audit gave an overall opinion of 'Reasonable Assurance'.

19. The agreed actions from the previous audit in March 2017 included the implementation of a secure key storage system at West Offices and that further audit checks would take place in 2017/18 once this had been implemented. At the time of the November 2017 audit, the secure key storage system had recently been implemented and was being used by 13 teams based in West Offices. These teams participated in piloting the system to ensure it worked well and the plan is to roll it out to all teams.

20. The expectation is for Internal Audit to conduct their next round of checks in Summer 2018, once new secure storage is in place at Hazel Court and the secure key cabinets are being used by all teams at West Offices and Hazel Court. The 2018/19 audit plan will include an allocation for information security, although this is subject to agreement by A&G committee.

Health and Safety monitoring

21. The council's Health & Safety Policy drives CYC's commitment to health and safety and is reviewed by the Chief Executive annually. The latest version was adopted in August 2017. The policy is implemented through the work of the CMT, individual directors and the Health and Safety Champions for each Directorate. This is further improved by elected member oversight of the management of health and safety undertaken by the Portfolio Holder for the Environment, and the Audit and Governance Committee who have requested reports in the past year in order to effectively scrutinise the activities of the council in relation to health and safety.

22. Most of the Health & Safety work is driven through the Joint Health and Safety Committee (JHSC) which consists of the champions for each department with Trade Union colleagues. The membership of and attendance at this committee has been improved and will continue to drive forward the health and safety agenda.

23. To support the work of the JHSC the shared H&S service is working with Department Management Teams to develop health and safety action plans that will focus on key priorities for up to the next 3 years. This not only allows the shared H&S service to ensure it is adequately resourced to undertake this work but ensure departments are fully engaged in the process to ensure that the plans are effective.

Annex B
Analysis of Key Corporate Risk 2 – Governance

24. There have been two recent audits of H&S related areas. The H&S follow up report (to follow up previous H&S actions) was discussed at A&G Committee on 7 February 2018. The second audit report covers Safety at Public Events, which is not just a council issue but looks at a key H&S risk area for the city, will be discussed at a future A&G.

Regular monitoring reports to Audit & Governance committee and Executive Member decision sessions

25. A&G Committee receive the following types of reports:
    - Annual Governance Statement
    - Policies and procedures covering governance
    - Head of Internal Audit Report
    - Regular reports on the results of internal audit work
    - Internal Audit Follow up reports
    - Treasury Management Strategy
    - Annual Financial Report
    - External Audit report
    - Finance and Performance Monitoring
    - Monitoring of Key Corporate Risks

26. In addition Executive Member Decision Sessions will cover more service specific follow up actions or updates to policies and procedures.

Open Data platform providing Freedom of Information (FOI) requested data

27. The Open data platform, www.yorkopendata.org continues to expand as the home for the councils and external partners raw data and transparency information. The platform now contains over 1000 datasets, mainly from the council, and covers a huge variety of thematic issues around council services and resident's lives, in a depersonalised or aggregated machine readable format. The Business Intelligence team since the setting up of the platform, have worked with internal council departments who have historically receive a large amount of data related FOI's, to make sure this information is already provided upon the platform.

28. Examples of data provided to the platform to mitigate some of the residents needs to request information via a FOI are; footfall data, business rates information, data on licensed premises, and cleansing and waste information. Work continues to pre-release information to the platform that is likely to be required or requested by residents and businesses.

Annex B
Analysis of Key Corporate Risk 2 – Governance

Regular review of transparency code legislation and compliance

29. The Business Intelligence Hub regularly review the statutory data requirements from the Transparency code for Local government, Transparency code for other bodies, and other transparency legislation such as Inspire (a requirement to publish geographic datasets), to make sure that there is compliance with the legislation and that the information is available to residents through the Open data platform. Compliance on the transparency code has been created in to performance measures and scorecards, so that it is alongside other performance information of the council and can have the necessary profile when required.

30. The Open data platform has been designed to have a specific section for transparency that this information is provided to, and we have worked to make sure the information is provided as quickly, regularly and automatically as possible. Where provision of information is challenging, and/or residents have asked for further clarity on information through FOI's (such as ones recently received on members expenses) we have re-looked at our processes to make sure information can be provided in a timely and accurate fashion.

Ongoing management of data architecture to provide de-personalised data to open data platform

31. The Business Intelligence Hub is responsible for the end to end data processes within the organisation and therefore requires relevant data architecture to manage the flow of information throughout the internal organisation. During the build of this data architecture, the council in conjunction with the Local Government Association (LGA) breakthrough fund implemented technology to provide information held centrally quickly and efficiently to the open data platform. This means that unlike the majority of Local Authorities, CYC is able to provide and update regularly, at the touch of a button, and does not have expensive data manipulation and publishing processes. This has allowed CYC to publish over 1000 depersonalised or geographic datasets.

Public Protection Annual Control Strategy

32. This is a new control which has been added. The Public Protection Service (encompassing Environmental Health, Licensing and Trading Standards) devises an annual business plan (or control strategy) based on strategic assessment of York's current economic, social and political situation. This enables the service to effectively prioritise resources for the forthcoming financial year. Resources are devoted to proactive measures, intelligence gathering and enforcement and performance is measured by a number of indicators. All other statutory duties are performed on a reactive basis.

Annex B
Analysis of Key Corporate Risk 2 – Governance

Additional resource, training and improved processes to deal with FOIA requests

33. This is a new control to deal with the risks in relation to the increased caseload and complexity of dealing with FOIA requests. The following controls are in place:
    - Additional funding provided to increase capacity in the team dealing with FOIA requests. The recruitment has just closed on this and interviews will be held in the next few weeks.
    - Continuous learning and development of team members to ensure we deal with FOIA requests including reviews and ICO cases appropriately and within the legal timescales.
    - Improving the current management and performance monitoring reports to encourage more timely scrutiny from all levels in the council, as well as from Elected Members and Committee(s).
    - Implementing an upgrade to the current system used to record and manage FOIA requests which will in turn provide opportunities for a more streamlined handling process, including customer contact and improved reporting capabilities.

Additional resource, training and improved processes to deal with the implementation of GDPR

34. This is a new control. To help mitigate the risk we are underway with the following:
    - Implementing corporate mechanisms to coordinate arrangements which are done by :
        - Using the ICO's checklists and other resources
        - Using the new guidance and other tools as they are released from the ICO
        - Using guidance from the Article 29 Working Party that is produced at the European level
        - Working closely with other authorities and organisations in the Yorkshire and Humberside region to share knowledge about implementation in our sector.
    - Additional funding provided to increase capacity in the team dealing with information governance. The recruitment has just closed on this and interviews will be held in the next few weeks.
    - Continuous learning and development of team members
    - Training and guidance provision for staff across the council
    - Improving the current management and performance monitoring reports to encourage more timely scrutiny from all levels in the council, as well as from Elected Members and Committee(s).
    - Implementing an upgrade to the current system used to record and manage information governance which will in turn provide opportunities for more streamlined processes, including customer contact and improved reporting capabilities.

Annex B
Analysis of Key Corporate Risk 2 – Governance

Outstanding Actions

35. Ongoing actions have been identified, which are reviewed annually. These are the provision of health and safety training programmes for all levels of staff and a regular review of internal audit reviews and recommendations.

Risk Rating

36. The gross risk score is 20 (likelihood probable, impact major). After applying the controls detailed above the net risk score is reduced to 19 (likelihood possible, impact major).