Appendix 1 – Corporate Risk Management Report

Background

1. Risk management is a key element of East Cambridgeshire District Council's Code of Governance. The Council has experience in Risk Management and has prepared Risk Registers which have been reviewed and approved by the senior management, Corporate Governance & Finance Committee, and full Council.

2. The current Corporate Risk Register was approved by the Corporate Governance and Finance Committee on 1st December 2016, the committee which preceded the Resources and Finance Committee.

3. The Resources and Finance Committee oversee the Council's Corporate Risk Register and recommend revisions to the Council's Risk Management Strategy.

4. The Annual Governance Statement for 2015/16 recognised an opportunity to review the Risk Management Strategy, aligning it to the Council's revised structure and to clearly define the roles and responsibilities of officers and members.

5. The Corporate Governance and Finance Committee noted, at the 1st December 2016 meeting, that a review had been commissioned to seek opportunities for improvement in the risk management arrangements.

Review of Corporate Risk Management

6. The Code of Governance is published on the Council's website. A key element of the Code, which is based on a prescribed best practice format, is to establish and maintain a systematic strategy, framework and process for managing risk.

7. If the Council does not maintain an up to date Risk Management Policy and Framework, there is a high likelihood that risks will not be managed effectively. Consequently avoidable incidents may happen and potential opportunities may be missed.

8. The objectives of the review were to consider the needs of the Council and propose a proportionate risk management approach. The findings have been approved by the Corporate Management Team.

9. As part of the review we have developed a Risk Management Framework which sets out the procedures for risk management, and a Risk Management Policy which sets out the strategic direction for risk management at the Council.

10. In addition the Council is setting up a Risk Management Group. It is good practice for employees, with a mix of professional expertise from across the Council, to work together to:

    - Provide support for the delivery of the Risk Management Policy across the Council.

    - Promote and advise upon risk management practices and procedures

    - Identify topical and emerging risks, based on their areas of expertise, and consider appropriate controls and actions.

11. This collaborative approach provides more assurance that all risks are being identified, and resources are being spent managing the important risks.

Risk Management Policy

12. The Risk Management Policy contains the Strategy and it is presented to the Resources and Finance Committee for their review.

13. The latest version of the Policy is included at **appendix 2**.

14. The Policy establishes the Council's appetite to risk. As an organisation with limited resources it is inappropriate for the council to seek to mitigate all of the risk it faces. The Council therefore aims to manage risk in a manner which is proportionate to the risk faced, based on the experience and expertise of its senior managers.

15. The risk appetite communicates the level of risk the Council is willing to take. In exceptional circumstances it may not be possible, or proportionate, to implement controls that reduce the residual risk score within this appetite. In this instance the risk would be managed, and the aim would be to reduce this below the risk appetite at the earliest opportunity.

16. The maximum risk appetite score is set at 15, as a multiple of residual likelihood and residual impact. The Risk Management Policy states that "*In exceptional circumstances residual risk in excess of the risk appetite can be approved if it is agreed that it is impractical or impossible to reduce the risk level below 16. Such risks should be escalated through the management reporting line to Corporate Management Team, Resources and Finance Committee and Council*".

17. The risk appetite is illustrated in the scoring matrix attached at appendix A of the Policy. This matrix is also used to highlight the significance of the residual risks in a "heat map", which accompanies the Corporate Risk Register.

18. The Policy has been approved by the Corporate Management Team and it provides the Council with an effective approach to risk management.

Corporate risk register

19. The template for the Corporate Risk Register has been updated, and is attached at **appendix 3.**

20. The template includes scores for **inherent** risks (before any mitigating controls are considered) and **residual** risk (after taking account of key controls, which are listed). Any planned actions to further mitigate risks are also shown.

21. Risks are grouped into categories, to help monitor them. The use of the "right" category is not critical, it is simply an aid to assist the identification of a risk. The critical factor is that all key risks are identified and then managed effectively.

22. The Corporate Risk Register will be reported to the Committee at least twice per year. Changes to the risk register, and relevant updates, will be reported to the Committee for awareness. Current developments are detailed below:

Risk	Description
C2 Information security C1 Business continuity and emergency planning	There was a recent large scale cyberattack on the NHS, which delivered ransomware to their IT systems, exploiting vulnerabilities such as out of date software. This had a subsequent impact on delivery of their services, as ICT systems could not be accessed. Reflecting the current environment it is appropriate to increase the inherent likelihood for this risk from 2 (unlikely) to 3 (possible) for risk C1 (information security). The Council is prepared for this risk, and it is already recognised in the risk register. There is a disaster recovery plan, and systems are proactively patched with security updates. In addition the Council has a process of structuring a security awareness programme for all staff, so that they are aware of the risks, which should also help to prevent the occurrence. In light of the recent NHS event, both risks were reviewed, and it was considered that the residual risk profile continued to be correct.

23. The Risk Management Group will complete a further detailed review of the risks within the register and this will be reported to the Corporate Management Team.

24. The Corporate Risk Register will be reported to full Council in October 2017. Any significant changes will also be reported to the Resources and Finance Committee for information.

Corporate residual risk heat map

25. An updated risk heat map is included at **appendix 4** which shows the residual risk level for each of the risks. This gives a quick view of where each risk sits in relation to the council's risk appetite, i.e. there should be no risks with a residual score greater than 15, unless it is exceptional circumstances.

Conclusion

26. Risk Management processes have been reviewed to follow good practice, and to ensure they are proportionate. A revised Risk Management Policy, with a supporting Framework and a Risk management Group has been established to embed good practice in the Council.

27. The Council has a Corporate Risk Register and each risk shows the owner and the key controls, both in place or planned, designed to minimise any impact on the Council and its provision of services to stakeholders.

28. The Risk Management Policy requires managers to keep all risks under review, and the Corporate Risk Register is updated accordingly.