A.3 CORPORATE RISK UPDATE
(Report prepared by Clare Lewis)

PART 1 – KEY INFORMATION

PURPOSE OF THE REPORT
To present to the Audit Committee the updated Corporate Risk Register.

EXECUTIVE SUMMARY
• The Corporate Risk Register is regularly updated and presented to the Audit Committee every 6 months, with the last update in January 2020. • Given the unprecedented impact of the COVID 19 crisis, the risk register will need to be reviewed going forward against a potential 'new normal'. Therefore only minor changes to the corporate risk register have been made at this stage. However to ensure the most up to date position and assurance is reported to the Committee, a more detailed interim update against key risks is set out in a separate table further on in this report.

RECOMMENDATION(S)
That the Audit Committee notes the updates provided to the current Corporate Risk Register.

PART 2 – IMPLICATIONS OF THE DECISION

DELIVERING PRIORITIES
Risk assessment, monitoring and control forms the central tool for managing the strategic risks that may prevent the Council from achieving the corporate priorities as identified in the Corporate Plan and associated corporate goals.

FINANCE, OTHER RESOURCES AND RISK
Finance and other resources The risk management approach can be delivered within existing budgets. **Risk** The subject of risk and its management by the Council is set out in the main body of this report.

LEGAL
There are no specific legal implications.

OTHER IMPLICATIONS
Consideration has been given to the implications of the proposed decision in respect of the following and any significant issues are set out below. **Crime and Disorder / Equality and Diversity / Health Inequalities / Area or Ward affected / Consultation/Public Engagement.** There are no other direct implications.

PART 3 – SUPPORTING INFORMATION

BACKGROUND
The Corporate Risk Register was last presented to the Committee in January 2020. The Terms of Reference for the Audit Committee include a responsibility to provide independent assurance of the adequacy of the risk management framework and the associated control environment. The Corporate Risk Register is therefore brought to the Committee at six monthly intervals to enable the Committee to fulfil its role.

CURRENT POSITION
Corporate Risk Management Framework This is currently being reviewed to reflect the new risk register format introduced earlier in the year. An updated framework will be presented to the Committee as part of future reports and will also need to reflect potential changes emerging from the COVID 19 crisis. **Corporate Risk Register** The risk register has been updated within the context of the usual and underlying risks that are included in the register. However it is recognised that the unprecedented events experienced this year in respect of the COVID 19 crisis will have a major impact on the Council and likely cut across many of the risks currently included within the register. Given the on-going and 'live' nature of the current COVID crisis, it is difficult to fully revise the register at this point in time to reflect what is deemed to be the 'new normal'. However it is timely to highlight the following two points to provide assurance around the Council's governance related response and reaction to the unprecedented position faced this year: • As set out in the Annual Governance Statement, that was published (subject to audit) with the Statement of Accounts 2019/20 at the end of July, a number of actions were set out including those directly relating to the COVID 19 crisis. Updates against these actions are set out within the Table of Outstanding Issues report elsewhere on the agenda. Although it is still relatively early in the wider 'recovery / response' phase, it is important to highlight that a review is planned to be undertaken by Internal Audit that will cover the impact on governance falling into the following broad categories:

- *Impact on business as usual in the delivery of services*

- *New areas of activity as part of the national response to coronavirus and any governance issues arising*

- *The funding and logistical consequences of delivering the local government response.*

- *Assessment of the longer term disruption and consequences arising from the coronavirus pandemic*

- As stated above, the risk register has been updated in terms of the usual and underlying risks that have been previously identified. To date the Council has been able to maintain, operate and deliver the majority of its operations and services as usual but specific comments in respect of key governance items is set out in the following table as an interim update set against the current COVID 19 crisis.

Risk As Included within the Register	Update / Comment
RISK 1b – Catastrophic IT network failure	Resilience is built into our IT Investment Strategies including 'mirrored' data storage at two national Microsoft Azure platform data centres delivering 85% of our hybrid Private/ Public Applications - all resulting in significantly increased resilience and much speedier 'disaster recovery' capability.
RISK 1c- Ineffective communication / management of information	Officers laptops have been upgraded during the last 6 months to ensure a smoother working from home process can be maintained. A significant amount has been undertaken to facilitate remote meetings at both officer and member level.
RISK 1d - Ineffective Cyber Security Physical and Application (software) Based Protection Management	Nationally cyber security attacks have increased by 700% during the COVID 19 crisis. The IT remain alert to these attacks and continue to carry out work in this area including increasing staff awareness on these issues while working remotely.
RISK 3b - Failure to comply with legislative requirements	The Council has remained alert to new legislative requirements such as the changes associated with holding remote meetings etc. The necessary decision making processes and practical arrangements have been put in place where necessary.

RISK 3d - Fraud and Corruption	During a major crisis such as COVID 19, there is unfortunately an increase in attempts to defraud organisations – this can range from organised and widespread 'attacks' to businesses wrongly claiming business rates grants. The Council has remained alert to such issues and where controls have had to be changed or implemented to accommodate new working practices (such as remote working), these changes have been made in consultation with Internal Audit and will form part of their follow up work later in the year.

A significant amount of assurance work has also been undertaken by the Revenues and Benefits Team in connection with the payment of various business grants to ensure money is paid out correctly to those eligible. |
| **RISK 4a – Loss of Key Staff**
RISK 4b – Lack of Capacity to Deliver Core Services | The Council remains alert to the pressures it currently faces, not only responding to COVID 19 issues which have been varied and challenging to resource over the past few months, but also to other emerging activities both locally and nationally.

Council staff have risen to the challenge in terms of being flexible, positive and willing to support different areas of the Council.

However with continuing changes in the Local Government sector, such as those emerging from the Government, the level of capacity to not only deliver against these emerging issues but also the day to day operations of the Council may become more challenging over time. |
| **RISK 5a - Financial Strategy** | There has been a significant impact on business rates and council tax (Risks 8a and 8b) during the 6 month period to date, along with losses of income from areas such as parking and leisure. The Government have provided financial support to the Council to underwrite some risks and an updated in-year position will be reported to members later in October.

It is very difficult to predict the longer term impact on the Council's financial strategy |

	at the present time. However an underlying strength in the financial resilience of the Council is the flexibility that the long term approach provides, which will enable any adverse impact to be managed over a longer period of time.
Risks: **3c - Health and Safety;** **9a - Ineffective Emergency Planning; and** **9b - Ineffective Business Continuity Planning**	At the beginning of the crisis earlier in the year the Council invoked its emergency planning and business continuity processes. Usually this response would be over a very short period of time dealing with a one-off major event such as coastal flooding, so they have never been tested in a long term scenario such as COVID 19. However the plans that have been put in place have enabled the Council to maintain business as usual over a major part of its normal operations. Arrangements have also continued to evolve over the course of the year in delivering a successful response to the longer term nature of the COVID 19 crisis. There will inevitably be lessons learnt that need to be reflected in any necessary revisions to emergency planning and business continuity arrangements which will form part of future updates.

The table below sets out amendments to the Risk Register since it was last considered by the Committee in January 2020.

Risk Register Item	Amendments / Comments
New Risks Identified	None
Risks Removed	None
Risk Scores Amended	None – however as mentioned elsewhere in this report, the corporate risk register will be reviewed in the context of the COVID 19 crisis along with lessons learnt which will undoubtedly require changes to be reflected in the register going forward.
Risk under review	

Risks Amended	Minor wording changes have been made for the following risks: **1b - Catastrophic IT network failure** **1c - Ineffective communication/management of information** **1d – Ineffective cyber security physical and application (software) based protection management** **2d – Ineffective delivery of transforming Tendring project** **6a – Loss of sensitive and/or personal data through malicious actions loss theft and/or hacking** **9a - Ineffective Emergency Planning**

Cyber Security Assessment

A Local Government cyber security self-assessment is undertaken by the Council in November each year with the latest one completed in November 2019. The Council achieved a robust Amber-Green score of 65-79%, but with areas of improvement identified. Our rating placed Tendring District Council in the top-quartile compared with our Essex Online Partnership (EOLP) peer group.

The Service will shortly be undertaking the 2020 self-assessment and it is planned to report any associated recommendations and actions to the January 2021 meeting of the Committee.

BACKGROUND PAPERS FOR THE DECISION
None

APPENDICES
Appendix A – Corporate Risk Register (OCTOBER 2020)