STRATEGIC RISKS 2021-22

REPORT OF:	Head of Corporate Resources
Contact Officer:	Peter Stuart
	Email: peter.stuart@midsussex.gov.uk Tel: 01444 477315
Wards Affected:	All
Key Decision:	No
Report to:	Cabinet
	7th June 2021

Purpose of Report

1. This purpose of this report is twofold: it presents a slightly revised Strategic Risk Policy Document for agreement, and also presents the Council's key strategic risks for 2021-22. These are assessed using that Risk Policy, and plans are presented for mitigating those risks such that the likelihood and impact of their occurrence is minimised.

Recommendations

2. That Cabinet:

   (i) Agrees the Strategic Risks for 2021-22 and management plans set out at appendix A; and,
   (ii) Agrees the MSDC Strategic Risk Management Policy, as set out at Appendix B and supports the consequent changes to the Constitution.

Background

3. Council approved the Corporate Plan and Budget for 2021-22 on 4th March 2021. This Plan is the outcome of a robust service and financial planning process. As with all plans it is, however, based on best known assumptions at the time. If these assumptions prove inaccurate because circumstances change during the year, there could be a potential impact on the Council's ability to fully deliver its plans during the year or to be able to do so within budget. It is therefore prudent that the Council identifies what significant factors or events might occur and to ensure it has in place appropriate arrangements for mitigating 'strategic risks'.

4. This is especially important given the nation is still dealing with the pandemic, which has made accurately forecasting financial and service trends very difficult over both the short and medium term.

Strategic Risk Management Policy

5. The Council adopted a Strategic Risk Management Policy back in 2006. This has been reviewed on an annual basis since then to ensure it remains fit for purpose. Our successful management of the identified risks since that time is evidence that the policy and the associated actions are in no great need of change. However, given the greater economic and societal uncertainty prevalent today, it makes sense to adjust the policy to get the best out of work in this area.

6. The Policy is set out at Appendix B for Cabinet's consideration. The main differences are:

   (a) A clarification of the thresholds between the impact categories. This should enable users to more accurately judge the level of risk threat;

   (b) A clarification of the probability criteria to offer clear guidance on the level of certainty attached to the likelihood of a risk manifesting ;

   (c) More description of the principles that guide the management of risk across the organisation as a whole; and,

   (d) The addition of a further level of Member oversight by fully implementing the Cipfa guidelines on the 'Role of the Audit Committee in Local Authorities 2018'. It should be stressed that this is a matter of choice for the Council but with the increased emphasis on the role of local authorities in dealing with the economic and social impact of the pandemic (particularly around the economic recovery) greater oversight and Member responsibility would be very much in line with our expanded role.

Risk Identification

7. Following consideration of the Councils strategic aims as outlined in the Corporate Plan, three strategic risks have been identified in 2021-22. The risks have been identified using the Council's Strategic Risk Management Policy which considers the likelihood of occurrence, and the level of impact on the organisation and/or the district should they occur. These risks are explained in Appendix A but focus on finance and contract risk and the ever-increasing cyber crime risks.

Initial Risk Score

8. Once risks have been identified, each one is assessed according to the impact on the service, if it occurred, and on the probability that it will happen.

9. Risks are prioritised using a coloured coded scoring system as set out in the risk assessment matrix in Table 1. Risks are assessed on both inherent risk level (no controls or mitigation in place) and residual risk level (after controls and mitigation are implemented). The assessment follows a standard hierarchy where Red risks are the highest, followed by Amber, Yellow, and then Green:

Risk Matrix:

Likelihood					
Almost Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Possible (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Almost Impossible (1)	1	2	3	4	5
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
	Impact				

Next Steps

10. Cabinet is asked to consider the strategic risks for the year and their mitigation plans. Upon this report being agreed, responsibility for management will be assigned and appropriate reporting built in to individual workplans. The appropriate Constitutional changes will also be recommended for implementation in the year.

11. A mid-year report will be produced to update the Executive on mitigation progress and any change in risk rating. In the event that new risks manifest, the appropriate Cabinet Member will be informed and mitigation strategies agreed.

Policy Context

12. The Council has a robust and effective approach to strategic risk management. Strategic Risk Management is an important aspect of every organisation's service and budget processes and the achievement of its corporate priorities. Its application cannot fully insulate the Council from the impact of unexpected external events but it will ensure the Council is best placed to respond if such events occur.

Financial Implications

13. There are no financial implications directly arising from this report.

Risk Management Implications

14. There are no other strategic risk implications aside from those set out in the report and the actions proposed in this report will better enable the Council to identify, mitigate and manage risk. It should, also, be noted that operational risk matters, such as specific business continuity issues, are managed at Service level and escalated as necessary through the Council's Corporate Safety and Risk Management Group which meets quarterly.

Equalities Implications

15. Where appropriate, Equality Impact Assessments are undertaken where service or policy changes are taking place.

Background Papers

None.

Appendix A: Recommendations for Strategic Risks 2021-22

Risk 1: Reserves are needed to balance annual budgets

Corporate Strategic Aim: Financial Independence

Risk Owner: Head of Corporate Resources
Cabinet Member: Councillor Judy Llewellyn Burke

Risk Description

1. The effect of the Covid pandemic has been very serious on the UK economy and local authorities have been as affected as the private sector.

2. The interaction of increased costs along with reduced income across a number of streams has tested the sector's resilience to the limit.

3. Mid Sussex is a strong financial performer yet has been deeply affected by the loss of income in its key income streams of leisure and parking. This position would have been much worse had the government not assisted all authorities with an income compensation and grant package.

4. It is likely that income shortfalls will continue for some time yet and to bridge the gap between income and expenditure some use of reserves will continue. Relying on the general reserve over the medium term is not financially sustainable.

5. A further cause of an imbalance could be the failure of a key contractor. There is a significant contract failure where the Council is exposed to poor performance, business closure or other substantial supply chain impacts.

Current mitigations

- Preparation and distribution of budget management reports and information
- Regular forecasting over the medium term to show national and local financial trends.
- Careful expenditure control.
- Marketing to increase income performance enhancement in key areas.
- Close contract monitoring of service and financial performance.

The consequences

Financial
- Ultimately that reserves are depleted beyond a reasonable and sustainable point
- Contract and/or contractor failure may lead to a compromised ability to deliver the required and stated services and/or the cost of providing those services may increase significantly.

Reputational
- Councils that suffer from chronic financial issues are often accused of mismanagement rather than unfair funding.
- Contractor failure would mean that responsibility would rest with the authority rather than the contractor with consequent negative associations.
- Trust and confidence in the Council may be eroded.

Operational

- Taking over key contracts would present resourcing challenges and may mean delays and slippage in other key work areas.
- The continual need to reduce expenditure to match income would lead to reductions in service levels and/or a withdrawal of services.

The key causal factors:

- Local retention of Business Rates is positive in normal times but can work against recipients when times are more uncertain.
- The Fair Funding review and the reset of Business Rates have been factored in to the financial outlook for 2022/23 but their timing is uncertain.
- General uncertainty in the UK and World economy. Instability and recent high-profile failures of contractors and companies can lead to nervousness which breeds further instability.
- The impacts of COVID-19 restrictions and the uncertain pace of recovery continue to make losses of contractors more likely. Losses can affect supplier chains far from the original problem.
- The financial impacts of the key contracts in light of government Covid19 restrictions

Initial Risk Score: 16

Risk 2: Operational Resilience: Cyber Security

Corporate strategic Aim: Effective and Efficient Services

Risk Owner: Head of Digital and Customer Services
Cabinet Member: Cllr Ruth de Mierre

Risk Description

1. Threat actors targeting local government, locally hosted, or cloud hosted systems and data Threat actors targeting data and systems hosted by 3rd parties that MSDC works with

2. Malicious software deployed across MSDC / 3rd party systems indirectly through phishing, malicious links or similar.

3. Data breach from deviation of best practice or from a targeted social engineering / phishing based attack.

Current mitigations

- Working with security agencies and employing best practice.
- Various cyber security protection techniques, software hardware and services.
- Staff education.
- Further mitigative actions are available but cannot be described in a document with wide or public circulation.

The consequences

Financial
- Any loss of operational capability will have a corresponding financial impact either in relation to lost income, the cost of correcting the issue or rebuilding infrastructure.
- Loss of some critical data could produce an un-recoverable situation which would have significant financial implications on income, such as with revenues and benefits data.
- Estimated average cost of local authorities recovering from cyber-attack is £500k, but has been seen as high as £10m

Reputational
- The loss of key systems relating to public facing services would likely gather negative publicity in the press and social media, especially if it resulted in poor outcomes for customers in significant need.
- Significant media coverage of cyber-attacks and an erosion of public trust in MSDC can be expected in the wake of any significant incident.

Operational
- Any lengthy downtime for key systems will likely create significant operational difficulties for extended periods of time. Previous incidents of downtime suggest that with some scenarios, only a few weeks of downtime can translate to many months of remedial actions and their associated labour costs.
- Catastrophic effect on operational capabilities if critical systems / data are destroyed and restoration capabilities are compromised or not present.

The key causal factors:

- Increased threat of cyber-attacks (viruses, malware, ransomware, etc.) Many sources report that targeted attacks on local authorities are on the rise, cyber-attacks globally are also increasing and are becoming more sophisticated.
- Local authority systems becoming increasingly attractive target to attackers due to factors such as limited digital budgets, legacy systems and large quantities of personal data.
- More flexible access to data and systems can create complacency, and mobile devices can be lost or stolen. As attacks become more sophisticated and convincing, even well-educated staff can fall victim to a phishing attempt.

Initial Risk Score: 15

Risk 3: Operational Resilience: Business Continuity

Risk Owner: Head of Digital and Customer Services
Cabinet Member: Cllr Ruth de Mierre

Risk Description

1. There is a risk that council operations are affected as a result of data being lost from either on-site or cloud systems and / or legacy physical infrastructure being affected by on-campus disasters such as fire and flood, power loss, or loss of connectivity / service.

Current mitigations

- Procurement policy of cloud-first to reduce reliance on physical infrastructure and active program to move as much existing infrastructure to the cloud as appropriate.
- Various backup and restoration capabilities that cannot be described in a widely circulated / public document.
- Further mitigations are available.

The consequences:

Financial
- Any loss of operational capability will have a corresponding financial impact either in relation to lost income, the cost of correcting the issue or rebuilding infrastructure.
- Loss of some critical data could produce an un-recoverable situation which would have significant financial implications on income, such as with revenues and benefits data.

Reputational
- The loss of key systems relating to public facing services would likely gather negative publicity in the press and social media, especially if it resulted in poor outcomes for customers in significant need.
- Significant media coverage of cyber-attacks and an erosion of public trust in MSDC can be expected in the wake of any significant incident.

Operational
- Any lengthy downtime for key systems will likely create significant operational difficulties for extended periods of time. Previous incidents of downtime suggest that with some scenarios, only a few weeks of downtime can translate to many months of remedial actions and their associated labour costs.
- Catastrophic effect on operational capabilities if critical systems / data are destroyed and restoration capabilities are compromised or not present.

The key causal factors:

- It is difficult to predict the likelihood of some scenarios, however on top of disasters and accidents, there are well documented upkeep challenges when operating physical infrastructure in a significantly well-established building such as Oaklands.
- The increasing prevalence of cyber-attacks for local government increases the risk of data loss greatly.
- Some new operating environments such as software and platforms provided as a service present data management and security challenges, and do not always include a backup and recovery solution as standard.

Initial Risk Score: 15

Appendix B

Strategic Risk Management Policy

2021-23

MID SUSSEX
DISTRICT COUNCIL

Strategic Risk Management Policy

Purpose

1. This policy sets out the Council's approach to the identification and management of Strategic Risk.

Definition

2. Strategic Risk Management is the way that the Council responds to uncertainty in the external environment. It allows the Council to:

   - Identify key strategic risks in the context of the Corporate Plan's objectives.
   - Assess risks to determine the potential likelihood and impact of each risk.
   - Determine the response that should be made to each risk.
   - Develop the necessary actions, controls and processes to implement the chosen response to each risk.
   - Communicate its approach to risk management and the results of risk management activity.
   - Deal with each risk – either avoid, reduce, share or accept it.

3. NB: In addition to its strategic risk management, the Council has a well-established approach to operational risk management and the principles and tools used to manage this are set out in a more detailed operational risk management strategy.

Risk Culture

4. A strong business wide risk culture is an important aspect of strong corporate governance. Risk Culture is the shared values, attitudes and practices that characterise how the Council considers risk on a day to day basis. The Risk Culture has developed at the Council over recent years so that as an organisation it is less risk averse.

5. Our experience - has been that this improved risk culture has been influenced by the following factors:

   - Awareness of risks faced by the Council
   - Understanding of the business and the relevance of risk
   - Clear ownership of risks
   - Clearly defined responsibilities for risk management activity
   - Effective monitoring and reporting of the effectiveness of risk Whilst the Council is not risk averse, the principles contained within this policy ensure that the Council strikes the right balance in its approach to strategic risk management.

Responsibility

6. As the Executive, the Cabinet is the body responsible for the Council's strategic risk management. Cabinet will approve the Council's strategic risks on an annual basis. Cabinet members will work with Heads of Service regarding the progress in managing risks that fall within their portfolio. In addition, Cabinet will:

   - Provide overall direction on strategic risk management.
   - Take account of recommendations from the Audit Committee;
   - Approve an annual Strategic Risk Profile.
   - Heads of Service have overall responsibility for managing risks in their service area. This may include any of the Risk Responses set out later and detailed within the risk management plans.

Governance

7. In adopting the 2018 Guidance for Local Authorities for Audit Committees, the Audit Committee will assume the following responsibilities:

   - Assurance over the governance of risk, including leadership, integration of risk management into wider governance arrangements and the top level ownership and accountability for risks;
   - Keeping up to date with the risk profile and the effectiveness of risk management actions, and;
   - Monitoring the effectiveness of risk management arrangements and supporting the development and embedding of good practice in risk management.

8. The Cabinet Member for Finance and Service Delivery is recognised as the Member Risk Champion and works with the Officer Risk Champion to embed risk management into the organisation.

Corporate Management and Reporting

9. Management Team is responsible for ensuring the Council's strategic risks are actively managed through the year. It will use its weekly meetings to monitor progress across all the risks and where it is found a risk has increased its risk profile, a report will be submitted to Cabinet.

10. In addition, Management Team has the following responsibilities:

    - Implementing the strategic risk management policy.
    - Reviewing the management of strategic risk.
    - Monitoring the effectiveness of the controls developed to implement the chosen risk response.
    - Integrating risk management into the service and budget planning process.
    - Promoting a robust and proactive risk culture throughout the staff organisation.

- Ensuring that appropriate training is put in place for appropriate officers and that it is reflected in the Member Development programme.

11. To gain third party assurance of the risk framework, Internal Audit will review the Strategic Risk Register and the management of those risks and will report to the Audit Committee on a regular basis. This then:

    - maintains independence from the responsibilities of management.

    - communicates independent and objective assurance and advice to the Council on the adequacy and effectiveness of governance and risk management (including internal control) to support the achievement of organisational objectives, and,

    - reports impairments to independence and objectivity to the Council and will enable the implementation of safeguards as required.

12. There must be regular interaction between internal audit and management to ensure the work of internal audit is relevant and aligned with the strategic and operational needs of the organisation. This is achieved through the setting of the annual audit plan.

Review

13. This Policy will be reviewed on every four years by Cabinet.

Identification of Risks

14. The Council approach to the identification of risk means:

    - Proactive risk identification, through identification of risks before they lead to harm. This includes regular Strengths, weaknesses, opportunities and threats (SWOT) and PESTLE analysis and scenario planning.

    - Reactive risk identification, through incident reporting processes. Once hazards and potential risks have been identified, they are formally assessed.

Evaluation of Risks

15. Once risks have been identified, each one is assessed according to the potential impact on the service, and the wider Council, if it were to occur and on the probability that it will happen.

16. Risks are prioritised using a colour-coded scoring system as set out in the risk assessment matrix in Table 1. Risks are assessed on both inherent risk level (no controls or mitigation in place) and residual risk level (after controls and mitigation are implemented). Red risks are the highest, followed by Amber risks and then Yellow, and then Green.

17. The Strategic Risk Register (SRR) typically but not always, includes those risks which are rated Red and Amber.

Table 1: Impact Criteria

18. This table is used to assess the impact that a manifestation of a risk would entail. Whilst these matters are never completely discrete, the descriptions act as a guide.

Risk Level		Financial *	Service	Reputation **
5	Catastrophic	More than £1m	Total service failure	National publicity more than 3 days. Resignation of leading member or Officer
4	Major	£500k-£1m	Serious disruption to service	National public or press interest
3	Moderate	£50-£500k	Moderate disruption to service	Local public/press interest
2	Minor	£5k – 50k	Some minor impact on service	Contained within service
1	Insignificant	Less than £5k	Annoyance but does not disrupt service	Contained within business unit

* Financial impact would include the costs of litigation, claims or fines
** The Reputational impact would include consideration of fatality/injury to persons linked to the Council's activities.

19. For example, a possible fatality would merit a 5 score, with 4 meaning a major injury/permanent disablement, 3 a severe injury to an individual, 4 a minor injury to several people, and 2 being a minor injury to an individual.

Table 2: Probability Criteria

20. This table sets out how probable is the manifestation of a risk event. A level of judgement is required and should be peer reviewed to assist with calibration.

Risk Level		Description
5	**Almost certain**	Expected to occur in most circumstances
4	**Likely**	Will likely occur in most circumstances
3	**Possible**	Fairly likely to occur
2	**Unlikely**	Could occur at some time
1	**Almost Impossible**	May occur only in exceptional circumstance

21. These two factors are then combined to give an overall risk score as per the matrix below.

Table 3: Risk Matrix

Likelihood	Almost Certain (5)	5	10	15	20	25
	Likely (4)	4	8	12	16	20
	Possible (3)	3	6	9	12	15
	Unlikely (2)	2	4	6	8	10
	Almost Impossible (1)	1	2	3	4	5
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
	Impact					

22. Each risk is then managed via a Risk Management Plan, which could include the following Risk Responses:

Avoid

23. As the name implies, stopping a particular action or opting to not start it at all is one option for responding to risk. When choosing the avoidance option, we are closing off any possibility that the risk will pose a threat to the Council, but this is not always practical or possible.

24. Exercising the avoidance option too much can result in operation well below risk appetite. However, if there is absolutely zero tolerance for the risk in question, then avoidance is the proper risk response strategy.

Reduce

25. Reduction or mitigation is to take action to reduce the likelihood or impact of a loss. If the risk in question currently sits slightly higher than the appetite, reduction is a reasonable strategy to employ to bring it within tolerance levels.

26. This is often the common approach yet a very careful assessment is needed that reduction actions are working or will actually work in the future.

Transfer

27. When doing so, we do not eliminate or reduce but rather delegate it to a third-party. The goal with risk transfer is to ultimately reduce the impact should something materialise. As an organisation we are willing to take a gamble on the risk occurring

Accept

28. The last option is to simply accept the risk as-is and do nothing. This risk response strategy is often used for risks with a low probability of occurring or that would have a low impact if they did happen. It is commonplace to have budget reserves set aside to deal with situations like this. Emerging risks, or ones that may pose some sort of threat in the distant future, are also ones commonly placed in the “accept” category.