Risk Management Policy and Strategy

Updated: March 2024

Next Review March 2025

Risk Management Policy Statement

St Albans City and District Council recognises risk management is a vital activity that both underpins and forms part of our vision, and key outcomes as set out in the Council Plan.

Risk is present in everything we do. The aim of our policy and strategy is to identify, assess and manage the key areas of risk on a pro-active basis. Risk needs to be managed rather than avoided and we recognise that effective risk management can provide opportunities. The Council has an open appetite for risk. Consideration of risk should not stifle innovation.

We seek to embed risk management into the culture of the organisation and the behaviour of our people. All processes, projects and strategic decisions will consider risk and opportunity, including procurement and contracting. We will seek to ensure, as far as possible, all partnerships and third-party relationships are in compliance with the risk management policy and strategy of the Council.

This risk management Policy Statement and supporting documentation and processes are an integrated framework that supports the Council in the effective management of risk and opportunity.

The aim of our risk management framework is to:

•   Be fit for purpose

•   Be representative of our various activities

•   Make best use of our skills and capabilities to ensure we can deliver our objectives.

For risk management to be most effective and become an enabling tool, we will ensure that we have a robust, consistent, communicated, and formalised process across the Council.

To gain a clear understanding of which risks will threaten the Council's ability to achieve its objectives, a risk appetite statement (the level of risk which Senior Leadership Team considers acceptable for the organisation to be exposed to) has been defined.

In implementing our Risk Management Strategy, we seek to assure our stakeholders (including residents, customers, businesses, councillors, colleagues, partners, contractors) that the identification and management of risk and opportunities is integral to the delivery of our strategy and related objectives.

We will involve and empower all our staff to identify and manage risk. Management of risk activity will be regularly supported through discussion and appropriate action by the Senior Leadership Team and the Wider Leadership Team. This will include a detailed review and confirmation of the significant risks and opportunities, evaluating their mitigation strategies and establishing further supporting actions to manage them to an acceptable level.

Responsible: Senior Leadership Team
Accountable: Chief Executive
Signed: Amanda Foley

Risk Management Strategy

The purpose of the strategy is to define our approach so that there is consistency and a shared understanding between staff, councillors, and key stakeholders. This approach aims to provide a practical, structured, and robust way of identifying, evaluating, and managing risks and opportunities.

The Council's approach to opportunity management will be developed over the coming months and will follow many of the principles set out in this strategy.
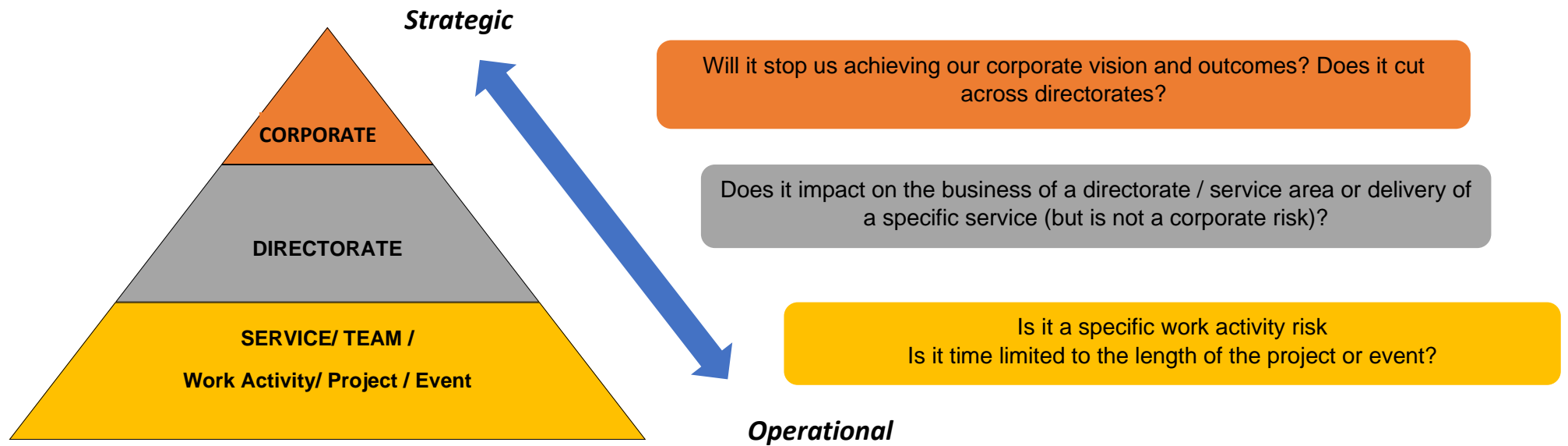
Council staff are members of ALARM (the Association of Local Authority Risk Managers), and our approach follows its recommended processes. Through the ALARM network, the Council:

- learns from best practice and gets insight into the risks other councils are facing.
- is able to advice and training for senior staff with risk management responsibilities.

The strategy is reviewed annually to make sure that it meets current organisational needs and best practice and is approved by the Strategy and Resources Committee. The Audit and Governance Committee carries out an annual review of how risk is being managed in the Council, and reviews corporate and directorate registers throughout the year.

Our risk management approach

1) Define strategic and operational risks – Our 'corporate' risks are the strategic level risks. Our operational risks include directorate, service, project or team risks. Our approach depends on which sort of risk it is.

Strategic

CORPORATE — Will it stop us achieving our corporate vision and outcomes? Does it cut across directorates?

DIRECTORATE — Does it impact on the business of a directorate / service area or delivery of a specific service (but is not a corporate risk)?

SERVICE/ TEAM / Work Activity/ Project / Event — Is it a specific work activity risk. Is it time limited to the length of the project or event?

Operational

2) **Appropriate roles, accountabilities, and responsibilities** - These are assigned to the appropriate level for each sort of risk using the RACI model http://racichart.org/the-raci-model/.

Responsible for managing the risk
Accountable if this goes wrong – the **responsible** person(s) is delegated to manage the risk on their behalf
Consulted as they can tell you more about the risk – this may be a stakeholder or subject matter expert
Informed about how risks are being managed – usually a one-way communication

OVERALL RISK ACCOUNTABILITY:					
	CORPORATE	**DIRECTORATE**	**PROJECT**	**EVENT**	**WORK BASED**
RESPONSIBLE	Delegated lead Strategic Director with assigned Assistant Director	Strategic Director assigned lead Assistant Director or service manager	Project manager	Event manager	Line manager
ACCOUNTABLE	Chief Executive	Strategic Director	Project sponsor	Event sponsor	Service Manager
Process for reviewing	Senior Leadership Team (SLT), (with support from Internal Audit), quarterly	Strategic Director/Assistant Directors at Management Team meetings quarterly	Project team meetings	Event management team meetings	Team brief, one to one meeting As in Safety Policy procedures
CONSULTED	Leader, Lead Councillors, managers, staff	Lead Councillor, staff, stakeholders, councillors	Project team, service users and stakeholders	Event team	Staff
INFORMED *Reported to*	Vice Chair of the Strategy and Resources Committee - by exception where the inherent or residual risk level has gone up to high (red)	Lead Councillors and SLT - by exception quarterly - all high (red) residual risks, significant changes up or down level and new risks	Project team or board meetings, line management arrangements, relevant Lead Councillor (high residual risks)	Event management meetings, line management arrangements, relevant Lead Councillor (high residual risks)	Line management arrangements

Roles and Responsibilities

Who	Key Roles & Responsibilities	Report Type	Frequency
Council	• Receive **Strategy and Resources** Committee minutes		• Annual or as required
Strategy and Resources Committee (supported by Lead Officer responsible for	• Agree the Risk and Opportunity Management Policy and Strategy • Hold the political responsibility for Risk and Opportunity Management within each individual service area.	• Risk and Opportunity Management Policy and Strategy	• Annually or as required

Who	Key Roles & Responsibilities	Report Type	Frequency
the administration of Risk Management)	• Identify a lead Councillor for Risk and Opportunity Management • Receive reports, recommendations, and advice from Audit and Governance Committee		
Audit and Governance Committee (supported by Lead Officer responsible for the administration of Risk Management)	• Oversee and challenge assurance and Risk and Opportunity Management arrangements • Provide feedback on Strategy and Policy to the Strategy and Resources Committee	• Review of Risk Management Policy, Strategy and Framework • Receive quarterly updates on the Corporate Risk and Opportunities Register and annual updates on Directorate Risk and Opportunity registers, supplemented with thematic risk reviews. • Receive assurance on effectiveness of risk and opportunity management	• Annual • Quarterly • Annual
SLT (risk led by lead Strategic Director (Customer Business and Corporate Support)	• Strategic leadership group for risk and opportunity management • Agree the risk appetite for the organisation. • Oversee the Risk and Opportunity Management Policy and Strategy • Responsible for effectiveness of risk and opportunity and assurance arrangements and any management or mitigation - sign off on assurance map. • Quarterly monitoring of corporate risks and opportunities and associated action plans • Allocate appropriate resources to address top risks and opportunities. • Create an environment and culture where Risk and Opportunity Management is embedded and facilitated by the organisation	• Review of Risk and Opportunity Policy and Strategy • Reviews of Corporate and Directorate Risk and Opportunity Registers • Review/benchmarking of Risk and Opportunity Management	• Annual • Quarterly • Annual
Internal Audit	• Use Assurance Mapping to ensure Audit Plan is aligned with top risks. • Review and challenge effectiveness of Risk and Opportunity Policy, Strategy and Framework	• Review of Risk and Opportunity Policy, Strategy and for Audit Committee • Review progress of planned actions and effectiveness of mitigations for the Audit and Governance Committee	• Annual • Annual
Lead Officer responsible for the administration of Risk Management (Currently the Senior Internal Auditor)	• Establish Risk and Opportunity Management Policy, Strategy and Framework • Maintenance of Corporate Risk and Opportunity Register • Review/benchmarking of risk and opportunity management • Quality check of registers and sharing best practice • Advising/supporting risk managers • Provide the link between risk management and other related disciplines e.g., insurance, business continuity,	• Review of Risk and Opportunity Policy, Strategy and Framework for SLT, Audit and Governance Committee and Strategy and Resources Committee • Sense check of Corporate and Directorate Risks and Opportunities Registers for SLT, Audit and Governance Committee and Strategy and Resources Committee • Review/benchmarking of Risk and Opportunity Management	• Annually • Monthly • Annual

Who	Key Roles & Responsibilities	Report Type	Frequency
	emergency planning and health and safety		
Strategic Director	• Identification and monitoring of directorate and corporate risks and opportunities • Escalation of corporate risks and opportunities to SLT as appropriate • Monitoring of high-level risks and opportunities facing the directorate or Council (including programme, partnership, project or service risks and opportunities) • Champion and raise awareness of benefits of Risk and Opportunity Management.	• Review of directorate and relevant corporate risk and opportunity registers as a standing agenda item at management team meetings. • Report to SLT on identified risks and opportunities that require consideration for escalation to the Corporate Risk and Opportunities Register • Report to Lead Councillors and Audit and Governance Committee on high level risks and opportunities facing the directorate/Council	• Quarterly or as required
Assistant Directors and service managers	• Identification, management and review of risks and opportunities within their area of responsibility • Monitoring and escalation of risks and opportunities to Strategic Directors as necessary	• Review of risks and opportunities registers as a standing agenda item at team meetings. • Report to management meetings on identified risks and opportunities that require consideration for escalation to the directorate or Corporate Risk and Opportunities Register	• Quarterly or as required
Programme and Project Board or Project Managers	• Responsible for the identification, management and monitoring of risks and opportunities within their given projects	• Review of risks and opportunities registers as a standing agenda item at project/programme boards. • Report on the management of risks and opportunities and escalation of high-level risks and opportunities as necessary	• Monthly minimum
All employees	• Consider and manage risk effectively in their job and report hazards, risks or opportunities to their manager or other responsible team/officer	• Report incidents, risks and opportunities following Risk and Opportunity Management Policy and Strategy	• As required

3) **Central to business management** - The cycle of identifying, evaluating, managing, and reviewing risk is an active and ongoing part of our business processes. Reviewing corporate and directorate risks is a key part of annual business planning, to make sure that these reflect new work plans and projects. This is also supported by a regular quarterly review of the risk registers. Risk management is also part of our project and event management approach.

Below are the main ways that new, emerging and changing risks are identified.

CORPORATE	DIRECTORATE	OTHER SERVICE/TEAM RISKS
• Standing Risk agenda item for weekly Senior Leadership Team • Tracker' spreadsheet of Corporate Plan projects • Horizon scanning and scenario planning e.g., for elections • Monitoring ALARM bulletins and alerts • Other councils' top risks • Chief Executive/Leader one to one meetings • Lead Councillor meetings • Emergency and Business Continuity Planning • Corporate Health and Safety Officer, Insurance Officer and Legal team monitor emerging issues	• Risk is a standing agenda item for team meetings • One to one meetings with line manager • Performance Conversations process • Responsible Reporting (Whistle blowing) Policy • Complaints discussed quarterly at Senior Leadership Team • Consultation and engagement • Feedback from Equalities and Sustainability Impact Assessments • Lead Councillor meetings • Business Continuity Planning	• Project scoping and other project meetings, and project risk registers • Event meetings • Consultation and engagement exercises • Feedback from Equalities and Sustainability Impact Assessments • Project board meetings

4) **Promotes a 'risk aware' not a 'risk averse' culture** – This is a behaviour that continues to be a key element of the current 'Building our Future' transformation programme to develop an 'Adaptive' Council supported by new ways of working.

Raising risk awareness is supported through specific opportunities as summarised in the table above. We also recognise that risk is an opportunity to challenge what we do and to find better ways of doing things. Risk registers are available for staff to see.

https://stalbanscdc.sharepoint.com/sites/CorporateandDirectorateRiskRegister

5) **Clear and consistent approach for identifying, assessing, and recording risk -** We use the same approach for recording and evaluating corporate, directorate and other risks as described in Appendix 1

Appendix 1: Recording and Assessing Risk – How to Complete a Risk Register

Individual corporate and directorate risks are recorded in word with each risk having its own document. All the risks are available for all staff to view on the Corporate and Directorate Risk Register Sharepoint site which can be accessed via STAN. Editing is restricted to the Chief Executive, the Strategic Directors, the Wider Leadership Team, Members of the Internal Audit Team, Risk Owners, and Executive Assistants.

Do not duplicate corporate risks in directorate risk registers, unless there are specific elements of a corporate risk which need tailored management by a directorate. Any further actions will then feed into the overall corporate risk assessment. For example, effective contract management is a corporate risk which applies to all Council contractors, but the risks associated with specific contracts will sit within the relevant directorate.

Risk Register Template

Risk Name	Include Risk Number and Name		
Council Plan	State which aspect of the Council or departmental plan the risk links to		
Risk Appetite	State the risk appetite	**Risk Category**	Note the risk category
Risk Owner	Note the Post Holder responsible for the risk	**Date Added to the Risk Register**	Either Pre 2015 or the actual date
Lead Directorate	Include the lead directorate	**Date Last Reviewed**	Note the date you are completing the register
Accountable Strategic Director	Note the accountable strategic director	**Date of Next Review**	This would be either monthly, quarterly, or ever six months
Risk	**RISK** -. **CAUSE** -. **CONSEQUENCE** -.		
Background	Give some context to the risk so that it may be understood		
Risk Likelihood	Explain the reason for the inherent risk score – that is why it is likely that the risk will happen. The levels of risk likelihood are shown below		
Risk Impact	Explain the reason for the inherent risk score – what will happen if you do nothing. The levels of risk impact are shown below		

Controls in Place	**Additional Actions to Mitigate Risks**
Consider what controls are in place to reduce or remove (mitigate) the risk. A risk can be mitigated by: a) reducing the likelihood of it happening b) reducing the impact to the Council should it happen. .	List any additional one-off actions that can be undertaken to reduce the risk still further. Note the officer responsible for the actions

Inherent Risk		**Residual Risk**		**Target Risk**	
Likelihood	Impact	Likelihood	Impact	Likelihood	Impact

The 'inherent risk score' assumes that there are no steps in place to reduce or remove the risk. Rate the **impact** of the risk on delivering services or meeting objectives and the **likelihood** of it happening. See Appendix 1b for definitions of the rating levels.

The residual risk is after the mitigations. A target risk is the score that can be achieved if the additional actions are undertaken. Assign a target risk rating based on the type of risk and the Council's risk appetite. This should be the level of risk that is realistically achievable once all mitigations and further actions are in place. See Appendix 1c for the Council's risk appetite to see what is realistic.

The risk score is the likelihood multiplied by the impact.

Risk Scores are Shown in the Table below:

Catastrophic	5	10	15	20	25
Severe	4	8	12	16	20
Moderate	3	6	9	12	15
Minor	2	4	6	8	10
Low	1	2	3	4	5
Impact	1	2	3	4	5
Likelihood	Very unlikely	Unlikely	Possible	Likely	Very Likely

Use the table below to plan the appropriate action for the level of risk.

Risk Level	Tolerability	Comments
1 – 4	Acceptable	No further action required, but ensure controls are maintained
5 – 9	Adequate	No further action required, but ensure controls are maintained and keep under close review
10 – 16	Tolerable	Look to improve level of risk if practical
17 – 25	**Unacceptable**	**Stop activity (where possible) and make immediate improvements**

Based on the risk score these are the actions to consider

Actions to take:		
1	**Terminate the risk**	Decide to stop the activity e.g., if it is felt that the risk is too great or that the financial cost of mitigating controls was too high
2	**Transfer the risk**	Pass the risk on e.g., to an insurer
3	**Treat the risk**	Decide to manage the risk by putting further controls in place to reduce impact or likelihood
4	**Tolerate the risk**	Decide to accept the risk without transferring or treating it but to monitor and re-evaluate it in the future

For high tolerable risks, list what will be done to reduce the residual risk score or explain why this is not practical in the 'action' column. Then ensure these actions have a realistic 'completion date' and are assigned to a specific officer.

Appendix 1a – Types of Risk

Reputation	Related to the Council's standing with residents, wider public, key stakeholders and influencers, and the public e.g., through adverse publicity.
Finance	Related to financial planning and control, ensuring sufficient funding to meet expenditure commitments and the adequacy of insurance cover.
Compliance	Associated with current or potential changes in national or International Law and adhering to legislation, regulations, procedures e.g., age discrimination legislation.
Corporate Priorities	Relating to delivering the Council's corporate priorities, and the effectiveness of these priorities in the wider context
People	Related to the Council's workforce including staff wellbeing, recruitment and retention of qualified staff, succession planning, establishing clear roles and responsibilities, over reliance on key officers.
Health and Safety	Related to fire, security, accident prevention and health and safety.
Information Governance	Related to the security, accuracy, timeliness of any information held or given by the organisation.
Customer Delivery	Related to meeting current and changing needs and expectations of residents, customers, and citizens.
Environment	Related to the Council's influence on the health of the environment including sustainability, impacts of materials use and waste, pollution, transport, noise, and greenhouse gas emissions
Climate	Related to the Council's influence on making the Council carbon neutral by 2030
Cyber Security	Related to the need to ensure cyber security in a digital world

Appendix 1b – Likelihood and impact definitions

To estimate the likelihood and impact of the risk use the following descriptions and definitions of the rating.

LIKELIHOOD

Rating	Description	Likelihood of Occurrence
1	Very Unlikely	Rare, but it may occur in exceptional circumstances. It could happen, but probably never will.
2	Unlikely	Not expected, but there is a slight possibility it may occur at some time.
3	Possible	The event might occur at some time as there is a history of casual occurrence at the Council and/or similar organisation.
4	Likely	There is a strong possibility the event will occur as there is a history of frequent occurrence at the Council and/or similar organisation.
5	Very Likely	Almost certain. The event is expected to occur in most circumstances as there is a history of regular occurrence at the Council and/or similar organisation.

IMPACT

Rating	1	2	3	4	5
Description	Low	Minor	Moderate	Severe	Catastrophic
Finance	Lower level of financial loss; Less than £10,000	£10,000 to £100,000; not covered by insurance	£100,000 to £300,000; not covered by insurance	£300,000 to £400,000; not covered by insurance	Above £400,000; not covered by insurance
Compliance	Minor civil litigation or regulatory criticism Breach of guidance / statuary duty	Minor regulatory enforcement Informal recommendation from regulator	Major civil litigation and/or local public inquiry	Major civil litigation setting precedent and/or national public enquiry. Enforcement action Multiple breeches in statutory duty Improvement notices	Section 151 or government intervention or criminal charges
Customer Delivery	Insignificant disruption on internal business - no loss of customer service	Some disruption on internal business only - no loss of customer service	Noticeable disruption affecting customers Loss of service up to 48 hours	Major disruption affecting customers Loss of service for more than 48 hours	Loss of service delivery for more than seven days
People	Short-term staffing absence (less than 2 weeks) that temporarily reduces service quality	Low staffing level (up to 1 month) that reduces service quality	Low staffing level (up to 2 months) or lack of skills/experience that reduces service standards or leads to late delivery of objectives	Low staffing level (more than 2 months), lack of skills/experience and/or loss of key staff that leads to uncertain delivery of key corporate services or objectives	Low staffing level (more than 2 months), lack of skills/experience and/or loss of key staff that leads to non-delivery of key corporate services or objectives
Environment	Minor or negligible danger to the environment.	Some short-term impact to the environment	Long term impact to the environment	Major ongoing impacts to the environment, including raising greenhouse gas (GHG) emissions	Breach of statutory environment duties, increasing GHG emissions

Rating	1	2	3	4	5
Description	Low	Minor	Moderate	Severe	Catastrophic
Health and Safety	No or only minor personal injury - first aid needed but no days lost	Minor injury - medical treatment and some days lost	Injury - possible hospitalisation and numerous days lost	Single death and/or long-term illness or multiple serious injuries	Multiple deaths or permanent disability or ill-health
Information Governance	Minor breach affecting single individual	Minor breach or sharing of inappropriate information affecting up to 20 people	Minor breach or sharing of inappropriate information affecting 21-100 people or very sensitive breach relating to 2 to 5 people	Minor breach or sharing of inappropriate information affecting 101-500 people or very sensitive breach relating to 5 to 20 people	Minor breach or sharing of inappropriate information affecting over 500 people or very sensitive breach relating to over 20 people
Reputation	Negligible impact	Adverse minor comment including on social media	Adverse social and local media coverage	Adverse national coverage	Demand for government inquiry
Corporate Priorities	Resolved in day-to-day management	Minor impact	Significant impact	Major impact	Disastrous impact
Climate	Minor or negligible impact on the delivery of a carbon neutral council	Medium impact	Large impact on the delivery of the carbon neutral programme	There is a major concern to the delivery of the carbon neutral target	The council will not meet its carbon neutral target
Cyber Security	Minor breach affecting single individual. No loss of systems or delays in service delivery from breach.	Minor breach affecting one team or up to 20 people and limited to one system. Minor delays in service delivery less than 7 days to recover systems/ restore data.	Breach affecting the whole of one service area and / or limited to no more than two systems. Delays in service delivery less than 2 weeks to recover systems/ restore data.	Breach affecting more than one service area and three or more of the systems. Delays in service delivery of up to 4 weeks to recover systems/ restore data. Financial cost less than £250k.	Whole business of the Council compromised/ all systems impacted. Delays in service delivery over 4 weeks to restore systems/ recover data. Significant financial cost to Council to recover systems/ data £250k +.

Appendix 1c – Risk Appetite Statement

Risk appetite is the amount of risk the Council is prepared to accept in the pursuit of its strategic objectives.

The overall risk appetite that SLT considers appropriate taking all strategic objective risk appetite alignment into consideration is **'Open.'** This means that SLT is prepared to consider all delivery options and will select those with the highest probability of productive outcomes, even when there are elevated levels of associated risks. Different areas of the organisation will accept more or less risk than others. For example, the Council will accept more risk for areas of growth than in those relating to Governance and Compliance. **The amount of risk the broader Council is willing to take will vary depending on the risk category**.

Health and Safety | Information Governance/ Cyber Security | Environment/ Climate | Compliance | Finance | Customer Delivery | People | Corporate Priorities | Reputation

Low acceptable risk → **High acceptable risk**

Averse	Cautious	Open	Hungry
• Preference for safe business delivery options that have a low degree of current risk and potential for limited reward. • Low risk options taken to minimise exposure – reluctant to act given uncertainty – highly influenced by experience	• Preference for safe delivery options that have a medium degree of risk and may only have limited potential for reward. • Willing to take risks but prefer to take the *safe delivery option* minimising the exposure with tight corporate controls over change	• Willing to consider all potential delivery options and chooses the one that is most likely to result in successful delivery whilst also providing a good level of reward. • *No surprises* – well measured risk taking. • Willing to take risk with a degree of uncertainty recognising that things may go wrong. • Learns from mistakes	• Eager to be innovative and chooses options offering potentially higher business rewards despite greater inherent risk. • Recognises highly devolved decision-making meaning that not all risks are known. • Acts when uncertain of results with uncertain information. • Willing to accept significant loss for potentially higher reward
1-4	5-9	10-16	17-25