RISK AND OPPORTUNITY MANAGEMENT STRATEGY 2023-2025

PLYMOUTH
CITY COUNCIL

Contents

INTRODUCTION

We live in very challenging times, where the city and its citizens face significant risks but also where innovation is critical. We are a large, complex organisation and need to continuously look at how we can safeguard and support our communities in challenging financial circumstances.

Risk and opportunity management is both a statutory requirement and an indispensable element of good corporate governance and good management. It has never been more important to have an effective Risk and Opportunity Management Strategy in place to ensure we are able to discharge our various functions and deliver public services efficiently and cost effectively.

Risk is unavoidable. It is an important part of life that allows us all to move forward and develop. Successful risk management is about ensuring that we have the correct level of control in place to provide, as far as reasonably practicable, sufficient protection from harm without stifling our development.

The Council will record the significant risks identified as potential threats to the delivery of its objectives within Risk and Opportunity Registers and incorporate mitigation controls within action plans to include details of any opportunities that may arise from the successful management of each risk. Strategic Risks will be monitored every three months and Operational Risks every six months. Findings will be reported via the Council's formal reporting process.

The benefits gained with a Risk and Opportunity Management Framework are improved strategic, operational and financial management, better decision making, improved compliance and, most importantly, improved customer service delivery and better outcomes for the citizens of Plymouth.

We embrace risk and opportunity management to support the delivery of our vision for the city and to enable the provision of high quality services to the citizens of Plymouth.

Cllr Mark Lowry	Tracey Lee	Giles Perritt
Cabinet Member for Finance	Chief Executive	Assistant Chief Executive

RISK AND OPPORTUNITY MANAGEMENT STRATEGY

What is a Risk?

Risk is commonly understood as something to be avoided but it has another face – that of opportunity. Improving public services requires innovation – seizing new opportunities and managing the risks involved. In this context risk is defined as uncertainty of outcome, whether positive opportunity or negative threat of actions and events. It is the combination of likelihood and impact, including perceived importance.

What is Risk and Opportunity Management?

Risk and opportunity management is the culture, processes and structures that are directed towards effective management of potential opportunities and threats to an organisation achieving its objectives and delivering services to the community.

This Strategy is intended to reaffirm and improve effective risk and opportunity management in Plymouth, comply with good practice and in doing so, effectively manage potential opportunities and threats to the Council achieving its objectives.

Risk and Opportunity Management Policy Statement

Plymouth City Council is aware that, as a large organisation, it is exposed to a very wide range of risks to the delivery of key services to the community it serves.

The Council recognises that it has a responsibility to identify, evaluate and manage risk whilst still creating a fertile climate for innovation. It therefore supports a structured approach to risk and opportunity management through this corporate Risk and Opportunity Management Strategy, the aims and objectives of which are described below:

The aims of the Risk and Opportunity Management Strategy are to:

- Integrate and raise awareness of risk and opportunity management for all those connected with the delivery of Council services;
- Embed risk and opportunity management as an integral part of our organisational culture and project planning and policy making processes;
- Establish a standard systematic approach to risk identification, analysis, control and monitoring and reviewing;
- Provide a process for identifying threats or drawbacks that also includes finding and considering opportunities;
- Provide a robust and transparent framework for managing risk and supporting decision making;
- Support well thought-through risk taking, which enables a risk aware organisation that takes well-managed risks;
- Anticipate and respond to changing external and internal environment;
- Embed risk and opportunity management as an integral part of delivering and aligning successful partnerships and enabling organisational objectives and business planning processes.

The objectives of the Risk and Opportunity Management Strategy are:

- To embed Risk and Opportunity Management as part of the Council's culture of governance

- To provide a robust and systematic framework for identifying, managing and responding to risk
- To provide a robust and transparent track record of managing, communicating and responding to risk
- To encourage staff to think creatively about ways to work better, simpler and more effectively.

Types of risk

Strategic and Operational

Strategic risks affect or are created by our business strategy and strategic objectives. They can be defined as the uncertainties and untapped opportunities embedded in strategic intent. As such, they are key matters for our political and managerial leadership and impact on the whole organisation. Inclusion of a risk in the strategic risk and opportunity register indicates that it is one of a number of risks that the Council (particularly elected members and senior managers) need to be aware of and ensure appropriate management arrangements are in place to manage/mitigate them.

Operational risk is defined as the risk of loss resulting from inadequate or failed processes, people and systems whether within the "business as usual" of the Council or through change management programmes, new protocols ways of working, new structures and new technologies. All major risks facing the service and to other services and partners resulting from the consequences of a service's plans should be recorded with brief mitigation and potential outcome.

Programme Risks

Risks that relate to a specific programme are likely to comprise of a mixture of the most serious project risks **and** cross-cutting risks that could affect two or more of the projects within the programme. All major programmes must have a risk register, owned by the programme manager. It should be reviewed by the programme board and at the most senior level of the directorate in question. HSW risks must be considered alongside every programme and documented on SHE Assure.

Project Risks

Risks relating to or that flow from a specific project. A project risk has the potential to impact on the project's scope, outcomes, budget or timescales. Where the risk could impact on other projects or objectives, or the project is considered a high priority and the level of risk is such that it could lead to a failure to deliver project objectives, the risk should be escalated to the programme level. HSW risks must be considered alongside every project and documented on SHE Assure.

Partnership Risks

Plymouth City Council has recognised the need to include "Partnership working" within this risk management framework. Partnership working presents a number of new risks -

- Partner organisations will have different aims and objectives;
- Often Partnerships are innovative, and there is no proven track record for the work they are undertaking;
- By definition, they involve different organisations, with different cultures and systems;
- It is likely each organisation will have a different approach to the management of risk;
- Organisations will have differing risk appetites.

It is essential that the Partnership manages risks (and maximises opportunities) that can impact upon the aims and objectives of the Partnership as a whole.

Equally, Partner organisations need to understand the nature and extent of the risk they face individually through Partnership working.

As part of the development of the Council's Risk and Opportunity strategy a common approach to managing risk in partnership will be developed that enables the joint assessment of risk against partnership objectives to be made and managed through shared risk registers.

Risk management responsibilities

Risk and opportunity management is the responsibility of all employees, working together within teams and management structures to ensure timely consideration and control at the appropriate level.

Any risks to health, safety or wellbeing (HSW) of our employees or others affected by our operations are compiled into the HSW risk register held on SHE Assure and risks rated high will be additionally monitored by the HSW Steering Group on a quarterly basis. This may result in additional assurance being required to ensure controls are reducing risk to as low as reasonably practicable. The HSW Team support service areas to ensure risk assessments are suitable and sufficient. Risks reviewed at the HSW Steering Group may be escalated to the Strategic Risk Register if they meet the relevant criteria (see Risk Tolerance section)

APPROACH

All risks recorded on our Risk Register are discussed by Departmental Management Teams (DMT) monthly and by the Corporate Management Team on a quarterly basis. HSW risks rated high are discussed at JCC / HSW Committees at every meeting and at HSW Steering Group quarterly and may be escalated as per risk tolerance section.

All risks will accompanied with the following information:-

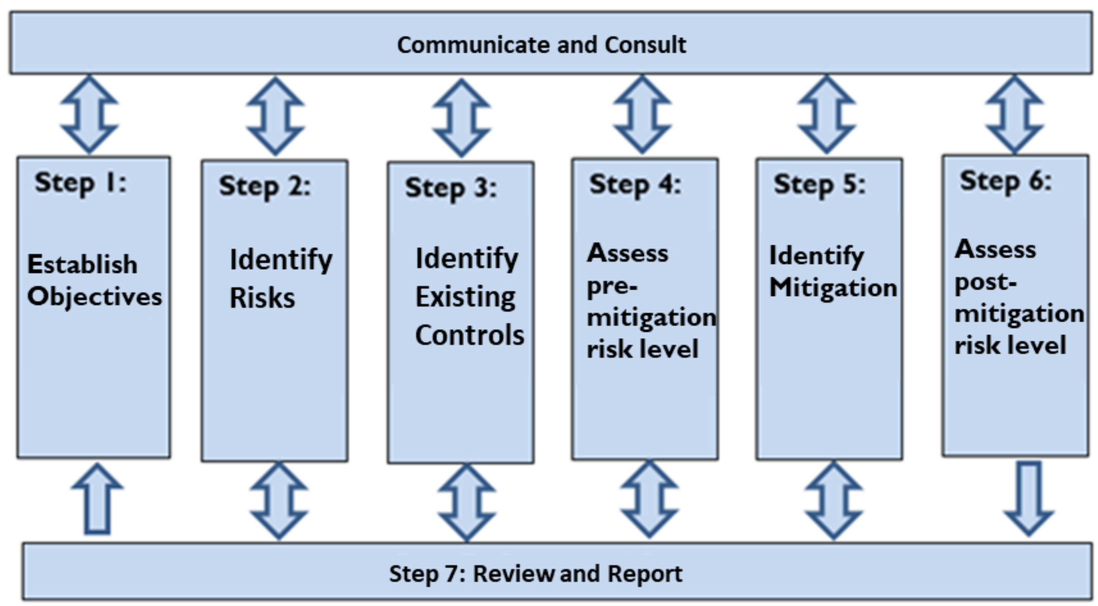
- possible consequences of the risks identified, both negative (risks and threats) and positive (opportunities);
- potential impact and likelihood of the risk identified;
- existing controls in place to mitigate the risks;
- actions planned to mitigate the risks with relevant timescales and the responsible officers.

For a number of years the Council has been working towards a comprehensive and integrated approach to risk management where:

- staff are clear about what risk management is intended to achieve;
- significant risks are being identified and managed effectively;
- training and guidance on risk management are easily accessible;
- a consistent corporate approach is followed using a common ‘risk language’; and
- It is seen as an integral part of good corporate governance.

This section details the agreed arrangements that are needed to ensure the effective management of all risk (with the exception of HSW risks) across the organisation. The Council’s approach to risk management is based on best practice and involves a number of key steps as outlined in the figure below:-

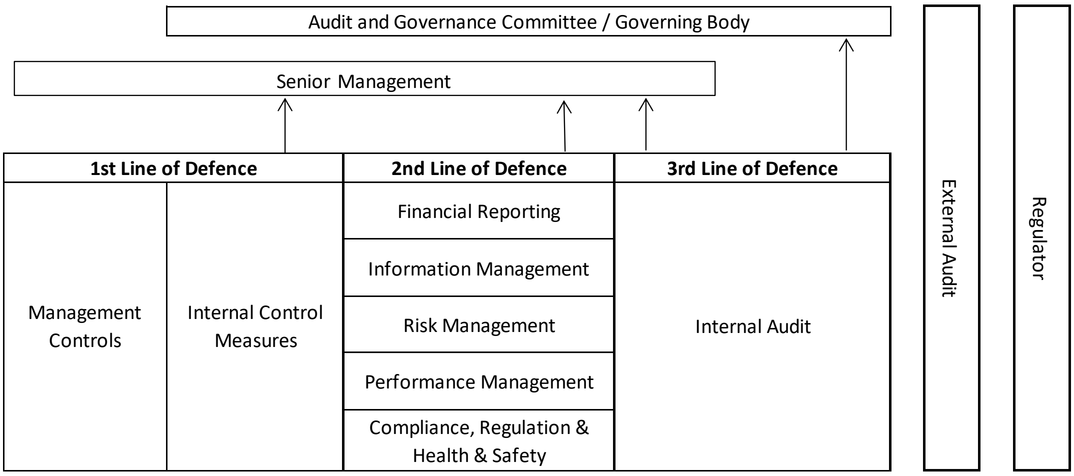
Note – for HSW risk assessment please refer to the process detailed in HSPS01 – Risk Assessment



Integrated Assurance has resulted in risk management being formally aligned and working alongside other compliance functions to promote a joined-up approach to all aspects of corporate governance.

Three Lines of Defence

The Three Lines of Defence Model is used as the primary means to demonstrate and structure roles, responsibilities and accountabilities for decision making, risk and control to achieve effective governance and integrated assurance. The diagram below shows the relationship between these functions:-



First Line of Defence – Management Controls and Internal Control Measures

Line managers are responsible for ensuring that a risk and control environment is established as part of day-to-day operations. Line management should be adequately skilled to create risk definitions and make risk assessments. The risk profile needs to be proactively reviewed, updated and modified for changes to the business environment and emerging risk changes. Active risk management and periodic reporting on risk is crucial to quick identification and response.

The first line of defence provides management assurance by identifying risks and business improvement actions, implementing controls and reporting on progress.

Second Line of Defence – Oversight Functions

The second line of defence consists of activities covered by several components of internal governance. This line of defence monitors and facilitates the implementation of effective risk management practices by operational management and assists the risk owners in reporting adequate risk related information across the organisation. These are usually management functions that may have some degree of objectivity, but are not entirely independent from the first line.

Second Line of Defence – Financial Reporting

Financial Regulations provide the framework for managing the Council's financial affairs. They apply to every member, committee, school governing body, department, officer, partner, employee of the Council, and anyone acting on behalf of the Council. The Responsible Finance Officer (Section 151 Officer) carries out the statutory duties in relation to the financial administration and stewardship of the Council. Departmental finance managers are required to bring the Responsible Finance Officer's attention to any section 151 issue they are unable to resolve.

Second Line of Defence – Information Management

Like its people, information is a key Council asset. Information management is how our information is collected, used, evaluated, protected and distributed. Information must be obtained, handled, retained and disposed of in line with organisation guidelines.

Information practices must help to improve the efficiency of the services offered by the Council.

Second Line of Defence – Performance Management

Managing employee or system performance and aligning their objectives facilitates the effective delivery of strategic and operational goals and maintains transparency. Effective performance management by using performance indicators to monitor performance of action plans and risk mitigation can also provide an early warning indicator so that issues can be resolved before they become a risk to the achievement of objectives.

Second Line of Defence – Compliance, Regulation and Health and Safety

Adequate compliance monitoring is required to ensure we are working within applicable laws and regulations in areas such as health and safety, supply chain, business continuity, civil protection, statutory complaints, environmental, anti-fraud, legal, safeguarding, HR and equalities.

Third Line of Defence – Internal Audit

Internal audit forms the third line of defence. An independent internal audit function will, through a risk-based approach to its work, provide assurance to the organisation's senior management. This assurance will cover how effectively the organisation assesses and manages its risks and will include assurance on the effectiveness of the first and second lines of defence. It encompasses all elements of the council's risk management framework (from risk identification, risk assessment and response, to communication of risk related information) and all categories of organisational objectives.

External Auditors and Regulators

External auditors and regulators reside outside of the Council structure but have an important role in the overall governance and control structure by providing an independent and objective function to assess the whole, or some part of the first, second or third line of defence.

Audit and Governance Committee

All three lines of defence have specific tasks in the internal control governance framework. It is the Audit and Governance Committee's role to maintain oversight and to monitor the effectiveness of internal controls and risk management processes, as well as internal audit activities.

Step by Step

There are a number of different types of risks that an organisation may face including financial loss, failure of service delivery, risks to people and damage to reputation. The process involves managers and their teams identifying what outcomes are expected from planned activities and what factors might hinder their delivery.

Step 1: Core purpose / outcomes
Before we can identify our risks, we need to establish the context by looking at what we are trying to achieve and what our proposed outcomes are. Depending on the area under review, the relevant objectives and outcomes will usually be detailed in existing documents, including the following: • Corporate Plan (for core purpose, priorities and outcomes) • Business Plans (for directorate/departments aims, priorities and actions) • Project Plans (for project aims and objectives) • Partnership Agreements (for partnership aims and objectives)
Step 2: Identify risks
To identify and articulate potential risks, managers and teams should consider their objectives and consider what factors may hinder delivery. The detail of any such factors should be explored to ensure that the underlying causes relating to potential risks are appropriately articulated. Risk is a key element of developing business cases for implementation of new programmes, projects or policy changes. Risks, particularly financial, are identified in reports to committees and out treatment of risk is public, open and transparent. Describing the Risk - The risks and opportunities identified need to be recorded in a structured format. A description covering the Cause, Event and Effect is used to scope a risk or opportunity. Guidance is appended to this strategy to assist in the development of the Risk Description.
Step 3: Identify existing risk controls / actions
Existing controls and actions, which are helping to eliminate or minimise the likelihood and/or impact of the risk occurring, are identified for each risk. These actions are specifically those already in place or completed. If there are no controls in place, this should be dealt with through mitigating actions. These controls and actions form part of the recorded risk when considered through the governance process.
Step 4: Assess pre-mitigation risk level
To ensure resources are focussed on the most significant risks, the Council's approach to risk management is to assess the risks in terms of both the potential likelihood and impact so that actions can be prioritised.

The risk management process requires each new risk to be assessed twice – pre-mitigation and post-mitigation. When undertaking the first assessment, the operation of key controls (above) should be considered. If key controls are likely to be ineffective this should be reflected in the initial risk score. Risk scoring guidance is appended to this strategy.
Step 5: Identify Mitigation
Not all risks can be managed all of the time, so having assessed the identified risks, cost effective action needs to be taken to manage those risks. When considering the application of mitigation, officers should consider – • What actions are required? • When must these actions be accomplished? • Who is responsible for taking action? • What resources are needed? • How will the action reduce the risk's probability or severity?
Step 6: Assess pre-mitigation risk level
The second assessment (the residual or net level) re-evaluates the risk, taking into consideration the effectiveness of the identified existing/mitigating actions. In considering the post-mitigation risk score the same criteria and matrix for assessing the pre-mitigation risk level is used. It is the risk owner's responsibility to ensure the agreed post-mitigation risk level for each risk is an accurate reflection of the likelihood and impact measures.
Step 7 – Review and report
The Risk Register is dynamic and the associated dashboard must be regularly reviewed and amended. Risks will be formally monitored every month by departmental management teams (DMTs). The questions asked during monitoring are: • Is the risk still relevant?

- Is there any movement in the risk score?
- Are the controls still in place and operating effectively?
- Has anything occurred which might change its impact and/or likelihood?
- Have potential opportunities been considered and maximised?
- Have any significant control failures or weaknesses occurred since the last monitoring exercise?
- If so, does this indicate whether the risk is increasing or decreasing?
- If the risk is increasing do I need to devise more controls or think of other ways of mitigating the risk?
- If the risk is decreasing can I relax some existing controls?
- Are controls/actions built into appropriate documented action plans?
- Are there any new or emerging risks?
- Have any of the existing risks ceased to be an issue (and can therefore be archived?)

When considering departmental risks, DMTs will consider the Council's agreed Risk Appetite and Risk Tolerance, before making decisions on the application of risk treatments as defined in the appendix.

Quarterly monitoring reports are presented for consideration by the Corporate Management Team prior to final ratification by the Audit and Governance Committee.

The Council's scrutiny function will play an increasingly important, open and transparent role in risk management. Scrutiny committees now consider risks pertinent to the terms of reference of the committee. This approach allows for detailed review of risk, its cause and mitigation, in the wider context of associated policy, performance and financial considerations.

RISK APPETITE

Risk appetite is the amount of risk, on a broad level, that Plymouth City Council is willing to accept in pursuit of value. It is strategic and reflects the organisations risk management philosophy, and in turn influences the organisation's culture and operating style. Risk appetite guides resource allocation and provides the infrastructure necessary to effectively respond to and monitor risks.

Risk appetite is an important tool for effective risk monitoring and provides the following benefits:-

- Forms an integral part of corporate governance
- Guides the allocation of resources
- Guides an organisations infrastructure, supporting its activities related to identifying, assessing, responding to and monitoring risks in pursuit of organisational objectives
- Is multi-dimensional, including when applied to the pursuit of value in the short term and the longer term of the strategic planning cycle
- Requires effective monitoring of the risk itself

Our aim is to consider all options to respond to risk appropriately and make informed decisions that are most likely to result in successful delivery of benefits whilst also providing an acceptable level of value for money.

Risk Appetite Statements

Compliance, Regulation and Safeguarding	No appetite for risk	The Council recognises the need to place high importance on compliance, health, safety and wellbeing, regulation, and public protection and has no appetite for breaches in statute, regulation, professional standards, ethics, bribery or fraud. It is not acceptable for any hazard, risk or safety incident to be ignored by any member of our workforce and the Council will ensure that systems and processes exist to identify and mitigate risk as well as for reporting, investigating and learning from incidents when they do occur. All health, safety and wellbeing risks should be managed as per absolute duties cited in relevant regulations or to as low as reasonably practicable irrespective of risk score.
Operational/Service Delivery	Medium appetite for risk	The Council accepts a medium to high level of risk arising from the nature of the Council's business operations and service delivery to deliver an appropriate level of service at value for money, whilst minimising any negative reputational impact.
Financial	Low appetite for risk	The Council acknowledges the responsibility it has for administration of public funds and wishes to emphasise to both the public and its employees the importance it places upon probity, financial control and honest administration.

		Financial Regulations provide the framework for managing the Council's financial affairs and should be adhered to at all times. Finance Business Partners are an integral part of Department Management Teams and should be consulted when planning any new project.
Reputation	Low appetite for risk	It is regarded as essential that the Council preserves a high reputation and hence it has set a low appetite for risk in the conduct of any of its activities that puts its reputation in jeopardy through any adverse publicity.
Strategic Change	High appetite for risk	The environment the Council works in is continually changing through both its internal operations and the services it provides. Change projects provide the Council with an opportunity to move forward and develop and establish benefits for the longer term. The Council recognises that this may require increased levels of risk and is comfortable accepting the risk subject to always ensuring that risks are appropriately managed.
Development and Regeneration	High appetite for risk	The Council has a continuing obligation to invest in the development and regeneration of the city. To continue to be progressive and innovative in the work performed the Council is willing to accept a higher risk appetite whilst ensuring that benefits are assessed and risks are fully scrutinised and appropriately mitigated in both economic terms but also social and environmental terms before developments are authorised. People and Culture
People and Culture	High appetite for risk	The Council recognises that staff are critical to achieving its objectives and therefore the support, development and wellbeing of staff is key to making the Council an inspiring and safe place to work. It has moderate to high appetite for decisions that involve staffing or culture to support transformational change and ensure the Council is continually improving.

The Council's Risk Appetite Statements will be continually monitored to ensure it supports the organisation's risk and opportunity management strategy.

RISK TOLERANCE

Risk tolerance is the level of risk the Council is willing to take on in terms of individual risks. When determining our risk tolerance the Council recognises that each risk is unique in nature.

The risk tolerance table below helps to align risk exposure with management and escalation activities. An event or risk is assessed and assigned a risk score by multiplying the impact and likelihood scores. Ranges of risk scores are then associated with different levels of management attention.

The acceptance of risk is subject to ensuring that all potential benefits and risks are fully understood and that appropriate measures to mitigate risk are established before decisions are made.

	Residual Risk Score	1-4	5-10	10 - 15	15-20	20-25
Risk Category	Compliance, Regulation & Safeguarding (including Health, Safety & Wellbeing)	Accept	Accept but monitor	Management effort worthwhile	Management effort required	Extensive management essential
	Financial	Accept	Accept but monitor	Management effort worthwhile	Management effort required	Extensive management essential
	Reputation	Accept	Accept but monitor	Manage effort worthwhile	Management effort required	Extensive management essential
	Operational/Service Delivery	Management effort to identify opportunities	Accept but monitor	Manage & monitor	Management effort worthwhile	Extensive management essential
	Strategic Change	Management effort to identify opportunities	Accept but monitor	Manage & monitor	Management effort worthwhile	Extensive management essential
	Development & Regeneration	Management effort to identify opportunities	Accept but monitor	Manage & monitor	Management effort worthwhile	Extensive management essential
	People & Culture	Management effort to identify opportunities	Accept but monitor	Manage & monitor	Management effort worthwhile	Extensive management essential

Evaluating Key Controls

A framework exists to performance measure effectiveness of key controls aligned to the Council's risk appetite. Risks where we have a lower appetite for risk taking are treated with a higher level of management activity and oversight.

Examples of key controls

Preventative key controls	Detective key controls	Corrective key controls
Policies and procedures	Review of performance	Business continuity plans

Authorisation and approval Verifications Staff training	Reconciliations Audit and investigations Data analysis Monitoring	Insurance Disaster recovery plans Variance reports Case reviews

Managers should contact the Performance and Risk Team for further advice on setting up key control performance measures for risks categorised under compliance, regulation, safeguarding, financial and reputation.

OPPORTUNITIES

Opportunities can also be identified by giving consideration to those that have been neglected because of perceived, but unexamined risk. These include:-

- Learning from the past – whilst past experience cannot necessarily be a predictor for future performance, signals that were ignored and missed opportunities can provide insight into organisational blind spots.
- Customer sensitivity – trying to understand customer needs and creating systems to exploit this information can lead to great gains.
- Learning from others – exploring and sharing best practice with other organisations can lead to benefits.
- Scenario planning – can be a powerful tool for generating new ideas.

Once the opportunity has been identified it should be described to include the expected benefits, contributions to business objectives and stakeholders.

Opportunity Types (not exhaustive list)	Opportunity response
Shared resource/technology/infrastructure, Improved designs	**Share** – An opportunity is shared with a partner or supplier to maximise the benefits
Economic/financial/market e.g. new and emerging markets, positive changes in exchange rates or interest rates	**Exploit** – A project could be adjusted to take advantage of a change in technology or a new market
Strategic/commercial opportunities such as new partnerships, new capital investment, new promoters	**Enhance** – Action is taken to increase the likelihood of the opportunity occurring or the positive impact it could have
*Contingency plans may be put in place should the opportunity occur. Political or environmental e.g. new transport links, change of government bringing positive changes in policy/opportunities for lobbying etc.	**Reject** – Here no action is taken and the chance to gain from the opportunity is rejected

HEALTH, SAFETY AND WELLBEING

The Council's HSW Policy and associated Health and Safety Performance Standards (HSPS) must be regarded as the standard that each department, service unit and team is expected to achieve and against which health and safety performance will be monitored and audited.

Refer to HSPS01 – Risk Assessment for the management of health and safety risks at the Council..

Risk assessments follow Health and Safety Executive (HSE) guidance and scoring methodology.

Any significant hazard requires risk control measures to be put into place in order to minimise risk to an acceptable level either by reducing the likelihood of an adverse event or the severity of its consequence, or both.

HSW Risk Escalation

Generally actions relating to risk assessments can be managed locally at team level, however, it may be necessary to escalate a health, safety and wellbeing risk to the departments Operational Risk Register in order to achieve a higher degree of management oversight. Examples of escalation criteria are:-

- Treatment of the risk requires decisions/actions, e.g. expenditures that are beyond what the budget holder is authorised to decide;
- risk controls cannot be implemented within appropriate timescales (as identified in consultation with a HSW Advisor);
- the risk is widespread beyond local area span of control;
- the risk is assessed to be significant - one in which staff, members of the public or facilities may be subject to legal, media or other interest and where, if not managed effectively, the risk could result in loss of life or significant loss of the council's assets or reputation;
- addressing the risk requires corporate changes to policy;
- Grievances from stakeholders have been received to which the risk owner cannot impartially and/or effectively respond.

HSW risks rated high will be reviewed at the HSW Steering Group and may be escalated to the Strategic Risk Register according to the Risk Tolerance criteria.

Fraud Risk Controls

Fraud is a major drain on the public purse and it is therefore imperative that all staff prevent fraudulent activity and understand the threats and risks. The Anti-Fraud, Bribery and Corruption Strategy and Policy will assist the Council in becoming more resilient to fraud risks. The aim is to minimise fraudulent activity with a zero tolerance approach to those who commit criminal acts of fraud against Plymouth City Council whether the threat is from outside or internally within the Council.

Guidance and Assistance

The Chief Executive Office, through the Head of Governance, Performance and Risk and the Performance and Risk Team, will promote and monitor good practice, provide guidance, support, advice and information and organise training. A Risk Management eLearning module is available on the Staff Room Page of the intranet within the Learning Zone.

Advice and guidance related to HSW risks can be sought by contacting the HSW Team.

APPENDIX I

Risk Categories

Category of Risk	Risk Examples
Compliance, Regulation and Safeguarding	▪ Legislation and internal policies/regulations ▪ Health, safety and wellbeing ▪ Grant funding conditions ▪ Legal challenges, legal powers, judicial reviews or public interest reports ▪ Change in government policy
Operational/Service Delivery	▪ Emergency preparedness/business continuity ▪ Poor quality/reduced service delivery ▪ Health and safety ▪ Information security and retention accuracy ▪ ICT integrity and availability ▪ Damage to physical assets ▪ Changing needs and expectations of customers – poor communication/consultation
Financial	▪ Budgetary pressures ▪ Loss of/reduction in income/funding, increase in energy costs ▪ Cost of living, interest rates, inflation etc. ▪ Financial management arrangements ▪ Investment decisions, sustainable economic growth ▪ Affordability models and financial checks ▪ Inadequate insurance cover ▪ System/procedure weaknesses that could lead to fraud
Reputation	▪ Negative publicity (local and national) ▪ Image ▪ Increase in complaints ▪ Brand building ▪ Fines
Strategic Change	▪ New initiatives, new ways of working, new policies and procedures ▪ New relationships – accountability issues/unclear roles and responsibilities ▪ Monitoring arrangements ▪ Managing change

	▪ Add value or improve customer experience/satisfaction ▪ Reduce waste and inefficiency ▪ Improve staff skills/morale ▪ Business alignment ▪ New operating models and revenue streams ▪ Market needs/growing competition ▪ New technologies
Development and Regeneration	▪ Demographics ▪ Economic downturn – prosperity of local businesses/local communities ▪ Impact of planning or transportation policies ▪ Environmental, landscape, countryside, historic environment, open space ▪ Property, land, buildings and equipment
People & Culture	▪ Political personalities ▪ Member support/approval ▪ New political arrangements ▪ Loss of key staff, recruitment and retention issues ▪ Training issues ▪ Lack of/or inadequate management support ▪ Poor communication/consultation ▪ Capacity issues – availability, sickness and absence etc.

Risk Description

Cause	Event	Effect
Because of …. As a result of …. Due to ….	<an uncertain event i.e. risk or opportunity> may occur	which would lead to <effect on objective(s)>
Event	**Cause**	**Effect**
Risk of …. Failure to …. Failure of …. Lack of …. Loss of …. Uncertainty of …. Delay in …. Inability to …. Inadequate …. Partnership with …. Development of / Opportunity to ….	…. due to ….	…. leads to …. and/or …. result in ….

Example of risk description – Risk of being unable to deliver Council services within the envelope of the resources provided in (year) which would lead to a negative impact on budgets, loss of reputation, negative impact on front line services and a negative opinion from external audit.

Risk Analysis and Scoring Guidance

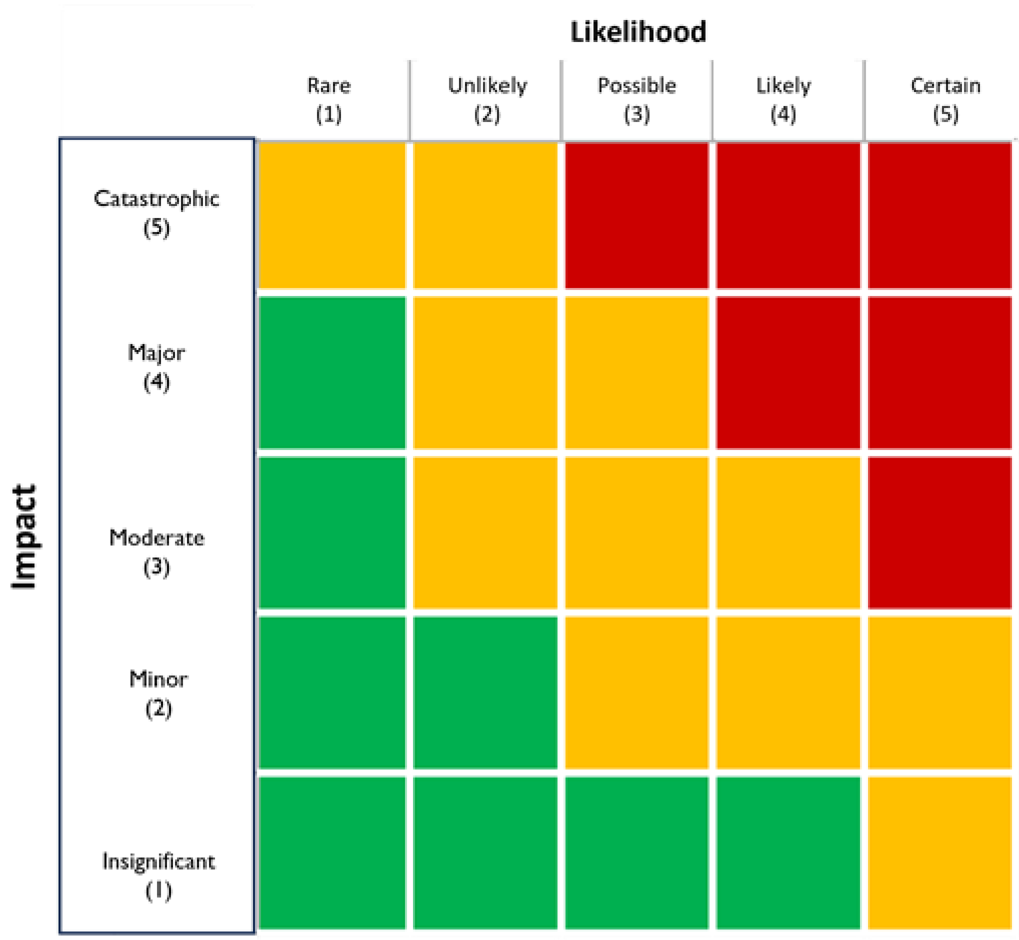
Note: refer to HSPS01 – Risk Assessment for Health, Safety and Wellbeing risks

Score	Likelihood	Threat / Risk
5	Almost Certain (81-100%)	• Is expected to occur within twelve months in most circumstances • Imminent/near miss
4	Likely (51-80%)	• Will probably occur in many circumstances • Will probably happen, but not a persistent issue e.g. once in three years • Has happened in the past
3	Possible (26-50%)	• Could occur in certain circumstances • May happen occasionally, e.g. once in 10 years • Has happened elsewhere
2	Unlikely (11-25%)	• May occur only in exceptional circumstances • Not expected to happen, but is possible e.g. once in 25 years • Not known in this activity • happening
1	Rare (0-10%)	• Is never likely to occur • Very unlikely this will ever happen e.g. once in 100 years
Risk Impact (Severity)		
Score	Impact	Threat / Risk
5	Catastrophic Risk	Risks which can have a catastrophic effect on the operation of the Council or service. This may result in critical financial loss, severe service disruption or a severe impact on the public. Examples:- • Unable to function without the aid of government or other external Agency • Inability to fulfil obligations • Medium – long term damage to service capability • Severe financial loss – supplementary estimate needed which will have a catastrophic impact on the Council's financial plan and resources are unlikely to be available • Death (single or multiple) or work related diagnosis leading to death

		- Adverse national publicity – highly damaging, severe loss of public confidence - Very significant exposure of public funds with funding being managed across organisations and complex reporting - Very complex stakeholder community with new partnerships, collaborations and suppliers/stakeholder environment volatile or with significant external change factors
4	Major Risk	Risks which can have a major effect on the operation of the Council or service. This may result in major financial loss, major service disruption or a significant impact on the public. Examples:- - Significant impact on service objectives - Short–medium term impairment to service capability - Major financial loss – supplementary estimate needed which will have a major impact on the Council's financial plan - Extensive injuries, major permanent harm, long term sick - Permanent/significant disability - Major adverse local publicity, major loss of confidence
3	Moderate Risk	Risks which have a noticeable effect on the services provided. Each one will cause a degree of disruption to service provision and impinge on the budget. Examples:- - Service objectives partially achievable - Short term disruption to service capability - Significant financial loss – supplementary estimate needed which will have an impact on the Council's financial plan - RIDDOR (Reporting of injuries, diseases and dangerous occurrences regulations) or major injury - Medical treatment required, semi-permanent harm up to one year - Some adverse publicity, needs careful public relations - High potential for complaint, litigation possible - Breaches of law punishable by fines only
2	Minor Risk	Risks where the consequences will not be severe and any associated losses will be minor. As individual occurrences they will have a negligible effect on service provision. If action is not taken, then such risks may have a more significant cumulative effect. Examples: - Minor impact on service objectives - No significant disruption to service capability - Moderate financial loss – can be accommodated at head of service level - Three day + injury - First aid treatment, non-permanent harm up to one month - Some public embarrassment, no damage to reputation

		• May result in complaints/litigation • Breaches of regulations/standards • Budget within delegation
I	Insignificant Risk	Risks where the consequences will not be severe and any associated losses will be relatively small. As individual occurrences they will have a negligible effect on service provision. If action is not taken, then such risks may have a more significant cumulative effect. Examples:- • Minimal impact, no service disruption • Negligible impact on service capability • Minimal loss – can be accommodated at senior technical accounting level • First aid injury • Unlikely to cause any adverse publicity, internal only • Breaches of local procedures/standards • Budget within delegation and relatively small or within operational costs

Risk Matrix Table



Risk Tolerance

Risk Tolerance		
Red (High Risk)	20 - 25	Must be managed down urgently.
Amber (Med/High Risk) Amber (Medium Risk)	12 - 16	Seek to influence medium term/monitor (as per risk appetite escalation)
Green (Low Risk)	6 - 10	Acceptable – continue to monitor if circumstances are subject to change, if not, remove from register
Yellow (Very low risk)	1 - 5	Can be removed from register and managed locally within team but consider adding to risk register if controls are likely to change

Risk Tolerance Actions

Tolerance Level	Escalation / Action Required
Extensive management essential	Escalate to Strategic Risk Register and brief Portfolio Holder. Monthly review at Senior Leadership Team level. Programme/project risks - Programme Board escalate to Strategic Risk Register. Quarterly review at Corporate Management Team. Risk owner to review monthly. Consider use of performance indicators to monitor performance of action plans and key risk controls.
Considerable management required	Consider escalation to Strategic Risk Register and brief Portfolio Holder. Monthly review at Department Management Team level. Programme/project risks - Programme Board consider escalation to Strategic Risk Register. Quarterly review at Corporate Management Team. Risk owner to review monthly. Consider use of performance indicators to monitor performance of action plans and key risk controls.
Management effort required	Add to Operational Risk Register and review at least quarterly at Department Management Team level (consider escalation to Strategic Risk Register if risk cannot be mitigated at department level and ensure Portfolio Holder is briefed).

	Programme/project risks - Programme Board oversight and consider escalation to Directorate Operational Risk Register. Six month review by Corporate Management Team. Risk owner to review monthly. Consider use of performance indicators to monitor performance of action plans and key risk controls.
Management effort worthwhile	Add to Operational Risk Register and review quarterly at Department Management Team level. Risk owner to review at least quarterly. Consider use of performance indicators to monitor performance of action plans and key risk controls.
Manage and monitor	Add to Operational Risk Register. Risk owner to review at least quarterly.
Accept but monitor	Risk owner to review every six months.