Appendix A

Eastern Shires Purchasing Organisation

RISK MANAGEMENT POLICY STATEMENT

Version Control

Version	Date	By whom	Changes	Comments
1	Feb 2007		Formulated	Committee March 2007
2	Jan 2012	DS	Review and Update	Circulation to SMT and Audit for comment
2b	Feb 2012	DS	Updated by strengthening commitment	Committee March 2012
2c	Feb 2013	CP	Review and Update	Committee March 2013
2d	May 2014	CP	Review and Update	Committee March 2014
3	May 2015	CP	Review and Update	Committee June 2015
4	Feb 2016	SL	Review and Update	Committee March 2016
5	Feb 2017	SL	Review and update	Committee February 2017
6	Aug 2018	SL	Review and Update	Committee September 2018

Risk Management Policy Statement

Contents

RISK MANAGEMENT POLICY

Definitions

Eastern Shires Purchasing Organisation - "The Organisation"

Eastern Shires Purchasing Organisation's Risk Management Policy - "The Policy"

Definition of Risk

"The effect of uncertainty on objectives. This effect may be positive, negative or a deviation from the expected."

Definition of Risk Management

"The process, by which risks are identified, evaluated and controlled".

Purpose of this document

The Organisation recognizes that it has a responsibility to manage risks effectively. This should help to anticipate and provide a better understanding and respond to changing social, political, technological, economic, legislative and environmental threats.

Understanding the above should help the Organisation to minimise uncertainty in achieving its objectives and maximise the opportunities to achieve its vision.

The policy forms part of the Organisation's internal control and corporate governance arrangements.

The policy explains the Organisation's underlying approach to risk management, documents the roles and responsibilities of the Management Committee, the Director and Leadership Team, and other key parties. It also outlines key aspects of the risk management process, and identifies the main reporting procedures.

In addition, it describes the process the Management Committee will use to evaluate the effectiveness of the Organisation's internal control procedures.

The benefit of risk management is having the knowledge both to anticipate potential risk, but also to understand how through choice such risks can be minimised. ESPO's aim is to reduce the effects of risk, and/or increase its ability to react by maximising its flexibility through responding whilst maintaining organisational stability. Risk management therefore not only includes the ability to anticipate forward events through the marshalling of data into intelligence but also involves developing the organisation's capabilities through continuous improvement.

Underlying approach to risk management

The following key principles outline the Organisation's approach to risk management and internal control:

- The Management Committee has ultimate responsibility for overseeing the process of risk management within the Organisation as a whole and they will approve the Risk Management Strategy on an annual basis.

- The Director and the Leadership Team are responsible for anticipating and identifying, assessing and managing risk, and advising and implementing policies approved by the Management Committee. Managing risk will involve ensuring controls are in place and are regularly monitored. In addition the Director is responsible for alerting the Management Committee on new identified risks that are deemed to have a potential serious impact on ESPO business.

- The Organisation makes conservative and prudent recognition and disclosure of the financial and non-financial implications of risks.

- The Director and Assistant Directors are responsible for ensuring good risk management practice within their divisions

- The Director will report to the Chief Officers Group and Management Committee quarterly on the Corporate Risk Register.

Role of the Management Committee

1. The Management Committee has a fundamental role to play in the management of risk. Its role is to:

   i) Influence the culture of risk management within the Organisation.

   ii) Determine the appropriate risk appetite or level of exposure for the Organisation.

   iii) Approve major decisions affecting the Organisation's risk profile or exposure.

   iv) Ensure that a Corporate Risk Register is established, including details of the actions taken to mitigate the risks identified.

   v) Consider risks attached to proposals for new, or changes to, policies and service delivery arrangements

   vi) Annually review the Organisation's approach to risk management and approve changes or improvements to key elements of its processes and procedures.

Role of the Director and Leadership Team

2. Key roles of the Director and Leadership Team are to:

   i) Establish, gain approval from the Management Committee and implement policies on risk management and internal control i.e. to ensure that an adequate risk management framework and associated control environment is in place. Liaise with the servicing authority on all aspects of risk management.

   ii) Identify, evaluate, and manage the fundamental strategic risks faced by the Organisation for consideration by the Management Committee.

   iii) Determine the level of risk appetite, currently set at 10.

   iv) Ensure regular updating of the Corporate Risk Register.

   v) Identify, evaluate, and manage all operational and strategic risks faced by the Organisation. These should be clearly identified as such on the organisation's Corporate Risk Register.

   vi) Business Continuity and Procurement, Health and Safety – sit at Operational risk register level but flow into the Corporate Risk Register because of their significance. The responsibility for managing these is still at Assistant Director level but with scrutiny and challenge by Director as to movement on actions.

   vii) Provide information in a timely manner to the Management Committee on the status of risks and controls. Timing will depend on the level of risk, but quarterly, and where addition or new risks are evaluated and escalated (such as new procurement projects) then these will be approved prior to sign off.

   viii) To maintain awareness of and promote the risk management policy to all relevant staff (use of key documents published via intranet).

   ix) Arranging/providing risk management training as appropriate

x) Ensure synergy with other “risk” systems, e.g. Health and Safety, business continuity and project management

xi) Undertake an annual review of effectiveness of the system of internal control and provide a report to the Management Committee.

Role of Procurement Management

3. Key roles of Procurement Management are to:

i) Maintain awareness of risk management principles and take responsibility for managing risk within their own working environment.

ii) Apply risk management to those risks requiring further action, particularly new developments and “procurement or project" work.

iii) Maintain, and update where appropriate any project records of risk assessments undertaken and resulting action plans.

iv) Reporting systematically and promptly to their managers or Leadership Team any perceived new risks or failures of existing control measures.

Risk management as part of the system of internal control

4. The system of internal control incorporates risk management. This system encompasses a number of elements that together facilitate an effective and efficient operation, enabling the Organisation to respond to a variety of operational, financial, and commercial risks. These elements include:

a. Policies and procedures

Standard Operating Procedures and policies are used to improve business efficiencies and reinforce a standard approach to documents that are used externally, whilst at the same time underpinning internal control processes. The policies are approved by the Leadership Team and implemented and communicated by senior management to staff. Written procedures support the policies where appropriate.

b. Reporting

Comprehensive reporting is designed to monitor performance, reviewing key risks where appropriate. Decisions to rectify concerns are made at regular meetings of the Leadership Team, and the Management Committee if appropriate. Market information is vital for developing management knowledge as a core element of the business.
The mastering of such information through the monitoring of the external environment goes hand-in-hand with a comprehensive risk management process. Capturing and centralising such market intelligence will lead to developing better expertise and organisational capabilities, improving the quality of decision making, and enable a quick response to changing external conditions.

c. Business planning and budgeting

The business planning and budgeting processes are used to set targets, agree action plans, and allocate resources in order to achieve the long term objectives of the organisation articulated in the MTFS for 2017-2019. Progress towards meeting business plan targets is monitored weekly/monthly depending on individual targets.

d. High level risk framework (strategic risks)

This framework is compiled by the Leadership Team and helps to facilitate the identification, assessment and ongoing monitoring of risks fundamental to the Organisation. These are strategic risks that might impact on the high level, medium to long-term, goals and objectives of ESPO, together with those cross cutting issues that have potential to impact significantly on service delivery, business continuity and profit generation.

The Corporate Risk Register document is reviewed quarterly with emerging risks being added as required, and improvement actions and risk indicators are monitored regularly.

e. Operational risk management

These have been considered as the following:

- Health and Safety (Office, warehouse, transport);
- Procurement Projects;
- Business Continuity.

The latter has both strategic and operational aspects and has been considered in **separate documentation**.

i) Health and Safety is discussed quarterly by the Leadership Team in conjunction with risk management. It is chaired by the Director and attended by the full Leadership Team and the Health, Safety and Wellbeing Advisor. Meeting every six weeks, the Joint Consultative Committee acts as a conduit to the quarterly risk management meeting and is chaired by the Assistant Director – Operations and attended by the HR Advisor, trade unions, staff representatives and Health, Safety and Wellbeing Advisor. The function of the two groups is to review the measures taken to ensure the health and safety at work of employees. One of the main objectives of these groups is to promote co-operation between staff and management in instigating, developing and carrying out measures to ensure the health and safety at work of the employees.

Specific Objectives are:

- The study of accident and notifiable disease statistics and trends, so that reports can be made to management on unsafe and unhealthy conditions and practices, together with recommendations for corrective action;
- Examination of safety audit reports on a similar basis;
- Consideration of reports and factual information provided by inspectors of the enforcing authority appointed under the Health and Safety at Work Act;
- Consideration of reports which safety representatives may wish to submit;
- Assistance in the development of works safety rules and safe systems of work;

- A watch on the effectiveness of the safety content of employee training;
- A watch on the adequacy of safety and health communication and publicity in the workplace;
- The provision of a link with the appropriate enforcing authority;
- To fulfil the employer's legal duty to consult with Health & Safety Representatives;
- To discuss and review the effect of new Health and Safety law and the organisation's proposals for implementing the new law;
- To monitor and review the effectiveness of the organisation's safety policy;
- To develop and agree health and safety standards and procedures applicable to the workplace;
- To review the organisation and administration of any occupational health and safety services provided by the organisation.
- Review of insurance or other such claims and recommend measures to reduce the likelihood of future claims

ii) Procurement. ESPO has significant procurement expertise to enable it to handle a diversity of contracts, some of which are particularly complex. ESPO has developed a business case process that requires both reward and risk to be evaluated and assessed as part of the compliance process. Risks are assessed at a Pre-Procurement Panel and at Contracts Panel (contract award) and on rare occasions are escalated to the Leadership Team. Supporting the tender process are a series of Standard Operating Procedures and a library of standard documentation.

iii) Business Continuity. A complete rewrite of our Business Continuity documentation has been undertaken by our recently appointed Business Continuity consultants, Phoenix. It was considered important to appoint experts in the field to update our existing documentation. This policy is reviewed on an annual basis.

iv) The risks within the change programme have now been incorporated in to the CRR. Alongside the risks within the CRR, any risks that have a residual score of 10 or more are reviewed on a quarterly basis. Any new risks are added and obsolete risks are deleted from the register.

The following statements may be applicable for inclusion within the policy:

f. Fraud and Corruption

The organisation is set against fraud and corruption and is committed to an effective Anti-Fraud and Corruption Strategy. Identification and addressing the risk of fraud and corruption are a key element within this risk management strategy. All members of staff are also required to undertake a mandatory course on fraud and Awareness to facilitate the above.

g. Auditors

LCC Internal Auditors are required to report to the Director and Consortium Treasurer on internal controls and alert Management to any emerging issues. In addition, the Director and Treasurer oversee internal audit, external audit and management as required in their review of internal controls. They are therefore well-placed to provide advice to the Management Committee on the effectiveness of the internal control system, including the Organisation's system for the management of risk.

h. Internal audit programme

Internal audit is an important element of the risk management process. Apart from its normal programme of work, internal audit is responsible for aspects of the annual review of the effectiveness of the internal control system within the organisation.

i. External audit

External audit provides feedback to the Management Committee on the operation and adequacy of the internal financial controls reviewed as part of the annual audit.

j. Third party reports

From time to time, the use of external consultants will be necessary in areas such as marketing, IT systems and human resources. The use of specialist third parties for consulting and reporting can increase the reliability of the internal reporting systems.

k. Chief Officer Group (COG)

The COG consists of chief officers from all member authorities who meet regularly with the Organisation's senior management. The COG provides advice and guidance to facilitate the identification and assessment of procurement risks to the Organisation.

Annual review of effectiveness

5. The Management Committee is responsible for reviewing the effectiveness of internal control of the Organisation, based on information provided by the Director, Treasurer and auditors. Its approach is outlined below.

6. For the fundamental risks identified, the Director will seek the Management Committee's approval on the results of:

- A review of the Organisation's prior year record on risk management and internal control

- A Review of the risk profile for the coming year and of the adequacy of current internal control arrangements.

- A recommendation, if required, for investment in further control arrangements.

7. In determining recommendations the Management Committee, the Director will consider the following aspects.

   a. Control environment:

      - The Organisation's objectives and its financial and non-financial targets
      - Organisational structure and calibre of staff available.
      - Culture, approach, and resources with respect to the management of risk
      - Delegation of authority
      - Public reporting.

   b. On-going identification and evaluation of fundamental risks:

      - Timely identification and assessment of fundamental risks
      - Prioritisation of risks and the allocation of resources to address areas of high exposure.

   c. Information and communication:

      - Quality and timeliness of information on fundamental risks
      - Time it takes for control breakdowns to be recognised or new risks to be identified.

   d. Monitoring and corrective action:

      - Ability of the Organisation to learn from its problems
      - Commitment and speed with which corrective actions are implemented.

8. The Director prepares a report of his review of the effectiveness of the Organisation's internal control system within the Annual Statement of Accounts and presented to the Management Committee for consideration and approval (normally the Committee meeting in June), prior to the final approval of Accounts in September.

RISK MANAGEMENT GUIDE

Background

ESPO Management and staff have been facing and managing risk for over thirty years resulting in a successful organisation that has exploited opportunities to become one of the UK's largest local authority purchasing consortiums.

However, in recent years there has been increasing focus on the corporate governance arrangements of both public and private companies with the aim of achieving greater transparency. This requirements is reinforced by the recommendation that local authorities should make a statement as to how they have complied with their local governance code, and how they have monitored the effectiveness of their corporate governance arrangements in their annual Statements of Accounts.

Risk Management provides assurance that:

- objectives are more likely to be achieved;
- damaging events will not happen or are less likely to happen
- beneficial events will be or are more likely to be achieved
- make more informed decisions
- prevents injury, damage and losses and reduces the cost of risk.

The risk management method enables:

- the identification and evaluation of risks;
- helps in setting acceptable risk thresholds;
- the identification of controls against such risks; and
- helps identify indicators that give early warning that a risk is becoming more serious
- embraces and exploits opportunities to explore new innovative ways of working and identifying opportunities to reduce costs and improve outcomes
- Improve co-ordination and consistency of service delivery
- Supports sustainable improvements in our activities and the achievement of value for money.

Risk Definition

Risk is the threat or possibility that an action or event will adversely or beneficially affect the organisation's ability to achieve its objectives.

This definition links risk to achieving the strategic and business objectives and also identifies that risk management is not just about recognising and mitigating negative risks but also identifies risk-taking opportunities that may lead to positive benefits.

Risk can be seen as short term, such as an event, or a conjunction of events harmful to both tangible and intangible assets. It can be also be long term where there is a gradual disconnect between the organisation and its external environment.

Risk management is having the knowledge both to anticipate potential risk, but also to understand how through choice such risks can be minimised. ESPO's aim is to reduce the effects of risk, and/or increase its ability to react by maximising its flexibility through responding whilst maintaining organisational stability.

Risk management therefore not only includes the ability to anticipate forward events through the marshalling of data into intelligence but also involves developing the organisation's capabilities through continuous improvement.

Internal controls

Internal controls are a range of regulations, procedures and policies the organisation uses to manage its work and any additional controls or mitigating actions taken to deal with a particular situation.

The aim of risk management is to ensure that these controls are effective in identifying, evaluating, monitoring and minimising the risks ESPO faces in its day-to-day activities or any future ventures.

The level of risk faced by an organisation before any internal controls are applied is known as the gross or raw risk.

The level of risk faced by ESPO after internal controls have been applied is known as the net or residual risk. Controls will not eliminate the risk but help us to manage it; therefore this is also known as the organisation's "exposure to risk".

The controls are those management actions taken to deal with a particular risk. A judgement is made on the numerical reduction to the raw risk score to produce the residual risk score.

Risk Indicators provide a series of 'warning lights' which provide early warning that action may be required to mitigate a particular risk through stronger internal controls, or if it is outside ESPO's control, to be aware of it and closely monitor.

ESPO also has to determine where it resides it terms of a spectrum ranging from 'risk-taking' to being 'risk averse'. The amount of risk ESPO is prepared to tolerate before action is required is known as 'risk tolerance'

The Size of Risk - Heat Map represents the ESPO's risk scoring matrix.

The risk appetite is reviewed by the Management Committee and is currently set at 10. In the quarterly risk review meetings, all risks over 10 are reviewed. New risks and opportunities are added and obsolete risks are removed.

ESPO's Corporate Risk Register has a summary table ranking each risk according to its score.

The Management Committee will receive reports, at least annually, on risk management arrangements and assessments. This will include where appropriate any revised policy, and the corporate risk register. Any changes to risk levels highlighted as a result of the Health and Safety and the management of Business Continuity will be reported upon through the corporate risk register together with a report on risk management included within the annual statement of Accounts.

Risk Management Process

The stages are summarised below with a commentary on the arrangements at ESPO.

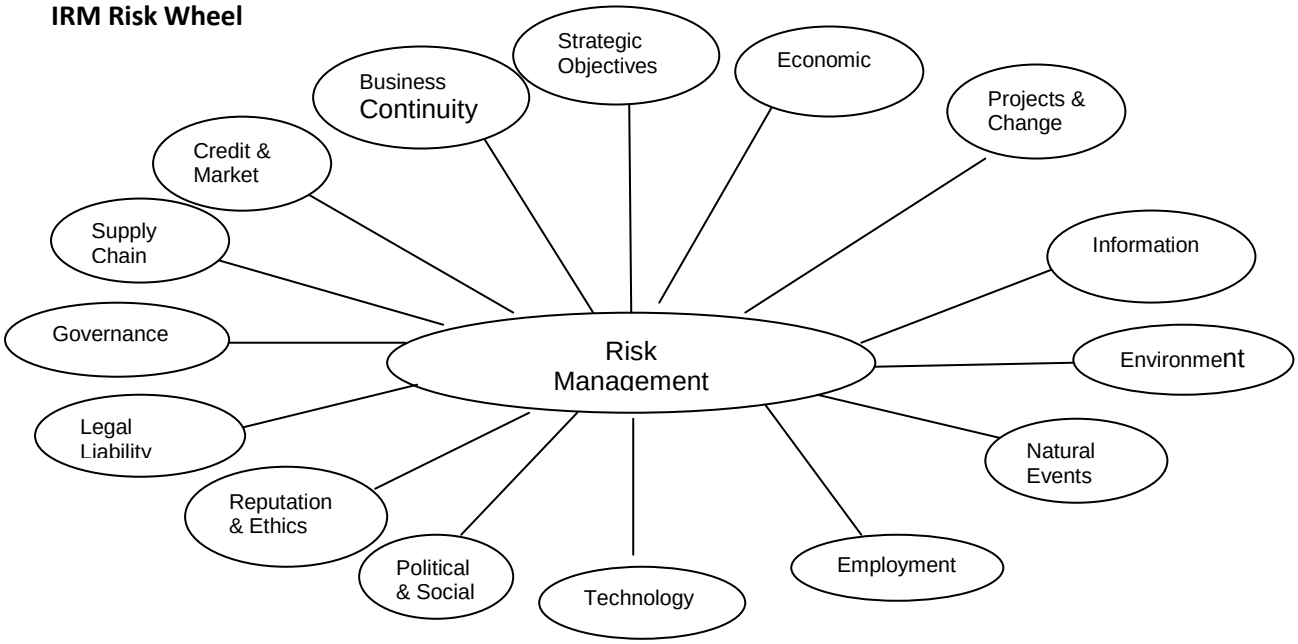
Identify the risks

This is the first stage to use where the risks that may affect a particular new activity, existing operational activity or project are listed. At this point opportunities can be considered and risks grouped. This work forms the basis of the risk register.

Risks can be classified as Internal or External with the latter being categorised as:

- Reputation
- Financial Loss
- People
- Regulatory
- Business Objectives

IRM Risk Wheel



Identify probable risk owner(s) and a risk co-ordinator

The risk owner assesses the risk, detailing how actions can be taken and by when to reduce the likelihood and severity of the risk to an acceptable level. All actions detailed need to consider and detail who is do what and when. If monitoring or reporting is involved the frequency and responsibility for such reports should also be included.

- All risk assessments should be dated (i.e. date of completion) and certified by the risk owner.
- Responsibility and an action completion date should be assigned to all actions on the CRR.
- Where risks are high, above a residual score of 10, with further action required, action taken and progress on further action taken should be monitored by the leadership team on a quarterly basis. Any new risks are added and obsolete risks are deleted.

All Risk owners for those risks that affect the whole organisation will be the Leadership Team. At a project level the risk owner should be the project manager. Risk owners should be added to the risk register.

The risk co-ordinator collates all the risks to create a risk register and manages the risk reporting process.

Evaluate the risks

The risks should then be evaluated for impact and likelihood. An assessment of the timing of the risk can also be made.

The scales used for impact and likelihood are as follows:

Impact:

1. Negligible
2. Low
3. Medium
4. High
5. Very High

Likelihood:

1. Very Low
2. Low
3. Medium
4. High
5. Very High

The combined scores on a 5 x 5 matrix will give scores ranging from 1 to 25 depending on the severity of the risk. These numbers are indicative only as the process is not an exact science but most importantly it assists in thinking about the risk.

The total risk score divisions are as follows:

1 – 6 - Low
8 - 12 - Medium
14 - 20 - High
Over 20 - Very high

The Size of Risk - Impact Guide provides examples for likelihood, impact and total risk score. Once this has been completed the risks are prioritised and ranked according to score and proximity. The risk register is updated accordingly.

Identify suitable responses to risk

Where needed, a range of practical responses to each significant risk on the risk register is be identified and recorded on the register.

Range of responses (controls) to a risk:

- **Reduce** - take action to reduce either the probability of the risk developing further, or its impact.
- **Accept** - when the probability and impact are low producing a total risk score below 7, or when it would be too expensive to mitigate a risk.
- **Transfer** - transferring the risk to a third party, e.g. insurance.
- **Terminate** - identifying actions to eliminate the risk such as withdrawing from the activity.
- **Contingency** - a plan of action to be implemented when a risk develops further or passes through a risk threshold.
- **Prevent** - identifying measures to prevent a risk having an impact on an organisation.

Responses are proportional to the risk and mapped against the risks on the risk register.

Implement responses

The most appropriate responses to each risk will be determined and implemented by ESPO Management in order of priority. Approval for additional earmarked funding required to implement responses may be requested from the Management Committee. Responses when implemented should bring the most serious risks below the risk tolerance thresholds. Once implemented the responses will be monitored by Management and amended as necessary

The risk tolerance threshold score has been set at 10 or less. The exact meaning of this value is somewhat subjective and this is will be reviewed annually to assess whether it is appropriate as a methodology to highlight the key risk areas. All strategic risks even with a score less than 10 will appear on the register. Those that are red will be prioritised and will be considered quarterly by the Leadership team.

Assurances about effectiveness

The risk responses implemented are assessed for effectiveness in keeping the risks within agreed tolerance levels by regular monitoring of the risk indicators. Internal and external audit reports provide further assurance on effectiveness.

Embed and review

The risk management arrangements are reviewed on a regular basis including a review of the risk register and a report will be produced for the Management Committee, normally in June. The report will assess the effectiveness of the measures to control risk with recommendations for improvement or development.

All risks are reviewed quarterly by the relevant Assistant Directors for their operational areas, but those risks above the risk appetite (>10) should feature in the CRR for review and monitoring by the Leadership Team with subsequent reporting to Chief Officer Group and Management Committee.

The Annual Governance Statement (June Committee) will also include a review of Risk Management policy and processes.

Size of Risk - Impact Guide

This Impact Guide is designed to assist in determining the scores applied to any risk. In the application within ESPO a 5 x 5 scale for impact and likelihood is used.

Impact ranges from Negligible (1) to Very High (5). Likelihood ranges from Very Low (1) to Very High (5). The combined scores on a 5 x 5 matrix will give scores ranging from 1 to 25. The scoring will be determined on the basis of the Leadership Team's opinion of the residual risk after taking account of their perception of the effectiveness of the existing controls. These numbers are indicative.

The combined risk score can then be calculated to determine the severity of the risk on the following scale:

- 1 - 6 Low
- 8 - 12 Medium
- 14 - 20 High
- Over 20 - Very high

Impact Grid

The Impact Grid is the scoring matrix referred to above with risk thresholds applied according to the total risk score. Applying colours in this way is sometimes known as the 'traffic light' method. This gives 3 levels of risk denoted by colours in this case - red being the most serious; yellow being the middle level; and blue the least serious.

If, upon review, a risk crosses one of the thresholds it should trigger either an increase or decrease in the internal controls applied to it.

Severity						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Likelihood				

Red
Yellow
Blue

Size of Risk – Impact Guide

The Impact guides are only for guidance and are not intended to be prescriptive.
It should be the worst-case scenario that is usually used to rate the risk.

Level	Severity	Reputation	Financial (per	People	Regulatory	Business Objectives
1	**Negligible**	Internal	Less than £50,000	No	No	• No impact
2	**Low**	Local (Minor adverse publicity)	Between £50,000 - £250,000	Minor Injury	No Consequence	• Loss of a minor contract
3	**Medium**	Local or limited adverse publicity	Between £250,000 - £500,000	Major reversib le injury	Limited regulatory consequence	• Major IT Project is late • Loss of a major contract
4	**High**	Negative headlines in national press	Between £500,000 - £750,000	Serious Injury	Significant regulatory consequence	• Member authority leaves Consortium • ESPO IT systems fail and cannot be recovered • Major loss of sales due to staff shortages in the warehouse e.g. Flu pandemic
5	**Very High**	Sustained negative headlines in regional/nation al press	Greater than £750,000	Fatality	Substantial regulatory consequence	• Major buildings fire resulting in closure • Sustained failure to recruit staff

Size of Risk – Likelihood

Level	Descriptor	Likelihood	Description
1	**Negligible**	2% Likely	May occur only in exceptional circumstances
2	**Low**	5% Likely	Not likely to occur in normal circumstances
3	**Medium**	10% Likely	Could occur at some time
4	**High**	20% Likely	Will probably occur in most circumstances
5	**Very High**	50% Likely	Is expected to occur in most circumstances.

This page is intentionally left blank