.

Shropshire
Fire and Rescue Service

Brigade Order

Administration	
Title	**Risk Management**

Contents	Page No.

Roles, Responsibilities and Review

The **Assistant Chief Fire Officer (Service Support)** is responsible for ensuring this Order is implemented across the Service.

The **Transformation and Collaboration team** will be responsible for the day-to-day operation of the Order.

The **Transformation and Collaboration team** will review this Order when new legislation arises or as and when organisational needs require.

Brigade Order: Administration

Risk Management

Purpose

This Order guides the way in which the Authority will identify, quantify, control, and manage its risks.

Strategic Goals

This Order supports all of the services Strategic goals as outlined in the Service Plan.

Introduction

The aim of Shropshire and Wrekin Fire Authority's Risk Management policy is to mitigate risk events occurring (wherever this is possible) and minimise the severity of their consequences if they do occur or increase the likelihood of a positive risk (opportunity) occurring and the benefits that could be gained. Even when the likelihood of an event occurring cannot be controlled, steps will be taken to ensure the resultant impact on the Service is within the Authority's defined level of tolerance as guided by the risk assessment (rating) or each risk.

Risk Management is critical to the effective delivery of the Fire Authority Community Risk Management Plan, strategic goals and priorities. Both the Fire Authority and Service are committed to embedding the application of this policy to ensure a strong and consistent approach to risk management.

What is risk management?

Risk management is the process of identifying risks (both negative 'threats' and positive 'opportunities'), evaluating their potential consequences and determining the most effective and efficient methods of mitigating and/or responding to them. It is not an end in itself. Rather, risk management is a means of minimising the costs and disruption to the Service caused by undesired events, ensuring that services to Shropshire communities are not negatively impacted

The benefits of managing risks

Effective risk management will deliver a number of benefits to the Service as a whole. Risks will vary in their nature and extent from department to department. They are all important, and often a risk will not be able to be addressed by one role or department. Usually it will take collaborative working to resolve a risk and therefore it is vital that the linkage is made between the various elements of the Fire and Rescue Service, if the Authority wants to safeguard its reputation and demonstrate its ability to deliver best value. Potential benefits to come from effective risk management arrangements include:

- **Improved strategic management**
    - Better informed selection of strategic priorities and associated Corporate Performance Indicators as a result of the risk identification, analysis, control and

monitoring process

- Greater ability to deliver against more realistic and achievable priorities and Corporate Performance Indicators

- Allowing informed decisions to be made by the right people at the right time.

- **Improved operational management**

  - Reduction in interruptions to service delivery

  - Reduction in managerial time dedicated to dealing with the consequences of a risk event having occurred

  - Enhanced managerial control as a result of risk identification, analysis, control and monitoring

  - A more systematic approach to addressing legislative, regulatory or competitive demands

  - Improved control of the risks associated with any indirect or contractual working arrangement

  - Improved health and safety and the enhanced condition of property and equipment

  - Creating positive risk management behaviours and culture.

- **Improved financial management**

  - Better informed financial decision-making on investment, insurance, option appraisal, etc.

  - Enhanced financial control as a result of risk identification, analysis, control and monitoring

  - Reduction in the financial costs associated with losses due to service interruption, litigation, poor investment decisions, etc.

  - Reduction in insurance premiums and/or direct costs met through self-insurance

- **Improved service's to local communities**

  - Minimal service disruption to service users and stakeholders and a positive external image as a result of all of the above.

Roles and responsibilities for risk management

Identifying and allocating roles and responsibilities for risk management is essential if the process is to be implemented and reviewed effectively.

Risk management as explained further into this policy is undertaken through a standard and consistent approach whichever type of risk. Risk owners from officers to members, should receive the appropriate training and guidance to ensure a confident and consistent approach across the Service in managing risk.

All staff have a role in mitigating and managing risk through the activities they undertake in their roles. Separate to this there are responsible 'risk owners' and 'stakeholders' that have responsibility in owning departmental, project, programme, , or corporate risks.

Key owners and stakeholders are set out below:

Fire Authority Members

Members have the role of overseeing the effective management of risk by officers. In effect, this means that they will agree the strategy, framework and process put forward by SMT– as well as the corporate risks for action. They will also review the effectiveness of corporate risk management. This role is delegated to the Standards Audit and Performance Committee.

They may also be involved in providing reports to stakeholders on the effectiveness of the risk management framework, strategy and process.

Service Management Team (SMT)

SMT has a crucial role to play in risk management. The management team need to take a lead in identifying and managing the risks and opportunities facing the Authority. As risk management needs to be fully embedded into the culture and operations of a Fire Authority, it is essential that the process is led from the top.

So, SMT are not only responsible for determining the Risk Management strategy, framework and process, it also will identify, analyse and profile the corporate and crosscutting risks associated with any new policies, service delivery methods, or existing operations and will determine Shropshire and Wrekin Fire and Rescue Authority's risk appetite and priorities for action.

The SMT will also be involved in providing reports to SAP and stakeholders such as the HMICFRS, on the effectiveness of the risk management framework, strategy and process.

SMT also has responsibility for providing assurance and challenging each other on a peer to peer basis regarding corporate performance and corporate risk at the Performance and Risk Group (PRG) which meet quarterly.

Heads of Service (SMT)

Heads of Service will also extend the process cascaded from levels above to within their own service areas, these will usually be project and/or departmental risks. Some risk

actions and tasks will be cascaded to them from processes above, but there will be other risks that are important to the section concerned.

Middle Managers

This group of staff will often own risks through departmental or project planning processes as they may be the lead in this area.

All staff and other service providers

Individuals involved in service delivery, whether employed by Shropshire and Wrekin Fire Authority or by its partners, have a crucial role to play as they deal with risk on a daily basis. Usually they will be carrying out tasks which support controlling risks and as such need to have a more general awareness of risk issues and are therefore encouraged to feed views into the formal processes above them.

Partners

Shropshire and Wrekin Fire and Rescue Authority works with a wide range of partners in delivering its services. It is important that those partners are brought into the risk management framework and this will be usually achieved by the risk owner.. It is essential that accountabilities are adequately determined and that Shropshire and Wrekin Fire Authority does not overlook any risks that may fall on it arising from its part in a joint venture. Even where there is transfer of operational risks, for example under a PFI, there will undoubtedly be some residual risks falling on the Authority. It is not possible to outsource the risk management process.

Internal Audit

Should provide independent and objective assurance on the effectiveness of the organisation's risk management arrangements and share good practice through comparative assessment.

Appendix B details the various activities undertaken in the Risk Management process and each key player's responsibilities in that area.

Defining risk

Risk has been defined as '**the uncertainty of outcome'**, whether it be a positive **opportunity** or negative **threat** (Cabinet Office; Management of Risk in Government).

For all of us, the future contains an element of the unknown. The public has a right to expect public services, such as the Fire and Rescue Service, to anticipate events that could occur in the future and plan to reduce either the likelihood of their happening, or the disruption they could cause.

Risk management is very much a part of every manager's day-to-day responsibility. It should not be considered as a 'bolt-on' activity. It helps to inform judgements about the appropriateness and effectiveness of policy options or service delivery methods. As such, it is integral to both strategic planning and service management. It will also inform decisions about the level and nature of insurance cover required.

To manage risk effectively, the risks associated with each policy option or service delivery method must be systematically and continuously identified, analysed, controlled, reviewed and monitored. This process is referred to as 'the risk management cycle'.

Risk Management is identified earlier in this policy. Corporate Risks specifically are those risks that if realised will result in significant impact on the Authority's ability to provide services to its communities.

The risk management cycle is set out below.

Figure 1.

Corporate risks

Corporate risks are those which need to be take into account in judgements about the medium to long term goals and objectives of the Service as a whole. These are likely to have significant impact across more than one department in the Service and could prevent the Authority and Service from delivering its statutory duties and strategic objectives as defined in its Community Risk Management Plan and strategy. The management of these risks could involve significant resources and therefore the Risk Owner is likely to be one of Service Management Team

The sort of risks that could impact in this way include:

- **political:** those associated with a failure to deliver either local or central government policy, or meet the Combined Fire Authority's objectives

- **economic:** those affecting the ability of the Authority to meet its financial commitments. These include internal budgetary pressures, the failure to purchase adequate insurance cover, or even external macro level economic changes

- **social:** those relating to the effects of changes in demographic, residential or socio-economic trends on the Authority's ability to deliver its objectives

- **Commercial:** those relating to the failure of suppliers or our commercial relationship with these suppliers

- **technological/information:** those associated with the capacity of the Fire and Rescue Service to deal with the pace/scale of technological change, or its ability to use technology/information systems to address changing demands. They may also include the consequences of internal technological failures on the Fire and Rescue Service's ability to deliver its objectives such as cyber security.

- **legislative:** those associated with current or potential changes in national or European law e.g., the appliance or non-appliance of Transfer of Undertakings, Protection of Employment Regulations 1981 (TUPE),

- **environmental:** those relating to the environmental consequences of progressing the Authority's strategic objectives e.g., in terms of energy efficiency, pollution, emissions, etc.

- **competitive:** those affecting the competitiveness of the Service (in terms of cost or quality) and/or its ability to deliver best value

- **customer / stakeholder:** those associated with a failure to meet the current and changing needs and expectations of customers and stakeholders.

Departmental, Programme and Project risks

Departmental risks relate to the achievement of a single department /sections stated objectives and relate to matters which managers and staff will encounter in the daily course of their work.

The management of these risks will not typically involve resources beyond those available to the department and therefore the Risk Owner is likely to be the head of that department or manager of that section.

Programme risks encompass the achievement of multiple projects within a programme and relate to matters which the programme manager will encounter more broadly across a programme of work.

Project risks relate to the individual projects which project managers will encounter which are localised and more specific to the management of their project/s. These risks may be short term and can usually be managed within the project. However, they may rely on a

number of departments to support resolution of the risk and these dependencies need to be addressed in a collaborative way.

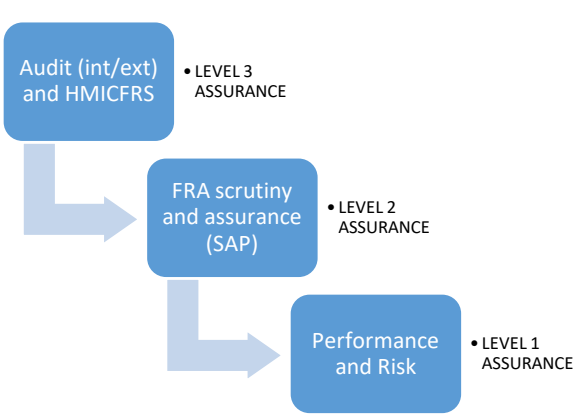
The sort of risks that could potentially impact in this way include:

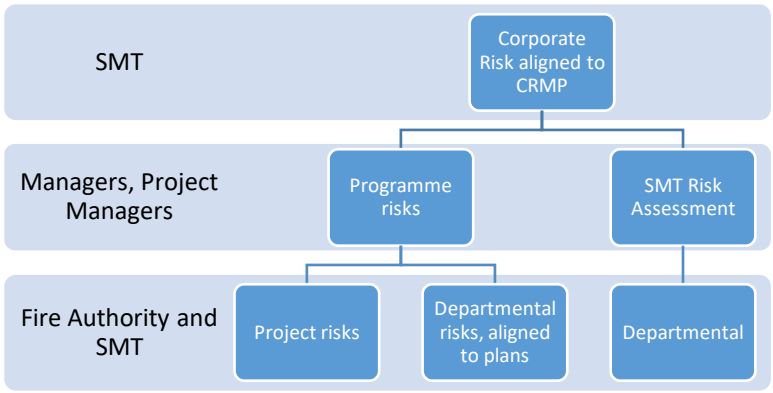
- **professional:** those associated with the particular nature of each profession (where the profession could be IT, administration, HR or operational etc.)
- **financial:** those associated with financial planning and control and the adequacy of insurance cover
- **legal:** those related to possible breaches of legislation or changes in regulations
- **physical:** those related to fire, security, accident prevention and health and safety (e.g., hazards/risks associated with buildings, vehicles, plant and equipment, etc.)
- **contractual:** those associated with the failure of contractors to deliver services or products to the agreed cost and specification
- **technological/information:** those relating to reliance on operational equipment (e.g., IS/IT systems or equipment and machinery)
- **environmental:** those relating to pollution, noise or energy efficiency of ongoing operations.
- **project:** those relating to missed milestones/deadlines, technical failures and budget increases.

Department, programme and project risks should be regularly managed and reviewed as part of the department's/project's/programme's ongoing performance/project management meetings. If not managed effectively, the escalation or accumulation of these risks may trigger a corporate risk as defined above. The broad escalation process is demonstrated in the diagram below.

The risk categories given above are neither prescriptive nor exhaustive. However, they do provide a framework for identifying and categorising the broad range of hazards and risks facing the Authority and its constituent departments.

Figure 2.





Allocating ownership

An essential requirement for the assessment of any risk is to have as much information and understanding about the risk as possible. To ensure this is the case, it is crucial that the right people are involved in the assessment process. With a clear description of the risk available and the roles and responsibilities defined earlier in the policy, it should be possible to identify potential Risk and Control Owners, who must be involved in the risk assessment process.

The **Risk Owner** is the person responsible for monitoring and reporting the progress being made towards the management of a particular risk. Each Corporate Risk will be owned by a member/s of the Service Management Team. Departmental and project risks may be owned by a Head of Service (SMT member), or a middle manager.

The risk owner is the person who has overall responsibility for the area of the Service most likely to be impacted by the risk. By definition, most corporate risks will have an impact across more than one department and therefore, the Risk Owner is likely to be an executive or senior level member of the Service.

Departmental/programme/project risks would only be expected to impact on that department/programme/project, or a section within the department and the Owner would therefore normally be the Department/Section Head/ programme or project manager.

The **Control Owner** is the person responsible for putting the agreed control measures in place and their operation. This person must have the authority over the people and resources involved in controlling / mitigating a particular risk.

With Corporate risks this is likely to be a Head of Service (SMT member), whereas with Departmental/programme/project risks it is likely to be a named member of that department/section charged with implementing the required control measures.

The initial selection of Risk and Control Owners may be subject to change depending upon the outcome from an initial risk assessment. Where this is the case, the new Risk

and/or Control Owners should be involved in the final, as well as all future, risk assessments.

Risk Management Process

The risk management process as outlined in figure 1 is set out in more detail below.

Risk Identification

Understanding the breadth of hazards facing the Service will help officers and members to effectively identify the potential risks associated with providing and delivering Services. Once a risk is identified and understood they can then be managed effectively by the controls that are put into place.

Risk assessment

Risk Assessment is defined by the ISO (International Organisation for Standards) Guide 73 as the overall process of risk analysis and risk evaluation.

The process used to analyse a risk can be sub-divided into four distinct elements:

- risk identification
- risk description
- allocating ownership, and
- risk estimation

The estimation of risk can be quantitative or qualitative and comprises the two elements of the likelihood of the risk occurring and the severity of the loss (or benefit) should it occur, commonly referred to as the 'impact'. Generally, the best people to undertake this assessment will be those that have a full understanding of the risk and its potential affects. This assessment will therefore normally be undertaken by the Risk Owner in collaboration with the Control Owner.

The impact likely to occur should a risk materialise is usually seen as being a negative event (i.e., is a threat), however, as part of the risk management process it is important that positive risks (opportunities) are also identified. Opportunities will also be subject to risk assessment. A significant difference in this assessment, however, is that the purpose of managing 'Opportunity Risks' is to encourage them to happen and to make sure that greatest benefit will be obtained.

Regardless of whether the risk is a 'threat' or an 'opportunity', the level of risk it poses is calculated by comparing their probable 'Likelihood' and 'Impact' against a set of standard measures. This results in a very high, high, medium, low or very low rating for both 'Likelihood' and 'Impact' which also provides scores against each element of between 1 and 5? (1 = very low, 2 = low, 3 = medium, 4 = high and 5 = very high). It is then simply a matter of multiplying the two scores together to get an overall Risk Score.

Likelihood x Impact = Risk

This results in Risk Scores ranging from 1(very low risk), through to 25 (very high risk).

Appendix A provides the standard measures to be used in the risk assessment process within Shropshire and Wrekin Fire Authority.

Risk evaluation

The Risk Evaluation process will be used to make informed decisions as to the significance of the risks to the Authority, whether they should be accepted or treated and what level of monitoring is required.

The purpose of risk management is not to eliminate all risk, but simply to reduce the risk to a level that the Authority is prepared to tolerate. This will vary depending on the Authority's current level of 'Risk Appetite' and is defined by the Authority setting its '**Risk Tolerance Level**'. This level essentially acts as a target, with any risks higher than this level attracting appropriate effort and resources in an effort to reduce it to below this level. This target therefore acts as a management indicator, with greater levels of monitoring being required for those risks above the level, than for those below it.

In addition to the upper level, it is also appropriate to set a lower-level target, called the '**Risk Acceptance Level**'. Any risks assessed as being lower than this level should attract minimal effort and resources. This helps to ensure that resources are not wasted trying to reduce risks unnecessarily.

The Authority will set and review the levels it wishes to use for its Corporate risks on a regular basis. SMT must then use these to ensure their day-to-day risk management activities are consistent with these strategic targets. The Authority's current risk Tolerance and Acceptance levels are shown in figure 3 below. Although the Authority specifically sets these levels only in relation to its Corporate risks, the levels depicted also form a sound base for the management of Departmental risks. All managers should therefore use the same levels to inform their evaluation of their own Departmental and programme/project risks.

Figure 3.

Risk Acceptance and Risk Tolerance Levels	Acceptance	Tolerance	Unacceptable

Impact						
	Very High	5	10	15	20	25
	High	4	8	12	16	20
	Medium	3	6	9	12	15
	Low	2	4	6	8	10
	Very Low	1	2	3	4	5
		Very Low	Low	Medium	High	Very High
		Likelihood				

Risk Treatment and Control

Having identified that a risk needs to be reduced, it is imperative that this is done. Risk treatment and control is the process of taking action to minimise the likelihood of the risk event occurring and/or reducing the severity of the consequences should it occur. This is achieved through the identification and implementation of control measures. This may be achieved through the identification and implementation of projects, new or revised policy and practice. Risk treatment and control generally involves implementing measures to control a risk before it occurs, or to mitigate the risk after it happens. This generic treatment can be further broken down into measures that will ensure the risk is terminated, treated, transferred, tolerated, or insured against.

The Service may seek to mitigate risks in the following ways:

1. **Terminate:** use an alternative approach that does not have the risk. This mode is not always an option. There are programmes that deliberately involve high risks in the expectation of high gains. However, this is the most effective risk management technique if it can be applied.

2. **Treat:** methods used to treat and control risks can be proactive (measures that try to contain the risk by reducing the likelihood of it occurring) or reactive (measures that lessen the impact when they do occur). The treatment chosen is likely to depend on the level and type of risk being considered and could be a combination of both treatment types. Risk treatment requires that a 'risk reduction plan' is developed and then monitored against. A very important aspect of this approach is that the planning is undertaken by people who have some experience in the particular area of risk being considered.

3. **Transfer:** an attempt to pass the risk to another element. Typically, used in the context of this Service by passing some or all of the risks to a contractor. This is a relatively effective method but will come at an additional cost. It is useful where the required expertise does not exist in the Service.

4. **Tolerate:** simply accepting the risk and proceeding. A word of caution: there appears to be a tendency within organisations to gradually let the assumption of this approach to take on the aura of a controlled risk.

5. **Insurance:** insurance policies are specifically designed to meet the financial consequences experienced by the organisation, should certain risks occur. Insurance is probably the most common of all tools used in Risk Management and is usually used in addition to the risk treatment methods described above. However, insurance cover does require careful monitoring and frequent review to ensure that the Service continues to receive value for money and the correct level of cover.

It is very common for more than one of these treatments to be used in order to ensure the risk is reduced to an acceptable level.

When considering corporate risks, these are complex risks which have a number of associated triggers and therefore control measures. In most cases it is likely that the Service would seek to 'treat' the risk through applying a variety of control measures.

Risk review, reporting and assurance

All risk Owners must be clear as to the cycle for risk reassessment in each service area. Risks identified as 'very high' and 'high' should be assessed on a regular basis. Medium or low risks will be reassessed less frequently. A regular reassessment of the entire Service should also be undertaken on an annual basis and will provide reports to SMT and Members.

All details about the risk under consideration will be captured in either the Authority's Corporate Risk Register), or each department's Departmental Risk Register (administered by the Head of each department or section). The level of detail required for corporate risks is much greater than for departmental risks, because of the increased potential impact on the Authority's aims and objectives.

The corporate risk review process should be undertaken on a regular basis via the risk owner and be recorded in real time to enable effective reporting.

Programme and project risks will be reviewed and reported through project and programme board meetings as appropriate.

Corporate Risks will be monitoring and reviewed through the following mechanisms:

- SMT review aligned to the Risk, Assumption, Issue, Dependency, Opportunity (RAIDO) process. This is a two-weekly review at a strategic level.

- Review and assurance through quarterly Performance and Risk group. This is an SMT assurance meeting which seeks to understand Service performance against Corporate Performance Indicators, Corporate Risk and HMICFRS Areas for Improvement.

- Standards Audit and Performance. This is an Authority committee with delegations to review and scrutinise corporate risk, providing assurance of the management of risk throughout the year. This is facilitated through quarterly progress reports and an annual summary report.

The minutes of Performance and Risk Group will be forwarded to SMT which will form part of the Service's overall Performance Management System and will also be used to inform the Annual Strategic Planning process.

Additional areas of risk management:

Working with key partners / stakeholders

Multi-agency approaches to risk management are also important. In some instances, joint operational risk assessments will help to ensure that an overarching risk perspective is taken (e.g. Joint use of premises). At the strategic level, it will be the responsibility of senior management to identify and liaise with key partners in managing strategic risk. Service managers will then work with these agencies as part of their operational duties.

Insurance

Clearly, placing some of the identified risks on cover with a reputable Insurance Company is a risk reduction measure that the Fire Authority would wish to explore.

The Head of HR and Administration, in consultation with the Treasurer and Head of Finance, will from time-to-time conduct reviews of the level of insurance cover in place, the level of self-insurance and alternative risk placement systems used by the Authority. This will be to ensure that best value, in terms of the cost of insurance premiums balanced against the level of risk exposure, is maintained and demonstrated at all times.

Business continuity and disaster recovery planning

It is far better for the Authority to prevent chaos during any crisis that may affect the organisation, rather than trying to recover from a disaster. Business Continuity Planning will help the Authority to avoid chaos by ensuring those involved in the process concentrate on the important issues, thereby helping to ensure that the key service delivery elements are addressed in priority order, regardless of what the catastrophe is.

Risk Assessment - IMPACT assessment ratings of risk if it does occur **Appendix A**

Impact	Score	Corporate threats/ opportunities
Very High	**5**	• Financial impact on the Authority likely to exceed £5M • Severe/catastrophic impact on the Authority's statutory duties and strategic objectives • Significant stakeholder concern
High	**4**	• Financial impact on the Authority likely to be between £1M and £5M. • Significant impact on the Authority's statutory duties and strategic objectives • High stakeholder concern
Medium	**3**	• Financial impact on the Authority likely to be between £250K and £1M • Moderate impact on the Authority's statutory duties and strategic objectives • Moderate stakeholder concern
Low	**2**	• Financial Impact on the Authority likely to be between £250K and £50K • Low impact on the on the Authority's statutory duties and strategic objectives • Low stakeholder concern
Very Low	**1**	• Financial Impact on the Authority likely to be less than £50K • Insignificant/negligible impact on the Authority's statutory duties and strategic objectives • Very low stakeholder concern.

Risk Assessment - LIKELIHOOD assessment ratings of risk if it does occur

Likelihood	Score	Definition
Very High	**5**	The risk has occurred and will continue to do so without further action being taken
High	**4**	The risk is likely to occur this year
Medium	**3**	The risk is likely to occur more than once in the next 5 years
Low	**2**	The risk may occur in the next 5 years
Very Low	**1**	The risk may occur in exceptional circumstances

Appendix B

Group/Individual roles and responsibilities as they relate to the Authority's Risk Management process

Risk Management Process	**Fire Authority Members**	**SMT**	**Performance and Risk Group**	**Heads of Service/Unit Heads**	**All staff and other Service Providers including Partners involved in service delivery or support**
Framework, Strategy and Process	Agreeing the framework, strategy and process determined by officers	Determining the framework, strategy and process	Providing advice and support to SMT and Elected Members		
Identifying Risk	Risk impact recognising wider political and social context.	Identifying strategic and cross-cutting risks	Providing advice and support	Identifying service risks	Maintaining awareness of risks and feeding these into the formal processes
Analysing Risk	Analysing risk Options appraised	Analysing strategic and cross-cutting risks	Providing advice and support	Analysing service risks	Maintaining awareness of the impact and cost of risks and feeding information and data into the formal processes
Profiling Risk	Profiling risk Approach determination	Profiling strategic and cross-cutting risks	Providing advice and support	Profiling service risks	
Prioritising Action based on the Risk Appetite	Determining the risk appetite and prioritising risk Agreeing the priorities determined by officers	Determining the risk appetite and prioritising strategic and cross-cutting risks	Providing advice and support	Prioritising action on service risks	