

Policy, Performance and Programmes

RISK MANAGEMENT POLICY

Document Management No.	
Author	██████████
Date of original issue	September 2007
Updated by ██████████	May 09
Revised by ██████████	October 2010
Due for review	October 2011
Version No.	03



South Yorkshire
Fire & Rescue
WORKING FOR A SAFER
SOUTH YORKSHIRE

RISK MANAGEMENT POLICY

Contents

POLICY STATEMENT	3
Statement of Intent	3
Objectives.....	3
Responsibilities.....	3
WHAT IS RISK?.....	4
Risk Definitions.....	4
RISK MANAGEMENT INTEGRATION.....	4
RISK MANAGEMENT PROCESS.....	8
Risk Identification	9
Types of Risk.....	9
Assessing the Level of Risk	10
Risk Matrix.....	11
Treatment of Risk	12
Risk Recording	13
Risk Monitoring and Review	14
Risk Audit	16
Fire Authority Governance.....	16
Help & Additional Support.....	16
APPENDIX 1A	18
SOUTH YORKSHIRE FIRE AND RESCUE.....	18
EXAMPLE – INITIAL RISK	18
APPENDIX 1B	19
EXAMPLE - RISK PROFILE AND PROGRESS.....	19
APPENDIX 2.....	20
ROLES AND RESPONSIBILITIES	20
APPENDIX 3.....	22
EXAMPLES OF CATEGORIES OF RISK.....	22

RISK MANAGEMENT POLICY

POLICY STATEMENT

Statement of Intent

South Yorkshire Fire and Rescue Authority is committed to protect the health, safety and welfare of its employees and the people it serves; to protect its property, assets and other resources, and to maintain its reputation and good standing in the wider community. This will be achieved by embedding at all levels within the authority the principles of risk management, thereby continually assessing and reducing the risks faced by the communities of South Yorkshire.

Risk Management is a central part of the Authority's strategic & operational management. It is the process whereby the risks to achievement of priorities, objectives and delivery of service are considered identified and managed, to minimize losses and maximize opportunity. It is designed to protect and enhance the delivery of corporate objectives.

Objectives

The objectives of the policy are to:

- Safeguard the employees, the public and others affected by the Authority's operations by preventing injury, damage and loss.
- Anticipate and respond to changing social, cultural, environmental and legislative requirements;
- Safeguard the resources of the Authority;
- Safeguard the reputation of the Authority;

These objectives will be achieved by:

- Raising awareness of, and integrating risk management into the culture and day to day management of the Authority;
- Managing risk in accordance with best practice by ensuring that, where ever practicable, risks are eliminated or reduced to an acceptable level;
- Establishing risk groups with clear roles and responsibilities and reporting lines within the Authority for risk management;
- Incorporating risk management into the decision making, business planning and performance management processes;
- Effective governance arrangements - monitoring risk management and internal control arrangements on a regular basis.

Responsibilities

It is the responsibility of members, managers and all other staff to actively engage in the risk management process. Key responsibilities in this respect are:

- **Members** – to champion risk management and actively engage in the risk management process, and challenge where appropriate.
- **Service Managers** – to actively engage in the risk management process and take a proactive stance in ensuring the participation of staff within their area of responsibility.
- **All other staff** – to actively engage in the risk management process, working with managers and colleagues to identify risks and take the required actions to reduce their likelihood and impact.

RISK MANAGEMENT POLICY

- **Policy Performance & Programmes Department** – to act as gatekeepers of the risk management methodology, facilitate the embedding of risk management throughout the service and ensure members, managers and all other staff adhere to the agreed policy and strategy.
- **Project Managers** – to undertake a risk assessment of their project(s) in accordance with the agreed project management methodology.

Appendix 2 provides a more detailed outline of the responsibilities of each of the above groups.

Risk Owners

Every risk must have an owner. The owner will take lead responsibility for ensuring the risk is managed effectively. The risk owner will also be the first point of contact for the risk manager when carrying out his/her monitoring duties.

Audit

Compliance with the CIPFA/SOLACE framework for the risk management elements of corporate governance will be carried out by Internal Audit as part of the audit of the Authority's governance arrangements.

Review

The strategy will be reviewed regularly and updated with any changes necessary to ensure that the Authority maintains best practice.

WHAT IS RISK?

Risk Definitions

Risk

Is the possibility of undesirable events occurring that might prevent or impact upon the achievement of business objectives? The impact can be a threat to the delivery of the objectives or a missed opportunity.

Strategic Risk

Any risk which has a direct impact on the achievement of the overall objectives of a Department/Service or which cuts across operational/divisional boundaries as opposed to risks that impact on any discrete part of the organisation.

Operational Risk

Any risk that impacts on the achievement of operational or departmental objectives and impacts on a discrete part of the organisation.

Risk is considered proportional to the expected threat / opportunity (impact) which can be caused by an event and to the probability (likelihood) of this event occurring. The greater the potential impact and the more likely the event, the greater the overall risk.

Risk = Impact of an event if it happens x likelihood of it happening

RISK MANAGEMENT INTEGRATION

Risk Management is an integral part of the organisation's management processes, such as service planning, business continuity, emergency planning and resilience, performance management, integrated risk management planning activities as well as day to day operational activities. Risk Management is not a stand-alone function.

RISK MANAGEMENT POLICY

Risk is something that everyone manages on a day to day basis, whether in the workplace or in the home, as we automatically process and evaluate threats in our environment and decide how we handle them.

Risk Management as a function is a way of formally capturing these processes. Operationally within SYFR Dynamic Risk Assessments (DRAs) are tools for personnel on the fire ground to quickly review and assess the hazards and threats of the incident and plan how to deal with them to achieve acceptable levels of safety. Corporate Risk Management is an extension of this process, which enables managers and staff to consider the threats and opportunities to the whole range of services we provide. As with DRAs it is a continual process which requires review monitoring and re-evaluation.

'Sphere of influence'

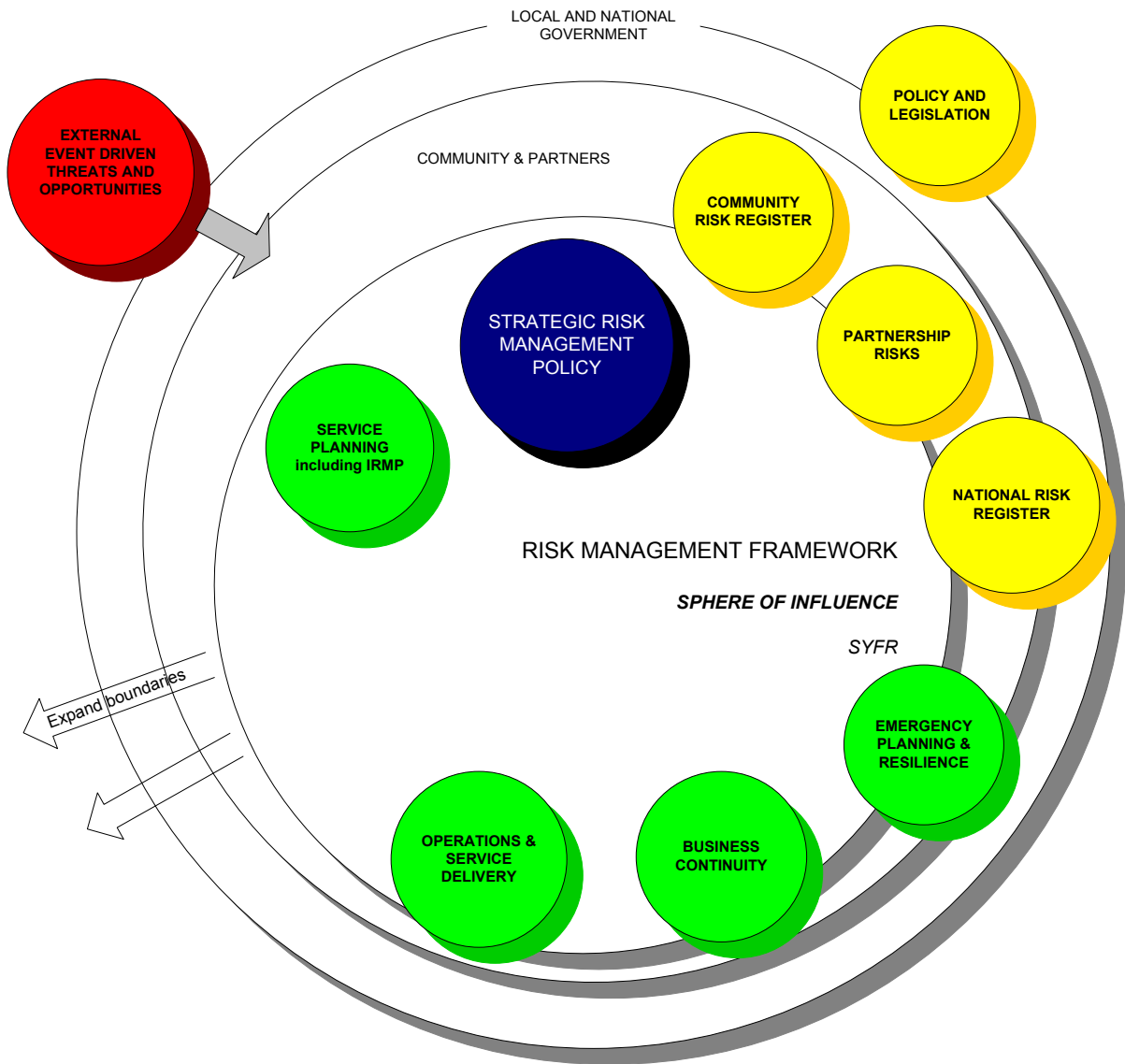
Through consideration of the environment we are working in, and the level of control and influence we have over the various levels of risks to our service provision, we can improve our chances of being able to take mitigating actions to achieve our objectives.

The level of control that can be achieved over a risk, or the boundaries of our influence over threats and opportunities in the environment we operate in, can be referred to as our 'sphere of influence'.

- Risks within our control – a risk that we can directly control or manage
- Risks within our sphere of influence – a risk which we can partly control/ manage or we can influence how it is controlled / managed
- Risk outside our sphere of influence – a risk over which we have no control or influence

There are different levels or layers that we have influence over within the environment we operate in, as we interact with others in delivering our services, as shown in the model below:-

RISK MANAGEMENT POLICY



1. Internal – Operational/ Workplace

Direct control over (working within government policy and laws)

- Service Delivery
- Resources
- Resilience
- Security
- Governance

2. External – partly within our control/ influence

• Community

Control and influence over the threats and opportunities that can arise from engagement with the community in the services we provide, i.e.: responding to incidents, consultation, recruitment, educating communities to enable them to reduce risk of fires in the home. We also have control and influence through statutory powers ie: legislative fire safety.

RISK MANAGEMENT POLICY

- **Partners**

Statutory responsibilities to work with partners in Crime and Disorder Reduction Partnerships, involvement in multi-agency planning for resilience, joint control over identification of risks and maintenance of community risk register

- **Political – Local and National Government policy**

Grants and funding pay, policy direction (national framework), regulation and audit. Changes in national policy can impact on the Services we provide and how we deliver them. We can influence via CFOA / consultation.

Council tax precept makes up part of our funding; councillors are SYFRA members who provide direction and scrutiny.

- **Environmental**

Our activities have an impact on the environment – use of water, power etc. Environmental events and changes can impact on our operations ie: flooding, as can changes in attitude to environmental issues by government, consumers etc

3. External – outside our sphere of influence

- **Economic** - global economic conditions may affect our services ie: our suppliers

- **Socio-cultural** - demographic changes within our communities that may impact on community needs for our services ie: aging population, changing migrant population.

The level of influence and control over events in each of these layers will vary depending on the type of event, threat or opportunity. Some of these we can predict, others we cannot, as risks are dynamic and emerging.

How to expand our sphere of influence

Effective risk management is about understanding our response to an event, how we can minimise the impact of threats or maximise opportunities through the action we take.

By considering the most appropriate response in advance we can plan for a given scenario and be better prepared if and when it happens. We can do this proactively by considering the types of risks we may be exposed to, for instance at a strategic level during the business planning process when we develop our priorities and corporate plan, at an operational level when we produce station plans or consider initiating new partnerships.

Through proactive identification and analysis of the risks within the environment we operate in, we can expand the influence we have over control measures to reduce the likelihood and impact these may have. By focusing on those areas within our sphere of influence will enable us to consider how we can expand it in the future.

RISK MANAGEMENT POLICY

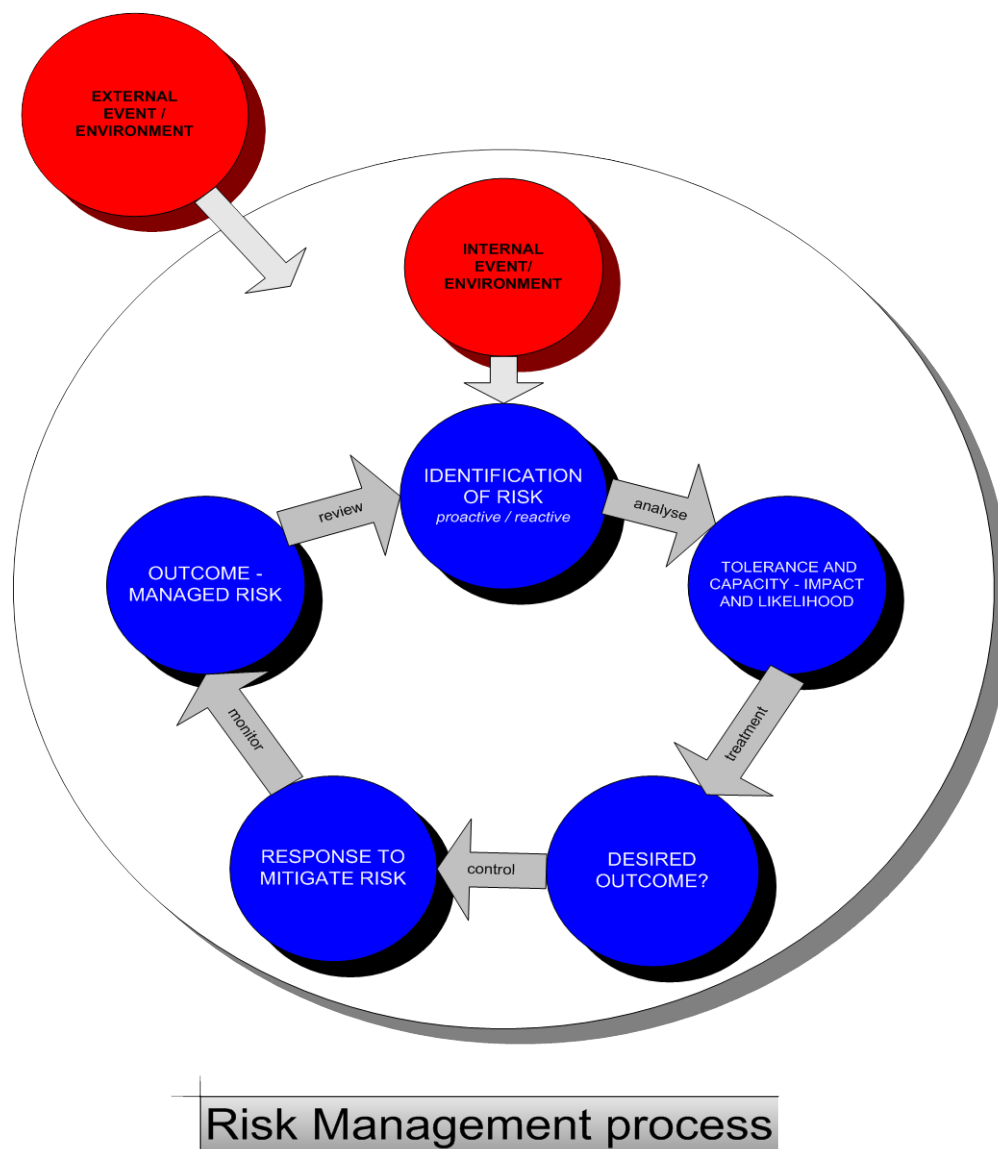
In considering and identifying potential risks to our operations, and delivery of our priorities and objectives, we can plan to mitigate the risk by planning our response, and considering the desired outcome we want to achieve. What is our tolerance to the threat, what are we willing to accept as an end result?

The weight of response should be proportionate to the threat, the probability of an event occurring considered against its impact.

Effective risk management should also enable staff to take risks, so that it drives rather than prohibits the organisation's ability to innovate and strive for achieving excellence.

RISK MANAGEMENT PROCESS

The diagram below shows the phases of managing risks in response to both external and internal events that may pose a threat or opportunity.



There is a continuous cycle to the risk management process. Through this cycle a programme of continual improvement is carried out and reviewed.

RISK MANAGEMENT POLICY

Risk Identification

Risks are dynamic therefore their potential impact on the Authority & Service will change from time to time. Risks are inherent at all levels therefore involvement of staff at all levels is essential. The process covered in this strategy will enable staff at all levels to identify risks within their area.

It is important that the Service takes every opportunity to consider whether there are any new or emerging risks. There are a number of methods that can be used to help identify risks – these are listed below:

- **Proactive consideration of risks** – when undertaking planning activities, developing business plans, new partnerships or projects, consider what threats and opportunities there may be to success.
- **Reactive identification by staff and members** – on a day to day basis new risks may present themselves as part of daily business as a result of events that occur. It is important to bring these risks to the attention of the appropriate manager to ensure they are properly assessed.
- **Previous experience & comparison with other organisations** – it is important that lessons are learnt and acted upon. One way of achieving this is to benchmark and monitor issues affecting other organisations (i.e. through forums such as the ALARM Fire Group).
- **Discussions at meetings** – it is considered good practice to include risk management as a standard agenda item on all regular meetings - emphasis should be put on the identification of new risks.
- **Checklists** – creating a standard checklist of things to look out for can help stimulate thought processes when considering risks.

The role of the Risk Team in risk identification

The Risk Team will take a proactive role in the identification of new risks at a strategic level. It is important however that the Service has a mechanism in place for identifying and capturing risks at all levels.

Through regular meetings with Directors, Functional Heads, District Managers, Station Managers and Section Managers, the Policy, Performance and Programmes Department will support the organisation in managing risks facing the Service. They will actively encourage managers to employ the above range of risk identification techniques to ensure such activities become a regular part of the day job. This will include risk management training for those responsible for risk register maintenance.

Types of Risk

Risk identification is concerned with the effect of risk on service objectives. In the context of the recent developments in corporate governance, consideration should be given to all categories of risk.

If a full risk assessment is to be undertaken, managers and supervisors must consider risks associated with each appropriate category and their inter-relationships. The simplified list below will cover most categories.

- **Strategic risks** – Risks that relate to doing the wrong thing for the organisation. eg. Failure to maintain staffing levels at optimum level.

RISK MANAGEMENT POLICY

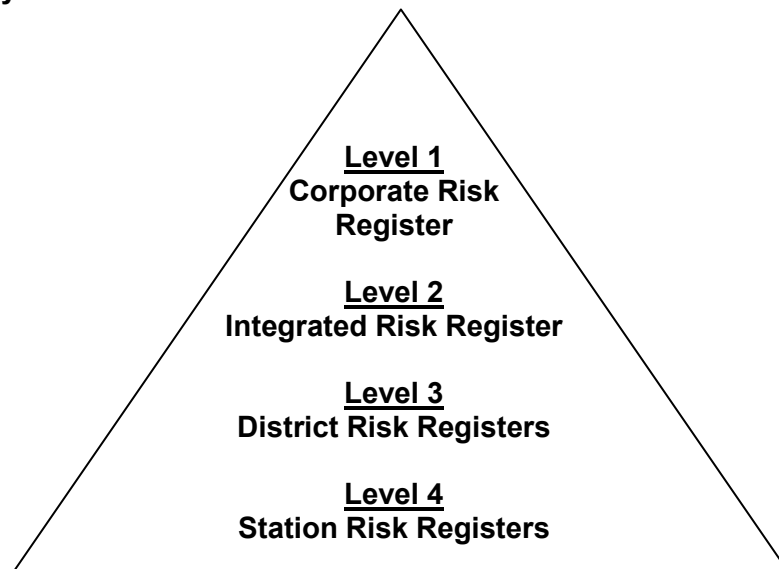
- **Operational risks** – Risks that relate to doing the right things but doing them in the wrong way, e.g. delay in delivering a key project by the required timescale
- **Information risks** – Risks that relate to loss or inaccuracy of data, systems or reported information, e.g. Management Information System crash resulting in the loss of incident data.
- **Reputation risks** – Risks that relate to the organisation's brand or image, e.g. negative reports in the local media due to a failure to effectively manage press and publicity.
- **Financial risks** – Risks that relate to losing monetary resources or incurring unacceptable liabilities, e.g. failure to anticipate the increased revenue costs of implementing a new piece of legislation
- **People risks** – Risks associated with employees and management, e.g. industrial action caused as a result of the mismanagement of a change in staff terms and conditions
- **Regulatory risks** – Risks related to the regulatory environment, e.g. failure to introduce a new piece of legislation by the required deadline.

Further examples can be found at appendix 3

- NB - Operational risk assessment for health and safety purposes, is an integral part of front line and support activities, and will continue to be an important tool for prevention of accidents and other unplanned losses.
- Information Risk is a key area within the Protective Security Strategy, and as such requires special management arrangements to ensure that information risk is handled according to the mandatory requirements of the HMG Security Policy Framework, Security Policy No 4. Information Security and Assurance. Refer to the Information Risk Policy for further information.

Assessing the Level of Risk

The Risk Pyramid



Risks can be escalated, or downgraded through the levels as deemed necessary at each appropriate level. All staff should be kept aware of the importance of Risk, via induction and ongoing training sessions.

RISK MANAGEMENT POLICY

Corporate Risk Register (Level 1)

The Corporate Risk Register is a controlled register that can only be updated by the Risk Team after authorisation from the Corporate Management Board or Executive Team. Directors will keep a copy to hand and only destroy them when in receipt of a revision – hence a more robust version control. The dynamic process of risk means that the register may change on a regular basis.

Executive team members are responsible for notifying the Risk Team of any changes i.e. new risks as well as any changes to existing risks. The Risk Team will amend as necessary and distribute the revised risk register. New Risks may have been previously registered on the Departmental Risk Registers by Heads of Function, although the risk ratings may vary between levels.

Integrated Risk Register (Level 2)

This register should reflect the risks to the Directorates in not achieving their objectives, IRMP and Programme Risks. New Risks will usually be logged on this Register prior to escalation, if necessary, to Corporate level 1 via CMB.

Function / District Risk Register (Level 3)

At a lower level there is a requirement to cover the day to day risks that are an inherent part of business activity. This needs to be controlled by the Functional Head as ultimately these risks could have an impact upon key business objectives.

Station/Section Risk Register (Level 4)

Each Station will have a Risk Register which will be the responsibility of the Station. Sections may decide to maintain a Risk Register below that of the Functional Register.

Risk Matrix

A 4 x 4 risk matrix covering impact and likelihood is used in assessing the level of risk. This analysis should be undertaken by managers and supervisors with experience in the area affected. It should be noted that the best assessment is found from a group judgement and not a single person.

Role of the Policy Performance & Programmes Department – the department will facilitate the implementation of the risk management processes and will play a key role in ensuring the risk matrix is regularly applied to all areas of the Service. (see earlier comments)

A risk rating is obtained by considering the likelihood of the event occurring and the impact (severity) of such an event. This is obtained from a risk matrix and by following the guidance for assessing likelihood and impact. The scores from each table are **multiplied** together to produce a score for the risk. This can be used to position the risk on a risk profile enabling high risks to be quickly identified and acted upon e.g. a red risk will usually be escalated to the next level. Green risks may be downgraded, or closed.

Risk ratings are normally calculated for pre and post control measures. The post control risk rating (residual risk) assumes the controls are in place and are working effectively.

RISK MANAGEMENT POLICY

Treatment of Risk

The aim at all times will be to reduce the negative risks “As Low As Reasonably Practicable” (ALARP). The options available for controlling risks can be summarised as follows:

- Tolerate (retain) a risk;
- Terminate (avoid) a risk;
- Transfer a risk;
- Treat a risk;
- Take the Opportunity

Tolerate a risk

Risks can be tolerated at their existing levels where no effective controls can be put in place i.e. the level of risk is within the ‘risk appetite’ of the Service.

Terminate a risk

This can be achieved by not performing the activity, considering other courses of action, or deferring a decision until more information is obtained.

Transfer a risk

This is normally achieved by insuring against any adverse outcome, or contracting out the activity e.g. workshop maintenance carried out by a third party. It must be remembered however that in the case of insurance there are a number of residual risks that cannot be insured e.g. reputational issues arising from an incident, indirect litigation costs resulting from a failure in our duty of care to both employees and non employees.

Treat a risk

Treatment involves the application of suitable control measures that will reduce the likelihood of occurrence of a risk, e.g. eliminating the cause of risk, minimising the probability of something going wrong by preventative measures, or reduce the consequences of impact of a risk, e.g. ensuring effective monitoring and taking necessary steps to prevent, minimise or contain adverse impacts. Very often these reductions incur a cost, and a decision has to be made as to the practicability of the cost in relation to the benefits achieved.

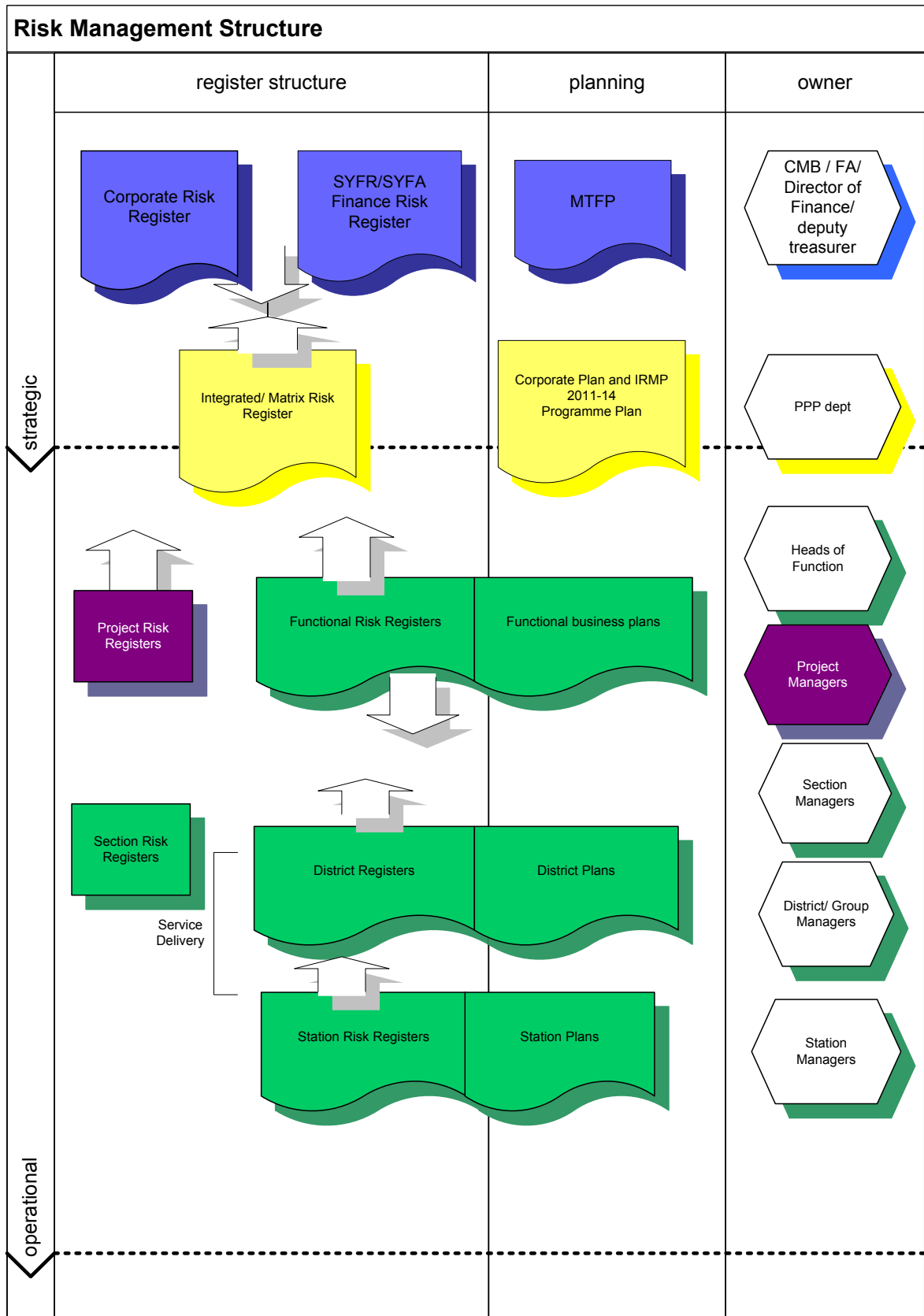
Take the Opportunity

There are various aspects to this, e.g. whether or not at the same time as mitigating threats, an opportunity arises to exploit positive impact. Do circumstances exist which, whilst not generating threats, offer positive opportunity?

Role of the Policy, Performance & Programmes Department – as the Service experts in the application of the risk management methodology, they can assist managers in risk identification and the most effective way of treating a risk.

RISK MANAGEMENT POLICY

Risk Recording



The diagram above shows the proposed new risk register structure and ownership.

RISK MANAGEMENT POLICY

The format to be used for recording the basic risk rating, for all levels of risk, is shown in Appendix 1A. This format shows the risk rating both before and after treatment of the risk using control measures.

The Corporate Risk Profile and Progress (1B) will show the movement in each risk since it was first identified, and uses the traffic light system to highlight risks requiring immediate action (red); risks being adequately managed (amber) and those risks where no further controls are required (green). In addition it will provide a commentary on the current status of all risks with reference to any movement since the last report, or actions to reduce the level of risk further. This full profile, after CMB approval, is presented to the Fire Authority Audit Committee, to review the high impact & likelihood **red risks**.

The risk assessment process is dynamic and therefore the status of the risk is at the point the assessment was made, and therefore the Profile should be used to show the most recent level of risk, rather than the assessment as shown on the Initial Risk page.

Risk Monitoring and Review

Risks are dynamic and therefore it is important they are reviewed regularly to decide whether:

- the risk is still relevant
- anything has occurred which would change the impact / likelihood
- the controls are still effective
- the Service is prepared to tolerate the risk
- the service provided has changed significantly – if so have any new risks emerged
- there any new Strategic, Operational, Information, Reputation, Financial, People or Regulatory risks

Escalation & Downgrading of Risks

Within the risk monitoring process there will be risks that have increased to 'red' and conversely risks that have decreased to 'amber' or 'green'.

Escalating 'red' risks – Any Integrated Risk Register level risk that is escalated to 'red' status should be discussed at Executive Meetings, to consider adding it to the Corporate Risk Register – it should also remain on the Integrated Risk Register as this is where the majority of remedial action will be undertaken.

In some cases the Executive Team may decide to retain lower graded risks on the Corporate Risk Register due to their high profile and potential impact.

Downgrading a 'red' risk - Where risks are controlled and re-evaluated to 'amber' or less, they may drop from the Corporate Risk Register to the appropriate lower level Risk Register, and ultimately may be closed altogether.

Programme & Project Risk

All projects within the Service Development Programme will have a risk register which will be reviewed regularly by their respective Project Manager. If / when it is deemed necessary risks may be escalated to the Integrated Risk Register. Where the risk cannot be dealt with by the Programme Manager it will be escalated. The usual route would be potentially to the Corporate Risk Register. Suitable remedial action will then be considered in accordance with the process for monitoring and managing Corporate Risk.

RISK MANAGEMENT POLICY

IRMP Risk

IRMP risks will be reviewed at the Operational Improvement Board and where it is deemed necessary will be escalated to the Integrated Risk Register.

Partnership Risk

All Partnerships will have a risk assessment, which assesses risk to the Partnership, the Authority and the risk of not engaging in the Partnership. This assessment is regularly reviewed and shared within the Partnership as appropriate.

The Role of Corporate Management Board (CMB) and Directorate Meetings in monitoring risk

Corporate Management Board – Audit reports

The reports necessary for the Audit committee will be an agenda item at the CMB. The reports will be approved for release, or final amendment instructions given. This will be included in the monthly meeting nearest to, and prior to, the Audit Committee meeting.

CMB Meetings – Level 1 Risks

On a monthly basis a standing agenda item will be included in CMB meetings to review the Corporate Risk Register.

The Head of Policy, Performance and Programmes, or the Corporate Performance and Governance Manager will attend and undertake the following duties:-

- ensure that the latest version of the Corporate Risk Register is available to officers
- facilitate a review of the corporate risk register highlighting any key issues and receiving any progress updates
- capture any new and emerging risks
- update officers of any changes to the grading of risks since the previous meeting, authorised by the Executive Team, noting any that need to be downgraded to Directorate level or require closure.
- respond to any requests for further risk assessments to be undertaken as and where directed

Directorate Meetings - Level 2 Risks

On a monthly basis each Directorate should take time to review their risk registers – risk management should therefore be included as a standard agenda item at all Directorate Meetings.

- Review the risk registers highlighting any key issues and receiving any progress updates
- ensure any Directorate/Functional level risks included on the Corporate Risk Register are up to date, and accurately reported
- Capture any new and emerging risks
- Consider the grading of risks noting any that need to be escalated or downgraded

RISK MANAGEMENT POLICY

The Risk Team can assist managers in this task by:-

- providing any advice, guidance and training
- responding to any requests for further risk assessments to undertaken with in the directorate

Risk Audit

Risk Registers are a key requirement within the Accounts and Audit Regulations. Internal Audit will, as part of the audit process, carry out a regular review of risk management arrangements. This will provide independent assurance as to the effectiveness of our risk management procedures. In particular this audit will:

- Verify the existence of risk registers and risk management action plans
- check whether risk management is being actively undertaken throughout the Service
- Provide advice and guidance on how to further improve risk management processes and procedures

Additionally the Authority will allow for peer review and benchmarking of risks where appropriate.

Fire Authority Governance

Members have a responsibility to understand the strategic risks that the Authority faces and to support and monitor the risk management process. In order that members are kept informed of the risks, regular reports are required, detailing the current risk status of the Service.

The Risk Register and its supporting reports are a means of summarising the risks to the Service and the Authority within the various functions. The following reports will be submitted to members:-

- A quarterly report will be made to the Audit Committee on the progress made in reducing the "red" Corporate Risks to the Authority. This report will include a profile listing of all open risks on the Corporate Risk Register
- An annual report will be made to the full Fire Authority detailing progress made in addressing all Corporate Risks for the past year
- All reports to the Fire Authority include Risk Management implications.

Any new Corporate Risks of high severity that are raised between quarterly meetings will be communicated to members via the Chairs Group.

Help & Additional Support

The Performance & Governance Manager has primary responsibility for the risk management process and ensuring that systems and processes remain in place for the effective management of risk.

RISK MANAGEMENT POLICY

For help and guidance in all aspects of risk management, please contact Policy, Programmes and Performance. Contact details can be found below:

Risk Inbox – risk@syfire.gov.uk

Performance & Governance Manager – 0114 2532282

The following publications have been taken into account in the compilation of this policy:

- The ALARM National Performance Model for Risk Management in the Public Services (www.alarm-uk.org)
- Managing Risks with delivery Partners (HM Treasury, www.ogc.gov.uk)
- Governance of Risk: Improving Strategic Risk Management Arrangements in Local Public Bodies and Partnerships – Audit Commission (www.audit-commission.gov.uk)
- Risk Management Assessment Framework (www.info4local.gov.uk)

RISK MANAGEMENT POLICY

APPENDIX 1A

SOUTH YORKSHIRE FIRE AND RESCUE

EXAMPLE – INITIAL RISK

No.	Date Raised	Risk (Threat to achievement of the business objective)	Current Risk Owner	Original Risk [No controls in place]			Risk Control Measures	Residual Risk [Control measures implemented]			Business Objective Reference
				I (1 - 4)	L (1 - 4)	Risk Rating		I (1 - 4)	L (1 - 4)	Risk Rating	
FR18	Jul-08	Intranet & Internet Service intranet and internet do not meet user requirements	Head of Corp. Comms & Admin. S Chu	3	3	9	Secure funding for wholesale redevelopment of the intranet and internet	2	2	4	
FR31	Nov-08	Sponsorship policy Lack of a sponsorship policy could result in missed opportunities for additional funding and/or a reputational risk due to obtaining funds from inappropriate sponsors	Head of Corp. Comms & Admin. S Chu	3	2	6	Adopt a sponsorship policy	2	1	2	
PS5	Dec-08	Effective Health & Safety (H & S) systems If H & S systems are not aligned to Health & Safety Executive (HSE) guidance, and are not effective and timely, SYFR and SYFRA are exposed to legal and financial reputational damage.	Head of OpS&S R Chandler	4	3	12	Audit of H & S team functions Ineffective systems identified New systems installed	3	2	6	

RISK MANAGEMENT POLICY

APPENDIX 1B

SOUTH YORKSHIRE FIRE AND RESCUE

EXAMPLE - RISK PROFILE AND PROGRESS

Risk Ref	Risk Description	Current Risk	Progress ↓	Risk – Impact x Likelihood									
				Apr-10	May-10	Jun-10	Jul-10	Aug-10	Sep-10	Oct-10	Nov-10	Dec-10	
FR18	Intranet & Internet Service intranet and internet do not meet user requirements	Head of Corp. Comms & Admin. S Chu	20/7/10 - S Chu intranet refresh still scheduled for 2010/11	2x2 Risk Level 4	2x2 Risk Level 4	2x2 Risk Level 4	2x2 Risk Level 4	2x2 Risk Level 4	2x2 Risk Level 4				
FR31	Sponsorship policy Lack of a sponsorship policy could result in missed opportunities for additional funding and/or a reputational risk due to obtaining funds from inappropriate sponsors	Head of Corp. Comms & Admin. S Chu	20/7/10 - S Chu Policy has been drafted and circulated for consultation. It will go to the September FRA meeting	3x2 Risk Level 6	3x2 Risk Level 6	3x2 Risk Level 6	3x2 Risk Level 6	3x2 Risk Level 6					
PS5	Effective Health & Safety (H & S) systems If H & S systems are not aligned to Health & Safety Executive (HSE) guidance, and are not effective and timely, SYFR and SYFRA are exposed to legal and financial reputational damage.	Head of OpS&S R Chandler	16/08/10 Update provided by Lee Patterson (LP) Work is on-going - Accident Reporting Investigation Procedures in place; LP is working on the Health & Safety Policy; Risk Control Systems Reviews ongoing in line with the Health & Safety Plan. Ratings reduced to 3 x 2 = 6	4x2 Risk Level 8	4x2 Risk Level 8	4x3 Risk Level 12	4x3 Risk Level 12	3 x 2 6					

APPENDIX 2

ROLES AND RESPONSIBILITIES

South Yorkshire Fire and Rescue Authority

Elected members are responsible for governing the delivery of services to the local community. Members have a responsibility to understand the strategic risks that their Service faces, and to decide how these risks should be managed. They should not seek to avoid or delegate this overall responsibility as it is key to their stewardship responsibilities. Members should:

- correctly position risk management as a strategic and operational tool that can help officers and members to meet the new and existing challenges and demands facing them, rather than as a mere compliance exercise;
- view the process as a significant long term exercise: there is no 'quick-fix' solution and the right level of resources will need to be committed to implementation and training over the medium term;
- take a top-down approach by managing and monitoring risks, focusing on issues of corporate significance rather than a 'bottom-up' exercise which would be too large for members themselves to manage;
- aim for continual improvement on a longer-term basis supplemented by increasing their knowledge through regular training;
- appoint a member champion who will communicate the risk management process to others.

Members of the Corporate Management Board

The Corporate Management Board will be responsible for identification; evaluation and action planning to mitigate the effect of risks on the successful achievement of the Fire Authority's objectives. This will involve:

- implementing the risk management policy,
- own and take responsibility for specific risks
- reviewing and managing risk controls,
- being a risk management champion,
- being responsible for resolving their own risks,
- regularly reviewing the Corporate Risk Register
- encourage staff within their area of responsibility to actively support the risk management process
- identify individuals within their functional areas to take ownership of maintaining and updating risk registers
- providing full support to the Risk Team in execution of their duties.

Risk Team

The Risk Team is responsible for developing specific programmes and procedures to establish and maintain risk management activities.

The main duties can be summarised as follows:

- advising managers, supervisors and staff on the risk management process to ensure adoption of consistent methodologies across the Service;
- supporting managers to undertake risk analysis;

RISK MANAGEMENT POLICY

- updating the Corporate risk register, and monitoring all other SYFR Risk Registers based on information supplied from owning managers;
- developing and promulgating risk management policy and processes;
- preparing strategic risk management action plans that include education, awareness, training & cultural embedding;
- preparing strategic risk management reports.

Managers

All other Managers will:

- maintain an awareness of risk management, and its importance to the effective operation of the Service.
- own and take responsibility for specific risks and risk registers
- use all appropriate forums to regularly review risks and identify new risks as appropriate.
- communicate the importance of risk identification and management of risk to staff.
- Maintain a robust and fully up to date register of risks for their functional area.

Project Managers

For all projects they are responsible for, project managers will:-

- conduct an initial risk assessment of the project in accordance with the project management methodology developed by the Programme Office
- maintain a risk register for the project
- own and take responsibility for specific risks
- regularly review and update project risks
- escalate any appropriate 'red' risks to the Programme Manager for possible inclusion on the Integrated Risk Register

Programme Office Manager

Will:-

- work with Project Managers to ensure that risks are appropriately identified, captured and managed, with support from the Risk Team
- Review project risks and ensure they are regularly reviewed at Programme Board meetings
- Escalate project risks to the Integrated Risk Register as appropriate

APPENDIX 3

EXAMPLES OF CATEGORIES OF RISK

The risk categories given below are examples and provide a framework for identifying and categorising a broad range of risks. The categories/examples may overlap and cannot be considered in isolation.

<p>STRATEGIC RISKS</p> <p>Doing the wrong things e.g.</p> <ul style="list-style-type: none"> • Failure to meet the Government agenda, • Mismanagement resulting in corporate objectives not being achieved. • Failure to manage corporate risk.
<p>OPERATIONAL RISKS</p> <p>Doing the right things in the wrong way e.g.</p> <ul style="list-style-type: none"> • Failure to communicate effectively with employees, • Serious injury from our activities to an employee or third party. • Overly bureaucratic processes resulting in poor quality service delivery
<p>INFORMATION RISKS</p> <p>Loss or inaccuracy of data, systems or reported information e.g.</p> <ul style="list-style-type: none"> • Data loss caused by a failure to back up key information, • Inaccurate data presented to third parties. • Leaking of confidential and personal data
<p>REPUTATION RISKS</p> <p>Service brand or image e.g.</p> <ul style="list-style-type: none"> • Adverse media coverage resulting from a failure to manage an incident effectively, • Serious incident caused by a failure to adhere to policies & procedures. • Poor CPA rating publicised in the national press
<p>FINANCIAL RISKS</p> <p>Losing monetary resources or incurring unacceptable liabilities e.g.</p> <ul style="list-style-type: none"> • Missed funding opportunities, • Failure to adequately manage budgets. • Failure to insure against loss or damage
<p>PEOPLE RISKS</p> <p>Employees and management e.g.</p> <ul style="list-style-type: none"> • Failure to recruit or retain qualified staff, • Inadequate training for the requirements of the post. • Industrial tribunal caused by mismanagement
<p>REGULATORY RISKS</p> <p>Regulatory environment e.g.</p> <ul style="list-style-type: none"> • Inadequate response to the introduction of new legislation or guidance, • Misinterpretation of legislation/regulations resulting in a serious breach. • Deliberate breaking of the law