# RISK MANAGEMENT PROCEDURE

SHQ - Alicehajic, Esma

LANCASHIRE FIRE AND RESCUE SERVICE

# Table of Contents

## Purpose

The purpose of this Risk Management Procedure is to establish a framework that ensures effective and consistent risk management practices throughout Lancashire Fire and Rescue Service. This procedure should be well-communicated to all personnel and should be read alongside the Risk Management Policy specific to Lancashire Fire and Rescue Service.

## Benefits of Effective Risk Management

Effective risk management provides the following benefits:

- A robust and systematic process to identify, assess, treat, report, and review risks, leading to proactive risk mitigation.
- A clear audit trail of all key risks facing the organisation and the necessary actions in place to mitigate them, ensuring accountability and transparency.
- Improved decision-making based on risk assessments and analysis, enhancing the organisation's ability to achieve its objectives.
- Clear ownership of risks across the organisation, promoting a proactive risk management culture.
- Identification and appropriate ownership of cross-cutting risks, facilitating a coordinated and integrated approach to risk management.
- Enhanced corporate governance, fostering confidence and trust among stakeholders.
- Decline in the number of interruptions to service delivery (minimal service disruption and a positive external image as a result).
- Reduction in managerial time devoted to managing the results of a risk event having taken place.
- A more systematic method to addressing legislative, regulatory or competitive demands.
- Improved financial control as a result of risk identification, analysis, treatment, and monitoring.
- Improved health and safety and the superior condition of property and equipment.

## Aims and Objectives

The primary aim of this procedure is to outline the practical methods for implementing the Lancashire Fire and Rescue Service Risk Management Policy.

The objectives of the Risk Management procedure are as follows:

- Establish a standardised set of risk management tools applicable to all areas of the organisation to manage risks.
- Adopt consistent definitions and risk ratings to ensure the identification, assessment, treatment, reporting, and review of all significant risks within the defined risk appetite.
- Integrate risk management into all planning processes, projects, activities, and day-to-day operations.
- Ensure that managers are aware of their responsibilities in managing risks associated with their respective service areas.
- Communicate risk management information transparently and accessibly.

For definitions of risk management terms, please refer to Appendix A.

## Responsibilities

Accountability for this risk management procedure lies with the Combined Fire Authority and the Chief Fire Officer. The Director or Corporate Services is responsible for the oversight of the associated Risk Management policy, while the Service Improvement Department, through the oversight of the Deputy Chief Fire Officer, holds responsibility for the development, review, and monitoring of compliance with this procedure and its associated policy.

All employees are responsible for identifying, reporting, and managing existing risks, as well as potential risks not previously recognised and recorded, as part of their daily duties.

Further responsibilities are detailed in Appendix B.

## What Is Risk Management

Risk management is the systematic and cyclical process of identifying, assessing, evaluating, treating, and monitoring risks to achieve organisational objectives. It involves the continuous cycle of identifying potential events or situations that could have adverse effects on achieving objectives and taking proactive measures to manage or mitigate those risks. Risk management is integrated into all aspects of

Lancashire Fire and Rescue's operations to enable informed decision-making, prioritise resource allocation, and enhance overall resilience.

In lieu of an effective Risk Management process, risks can threaten the assets of an organisation or the ability to provide a service. Therefore, Risk Management should not be seen as a "bolt on"; it should be integral to planning and operational management within the organisation.

Applying the risk management cycle will help the CFA and management make informed decisions. The risk management cycle will generate information that will help ensure that risks can be avoided or minimised in the future. It will also inform judgements on the type and degree of insurance cover and the balance to be reached between self-insurance and external protection.

## Risk Management Process

The risk management process at Lancashire Fire and Rescue Service covers corporate, department, programme, and project risks.

- **Corporate risks:** These risks have a significant impact on the organisation's medium and long-term goals. They are managed by the Service Management Team (SMT) and discussed as a standing agenda item at quarterly Corporate Programme Board (CPB) meetings.
- **Department risks:** These risks are encountered in the daily corporate and/or operational environment. Department Heads and their staff manage these risks.
- **Programme risks:** These are risks which are common to a particular project programme and are discussed as a standing item in the programme board quarterly meetings.
- **Project risks:** These are uncertain events that may or may not occur during a project. The appropriate project manager manages these risks.

LFRS follow a structured approach to risk management and assurance which involves five processes, as seen below, ahead of being captured within a risk register. Each stage of the process should be recorded on the relevant risk register, according to the categories outlined above, which for Corporate and Department risk is held within the designated Risk Register Microsoft Teams Channel, in the CPB Team. Programme and Project risk information is contained within the respective programme and project files.

Details of the risk, triggers, consequences, current controls/mitigations, and outstanding exposures are recorded in the relevant risk registers. The inherent risk scoring is conducted based on the risk with the current controls/mitigations considered. Any risk treatment is recorded under actions and the residual risk

scoring is conducted based on the predicted effect of the risk treatment on the likelihood and impact. The risk manager is recorded under the by whom section. The date for action implementation, risk owner and Directorate are also recorded for each risk.

The risk management process involves the following five stages:


### Identify the risk:

Risks can be identified proactively during planning activities, development of department plans, and new projects. They can also emerge during day-to-day activities or as a result of assurance activities. Historic review and group discussions are also useful methods for risk identification.

It is important that we take every opportunity to consider whether there are any new or emerging risks. Risks are dynamic and therefore potential impacts will change over time. There are a number of methods that can support risk identification:

- Proactive – when undertaking planning activities, developing department plans and new projects, consider what threats and opportunities are associated with the risk.
- Reactive – new risks may present themselves during day-to-day activities or as a result of events during Performance and Review (P&R), Business Interruption Reporting (BIR) or other assurance activities.
- Historic review – risks that have been logged as a result of previous events can be considered again for similar planning activities or projects.

- Group discussion – it is good practice to include risk management as a standard agenda item on all regular meetings, in particular the Corporate Programme Board (CPB) meetings, with the potential escalation of departmental risks being discussed within this forum and reported to the SMT appropriately. In addition to this the identification of emerging risks should also form part of the discussion and escalation process.

Identified risks must be described in a way that they can be understood by all. The accepted method is to create a description that separates the cause, triggers (uncertainty) and effect (impacts) as outlined below:

Risk Cause: Describes the source of the risk, i.e. the event or situation that gives rise to the risk. They are the potential trigger points for risk but are not risks in themselves; they may be either internal or external to LFRS.

Risk Event: Describes the area of uncertainty in terms of threat or opportunity (using 'may' or 'might' in this part of the description is helpful).

Risk Impacts: Describes the consequence that the risk would have on LFRS activities should the risk materialise.

Examples of relevant, but not exhaustive, risk categories are included in Appendix C.

### Assess the risk:

Before treating risks, they need to be assessed to prioritise them. This is done by measuring the likelihood of the event occurring and the impact/severity if the event occurs. Lancashire Fire and Rescue Service uses the Risk Criteria and Risk Matrix provided in Appendix D for risk assessment.

Bespoke risk assessments are used for various functional activities including Health & Safety as part of their ISO accreditation.

It is important to define the Risk Appetite for LFRS. For all Corporate, Department, Programme and Project risks the risk appetite is set at "Tolerable". Any risk calculated from 1 to 4 for the inherent risk score is determined to be within the risk appetite of LFRS so will be monitored but not treated as a priority. Any risk above this threshold (i.e. scoring above 4 for the inherent risk score) would need further consideration and a decision taken as to how the risk should be treated. Any risk scoring 15 or above should be considered as an intolerable risk for which reduction activities should be prioritised.

There are some instances, however i.e. Operational Assurance, Health and Safety, Business Assurance, where all risks are treated and action plans are developed to support the Service's assurance processes. Risks identified at operational incidents

should be escalated via the operational debrief processes and active incident monitoring.

Risk ratings are calculated at 3 key stages, which are:

- **Initial Inherent Risk Rating** – this should be carried out by the individual/team as soon as the risk is identified, can be informal.
- **Inherent Risk Rating** – to avoid subjectivity the initial risk rating should be discussed, and a rating 'agreed' with the relevant department head or group i.e. SMT.
- **Residual Risk Rating** – Once risk controls have been implemented it is necessary to review the risk rating to identify if the risk has been sufficiently reduced so that it falls within LFRS' risk appetite.

Any risk rating that exceeds the defined appetite, as described above, prompts an action plan to allocate necessary control measures to reduce the likelihood or impact until the risk is tolerable.

### Treat the risk:

Risks are treated appropriately:

- **Avoid** the risk by removing the cause of a threat. This may be adopted at no cost by changing work practices, however any costs incurred as a result of the actions should be justified.
- **Reduce** the risk by taking actions that mitigate or reduce the likelihood/impact.
- **Transfer** the risk by passing part of it to a third party i.e. insurance or share amongst multiple parties.
- **Accept** that the risk will occur and accepting the impact if it does. This action is not appropriate if the risk exposure exceeds the risk appetite (Moderate/Substantial/Intolerable).

### Report the risk:

Risk must be reported at the appropriate level.

The Corporate Risk Register (CRR) provides an overview of all identified corporate live risks. The Director or Corporate Services has oversight of the Risk Management framework and maintains the CRR. The CRR is developed, with the coordination of the Senior Business Continuity and Emergency Planning Officer and agreed upon by the SMT on a quarterly basis through the CPB meetings. The Director of Corporate Services is responsible for reporting on the CRR to the CFA through the Audit Committee at least annually.

Department Risk Registers provide an overview of all identified departmental risks. The respective Department Heads, with the support from the Senior Business Continuity and Emergency Planning Officer, are responsible for reporting their risks through the department risk registers. Should a Department Head consider a risk on their register requires escalating to the CRR, the respective Department Head can raise the specific risk during the quarterly CPB meetings, where a consensus can be drawn by the SMT.

project and risk registers are held for each programme board. Any new risks reported to a Programme Board should be assessed to consider whether it needs consideration by the SMT for escalation to the CRR and minuted as an action to raise with the Senior Business Continuity and Emergency Planning Officer.

### Review the risk:

Regular reviews are conducted to assess the effectiveness of risk control measures and to monitor changes in risks over time.

Risks that appear in the CRR (Corporate Risks) are reviewed by the Senior Business Continuity and Emergency Planning Officer and risk managers, subsequently with risk owners on a quarterly basis, on behalf of the Director of Corporate Services, making any required changes ahead of being reported to the SMT during the CPB meeting. The SMT proactively monitor progress in the intervening period. This allows the opportunity to archive or de-escalate risks between the CRR and departmental risk registers, in addition to horizon scanning to identify any emerging risks.

Department risks are also reviewed quarterly by the Senior Business Continuity and Emergency Planning Officer and relevant Department Head during individual meetings. The onus for continuous monitoring of these risks lays with the relevant Department Head, who can present the risks at the quarterly CPB meeting for SMT consideration and decision of whether the risk requires escalation onto the CRR during the quarterly CPB Risk Management standing agenda item. The Senior Business Continuity and Emergency Planning Officer will conduct analysis on all of the departmental risk registers in aim of identifying any common themes that can also be brought to the CPB and discussed for broader treatment, if required.

Project risks are reviewed in conjunction with the project requirements at project meetings (frequency depends on the project but usually monthly).

## Monitoring And Review

This Risk Management Procedure shall be reviewed annually and updated as required by the Service Improvement department.

Next Review Date: August 2024

# Document Control

**Amendment History**

| Version | Date | Reasons for Change | Amended by |
|---|---|---|---|
| 0.1 | August 2023 | First draft | Esma Alicehajic |
| 0.2 | March 2024 | Elaboration of the risk scoring criteria | Esma Alicehajic |
| | | | |
| | | | |

Related Documents (If applicable)

| Document Type | Reference Number | Title | Document location | Date Reviewed |
|---|---|---|---|---|
| Policy Document | | Risk Management Policy | LFRS Risk Management Policy draft v0.1.docx | August 2023 |
| | | | | |

## Appendix A – Glossary of terms

**Risk** - an uncertain event(s) that, should it occur, will have an effect on the achievement of objectives. A risk is then measured by a combination of the likelihood of a perceived threat or opportunity occurring and the magnitude of its impact on objectives.

**Threat** - an uncertain event that could have a negative impact on objectives or benefits.

**Opportunity** - an uncertain event that would have a favourable impact on objectives or benefits if it occurred.

**Issue** - an event that has happened was not planned and requires management action. It could be a problem, benefit, query, concern, or the result of an assurance activity.

**Risk Management** - the process directed towards the effective management of threats and opportunities to the organisation achieving its objectives.

**Risk Appetite** - the amount and type of risk that an organisation is willing to accept.

**Risk Tolerance** - the threshold level of risk exposure which when exceeded triggers some form of response (e.g., escalation or action)

**Control measure** - a structure, system, process, procedure, policy, or any other action designed to modify/mitigate the risk i.e., reduce the likelihood and/or impact of a risk.

**Risk Owner** – a person delegated/ assigned with the authority and accountability to manage a risk.

**Risk Manager** – a person responsible for implementing risk management processes within a department.

**Risk Actionee** – a nominated individual responsible for undertaking activities associated with a risk.

**Stakeholder** – a person or organisation that can affect, be affected by, or perceive themselves to be affected by decisions or activities relating to the risk.

**Risk Register** – a record of information detailing type and exposure of risks across the Service.

# Appendix B – Responsibilities for Risk Management

## Corporate Risk Management

### Combined Fire Authority (CFA) Members (Audit Committee)

Combined Fire Authority Members will:

- Be aware of the risk management implications of decisions.
- Receive annual reports on Corporate Risk Management activities.
- Ensure that there is an effective strategy to manage risks throughout the Authority.

### Service Management Team (SMT)

The specific role of the SMT in respect of Corporate Risk Management will be to:

- Ensure that there is an effective framework for the management of all risks throughout the organisation.
- Advise the CFA of the risk management implications of key proposals.
- Ensure appropriate management of corporate risks that could significantly affect the medium and long-term goals of the organisation providing corporate oversight of these activities as part of the group's quarterly standing agenda item.
- Review the CRR on a quarterly basis and record mitigation appropriately, assessing risks and agreeing a strategy to manage those risks raised within the CRR.
- Develop, implement, and monitor action plans to minimise risks identified in the CRR.
- Review and moderate risk management action plans for relevance, consistency, and appropriate risk control measures.

## Department Risk Management

It is imperative that all Heads of Department ensure that they continually manage those department risks that are encountered on a daily basis.

All employees must have an awareness of risk management and an understanding of their role in the risk management process with regard to identifying risks and reporting them to their line manager.

Department Heads have responsibility to:

- Ensure that department risks are aligned with department plans and any associated Key Performance Indicators
- Monitor the progress of planned actions to ensure that risk is minimised.
- Report the progress of risk management action plans on a quarterly basis.
- Ensure that, where appropriate, action plans are produced, and risk control measures are introduced.

## Responsibilities In Risk Management

The following roles associated with risk management are defined as:

**Risk Owner** – A member of SMT who has overall accountability for the management of an identified risk. The risk owner is responsible for:

- approving changes to the risk's profile and action plan.
- ensuring that appropriate resources and importance are allocated.
- confirming the existence and effectiveness of the mitigating actions and ensuring that any proposed mitigating actions are implemented.
- providing assurance that the risks for which they are Risk Owner are being effectively managed.

**Risk Manager** – A senior manager (Dept. Head/Senior Manager) who has been delegated the responsibility for managing an identified risk including the implementation of mitigating actions. Responsibility to delegate to suitable team member for actions.

# Appendix C – Risk Categories

**Categories of Risk**

Risks can be strategic or operational.

- **Strategic/Corporate** – risks that need to be taken into account in judgements about the medium to long-term goals and objectives of the authority.
- **Political** – Those connected with the failure to deliver either local or central government policy.
- **Economic** – Those affecting the authority's ability to meet its financial commitments. These include internal budgetary pressures, the failure to purchase sufficient insurance cover or the effects of proposed investment decisions.
- **Social** – Those relating to the consequences of changes in demographic, residential or socio-economic trends on the authority's' ability to meet its objectives.
- **Technological** – Those associated with the authority's' ability to cope with the scale and pace of technological change, and its ability to use technology to meet changing demands.
- **Legislative** – Those associated with present or future national and European law.
- **Environmental** – Those relating to the environmental consequences of progressing the authority's' strategic objectives (e.g., in terms of pollution and energy efficiency).
- **Customer/Citizen** – Those connected with the failure to meet the present and shifting needs and expectations of the customers and citizens.
- **Operational** – risks encountered in the everyday work of managers and staff.
- **Professional** – Those involved with the specific nature of each profession.
- **Financial** – Those linked to financial planning and control and sufficiency of insurance cover.
- **Legal** – Those connected to possible violations of legislation.
- **Physical** – Those associated with fire, accident prevention and health and safety.
- **Contractual** – those related to the failure of contractors to deliver services or products to the agreed cost or specification.
- **Technological** – Those linked with the reliance on operational equipment.
- **Environmental** – Those relating to pollution and energy efficiency of ongoing service operations

# Appendix D – Risk Criteria

## Introduction

Once a risk is identified is it important to prioritise it. This will ensure appropriate resources are allocated to those risks that require them. To prioritise risks, we assess the likelihood of occurrence, and the impact should it occur. It is important that the risk description is carefully constructed so that we can fully understand and assess the risk, this is particularly important when assessing the impact.

## Likelihood

Likelihood looks at when the risk is probably going to take effect. To improve consistency when measuring likelihood guidance on the scoring criteria is provided below.

## Impact

The impact examines what effect the risk's occurrence will have upon us. When assessing the impact, a number of factors are considered including delivery of objectives, service delivery, finance, and reputation.

## Risk Matrices

Using a 5x5 scoring matrix we prioritise the risks by multiplying impact and likelihood scores together. The higher the score, the higher the risk rating is.

### Impact

The impact of risks should be scored using the below criteria. If a single risk impacts multiple categories in different severity, than the average impact score should be used in the inherent and residual risk score. For example, the risk of loss of SHQ due to fire scores a 5 in the financial category, but a 1 in Government relations, then the score of 3 should be used for the purposes of the risk register.

| **Score** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|
| | **Minor** | **Noticeable** | **Significant** | **Critical** | **Catastrophic** |
| Financial | £0k - £100k | £100k - £250K | £250k - £1m | £1m - £2m | £2m+ |
| Service Provision | No impact | No impact | Services reduced but still able to meet statutory duties | Services suspended and unable to meet statutory duties for a short period | Services suspended and unable to meet statutory duties for a long period |

| | | | | | |
|---|---|---|---|---|---|
| Health & Safety | Cuts & bruises | Broken bones/illness | Loss of life/ major illness | Significant loss of life/ major illness | Major loss of life/ large scale major illness |
| Objectives | No impact on objectives | Several departmental objectives not met | One corporate objective not met | Two corporate objectives not met | Several corporate objectives not met |
| KPIs | No impact on corporate Key Performance Indicators | Several corporate Key Performance Indicators not met by less than 10% | Several Key Performance Indicator not met by between 10% & 20% | Several corporate Key Performance Indicators not met by between 20% and 50% | Several corporate Key Performance Indicators not met by more than 50% |
| Reputation | - | - | Adverse local publicity | Adverse national publicity | Adverse national publicity for an extended period |
| Government Relations | - | - | Poor assessments | Service taken over temporarily | Service taken over permanently |

## Likelihood

Likelihood of risk can be determined using quantitative and/or qualitative data, historical data, expert judgment, and any other available evidence.

| Score | | Probability |
|---|---|---|
| 5 | Certain/ Almost certain | Greater than 90% |
| 4 | Very likely | 65% to 90% |
| 3 | Likely | 35% to 65% |
| 2 | Unlikely | 5% to 35% |
| 1 | Rare/Very Unlikely | Less than 5% |

## Scoring Matrix

The Impact and the Likelihood scores of risks are multiplied and the score is referenced using the below risk matrix to determine the priority of the risk mitigations.

| Likelihood | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 5 | Certain Almost certain | 5 | 10 | 15 | 20 | 25 |
| | 4 | Very likely | 4 | 8 | 12 | 16 | 20 |
| | 3 | Likely | 3 | 6 | 9 | 12 | 15 |
| | 2 | Unlikely | 2 | 4 | 6 | 8 | 10 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | Rare/Very Unlikely | 1 | 2 | 3 | 4 | 5 |
| | | | Minor | Noticeable | Significant | Critical | Catastrophic |
| | | | 1 | 2 | 3 | 4 | 5 |
| | | | Impact | | | | |

Generally, any red risks are viewed as unacceptable and must be treated as a matter of priority. It may be necessary to carry out a cost benefit analysis to ensure that the cost of introducing further mitigating action(s) does not outweigh the cost of tolerating the risk.

Amber risks are acceptable; however, the risk should be reduced as low as is reasonably practicable and contingency plans must be developed.

Green risks are broadly acceptable, but close monitoring must be maintained.

The acceptance of a risk represents an informed decision to accept the impact and likelihood of that risk and therefore falls within the organisation's risk appetite.

A risk owner must be allocated to each identified risk. This ensures the 'ownership' of the risk is identified and that the appropriate resources are allocated.