



Staffordshire
Fire and Rescue Service
preventing • protecting • responding



Equality, Diversity
and Inclusion



Leadership



Dignity and Respect



Integrity



Putting our
Communities first

RISK MANAGEMENT FRAMEWORK

2025-2028

Contents

	<u>Policy Statement</u>	2
1.	<u>Introduction</u>	4
2.	<u>Our Approach to Risk Management</u>	4
3.	<u>Governance and Leadership</u>	5
4.	<u>Risk Culture</u>	6
5.	<u>Risk Appetite and Risk Tolerance</u>	7
6.	<u>Roles and Responsibilities</u>	8
7.	<u>Embedding Risk Management</u>	11
8.	<u>Recording and Reporting Risks</u>	11
9.	<u>Issues</u>	12
10.	<u>Project Risk Registers</u>	12
11.	<u>Information and Collaboration</u>	12
12.	<u>Review and Continuous Improvement</u>	13
13.	<u>Risk Management Process</u>	13
14.	<u>Opportunity Risk</u>	14
15.	<u>Insurance</u>	15
16.	<u>Risk Management Guide</u>	16
	Appendix 1 - <u>Risk Appetite and Tolerance Statement</u>	29

Policy Statement

Staffordshire Fire and Rescue Service recognises that in order to continue to improve and enhance our service to the community, we must take some organisation risks. In order to do this, we must ensure that our risk management is effective by making informed decisions based on sound data and measured against our risk appetite.

It is our policy to ensure that we take all reasonable and cost-effective steps in the identification, analysis and economic control of the risks that could threaten the achievement of strategic aims and objectives and which have the potential to result in loss or harm to our assets and or damage to the Service's reputation. We aim to manage threats whilst maximising opportunities.

Good risk management must be embedded into everything we do including our activities and our partnerships, in order to achieve our goals and objectives which are set out in our Safety Plan.

Everyone has a responsibility to manage risk. We are all accountable for the decisions we make. Part of the decision-making process should involve the consideration of threats, their likely impact, and identification of any opportunities.

Our Risk Management Objectives

Objective 1

We will promote awareness of risk amongst staff and embed the approach to its management throughout Staffordshire Fire and Rescue Service.

Objective 2

We will use the risk management to identify, assess and act on risks.
We will monitor this action and report to the appropriate Manager or Board.

Objective 3

We will approach the management of risk as something that provides Staffordshire Fire and Rescue with an opportunity to improve our service delivery as well as something that has negative consequences

Objective 4

We will continue to learn, develop and improve our risk management practices

By adopting effective risk management practices across the organisation, we will demonstrate our ability to: -

- Protect our assets against loss, damage or disruption
- Protect our reputation
- Enhance Stakeholder confidence in the organisation

- Comply with Corporate Governance
- Enable effective and sound decision making by having quality information and data about current or potential risks which we may encounter
- Protect our insurance profile.

The Senior Leadership Team fully support and endorse the Risk Management Framework and expect all staff to comply with the policy and procedure contained within it.

Equality, Diversity and Inclusion in Risk Management

The Service will consider Equality, Diversity and Inclusion in risk management decisions by ensuring that it invites scrutiny and evaluation from across the business.

By adopting a risk aware culture, it will enable us to make risk-based decisions whilst supporting our long-term service goal and objectives.



Rob Barber

Chief Fire Officer Rob Barber KFSM MBA

Date: 18/02/2025

Signed on behalf of Staffordshire Fire and Rescue Service

1. Introduction

In successful organisations, risk management enhances strategic planning and prioritisation, assists in achieving objectives and strengthens the ability to be agile to respond to the challenges faced. (The Orange Book).

Risk is inherent in everything we do. In order to be successful, the Service cannot be risk adverse, providing that every risk assessment has been evaluated and assessed against our risk appetite, risk owners will be supported in their decisions. We should at risk as an opportunity. Risk can be a source of opportunity as well as a source of loss. Risk management is as much about maximising opportunities as it is about minimising negative consequences.

Risk Management should be integral part of all decision-making activity and should be applied through policy from project inception to everyday management of our Service. Our approach to Risk Management is aligned to ISO 3100, Institute of Risk Management and The Orange Book. As a Service, we have continued to enhance our risk management process by investing in our systems and providing training.

The effectiveness of our risk management processes are built on those managing risks and the governance in place. Accountability, transparency and clarity encourage organisation risk awareness. By having access to succinct, comprehensive information facilitates good decision making and the ability to effectively anticipate and manage risks. Our risk culture must encourage constructive challenge and promote collaboration.

2. Our Approach to Risk Management

The aim of this risk management framework is to enable the identification, evaluation and control of residual risks to an acceptable level.

In order for our risk management framework to be effective we aim to adhere to the following principles.

- Risk management shall be an essential part of **governance and leadership** and fundamental to how the organisation is directed, managed and controlled at all levels
- Risk management shall be an **embedded** part of all organisational activities to support decision-making in achieving objectives
- Risk management shall be **collaborative and informed** by the best available information and expertise
- Risk management processes shall be structured to include:
 - Risk identification and assessment to determine and prioritise how the risks should be managed.

- The selection, design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level; the design and operation of integrated, insightful and informative risk monitoring; and
 - Timely, accurate and useful risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.
 - Risk management will be used to identify opportunities.
- Risk management shall be continually improved through learning and experience.

3. Governance and Leadership

Effective governance and leadership are critical components of a robust risk management framework. They ensure that risk management practices are integrated into the organisation's strategic objectives and daily operations.

Governance

Governance begins with the development of a comprehensive risk management policy that outlines the approach to identifying, assessing, and mitigating risks. Our policy is aligned with our Community Risk Safety Plan (CRMP) and the Staffordshire Commissioner's Fire Plan.

Clear roles and responsibilities are established for all stakeholders involved in risk management.

Governance structures should promote accountability and transparency in risk management activities. Regular reporting and communication channels have been established to keep all stakeholders informed about risk exposures and mitigation efforts. This will be done through various directorate boards. This helps in building trust and ensuring that risk management practices are consistently applied across the Service.

Governance frameworks must ensure that the Service complies with relevant laws, regulations, and ethical standards. This includes adhering to industry best practices and maintaining high standards of integrity in all risk management activities.

Leadership

Leadership plays a crucial role in fostering a risk-aware culture within the Service. Senior leaders must demonstrate a commitment to risk management by setting the tone at the top. This involves actively participating in risk management activities, promoting a culture of open communication, and encouraging employees to report potential risks without fear of retribution.

Leaders must integrate risk management into strategic decision-making processes. This means considering potential risks and their impacts when making key business decisions. By doing so, leaders can ensure that the organisation is better prepared to handle uncertainties and recognise opportunities.

Effective leadership involves allocating sufficient resources, which includes time, to risk management activities. Investing in risk management tools, training programs and personnel ensures that adequate resources are available to effectively identify, assess, and mitigate risks.

Leaders should promote a culture of continuous improvement in risk management practices. This involves regularly reviewing and updating risk management policies, procedures and frameworks to ensure they remain effective and relevant in a changing environment.

By establishing strong governance and leadership, it creates a resilient risk management framework that not only protects against potential threats but also enhances overall Service performance.

4. Risk Culture

Our Risk Culture

Figure 1 – IRM Risk Culture Framework



Risk culture is a term describing the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose. This applies to all organisations - including private companies, public bodies, governments and not-for-profits. (IRM).

An effective risk culture is one that supports individuals taking organisational risks in the right manner. For this to be achieved the Senior Leadership Team will ensure that the expected values and behaviours are embedded throughout the organisation.

Integrating Equality, Diversity, and Inclusion (EDI) into this culture ensures that diverse perspectives are considered in risk assessments and decision-making processes. This inclusivity helps identify a broader range of risks and develop more effective mitigation strategies. By valuing EDI, this promotes transparency, accountability and fairness, reducing the likelihood of biases and discrimination. Ultimately, a risk culture that embraces EDI principles strengthens our ability to navigate complex risks and maintain a positive reputation.

5. Risk Appetite and Risk Tolerance

Risk appetite is defined as the level of risk the Service is prepared to accept to fulfil its mission and achieve its objectives. Risk appetite helps organisations establish a threshold of impacts they are willing and able to absorb in pursuit of objectives, which may include but is not limited to financial loss. Risk appetite provides a framework which enables an organisation to make informed decisions. Our Risk Management Appetite Statement can be found in [appendix 1](#). Levels of reward and costs of managing risks will determine the Service's Risk Appetite. Risks outside the Service's Risk Appetite will not be tolerated and must be managed (reduced, transferred, mitigated etc.)

Risk tolerance refers to the level of risk and Service is willing to accept in pursuit of its objectives. It is a critical component of risk management, as it helps define the boundaries within which we operate. Risk tolerance varies depending on factors such as the strategic goals, financial stability, regulatory environment, and stakeholder expectations. By clearly articulating its risk tolerance, we can make informed decisions that balance potential rewards with acceptable levels of risk. This ensures that the Service remains resilient and capable of achieving its long-term objectives while effectively managing uncertainties.

Figure 2 – Risk Appetite and Risk Tolerance



6. Roles and Responsibilities

Everyone in an organisation has some responsibility for risk management. The “three lines of defence” model provides a simple and effective way to help delegate and coordinate risk management roles and responsibilities.

Figure 3 – Three Lines of Defence Model



- **First Line of Defence** - management have responsibility and accountability for identifying, assessing and managing risks. The first line ‘own’ the risks and are responsible for execution of the Services response to those risks through executing internal controls on a day-to-day basis and for implementing corrective actions to address deficiencies.
- **Second line of Defence** - consists of functions and activities that monitor and facilitate the implementation of effective risk management practices. They also facilitate the reporting of adequate risk related information up and down the organisation. The second line supports management by bringing expertise and monitoring alongside the first line to help ensure that risk is effectively managed.
- **Third Line of Defence** - the internal audit function will, through a risk-based approach to its work, provide an objective evaluation of how effectively the organisation assesses and manages its risks, including the design and operation of the “first and second lines of defence”.

- **External Assurance** - sitting outside of the Service's own risk management framework and the three lines of defence, are a range of other sources of assurance that support an organisation's understanding and assessment of its management of risks and its operation of controls such as external audit, HMICFRS and other regulatory bodies.

To support effective governance and decision-making at each level, the roles and responsibilities for risk management are clarified and defined below:

Role	Responsibilities
Service Delivery Board (SDB)	<ul style="list-style-type: none"> • Understand the Services strategy, operating environment and the associated risks. • Understand the role and activities of the Senior Leadership Team in relation to managing risk. • Discuss with the Senior Leadership Team their attitude to and appetite for risk to ensure these are appropriately defined and communicated so that management understands these parameters and expectations. • Understand the risk management framework and the assignment of responsibilities. • Review the risk management framework to evaluate how well the arrangements are actively working in the organisation; and • Consider the adequacy and effectiveness of control processes in responding to risks within the organisation's governance, operations, compliance and information systems.
Senior Leadership Team	<ul style="list-style-type: none"> • Lead the assessment and management of risk and take a strategic view of the risks identified by the Service • Ensure that there are clear accountabilities for managing risks and that managers are equipped with the relevant skills and guidance to perform their assigned roles effectively and efficiently. • Ensure that roles and responsibilities for risk management are clear to support effective governance and decision-making at each level with appropriate escalation, aggregation and delegation. • Determine and continuously assess the nature and extent of the strategic risks that the Service is willing to take to achieve its objectives - its "risk appetite" - and ensure that planning and decision-making appropriately reflect this assessment. • Agree the frequency and scope of its discussions on risk to review how management is responding to risks and how this is integrated with other matters including business planning and performance management processes. • Specify the nature, source, format and frequency of the information that it requires. • Ensure that there are clear processes for bringing significant issues to its attention more rapidly when required, with agreed triggers for doing so. • Use horizon scanning to identify emerging sources of uncertainty, threats and trends. • Assure itself of the effectiveness of the organisation's risk management framework. • Designate an individual to be responsible for leading the organisation's overall approach to risk management, who should be of sufficient seniority and should report to a level within the organisation that allows them to influence effective decision-making. • Ensure the allocation of appropriate resources for risk management, which can include, but is not limited to people, skills, experience and competence. • Chair Directorate Risk Management Group meetings, or nominate a suitable chair. • Incorporate risk management into Directorate Management Team agendas.

Strategic Risk Manager	<ul style="list-style-type: none"> Periodically assess the robustness of the Service's Risk Management Framework and culture. Ensure that expected values and behaviours are communicated and embedded at all levels to support the appropriate risk culture. Establish the organisation's overall approach to risk management. Establish risk management activities that cover all types of risk and processes that are applied at different organisational levels. Ensure the design and systematic implementation of policies, procedures and practices for risk identification, assessment, treatment, monitoring and reporting. Consider the organisation's overall risk profile, including risk management within shared services. Monitor the quality of the information received and ensure that it is of a sufficient quality to allow effective decision-making. Schedule, Chair and arrange minutes for a Directorate Risk Management Group at least twice a year. Ensure appropriate representation (and a nominated deputy is identified) from all service areas at the Directorate Risk Management Group. Promote risk management best practice. Represent the department at Corporate Risk Management Group, acting as a link between the directorate and the corporate group. Champion, monitor and report on the implementation of risk registers and business continuity plans.
Heads of Directorates	<ul style="list-style-type: none"> Maintain risk registers for their Directorate, ensure reviews are undertaken every quarter and ensure that all risks are aligned to corporate objectives. Ensure that mitigating actions are carried out and controls are in place to reduce risks, whilst identifying and enabling cost-effective strategies to be put in place to minimise the incidence of these. Encourage and develop positive risk taking in relation to service development and modernisation within a controlled and monitored process. Feedback on the effectiveness of the risk management process. Ensure that all partnerships entered into have appropriate risk management arrangements, including a risk register and regular reporting to the governing board. Promote effective risk management in service areas. Ensure all significant projects entered into follow an appropriate project management methodology and project risks are identified and managed.
Heads of Department	<ul style="list-style-type: none"> Contribute to the maintenance of a risk register for their department/service area. Share relevant information with colleagues. Feedback on effectiveness of the risk management process to their Directorate Heads. Encourage and develop positive risk taking in relation to modernisation and business change within a controlled and assessed process. Utilise risk management data to minimise unwanted incidents and outcomes at operational level.
Employees	<ul style="list-style-type: none"> Liaise with their line manager to assess areas of risk and opportunity in their job. Identify new or changing risks in their job and feed this back to their line manager. Highlight any risk management issues or inadequacies with their job or department. Be aware of their accountability for ensuring that risks are adequately managed. Understand how they can make a positive contribution to the improvement of risk management practices.

7. Embedding Risk Management

The assessment and management of opportunity and risk should be an embedded part of, and not separate from:

- Setting strategy and plans
- Evaluating options and delivering programmes, projects or policy initiatives
- Prioritising resources
- Supporting efficient and effective operations
- Managing performance
- Managing tangible and intangible assets and
- Delivering improved outcomes.

The Senior Leadership Team, supported by the Strategic Risk Manager, will ensure that risks are transparent and considered as an integral part of appraising options, evaluating alternatives and making informed decisions. Effective appraisal supports the assessment of the costs, benefits and risks of alternative ways to meet objectives.

When conducting an appraisal, consideration will be given to the identification and analysis of risks in the design and implementation of options. This analysis and evaluation will provide the foundation to understand the risks arising through chosen options and how these will be managed, including how these will be subject to effective and on-going monitoring. Delivery confidence will be supported through the transparent identification of the risks faced and how those risks will be managed within business and financial plans.

8. Recording and Reporting Risks

A Risk Register is used for recording risk information. Our policy will be that.

- The Service has a Strategic Risk Register that contains our “top” risks that face us on an organisational level
- Each Directorate has a Risk Register which feeds into the Strategic Risk Register
- Each Service Delivery Group must have a Risk Register that feeds into the Directorate risk register
- Key Departments must have a Risk Register.

Key Departments are those considered critical to service delivery.

Recording and Reporting aims to:

- Transparently communicate risk management activities and outcomes across the organisation
- Provide information for decision-making
- Improve risk management activities and

- Assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

9. Issues

Issues are current problems or challenges that are already being experienced. They are known and present obstacles that need to be addressed and resolved. Issues can arise from various sources, such as operational inefficiencies, compliance failures, or resource shortages. They require immediate attention and action to prevent further negative impact on the Service.

Risks, on the other hand, are potential future events or conditions that may occur and have an impact on the Service. Risks are uncertain and can have both positive and negative outcomes.

An issue log is, at its most basic, a list where issues are collected as either ongoing or closed. This way you can track the issue from the time it's identified until you have resolved it. Each Department and Directorate should keep an active issues log.

10. Project Risk Registers

A project risk register is a crucial tool in project management that helps identify, assess and manage risks throughout the lifecycle of a project. It serves as a centralised repository where all potential risks are documented, along with their descriptions, likelihood, impact, and mitigation strategies. By maintaining a risk register, project managers can systematically track and prioritise risks, ensuring that appropriate actions are taken to minimise their impact on project objectives.

The risk register also facilitates communication among stakeholders, providing a clear and transparent view of the project's risk landscape. Regularly updating the risk register helps in adapting to new risks and changing circumstances, contributing to the successful delivery of the project.

Every project undertaken in the Service should have an active project risk register that is updated regularly.

11. Information and Collaboration

In order to effectively manage all organisational risks, it is imperative to have oversight of internal controls to ensure that our risk management practises are aligned.

This requires collaboration across Directorates and departments but also with our strategic partners. To support a comprehensive view of the risk profile and to support of governance and decision-making requirements, all relevant stakeholders should be involved in the risk management process. This enhances systematic, iterative and collaborative risk information drawing on the knowledge of experts and stakeholders. By adopting this approach, we aim to.

- Bring together different functions and areas of professional expertise in the management of risks
- Ensure that different views are appropriately considered when defining risk criteria and when analysing risks
- Provide sufficient information and evidence to facilitate risk oversight and decision making; and
- Build a sense of inclusiveness and ownership among those affected by risk.

12. Review and Continuous Improvement

This Framework will be reviewed in line with the Community Risk Management Plan, however it will be reviewed and adapted taking into consideration internal and external changes to improve the effectiveness of our Risk Management System.

13. Risk Management Process

The Orange Book, published by HM Treasury, provides comprehensive guidance on risk management principles and processes for public sector organisations. The risk management life cycle outlined in the Orange Book includes several key stages:

- **Risk Identification:**

Identifying potential risks that could impact the organisation. This involves gathering information from various sources, such as historical data, expert opinions and stakeholder input.

- **Risk Analysis:**

Assessing the identified risks to determine their likelihood and potential impact. This can be done using qualitative methods (e.g., risk matrices) or quantitative methods (e.g., statistical analysis).

- **Risk Evaluation:**

Evaluating the assessed risks to prioritise them based on their severity and the organisation's risk tolerance. This helps in focusing on the most critical risks that need immediate attention.

- **Risk Treatment:**

Developing and implementing strategies to mitigate or manage the prioritised risks. This could include preventive measures, contingency plans, or transferring the risk through insurance.

- **Risk Monitoring and Review:**

Continuously monitoring the risks and the effectiveness of the mitigation strategies. Regular reviews and updates to the risk management plan are essential to adapt to new risks and changing circumstances.

Communication and Consultation:

Ensuring effective communication and consultation with stakeholders throughout the risk management process. This helps in building a risk-aware culture and ensuring that all relevant parties are informed and engaged.

Figure 4 – Five Steps of Risk Management Process

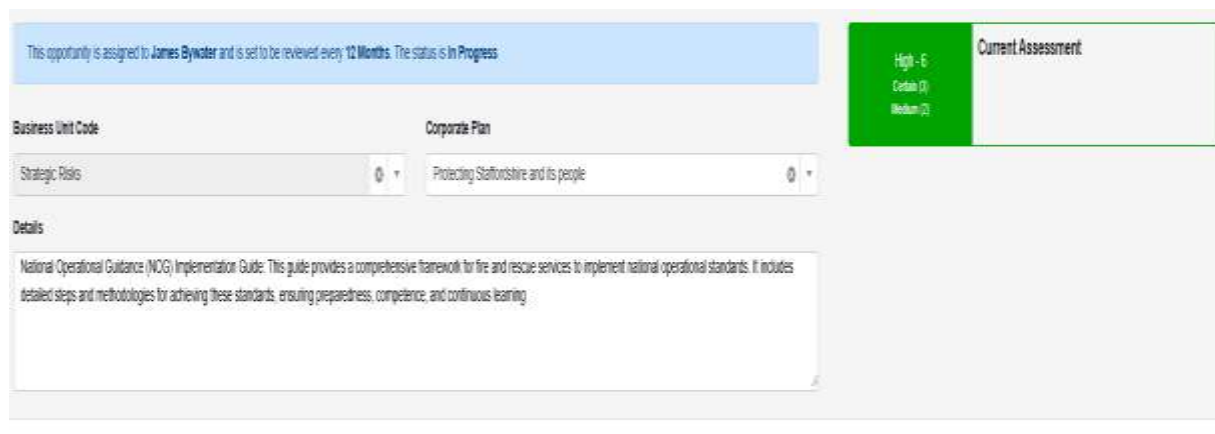


14. Opportunity Risk

Risk should be considered both threat and opportunity, by identifying risk better ways of working or alternative solutions can be considered such as partnerships. We record opportunity risks in much the same way and traditional risks and project risks.

An opportunity risk register is a strategic tool used in to identify, assess, and manage potential opportunities that could positively impact a project's objectives. Unlike traditional risk registers that focus on threats, an opportunity risk register highlights favourable events or conditions that, if seized, can enhance project outcomes. It includes details such as the description of the opportunity, its potential benefits, the likelihood of occurrence and the actions required to capitalise on it. By systematically tracking and evaluating opportunities, we can proactively leverage these chances to improve efficiency, reduce costs and achieve better results, ultimately contributing to the organisational success.

Figure 5 – Opportunity Register



This opportunity is assigned to James Bywater and is set to be reviewed every 12 Months. The status is In Progress.

Business Unit Code: Corporate Plan

Strategic Risk: Protecting Staffordshire and its people

Details: National Operational Guidance (NOG) Implementation Guide: This guide provides a comprehensive framework for fire and rescue services to implement national operational standards. It includes detailed steps and methodologies for achieving these standards, ensuring preparedness, competence, and continuous learning.

High - 6
Certain (1)
Medium (2)

Current Assessment

15. Insurance

Staffordshire Fire and Rescue Service are part of the Fire & Rescue Indemnity Company (FRIC). FRIC is a hybrid discretionary mutual established to provide tailored insurance solutions for fire and rescue services in the UK.

What is FRIC? FRIC was formed in 2015 by a group of fire and rescue authorities to address the need for a specialised insurance product that combines the benefits of traditional insurance with risk and financial pooling. It operates as a mutual, meaning it is owned and controlled by its members, focusing on service and satisfaction rather than profit.

Membership and Contributions Members of FRIC pay contributions instead of premiums. These contributions are pooled to cover the running costs and agreed claims. The mutual nature ensures that all members have equal voting rights, regardless of size or contribution.

Coverage and Claims FRIC offers discretionary protection backed by supporting insurance for statutory classes and large losses. Claims within FRIC's retention are paid from the pooled funds on a discretionary basis, while larger claims are covered by supporting insurers. This model provides flexibility and ensures that members are protected against significant financial risks.

One of the key benefits of FRIC is the emphasis on risk management. Members work together to improve risk management practices, share learning, and implement best practices. This collaborative approach helps in reducing the overall cost of accidents and improving safety standards.

16. Risk Management Guide



Risk Management Tools

The Service utilises JCAD Core to manage all its service risks effectively. JCAD Core is a comprehensive risk management software that enables the Service to identify, assess, and monitor risks systematically. By leveraging this tool, the Service can maintain a centralised risk register, ensuring that all potential risks are documented and addressed promptly. JCAD Core also facilitates real-time reporting and analysis, allowing for informed decision-making and proactive risk mitigation. This robust approach to risk management helps the Service maintain operational resilience and achieve its strategic objectives.

System Access

The system administrator is Vicky Adams. All record owners and control owners have view only access.

For new identified risks or risk registers

For any new risks or risk registers contact businessresilience.coordinator@staffordshirefire.gov.uk

Responsibilities

Strategic Risk Manager	Support and guidance on risk management process.
	Responsible for the Strategic Risk register and assisting the board with organisational risk awareness.
	Inputting of registers onto the JCAD system.
	Arranging periodic reviews and audit of the risk registers, controls and mitigations.
	Administrator of the JCAD system.
Directorate Leads	Regularly review the Directorate risk registers with the Strategic Risk Manager.
	Have risk as an agenda item at all Directorate meetings.
	Escalate risks to the Strategic Risk Board.
Department Leads	Regularly review departmental risk registers with the Strategic Risk Manager.
	Have risk as an agenda item at all department/team meetings.
	Escalate risks to the Directorate.
All Staff	Report any risks to the relevant department and the Strategic Risk Manager.

Risk Management Process

1. Identify

The purpose of risk identification is to collate all risks that might prevent or disrupt the delivery of the Service's or Departments objectives. This may include delivery of the Community Risk Management Plans, Departmental Annual Plans, Project Plans or other programmes of work.

- Risks should be identified at all levels of the Service including those that relate to collaborative working, partnerships and projects
- It is important to take the wider environment into consideration our Stakeholders and the environment in which the Service operates, when identifying risks.

The Service needs to understand what risks it faces in order to decide how to manage them. This step is about indenting what risks are. There are a number of methods that can be selected but will depend upon the type of risks that you have identified.

Risks can be identified in a number of ways, including:

- A workshop or brainstorming session with the whole management team
- Interviews
- Small group sessions
- Questionnaires.

Existing sources of information could help to inform the Identification stage.







Examples are listed below:

- Existing Risk Registers both directorate and departmental
- Committee reports
- Internal or external research papers or statistical information
- Risks or issues raised by internal or external audit
- Risks identified through budget setting activities
- Health and Safety risk assessments
- Business Continuity Risk Assessments
- Protective Security Risk assessments
- Project documentation such as risk registers and business cases
- Experience of colleagues who are experienced in risk identification processes.

Risk Categories

Potential risks are systematically identified and categorised based on their nature and source. By assigning risk categories at this early stage, risks can be organised and prioritised making it easier to develop targeted mitigation strategies later in the process. Our risk categories are set out in [table 1](#).

Table 1 – Risk Categories

Risk Category	Risk Description
Workforce 	<p>Risk arising from:</p> <ul style="list-style-type: none"> • The unavailability of people such as sufficient capacity and capability, industrial action • Health, safety and wellbeing of staff • Culture.
Service Delivery & Performance 	<p>Risks arising from:</p> <ul style="list-style-type: none"> • Failures in operational and support delivery • failing to meet performance targets.
Reputational 	<p>Risk arising from:</p> <ul style="list-style-type: none"> • Adverse events, including ethical violations, a lack of sustainability, systemic or • Repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.
Governance, Compliance & Legal 	<p>Risk arising from:</p> <ul style="list-style-type: none"> • The non-compliance with laws, regulations, contracts, licences policies and procedures • Failure of external audit or HMICFRS inspections.
Financial 	<p>Risks arising from:</p> <ul style="list-style-type: none"> • Adverse impacts on budgets or the Medium- Term Financial Strategy • Not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, • Failure to manage assets/liabilities or to obtain value for money from the resources deployed, • and/or non-compliant financial reporting.
Technology, Information and Data 	<p>Risk arising from:</p> <ul style="list-style-type: none"> • Technology not delivering the expected services • Inadequate ICT resilience • Failure to produce robust, suitable and appropriate data/information to exploit data/information to its full potential • Risk arising from failure to prevent unauthorised or inappropriate access to our systems/assets and information, including cyber-security and non-compliance with up data protection laws.

2. Risk Analysis – Analysing the Risk

In order to assess each risk a measurement is used to evaluate the overall significance to support decision making.

The Service has adopted a 5x5 matrix ([figure 1](#)) which is used to provide an overall risk score measured against risk categories ([table 1](#)), likelihood and impact. Once scored, the matrix identifies four possible risk priority levels as **Green**, **Amber**, **Red** and **Black** ([figure 7](#)).

Figure 1 – Risk Matrix

Impact	Critical	0	0	0	0	0
	Major	0	0	0	0	0
	Moderate	0	0	0	0	0
	Minor	0	0	0	0	0
	Insignificant	0	0	0	0	0
		Very Low	Low	Medium	High	Very High
		Probability				

The purpose of this risk analysis is to document the agreed level and priority of risk. The outcome of the risk should be recorded on a risk register and validated through the agreed governance structure.

Key Questions for a Risk Assessment

1. What can go wrong? – (and if you think that there really are things that can go wrong---)
2. How much can it go wrong? – (and if you think this is serious---)
3. How often can it go wrong? – (and if this is too often for comfort ----)
4. So, what are you going to do about it? – (if this is necessary/ possible?).

Risk Description – How to Express a Risk

Risk descriptions should be brief but fully communicate the risk identified. The description should capture the Risk, its Cause and Consequences.

Risks should be defined properly as failure to do so could result in confusion about the nature of the risk, ineffective or unnecessary controls being put in place or the overall analysis of the risk being over or underestimated.

Examples of Risk Descriptions

Objective – to travel by train from A to B for a meeting at a certain time	
Failure to get from A to B on time for the meeting	✗ this is simply the converse of the objective
Being late and missing the meeting	✗ this is a statement of the impact of the risk, not the risk itself
There is no buffet on the train, so I get hungry	✗ this does not impact on the achievement of the objective
Missing the train causes me to be late and I miss the meeting	✓ this is a risk which can be controlled by making sure I allow plenty of time to get to the station
Severe weather prevents the train from running and me from getting to the meeting	✓ this is a risk which I cannot control, but against which I can make a contingency

Phrases to begin with when articulating risk could be:

Failure to	Leads to a	Reduction of
Loss of		Disruption to
Inability to		Increase in
Inappropriate	Could mean	Lack of
Exploitation of		Realisation that
Enhancement of	Will have an impact on	Empowerment of

Risk Estimation

It is important that the Service has a common language of risk, therefore the Service must use the same methodology to calculate risk to ensure that there is an accurate overview of the risks that are posed.

The risks are score using two sets of criteria that are multiplied together to produce a total score which will provide a **GROSS** and **RESIDUAL** Risk Score.

Figure 2 – Risk Scores

Critical – 20 Critical (5) High (4)	Gross Risk Exposure: £0
Major – 16 Major (4) High (4)	Residual Risk Exposure: £0

The criteria's measured are **Impact** an event could have and the **Likelihood** of the event occurring.

Impact

Risk Impact is the expected harm or adverse effect that may occur due to exposure to the Risk. In other words, it measures how bad things could get if a particular risk materialises.

The impact is measured against the following categories to give an overall impact score.

Figure 3 – Impact Categories

	Insignificant Not Set	Minor	Moderate	Major	Critical
Financial	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Governance, Compliance & Legal	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reputational	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Service Delivery & Performance	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Workforce	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Likelihood

Risk Likelihood means the possibility of a potential risk occurring, interpreted using qualitative values such as low, medium, or high. This is in comparison with quantitative assessments, which use data and numbers. Our matrix assesses the risk based on qualitative and quantitative information.

Gross Risk

The level of risk faced by an organisation before internal controls/mitigating actions have been applied/implemented. Both the severity and probability of the risk are taken into account in generating the gross risk.

The assessment of gross risk could be seen as an exercise because in reality there are usually some controls in place, however, an initial assessment of gross risk does have a purpose when considering where in the range of ineffective to effective to excessive the controls actually are.

Residual Risk

The level of risk faced by an organisation after any internal controls/mitigating actions have been applied/taken into account. Both the severity and probability of the risk are taken into account in generating the net risk.

Target Risk Score

Target Risk means any acceptable specified risk level. When initially assessing the risk, you should agree the target residual risk rating and reviewed as part of the Reporting, Monitoring and Review stage against current controls, mitigations, risk information and appetite.

Figure 4 – Risk Scores

Critical - 15 Moderate (3) Very High (5)	Gross Risk Exposure: £0
Moderate - 12 Moderate (3) High (4)	Residual Risk Exposure: £0
Minor - 4 Minor (2) Low (2)	Target Risk Exposure: £0

3. Evaluating the Risk

Based on the risk assessment, the next step is to prioritise the risks based on their level of importance to the organisation's objectives. This step involves determining which risks require immediate attention and which risks can be managed over the long term.

Figure 5 - Risk Appetite

Statement	Description	Category	Level
Compliance & Legislation	a low appetite to accept any risk that could result in the non-co...	Governance, Compliance & Legal	Low or no appetite
Finance	a moderate appetite to accept risks that may impact on finance.	Financial	Moderate appetite
Safety of the Workforce	a low appetite to accept risks that could have a negative impac...	Workforce	Low or no appetite
Partnerships and Collaboration	a moderate appetite to risk with regards to the pursuit of partne...	Service Delivery & Performance	Moderate appetite
Values, Culture & Reputation	a low appetite to accept risks to organisational values, culture ...	Reputational	Low or no appetite

Figure 6 – Tolerance Rating

Name	AppetiteRating	ToleranceRating	Colour
Higher appetite	15	15	
Low or no appetite	4	10	
Moderate appetite	9	15	

Figure 7 – Risk Priority Matrix

	Very Low	Low	Medium	High	Very High
Critical	Moderate (3)	Moderate (10)	Major (15)	Critical (20)	Critical (25)
Major	Moderate (4)	Moderate (8)	Moderate (12)	Major (16)	Critical (20)
Moderate	Minor (3)	Minor (5)	Moderate (9)	Moderate (12)	Critical (18)
Minor	Minor (2)	Minor (4)	Moderate (5)	Moderate (8)	Major (10)
Insignificant	Minor (1)	Minor (2)	Minor (3)	Moderate (4)	Major (5)
	Very Low	Low	Medium	High	Very High
	Tolerable	Low Priority	Activity Necessary	High Priority	

4. Treating the Risk - Mitigations, Controls and Action Plans

Although, identifying and evaluating the risks, the key element is to determine a strategy to manage the risks effectively and efficiently, risk treatment is the process of taking action to minimise the likelihood of the risk occurring and reducing the severity of the impact should the risk materialise.

Selecting the most appropriate risk treatment options involves managing potential benefits of taking the risk against cost, effort, detriment, statutory obligations, Stakeholder and Service priorities. The following strategies can be adopted to mitigate the risk.

Treatment	Description
Tolerate	Do nothing and continue as planned. Unable to act or costs out way the benefit
Treat	Introduce control measures
Transfer	Share the exposure of the risk via insurance or partner.
Terminate	Withdraw from the activity

Controls and Mitigation.

The Institute of Risk Management guidance tells us that control actions are specific actions to reduce a risk event's probability of happening. Whereas defining a mitigation action reduces the impact of a Risk Event.

Control

Control involves implementing measures to prevent a risk from occurring or to reduce its likelihood. The goal is to manage the risk proactively by addressing its root causes.

Control measures are often put in place during the risk identification and assessment phases and are designed to prevent risks from materialising in the first place.

Examples: Installing fire alarms and sprinkler systems, enforcing security protocols, or conducting regular maintenance to prevent equipment failure.

Mitigation

Mitigation involves taking actions to reduce the severity or impact of a risk if it occurs. The goal is to lessen the potential negative consequences of the risk.

Mitigation strategies are typically developed during the risk planning phase and are implemented to minimise the impact of risks that cannot be entirely avoided.

Examples: Developing a disaster recovery plan, creating backup systems, or implementing training programs to reduce the impact of potential risks.

Risk Action Plans

Risk action plans are detailed strategies developed to address identified risks within an organisation or project. These plans outline the specific actions that need to be taken to mitigate, transfer, avoid, or accept risks.

Risk Strategies Explained

Risk management involves various strategies to handle potential risks effectively. Common risk strategies:

Risk Avoidance:

This strategy involves taking actions to avoid risks altogether. For example, a company might decide not to enter a market with high political instability to avoid associated risks.

Risk Reduction (Mitigation):

Risk reduction aims to minimise the impact or likelihood of risks. This can include implementing safety protocols, conducting regular maintenance, or training employees to handle emergencies.

Risk Transfer:

Risk transfer involves shifting the risk to another party. Insurance is a prime example of this strategy. By purchasing insurance, an organisation transfers the financial burden of certain risks (e.g., property damage, liability) to the insurer in exchange for premium payments.

Risk Retention:

Sometimes, we may choose to retain or accept certain risks, especially if the cost of mitigation or transfer is higher than the potential impact. This is often done for minor risks that have a low likelihood of occurring.

Risk Sharing:

Risk sharing involves distributing the risk among multiple parties. This can be seen in joint ventures or partnerships where risks and rewards are shared among the involved entities.

5. Monitoring and Reviewing the Risk

It is important that we monitor and review risks to ensure that the risks identified are still current and relevant and that the controls that we have in place are effective and achieving the desired outcomes, it also supports understanding whether and how the risk profile has changed. This process is ongoing and continuous.

When undertaking risk monitoring the risk owner/risk manager should consider:

- Are the key risks still relevant?
- Has anything occurred which could impact upon them?
- Are performance indicators appropriate?
- Are the controls in place effective?
- Have risk scores changed and if so, are they decreasing or increasing?

Escalating Risks

In the event that a risk has or has the potential to go outside of risk appetite then this should be escalated to the appropriate board for decision or awareness.

Reporting Risks and Risk Approvals

All risk registers should be reported through the following boards for approval.

Risk Register	Frequency	Approval	Oversight	Escalate to
Strategic Risk Register	Every quarter	Service Delivery Board	Service Governance Board	ETAP
Response Directorate Risk Register	Every quarter	Response Board	Strategic Risk Management Board	Service Delivery Board
Prevent & Protect Risk Register	Every quarter	Prevent & Protect Board	Strategic Risk Management Board	Service Delivery Board
Strategy & Intelligence	Every quarter	Prevent & Protect Board	Strategic Risk Management Board	Service Delivery Board
Human Resources	Every quarter	Strategic Risk Management Board	Service Delivery Board	Service Management Board
Protective Security Strategy Group	Every quarter	PSS Board	Strategic Risk Management Board	Service Management Board
Finance	Every quarter	Section 151 Officer/Director of Finance	Service Governance Board	ETAP
Shared Services	Every quarter	Strategic Risk Management Board	Service Delivery Board	Service Management Board
Service Delivery Groups	Every six months	Appropriate SDG Board/Meeting	Appropriate Directorate Board	Strategic Risk Management Board
Departments/Teams	Every six months	Appropriate Department/Team Meeting	Appropriate Service Delivery Group Meeting	Appropriate Directorate Board
Projects	Every month	Appropriate project meeting	Appropriate Service Delivery Group Meeting	Appropriate Directorate Board



Page Intentionally Left Blank

Appendix 1:

Staffordshire Fire and Rescue Service

Risk Appetite and Tolerance Statement 2025/2028

Risk Appetite Levels

Operational Risks:

Low Risk Appetite: We have a low tolerance for operational risks that could compromise the safety of the public or our personnel. This includes risks related to emergency response times, equipment reliability, and adherence to safety protocols.

Financial Risks:

Moderate Risk Appetite: We are willing to accept moderate financial risks to achieve cost efficiencies and invest in innovative technologies that enhance our service delivery. However, we maintain strict controls to ensure financial stability and accountability.

Compliance Risks:

Low Risk Appetite: We have a low tolerance for risks associated with non-compliance with legal and regulatory requirements. Ensuring compliance with all relevant laws, regulations and standards is paramount to our operations.

Reputational Risks:

Low Risk Appetite: We are highly sensitive to risks that could damage our reputation and public trust. We strive to maintain the highest standards of integrity, transparency, and professionalism in all our activities.

Strategic Risks:

Moderate Risk Appetite: We are open to taking calculated strategic risks that align with our long-term goals and mission. This includes exploring new initiatives, partnerships, and technologies that can enhance our capabilities and service delivery.

Risk Management Approach

To manage these risks effectively, we employ a comprehensive risk management framework that includes:

Regular Risk Assessments: Conducting thorough risk assessments to identify, evaluate and prioritise risks.

Mitigation Strategies: Developing and implementing robust mitigation strategies to manage identified risks.

Continuous Monitoring: Regularly monitoring and reviewing risks to ensure our risk management practices remain effective and responsive to changing circumstances.

Stakeholder Engagement: Engaging with stakeholders to ensure transparency and build a risk-aware culture within the organisation.

Risk Tolerance Levels

Risk tolerance levels refer to the degree of risk an organisation or individual is willing to accept in pursuit of their objectives. These levels help in making informed decisions about managing risks and are typically categorised as follows.

Low Risk Tolerance:

Organisations or individuals with low risk tolerance prefer to avoid risks as much as possible. They prioritise safety and stability, often opting for conservative strategies that minimise potential losses. This approach is common in sectors where safety and compliance are critical, such as healthcare and public services.

Moderate Risk Tolerance:

Those with moderate risk tolerance are willing to accept some level of risk in exchange for potential benefits. They balance risk and reward, implementing strategies that allow for growth and innovation while still maintaining a reasonable level of security. This approach is often seen in businesses looking to expand or invest in new technologies.

High Risk Tolerance:

High risk tolerance indicates a willingness to take significant risks for the possibility of substantial rewards. Organisations or individuals with high risk tolerance are often more aggressive in their strategies, pursuing opportunities that have higher potential returns but also come with greater uncertainty.

By adhering to this risk appetite statement, Staffordshire Fire and Rescue Service aims to balance risk and opportunity, ensuring the safety and well-being of our community and personnel while achieving our strategic objectives.

Consultation End Date: N/A		People Impact Assessed: N/A			Review Date: 14/04/2028	
Personnel may share the information in this document with members of the public:					Yes	
Date of Issue:	Title of Document:	Job No.:	Author:	Department:	Manager Approval:	Additional Information:
14/04/2025	Risk Management Framework 2025 - 2028	1493	Vicky Adams	Strategic Risk Management	Nick Jones 14/04/2025	Strategic Risk Board approved 03/03/2025
05/03/2024	Risk Management Framework 2024-2025	1493	Vicky Adams	Strategic Risk Management	Nick Jones 05/03/2024	Strategic Risk Board approval
24/11/2022	Risk Management Framework 2022-2024	1493	Vicky Adams	Strategic Risk Management	Nick Jones 21/11/2022	SDB approved 13/06/2022