.

Shropshire
Fire and Rescue Service

Brigade Order

Administration	
Title	**Corporate Risk Management**

Contents	Page No.

Roles, Responsibilities and Review

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

The **Head of Strategy, Risk and Improvement** is responsible for the day-to-day operation of this Order.

The **Head of Strategy, Risk and Improvement** will review this Order when new legislation arises or as and when organisational needs require.

Brigade Order: Administration

Organisational Risk Management

Purpose

This Order sets out how the Authority and the Service identify, assess, treat, monitor and report risks and opportunities to support delivery of the Community Risk Management Plan (CRMP), the Service Plan and statutory duties.

Service goals

This Order supports all of the Service goals set out in the Service Plan.

Introduction

This Order applies to:

- Corporate risks, managed through the Corporate Risk Register.
- Departmental, functional and project risks, managed through local risk registers and project governance.
- The RAIDO log, used as an early warning and decision log, not as a substitute for risk registers.

Principles of risk management

- Risk management is part of day-to-day management and decision-making.
- Risks are owned and managed at the right level, and corporate risks remain live and are reviewed regularly.
- Controls must be specific, owned and supported by evidence. Residual risk must be justified by how effective the controls are.
- Risk appetite guides prioritisation, escalation and assurance.
- Risk interdependencies are identified and recorded so linked and cascading impacts are understood.

Roles and responsibilities for risk management

Risk management roles are summarised below.

Fire Authority / Chief Fire Officer
Provides strategic accountability for corporate risk management, oversight of significant corporate risks and assurance on the adequacy of the risk management framework.
.

Audit and Standards Committee

Review corporate risk, provide scrutiny and assurance. Receive a quarterly review of the Corporate Risk Register and undertake a deep dive into corporate risk at least once a year. Endorse risk appetite and key thresholds.

Service Management Team (SMT)
As owners of the Corporate Risk Policy, SMT will recommend and review risk appetite/tolerance, manage corporate risks, ensure integration across risk registers and improvement plans, oversee control effectiveness and provide assurance on the effective delivery of risk management.

Head of Strategy, Risk and Improvement
Lead the Service's strategic risk management and oversee the day-to-day operation of this Order to ensure the effective delivery of risk management.

Risk owners
Accountable for accurate scoring (inherent and residual), interdependency assessment, treatment plans and timely reporting.

Control owners
Accountable for control design and operation; provide quarterly evidence of control effectiveness.

Heads of Department, managers and project managers
Own local risks, maintain registers, apply escalation and de-escalation rules, and manage departmental, functional and project risks through local governance arrangements.

All staff and partners
Identify emerging risks and follow required controls; raise concerns promptly.

Internal Audit
Provides independent assurance over the effectiveness of risk management and controls.

Defining risk

What risk means

Risk is defined as the **uncertainty of outcome**, whether that outcome is a positive **opportunity** or a negative **threat** (Cabinet Office, *Management of Risk in Government*).

Fire and rescue services operate in an environment where future events cannot be predicted with complete certainty. The Service must therefore anticipate what could happen and take action to reduce the likelihood of events occurring or the disruption they may cause.

Why it matters

Effective risk management helps the Service make informed decisions about policy, service delivery and operations. It is not a separate activity, but a core part of day-to-day management and strategic planning.

It also helps the Service decide what controls, assurance arrangements and insurance cover may be required.

The risk management cycle

To manage risk effectively, the risks linked to each policy option or service delivery method should be handled through a continuous cycle.

- Identify risks
- Analyse their causes and potential effects
- Put controls and treatment measures in place
- Review and monitor them on an ongoing basis

This continuous and systematic approach is referred to as the **risk management cycle**.

Corporate risks

Corporate risks are risks that could significantly affect the Service's medium- to long-term objectives, statutory duties or strategic priorities.

They usually affect more than one department, may require significant resources, and are typically owned by a member of the Service Management Team.

Departmental, functional and project risks

Departmental, functional and project risks affect the objectives of a department, function or project and arise through day-to-day operations or change activity.

They are usually managed within local resources and governance arrangements and are typically owned by the relevant Head of Department, Section Head, strategic lead or project manager.

Project risks

Project risks affect individual projects and are usually specific to delivery, timescales, cost or technical performance. They can often be managed within the project, but some will depend on support from other departments and should be managed collaboratively.

Departmental, functional and project risks should be reviewed regularly through normal management and governance meetings. If they grow, combine or cannot be managed effectively at that level, they may need to be escalated as corporate risks.

Risk appetite and tolerance

What is risk appetite?

Risk appetite is the nature and extent of risk that the Authority is willing to take to achieve its objectives. It sets the overall direction for decision-making, prioritisation, control design and assurance, and helps the Service explain clearly what sits within appetite and what falls outside it.

Appetite, tolerance and acceptance

Risk appetite is a directional statement of how much risk the Service is willing to take in a particular area, such as a service goal or risk type.

Risk tolerance is the maximum level of residual risk the Service is prepared to tolerate before further action, escalation or review is required.
Risk acceptance is a conscious decision that a residual risk can remain within appetite with routine monitoring and no additional treatment at that time.

The tolerance levels applied in this Order are designed to ensure that the Service responds proportionately to risk while reflecting its statutory duties, operational responsibilities and public accountability.

Lower-level residual risks may be managed through routine arrangements where impacts are limited and controllable.

As risk exposure increases, stronger controls, more frequent review and higher levels of oversight are required.

Risks with the potential to compromise public safety, legal compliance, operational readiness, workforce wellbeing or public confidence are subject to lower tolerance and may require escalation even where the numerical score alone would not place them in the highest band.

Why risk appetite matters

- Supports consistent decision-making, prioritisation and resource allocation.
- Clarifies how much uncertainty the Service will accept across service goals and risk types.
- Improves transparency by making explicit what is within appetite and what breaches red lines.
- Supports managed innovation and improvement while maintaining low tolerance for risks affecting safety, legality, integrity or public confidence.

SFRS risk appetite scale

SFRS uses the following five-point scale when setting appetite statements:

Appetite level	Definition

Averse	All precautions and mitigations in place with very low appetite for risk (likelihood of risk is rare but not impossible).
Cautious	Preference for safe delivery options that have a low degree of inherent risk, and which may only have limited potential for reward.
Balanced	Accepting that there is a degree of risk in activities and prepared to put resource in place to monitor and mitigate risks where the benefits of the activities outweigh the risk.
Open	Willing to accept higher levels of risk where benefits are clear and controls are proportionate.

Corporate risk appetite statement

SFRS will take managed and proportionate risks to improve services, deliver the CRMP and support transformation, while maintaining low tolerance for risks that could compromise public safety, health, safety and wellbeing, legal compliance, organisational integrity or public confidence.

Detailed risk appetite tables are set out in Appendix A.

Governance and review

The risk appetite statements are reviewed through the Authority's governance and scrutiny arrangements. They are reviewed annually as part of the corporate planning and financial cycle, and earlier if triggered by significant change such as funding pressures, major incidents, inspection findings, organisational change or material control failure.

Risk ownership

Good risk assessment starts with a clear understanding of the risk and the right people being involved from the outset. Once the risk is clearly described, the risk owner and control owner should be identified and involved in the assessment.

The **Risk Owner** is responsible for overseeing how a risk is managed and for reporting progress. Each corporate risk should be owned by a member of the Service Management Team. Departmental, functional and project risks may be owned by a Head of Department, manager or project manager.

The risk owner is usually the person with overall responsibility for the part of the Service most likely to be affected. As most corporate risks affect more than one department, the risk owner will usually be a senior or executive-level member of the Service.

Departmental, functional and project risks are usually limited to that area of activity, so ownership will normally sit with the relevant Head of Department, Section Head, strategic lead or project manager.

The **Control Owner** is responsible for implementing and operating the agreed control measures. They must have authority over the people and resources needed to control or mitigate the risk.

For corporate risks, the Control Owner is likely to be a Head of Department. For departmental, functional and project risks, it is more likely to be a named manager or project manager within the relevant area who is responsible for implementing the controls.

The initial choice of risk owner and control owner may change after the first assessment. If it does, the revised owners should take part in the final assessment and in all future reviews.

Risk Management Process

Identify

Risks and opportunities are identified through planning, performance management, horizon scanning, operational learning, audits and inspections, and change activity. Each risk must be clearly described, including the objectives affected and the key triggers.

Assess (scoring)

Corporate risks must be scored for both inherent and residual risk using the impact and likelihood criteria (Appendices C and D). Residual risk scoring must be justified by the effectiveness of controls and supported by evidence sources.

Each risk is assigned an impact score between 1 (lowest impact) and 5 (highest impact), and a likelihood score between 1 (lowest likelihood) and 5 (highest likelihood). The combined risk score (impact x likelihood) has a maximum value of 25.

Assess interdependencies (linked and cascading risks)

For each corporate risk, and any local risk being considered for escalation, the risk owner must record interdependencies so linked and cascading impacts are understood and managed, including:

- Upstream triggers/assumptions
- Downstream consequences (secondary risks)
- Shared controls
- Single points of failure (people, systems, suppliers or controls)
- Plausible best-case and worst-case outcomes where interdependencies are material

Where interdependencies materially increase the plausible maximum impact or reduce confidence in controls, the risk must be rescored and escalated if thresholds are met.

Evaluate (appetite, tolerance and prioritisation)

Risk evaluation determines whether a risk is acceptable, tolerable or unacceptable in relation to risk appetite and tolerance thresholds. Evaluation informs prioritisation, resourcing and reporting frequency.

Where residual risk falls outside appetite, breaches a stated red line, or enters the unacceptable band on the matrix, it must be escalated and subject to immediate review and further action.

The available responses are to terminate, treat, transfer, tolerate or insure the risk, depending on the level of exposure and the Service's appetite for that category.

Treatment of risk (response and controls)

Risk owners must choose an appropriate response and make sure proportionate controls are in place. Typical responses are terminate, treat, transfer, tolerate and insure. Treatment actions must be time-bound and have clear owners and milestones.

Terminate: choose an alternative approach that removes the risk altogether. This is not always possible, particularly where programmes intentionally accept higher risk in pursuit of greater benefits. Where it can be applied, however, it is usually the most effective risk management option.

Treat: manage the risk through proactive controls that reduce the likelihood of it occurring, reactive measures that reduce its impact, or a combination of both. The approach chosen will depend on the nature and level of the risk. Treatment should be set out in a risk reduction plan, monitored regularly, and developed by people with relevant knowledge and experience.

Transfer: pass some or all of the risk to another party, such as a contractor. This can be effective where the required expertise is not available within the Service, but it will usually involve additional cost.

Tolerate: accept the risk and continue. Care is needed, as organisations can gradually begin to treat accepted risk as if it were actively controlled when it is not.

Insurance: use insurance to cover the financial impact if certain risks occur. Insurance is one of the most common risk management tools and is often used alongside other treatment methods. Cover should be reviewed regularly to ensure it remains appropriate and continues to provide value for money.

Record

Risks must be recorded in the appropriate register with, as a minimum: description; objectives impacted; inherent and residual scores; controls and control owners; treatment actions; due dates; interdependencies; and review date.

Control Assurance Framework

A Control Assurance Framework operates for corporate risks to provide confidence that controls are well designed and operating effectively.

- Control owners provide quarterly updates on design adequacy, operating effectiveness, evidence of operation and issues/actions.
- Controls must be specific and measurable, linked to management information wherever possible.
- Where control failure materially increases residual risk, SMT must be notified immediately and Members informed through Audit and Standards at the next available cycle (or sooner where urgent).
- Assurance mapping is maintained for corporate risks (first line controls, second line oversight, third line assurance).

Integration, escalation and archiving

Risk management operates as a single integrated system across corporate, departmental, functional and project registers and associated governance arrangements.

The RAIDO log may be used for early warning, decision capture and dependency tracking, but it must not replace the formal recording, scoring, review and ownership of risks within the appropriate risk register.

A risk must be escalated where it can no longer be managed effectively within local authority, resources or governance, or where it has actual or potential cross-service, statutory, financial, safety or reputational consequences that require corporate oversight.

Escalation to the Corporate Risk Register is required where any of the following apply:

- Residual risk falls outside the agreed risk appetite, breaches a stated red line in the relevant appetite statement, or enters the Authority's unacceptable band on the risk matrix. A breach of a stated red line requires escalation even where the overall residual score has not yet reached the highest scoring band.
- The risk has, or could have, a material impact on statutory duties, the CRMP, the Service Plan, approved improvement priorities or other key corporate objectives.
- Cross-departmental, interdependent or cascading impacts materially increase the plausible maximum impact of the risk, reduce confidence in existing controls, or create wider service vulnerability.
- Further mitigation requires authority, resources, coordination or decisions beyond the current level of management, project governance or departmental control.
- The issue is attracting, or is likely to attract, significant Member, public, regulatory, inspectorate, partner, media or stakeholder interest.

For the purposes of escalation, material impact includes, but is not limited to:

- actual or potential failure to discharge statutory duties;
- significant impact on delivery of the CRMP, Service Plan or improvement priorities;
- significant financial pressure, unplanned cost, loss or affordability concern;
- reduced operational readiness, resilience, competence or business continuity;
- significant workforce, health, safety or wellbeing consequences; and

- significant reputational harm, loss of public confidence, or increased regulatory, Member or partner scrutiny.

Where escalation criteria are met, the originating risk owner must notify the relevant Head of Department or project sponsor and the lead officer for corporate risk management without delay.

Where the issue is urgent, serious or fast-moving, this notification must take place immediately by the quickest appropriate means, with formal transfer to the appropriate register completed within 10 working days.

Urgent escalation is required where there is a material control failure, a breach of a red line, a significant adverse change in residual risk, or an immediate threat to statutory compliance, public safety, operational readiness or organisational reputation.

The originating risk owner is responsible for identifying when escalation criteria may have been met and for initiating escalation without delay.

The relevant Head of Department or project sponsor is responsible for confirming that the escalation case is complete and that the risk is appropriately recorded pending transfer.

The decision to accept a risk onto the Corporate Risk Register rests with the Service Management Team, or with a delegated senior officer acting on behalf of SMT between meetings where urgency requires.

Once accepted onto the Corporate Risk Register, ownership must transfer to the appropriate SMT member as corporate risk owner, with a named control owner also assigned.

The Risk Group should provide review, challenge and quality assurance of escalation decisions and support consistency of application across registers, but it does not replace SMT accountability for corporate risk acceptance.

Where there is disagreement about whether escalation is required, the matter must be referred to the relevant SMT member or, where necessary, to SMT for determination.

De-escalation should be considered where residual risk has been reduced sustainably, controls and assurance arrangements are operating effectively, and corporate oversight is no longer proportionate.

Any decision to de-escalate a corporate risk must be recorded with the rationale, the destination register, the new risk owner and the continuing review arrangements.

Closed risks must be archived with the closure rationale, supporting evidence (including revaluation score of risk post mitigating actions/treatment), date of closure and approving authority recorded so that a clear audit trail is maintained.

Monitoring, reporting and assurance

Review frequency must be proportionate to residual risk and volatility.

As a minimum: unacceptable risks are reviewed monthly; tolerable risks quarterly; acceptable risks at least annually (or sooner if triggers occur).

Governance and reporting:

- SMT: fortnightly strategic review at the Performance and Assurance Board, focusing on changes in risk profile, controls and interdependencies.
- Risk Group (RG): quarterly assurance meeting covering corporate, departmental, functional and project risks, improvement actions and control assurance.
- Portfolio Board: monthly governance, assurance, and escalation - ensures continuous oversight of portfolio and project-level risks across the entire project lifecycle. Projects cannot pass through stage gates without Portfolio Board verification of their risk profile.
- Audit and Standards Committee: quarterly corporate risk report and an annual risk management summary report.

Minimum content for Audit and Standards Committee corporate risk reports:

- Inherent and residual scores and movement since last report.
- Interdependencies summary (key triggers/cascades and shared controls).
- Key controls with effectiveness rating and evidence sources.
- Mitigation actions, milestones, and barriers/issues requiring decisions.
- Financial/MTFS implications and links to CRMP priorities and improvement actions.

Working with partners, insurance and business continuity

Where services are delivered with partners or contractors, risk owners must make sure responsibilities, information sharing and residual risks are understood and recorded.

Insurance and business continuity arrangements support risk treatment. Relevant leads must review adequacy of cover and continuity plans periodically and after significant changes.

Training and competency

Mandatory risk management training is required for Audit and Standards Committee, SMT, departmental, functional and project risk owners, control owners and relevant project managers.

Training must be completed on appointment and refreshed at least every 24 months (annually for SMT).

Completion is recorded and reported quarterly through the Risk Group and annually to Audit and Standards.

Review and change control

This Order, the scoring criteria and the Risk Appetite Statements are reviewed annually (Apr–Jun) and additionally on trigger events.

Reviews are documented and approved through SMT and Audit and Standards, as appropriate.

Key definitions

Risk: Uncertainty of outcome (threat or opportunity).

Likelihood: The chance that a risk will occur.

Impact: The effect a risk would have on objectives if it occurs.

Inherent risk: Risk level before considering any controls.

Residual risk: Risk level after considering controls and their effectiveness.

Risk appetite: The nature and extent of risk the Authority is willing to take to achieve its objectives.

Risk tolerance: The maximum level of residual risk that can be accepted before escalation or further action is required.

Risk acceptance: A conscious decision to take no further action on a risk beyond existing controls.

Control: A policy, process, system or action that reduces likelihood and/or impact.

Control effectiveness: An assessment of how well a control is designed and whether it is operating as intended.

Treatment action: A specific action taken to reduce, transfer, avoid or otherwise manage a risk.

Risk owner: Accountable for monitoring, managing and reporting a risk.

Control owner: Accountable for design and operation of a control and provision of evidence.

Escalation: The process of raising a risk to a higher level of management because of its severity, impact or cross-service effect.

Interdependency: A link between risks, controls, systems or activities where one issue may trigger or worsen another.

Corporate risk: A risk that could significantly affect the Service's strategic objectives, statutory duties or cross-service priorities.

Departmental, functional and project risk: A risk affecting a department, function or project, including delivery, service, cost, scope, quality or benefits.

Risk register: The formal record of identified risks, scores, controls, owners, actions and review dates.

Appendix A - Risk appetite by risk type

This table sets out the Service's risk appetite by risk type. It explains the appetite level for each risk type, the kinds of activity that are within appetite, and the red lines that require escalation or further action.

A1. Summary of risk appetite levels

AVERSE	CAUTIOUS	BALANCED	OPEN
Health, Safety and Wellbeing Risks Legal and Regulatory Compliance Risks Cyber Security Risks	People and Culture Risks Governance Risks Financial Risks Reputation and Public Confidence Risks	Response Risks Protection Risks Enablers and Infrastructure Risks Strategic Risks Digital and Data Risks Assets, Estates, Fleet and Supply Chain Risks	Prevention Risks Improvement and Transformation Risks Project Delivery Risks

The summary table provides a quick reference to the appetite level assigned to each risk type. The detailed table below explains how each appetite level should be applied, including examples of activity within appetite and red-line issues requiring escalation.

A2. Detailed risk appetite statements

Risk type	Risk appetite level and meaning	What we will accept	What we will not accept
Response Risks	**BALANCED** - The Service will accept managed operational change where assurance, competence, supervision and contingency are in place, with low tolerance for risks to safety, command assurance or readiness.	Assured changes to response arrangements. Use of learning, exercising and debriefs to improve readiness. Short-term disruption where cover, command and escalation routes are clear.	Operating without competence, command assurance or safe systems. Unassessed gaps in preparedness or cover. Failure to act on operational learning. Persistent loss of readiness without recovery action.
Prevention Risks	**OPEN** - The Service will support evidence-led prevention innovation, targeted intervention and partnership delivery where this improves community safety and safeguards are in place.	Innovation with clear objectives, benefits and safeguards. Targeted interventions based on risk, vulnerability and local intelligence. Partnership delivery with agreed responsibilities and oversight.	Poorly targeted or unsupported interventions. Inequitable delivery or unmanaged safeguarding concerns. Partnership activity without ownership or accountability.
Protection Risks	**BALANCED** - The Service will apply proportionate, risk-based protection activity and professional judgement, provided statutory duties and public safety outcomes remain controlled and assured.	Risk-based inspection, audit and enforcement. Regulatory decisions supported by evidence and oversight. Improvement activity that strengthens compliance and public safety.	Failure to discharge statutory protection duties. Weak inspection, enforcement or quality assurance. Unlawful, inconsistent or poorly evidenced decisions.
People and Culture Risks	**CAUTIOUS** - The Service will favour lower-risk options, consultation, support and clear standards because these risks affect trust, inclusion, competence, wellbeing and morale.	Planned workforce change with consultation and mitigations. Recruitment, development and succession planning. Professional standards, inclusion and wellbeing managed through clear processes. Constructive challenge and speaking-up arrangements.	Behaviour that undermines dignity, inclusion or wellbeing. Leadership conduct that damages trust or culture. Known workforce, conduct or competence risks left unmanaged. Avoidable loss of workforce confidence or morale.
Improvement and Transformation Risks	**OPEN** - The Service will accept controlled uncertainty where improvement benefits are clear and readiness, dependencies and continuity are actively managed.	Managed change that improves outcomes, resilience or efficiency. Pilots with clear benefits, success measures and controls. Transformation with readiness and dependency planning.	Change with unclear benefits or weak governance. Transformation that compromises resilience, safety or continuity. Unmanaged dependencies, poor readiness or avoidable failure.
Strategic Risks	**BALANCED** - The Service will accept managed strategic	Strategic decisions with ownership, evidence and	Unclear accountability or ineffective oversight.

	uncertainty where it supports the CRMP, statutory duties, improvement priorities and public value.	oversight. Managed risk-taking supporting CRMP, duties or public value. Informed judgement where assumptions and trade-offs are recorded.	Strategic decisions compromising duties, safety or sustainability. Known governance or performance weaknesses left unresolved.
Governance Risks	**CAUTIOUS** - The Service will accept residual governance risk only where ownership, authority, audit trail, oversight and reporting are clear and proportionate.	Decisions with clear authority, evidence and recorded rationale. Improvement activity with ownership, reporting and assurance. Residual governance risk with clear audit trail and escalation route.	Decisions without authority, evidence or ownership. Weak oversight or failure to escalate material issues. Incomplete audit trails, poor reporting or unresolved assurance weaknesses.
Health, Safety and Wellbeing Risks	**AVERSE** - The Service will accept only unavoidable residual health, safety and wellbeing risk where safe systems, competence, supervision, equipment and assurance are in place.	Unavoidable residual safety risk with effective controls. Safe systems, competence, supervision, equipment and PPE. Prompt reporting, learning and action on hazards or wellbeing concerns.	Preventable harm or unsafe systems of work. Statutory breaches or weak safety assurance. Tolerance of unsafe behaviours, environments or practices.
Legal and Regulatory Compliance Risks	**AVERSE** - The Service will accept only tightly controlled residual legal or regulatory exposure supported by advice, evidence, oversight and timely escalation.	Tightly managed legal exposure with advice and mitigation. Decisions supported by evidence and documented rationale. Proportionate compliance activity supporting lawful delivery.	Operating outside legal requirements. Delayed escalation of material legal or statutory issues. Weak controls exposing the Service to sanction or legal challenge.
Financial Risks	**CAUTIOUS** - The Service will accept limited financial risk only where affordability, value for money, transparency, control and approved governance are clear.	Risk managed within approved budgets, plans and controls. Investment or savings supported by affordability and value-for-money assessment. Use of reserves or contingencies where justified, approved and in line with financial regulations.	Uncontrolled overspend or hidden liabilities. Financial decisions undermining resilience, safety or statutory delivery. Failure to escalate material affordability pressures.
Digital and Data Risks	**BALANCED** - The Service will accept managed digital and data change where it improves efficiency, insight, resilience or service quality.	Digital change with benefits, testing and fallback arrangements. Use of data to improve insight, decisions and service quality. Information governance and recovery arrangements proportionate to risk.	Digital or data change without testing or assurance. Data loss, poor data quality or poor information governance. Technology decisions compromising continuity or resilience.
Cyber Security Risks	**AVERSE** - The Service will accept only tightly controlled residual cyber risk, with effective prevention, detection, response and recovery arrangements.	Residual cyber risk with tested controls and response plans. Patching, access controls and awareness activity with clear ownership. Temporary exposure only where assessed, approved and mitigated.	Unmanaged vulnerabilities or unsupported systems. Failure to act on known threats, incidents or critical patches. Cyber risks compromising systems, data, continuity or confidence.
Assets, Estates, Fleet and Supply Chain Risks	**BALANCED** - The Service will accept managed risk in planning, procurement, maintenance and replacement where this supports delivery and value for money.	Planned maintenance and replacement of stations, fleet and equipment. Procurement and supplier activity with clear specifications and oversight. Contingency arrangements for key assets and supplies.	Readiness, safety or compliance compromised by poor asset management. Single points of failure without contingency. Poor procurement or contract management causing avoidable disruption or cost.
Project Delivery Risks	**OPEN** - The Service will accept controlled uncertainty in project delivery, pilots and innovation where benefits are clear and governance is effective.	Minor cost, time, scope or benefit variances within tolerances. Pilots and innovation supporting learning and benefits realisation. Project change with governance, dependency and contingency planning.	Material changes outside approved tolerances that are not approved, controlled or escalated. Projects with weak governance or no recovery plan. Change compromising resilience, safety, statutory duties or compliance. Projects continuing to slip without corrective action.
Reputation and Public Confidence Risks	**CAUTIOUS** - The Service will accept limited reputational exposure only where decisions are lawful, transparent, ethical, evidence-based and well communicated.	Reputational risk managed through lawful, transparent decisions. Open communication explaining decisions, performance and improvement. Constructive handling of	Poor communication or failure to respond to legitimate concerns. Ethical failure, hidden issues or conduct undermining trust. Decisions or behaviours

		scrutiny, complaints and stakeholder concern.	creating avoidable harm to confidence.

Appendix B - Impact assessment ratings

Impact	Service delivery	Portfolio Delivery	Financial	Reputational	Examples (SFRS context)
Very High (5)	Catastrophic impact on statutory duties, public safety or strategic objectives, causing major external disruption or sustained loss of service.	Delay >6 months, catastrophic impact project delivery / functionality	Financial impact on the Authority likely to exceed £5M.	Extreme stakeholder concern with sustained national scrutiny and a strategic response required.	Examples: prolonged loss of critical response capability across multiple stations; major workforce failure affecting service resilience or leadership capacity; multiple serious health and safety failures causing severe disruption and lasting loss of confidence.
High (4)	Major impact on statutory duties or strategic objectives, causing significant service disruption or loss that is visible externally.	Delay 3-6 months, major impact delivery / functionality	Financial impact on the Authority likely to be between £1M and £5M.	High stakeholder concern with significant regional or national attention and senior-level response required.	Examples: prolonged unavailability of a specialist capability or key asset; significant recruitment delays or workforce shortages affecting station or department capacity; a serious health and safety failing requiring urgent recovery action.
Medium (3)	Noticeable impact on delivery of objectives, causing internal disruption, reduced performance or limited external service effects.	Delay1-3 months, some impact to key delivery / functionality	Financial impact on the Authority likely to be between £250K and £1M.	Moderate stakeholder concern with sustained local scrutiny and formal communications required.	Examples: temporary station, ICT or project disruption affecting local delivery; short-term backlog in recruitment, training or prevention activity; a local health and safety issue requiring additional controls and monitoring.
Low (2)	Limited impact on objectives, causing short-term internal disruption with little or no material effect on external service delivery.	Delay 1-4 weeks, minor impact to overall delivery / functionality	Financial impact on the Authority likely to be between £50K and £250K.	Low stakeholder concern with limited local interest and routine communications handling.	Examples: one-off delay in procurement, maintenance or a support system; minor delay in recruitment to a post or routine HR process; isolated health and safety concern resolved through normal management action.
Very Low (1)	Negligible impact on objectives with no meaningful interruption to service delivery.	Delay 1 week, Minor impact to secondary delivery / functionality	Financial impact on the Authority likely to be less than £50K.	Very low stakeholder concern with little or no media interest.	Examples: minor administrative or equipment issue with no operational effect; short-lived delay in a recruitment or HR process; minor health and safety paperwork issue with no external impact.

Appendix C - Likelihood assessment ratings

Likelihood	Description	Probability	Examples (SFRS context)
Very High (5)	Expected to occur frequently or is already occurring	(>70%), The risk has occurred and will continue to do so impacting project success without further action being taken.	Examples: repeated appliance or ICT disruption affecting service availability; repeated recruitment delays or workforce shortfalls affecting critical posts; repeated shortfalls in health and safety compliance or assurance.
High (4)	Likely to occur	(51-70%), The risk is likely to occur this year / this project or programme.	Examples: recurring delay in replacing key fleet, equipment or systems; recurring recruitment difficulties, absence pressures or retention issues; recurring backlog in health and safety actions, audits or training compliance.
Medium (3)	Could occur	(31-50%), The risk could occur or has occurred occasionally in comparable circumstances.	Examples: a local estates, ICT or project issue affecting delivery in one area; a delayed recruitment campaign or local workforce pressure; a local health and safety issue creating short-term resilience pressure.
Low (2)	Unlikely to occur	(11-30%), The risk is not expected to occur in most circumstances but remains possible.	Examples: one-off failure of a non-critical system or support process; isolated recruitment delay or minor HR case that can be managed locally; a minor health and safety action that can be completed through routine management.
Very Low (1)	Rare / exceptional	(0-10%). The risk may occur in exceptional circumstances.	Examples: simultaneous loss of multiple stations or critical assets from a single cause; an exceptional workforce event with limited credible precedent for the Service; an exceptional health and safety event despite established controls.

Appendix D – Risk escalation flow table

This appendix summarises the escalation route for risks moving from departmental, functional or project governance into corporate oversight. It is intended as a practical guide and should be read alongside the main section on integration, escalation and archiving.

Stage	Trigger / question	Required action	Responsible role	Output / governance record
1. Identify	Has a local risk changed, worsened, or shown cross-service consequences?	Review the risk description, causes, impacts, controls, dependencies and current score.	Originating risk owner	Updated entry in departmental, functional or project register.
2. Test for escalation	Is the risk outside appetite, in breach of a red line, in the unacceptable band, materially affecting statutory or corporate objectives, or beyond local authority/resources?	Apply the escalation criteria and record the reason escalation is or is not required.	Originating risk owner with Head of Department or project sponsor	Documented escalation assessment and rationale.
3. Immediate notification	Is the issue urgent, serious or fast-moving, including material control failure, red-line breach, significant adverse score movement, or immediate threat to compliance, safety, readiness or reputation?	Notify immediately by the quickest appropriate means and do not wait for the next routine meeting.	Originating risk owner	Immediate notification to Head of Department or project sponsor and lead officer for corporate risk management.
4. Prepare escalation case	Has the case been sufficiently evidenced for corporate consideration?	Confirm the risk description, affected objectives, inherent and residual scores, controls, control assurance, dependencies, mitigation actions, cost of mitigation v risk cost impact and reason for escalation.	Head of Department or project sponsor	Completed escalation submission and risk record pending transfer.
5. Corporate consideration	Should the risk be accepted onto the Corporate Risk Register?	Review the case, challenge the assessment, and decide whether the risk requires corporate ownership.	SMT or delegated senior officer acting on behalf of SMT. Portfolio Manager will escalate corporate risks from Portfolio Board.	Decision recorded in SMT governance and, where accepted, formal entry on the Corporate Risk Register.

6. Assign ownership	If accepted, who will own and control the risk corporately?	Assign an SMT member as corporate risk owner and a named control owner with clear treatment actions and review frequency.	SMT	Corporate risk ownership and action tracking recorded.
7. Assurance and review	Is the escalated risk being reviewed and challenged consistently?	Provide review, challenge and quality assurance, and monitor whether the risk should remain corporate, be de-escalated or be closed.	Risk Group with SMT oversight	Quarterly assurance record, updated register entry, and where relevant de-escalation or closure decision.
8. Timescale	Has the formal transfer been completed on time?	Complete formal transfer to the appropriate register within 10 working days, unless immediate escalation arrangements already require faster action.	Originating risk owner and lead officer for corporate risk management	Transferred record with clear audit trail from local to corporate governance.

Where there is disagreement about whether escalation is required, the matter must be referred to the relevant SMT member or, where necessary, to SMT for determination. Where a corporate risk is later reduced sustainably and corporate oversight is no longer proportionate, de-escalation should be recorded with the rationale, destination register, new owner and continuing review arrangements.

Appendix E – Risk Matrix

This matrix provides a consistent method for assessing and prioritising risk, but it must be read alongside the Service's risk appetite statements, tolerance thresholds and stated red lines.

The tolerance levels reflected in the matrix are based on residual risk and are intended to ensure that management attention, review frequency and escalation are proportionate to the potential effect on statutory duties, service delivery, public safety, workforce wellbeing, legal compliance and public confidence.

Lower-band risks will normally be managed through routine controls and periodic review.

Medium risks require active management and regular monitoring.

High risks sit at or near the Service's tolerance limit and therefore require senior oversight and specific treatment plans.

Very High risks are outside normal tolerance and require urgent action, executive oversight and escalation where existing controls are insufficient.

A breach of a stated red line, or any risk with potentially intolerable safety, legal or ethical consequences, requires escalation even if the numerical score does not fall within the highest scoring band.

Impact

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

Likelihood

Risk Matrix Descriptors	
Low	**Passively Accept.** These risks should be managed through normal service, people and safety management arrangements. They may cause limited local disruption, minor workforce pressures or low-level health and safety issues, but are not expected to affect wider service resilience. They require routine monitoring and proportionate controls to ensure that the score does not increase.
Medium	**Actively Manage.** These risks require active management because they may disrupt service delivery, create sustained people or recruitment pressures, or expose the Service to material health and safety concerns if not addressed. They should be monitored regularly, supported by clear controls and contingency arrangements, and escalated if performance, staffing or safety indicators deteriorate.
High	**Escalate immediately to senior accountable person.** These are significant risks that require senior attention. They may have major implications for operational delivery, workforce capacity or wellbeing, and health and safety assurance, whether the trigger is immediate or developing. Specific treatment plans, strong oversight, exercising or training, and regular review are required to reduce the likelihood or impact.
Very High	**Escalate to CFO.** These are critical risks requiring immediate action and executive oversight. They have the potential to cause severe operational disruption, major people or leadership impacts, or serious health and safety consequences, and must be treated as a priority regardless of how quickly they may materialise. Urgent control measures, specific planning, clear ownership and frequent monitoring are required, with escalation where existing arrangements are insufficient.