Essex County
Fire & Rescue Service

Risk Management Strategy 2020

Author:	H.O’Sullivan
Authorised:	D.Bill
Date:	June 2020
Version:	1.0

Table of Contents

Risk Management Strategy

Introduction

Essex County Fire and Rescue Service (ECFRS) Risk Management Strategy sets out the ways in which the organisation engages with the tenants of enterprise risk management in order to support The Authority in the delivery of its mission statement as set out in the Fire and Rescue Plan *'To make Essex a safe place, to live, work and travel'.*

Engaging with enterprise risk management and developing a risk aware culture ensures that risk based decision making is embedded in all processes across the Service, allowing the Service to plan for, anticipate and manage risks which may impact upon service delivery and the achievement of objectives.

In line with the principles of risk management staff are encouraged to consider the positive as well as the negative side of risk.

Planning future development and opportunities to engage in innovative ways of working ensure that the Service can continue to provide its core services in an effective and efficient manner adapting to wider changes and challenges.

Risk Management Framework and Principles

The Service has developed a framework for Risk Management which aims to integrate the principles of risk management into all processes and activities

The Services applies the Risk Management Principles as set out in ISO3000:2018; -

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives'

The adoption of the principles is laid out in the following strategy, by providing a clear structure for the management of risk which is adapted to the needs of ECFRS and the community it serves.

Ensuring accurate and relevant information forms the basis of decision making taking into account the views and needs of stakeholders.

All staff within the organisation have defined roles and responsibilities for ensuring effective risk management takes place. These are detailed in the following tables.

Roles and Responsibilities **ECFRS**
CEO/CFO
Determine the strategic approach to risk, understand the most significant risks and the implications of poor decision making. Manage the organisation in when business continuity arrangements are instigated.
Senior Leadership Team
Ensure Risk Management is embedded into all processes. Understand the risk profile for the Service and set the risk appetite. Receive reports on Strategic Risks and effectively manage these as risk owners.
Director of Innovation, Risk & Future Development
Oversee the corporate approach to risk management, including the management of strategic risks Develop and maintain the risk strategy, including an annual review Provide reports to SLT, PFCC and the Audit Committee as required Ensure SLT Risk Owners are regularly reviewing their risks as set out in the Strategy
Directorate Management
Prepare and keep up to date directorate risk registers. Set the directorate priorities. Track Risk Management Activity in Areas. Build risk aware culture in the area. Identify and report changed risks and circumstances.
Risk Advisor
Develop and establish the Risk Management Framework including policy, strategy and guidance documents. Support and co-ordinate implementation of Risk Management activity at all levels. Facilitate a risk aware culture. Compile risk information and prepare reports for the board.
Specialist Risk Functions including Health & Safety, Business Continuity and Data Protection
Assist in the development of specialist risk policies. Develop contingency and recovery plans. Keep up to date with developments in specialist areas. Support investigations and report near-misses. Prepare detailed reports on specialist risks.
Risk Owner
Develop risk treatment plans. Monitor progress of controls and actions. Report on treatment progress. Implement agreed actions to support treatment strategies. Report on progress and recommend any other controls or actions needed to manage the risk.
All Employees
Understand accept and implement the Risk Management Process. Assist in the Management of Controls reporting those which are inefficient or unworkable. Report Near Misses and Loss events. Ensure visitors and contractors comply with procedures.

Roles and Responsibilities
Change

Strategic Change Board

Review the Strategic Risk Register with a view to mitigating risk through the delivery of change.
Provide advice, support and guidance for escalated Programme and Project risks.
Escalate risks to the Service Leadership Team as required.

Senior Responsible Owners

Support and Encourage formal Risk Management programme with the Programme and Project
Set and Monitor thresholds
Attend risk workshops
Review risk outputs with relevant manager to ensure consistency and effectiveness
Make decisions regarding project strategy

Programme Board

Assess and approve Programme and Project risks and the proposed Control Measures.
Monitor the effectiveness of the Control Measures and provide assurance that the risk mitigation and control environment remain effective.
Escalate risks to the Strategic Change Board as required.
Provide oversight, at a Programme level, for Project risks, and monitor dependencies across Programmes and Projects.

Programme & Project Manager

Manage overall risk process for programmes and projects.
Work with Senior Responsible Owners to set thresholds.
Participate in workshops.
Approve treatment plans.
Oversee Risk Management of contractors and suppliers.
Report risk profile to Change board with recommendations for decisions and actions to maintain acceptable threshold.
Highlight identified risks which are outside of scope or require input from other areas.
Monitor the progress of control techniques.
Ensure risks are closed ahead of formal closure.

Organisational Risk Levels

Though the principle of risk management remains the same throughout, the Service manages risk at a number of levels; -

Strategic Risk

Risks at this level would have serious impact on service delivery, both in its core functions and delivery of the Fire and Rescue Plan objectives. These are risks which, should they materialise would have the most impact on the public, have media interest and significantly impact on key partners and other key stakeholders.

Ownership of strategic risk is a requirement of the Senior Leadership Team (SLT), in order to provide the appropriate direction and management. Risk Management is championed on SLT by the Director of Innovation, Risk and Future Development at SLT Meetings.

Assessment of Strategic Risk is based on the following:

- Legislative Requirements, for example The Fire and Rescue Service Act (2004)
- The Fire and Rescue Plan objectives
- Effective delivery of the Services Integrated Risk Management Plan
- Stakeholder Value and Expectations
- Provision of a fit for purpose Organisation through efficient and effective core responsibilities

Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services All new strategic risks must be formally agreed at a SLT meeting, as will any decision to remove any Strategic risk from the register.

Directorate Risk

This represents risk at the Tactical Level, risk which would prevent or hinder effective and efficient service delivery of the directorate objectives and will normally be managed within Directorate meetings. Directorate risk will be measured against the achievement of objectives and associated performance measures.

Assessment of Directorate Risk is based on the following:

- Control Measures and activities resulting from management of strategic risk
- Tasks allocated within the Services Annual Plan
- Directorate Activity Plan
- Implementation of legal compliance requirements

Operational Risk

The represents risk in delivery of the Service’s Prevention, Protection and Response activities, the management of which are set out within a number of strategies, policy and guidance documents. Though not an exhaustive list, this includes the Service’s;

- Health and Safety Policy
- Prevention, Protection and Response Strategies
- People Strategy
- Standard Operating Procedures
- Technical Bulletins

New and Emerging Risk

The Service will aim to identify and manage new and emerging risks. All new strategic risks must be formally agreed at a SLT meeting. Due to the long-term nature of emerging risk, The Service, will aim to integrate the identification of new and emerging risk into the strategic planning process. This will enable The Service to plan for any required mitigation to the development of negative risk and peruse opportunities for innovation and future developed of ECFRS.

The SLT should remain aware of changes to trends, performance and outside influences which may later have an impact on our business assumptions. It is required that SLT should include assessing new and emerging risk as an agenda item, separate to the general risk agenda point. Considerations for new and emerging risk would be;

- Legal, political or judicial development, including new law, judgements or public enquires
- Recommendations made in reports published by Her Majesty’s Inspectorate of Constabulary, Fire and Rescue, National Fire Chief Council and similar bodies
- Findings of reports or experiences of other Fire and Rescues Service or public body.

Programme and Project Risk

Delivery of change through programmes and projects is vital in mitigating the potential impacts of an identified risks being realised. It is therefore vital the Service fully understands the potential impacts of the risks of a programme or Project not being delivered in line with the agreed scope or tolerances.

The Risk Environment

The Service utilises the PESTLE classification systems for providing context to the External and Internal risk environment; this can be used in conjunction with other methods.

The **external** context may consist of, but not be limited to:

- The social, cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environments,
- Key drivers and trends having an impact on Service corporate objectives,
- Relationships with, and perceptions and values of, stakeholders and partners.

The **internal** context may consist of, but not be limited to:

- Governance, organisational structure, roles and responsibilities;
- Policies, objectives, and the strategies that are in place to achieve them;
- Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

Internal Context

The Service provides a public service, the key function of which are set out in a number of statutory obligations including those detailed in the Fire & Rescue Services Act (2004), the Regulatory Reform (Fire Safety) Order (2005), the Civil Contingencies Act (2004) and the Policing and Crime Act (2017).

The Service is governed by the Police, Fire and Crime Commissioner for Essex, and is subject to an inspection regime conducted by Her Majesty's Inspectorate of Constabularies and Fire & Rescue Services.

The Fire and Rescue Plan Priorities are:

- Prevention, protection and response
- Improve Safety on our roads
- Help the vulnerable stay safe
- Promote a positive culture in the workplace
- Develop and broaden the roles and range of activities undertaken by the service
- Be transparent, open and accessible
- Collaborate with our partners
- Make the best use of resources

In addition, the Service has identified the following priorities:

- Medium Term Financial Plan – from April 2020 the Service is having to do its financial planning only knowing its budget one year ahead, rather than establishing a long-term financial understanding of funding provided.
- The Service's response to the Grenfell incident and consequent resourcing of its Technical Fire Safety Team
- Additional funding has been identified to invest in operational training and our On-Call employees
- Significant investment is being allocated to improve and upgrade our ICT infrastructure
- Cultural change – The Service continues to build on the work completed so far in developing a safe and diverse workforce who we enable to perform well in a supportive, modern, forward looking, innovative and collaborative culture
- Data Management – the Service has experienced a number of challenges in its management of data, in particular the use of ICT systems.

External Context

As an active partner in the Local Reliance Forum for Essex, the Service is able to keep informed of and disseminate relevant information from The National Risk Assessment and the Community Risk Register. The outputs of which are used to inform the Strategic Risk Register.

The local context is further informed via the Strategic Assessment of Risk (SAOR) which complies relevant data and risk considerations into a single document specifically covering the Greater Essex Area in order to better pinpoint areas of potential risk in the delivery of Prevention, Protection and Response Activities.

The SAOR underpins and informs the Integrated Risk Management Plan (IRMP) by identifying risks and subsequent mitigations (at the strategic level) in order to assist with the identification of any gaps or required enhancements in capabilities and/or response.
This allows the Service to plan and allocate resource where it is likely to be needed the most, by considering the following information:

- The current issues and likely future trends of demography, house building, industry, and transport infrastructure within Essex.
- The National Risk Register and other National assessments
- The work of the Essex Resilience Forum in relation to the Community Risk Register.

- Likely risks to which ECFRS may have to respond if prevention and protection activities fail in preventing unwanted risk events.
- Environmental issues, including the impact climate change on service delivery
- Possible improvements in capabilities.
- Previous data and learning from previous incidents (both locally and Nationally, e.g. the Grenfell incident)

Risk Assessment

As part of the Risk Assessment process, risks should be identified against Objectives, Programmes and Projects, Core Process and any activity which may give rise to Hazard Risk. Identified Risks are analysed using qualitative and if possible quantitative measures, to create a risk profile. The profile creates a tool for evaluating risk and the action that needs to be taken.

Risk scores are analysed using a 5 x 5 matrix (Appendix One) which allows the Service to plan the appropriate action and report on an exception's basis in line with the Risk Appetite Statement.

In addition to the process outlined in ISO3100:2018 the Service advocates using the Bow-Tie methodology when carrying out a risk assessment. The Bow-Tie method enables the consideration of risk in the context of possible triggers, impacts and controls as well as providing a tool for Root Cause Analysis and the development of a business case for action.

Risk Treatment

In selecting the correct treatment options, the Service requires employees to consider the benefit of the selected treatment against the cost and effort involved in implementation and maintenance of that particular control. The Service advocates using the 4T's in deciding on the appropriate of control measures. These are:

- Transfer the risk through insurance or third parties
- Treat the risk until it is within acceptable limits
- Terminate the activity giving rise to the risk and explore other ways to achieve the objective
- Tolerate the risk, either because it is within acceptable limits or the cost of controlling the risk would require such a level of cost or resourcing that it would not be practical to implement the control.

These are not mutually exclusive, for example collaboration should be considered as a means of mitigating risk and generating an opportunity, what is important is that controls must be well thought out before implementation. Risk Owners are required to develop a risk treatment plan with the appropriate employees and subject matters experts. The table below provides a guide as to what action is likely to be appropriate based on the risk score.

	Risk Treatment Guide
High **15-25**	Critical Risk: these require immediate attention. Strategies must be developed in order to eliminate or reduce the risk; it may be necessary to halt the activity until adequate measures can be put in place. Action will center on eliminating or reducing the source of the risk wherever possible. Immediate action should be taken, escalation should be considered until the appropriate controls are in place and the risk decreased to a suitable level. These risks have breached the Services risk tolerance levels and should be reported on a monthly basis.
Medium **8-12**	These may have a high or low likelihood of occurrence but the consequences if they do occur are such that they should be given consideration. Treatment options would normally consider policies, procedures and training to minimize the risk, in addition to, contingency planning and insurance arrangement to deal with possible consequences should the risk occur. These risks have breached the Services stated risk appetite.
Low **4-6**	Whilst these risks are less significant, they may cause considerable upset and inconvenience in the short term. These risks should be monitored to ensure they are being effectively managed. Management of these risks will revolve around treatments which enforce desirable behaviors and reduce undesirable outcomes. These risks are within the Services stated risk appetite.
Very Low **1-3**	Those risks that are low likelihood and low impact. The organisation is able to tolerate these risks at their current level. These should be monitored, and awareness maintained of any changes which would require the risk being moved into another category of risk. These risks are to be monitored as possible candidates for new and emerging risks.

Reviewing, Recording, Reporting and Escalation

The Service uses the risk recording software JCAD Core to record risk and associated control measures. The software allows the Service to provide a transparent record through which reviews can be conducted and reports generated.

The reporting of risk is aligned with the Services strategic reporting regime, to ensure that consideration of risk plays a key role in decision making at all levels of the organisation.

SLT members will be owners of the Strategic risks. Red risks will be reviewed by risk owners at least once a month, amber risks at least once a quarter and yellow risks at least once every six months. The Strategic Risk Register shall be reported to SLT once a month, and the PFCC's Performance and Resources Board every quarter. SLT will also review all strategic risks in detail at least once a year.

Any new risk considered to be almost certain or likely and/or major or critical shall be escalated to the PFCC at the next Performance and Resources Board, any new red risks immediately.

Control owners should report regularly to the risk owner, it is recommended that this is done at team meetings as part of the normal reporting process.

It is the responsibility of the risk owner to ensure that controls are being implemented effectively and in a timely manner.

Risk Appetite

Risk appetite is best summarised as "the amount of risk an organisation is willing to accept" and considers the propensity to take risk. Risk appetite provides the means to assess whether the organisation is operating within acceptable limits.

Risk appetite enables the Service to communicate with staff the parameters within which they are allowed to take risk. If there is a case for taking on more risk to achieve specific objectives that will be beneficial to the organisation, this will be considered by the SLT.

Where risk is said to be outside of the desirable risk appetite, measures should be taken to treat the risk back within acceptable limits or options considered as to whether the risk can be transferred, terminated or tolerated at its current rating.

Where organisational performance as a whole exceeds the risk appetite limit, consideration will be given to providing a full stop on further change activity that may introduce more risk into the organisation.

Both the risk appetite and risk profile of the organisation will be regularly monitored by The Authority and the SLT through performance reports and formally reviewed on an annual basis unless circumstances demand otherwise, to assess if the statement remains appropriate.

Risk Appetite Statement

This statement sets out the thinking and guidelines behind our risk appetite. Risk appetite should be formally applied throughout the organisation[1].

Public Value – The Service has no appetite for tolerating a critical risk, a major risk will only be tolerated in order to meet a public need, i.e. response to a major operational incident. This will be monitored within the Service current budgetary assurance processes already in place.

People – The Service has no appetite for tolerating a critical risk. The Service is committed to providing a safe, well trained workforce with a positive and kind culture. People risks are monitored through the Learning and Development Steering Group and the People Strategy Board.

Infrastructure – The Service has no appetite for tolerating a critical risk, a major risk will only be tolerated where business continuity arrangements, although stretched will ensure that the Service core functions can be met. This will be monitored by individual department performance reports.

Reputation – Due to the Service's trusted brand, the Service has no appetite for critical or major risks. This will be monitored via the Service Communications and Media Department.

Compliance – The Service will not tolerate a risk, which would leave the Service being non-compliant with a legal duty.

The Service has no appetite for tolerating critical or major risks or any foreseeable risk that could result in injury or loss of life to the public or employees. This is monitored by the Strategic Assessment of Risk and the Service's Health and Safety Strategy Group, and results of which are published in the Annual Health and Safety Report.

In the pursuit of delivering the objectives of the Police and Fire Crime Commissioner's Fire and Rescue Plan's Objectives the Service is willing to accept some closely monitored minor or significant risks. Using the appetite maturity scale recommended by the institute of good governance (Appendix B) the SLT appetite is "Open" with a view to becoming 'seeking' providing control and monitoring of risk in place. The Effectiveness of this is measured through the Service's quarterly performance reports.

Communication and Consultation

The Service will, via Corporate Communications, dissimilate information from specialist risk functions concerning near misses and lessons learnt; this will include business continuity events, Health and Safety, near misses and data breaches. Lessons learnt from projects and operational incidents at the national and local level should also be shared to cultivate an awareness of risk.

The Service will also work with representative bodies and staff to encourage the ethos of a learning organisation whereby employees are encouraged to share information which may either present a risk or a potential opportunity for the Service.

[1] Note: Appendix One provides further detail on the risk descriptors

Development, Training and Awareness

Through training and development, staff will:

- Have a basic awareness of risk
- Be able to identify and manage risk
- Understand the Service's approach to risk
- Conduct risk analysis

This is will be achieved through:

- Adequate resourcing
- The SLT having collective risk management training
- Specific Risk Management Training
- Risk Recording Introduction supplement by refresher training
- Individual Risk Surgeries for Risk Owners

In addition, risk will be a regular agenda item at the following:

- SLT
- Directorate Team Meetings
- Department Team Meetings
- Strategic Change Board
- Programme and Project Meetings

Senior Managers including programmes are required to ensure that their teams are aware of how their work is helping to mitigate risk through an understanding of the Services Risk Profile.

Risk Assurance Model

The Service utilises The Three Lines of Defence Model which clarifies essential roles and duties in the management of risk as follows, each of the three lines plays a part ECFRS wider governance framework.

First Line of Defence

Manages are responsible for the day to day aspects of risk and control management. This includes implementing risk management practises in their departments which includes identifying, assessing, and managing risk.

In addition, managers are responsible for highlighting any control issues.

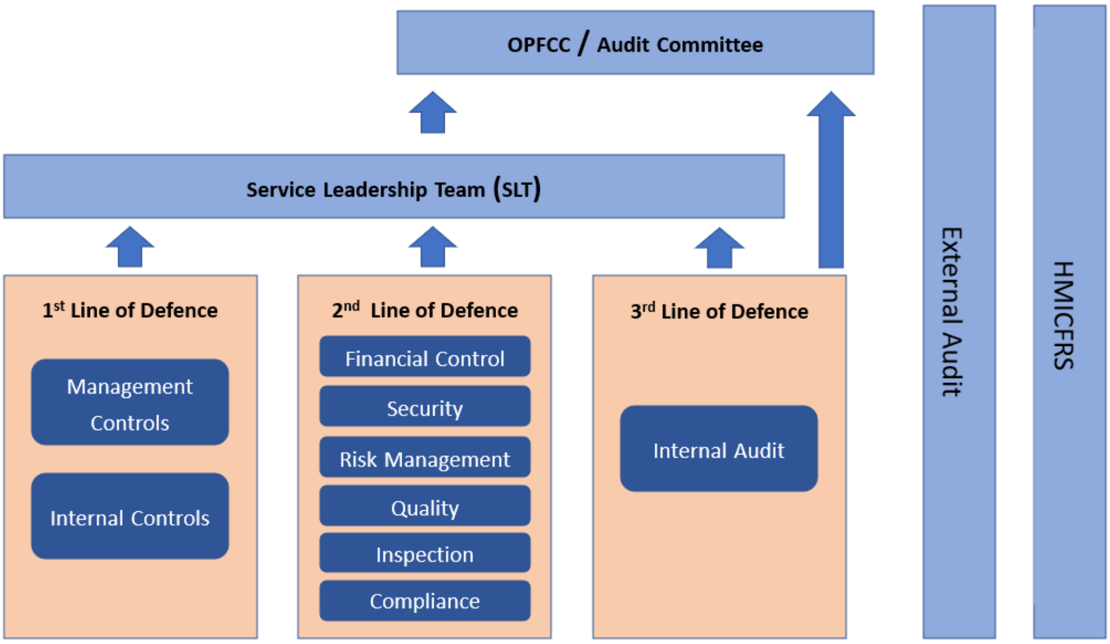
Second Line of Defence

The management functions in the second line of defence should operate with some independence from the normal management structure.

The second line should ensure that the first line is sufficiently designed to allow the above tasks to take place by designing frameworks, providing guidance, monitoring, and training to the first line.

Third Line of Defence

Internal Audit provide assurance with a degree of independence and objectivity that is not available to the second line.



Risk Maturity

Risk Maturity is used to assess the performance of risk management within the organisation, through the use of bench marking tools, we can determine how mature our risk management is against the set criteria and plan improvements. Utilising the assessment tool provided by ALARM (Appendix C), ECFRS sits within the 'happening' category.

Key areas of development to progress 'Working' are:

- Training in Risk Management Principles and Process to all levels of staff
- The ongoing development of Business Continuity Plans
- Early warning indictors should be developed with near misses and lessons learnt reported to the relevant Risk Owner
- Performance Management and Assurance is reported against relevant risks, and where a new or emerging risk has been identified through performance measures which is reported to the Risk Advisor
- Risk is built into the Business Planning Process
- Key risks to the delivery of Business Plan aims and objectives are identified and tracked through JCAD
- Partner and Supplier Risk is well managed
- Senior Managers taking the lead in applying Risk Management throughout the organisation

Definitions

BSI ISO 31000:2018

Risk – The effect of uncertainty on objectives

Risk Management – The coordinated activities to direct and control an organisation with regard to risk

Risk Source – An element, which alone or in combination, has the potential to give rise to risk

Trigger – An occurrence or change of a particular set of circumstances.

Consequence – Outcome of an event affecting objectives

Likelihood – The chance of something happening

Control – A measure that maintains and /or modifies risk

Risk Attitude – The opinion or chosen qualitative or quantitative value in comparison to the related loss or losses taken by individuals.

Risk Culture – The shared values, beliefs, knowledge, attitudes and understanding about risk; shared by a group of people with a common intended purpose, in particular the leadership and employees of an organisation.

Risk Perception – the judgement made by individuals with regard to risk both in terms of the potential impact of downside and the opportunities presented by the risk scenario.

Appendix A

Tools for assessing negative risk

Risk Matrix

Likelihood	Almost Certain	🟨	🟧	🟥	🟥	🟫
	Likely	🟨	🟧	🟧	🟥	🟥
	Possible	🟩	🟨	🟧	🟧	🟥
	Unlikely	🟩	🟨	🟨	🟧	🟧
	Rare	🟩	🟩	🟩	🟨	🟨
		Insignificant	Minor	Significant	Major	Critical
		Impact				

Likelihood Scale

Rare	Can reasonably be expected to occur but has only occurred a few times in this or similar organisation during the last 20 years
Unlikely	Can reasonably be expected to occur but has only occurred a few times in this or similar organisation during the last 15 years
Possible	Has occurred several times in the last 10 years or is likely to occur due to circumstances or has recently occurred in similar organisations
Likely	Has occurred several times in the last five years or is likely to occur due to circumstances or has recently occurred in similar organisations
Almost Certain	Has happened in this or a similar organisation in the last 12 months, and/or circumstances are such that the event could happen imminently without swift action

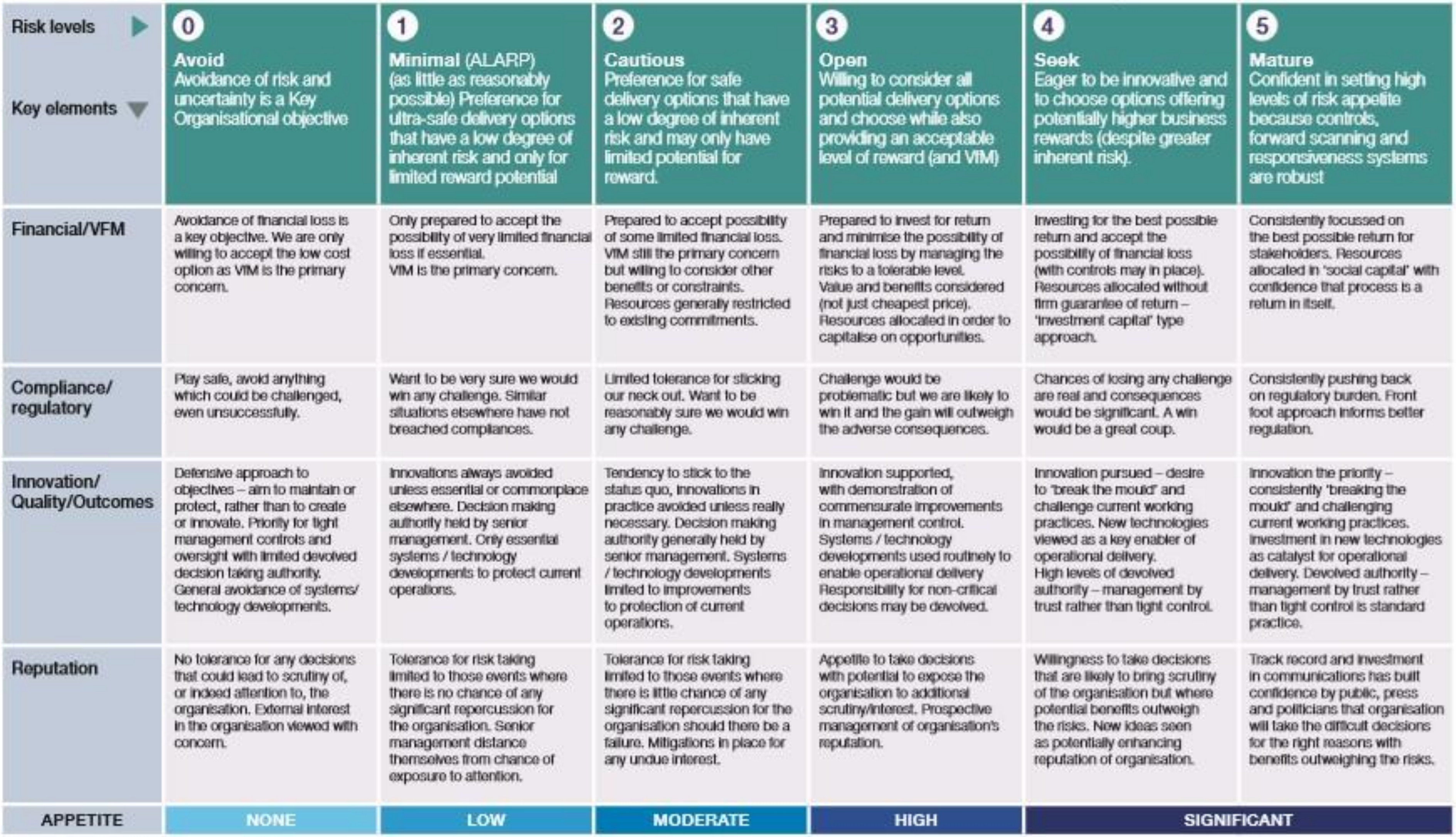
Impact Statement

	Public Value	People	Infrastructure	Reputation	Compliance
1. **Insignificant**	Solution not likely to require additional funds <25,000 Negative trend across specific KPI's, evidence of mitigating action in place. No impact on community work and partnerships	Minimal people issues raised. Delivery of people programmes on track.	Minor disruption to some non-critical services.	Little or no impact on public confidence. Some social media comments not picked up by local or national media. Good HMICFRS outcome with areas for improvement identified.	Minimal impact of breach of guidance/statutory duty. Minor cuts/abrasions requiring minimal treatment. Incidents involving an individual or a few data subjects that can be easily contacted and resolved.
2. **Minor**	Solution possible within amendments to current working practices. £26,000 - £100,000 Negative trend across several KPI's, evidence of mitigating action in place. Community Safety work is temporarily disrupted.	Minor levels of people issues. Delivery of people change programmes broadly on track.	Disruption to physical environment which would require some alternative working but no real impact on ability to perform.	Short term adverse local publicity Temporary reduction in public confidence Requires Improvement HMICFRS with areas for improvement identified in no more than two categories partnership work may be put on hold	Internal or external Audit criticism/failure to meet recommended best practice. 4 - 14 day lost time injury. Medical treatment required. A single incident involving less than 100 data subjects. no special category data is compromised.
3. **Significant**	Solution requires additional resources within organisation and potential over-spend. £101,000 – £500,000 Declining performance standards, with no evidence of mitigating action in place. Community activity is significantly disrupted.	Increasing levels of significant people issues. (e.g. regretted attrition and engagement) Significant delay or disturbance in delivery of people change programmes	Disruption which can be managed with existing BCP arrangements and is limited or short term in nature.	Sustained adverse local publicity and reduction in public confidence Requires Improvement HMICFRS with areas for improvement identified in multiple categories. Partnerships are not achieving expected benefits and savings.	Breach of statutory duty, legal/contractual obligation A major injury, including permanent disabling injury to an individual Multiple instances of data breech, no special category data is compromised

4. **Major**	Solution requires additional resources not within the current staff profile, inevitable overspend. Over £500,000 Performance targets not being achieved, with continuing negative trends, no evidence of mitigating action or actions in place having little or no impact on trend. Failure to meet primary objectives of the Fire and Rescue Plan. Community activity is not meeting legislative requirements.	High and increasing levels of complex people issues such as complex grievance and discipline. Major delay or disruption to delivery of people change programmes.	Disruption which is sustained or impacts multiple locations. Existing BCP arrangements may reach limits.	Short term national media coverage. Significant damage to reputation & public confidence. Inadequate HMICFRS, with area of improvements identified. We are unable to attract new partners or pursue collaboration opportunities.	Serious breach of statutory duty, legal/contractual obligation. Major injuries including permanent disabling injuries involving a number of people. A single incident in which special category data is compromised.
5. **Critical**	The additional resources required are not available within the Service's current financial position. The Impact of financial expenditure would not be covered by reserves, applicable for grant funding, and/or recoverable within the medium-term financial plan. Performance monitoring is no longer taking place and data is not be collated. Not meeting statuary duties or complying with the National Fire Service Framework Prevention and Protection work has not been completed for a period in excess of 3 months.	Unable to manage people issues or deliver people change programmes.	Disruption to critical services which would require emergency plans and leave the Service unable to attend or prevent incidents.	Loss of credibility and widespread & permanent reduction in public and partner confidence. Inadequate HMICFRS with immediate cause for concern identified. Extensive negative national media coverage over sustained period.	Serious breach of legal or contractual obligation. Single or multiple deaths involving any persons. Multiple or large data incident in which special category data is compromised.

Appendix B

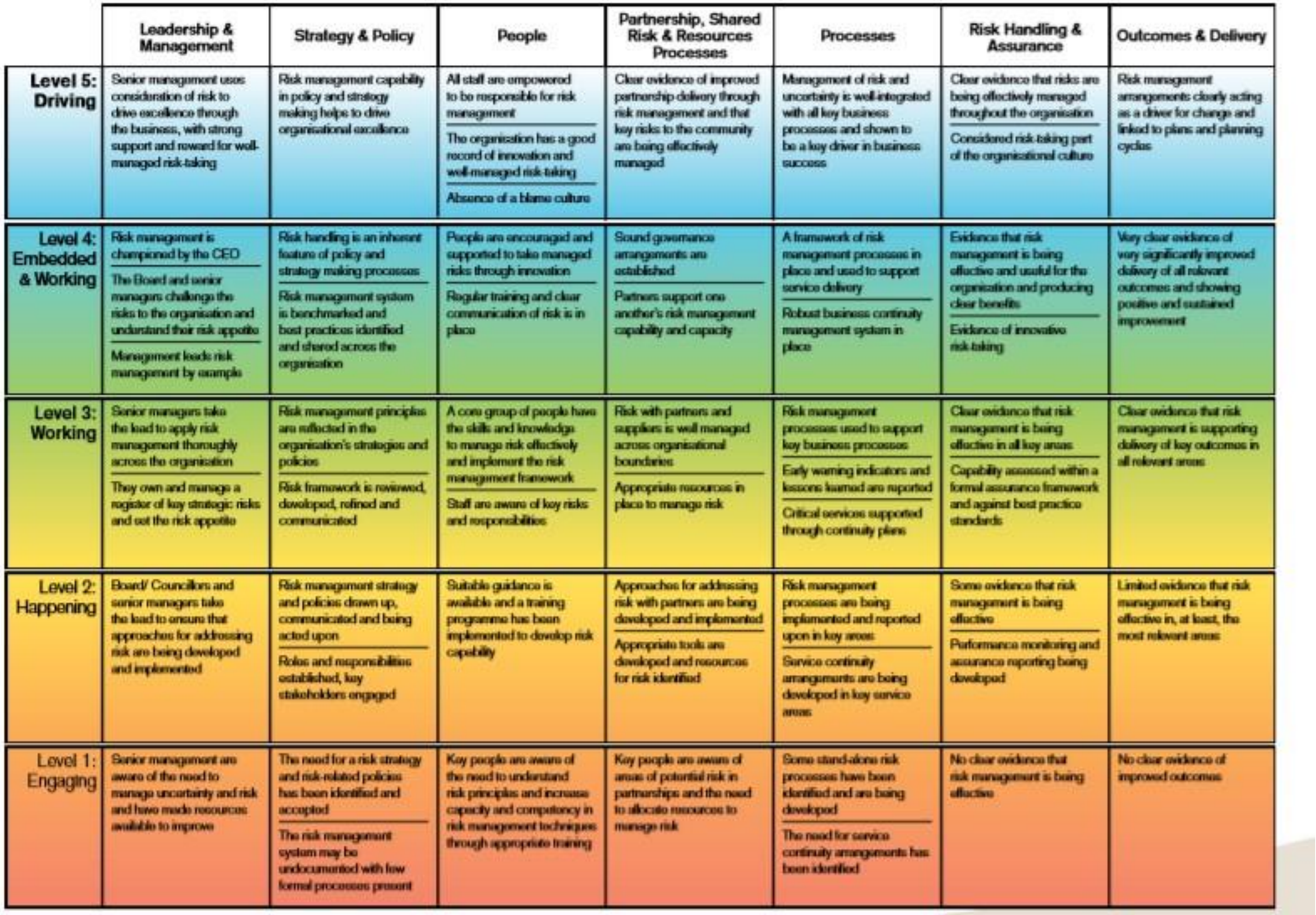
Risk Appetite Scale



Risk levels ▶ Key elements ▼	0 **Avoid** Avoidance of risk and uncertainty is a Key Organisational objective	1 **Minimal** (ALARP) (as little as reasonably possible) Preference for ultra-safe delivery options that have a low degree of inherent risk and only for limited reward potential	2 **Cautious** Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward.	3 **Open** Willing to consider all potential delivery options and choose while also providing an acceptable level of reward (and VfM)	4 **Seek** Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk).	5 **Mature** Confident in setting high levels of risk appetite because controls, forward scanning and responsiveness systems are robust
Financial/VFM	Avoidance of financial loss is a key objective. We are only willing to accept the low cost option as VfM is the primary concern.	Only prepared to accept the possibility of very limited financial loss if essential. VfM is the primary concern.	Prepared to accept possibility of some limited financial loss. VfM still the primary concern but willing to consider other benefits or constraints. Resources generally restricted to existing commitments.	Prepared to invest for return and minimise the possibility of financial loss by managing the risks to a tolerable level. Value and benefits considered (not just cheapest price). Resources allocated in order to capitalise on opportunities.	Investing for the best possible return and accept the possibility of financial loss (with controls may in place). Resources allocated without firm guarantee of return – 'investment capital' type approach.	Consistently focussed on the best possible return for stakeholders. Resources allocated in 'social capital' with confidence that process is a return in itself.
Compliance/ regulatory	Play safe, avoid anything which could be challenged, even unsuccessfully.	Want to be very sure we would win any challenge. Similar situations elsewhere have not breached compliances.	Limited tolerance for sticking our neck out. Want to be reasonably sure we would win any challenge.	Challenge would be problematic but we are likely to win it and the gain will outweigh the adverse consequences.	Chances of losing any challenge are real and consequences would be significant. A win would be a great coup.	Consistently pushing back on regulatory burden. Front foot approach informs better regulation.
Innovation/ Quality/Outcomes	Defensive approach to objectives – aim to maintain or protect, rather than to create or innovate. Priority for tight management controls and oversight with limited devolved decision taking authority. General avoidance of systems/ technology developments.	Innovations always avoided unless essential or commonplace elsewhere. Decision making authority held by senior management. Only essential systems / technology developments to protect current operations.	Tendency to stick to the status quo, innovations in practice avoided unless really necessary. Decision making authority generally held by senior management. Systems / technology developments limited to improvements to protection of current operations.	Innovation supported, with demonstration of commensurate improvements in management control. Systems / technology developments used routinely to enable operational delivery Responsibility for non-critical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. New technologies viewed as a key enabler of operational delivery. High levels of devolved authority – management by trust rather than tight control.	Innovation the priority – consistently 'breaking the mould' and challenging current working practices. Investment in new technologies as catalyst for operational delivery. Devolved authority – management by trust rather than tight control is standard practice.
Reputation	No tolerance for any decisions that could lead to scrutiny of, or indeed attention to, the organisation. External interest in the organisation viewed with concern.	Tolerance for risk taking limited to those events where there is no chance of any significant repercussion for the organisation. Senior management distance themselves from chance of exposure to attention.	Tolerance for risk taking limited to those events where there is little chance of any significant repercussion for the organisation should there be a failure. Mitigations in place for any undue interest.	Appetite to take decisions with potential to expose the organisation to additional scrutiny/interest. Prospective management of organisation's reputation.	Willingness to take decisions that are likely to bring scrutiny of the organisation but where potential benefits outweigh the risks. New ideas seen as potentially enhancing reputation of organisation.	Track record and investment in communications has built confidence by public, press and politicians that organisation will take the difficult decisions for the right reasons with benefits outweighing the risks.
APPETITE	NONE	LOW	MODERATE	HIGH	SIGNIFICANT	

Appendix C

Risk Maturity



	Leadership & Management	Strategy & Policy	People	Partnership, Shared Risk & Resources Processes	Processes	Risk Handling & Assurance	Outcomes & Delivery
Level 5: Driving	Senior management uses consideration of risk to drive excellence through the business, with strong support and reward for well-managed risk-taking	Risk management capability in policy and strategy making helps to drive organisational excellence	All staff are empowered to be responsible for risk management The organisation has a good record of innovation and well-managed risk-taking Absence of a blame culture	Clear evidence of improved partnership delivery through risk management and that key risks to the community are being effectively managed	Management of risk and uncertainty is well-integrated with all key business processes and shown to be a key driver in business success	Clear evidence that risks are being effectively managed throughout the organisation Considered risk-taking part of the organisational culture	Risk management arrangements clearly acting as a driver for change and linked to plans and planning cycles
Level 4: Embedded & Working	Risk management is championed by the CEO The Board and senior managers challenge the risks to the organisation and understand their risk appetite Management leads risk management by example	Risk handling is an inherent feature of policy and strategy making processes Risk management system is benchmarked and best practices identified and shared across the organisation	People are encouraged and supported to take managed risks through innovation Regular training and clear communication of risk is in place	Sound governance arrangements are established Partners support one another's risk management capability and capacity	A framework of risk management processes in place and used to support service delivery Robust business continuity management system in place	Evidence that risk management is being effective and useful for the organisation and producing clear benefits Evidence of innovative risk-taking	Very clear evidence of very significantly improved delivery of all relevant outcomes and showing positive and sustained improvement
Level 3: Working	Senior managers take the lead to apply risk management thoroughly across the organisation They own and manage a register of key strategic risks and set the risk appetite	Risk management principles are reflected in the organisation's strategies and policies Risk framework is reviewed, developed, refined and communicated	A core group of people have the skills and knowledge to manage risk effectively and implement the risk management framework Staff are aware of key risks and responsibilities	Risk with partners and suppliers is well managed across organisational boundaries Appropriate resources in place to manage risk	Risk management processes used to support key business processes Early warning indicators and lessons learned are reported Critical services supported through continuity plans	Clear evidence that risk management is being effective in all key areas Capability assessed within a formal assurance framework and against best practice standards	Clear evidence that risk management is supporting delivery of key outcomes in all relevant areas
Level 2: Happening	Board/ Councillors and senior managers take the lead to ensure that approaches for addressing risk are being developed and implemented	Risk management strategy and policies drawn up, communicated and being acted upon Roles and responsibilities established, key stakeholders engaged	Suitable guidance is available and a training programme has been implemented to develop risk capability	Approaches for addressing risk with partners are being developed and implemented Appropriate tools are developed and resources for risk identified	Risk management processes are being implemented and reported upon in key areas Service continuity arrangements are being developed in key service areas	Some evidence that risk management is being effective Performance monitoring and assurance reporting being developed	Limited evidence that risk management is being effective in, at least, the most relevant areas
Level 1: Engaging	Senior management are aware of the need to manage uncertainty and risk and have made resources available to improve	The need for a risk strategy and risk-related policies has been identified and accepted The risk management system may be undocumented with few formal processes present	Key people are aware of the need to understand risk principles and increase capacity and competency in risk management techniques through appropriate training	Key people are aware of areas of potential risk in partnerships and the need to allocate resources to manage risk	Some stand-alone risk processes have been identified and are being developed The need for service continuity arrangements has been identified	No clear evidence that risk management is being effective	No clear evidence of improved outcomes