10

Shropshire and Wrekin Fire and Rescue Authority
Standards, Audit and Performance Committee
10 July 2025

Corporate Risks 2025-2028 – process review and outcomes

Report of the Chief Fire Officer

For further information about this report please contact Simon Hardiman Chief Fire Officer, on 01743 260201 or Karen Gowreesunker, Assistant Chief Fire Officer Service Support, on 01743 26026.

1 Executive Summary

This report provides the Committee with an overview of the progress and outcomes that has been achieved in the identification of new Corporate Risks for the Authority. The report also details supporting process which will provide robust arrangements for monitoring, review and assurance. There is specific reference to how it is proposed the committee receive corporate risk updates.

2 Recommendations

Members are asked to:

a) note the report,
b) approve the new corporate risks,
c) agree the reporting of corporate risk into the committee at each of its meetings four times a year. Reporting of all risks at three of these meetings with one meeting enabling a deep dive into a risk, and
d) approve the amended policy to reflect the new process.

3 Background

The Authority and Service define in its risk management policy, risk as 'the process of identifying risks (both negative threats and positive opportunities), evaluating their potential consequence and determining the most effective methods of controlling them and/or responding to them. It is not an end in itself. Rather, risk management is the means of minimising the costs and disruption to the Service caused by undesired events.'

Corporate risk management is where those risks have the potential to cause serious disruption to the delivery of the Service's Community Risk Management Plan (CRMP) and Service Plan.

His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) inspection for the Service which took place in 2024, identified the management of corporate risk to be ineffective as part of the Best Use of Resources, Cause of Concern.

The inspection identified: '*ineffective processes, controls and internal governance arrangements in place to manage strategic risks. For example, the corporate risk register is ineffectively managed. The register contains a range of risks that have been included for a considerable time, but they don't have suitable controls in place. These include the security and resilience of the IT network and the lack of quality information and data to help managers make effective decisions.'*

The cause of concern identified the need to achieve the following as part of the Service's improvement plan:

'The corporate risk register is actively used to mitigate and manage known risks.'

On further review of the corporate risk register internally, it was clear that the risks cited were not all effectively managed or aligned to the Services CRMP and Service Plan.

4 Corporate Risk Review

The responsibility for managing corporate risk on a day-to-day basis sits with the Service Management Team (SMT). The accountability for overseeing these and seeking assurance sits with the Fire Authority.

A review of the corporate risk register and arrangements in place commenced in the last quarter of 2024. Initially identifying development needs across the SMT, as well as providing short information sources to build understanding of corporate risk and where this differs from other risks such as operational or project risks.

Several training sessions took place with both SMT and Fire Authority Members during January and February 2025 delivered by Zurich. These sessions were designed to provide a good basis of understanding around risk management and corporate risk itself. These training sessions will continue on a periodic basis and for new members a session will be planned in later this year.

Following these sessions there two corporate risk workshops were undertaken with SMT to define corporate risks that would be relevant to the CRMP and Service Plan for 2025 – 2028. These sessions also enabled SMT to map currently recorded risks to the new risks, as well as identify both triggers and control measures for the new corporate risks.

Throughout this review period, the Service and SMT continued to manage risks aligned to the existing risk register. This ensured ongoing management of risk areas, enabling Fire Authority assurance, as well as ensuring the detail within the risks recorded was up to date and any risk areas that were not relevant were removed. Therefore, cleansing and streamlining the information to ensure it was relevant and current, whilst the review took place.

Corporate risk reporting against the current recorded risks has continued into Performance and Risk Group (PRG) and into Standards Audit and Performance (SAP) Committee, quarterly.

An update of progress against this review has also been reported to members aligned to the above.

New Corporate Risks and Process July 2025 onwards

SMT have defined 7 corporate risks which present a realistic threat to the delivery of services to local communities as set out in the CRMP and strategic goals for 2025-2028.

The risks have been defined based on what could prevent the delivery of values for money services in creating a safe and strong community, economy and environment. In this we have considered:

- Effective and responsive services
- Sustainable economic growth
- Safe and resilient communities
- Financial independence

The new corporate risks are set out below and in more detail in Appendix A.

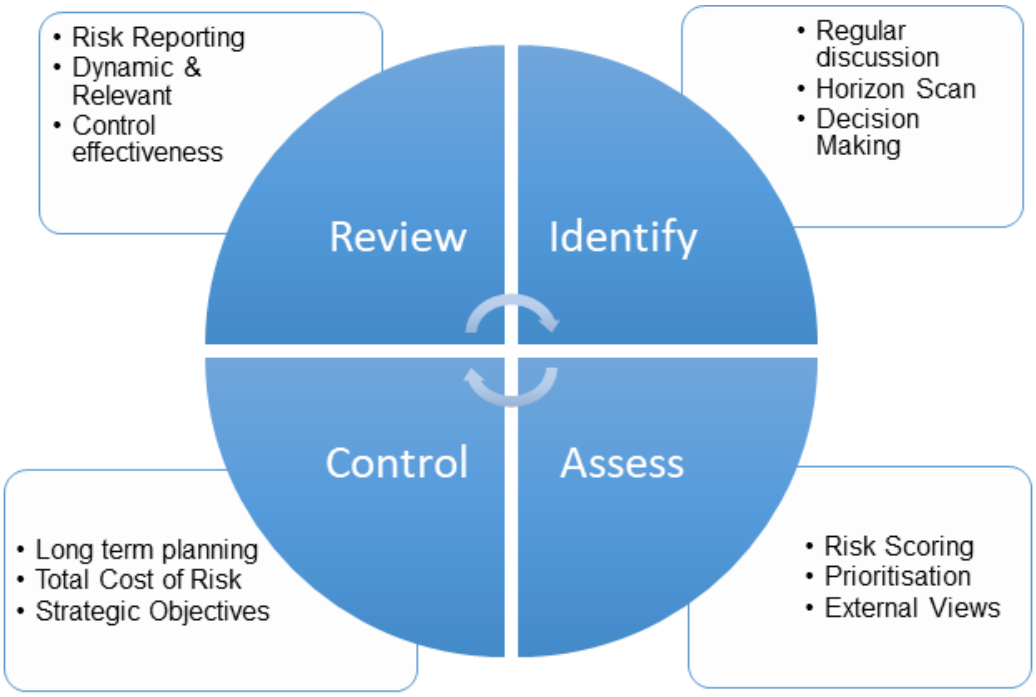
1. Staff Engagement
2. Political and Organisational Change
3. Cyber and Systems Resilience
4. Data and Digital Capability
5. Finance
6. Environment
7. Health and Safety

On approval of these risks at this SAP committee of the Fire Authority, these will form part of ongoing monitoring and review through SMT reporting and PRG.

These risks and their relevance to the delivery of the CRMP and strategic goals will be reviewed annually.

Process

Risk management requires identification of risk, assessment of the risk and how likely it is to occur as well as potential impact, control measures and ongoing review. As set out below:



SMT have already i***dentified, assessed and applied control measures*** against each of the 7 corporate risks cited in this report. The ongoing ***monitoring and review*** of corporate risk supports a current and dynamic approach to understanding the status of a risk, so that it can be mitigated and or managed in real time.

As previously set out SMT have responsibility for identifying and managing corporate risk and will own these risks. The Fire Authority are accountable as these risks are aligned to the achievement of our strategic goals. Members should seek to assure that risks are being effectively managed and or mitigated.

The following approach to review and monitoring will ensure corporate risks are appropriate and managed effectively. These will form part of the process and policy that has been developed.

Continuous monitoring: SMT will ensure continued monitoring and updating of corporate risks through the SMT environment. On a two-weekly basis SMT will review corporate risks, their triggers and control measures through an already established process which assesses Risks, Assumptions, Issues, Dependencies and Opportunities (RAIDO). This approach helps SMT to continuously horizon scan our internal and external environment.

Where changes are required to support the mitigation of a corporate risk there will be an audit trail through SMT discussion and/or decision items.

Monthly status update/review: It is expected that corporate risks will be updated monthly by SMT to identify any changes in status of the risks, the associated triggers and control measures. Ensuring this information and consideration of the risk is as current as possible. This is the responsibility of the SMT corporate risk owner.

Quarterly review and Assurance: SMT will assure corporate risks have been managed and mitigated appropriately through its quarterly Performance and Risk Group meetings.

Quarterly reporting into the Strategy Assurance Performance (SAP) committee will enable Fire Authority members to receive this same assurance and to actively scrutinise performance.

Appendix B provides a visual demonstration of this broad process.

Corporate risk is already a standing item at the committee meeting and the register is reviewed at each of its four (quarterly) meetings. It is proposed that all corporate risks are reviewed by the committee three times a year (September, April and July) with a deep dive into a corporate risk at least once a year (December). The deep dive risk will be as directed by the SAP or performance of a risk.

Risk Management Policy

The Risk Management policy has been revised to reflect the changes set out in this report, as well as the impacts and changes to other areas of day-to-day risk reporting within the Service. Appendix C sets out the proposed draft policy.

A more detailed approach to assessing the likelihood and impact of corporate risks using a 5x5 matrix also forms part of this policy review, to enable a more focused and meaningful approach to assessing our risks. This will provide more clarity regarding the rationale of a risk rating.

The policy proposed moves away from providing detailed instructions for the assessment of risk and offers the overall approach to risk management for the Service with a focus on corporate risk. Guidance for corporate risk owners will be developed outside of the policy, so that this can be used, adapted and changed as needed to support training and development.

Corporate Risk Register
A new corporate risk register has been created which will support the changes in both the risks and the way in which they are assessed and managed.

The format and approach to the register will be reviewed through the first 6 months of its application, to ensure that we continue to capture the necessary information and it enables effective reporting.

5 Conclusions

The outcomes of the corporate risk review has resulted in SMT proposing 7 new corporate risks to be agreed for implementation from June onwards. These risks, the process and policy that supports the ongoing monitoring review and assurance of these risks are set out in this report.

SAP Members are asked to approve these corporate risks and the recommendations set out in section 2.

6 Capacity

The management and reporting of corporate risks should not demand any more time from risk and control measure as this process already existed prior to this review. However, the HMICFRS report indicated that risks were not being managed effectively and therefore it is anticipated that the proper management of the corporate risk process will require additional capacity from SMT in the initial 6-9 months as the process embeds.

The Service and SMT should expect that the management of risks forms part of day-to-day planning and management of Service priorities.

7 Fire Alliance / Collaboration / Partnership Working

The management of corporate risk is very specific to the Service's CRMP and therefore it should not be expected that the accountability and responsibility of this would sit across a collaborative opportunity.

However, there is opportunity to manage and or mitigate corporate risks (depending on type) with the support of partners.

8 Financial Implications

There are no financial implications arising from this report.

It is however recognised that as the future Portfolio Management Office (PMO) develops a digital system which supports the management of projects and risks could extend to corporate risk.

9 Legal Comment

There are no legal implications arising from this report, however a robust approach to corporate risk will ensure the Service and Authority can maintain legal compliance aligned to its core role and CRMP.

10 HMICFRS Areas For Improvement, Cause of Concern, External Audit Recommendations

As set out in the background to this report, the HMICFRS inspection for the Service which took place in 2024, identified the management of corporate risk to be ineffective as part of the Best Use of Resources, Cause of Concern.

The cause of concern identified the need to achieve the following as part of the Service's improvement plan:

'The corporate risk register is actively used to mitigate and manage known risks.'

This review that is set out on this report including recommendations seeks to address the findings of the inspection process and achieve the above outcome for corporate risk.

11 Communications

Corporate risk management is a responsibility of the SMT and Fire Authority. There has been ongoing communication and engagement with these two stakeholders throughout the review process, ensuring SMT have been central to the development of the new corporate risks.

On approval of the new corporate risks and policy by SAP committee the Service will communicate the completion of this work with stakeholders and the HMICFRS Service Liaison Lead.

A re inspection process for the cause of concern issued will take place on the

21st July 2025. This process will support assure around the sufficiency of the changes recommended in this report.

12 Community Safety

The effective management of corporate risk will ensure the Service and Authority is able to deliver services effectively to its communities.

13 Environmental

The effective management of corporate risk will ensure the Service and Authority is able to mitigate environmental impacts aligned to its CRMP.

14 Equality Impact Assessment

An initial e-EQIA has been completed.

15 Health and Safety

A corporate risk proposed in the new suite of risks 'Health and Safety'. This has been incorporated in the new risks due to a lack of confidence in the robustness of our control measures.

The Service has focused the investment of resources into this area to support risk mitigation over the next 12 months here are no health and safety impacts arising from this report.

16 Fire Standard Core Code of Ethics and Human Rights (including Data Protection)

The embedding of the recommendations set out in this report support the Service and Authority in meeting the Internal Governance and Assurance Fire Standard.

This seeks to ensure:
A fire and rescue service whose communities have confidence in its ability to deliver its core objectives, identifies its strategic risks and publishes these in its community risk management plan. These objectives are clear, realistic and understood by all within the service, which is accountable to the relevant governing body.

Through this - identify and coordinate the management of risks associated with delivering its activities.

17 Training

There are no training impacts arising from this report. Training has been implemented as part of the review process and will continue on a periodic basis and for new members a session will be planned in later this year.

18 Appendices

Appendix A - New Corporate Risk Register entries
Appendix B - Overview monitoring, review and assurance process
Appendix C - Revised draft Risk Management policy

19 Background Papers

There are no background papers associated with this report

Appendix A - New Corporate Risk Register entries

Risk Number	Risk Title	Risk Description	Risk Triggers
CR1	Staff Engagement	There is a risk that low staff engagement and dissatisfaction within the workforce could impact operational effectiveness and service delivery. Changes to terms and conditions, including pay, pensions and shift patterns may lead to discontent, reduced morale and potential industrial action. If communication and engagement strategies are ineffective, staff may feel undervalued, leading to a decline in trust and employee relations between leadership and frontline personnel. This could result in increased absenteeism, lack of progression, higher staff turnover, resistance to change and reduced commitment to organisational objectives. A disengaged workforce may also impact public confidence in the service, effective recruitment and retention efforts. This could result in an inability for the Fire Authority to delivery its services to the public in line with its CRMP and a risk of not complying with Equality and Diversity legislation.	1. Changes to pay, pensions or working conditions and work practices without effective consultation 2. Perceived lack of transparency in decision-making 3. Insufficient communication on organisational changes and strategic direction 4. Failure to recognise and reward staff contributions 5. Increased workloads and operational pressures affecting wellbeing 6. Lack of culture transformation progress 7. External factors such as amendments to legislation resulting in mandatory changes outside of the Services control
CR2	Political and Organisational Change	There is a risk that political decision, local government reorganisation (LGR), or changes in governance structures could impact the fire service's strategic direction, funding, and operational effectiveness. Mergers, changes in oversight bodies, or increased	1. LGR / mergers impacting governance and funding 2. Political changes at national or local levels shifting fire & rescue service priorities

		diversification of responsibilities (e.g., broader community safety roles) may lead to a dilution of core fire and rescue priorities, creating uncertainty in long-term planning and resource allocation. The loss of funding or shifts in financial priorities could reduce service capacity, impact investment in training and equipment and place additional pressure on operational delivery. If decision-making is influenced by political priorities rather than risk-based assessments, it could result in misaligned strategies, inefficiencies, and a lack of clarity in leadership direction. Additionally, the pace of change – if too rapid or uncoordinated – could create disruption, staff disengagement, and resistance to new structures or ways of working and industrial action. This could result in an inability for the Fire Authority to delivery its services to the public in line with its CRMP.	3. Increased expectations to take on additional responsibilities outside of core fire and rescue duties 4. Policy decisions affecting funding models, workforce structure or performance targets 5. Lack of clear strategic direction or competing priorities from multiple stakeholders
CR3	Cyber and Systems Resilience	There is a risk that a cyber-attack, system failure, or data breach could compromise the fire service's ability to respond effectively to emergencies, protect sensitive information and ensure firefighter and public safety. A loss of access to critical IT systems – such as emergency dispatch, command and control, and mobile data terminals – could delay response times, disrupt incident coordination, and put lives at risk. A data breach could expose personal, operational or confidential information, leading to reputational damage, regulatory penalties, and loss of public trust. If	1. Targeted cyberattacks (e.g. ransomware, phishing, denial-of-service attacks) 2. Insider threats/malicious intent or accidental data breaches due to human error due to time and capacity caused by workloads. 3. Outdated or unpatched software and weak cybersecurity protocols 4. Failure to back up critical data and implement robust disaster recovery plans

		systems are not adequately protected, malicious actors may exploit vulnerabilities, resulting in operational paralysis and increased financial costs for recovery. This could result in an inability for the Fire Authority to delivery its services to the public in line with its CRMP.	5. Inadequate staff awareness and training on cyber risks and single points of failure
CR4	Data and Digital Capability	There is a risk that inadequate access to accurate, timely, and well-managed data could impact strategic decision-making, operational effectiveness, and compliance with data protection regulations. Without the right data, the fire service may struggle to assess risk accurately, allocate resources efficiently, and drive evidence based decision-making. A lack of investment in modern digital systems and data analytics tools may hinder innovation, slow response times, and reduce overall service effectiveness. Additionally, if the workforce lacks the necessary digital skills or capacity to manage and interpret data effectively, this could lead to inefficiencies, poor decision-making, and missed opportunities for service improvement. The rapid pace of technology change, coupled with evolving regulatory requirements such as GDPR, presents further challenges in ensuring data security, system integration, and ongoing compliance. Failure to address these issues could result in optional disruptions, financial losses, reputational damage and risks to firefighter and public safety. This could result in an inability for the Fire Authority to delivery its services to the public in line with its CRMP.	1. Inconsistent or incomplete data collection and analysis. 2. Outdated IT systems and lack of investment in digital transformation 3. Limited staff capacity or expertise in data and management analytics and single points of failure 4. Failure to comply with GDPR and other data protection regulations 5. Insufficient integration between digital systems and operational processes 6. Rapid technological advancements outpacing organisational readiness

CR5	Finance	There is a risk that the fire service may face challenges in delivering a cost-effective, high quality service to the community due to financial pressures, resource constraints, and increasing demand. Ensuring value for money requires efficient use of personnel, equipment, and funding while maintaining high operational standards and public safety. Budget reductions, rising costs and the need to invest in new technologies and infrastructure may create financial strain, leading to difficult decisions around service provision. Inefficiencies in resource allocation, procurement, or workforce management could result in wasted expenditure, reduced service capacity, or failure to meet public expectation. If financial and operational planning is not effectively aligned, there is a risk that strategic priorities may be compromised, impacting emergency response times, firefighter safety and long-term sustainability. This could result in an inability for the Fire Authority to delivery its services to the public in line with its CRMP.	1. Budget cuts / funding uncertainty – reductions in government or local authority funding affecting service delivery. 2. Resource Allocation – poor workforce planning, underutilised assets, or misalignment between demand and resource availability. 3. Rising costs – inflation, pay awards, increased fuel and equipment costs, higher training and compliance expenses. 4. Procurement – Ineffective contract management, failure to leverage economies of scale, delays securing essential equipment. 5. Workforce – Overtime costs, recruitment and retention issues, skill shortages affective efficiency. 6. Changing risk landscape – increase service demand due to climate change, population growth, or emerging risks without proportional funding adjustments. 7. Failure to identify efficiencies
CR6	Environment	There is a risk that the fire service may face barriers in achieving its goal to reduce its carbon footprint and overall environmental impact. Transitioning to more sustainable operations requires investment in green technologies, infrastructure upgrades and changes to fleet, equipment, and working practices. Constraints such as budget limitations, supply chain challenges,	1. Finance – limited budgets available for green investments, such as electric vehicle fleet or energy-efficient buildings. 2. Technology – Lack of suitable low-carbon alternatives for operational equipment and response vehicles.

		and regulatory complexities may slow progress. Additionally, balancing sustainable goals with operational effectiveness – such as ensuring electric or alternative-fuel fire appliances meet emergency response requirements-presents logistical and technical challenges. Failure to meet environmental targets could lead to reputational damage, missed government sustainability commitments, increased operational costs due to inefficient resource use, and potential non-compliance with environment regulations. The pace of change in green technologies may also create challenges in procurement, workforce adaptation, and interoperability with existing infrastructure.	3. Infrastructure readiness – Inadequate charging networks, station upgrades, or supply chain delays for sustainable equipment. 4. Operational – concerns over reliability, performance, and resilience of new green technologies in emergency scenarios. 5. Regulatory and policy – shifting environmental policies or stricter government targets require faster adaptation. 6. Workforce – Staff concerns over changes to operational procedures, training needs, or the effectiveness of new sustainable technologies. 7. Strategic – Lack of clarity of our priorities aligned to Service goals and CRMP
CR7	Health and Safety	The Fire Authority fails to meet statutory obligations under the Health and Safety at Work etc. Act 1974, Environment Act 1995, and Fire and Rescue Services Act 2004, due to gaps in policy implementation, ineffective governance, or a weak assurance framework. This could lead to criminal prosecution, civil litigation, regulatory enforcement, and reputational damage. There is a risk of significant physical harm to staff, contractors, or members of the public arising from systemic weaknesses in the design, management, or	1. A serious accident or near-miss prompts investigation (e.g. HSE notified under RIDDOR) 2. Receipt of an external complaint or whistleblowing report alleging unsafe conditions or malpractice 3. Regulatory body inspection (e.g. HSE, Environment Agency) announced or unannounced 4. Discovery of environmental contamination (e.g. fuel/oil leak, hazardous waste

		oversight of safe working practices, training environments, or operational response. This includes the cumulative impact of inadequate infrastructure, exposure to hazardous environments, or failure to maintain a strong safety culture across the organisation.	mismanagement) 5. A critical media exposé or FOI request highlights systemic safety issues 6. A policy or legislative change (e.g. new duty under environmental law) that the Authority has not yet implemented 7. High-profile case elsewhere (e.g. another FRS prosecuted under H&S law) leading to scrutiny of internal practice 8. Legal challenge or pre-action protocol letter from staff or third party 9. A serious injury or fatality linked to operational activity, training, or estate conditions 10. Emergence of a chronic health risk affecting multiple staff (e.g. contamination-related illness, respiratory issues) 11. A pattern of injuries or near-misses indicating systemic failure (not isolated incidents) 12. External alert or regulation identifying a significant threat to health and safety (e.g. new contaminant guidance) 13. Sudden failure of critical infrastructure or

			systems affecting operational safety 14. A judicial inquest, coronial report, or HSE intervention relating to a harm event within the service 15. Disproportionate impact on staff groups, e.g. linked to role, demographic, or location, raising equality concerns in safe systems of work

Appendix B – overview monitoring, review and assurance process