Joint Audit & Scrutiny Committee (JARC) – Strategic Risk Management Update
Date: 26th November 2025
Prepared by: Victoria Adams, Strategic Risk Manager
**For: Joint Audit & Scrutiny Committee**

1. Purpose

To provide assurance on the effectiveness of the Service's strategic risk management framework, including:

Current risk profile and recent changes.
Benchmarking against the National Risk Register and other UK Fire & Rescue Services.
Integration of horizon scanning using the Futures Toolkit.
Alignment with the Commissioner's Fire & Rescue Plan priorities.
Update on risk appetite and tolerance statements.

2. Strategic Context

The Service's risk management approach underpins delivery of the Commissioner's Fire & Rescue Plan, ensuring:

- Prevention and Protection: Risks relating to community safety and safeguarding are actively managed.
- Response and Resilience: Operational risks such as mobilisation system failures and workforce resilience are prioritised.
- People and Culture: Risks linked to wellbeing, inclusion, and EDI align with the Plan's commitment to a positive organisational culture.
- Value for Money: Financial sustainability risks are monitored to support efficient use of public funds.
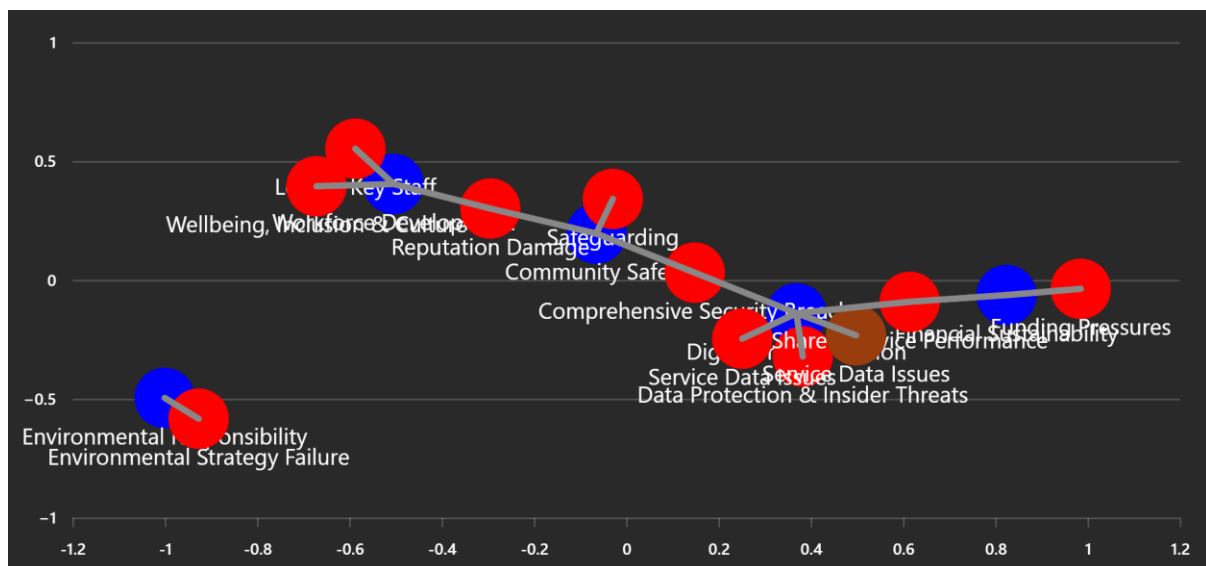
Blue nodes = Fire Plan Objectives
Red nodes = Strategic Risks
Edges = Links between risks and objectives.

3. Current Strategic Risk Profile

New Risk Added:

Failure of ICCS CAD Project (CORP0020) – residual rating 16 (Critical) due to potential disruption to mobilisation and operational efficiency.

Increased Ratings:

CORP0007 – Loss of Key Staff: Increased from 12 (Moderate) to 16 (Critical) due to concerns over the fair funding review and potential impact on morale and attrition.
CORP0008 – Financial Sustainability: Remains high at 16 (Major), previously 12, reflecting ongoing funding uncertainty and reliance on council tax increases.
CORP0013 – Data Protection & Insider Threats: Increased from 6 (Moderate) to 9 (Moderate) following incidents of unauthorised sharing of internal data.
CORP0015 – Damage to Public Trust: Increased from 9 (Moderate) to 12 (Major) due to insider threats and negative press coverage.
CORP0016 – Comprehensive Security Breach: Increased from 9 (Moderate) to 12 (Major) following recent cyber-threats and insider sabotage concerns.


Strategic Risk Rating Changes
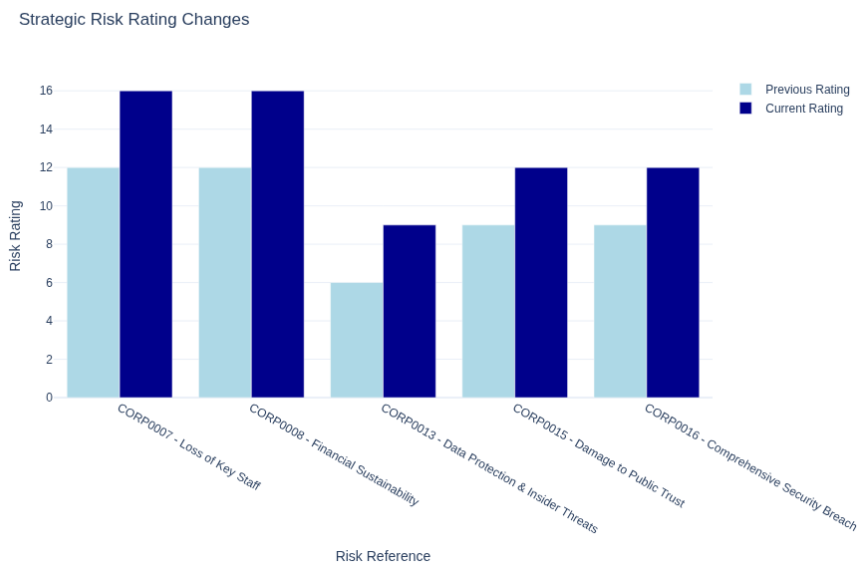
4. Benchmarking & Assurance

4.1 Control Assurance

The latest review of strategic risk controls assessed 99 controls across the Service's highest-level risks. The overall assurance position is rated as Partially Assured, reflecting that while 41 controls are fully embedded and effective, a significant proportion remain partially effective (22) or in progress (35), with 7 controls planned but not yet started. This indicates that although strong foundations exist, further work is required to close assurance gaps, particularly in high-risk areas such as cybersecurity, safeguarding, and environmental compliance. Key recommendations include prioritising completion of work-in-progress controls, enhancing partially effective measures, and

accelerating planned actions. Continuous monitoring and reporting to the Strategic Risk Board will ensure visibility, accountability, and improvement in assurance coverage.
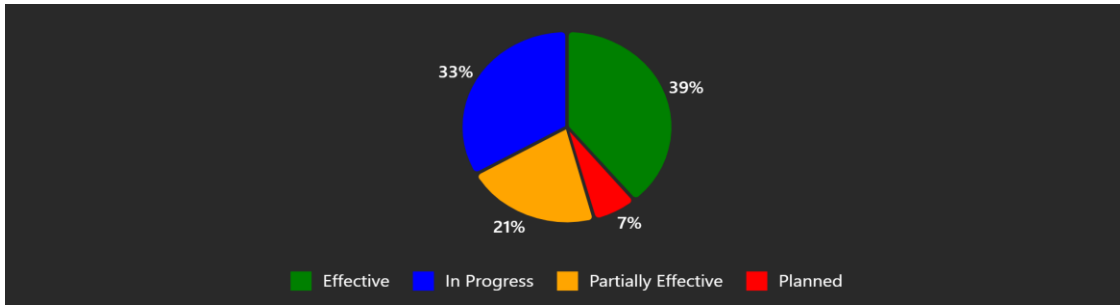
4.2 National Risk Register Alignment

Our Strategic Risk Register is deliberately aligned with the UK Government's National Risk Register (NRR) to ensure that local risk management reflects national resilience priorities. This alignment provides a consistent framework for identifying and mitigating risks that could impact both Staffordshire and the wider UK. By mapping our strategic risks, such as cybersecurity threats, environmental hazards, financial sustainability, and workforce resilience against NRR categories, we ensure that our planning is informed by the latest government intelligence and sector wide assessments. This approach strengthens our ability to anticipate emerging threats, comply with statutory obligations under the Civil Contingencies Act, and maintain interoperability with other agencies during major incidents. It also supports transparency and assurance for stakeholders by demonstrating that our risk profile is benchmarked against nationally recognised threats.

The diagram below illustrates how our strategic risks are linked to the NRR. Risks such as cybersecurity, pandemic resilience, and climate change impacts mirror UK Government priorities. Our high rated risks (e.g., financial sustainability, security breaches) align with national concerns around critical infrastructure resilience and public confidence.

4.3 Sector Benchmarking

NFCC and HMICFRS reviews confirm similar challenges across the sector:

Funding uncertainty and reliance on local precept increases.
Shared service performance risks due to complex governance arrangements.
Cultural and EDI risks remain a sector-wide focus following HMICFRS inspections.

Workforce Resilience: Staffordshire scores higher (16 vs 14) due to succession planning and industrial action risks.
Financial Sustainability: Slightly above sector average (16 vs 15) driven by funding volatility and reliance on precept increases.
Cybersecurity: Elevated (12 vs 10) reflecting insider threats and Citrix vulnerabilities.
Public Confidence: Higher (12 vs 10) due to reputational risks from data breaches and negative press.
Shared Services: Significantly higher (16 vs 14) due to governance and performance concerns with partner arrangements.

Staffordshire Fire and Rescue consistently scores above sector averages, indicating heightened exposure in workforce, financial, and governance related risks.

Benchmarking Strategic Risk Ratings: Staffordshire vs UK FRS Sector Average
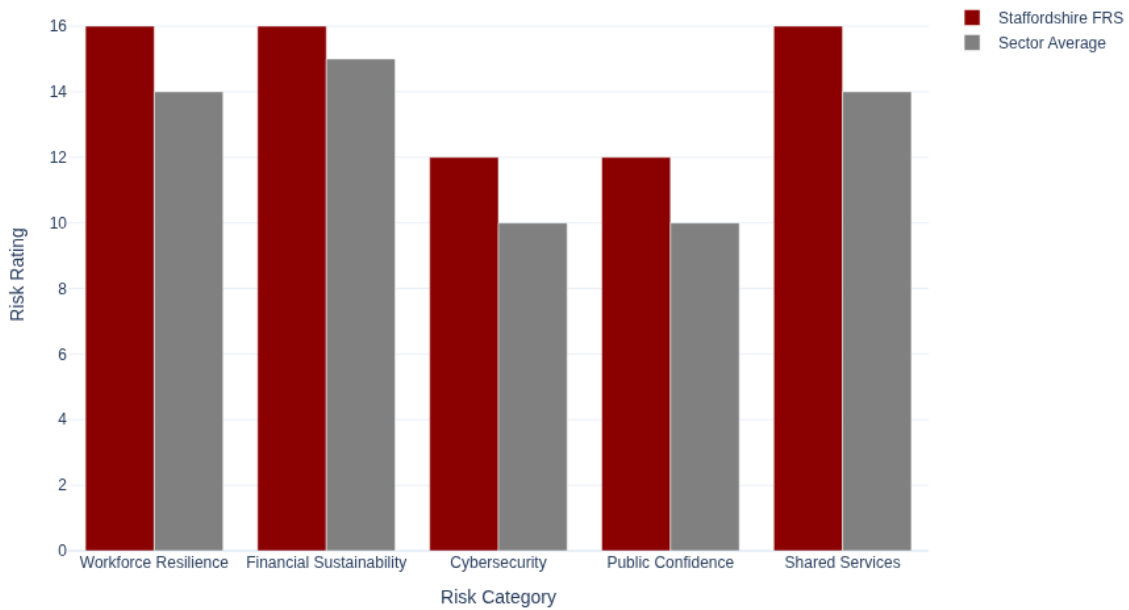
Our participation in the NFCC Risk Management Group has highlighted the diversity of approaches to strategic risk scoring and governance across UK Fire & Rescue Services. During recent discussions, it was evident that differences in risk appetite, tolerance levels, and assessment methodologies can significantly influence residual ratings.

Some services adopt a more conservative stance, prioritising precautionary scoring to drive robust mitigation, while others apply a pragmatic approach based on operational capacity and resource constraints. Environmental factors such as regional demographics, industrial risk profiles, and socio-

economic conditions also contribute to variations. These conversations reinforce the importance of benchmarking and sharing best practice, ensuring that while local context is respected, our framework remains aligned with national standards and sector expectations.

Factors Influencing Benchmarking of Risks

Risk Appetite and Tolerance

A more cautious approach may led to higher ratings

Subjectivity in Scoring

Judgment-based assessments can vary between organizations

Environmental Factors

Regional challenges or unique circumstances may justify higher scores

Emerging Threat Sensitivity

Anticipating future impacts may result in conservative estimates

Our main drivers are.

Risk Appetite and Tolerance

On speaking to my peers on the NFCC Risk Management group I would suggest that we may have a lower tolerance for uncertainty or a more cautious risk appetite, we may deliberately score risks higher to ensure stronger mitigation and governance.

Conversely, services with a higher tolerance may accept more residual risk, resulting in lower ratings for similar threats.

Subjectivity in Scoring

Risk assessment involves judgment based scoring, which can vary between organisations. Differences in interpretation of likelihood and impact scales, or how controls are factored into residual ratings, can lead to higher scores even for similar risk profiles.

Environmental and Regional Factors

Staffordshire may face unique local challenges that amplify certain risks:

Geography and demographics (e.g., rural areas increasing response time complexity).
Industrial profile (e.g., presence of high-risk sites or critical infrastructure).
Socio-economic conditions influencing workforce resilience and community risk.

These contextual factors often justify higher ratings compared to urban or differently resourced services.

Emerging Threat Sensitivity

Our proactive approach to horizon scanning and scenario planning means we may anticipate future impacts earlier, leading to higher ratings for risks like cybersecurity or climate resilience.

5. Futures Toolkit & Horizon Scanning

We are beginning to embed the Futures Toolkit into our strategic risk management process to strengthen long-term resilience. The toolkit is applied by integrating horizon scanning outputs with scenario planning techniques, enabling us to explore plausible futures and stress-test our risk controls. For example, insights from quarterly horizon scanning, such as cyber-threat trends, climate impacts, and societal shifts, are used to develop scenarios that challenge assumptions in our Strategic Risk Register. These scenarios inform decisions on risk appetite, resource allocation, and contingency planning. By adopting this structured approach, we aim to move beyond reactive risk management toward a proactive model that anticipates emerging threats and opportunities. This methodology is already proven in other Fire & Rescue Services, where it has enhanced planning for climate resilience, workforce sustainability, and digital transformation.

Integrating the Futures Toolkit
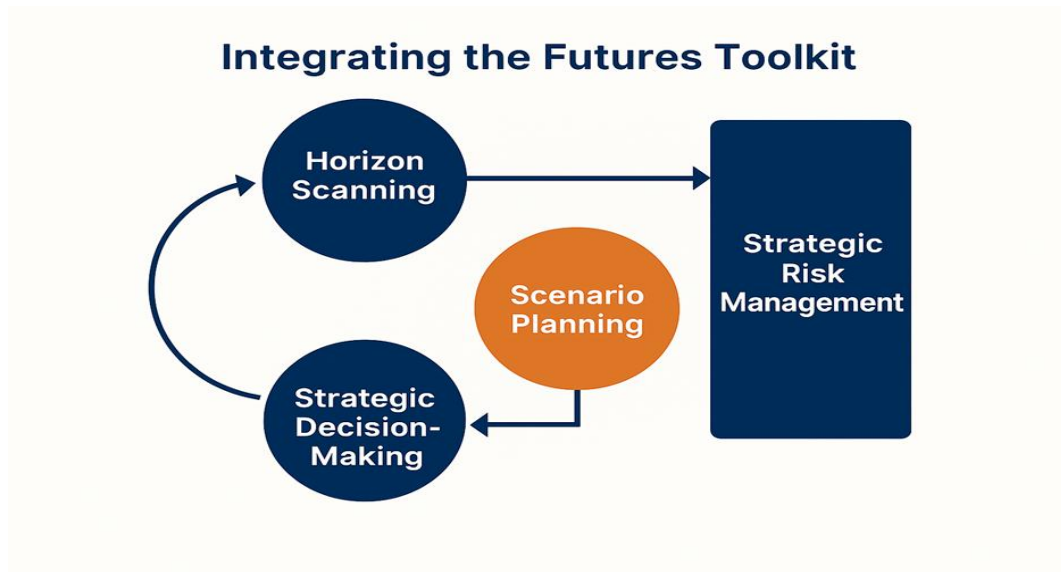
Applied scenario planning and trend analysis to identify emerging risks:

Digital transformation vulnerabilities (e.g., ICCS CAD integration issues).
Climate-related operational pressures (wildfire response, extreme weather).
Societal shifts impacting recruitment and workforce resilience.

These insights inform long term planning and support delivery of the Commissioner's Fire Plan objectives.

Horizon Scanning → Identifies emerging trends and weak signals.
Scenario Planning → Builds plausible futures to stress-test strategies.
Strategic Decision-Making → Informs choices aligned with long term resilience.

All feeding into Strategic Risk Management.

5.1 Quarterly Horizon Scanning

As part of our strategic risk management cycle, we conduct horizon scanning every quarter to identify emerging threats and opportunities. This process draws on national intelligence sources such as the National Risk Register, NFCC guidance, and government security alerts, as well as local

intelligence from operational data, partner agencies, and community feedback. Key areas of focus include:

Cybersecurity threats (e.g., ransomware attacks, vulnerabilities like Citrix exploits).
Environmental issues (e.g., climate change impacts, extreme weather events, wildfire risk).
Societal trends (e.g., workforce demographics, industrial action risks).
Technological developments (e.g., digital transformation challenges, CAD system resilience).

The insights from horizon scanning feed directly into our Strategic Risk Register updates, ensuring that our risk profile remains aligned with both national priorities and local operational realities.

5.2 Scenario Planning – Established Foundations

Our approach to scenario planning began several years ago as part of financial planning exercises and the Operational Research in Health (ORH) report, which provided evidence-based modelling of service demand and resource allocation. These early activities laid the groundwork for structured futures thinking by:

- Testing financial resilience under different funding scenarios, including variations in government settlements and council tax precepts.
- Exploring operational capacity models through ORH analysis to understand the impact of demographic changes, risk profiles, and incident demand.
- Conducting business continuity exercises to validate our ability to maintain critical services during disruptive events such as IT outages, industrial action, and severe weather.

This experience has positioned the Service to integrate scenario planning into the Futures Toolkit process, enabling us to stress test strategic decisions against multiple plausible futures. By combining financial modelling, operational research, and continuity testing, we are building a robust framework that supports long term resilience and adaptability.

6. Risk Appetite & Tolerance

At the last review (6th November), draft revised risk appetite and tolerance statements were considered. These will be taken to the next Principal Officers' meeting for in-depth discussion and formal approval.

7. Assurance for Audit & Scrutiny

7.1 Risk Management Framework

The risk management framework is embedded and regularly reviewed. The next review is due to take place in January 2026 however the Framework has been published in line with the CRMP and the Commissioners Fire Plan to run until 2028. I anticipate that there will be some changes to include new appetite and tolerance statements, the Futures Toolkit and governance and reporting.

7.2 Controls and High Rated Risks

Controls for high rated risks are monitored and reported to the Strategic Risk Board.

Independent scrutiny is welcomed to ensure transparency and alignment with statutory obligations.

7.3 Recommendations

Note the updated Strategic Risk Register (Version 87).
Endorse continued benchmarking and horizon scanning activities.
Support integration of Futures Toolkit outputs into strategic planning.
Acknowledge progress on risk appetite and tolerance statements.

Appendices

Appendix A: Strategic Risk Register (Version 87)