

## Corporate Risk Management Annual Report 2025/26

### Report of the Chief Fire Officer

For further information about this report please contact Simon Hardiman, Chief Fire Officer, on 01743 260201 or Marc Millward, Assistant Chief Fire Officer (Corporate Services), on 01743 260225.

### 1 Executive Summary

This report informs Members of the corporate risk management work that has been undertaken during the previous twelve months.

### 2 Recommendations

The Fire Authority is asked to

- a) consider and comment on the contents of the report; and
- b) delegate agreement of the proposed changes to the Corporate Risk Management Policy to the Audit and Standards Committee.

### 3 Background

The Performance and Risk Group (PRG) is responsible for ongoing monitoring of the Service's corporate risk management activity. The Audit and Standards Committee also receive regular corporate risk management reports.

Risk management best practice also recommends that the full Fire Authority receives a summary report at least once a year.

During 2025, the Service reviewed how corporate risks were recorded and managed. This included removing the Risk Management Group (RMG) and realigning risk reporting to other forums. The Service Management Team approved the revised approach in early June 2025, and Authority reporting was subsequently aligned to the updated corporate risks. The revised arrangements were reported to the Authority's Standards, Audit and Performance Committee in June 2025.

In early 2026, as part of good governance and good risk management practices, the Service carried out a review of the corporate risk process in conjunction with Internal Audit services. The outcomes of these reviews have helped to develop, embed and sustained strong risk management processes.

## **4 Risk Management Progress**

This section includes information about all events that have led to the current status with the Authority's corporate risk management system.

### **April 2025**

The Standards, Audit, and Performance Committee received a Corporate Risk Management Summary update. The update explained that the Service had responded proactively to His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) Cause of Concern, had recognised weaknesses in the previous corporate risk arrangements, and were undertaking a fundamental reset of the corporate risk management arrangements.

### **May 2025**

Service Managers attended a Corporate Risk workshop to further review and refine the new suite of corporate risks and assign risk owners.

### **June 2025**

The Fire Authority received the Corporate Risk Management Annual Report 2024/25.

The report confirmed that corporate risks were being actively monitored (12 current risks) and that improvements to risk management processes were underway in response to a HMICFRS Cause of Concern, with a stronger focus on using the risk register to manage and mitigate risk effectively.

### **July 2025**

The Standards, Audit, and Performance Committee received a Corporate Risk Management Summary update.

The update confirmed that all identified risks have been successfully mapped to the new framework, with no changes to existing open risks since the previous report and one exempt risk reduced in rating.

The report also set out a significant shift in approach, with the removal of "exempt risks" and a commitment to full transparency, meaning all risks will be reported in public sessions of Authority and Committee meetings.

The Committee noted the report and approved the closure of the current risk register and risk management approach, enabling transition to the revised, more open and integrated model.

### **September 2025**

The Standards, Audit, and Performance Committee received a Corporate Risk Management Summary update.

The update highlighted that while overall progress was on track, three risks remain outside tolerance due to early-stage mitigations, with ongoing pressures in areas such as workforce capacity, cybersecurity, and financial resilience.

A new Leadership and Culture risk was proposed, emphasising shared accountability between officers and Members and the need for sustained cultural transformation supported by improved staff engagement.

Members highlighted concerns regarding the clarity and accessibility of risk reporting and the effectiveness of engagement activity and requested improvements including clearer presentation of risk (with and without mitigation), reassessment of cyber risk levels, and deeper scrutiny of key risks.

The Committee noted the report, approved the inclusion of the Leadership and Culture risk, and supported further work to strengthen oversight, reporting quality, and long-term risk management maturity.

### **October 2025**

The Fire Authority received minutes from the Standards, Audit and Performance Committee meetings held in July and September 2025

### **December 2025**

The Audit and Standards Committee received a Corporate Risk Management Summary update.

The report explained that risk management processes had been strengthened following earlier HMICFRS inspection findings, with regular monitoring in place and clearer tolerance thresholds guiding action.

Three priority risks remained above tolerance and require close management - staff engagement, cybersecurity/system resilience, and data and digital capability.

The new “Leadership and Culture” risk had been refined and proposed for inclusion, recognising the potential impact of leadership effectiveness on organisational performance, culture, and trust.

Overall, the report emphasised ongoing improvement to risk management arrangements, continued mitigation activity across all risk areas, and the need for stronger governance, scrutiny, and capability to ensure the Service can deliver its Community Risk Management Plan effectively.

### **February 2026**

The Audit and Standards Committee received the External Auditors annual report 2024/25.

The Auditor’s Annual Report identified that, while the Authority had taken positive steps to strengthen its corporate risk management arrangements - including introducing a Risk Management Protocol and refreshing the Corporate Risk

Register - these remained at an early stage of implementation and were not yet fully embedded.

Consequently, significant weaknesses persisted throughout 2024/25, aligned to the HMICFRS Cause of Concern regarding the management of strategic risks, performance and improvement plans.

Although new governance arrangements had been put in place, including regular review and reporting of risks, assurance over their effectiveness was not yet sufficient, and internal audit had not provided a formal opinion on risk management.

These challenges were compounded by wider issues relating to leadership, culture, decision-making, and statutory officer capacity, which collectively undermined the maturity and effectiveness of the Authority's risk framework.

Continued, sustained delivery of the HMICFRS action plan - particularly strengthening risk-informed reporting, assurance processes and oversight - was therefore critical to achieving a robust and fully embedded corporate risk management approach.

#### **January to March 2026**

Worcestershire Internal Audit Shared Service (WIASS) reviewed Corporate Risk Management between January and March 2026. The outcome of the audit outlined the assurance level provided, key strengths, areas requiring improvement, and the actions that need to be taken to progress the Service's risk management maturity.

#### **April 2026**

The Audit and Standards Committee received a Corporate Risk Management Summary update.

The report showed that most key risks had remained stable while finance, environmental, and health and safety risks had increased due to budget pressures, ageing infrastructure, training facility issues, capacity gaps and system limitations.

Mitigations had been introduced, including interim training arrangements, additional health and safety support, improved cyber controls, digital governance, and budget engagement, while a wider review of corporate risk management with Internal Audit was underway to strengthen assurance, governance and risk maturity.

## **5 Summary of Corporate Risk Register (April 2026)**

The table below summarises the corporate risk, as reported to Audit and Standards Committee in April 2026.

| Risk   | Previous | Current | Movement              | Summary position   |
|--|----------|---------|-----------------------|--|
| <b>CR1 – Staff Engagement</b>                  | 15       | 15      | →<br>No change        | Several controls had been completed or introduced. Officers considered reducing the likelihood score but agreed to review this following staff survey results and further culture transformation progress.   |
| <b>CR2 – Political and Organisation Change</b> | 9        | 9       | →<br>No change        | The risk remained unchanged due to limited internal control over external political factors. Budget reductions and CRMP activity remained under review.  |
| <b>CR3 – Cyber Security</b>                    | 15       | 15      | →<br>No change        | Controls were strengthened through phishing simulations, managed detection and response, enhanced email security and AI-based threat detection. Likelihood remained medium due to geopolitical risk.         |
| <b>CR4 – Digital and Data Capability</b>       | 20       | 20      | →<br>No change        | Digital demand and hardware cost pressures continued. Controls included SAOR progress, FaRDaP transition, apprenticeships, improved device access, MDT replacement, recruitment and strengthened governance. |
| <b>CR5 – Finance</b>                           | 8        | 12      | ↑<br><b>Increased</b> | The rating increased following the final budget settlement and rising costs. Precept agreement improved stability, with further budget engagement underway.  |
| <b>CR6 – Environment</b>                       | 9        | 16      | ↑<br><b>Increased</b> | The rating increased due to ageing station and training facility infrastructure. Mitigations included a formal MOU with Staffordshire FRS and expedited upgrade works.                                       |
| <b>CR7 – Health &amp; Safety</b>               | 8        | 20      | ↑<br><b>Increased</b> | The rating increased due to capacity gaps, recruitment challenges, system end-of-life issues and links to environmental risk. Additional controls and interim support were introduced.                       |
| <b>CR8 – Leadership and Culture</b>            | 15       | 15      | →<br>No change        | The risk remained unchanged. Early signs of cultural improvement were noted, with staff survey results expected to support future assessment.  |

## 6 Internal Audit

Internal Audit concluded that the Service had established the foundations of a corporate risk management framework, but that arrangements were not yet sufficiently embedded to provide consistent assurance. The Limited Assurance

opinion reflected the Service's own assessment of risk maturity and confirmed the need to accelerate improvement activity.

Key strengths included effective Member oversight, a sound Corporate Risk Register design and positive SMT engagement.

### **Key Audit Findings**

The audit raised six findings, five rated Unacceptable:

1. Risk scoring: scoring criteria were not sufficiently tailored to the Service.
2. Risk appetite: there was no documented rationale for tolerance levels.
3. Risk integration: corporate, departmental and RAIDO processes were not fully aligned
4. Training and guidance: routine training and clearer role definitions were required.
5. Control assurance: controls required clearer monitoring and assurance
6. Inherent and residual risk (limited assurance): the protocol needed to explain these concepts more clearly.

### **Strategic Implications for the Fire Authority**

The findings did not indicate immediate operational risk, but could affect the reliability of strategic governance, including risk assessment quality, early warning indicators, Member assurance and HMICFRS compliance.

Strengthening corporate risk management therefore remained a priority ahead of the next scheduled HMICFRS inspection in November 2026.

### **Planned Improvement Actions (Appendix A)**

The improvement plan focuses on:

- **Framework and appetite:** revised scoring criteria and a documented risk appetite statement.
- **Integration:** clearer escalation and de-escalation between departmental, project and corporate risks.
- **Risk register management:** clearer processes for archiving, transferring and escalating risks.
- **Training and capability:** recurring training and competency records for managers, risk owners and Members.
- **Control assurance:** stronger control owner reporting and assurance mapping.

- **Policy enhancement:** clearer roles, responsibilities and guidance on inherent and residual risk.

### Additional Opportunities Identified

The audit also suggested linking future risk reports to service priorities and considering additional capacity through a Risk Management Co-ordinator role or enterprise risk management software.

## 7 Corporate Risk Register (June 2026)

The table below sets out the current status of the corporate risk register.

| Corporate risk                                     | Inherent impact | Inherent likelihood | Inherent score | Residual impact | Residual likelihood | Residual score |
|--|-----------------|---------------------|----------------|-----------------|---------------------|----------------|
| CR1 – Staff Engagement                             | 4               | 4                   | 16             | 3               | 3                   | 9              |
| CR2 – Political and Organisation Change            | 3               | 3                   | 9              | 3               | 3                   | 9              |
| CR3 – Cyber Security Threats and System Resilience | 5               | 5                   | 25             | 5               | 3                   | 15             |
| CR4 – Data & Digital Capability                    | N/A             | N/A                 | N/A            | 4               | 4                   | 16             |
| CR5 – Finance                                      | 5               | 4                   | 20             | 4               | 3                   | 12             |
| CR6 – Environment                                  | 4               | 4                   | 16             | 3               | 3                   | 9              |
| CR7 – Health and Safety                            | 5               | 4                   | 20             | 4               | 3                   | 12             |
| CR8 – Leadership and Culture                       | 5               | 4                   | 20             | 3               | 3                   | 9              |
| CR9 – ICCS Stability and Reliability               | 5               | 4                   | 20             | 4               | 3                   | 12             |
| CR10 – Industrial Action                           | 4               | 4                   | 16             | 4               | 3                   | 12             |
| CR11 – Operational Training Facilities             | 4               | 5                   | 20             | 4               | 3                   | 12             |

Following Internal Audit feedback, three additional risks have been added to the register: ICCS Stability and Reliability; Industrial Action; and Operational Training Facilities. Recording these as separate corporate risks, rather than including them within existing risks, provides greater transparency, improves the accuracy of risk assessment, and strengthens management oversight and assurance.

## 8 Supporting Considerations

- There are no financial, legal, environmental, or health and safety issues directly caused by this report.
- The report doesn't affect partnerships or public services directly.

- Additional Corporate Risk training is being scheduled for Service Management Team members and Fire Authority members to support ongoing responsibilities for assuring how these risks are being managed.

## **9 Appendices**

### **Appendix A**

Internal Audit Action Plan (Corporate Risk Management)

### **Appendix B**

Heatmap of Corporate Risks presented to Audit and Standards April 2026

### **Appendix C**

Heatmap of Corporate Risks presented to Fire Authority June 2026

## **10 Background Papers**

There are no background papers associated with this report.

# Worcestershire Internal Audit Shared Service Draft Internal Audit Report



**Shropshire**  
Fire and Rescue Service

## Corporate Risk Management 2025/26 23<sup>rd</sup> April 2026



### Distribution

Simon Hardiman – Chief Fire Officer

Jacqueline Dungey – s151 Officer

Mark Price - Area Manager, Head of Operations and Risk

Marc Millward – Assistant Chief Fire Officer

# Contents

|   |    |
|---|----|
| DISTRIBUTION .....  | 1  |
| CONTENTS .....  | 2  |
| 1 INTRODUCTION .....  | 3  |
| 1.1 Objective and Scope .....                                 | 3  |
| 1.2 Risks.....  | 4  |
| 2 AUDIT CONCLUSION AND EXECUTIVE SUMMARY.....                 | 5  |
| 3 FINDINGS AND RECOMMENDATIONS .....                          | 6  |
| 3.1 New Matters Arising .....                                 | 6  |
| 3.2 Clearance Meeting Discussion Points .....                 | 13 |
| 4 INDEPENDENCE AND ETHICS .....                               | 14 |
| 5 LIMITATIONS INHERENT TO THE WORK OF INTERNAL AUDIT.....     | 15 |
| 5.1 Conclusion.....   | 15 |
| 5.2 Internal Control.....                                     | 15 |
| 5.3 Future Periods.....                                       | 15 |
| 5.4 Responsibilities of Management and Internal Auditors..... | 15 |
| 6 APPENDIX A .....  | 16 |
| 6.1 Definitions of Audit Levels of Assurance.....             | 16 |
| 7 APPENDIX B .....  | 17 |
| 7.1 Definition of Priority of Recommendations.....            | 17 |
| 8 APPENDIX C .....  | 18 |
| 8.1 Summary of Management-Led Survey of SMT .....             | 18 |
| 9 APPENDIX D .....  | 20 |
| 9.1 Action Plan .....   | 20 |

# 1 Introduction

The audit of Corporate Risk Management was carried out in accordance with the Worcestershire Internal Audit Shared Service Audit Plan for Shropshire Fire and Rescue Service for 2025/26 as approved by the Audit and Governance Committee on 16<sup>th</sup> April 2025. The audit was a risk-based systems audit of Corporate Risk Management as operated by Shropshire Fire and Rescue Service.

In 2024, His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) issued a Cause of Concern stating that Shropshire & Wrekin didn't 'have adequate processes, controls or internal governance arrangements in place to manage strategic risks, performance and improvement plans'; consequently, work to ensure that 'the corporate risk register is actively used to mitigate and manage known risks' formed part of the Service's action plan. *(HMICFRS, Effectiveness, Efficiency and People 2023-2025, an inspection of Shropshire Fire and Rescue Service)*

In September 2025, HMICFRS undertook a Cause of Concern revisit and noted that good progress had been made against the recommendation and that the Service was on track to meet the deadline it has set in the action plan of 31<sup>st</sup> July 2026. Inspectors noted that work on the corporate risk register was still very new and that the service needs to take further action to ensure systems and processes are accepted and understood throughout the organisation. *(HMICFRS, Shropshire Fire and Rescue Service: Cause of concern revisit letter)*

This review was undertaken by Alex Vowles during the months of January to March 2026.

## 1.1 Objective and Scope

The objective and scope of this review were agreed after discussions with Joanne Coadey, Head of Finance, and Marc Millward, Assistant Chief Fire Officer (ACFO). The findings and recommendations were discussed with ACFO Millward.

The objective of this audit was to provide assurance that corporate risk management controls are effective, embedded to support informed decision-making, resource prioritisation, and service provision.

The scope covered:

- Governance & Oversight

- Evaluate whether appropriate strategic oversight arrangements are operating effectively
- Risk Management Controls
  - Assess whether corporate risk registers are appropriately designed and utilised to mitigate/manage known risks
  - Assess the design of the Risk Management Policy in respect of managing corporate risk.
  - Determine whether risk appetite is appropriately defined, communicated, and embedded into strategic risk management.
  - Review the extent to which the corporate risk register is embedded and operating effectively to mitigate/manage risk.

This review covered the controls in place at the time of the review.

This review did not cover:

- An assessment of the maturity of risk culture within the organisation.
- An opinion of assurance regarding operational risk management, including the Community Risk Management Plan.
- Cyber Security – final report issued June 2025
- Business continuity arrangements.
- An assessment of the extent to which the service has been successful in achieving its action plan

## 1.2 Risks

The following were identified as significant risks associated with the area audited:

- Failure of system governance and control to manage strategic risks and resources, resulting in material service disruption, reputational and financial damage.
- Increased scope for fraud occurrence resulting in reputational and financial damage.
- Failure to improve the system of strategic risk management in respect of the inspection conducted by His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS)

While the Worcestershire Internal Audit Shared Service cannot provide guarantees, no indication of fraudulent activity was identified during the review.

## 2 Audit Conclusion and Executive Summary

From the audit work carried out we have concluded that there is **limited** assurance over the control environment in this area. The level of assurance has been calculated using a methodology that is applied to all Worcestershire Internal Audit Shared Service audits and has been defined in the “Definition of Audit Levels of Assurance” table in Appendix A. However, it should be noted that statements of assurance levels are based on information provided at the time of the audit.

We have concluded that the level of assurance is limited in this area because significant gaps and weaknesses were identified and improvement to the system of governance, risk management, and control (GRC) is required to effectively manage corporate risk. While the service has made initial steps to develop corporate risk management processes, these remain relatively immature and fundamental weaknesses are present – particularly in relation to understanding responsibilities, processes, and risk assessment.

The review found the following areas of the system were working well:

- The Audit and Standards Committee is appropriately positioned to support governance, oversight, and scrutiny of the system of Corporate Risk Management.
- The fundamental design of the Corporate Risk Register is adequate to support effective management of corporate risks, although there are certain areas which require further development (see findings).
- Interviews with a sample of the Senior Management Team (SMT) indicated that, while staff were often unsure of the correct procedure and raised concerns in respect of consistency, there was no indication that staff overlooked risk management – rather they demonstrated a willingness to engage with the topic to their best abilities.

The review found the following areas of the system where controls could be strengthened:

| Finding Title            | Priority     | Ref. |
|--------------------------|--------------|------|
| Risk Scoring Criteria    | Unacceptable | 1    |
| Risk Appetite            | Unacceptable | 2    |
| Integration              | Unacceptable | 3    |
| Training & Guidance      | Unacceptable | 4    |
| Control Measures         | Unacceptable | 5    |
| Inherent & Residual Risk | Acceptance   | 6    |

## 3 Findings and Recommendations

The issues identified during the audit have been set out in the table below along with the related risks, recommendations, management responses and action plan. The issues identified have been prioritised according to their significance / severity using the service's definitions of impact, likelihood and risk appetite which are set out in the "Definition of Priority Recommendations" table in Appendix B.

The service's risk matrix denotes, based on the product of impact and likelihood scores, whether the risk is 'acceptable', 'tolerable', or 'unacceptable' and, for the avoidance of doubt, these are not classifications produced by Internal Audit; crucially, senior management and the Fire Authority are responsible for determining whether the service is willing to tolerate a risk.

### 3.1 New Matters Arising

| 1. Risk Scoring Criteria  | Unacceptable |
|---|--------------|
| <p><b>a) Finding:</b><br/>Risk scoring criteria (Appendix B) are not adequately designed to support the effective assessment of corporate risks. For example, under the current definitions, at Appendix B, a high likelihood (4) of a financial impact on the Authority of up to £1 million would be tolerated. It seems unlikely the Authority would be willing to tolerate a financial impact of this size which was deemed likely to occur within the year.</p> <p>Impact descriptions are not adequately developed to support the effective assessment of risks relating to compliance, opportunity loss, and cross-departmental impacts; particularly where actual occurrence may result in the occurrence of multiple contingent risks.</p> <p>Management were not able to provide the auditor with sufficient evidence to support the rationale for selecting the chosen criteria; upon further investigation, the auditor identified that the criteria used closely resembled those used by a Telford &amp; Wrekin Council. Together, this may suggest that risk assessment criteria are not suitably tailored to the organisation. Interviews conducted by the auditor with a sample of members of the Senior Management Team (SMT) supported the above observation – in particular, management expressed a desire to enhance cross-departmental risks to better understand the maximum level of risk that could be reasonably expected to occur.</p> <p>The Risk Management Protocol does not contain a mechanism to ensure regular reassessment of risk scoring criteria, or that of the Protocol itself.</p> |              |
| <p><b>b) Risk:</b><br/>Inadequately designed criteria may reduce the effectiveness of the assessment of risk with potential to materially affect the success of corporate risk management, resulting in an unknown level of risk to the service.</p> <p>Where criteria are not regularly reassessed, these may become unsuitable for the service to effectively manage risk. For example, the service's ability to tolerate financial damage may vary from one financial period to the next as funding levels fluctuate.</p>  |              |

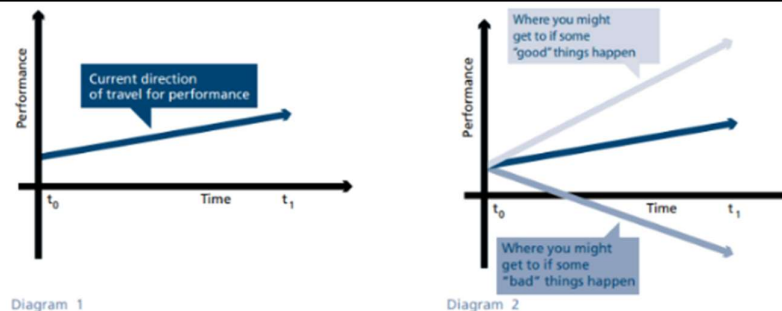
Untimely reassessment of the Protocol may reduce its effectiveness in supporting consistency and to providing guidance.

**c) Recommendations:**

Assess and document the extent to which criteria are adequately designed for the effective assessment of risk, with consideration of material pressures such as financial position, reputational standing, and regulatory environment.

Enhance criteria to enable effective assessment of contingent risks. In particular, management should work to better understand the minimum and maximum outcomes which may occur.

Establish and document a mechanism to ensure the routine assessment of criteria to ensure suitability.



*Institute of Risk Management, Risk Appetite & Tolerance*

**d) Management Response/Action Plan:**

See Appendix D.

**2. Risk Appetite**

**Unacceptable**

**a) Finding:**

Management were unable to evidence the rationale behind the setting of risk appetite levels, something further supported by interviews conducted with SMT members. The auditor identified that the levels of appetite are identical to that published by West Midlands Fire & Rescue Service.

While having a similar level of risk appetite to another authority is not indicative of a failure, where the rationale for setting of risk appetite and tolerance is unknown management fundamentally fail to understand a fundamental component of their system of corporate risk management.

**b) Risk:**

Management may not understand a fundamental component of the service's approach to risk management. Where risk management is not properly understood, the effectiveness of the Risk Management Protocol is expected to materially reduced. Consequently, an unknown level of risk is deemed to be present on the basis that corporate risks may be improperly assessed in relation to the service's actual risk appetite and tolerance.

**c) Recommendations:**

Develop a robust understanding of risk management, and an appropriate programme of training (see ref. 4) including:

- Assessing the suitability of the current risk appetite and tolerance levels, documenting the rationale for the decision and ensure members are appropriately informed.

- Amend the Risk Management Protocol to ensure there is a mechanism to ensure risk appetite and tolerance are reviewed on a regular basis, including where external environmental factors materially impact the service's willingness to accept e.g. financial settlement outcome.
- Develop the Senior Management Team's understanding of risk appetite and tolerance through training and enhanced guidance notes.
- Consider implementation of a risk appetite statement. For guidance, management may wish to refer to the Orange Book, Risk Appetite Guidance and/or examples available from partner authorities.

**d) Management Response/Action Plan:**

See Appendix D.

**3. Integration**

**Unacceptable**

**a) Finding:**

Corporate risk management is not adequately integrated with the wider system of risk management and there is a non-uniform understanding of how corporate and departmental risks are related. There is no process for escalating non-corporate risks where the level of risk becomes such that it cannot be managed at the current level of management, including those identified by department risk registers and the Risk, Assumption, Issue, Dependency, Opportunity (RAIDO) process. Based on a review of the RAIDO log and supporting information from the management-led survey in Appendix C and SMT minutes, management are successful in identifying risks, but these are generally risks which could be managed at the departmental level. At present, there is a high likelihood that the RAIDO is being utilised as an alternative to department and corporate risk registers which may result in risks being improperly managed. Similarly, there is no process for archiving risks that are no longer relevant, such as due to regulatory change, or have been reduced to a level such that corporate oversight is no longer appropriate.

Staff raised concerns over the integration of risk management processes and indicated that additional clarity was needed; likewise, management undertook their own survey independently of Internal Audit (Appendix C) in which 64% of staff disagreed that they understood the triggers for escalating or de-escalating a risk. Some staff also indicated that IT privileges were not correctly set for them to access and update the necessary registers. For corporate risk management to operate effectively, proper integration with non-corporate risk is crucial and management should not consider corporate risks to be static – these should develop over time, with new entries added as required. Only 26% of SMT members agreed that corporate risks were 'appropriate and sufficient' and interviews undertaken identified a reluctance to alter corporate risks.

The scope of the Risk Management Protocol is not clearly defined and, where management intend to apply this to non-corporate risk, additional guidance would be necessary for the control to operate effectively in the 2<sup>nd</sup> line of defence.

**b) Risk:**

Corporate risk management is not adequately integrated resulting in emerging or escalating risks not being handled appropriately, consequently resulting in the actual occurrence of risk. Associated financial and reputational damage may occur.

Co-existence of department risk registers and RAIDO may result in duplication of duties, particularly where no integration processes exist to move risks from the RAIDO to a register where they may be managed effectively.

Ineffectiveness or absence of a 2<sup>nd</sup> line policy control to support the effectiveness and consistency of non-corporate risk management. Potential for material risk occurrence such that the achievement of the service's strategic objectives may be impacted.

Corporate risk register may become static and fail to operate effectively to manage risk. Staff may also feel unable to raise corporate risks with a potential for a cultural issue to develop if not addressed.

**c) Recommendations:**

Develop the Risk Management Protocol to better integrate corporate and non-corporate risk management including:

- Establish a robust method for escalating risks from department risk registers, such as escalation thresholds triggering a review by SMT based on a risk exceeding a critical risk value.
- Develop the intended purpose of the RAIDO, including the intended output once risks have been identified such as transfer to a risk register for management by a suitable department. Where risks are to be kept on the RAIDO, a timeframe for review should be established and off-loading to a more appropriate register.
- Design an adequate process for archiving risks or de-escalating them where events render risks irrelevant.
- Ascertain the intended scope of the Risk Management Protocol and, where this will include non-corporate risk, expand guidance accordingly to support the objectives of the document.
- Clearly define the roles and responsibilities of staff, with sufficient guidance available. Risk management should ultimately be owned and championed and it must be clear who will do so.
- Ensure the Corporate Risk Register is fluid and regularly changes with seamless integration with other registers to ensure that a 'live' understanding of risk is possible. Management may wish to consider the use of enterprise risk management software.

**d) Management Response/Action Plan:**

See Appendix D.

**4. Training & Guidance**

**Unacceptable**

**a) Finding:**

The Risk Management Protocol does not contain a mechanism to ensure regular risk management training is provided to staff and members of the Audit and Standards Committee. While the auditor was provided with evidence of a previous training session provided to the SMT by a third party, robust controls should be in place to ensure that training needs are not overlooked and that those responsible for risk management are adequately trained to perform their duties. This should include refresher training. Staff indicated they feel additional training is required for them to fully own their responsibilities in respect of risk management.

The Risk Management Protocol does not adequately define the roles, responsibilities, and processes to provide staff with sufficient information to perform their duties. Additional guidance for risk and control owners are required for processes to become properly embedded and operate as intended.

**b) Risk:**

Staff and/or members may lack the required knowledge to effectively fulfil their responsibilities as outlined in the Risk Management Protocol resulting in the inappropriate management of risk. In severe cases, this may result in risks being mismanaged and materially impeding the service's ability to achieve its strategic objectives.

Staff may lack sufficient guidance to properly own their responsibilities. Where procedures are not properly defined, such as control ownership, the effectiveness of the corporate risk register is expected to be substantially reduced.

**c) Recommendations:**

Demonstrate an on-going commitment to the training of staff and members including:

- Amending the Risk Management Protocol to establish a robust control for ensuring the regular training of staff and members, with topic specific training where competency gaps are identified. Management may wish to consider engaging an external specialist who can provide bespoke additional support and assist to transform the risk management framework.
- Determine a means of monitoring competency and training of staff and members, such as the adoption of a training record or competency framework. Some examples management may wish to use:
  - Risk Management Skills and Capability Framework, Orange Book
  - Professional Standards in Risk Management, Institute of Risk Management
- Provide staff with additional guidance for managing corporate risk, in particular where new staff enter positions of senior management.
- Consider whether risk management qualifications may be beneficial for the development of specific staff, such as use of a risk management co-ordinator. Possible qualifications include:
  - International Certificate in Enterprise Risk Management, (Institute of Risk Management)
  - Introduction to Risk Management (ISO 31000:2018), (British Standards Institution)
  - Certification in Risk Management Assurance (Institute of Internal Auditors)
- Amend the Risk Management Protocol to provide staff with additional guidance in respect of:
  - Clarity regarding expectations – what should be updated, when, by who etc.
  - Guidance in terms of integrating their risk management ownership to control owners, including in the non-corporate domain
  - Clear direction on ownership of risk management and who can provide support in the event of queries

**d) Management Response/Action Plan:**

See Appendix D.

**5. Control Measures**

**Unacceptable**

**a) Finding:**

The Corporate Risk Register identifies relevant controls for each risk entry and, for this to be effective, management must assess the effectiveness of these controls on a regular basis. Currently, identified controls and supporting monitoring arrangements are not appropriately designed to effectively mitigate risk.

Control measures identified are generally high-level and broadbrush, limiting the extent to which they may be tied to a specific item in the control environment. Furthermore, there is currently no means of assessing control operation to provide assurance that, where controls have been identified, these are suitably designed and operating effectively to mitigate the risk they are assigned to.

Based on interviews with a sample of SMT members, staff indicated they had limited assurance as to whether controls were operating or suitable for the risk to which they were assigned. Interrogating these risks properly would likely be onerous and a lack of management information was communicated. Based on the management-led survey (Appendix C), only half of respondents confirmed they regularly assess their controls.

**b) Risk:**

Key controls are not effectively monitored and the process of doing so is onerous, resulting in control failure going unidentified and the scoring of residual risk may be materially distorted. Where this occurs, the likelihood and impact of risks may be significantly greater than expected and the service may have an incomplete understand of its actual enterprise risk.

Where control failure is not identified, a trivial cost of rectification may develop into one with more considerable budgetary impact due to risk escalation. Potential for financial damage.

**c) Recommendations:**

- Establish a robust control assurance framework to ensure controls are regularly reassessed and management information is easily available to assess operation. Management may wish to consider the following approaches:
  - Dashboard style reporting of controls suitable for quantitative scoring
  - Regular updates from control owners on the effectiveness of controls
  - Structured assurance framework including reporting lines
  - Traditional approach to control addressing control such as COSO (Committee of Sponsoring Organisations of the Treadway Committee), or the 5 Dimensions of Control model.
- Amend the Risk Management Protocol to suitably define the reporting relationship for control owners. This should include the frequency of reporting and the role of SMT in providing oversight.
- Where controls are found to be ineffective such that residual risk is materially different to previously reported to the Audit and Standards Committee, Members should be informed in a timely manner such that they are cognizant of the service's risk profile.
  - There is scope for the programme of internal audit work to be enhanced through targeted testing of declared risk mitigation controls to assess effectiveness.
- Map corporate risk areas to the three lines of defence, assessing sources of control and assurance currently in place (assurance mapping).

**d) Management Response/Action Plan:**

See Appendix D.

| 6. Inherent & Residual Risk   | Acceptance |
|---|------------|
| <p><b>a) Finding:</b><br/>The Corporate Risk Register utilises the concept of inherent and residual risk, however the Risk Management Protocol does not reference this concept and thus provides no guidance to users of the policy.</p>  |            |
| <p><b>b) Risk:</b><br/>The Protocol's effectiveness as a 2<sup>nd</sup> line control to support consistency and effectiveness of risk management activities may be diminished where insufficient guidance is provided to users. Users may have insufficient information to properly perform their duties, resulting in increased potential for inappropriately managed risks or actual occurrence of risk including reputational and/or financial damage.</p> <p>Risk level is considered to fall within the organisation's definition of "acceptance" on the basis that risk owners are expected to have requisite knowledge such that this would not materially endanger the success of corporate risk management. This is supported by the outcomes of interviews with members of SMT.</p> |            |
| <p><b>c) Recommendations:</b><br/>Amend the Risk Management Protocol to include the use of inherent and residual risk, providing sufficient and appropriate guidance for staff to be able to undertake their duties as required.</p>  |            |
| <p><b>d) Management Response/Action Plan:</b><br/><br/>See Appendix D.</p>  |            |

## 3.2 Clearance Meeting Discussion Points

The following matters were discussed with management at the clearance meeting as advisory observations:

### Service Priorities

Management have mapped relevant service priorities to entries on the Corporate Risk Register. Reporting provided to the Audit and Standards Committee does not include links to service priorities. Management should consider the extent to which service priorities may be beneficial for members.

### Co-ordination

Management may wish to explore the use of a Risk Management Co-Ordinator and/or system-based enterprise risk management software to and act as a central hub for organisational risk management. The Co-Ordinator may also be able to provide expert guidance to managers as required, especially where risk management qualifications are obtained.

## 4 Independence and Ethics

WIASS confirms that in relation to this review there were no significant facts or matters that impacted our independence as Internal Auditors that we are required to report.

WIASS conforms with the Institute of Internal Auditors Public Sector Internal Audit Standards as amended and confirms that we are independent and are able to express an objective conclusion in relation to this review.

WIASS confirm that policies and procedures have been implemented in order to meet the IIA Ethical Standards.

Prior to and at the time of the audit, no non-audit or audit related services have been undertaken for the Council within this area of review.

**Chris Green**  
**Head of Internal Audit Shared Service**

[chris.green@worcester.gov.uk](mailto:chris.green@worcester.gov.uk)

## 5 Limitations Inherent to the Work of Internal Audit

Internal Audit undertakes a programme of work agreed by the Council's senior managers and approved by the Audit Committee subject to the limitations outlined below.

### 5.1 Conclusion

Each audit assignment undertaken addresses the control objectives agreed with the relevant responsible managers. There might be weaknesses in the system of internal control that Internal Audit are not aware of because they did not form part of the programme of work, were excluded from the scope of individual internal audit assignments or were not brought to the attention of Internal Audit. As a consequence, the Audit Committee should be aware that the Audit conclusion for each assignment might have differed if the scope of individual assignments was extended or other relevant matters were brought to Internal Audit's attention.

### 5.2 Internal Control

Internal control systems identified during audit assignments, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgement in decision making, human error, control processes being deliberately circumvented by employees, management override of controls, and unforeseeable circumstances.

### 5.3 Future Periods

The assessment of each audit area is relevant to the time that the audit was completed. In other words, it is a snapshot of the control environment at that time. This evaluation of effectiveness may not be relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in operating environment, law, regulatory requirements or other factors; or
- The degree of compliance with policies and procedures may deteriorate.

### 5.4 Responsibilities of Management and Internal Auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance, and for the prevention or detection of irregularities and fraud. Internal Audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems. Internal Audit endeavours to plan its work so that there is a reasonable expectation that significant control weaknesses will be detected. If weaknesses are detected, additional work is undertaken to identify any consequent fraud or irregularities. However, Internal Audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected, and its work should not be relied upon to disclose all fraud or other irregularities that might exist.

# 6 Appendix A

## 6.1 Definitions of Audit Levels of Assurance

| Conclusion                   | Definition   |
|------------------------------|--|
| <b>Substantial Assurance</b> | A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied with only minor issues identified to support the achievement of objectives in the area audited.            |
| <b>Reasonable Assurance</b>  | There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.                     |
| <b>Limited Assurance</b>     | Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.                       |
| <b>No Assurance</b>          | Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited. |

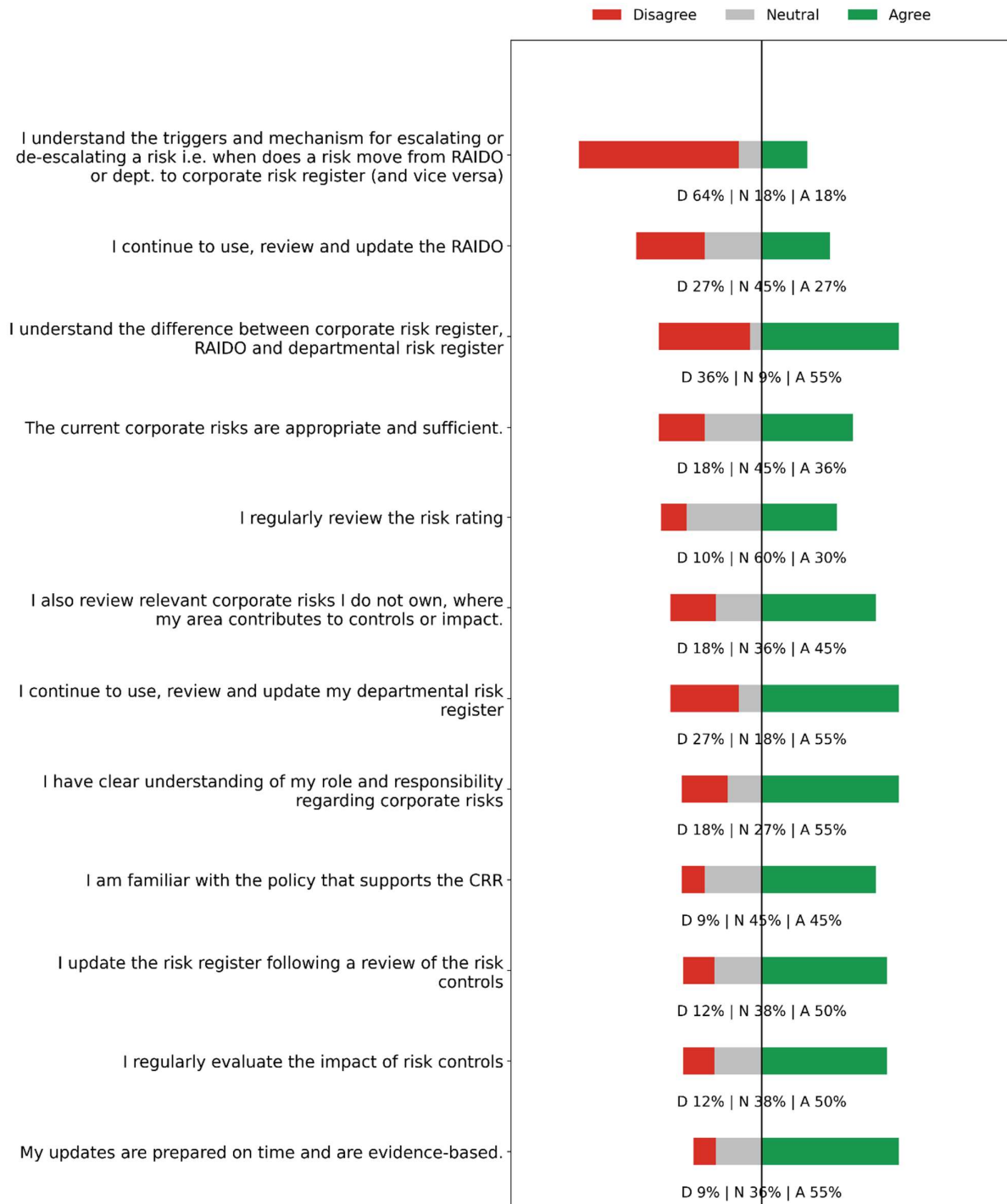
# 7 Appendix B

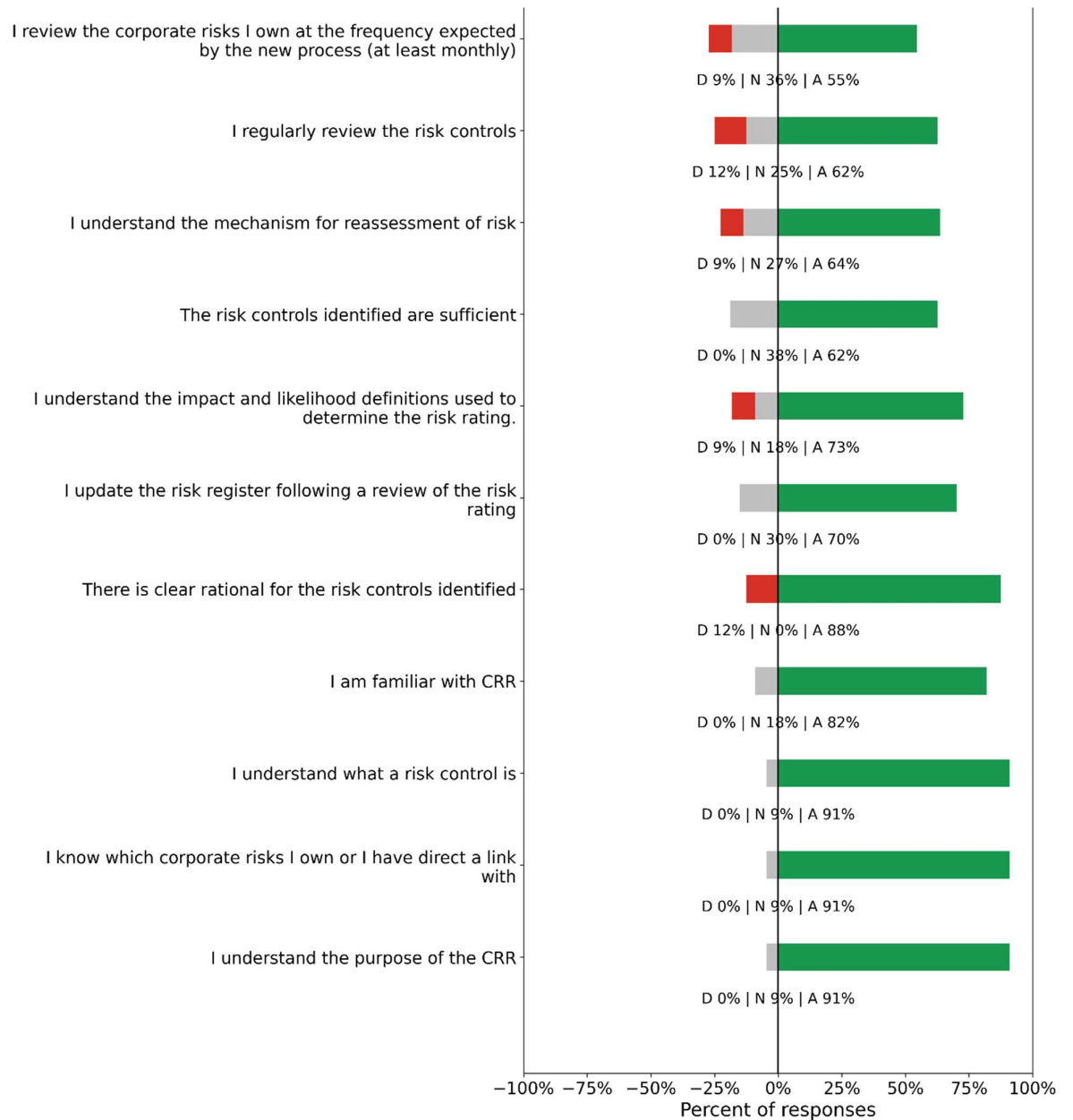
## 7.1 Definition of Priority of Recommendations

| Impact     | Score      | Definitions   | Matrix  |              |            |           |              |        |           |   |    |    |    |    |      |   |   |    |    |    |        |   |   |   |    |    |     |   |   |   |   |    |          |   |   |   |   |   |  |  |          |     |        |      |           |            |  |  |  |  |  |  |
|------------|------------|---|---|--------------|------------|-----------|--------------|--------|-----------|---|----|----|----|----|------|---|---|----|----|----|--------|---|---|---|----|----|-----|---|---|---|---|----|----------|---|---|---|---|---|--|--|----------|-----|--------|------|-----------|------------|--|--|--|--|--|--|
| Very High  | 5          | <ul style="list-style-type: none"> <li>- Financial impact on the Authority likely to exceed £5M</li> <li>- Severe/catastrophic impact on the Authority's statutory duties and strategic objectives</li> <li>- Significant stakeholder concern</li> <li>- The risk has occurred and will continue to do so without further action being taken</li> </ul> | <div style="text-align: center;"> <p><b>Risk Acceptance and Risk Tolerance Levels</b></p> <table border="1" style="margin: 0 auto;"> <tr> <td></td> <td style="background-color: #90EE90;">Acceptance</td> <td style="background-color: #FFD700;">Tolerance</td> <td style="background-color: #FF0000;">Unacceptable</td> </tr> </table> <br/> <table border="1" style="margin: 0 auto;"> <tr> <td rowspan="5" style="writing-mode: vertical-rl; transform: rotate(180deg);">Impact</td> <td>Very High</td> <td style="background-color: #90EE90;">5</td> <td style="background-color: #FFD700;">10</td> <td style="background-color: #FF0000;">15</td> <td style="background-color: #FF0000;">20</td> <td style="background-color: #FF0000;">25</td> </tr> <tr> <td>High</td> <td style="background-color: #90EE90;">4</td> <td style="background-color: #FFD700;">8</td> <td style="background-color: #FF0000;">12</td> <td style="background-color: #FF0000;">16</td> <td style="background-color: #FF0000;">20</td> </tr> <tr> <td>Medium</td> <td style="background-color: #90EE90;">3</td> <td style="background-color: #FFD700;">6</td> <td style="background-color: #FF0000;">9</td> <td style="background-color: #FF0000;">12</td> <td style="background-color: #FF0000;">15</td> </tr> <tr> <td>Low</td> <td style="background-color: #90EE90;">2</td> <td style="background-color: #FFD700;">4</td> <td style="background-color: #90EE90;">6</td> <td style="background-color: #FFD700;">8</td> <td style="background-color: #FFD700;">10</td> </tr> <tr> <td>Very Low</td> <td style="background-color: #90EE90;">1</td> <td style="background-color: #90EE90;">2</td> <td style="background-color: #90EE90;">3</td> <td style="background-color: #90EE90;">4</td> <td style="background-color: #90EE90;">5</td> </tr> <tr> <td></td> <td></td> <td style="background-color: #000000; color: white;">Very Low</td> <td style="background-color: #000000; color: white;">Low</td> <td style="background-color: #000000; color: white;">Medium</td> <td style="background-color: #000000; color: white;">High</td> <td style="background-color: #000000; color: white;">Very High</td> </tr> <tr> <td colspan="7" style="text-align: center;">Likelihood</td> </tr> </table> </div> |              | Acceptance | Tolerance | Unacceptable | Impact | Very High | 5 | 10 | 15 | 20 | 25 | High | 4 | 8 | 12 | 16 | 20 | Medium | 3 | 6 | 9 | 12 | 15 | Low | 2 | 4 | 6 | 8 | 10 | Very Low | 1 | 2 | 3 | 4 | 5 |  |  | Very Low | Low | Medium | High | Very High | Likelihood |  |  |  |  |  |  |
|            | Acceptance | Tolerance   |   | Unacceptable |            |           |              |        |           |   |    |    |    |    |      |   |   |    |    |    |        |   |   |   |    |    |     |   |   |   |   |    |          |   |   |   |   |   |  |  |          |     |        |      |           |            |  |  |  |  |  |  |
| Impact     | Very High  | 5   |   | 10           | 15         | 20        | 25           |        |           |   |    |    |    |    |      |   |   |    |    |    |        |   |   |   |    |    |     |   |   |   |   |    |          |   |   |   |   |   |  |  |          |     |        |      |           |            |  |  |  |  |  |  |
|            | High       | 4   |   | 8            | 12         | 16        | 20           |        |           |   |    |    |    |    |      |   |   |    |    |    |        |   |   |   |    |    |     |   |   |   |   |    |          |   |   |   |   |   |  |  |          |     |        |      |           |            |  |  |  |  |  |  |
|            | Medium     | 3   |   | 6            | 9          | 12        | 15           |        |           |   |    |    |    |    |      |   |   |    |    |    |        |   |   |   |    |    |     |   |   |   |   |    |          |   |   |   |   |   |  |  |          |     |        |      |           |            |  |  |  |  |  |  |
|            | Low        | 2   |   | 4            | 6          | 8         | 10           |        |           |   |    |    |    |    |      |   |   |    |    |    |        |   |   |   |    |    |     |   |   |   |   |    |          |   |   |   |   |   |  |  |          |     |        |      |           |            |  |  |  |  |  |  |
|            | Very Low   | 1   | 2   | 3            | 4          | 5         |              |        |           |   |    |    |    |    |      |   |   |    |    |    |        |   |   |   |    |    |     |   |   |   |   |    |          |   |   |   |   |   |  |  |          |     |        |      |           |            |  |  |  |  |  |  |
|            |            | Very Low  | Low   | Medium       | High       | Very High |              |        |           |   |    |    |    |    |      |   |   |    |    |    |        |   |   |   |    |    |     |   |   |   |   |    |          |   |   |   |   |   |  |  |          |     |        |      |           |            |  |  |  |  |  |  |
| Likelihood |            |   |   |              |            |           |              |        |           |   |    |    |    |    |      |   |   |    |    |    |        |   |   |   |    |    |     |   |   |   |   |    |          |   |   |   |   |   |  |  |          |     |        |      |           |            |  |  |  |  |  |  |
| High       | 4          | <ul style="list-style-type: none"> <li>- Financial impact on the Authority likely to be between £1M and £5M</li> <li>- Significant impact on the Authority's statutory duties and strategic objectives</li> <li>- High stakeholder concern</li> <li>- The risk is likely to occur this year</li> </ul>  |   |              |            |           |              |        |           |   |    |    |    |    |      |   |   |    |    |    |        |   |   |   |    |    |     |   |   |   |   |    |          |   |   |   |   |   |  |  |          |     |        |      |           |            |  |  |  |  |  |  |
| Medium     | 3          | <ul style="list-style-type: none"> <li>- Financial impact on the Authority likely to be between £250K and £1M</li> <li>- Moderate impact on the Authority's statutory duties and strategic objectives</li> <li>- Moderate stakeholder concern</li> <li>- This risk is likely to occur more than once in the next 5 years</li> </ul>                     |   |              |            |           |              |        |           |   |    |    |    |    |      |   |   |    |    |    |        |   |   |   |    |    |     |   |   |   |   |    |          |   |   |   |   |   |  |  |          |     |        |      |           |            |  |  |  |  |  |  |
| Low        | 2          | <ul style="list-style-type: none"> <li>- Financial impact on the Authority likely to be between £50K and £250K</li> <li>- Low impact on the Authority's statutory duties and strategic objectives</li> <li>- Low stakeholder concern</li> <li>- The risk may occur in the next 5 years</li> </ul>   |   |              |            |           |              |        |           |   |    |    |    |    |      |   |   |    |    |    |        |   |   |   |    |    |     |   |   |   |   |    |          |   |   |   |   |   |  |  |          |     |        |      |           |            |  |  |  |  |  |  |
| Very Low   | 1          | <ul style="list-style-type: none"> <li>- Financial impact on the Authority likely to be less than £50K</li> <li>- Insignificant/negligible impact on the Authority's statutory duties and strategic objectives</li> <li>- Very low stakeholder concern</li> <li>- The risk may occur in exceptional circumstances</li> </ul>                            |   |              |            |           |              |        |           |   |    |    |    |    |      |   |   |    |    |    |        |   |   |   |    |    |     |   |   |   |   |    |          |   |   |   |   |   |  |  |          |     |        |      |           |            |  |  |  |  |  |  |

# 8 Appendix C

## 8.1 Summary of Management-Led Survey of SMT





For the avoidance of doubt, this survey was created and circulated by management of the activity under review. Results of the survey have been used to compliment existing independent audit work undertaken and have not been used to fully evidence any of the findings raised.

## 9 Appendix D

### 9.1 Action Plan

#### 1. Risk Scoring Criteria – Unacceptable Priority

**Audit Finding:** Current impact and likelihood definitions are not tailored to SFRS and allow for unrealistic or inappropriate tolerances. No mechanism exists for routine review.

##### Actions

| Action   | Target Date | Success Measure  |
|--|-------------|--|
| Review of impact and likelihood criteria to ensure alignment with service financial thresholds, service priorities and goals, reputational considerations and regulatory compliance. | July 26     | Revised scoring matrix approved by SMT and Fire Authority.                         |
| Create clearer explanations for risks that affect more than one department, are dependent on other events, or build up over time.  | July 26     | New criteria published in updated Protocol.  |
| Introduce an annual review cycle for risk scoring criteria within the Risk Management Protocol. Aligned to revised internal governance structure.                                    | July 2026   | Review cycle embedded and minuted annually by SMT/Performance and Assurance Board. |

#### 2. Risk Appetite – Unacceptable Priority

**Audit Finding:** No evidence-based rationale for risk appetite levels; appetite appears copied from another FRS. SMT understanding is limited.

##### Actions

| Action   | Target Date | Success Measure   |
|--|-------------|---|
| Develop clear, evidence-based rationale for SFRS's risk appetite and tolerance levels.                                 | July 26     | Risk Appetite Statement drafted and agreed by Fire Authority. |
| Add formal review mechanism for risk appetite (e.g., annual review or triggered by major financial/regulatory change). | July 26     | Change control and review cycle inserted into Protocol.       |

| Action   | Target Date | Success Measure   |
|--|-------------|---|
| Deliver awareness training to SMT and Members on appetite, tolerance, and decision-making. | Dec 26      | 100% SMT and Member attendance recorded; improved understanding measured in post-training evaluation. |

### 3. Integration Between Corporate, Departmental & RAIDO Risk – Unacceptable Priority

**Audit Finding:** No formal escalation pathways; RAIDO being used inconsistently; risk registers not aligned; only 26% of SMT believe corporate risks are appropriate/sufficient.

#### Actions

| Action   | Target Date | Success Measure   |
|--|-------------|---|
| Define escalation and de-escalation triggers between departmental and corporate risks.                           | July 26     | Documented model approved and communicated.                         |
| Clarify intended purpose of RAIDO and embed a structured flow (identify → analyse → allocate → monitor → close). | July 26     | RAIDO guidance integrated into Protocol; usage monitored quarterly. |
| Create a formal process to archive obsolete risks and transfer appropriate risks to/from the corporate register. | July 26     | Archived log maintained; movement of risks recorded.                |
| Ensure IT access permissions allow relevant staff to update registers.   | May 26      | Access audit confirms 100% relevant staff permissions.              |

### 4. Training & Guidance – Unacceptable Priority

**Audit Finding:** No routine training; roles and responsibilities unclear; SMT and staff report low confidence; guidance insufficient.

#### Actions

| Action   | Target Date | Success Measure                 |
|--|-------------|---------------------------------|
| Establish a mandatory risk management training programme for SMT, managers, risk owners and Members. | July 26     | Training completion rate > 90%. |
| Develop a competency framework or training record for risk management roles.                         | July 26     | Framework approved and in use.  |

| Action  | Target Date | Success Measure                        |
|---|-------------|--|
| Produce practical guidance notes for risk owners and control owners (e.g., "how to update a risk," "what to record," "when to escalate"). | July 26     | Guidance published alongside Protocol. |
| Consider accessing external professional development.   | April 26    | Business case presented to ELT.        |

## 5. Control Measures – Unacceptable Priority

**Audit Finding:** Controls are high-level and lack monitoring; SMT unsure whether controls operate effectively; only half of SMT assess controls regularly.

### Actions

| Action   | Target Date | Success Measure                               |
|--|-------------|---|
| Develop a Control Assurance Framework, including control owner reporting, assurance mapping, and monitoring frequency. | July 26     | Framework approved and embedded.              |
| Implement regular control testing (quantitative dashboard or qualitative assessment).                                  | July 26     | Dashboard/assurance cycle reported quarterly. |
| Update the Protocol to formalise roles, responsibilities and reporting lines for control owners.                       | July 26     | Protocol updated and approved.                |
| Introduce escalation requirement where control failure materially alters residual risk.                                | July 26     | Reporting built into Committee reporting.     |

## 6. Inherent & Residual Risk – Acceptance Priority

**Audit Finding:** These terms are used in the register but not explained in the Protocol; inconsistent understanding risk.

### Actions

| Action   | Target Date | Success Measure                  |
|--|-------------|----------------------------------|
| Update the Protocol with clear definitions, examples and guidance on inherent and residual risk. | July 26     | Protocol updated and authorised. |

| Action  | Target Date | Success Measure                                   |
|---|-------------|---|
| Include this topic within mandatory training. | July 26     | Understanding tested in post-training evaluation. |

## 7. Other opportunities (Non-mandatory but beneficial)

**Audit Suggestions:** Explore Risk Management Coordinator role; consider enterprise risk management software; consider linking service priorities more clearly to risks.

### Actions

| Action  | Target Date | Success Measure                   |
|---|-------------|-----------------------------------|
| Develop service priority mapping to corporate risk register.              | July 26     | Included in Protocol.             |
| Add service priority mapping to risk register reports for Fire Authority. | July 26     | Included in next Committee cycle. |

### Corporate Risk Heatmap: April 2026

|                      |                   |                                 |                        |
|----------------------|-------------------|---------------------------------|------------------------|
| <b>Risk position</b> | <b>Acceptable</b> | <b>Tolerable with oversight</b> | <b>Above tolerance</b> |
|----------------------|-------------------|---------------------------------|------------------------|

| Impact \ Likelihood | 1 Very Low | 2 Low | 3 Medium        | 4 High     | 5 Very High |
|---------------------|------------|-------|-----------------|------------|-------------|
| <b>5 Very High</b>  |            |       | <b>CR3, CR8</b> | <b>CR7</b> |             |
| <b>4 High</b>       |            |       | <b>CR5</b>      | <b>CR4</b> |             |
| <b>3 Medium</b>     |            |       | <b>CR2, CR6</b> | <b>CR1</b> |             |
| <b>2 Low</b>        |            |       |                 |            |             |
| <b>1 Very Low</b>   |            |       |                 |            |             |

## Corporate Risk Heatmap: June 2026

| Risk position       | Acceptable | Tolerable with oversight | Above tolerance                       |            |             |
|---------------------|------------|--------------------------|---------------------------------------|------------|-------------|
| Impact \ Likelihood | 1 Very Low | 2 Low                    | 3 Medium                              | 4 High     | 5 Very High |
| 5 Very High         |            |                          | <b>CR3</b>                            |            |             |
| 4 High              |            |                          | <b>CR5, CR7, CR8, CR9, CR10, CR11</b> | <b>CR4</b> |             |
| 3 Medium            |            |                          | <b>CR1, CR2, CR6</b>                  |            |             |
| 2 Low               |            |                          |                                       |            |             |
| 1 Very Low          |            |                          |                                       |            |             |