

**16<sup>th</sup> November 2020**

**Risk Management**

**Purpose of Report**

Following a full internal Management Board review and an Internal Audit Report, the risk management framework of the MCA has been revised and refreshed. This report presents a new risk management policy and process.

**Thematic Priority**

Cross cutting.

**Freedom of Information and Schedule 12A of the Local Government Act 1972**

Under the Freedom of Information Act this paper and any appendices will be made available under the Combined Authority Publication Scheme.

**Recommendations**

The Mayoral Combined Authority is asked to consider and approve the revised Risk Management Policy (Appendix 1).

**1. Introduction**

- 1.1** Part 6F of the Constitution specifies that the Mayoral Combined Authority will put in place a Risk Management Policy.

A recent Internal Audit Report on risk management concluded that the processes of the MCA Executive in monitoring and managing risk on behalf of the MCA provide 'significant assurance with some improvements required'.

The recommendations of the audit included refreshing authority's Risk Management Policy and Process to ensure they; accurately reflect the structure of the organisation, set out reporting requirements, clarify escalation and de-escalation procedures and outlines how the MCA oversees the risk management arrangements of the PTE.

The audit report also recommended that a consistent approach to scoring and moderating risks should be developed as well as ensuring adequate training and development for roles with specific risk management responsibilities.

- 1.2** This paper presents a revised Risk Management Policy and Process, strengthened to address the recommendations of the internal audit report. The MCA Audit and Standards Committee, who are charged with overseeing the effectiveness of the Authority's risk management arrangements, endorsed the revised policy and process at their meeting on the 29<sup>th</sup> October 2020.

## **2. Proposal and justification**

- 2.1** The existing Risk Management Policy and Process have been reviewed and strengthened, and now follow the 'Management of Risk' (MoR®) principles of risk management which are aligned to the international standard for risk management ISO31000:2009 (There are currently 9 MoR® formally trained risk champions in the MCA Executive Team).

The refreshed Risk Management Policy and Process describes why risk management is important to the organisation and the objectives served by implementing a formal risk management approach. It sets out the approach to risk appetite and risk tolerance thresholds, the procedure for escalation/de-escalation, risk management duties of roles within the organisation and reporting requirements. It also sets out how the organisation plans to carry out risk management and the approach to identifying, assessing and evaluating risk, and planning and implementing mitigations.

The content of the documentation now addresses a number of recommendations made by the internal audit. These have been considered by the Audit and Standards Committee who have endorsed the approach taken.

### **2.2 Next steps**

Further to approval by the MCA, the Risk Policy will be published on the Authority's website.

## **3. Consideration of alternative approaches**

- 3.1** The MCA Executive respects the recommendations of the recent internal audit of risk management and, having considered various options, believes that the proposed risk management policy and process addresses the improvement points raised in the audit.

## **4. Implications**

### **4.1 Financial**

Failure to adequately manage risk could have significant financial implications for the MCA. The financial risk analysis has been redefined as follows:

- Extreme – Loss that could destabilise the financial health of the MCA Executive and / or destabilise a programme of activity (most likely a multi-year issue, or one which would take multiple years to resolve);
- Major/Serious – Loss that could be detrimental to the financial health of the MCA Executive and / or detrimental to delivering a programme of activity (most probably a single year issue);
- Moderate - Loss that is significant which cannot be contained within budget but that would require a new budget to be developed and approved
- Minor – Minor loss that can be contained within budget but would result in some planned spend being cancelled or delayed
- Immaterial – Minor loss that can be contained within budget with no detrimental impact on other planned activity

These impact levels are set out on page 11 of the Risk Management Policy and Process along with a description of different levels of impact in the categories of 'political', 'reputational' and 'economic'.

### **4.2 Legal**

There are no legal implications relating to the development and embedding of risk management processes.

#### **4.3 Risk Management**

Risk management is vitally important to the successful delivery of objectives. A defined risk management process is a key component of the governance and control framework that underpins this.

#### **4.4 Equality, Diversity and Social Inclusion**

There are no equality, diversity and social inclusion issues relating risk management processes.

### **5. Communications**

**5.1** Risk management processes are internal and do not require external communications. However, the Policy will be publicly available. Internal communication will be undertaken appropriately.

Should a risk materialise that has the impact of adverse public or Government reaction communication will be managed appropriately.

### **6. Appendices/Annexes**

**6.1** Appendix 1 – Risk Management Policy & Process

<b>REPORT AUTHOR</b>	<b>Claire James</b>
<b>POST</b>	<b>Governance &amp; Compliance Officer</b>
Officer responsible	<b>Ruth Adams</b>
Organisation	<b>Sheffield City Region</b>
Email	<b>Ruth.adams@sheffieldcityregion.org.uk</b>
Telephone	<b>0114 220 3442</b>

Background papers used in the preparation of this report are available for inspection at: 11 Broad Street West, Sheffield S1 2BQ

Other sources and references: n/a