WEST MIDLANDS FIRE AND RESCUE AUTHORITY

AUDIT AND RISK COMMITTEE

6 JUNE 2022

1. CREATION OF ADDITIONAL CORPORATE RISK RELATED TO CYBER SECURITY

Report of the Chief Fire Officer

RECOMMENDED

1.1 THAT the Committee note the change to Corporate Risk 7, with the addition of a distinct category for Cyber Risk 7.3 to provide greater focus and assurance in this area.

2. PURPOSE OF REPORT

2.1 This report provides the rationale for the inclusion of a separate distinct category within the current Corporate Risk Report related to Cyber Security.

3. BACKGROUND

3.1 As advised in the previous Audit and Risk Committee meeting on 21 March 2022 within the Annual Report of the SIRO, cyber security risks are increasing.

3.2 The organisation has existing corporate risks related to digital and data that are continually monitored under Corporate Risk 7.1 and 7.2.

3.3 Corporate Risk 7.1

The Fire Authority is unable to provide and maintain an effective IT provision to support the delivery of core functions, resulting in significant disruption to the organisation's functionality, reduced confidence, credibility, reputational damage, and external scrutiny.

Corporate Risk 7.2

The Fire Authority is unable to provide effective management and security of organisational information and documentation including the receipt, storage, sharing and transfer of information and data, resulting in reputational damage, litigation, substantial fines and external scrutiny.

3.4 The digital transformation that the organisation has undertaken has delivered many benefits including increasing reliance on the underlying information systems, infrastructure and data.

3.5 Cyber security risk is a significant risk for all organisations locally, nationally, and globally, with risks of accidental data loss, physical system failures and direct malicious cyber-attacks being an area requiring focus.

3.6 The National Cyber Security Centre (NCSC) produces a weekly cyber security threat bulletin that evidences the risks to organisations both within the public and private sector.

3.7 Since the beginning of the crisis in the Ukraine, the NCSC has advised organisations to take action and strengthen their cyber security defences to improve resilience against the threat of cyber security attacks emanating from Russia.

3.8 There is an ongoing need for the organisation to address all aspects of this risk through robust technical solutions and risk management processes, hence this request to create a separate risk within the Corporate Risk Register to govern and manage this important and significant risk.

3.9 The proposal is to create Corporate Risk 7.3

The Fire Authority is unable to prevent, respond to or recover from malicious attempts to damage or disrupt devices, services and networks - and the information on them.

4. EQUALITY IMPACT ASSESSMENT

4.1 This is not required as this report does not impact any positive characteristics.

5. LEGAL IMPLICATIONS

5.1 It is considered best practice for organisations to follow cyber security risk mitigation advice from the National Cyber Security Centre (NCSC).

6. FINANCIAL IMPLICATIONS

6.1 There are no financial implications.

7. ENVIRONMENTAL IMPLICATIONS

7.1 There are no environmental implications.

BACKGROUND PAPERS

Annual Report of the SIRO

PHIL LOACH
CHIEF FIRE OFFICER