Risk and Enterprise Resilience Policy

Contents

1 Introduction and definitions

1.1 The Risk and Enterprise Resilience Policy (the Policy) details De Montfort University's (the University's) risk and enterprise resilience management framework and associated governance structure. The Policy sets out the University's approach to *enterprise resilience* in order to best achieve its strategic objectives and to ensure the continuity of business-critical activities.

1.2 The Policy will be referred to:

1.2.1 By any member of staff involved in making decisions that could have a material impact on the University's resources;

1.2.2 For the risk management framework (the Framework);

1.2.3 For the risk and enterprise resilience governance architecture; and

1.2.4 For the University's approach to enterprise resilience, which ensures threats to strategic objectives and business-critical activities are appropriately managed.

1.3 The Policy uses the following definitions when referencing risk and enterprise resilience:

1.3.1 *Risk*: The threat or possibility that an action or event will adversely or beneficially affect an organisation's ability to achieve its objectives.

1.3.2 *Enterprise Resilience*: The ability of an organisation to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper. Resilience encompasses proactive measures to reduce a likelihood of occurrence (e.g., risk management) and reactive measures to reduce impacts if risks come to fruition (e.g., business continuity).

1.3.3 *Business Continuity*: The capability of an organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

2 Scope

2.1 The Policy focuses on the overall enterprise resilience of the University, concentrating on key risks that threaten the University's strategic objectives and business-critical activities. It ensures that emerging risks are escalated from business units (e.g. Faculties and Directorates) providing insight to the overall risk landscape.

2.2 The Policy does not reference day-to-day operational risk, although it is recognised that there is an overlap. Further policies explore the management and governance of risks associated with day-to-day Health and Safety (see the Management of Health and Safety Policy). The Policy does however include information about the escalation of operational risks if they were to have a significant impact on the University, or in the delivery of strategic aims and objectives.

3 **Principles**

3.1. The following principles provide the University's overarching approach to risk and enterprise resilience management. These principles shape and define the Policy to ensure a fit-for purpose, clear, and flexible approach to risk and enterprise resilience at the University.

Principle 1: Governance architecture

3.2. The University will apply a strong governance structure to prepare for and reflect on risk and enterprise resilieie-0.002 Tc 0.003 Tw 2.28 0 Td6.66rie (e r)2 (e)01 Tw [l (e r)2 (e) a1 (ng appr)-1 (ol

Audit Committee

- Strategic risks have suitable levels of mitigation and control, in line with the risk appetite and tolerance levels;

- The levels of resilience of the University's key business critical activities are in accordance with the risk appetite and tolerance level; and

- That the University's crisis management plan is effective and fit for purpose.

3.10.8. Be a forum for emerging risks that exceed risk appetite and tolerance levels, ensuring appropriate resilience and levels of control and mitigation are in place by:

- Agreeing the prioritisation of risks brought to its attention;

- Selecting the appropriate risk controls or treatment plan if further control is required; and

- Providing direction to ensure controls and treatments are carried out.

3.11. Faculties and Directorates have a key role to support Principle 2 through:

3.11.1. Utilising the Framework to ensure that risks to local strategic objectives are effectively identified, assessed and monitored;

3.11.2. Providing assurance to Risk Management Committee and University Leadership Board regarding the effectiveness of their risk management through established performance review mechanisms; and

3.11.3. The escalation of risks where either the risk exceeds appetite or tolerance, or that are outside local control.

Principle 3. Risk ownership

3.12.

- The ability to track and audit changes to risks and risk levels; and

- Evidence that mitigating actions are being carried out and are effective.

4.1.3   To have explicit and frequent conversations about risk and enterprise resilience, whether in specific fora such as the Risk Management Committee, or in other University committees or boards;

4.1.4   To capture key discussions about risk acceptance (e.g., through committee minutes); and

4.1.5   To demonstrate what is in place to respond to significant risks and identify gaps in our response plans.

5   Reporting

5.1   Risk and enterprise resilience will be reported at least biannually. This should be aligned to existing reporting processes, via Audit Committee to the Board of Governors.

6   Monitoring and review

6.1   The Policy will be reviewed annually by the Risk Management Committee each September in conjunction with a review of all key corporate risks. Any changes will be recommended to the University Leadership Board, Audit Committee and Board of Governors.

Appendix A: Risk and Enterprise Resilience Management Framework

Figure 1: Risk and Enterprise Resilience Management Framework