DE MONTFORT UNIVERSITY LEICESTER

Strategic Planning Service

Risk and Enterprise Resilience Policy

December 2015
Revised October 2019

Contents

1 Introduction and definitions 3
2 Scope 3
3 Principles 4
4 Documentation 8
5 Reporting 9
6 Monitoring and review 9
Appendix A: Risk and Enterprise Resilience Management Framework 10

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;

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 resilience. This is achieved by:

3.1.1 Assigning and aligning responsibilities for individuals and committees, providing accountability for risk and enterprise resilience management across the University. This includes the responsibilities required of the Board of Governors.

3.2.1. Integrating risk management and controls within existing systems and processes.

3.2.2. Facilitating the assessment of risk and providing appropriate responses to emerging risks (including mitigation) outside of risk appetite.

3.2.3. Providing assurance regarding the extent of compliance with the Policy.

Governance architecture in practice

3.3. The University's risk and enterprise governance architecture ensures there are clear lines of accountability, communication and the permeation of decision-making across different hierarchical layers. The expectation of individual committees is detailed below.

Board of Governors

3.4. The Board of Governors will:

3.4.1. Set the tone and embed the culture of risk and resilience management across the University.

3.4.2. Approve the appropriate risk appetite or exposure for the University.

3.4.3. Actively participate in major decisions affecting the University's risk profile or exposure to risk.

3.4.4. Monitor the management and implementation of the Policy ensuring that significant risks are addressed to reduce the likelihood of adverse events occurring.

3.4.5. Satisfy itself of the effectiveness of the University's risks and enterprise resilience management.

Audit Committee

3.5. Audit Committee will:

3.5.1. Consider risk alongside performance management bi-annually, paying particular focus to changes to the University's risk landscape, seeking management representation in respect to risk responses.

3.5.2. Provide assurance to the Board of Governors, by informing them about the University's approach to risk and resilience management through, among other means:

- Directing internal auditors to conduct reviews of the risk and resilience management process.
- Ensuring external auditors plan to satisfy themselves on the adequacy of risk and resilience management.
- Reviewing periodically subsidiary risk registers, business continuity plans, major incident plans, and specific risk assessments (e.g. for major capital projects, reorganisations or new Directorate or Faculty strategies).
- Requesting that external auditors contribute to the annual review of effectiveness and report to the Committee, as required.
- Seeking assurances from key committees, such as Executive Board and the Risk Management Committee. By requesting representation from risk owners, departmental and functional heads.

Executive Board

3.6. Executive Board, supported by the Risk Management Committee, will play a key role in ensuring that the University's Framework is implemented and adhered to.

3.7. Executive Board will provide assurance to Audit Committee on the effectiveness of the University's risk management.

Principle 2: The risk and enterprise resilience framework

3.8. The University's strategic aims and objectives drive the risk and enterprise resilience of the organisation. This is achieved by:

3.8.1. Ensuring a focus on risks that threaten the University's business model and strategic aims.

3.8.2. Establishing key operations and the corresponding institutional appetite for risk for these areas.

3.8.3. Strengthening the connection between business continuity and crisis management as key aspects of enterprise resilience.

3.8.4. Scoping internal and external factors to identify changes to the risk landscape.

The Framework in practice

3.9. Appendix 1 illustrates the mechanisms and structure of the Framework. The Framework coordinates the University's approach to managing risk through identification, assessment, treatment, monitoring and communication. The Framework ensures there is:

3.9.1. A clear line of responsibility and accountability of individual officers and committees for risk and resilience management.

3.9.2. A regular review of risk which considers external and internal influences and impacts.

3.9.3. A clearly defined set of risk appetite and risk criteria (or threshold) statements, and that these are directly linked to business-critical process and strategic objectives.

3.9.4. Appropriate escalation routes to report emerging risks (including those which breach risk appetite), triggering escalation from local to strategic levels and appropriate response mechanisms.

3.9.5. A strong relationship between business continuity, crisis management and risk management.

3.9.6. Assurance regarding the extent of compliance with the Policy and review of the effectiveness of the management framework to Executive Board, Audit Committee and the Board of Governors.

3.10. Principle 2 is supported through the establishment of the *Risk Management Committee*. The Risk Management Committee will:

3.10.1. Implement the University's Framework. It will provide assurance to Executive Board that risks at all levels are suitably identified, monitored and controlled.

3.10.2. Link the management of risk firmly to the strategic and business planning processes of the University.

3.10.3. Set the risk appetite for the University, and associated criteria for risk escalation.

3.10.4. Satisfy itself that strategic risks have suitable levels of mitigation and control, in line with the risk appetite.

3.10.5. Ensure that risk management remains a dynamic and business-focused process.

3.10.6. Continuously monitor the development of the University's risk management strategy, and where appropriate, to instigate changes in process and procedure to ensure that it remains fully fit for purpose.

3.10.7. Be a forum for emerging risks that exceed risk appetite levels, ensuring appropriate 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;
- Providing direction to ensure controls and treatments are carried out.

3.10.8. Agree the priorities for and planning direction of the University's business continuity planning to ensure that all key business critical activities are protected.

3.10.9. Satisfy itself that the University's crisis management plan is fit for purpose.

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 Executive Board regarding the effectiveness of their risk management through established performance review mechanisms.

3.11.3. The escalation of risks where the risk exceeds appetite and that are outside local control.

Principle 3. Risk ownership

3.12. Ownership and accountability are fundamental to the reporting and mitigation of risks. This is achieved by:

3.12.1. Establishing and empowering risk owners to be accountable for risk and resilience across the University.

3.12.2. Facilitating the identification, analysis and evaluation of risks, with a focus on those that can have significant impact on the University's business needs.

3.12.3. Ensuring appropriate responses to risk within the established boundaries for risk-taking are applied.

3.12.4. Establishing a culture of monitoring and evaluation of the effectiveness of risk treatments.

<u>Risk ownership in practice</u>

3.13. Risk owners will:

3.13.1. Manage risks that threaten the University's strategic objectives and associated key performance targets (KPTs). They have a duty to ensure that risks have been appropriately assessed and that mitigations and controls are in place in accordance the University's risk management procedures.

3.13.2. Proactively and continuously scope internal and external influences (including emerging risks from key business areas) to review and update risk scores, mitigations and controls as appropriate.

3.13.3. Escalate risks to the Risk Management Committee when emerging risks fall outside the University's risk appetite.

3.13.4. Consider local risks which align to their thematic area, and where appropriate incorporate these risks into their consideration of the strategic risk landscape.

3.13.5. Work with appropriate Faculties and Directorates to utilise the Framework to ensure that significant risks that impact on local and strategic objectives are effectively identified, assessed, and monitored.

3.14. Those accountable for business-critical activities will:

3.14.1. Utilise the Framework to ensure that significant risks to these activities are considered and mitigated against through business continuity and crisis management plans.

3.14.2. Escalate risks outside risk appetite to the Risk Management Committee as appropriate for consideration and to trigger response mechanisms to further mitigate the risk as necessary.

4 Documentation

4.1 Documentation should be kept practical, relevant. This is best achieved by integrating with existing reporting mechanisms. However, the documentation must be meaningful and support the risk and resilience management process. In terms of the balance it is important that:

4.1.1 Risk management documentation consists of a strategic risk register, and local risk registers at Faculty and Directorate level, supported by minutes of groups reviewing risk management.

4.1.2 Documentation supporting risk and resilience management is clear to all concerned, with:

- A common format for risk and resilience documentation;
- A common assessment and scoring methodology;
- The ability to track and audit changes to risks and risk levels;
- Evidence that mitigating actions are being carried out and are effective.

4.2 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.

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

4.4 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 in a biannual Risk and Performance Report. 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 Executive Board, Audit Committee and Board of Governors.

Appendix A: Risk and Enterprise Resilience Management Framework

Figure 1: Risk and Enterprise Resilience Management Framework