**A close-up of a logo

Description automatically generated**

**Risk Management Policy**

|  |  |
| --- | --- |
| **Academic Board Approval** | 6 March 2024 |
| **Audit Committee Approval** | 18 March 2024 |
| **Board of Governors Approval** | 22 March 2024 |
| **Lead:** | University Risk and Compliance Analyst |
| **Date of next review:** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Amendment History** | | | |
| Version | Amendments | Reason | |
| 1.1 | Purpose and scope have been combined and simplified | To aid understanding for readers |
| 1.1 | Amendment to section 5 risk appetite and tolerance statement | To further explain appetite and tolerance approach |
| 1.1 | Section 6 – Risk analysis added and removal of Risk Management plan. | To aid understanding of risk scoring and mitigation. |
| 1.1 | Section 7 – Roles and responsibilities have been amended | To reflect the current roles and responsibilities of staff |
| 1.1 | Change of job title from Risk Manager to Risk and Compliance Analyst throughout the policy | At the request of auditors and to ensure accuracy. |
| 1.1 | Risk scoring matrix included within the policy document (Appendix A) | To provide readers with the risk scoring matrix to aid understanding |
| 1.1 | The risk appetite and tolerance statement has been removed and will be presented as a separate document on an annual basis | The risk appetite and tolerance statement needs to be reviewed annually whereas the policy is reviewed every three years |

# Purpose and scope

* 1. The purpose of this policy is to outline a consistent approach towards risk across the University, it defines the responsibilities of risk managers, owners and the Board of Governors and provides risk assurance and management process.
  2. Cardiff Met’s risk management policy is designed to:
* minimise the likelihood and impact of risks; and
* maximise the likelihood and benefit of taking opportunity risks.  
  1. All risk management activity, protocols, processes, procedures, and structures required to manage risks relating to health, safety and wellbeing within the workplace are detailed within the University Health and Safety Policy.
  2. This Policy does not apply to Cardiff Met Students’ Union.

# Definitions

* *Organisational risk*: the combination of the likelihood and impact of an event which, should it occur, would have an effect on the achievement of Cardiff Met’s academic and business objectives or operations.
* *Risk appetite: t*he nature of risk, in a broad strategic sense, that Cardiff Met is prepared to seek, be exposed to or to tolerate.
* *Risk tolerance:* Risk tolerance is the level of risk that the University can accept per individual risk. It is accepting the outcome of a risk should it occur and having the right controls in
* *Risk likelihood:* refers to the chance of the risk materialising.
* *Risk impact:* the adverse effect that may occur due to exposure to the risk.
* *Risk mitigation:* any process, policy, practice, or other conditions and/or actions which maintain or modify the risk.
* *Risk proximity: t*he period of time before the risk might have an impact on the University.

# Policy Statement

* 1. Risk management should enhance strategic planning and prioritisation, assist in achieving objectives and strengthen the ability to be agile to respond to challenges. It is an integral part of the management of the University, its Schools, professional services, and the projects run at all levels across the institution, helping to ensure objectives are met, improve service delivery and achieve value for money.
  2. The Board of Governors, working collectively with the Executive, has ultimate responsibility for the University’s management of risk. It acknowledges that risk can never be eliminated and recognises the value for Cardiff Met in pursuing innovative and ambitious goals which have high potential rewards, but which must often necessarily entail a greater exposure to inherent risk.
  3. The University is committed to ensuring that there is a proactive and effective system for managing and monitoring the organisational risks it faces in delivering its ambitions.
  4. The University, in laying out its strategic aims and objectives, will ensure that these are appropriately and responsibly aligned with and monitored in accordance with the University’s risk appetite and risk tolerances.
  5. This Policy complies with the Governance Code of Practice and General Principles established by the Committee of University Chairs, and the requirements specified by HEFCW its Financial Memorandum and Financial Management Code.

# Approach

* 1. The following principles underpin the University’s approach to organisational risk management:

1. ***Integration*:** Risk management processes will be appropriately integrated with the University’s strategic planning processes and the University risk appetite and tolerance statement.
2. ***Alignment with objectives*:** Organisational risk management will be aligned with the University’s strategic objectives and the University’s risk appetite and tolerance statement.
3. ***Risk imagination*:** Managers will have the discretion to define organisational risks, thereby helping to ensure a broad organisational ‘risk imagination’.
4. ***Risk owners and managers*:** Organisational risks will each have an individual, named, risk owner (executive level) and risk manager identified.
5. ***Indicators*:** Valid and reliable data will be utilised to provide early indications of changes in the institution’s risk exposure.
6. ***A living document:*** Risk registers are a living document and help decision-making process.
   1. There are significant advantages to be gained from engaging organisational risk management as part of a holistic approach which integrates with strategic planning and performance management. In taking this approach we aim to:
7. Protect value by minimising losses, adverse events and reputational damage;
8. Protect and enhance value by strengthening strategy formulation and objective setting, thereby increasing the likelihood of their achievement;
9. Protect and enhance value by strengthening strategy implementation and providing a more reliable basis for proactive decision-making and resource allocation;
10. Enhance governance.
    1. The mechanisms through which the University will manage its risks include:
11. Ensuring that an organisational risk assessment is included as part of its normal due diligence processes where decisions have a significant reputational or financial risk.
12. Maintaining a University risk register and local divisional risk registers (i.e. at the level of individual Schools and Professional Services).
13. The University risk register and accompanying risk report will be presented through the University committee cycle for review and approval on a termly basis.

# Risk Appetite and Tolerance

* 1. The University will accept a level of risk proportionate to the expected benefits to be gained, and the scale of likelihood of damage. The risk appetite will be aligned with the University’s aims and strategic direction. The University has a higher appetite for risk in the context of strategic development activities, new funding opportunities, improving student experience, innovation, academic freedom, and academic expression. The University has a low appetite for risk where there’s a likelihood of serious reputational damage; significant lasting damage to its research and teaching; cyber security; significant financial loss; harm to staff, students, or visitors; illegal or unethical activity; and regulatory compliance.
  2. This will be articulated within a University Risk Appetite and Tolerance Statement agreed annually at the beginning of each academic year by the Board of Governors. The Statement will include:

1. The assignment of a risk appetite classification to key risk areas. Key risk areas will be determined on an annual basis and will be aligned with the University’s aims and desired future state or direction.
2. The specification of corporate level Risk Tolerances which will include both quantitative and observable qualitative tolerances.
   1. When setting the risk appetite, the University will assign one of the following classifications to each key risk area:
3. ***Averse*** – avoidance of risk and uncertainty is key.
4. ***Cautious*** – preference for safer options that have a low degree of inherent risk and may only have limited potential for reward.
5. ***Open*** – willing to consider all potential options and choose the one most likely to result in successful delivery, while also providing an acceptable level of reward and value for money.
6. ***Hungry*** – eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk.
   1. The University’s risk appetite:

* is related to the pursuit of the University’s objectives and its strategic direction as outlined within the strategic plan;
* is a fundamental part of the University’s overall governance arrangements;
* guides the allocation of resources at a strategic level;
* influences managers’ attitudes to risk and their objectives; and
* drives the management of the University’s risks.
  1. The University makes a clear distinction between having an appetite to consider and adopt different options to achieve its objectives, and the level of risk appetite that is acceptable when it is implementing any chosen option.
  2. The Board of Governors may agree specific Risk Tolerances. These represent an acceptable level of variation relative to the achievement of a specific objective.
  3. The University Risk Appetite and Tolerance Statement can be found at Appendix A.

# Risk analysis

* 1. A risk is assessed and analysed by using a risk scoring matrix which can be found at Appendix A. Using a scoring matrix standardises scoring and helps to limit subjectivity. The University uses a 5x5 system for scoring matrix:

1. ***Impact:*** A score of 1 to 5 is applied according to the severity of the impact if the risk was to materialise. (The impact scoring guidance can be seen in Appendix A).
2. ***Likelihood:*** A score of 1 to 5 is applied according to the probability of the risk happening. (The likelihood scoring guidance can be seen in Appendix A).
3. ***Gross*** ***score:*** The likelihood score is multiplied by the impact score to give a gross risk score of 1 to 25. The risk score can be plotted on the heat map (Appendix A) to determine the severity of the risk and provide the risks status.
   1. Following a risk’s gross scoring, the risk owner should decide on appropriate controls for mitigation. The University uses the following options:

* ***Treat****:* Take action to reduce the risks likelihood and/or impact by implementing mitigating controls.
* ***Tolerate****:* Accept the risk, making sure it is monitored. The current risk exposure is deemed acceptable.
* ***Terminate****:* Exit the activities causing the risk as the exposure and risk to the University is deemed unacceptable.
* ***Transfer****:* The risk likelihood and/or impact is reduced by transferring the risk to another party.
* ***Risk mitigation:*** Control measures are put in place to minimise the impact of the risk or the likelihood of the risk occurring. The risk is then re-scored using the risk scoring matrix and a residual risk score is recorded.
* ***Proximity:*** The University assesses the expected lifecycle of the risk to determine when the risk is expected to occur. The University uses the following options:
  + ***Short term:*** The risk is likely to occur within 6 months.
  + ***Medium term:*** The risk is likely to occur within 6 to 12 months.
  + ***Long term:*** The risk is likely to occur after 12 months.

# Roles and Responsibilities

## Board of Governors

* 1. The Board of Governors is responsible for determining the overall direction for the management of risk within the University and having oversight of risk management activity and the risk management systems. This includes:

1. Approving the Risk Management Policy.
2. Determining and reviewing the University’s risk appetite and University level risk tolerances.
3. Ensuring that both the University’s long-term academic and business plans, and its actions in attaining or delivering those plans, are in line with the approved Risk Appetite and Tolerances.
4. Approving major decisions affecting the University’s risk profile or exposure, particularly those that may risk the good name and values of the University and its sustainability.
5. Receiving and challenging reports on matters of institutional risk and the management thereof.

## Audit Committee

* 1. The Audit Committee is responsible for keeping under review and evaluating the effectiveness of the management of risk within the University and the effectiveness of its risk management system. This includes:

1. Considering revisions to the Risk Management Policy prior to seeking the approval of the Board of Governors.
2. Ensuring that risk management is being carried out effectively at all levels of the University.
3. Receiving and evaluating updates from the University risk register to enable it to assure itself that there are appropriate linkages between the University’s organisational risks and its assurance activities, including internal audit.
4. Receiving and evaluating feedback from assurance bodies, including from external auditors, on the operation and effectiveness of the University’s management of risk.
5. Receiving and considering termly reports on risk from the University Risk and Compliance Analyst.
6. Conducting deep dives into the management of risks in specific areas as deemed appropriate.

## Academic Board or Management Board

* 1. Academic Board acts as the University’s Risk Management Committee and as such is responsible for ensuring the effective implementation of the University’s Risk Management Policy. This includes:

1. Ensuring that there is a co-ordinated approach between the management of risk and the University’s strategic decision-making and planning, and that these are consistent with the University’s Risk Appetite and Tolerance Statement.
2. Reviewing University level risks on a termly basis and, where required, making recommendations to ensure their effective management.
3. Making recommendations to ensure the effective management of any risks that are in breach of the Risk Appetite and corporate level Risk Tolerances.

## Level 2 Staff

* 1. Led by the Vice-Chancellor, Level 2 staff are responsible for:

1. Raising the profile of and providing leadership on organisational risk management best practice within their portfolio and across the University.
2. Ensuring that objectives are set, and that their delivery is conducted, in accordance with the University’s Risk Appetite and Risk Tolerances.
3. Reviewing any Divisional level risks escalated to them and making recommendations for their management where necessary, and/or ensuring that mitigating action is undertaken.
4. Scrutinising the University risk register on a termly basis prior to Academic Board consideration.
5. Allocating sufficient resources within their portfolio to adequately manage organisational risks and ensure managers are managing risks in accordance with the Risk Management Policy.
6. Undertaking training and development activities associated with organisational risk management.
7. Where required, acting as risk owners for organisational risks taking on the responsibilities listed in paragraph 7.7.

## University Risk and Compliance Analyst

* 1. The University Risk and Compliance Analyst is responsible for:

1. Leading on the development, communication, implementation and review of the University’s Risk Management Policy.
2. Leading on the co-ordination of organisational risk management activities.
3. Preparing reports for boards and committees on organisational risk management matters and institutional level risks.
4. Facilitating communication on risk management matters between Academic Board, Audit Committee, the Board of Governors and its other relevant Committees, the Executive and other stakeholders.
5. Conducting regular ‘top-down’ reviews of organisational risks as deemed necessary, with an emphasis on reviewing the effectiveness of the mitigating controls for institutional level risks.
6. Developing and delivering specialist organisational risk management training, support and guidance to University staff.

## Risk Division Managers

* 1. The University’s Risk Division Managers, i.e. Deans of School, Directors/Heads of Professional Services, Project and Programme Managers, Secretaries of Subsidiary Companies are responsible for:

1. Raising the profile of, and providing leadership for, organisational risk management for those staff within their management remit.
2. Ensuring that objectives are set, and that their delivery is conducted in accordance with, the University’s Risk Appetite and Risk Tolerances.
3. Where required, acting as risk owners for organisational risks taking on the responsibilities listed in para. 7.7, including acting as risk owners for cross-cutting risks shared across risk divisions.
4. Allocating sufficient resources to manage any organisational risks as required, and ensuring staff are operating in accordance with the Risk Management Policy.
5. Providing adequate information in a timely manner to the University Risk and Compliance Analyst in relation to risk management.
6. Undertaking and engaging with training and development activities associated with organisational risk management.

**Risk Owners**

* 1. In relation to each risk they are assigned, the Risk Owner is responsible for:

1. Determining an effective and proportional management or treatment plan, including control measures, to manage the likelihood and/or impact of the assigned risk being realised, to at least within the University’s risk appetite and risk tolerances.
2. Reviewing each assigned risk on a termly basis.
3. Monitoring the implementation and/or effectiveness of all management or treatment plans, including their control measures, on an on-going basis.
4. Reporting to the University Risk and Compliance Analyst on the management of their assigned risk where required to do so.
5. Receiving and giving due consideration to reports from the University Risk and Compliance Analyst or assurance providers on the management of their assigned risk.

# Contacts

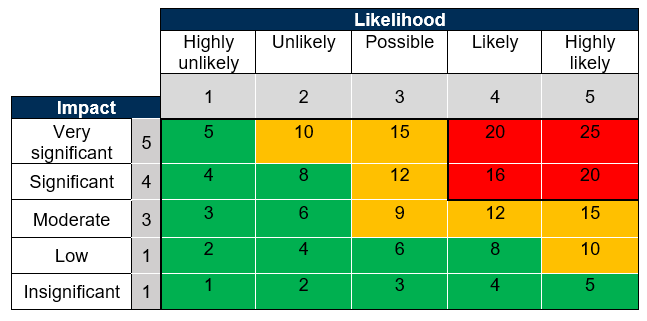
* 1. Queries regarding this Risk Management Policy should be directed to the Risk and Compliance Analyst in the Strategy, Planning and Performance team.

**Review**

* 1. This Policy will be reviewed every three years.

**Appendix A: University risk scoring matrix**

All University risks are scored using the Risk Scoring Matrix as laid out below. This Risk Scoring Matrix shows, via shaded bands overlaid onto it, both the University’s Risk Appetite classifications and its overall risk tolerance threshold.



|  |  |  |
| --- | --- | --- |
| The score should reflect the higher of the financial value, the proportion of the institution affected, or the degree to which the whole University is affected. | | |
| 5 | Very significant | • The incident would significantly affect the operation, reputation or strategic direction of the whole University. • The financial impact would cost the University => £5M.  • Fatalities caused by University actions/inactions. • Threats of targeted terrorist actions against groups or specific threat to University as a whole or widespread and extreme dissatisfaction with protests • Quality of academic provision seriously jeopardised and long term viability undermined • Long term/permanent loss of use of entire sites • Formal external regulatory investigation involving high profile criminal allegations against management and threat of imprisonment or withdrawal of status or imposition of sanctions resulting in forced termination of mission critical activities. |
| 4 | Significant | • The incident would affect the operation, reputation or strategic direction of the whole University but not significantly; or • The incident would significantly affect the operation, reputation or strategic direction of more than one College or Professional Service department (but does not affect the whole University). • Financial impact => £250K <£5M • Major life changing injury (e.g. paraplegia) or threats to kill or maim individual in connection with University activity • Spread of life-threatening disease • Disruption which has a medium to long term affect adverse on business critical activity or loss of key student markets • Formal external regulatory investigation into organisational practices with potential for suspension of significant elements of University operations or fines. |
| 3 | Moderate | • The incident would affect the whole University to a some extent; or • The incident would significantly affect the operation, reputation or strategic direction of several Schools (possibly a whole College) or Professional Services department. • Financial impact => £50K < £250K. • Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) major incidents or injuries or cases of life threatening disease. • Disruption which compromises ability to undertake business critical activity within required timescales. • Student recruitment markets adversely affected. • Case referred by complainant to regulatory authorities and potential for regulatory action with more than localised effect or fines. |
| 2 | Low | • The incident would affect the operation, reputation or strategic direction of a small number of Schools or Professional Services departments but would have little or no effect on other areas of the University. • Financial impact <£50K • RIDDOR minor injuries or stress on individual or morale of small group damaged • Disruption which interferes with business activity – tasks are made more difficult but are not impossible to complete within required timescales • Fines or claims brought. |
| 1 | Insignificant | • The incident would affect the operation, reputation or strategic direction of a single School or Professional Services department but would have little or no impact on other areas of the University. • Financial impact negligible. • Minor dissatisfaction of an individual or small group. • Disruption which interferes with non-business critical. • Regulations breach that results in minimal or no damage or loss. |
|  | | |
|  | | |
| **Likelihood** | | |
| 5 | Highly likely | It is expected that this risk will materialise at least once within the next two years, or has already materialised. A risk of this kind is likely to be reflected as a contingency or directly in the University’s budgets and medium-term financial plan. |
| 4 | Likely | It is reasonable to assume that this risk will materialise at some point (possibly once or twice within the next five years). |
| 3 | Possible | It is reasonable to assume that the risk will materialise once or twice within a period of five to ten years. |
| 2 | Unlikely | There is a low probability of the risk materialising (there is a possibility that this could happen at least once within a period of five to ten years, but it is considered unlikely). |
| 1 | Highly unlikely | There is a very low probability of the risk materialising (this is not expected to happen but it may do in exceptional or unusual circumstances - it has been known to happen at this or another University once in the past). |

|  |  |
| --- | --- |
| **Risk Appetite** |  |
| Averse | Avoidance of risk and uncertainty is key. |
| Cautious | Preference for safer options that have a low degree of inherent risk and may only have limited potential for reward. |
| Open | Willing to consider all potential options and choose the one most likely to result in successful delivery, while also providing an acceptable level of reward and value for money. |
| Hungry | Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk. |

|  |  |
| --- | --- |
| **Risk Proximity** |  |
| Short-term | If it happens it is likely to happen within 6 months |
| Medium-term | If it happens it is likely to happen within 6-12 months |
| Long-term | If it happens it is likely to happen after 12 months |