Risk Management Policy

Principles

- Through a process of Risk Management, the University seeks to reduce the frequency and impact of Adverse Events that may affect the achievement of its objectives. In particular, Risk Management aims to protect people, quality, reputation, assets and finance.
- To achieve maximum effect, the University’s Risk Management is centrally co-ordinated, proactive and integrated into normal management and planning processes. Although not seeking formal certification, the University recognises the benefits of ISO 31000, which outlines a series of risk management principles, describes the implementation of a risk management framework and explains how to implement risk management processes.
- Whilst the University is committed to avoiding, controlling or mitigating Adverse Events, it continues to value innovation and seeks to maximise opportunities. The institution explicitly recognises that excessive Risk aversion would be detrimental and will, where necessary to achieve its aims, embrace a degree of Risk. The Risk tolerance of the University is ultimately determined by the University Court and, in particular, by its Audit & Risk Committee, guided by the Risk Management Group and Heads of Schools and Units.

Definitions

- “Risk” - a description of the uncertainty associated with the potential failure of processes which are designed to prevent a foreseeable Adverse Event, or to respond adequately to its potential impact. Risk can arise either from internal weaknesses or from external threats.
- “Adverse Event” - the realisation of a Risk, commonly experienced as accidents, breakdowns, errors or omissions.
- “Risk Management” - the identification and evaluation of Risk, followed where necessary by measured application of resources, in order to reduce the frequency or impact of each Risk to a degree deemed tolerable
- “Risk Register” – a collection of data regarding key Risks, including Risk description, Risk assessment, control measures and actions required to further mitigate the impact and/or frequency. The Risk Register is the primary means by which Risks are regularly monitored and Risk assurance reports are provided to the Audit & Risk Committee.

Framework

- The University has a formal planning process to agree School and Unit objectives and resource allocation. Within this process, Heads of Schools and Units are required to identify Risks which may threaten achievement of their objectives. These are cross-checked against the Risk Register to identify new Risks and to improve the evaluation of existing Risks.
- The University has well-established processes to provide oversight of learning and teaching and implementation of the University’s quality enhancement strategy. Regular updates are provided via the Risk Register by the Proctor and the Academic Assurance Group.
Framework (cont’d)

- The University has a programme for continuous improvement of crisis management capability and creation of business continuity plans. Continuity planning incorporates business impact analyses and the outputs are cross-checked against the Risk Register and against the insurance programme, as are the outcomes from crisis management exercises.

- The University has a comprehensive insurance programme which is maintained by experienced staff, with the assistance of qualified and independent external Advisers. Insurance is treated as a key Risk control measure and the Risk Register reflects coverage provided by the insurance programme.

- The University employs experts in contract negotiation, backed by external legal advice where necessary, focusing particularly on research contracts. Where possible, we aim to mitigate uninsured risks which are contractually transferred to the University, or otherwise take informed decisions as to whether the residual risk is tolerable.

- The University has health and safety, environmental, food safety and fire safety management programmes which have their own governance mechanisms. Upon referral from topic experts in those areas the Risk Register hosts data concerning any associated Risk which may be intolerable or which requires input from outwith the normal topic boundaries. This is the exception rather than the rule.

- Projects in IT and Estates are managed using established methodologies, which explicitly consider Risk. The University also has a formal change management process to facilitate business transformation via major projects.

- The University has groups to manage Security and also Events co-ordination, with personnel from both of those groups sitting also on the Risk Management Group.

- The University has an incident reporting system for Adverse Events from which it aims to learn from experience by disseminating key learning points and actions in order to either prevent recurrence or better mitigate the adverse effects of such recurrence.

- Updates on Risk Register data are requested by the Risk Adviser from Risk and Action owners on a quarterly basis. Periodically, the Risk Adviser also schedules workshops with key Risk owners, such as the Proctor, VP Research, Director of Finance and Chief Information Officer in order to fully review their data and identify any new exposures.
Risk Management Policy

Responsibilities

- The Risk Management group performs a dual role, in that it takes an initial view on Risk tolerability prior to referral to the Audit and Risk Committee, but it also provides a forum for cross-disciplinary discussion of current and emerging Risk. The group has representation from senior staff drawn from Principal’s Office and certain Service Units. The Risk Management Group terms of Reference are contained in Appendix 1.

- The Audit and Risk Committee receives assurance reports on major Risks from the Risk Management Group. These Risks are escalated to the Audit and Risk Committee based upon an algorithm hard coded into the Risk Register. The Audit and Risk Committee may seek clarification from the Risk Management group based on the escalated Risks or on any other Risk-related information which comes before the committee.

- The Risk Adviser is responsible for maintaining the Risk Register, for ensuring that significant risks are recorded as and when they are identified and for providing guidance on risk assessment, proposed actions and risk control. The Risk Adviser will also deliver project risk management support as requested from any source within the University and any training requirements on risk management will be co-ordinated or delivered by the Risk Adviser. The Risk Adviser prepares quarterly and ad hoc reports from the risk register for issue to Risk Management Group, Audit & Risk Committee, and Risk and action owners.

- Risk and action owners are identified on the risk register and have responsibility for maintaining their data online within the system, or for liaising with the Risk Adviser in timely fashion to enable this task to be carried out on their behalf, and for ensuring that the details on the system provide a true reflection of the Risk.

Methods

- The University maintains a Risk Register database to record, report and manage key Risk-related data. All Risks recorded on the Risk Register are evaluated against their potential impact on the University’s strategic objectives and each Risk is mapped to one of the University’s eight formal Key Performance Indicators. This database is maintained by the Risk Adviser who also leads development of the system where required.

- The University deploys a variety of Risk analysis techniques tailored to the situation at hand, for instance those for “Fieldwork” (EHSS) and “Risk Assessment Protocol Following Student Misconduct Reports” (Student Services). The Risk Adviser carries out risk reviews upon request from management of any Unit or School, or upon instruction from the Risk Management Group.

- Guidance is provided by the Risk Adviser to staff directly involved in the formal Risk Management programme and, upon request, to any other staff or students with an interest in the topic area, in recognition of the daily role of all staff in managing risk, whether express or implied.

- The Risk Adviser produces template solutions for staff to use in the course of Risk Management activity including, but not restricted to: the Risk Register user interface; business continuity plans; crisis management checklists; hazard and operability studies; Risk assessment forms.

- Any member of staff accessing this policy and wishing guidance should contact the Risk Adviser who works within Environmental Health and Safety Services.
Risk Management Policy

Performance
- The University recognises the importance of setting appropriate performance benchmarks and uses a variety of techniques to gauge Risk Management performance, including: the occurrence of unforeseen events; internal audit reports; benchmarking against good practice from elsewhere; cost-effectiveness of the Risk Management programme; quality and timeliness of reporting to Audit and Risk Committee.

Interpretation
- The Risk Management Group shall be the arbiter for queries as to the meaning and application of this policy which cannot be resolved locally.

Dissemination
- This Policy is published on the University website.

Contacts
- Enquiries regarding this Policy can be directed to the University Risk Adviser.

Review
- This policy will be reviewed on or before 31 December 2017, and every two years thereafter.
Risk Management Policy – Appendix 1
Risk Management Group Terms of Reference

1. Remit

1.1 To support and advise the Audit and Risk Committee (hereafter known as the ‘ARC’) and through it Court, on the implementation and monitoring of the Risk Management Policy.
1.2 To identify and evaluate risks which are material to the wellbeing of the University, whether connected to specific short-term projects or to the regular business of the University.
1.3 To consider serious adverse events and/or direct any member of the Risk Management Group (hereafter known as the ‘RMG’) to further investigate such events and report back to the RMG.
1.4 To monitor at each meeting the exposure presented by those risks designated for ‘escalation’ to the ARC, and on a rolling basis all other risks identified within the risk register.
1.5 To contribute to raising awareness of risk management generally across the University and to maintaining the profile of risk management.
1.6 To receive reports, either verbal or written, from the Security and Strategy Group and the Events Co-ordinating Group relative to areas of concern and risk mitigation.
1.7 To co-operate with Internal Audit who will periodically review the effectiveness of the RMG.

2. Composition

2.1 The RMG shall be comprised as follows: VP Governance; Quaestor; Chief Legal Officer; Dean of Science; Dir of Corporate Communications; Dir of Student Services; Dir of RBS; Dir of Estates; Security Manager; Chief Information Officer (CIO); Associate CIO; Dir of EHSS; Risk Adviser
2.2 The RMG shall be chaired by VP Governance, in whose absence Quaestor, in whose absence Chief Legal Officer or Risk Adviser.
2.3 The members of the RMG shall be appointed by VP Governance or Quaestor. Additional attendees may from time to time be invited to any meeting by VP Governance or Quaestor relative to agenda items which may require specific expertise beyond normal RMG membership.
2.4 Any member of Principal’s Office, any Director or any Dean may at their discretion send in his/her place a delegate to any meeting of the RMG if they cannot personally attend.
2.5 The RMG is authorised to obtain information from University employees or external professional advisers as required to fulfil its remit.

3. Meetings

3.1 The RMG will meet four times per annum, and VP Governance will report to the subsequent ARC by submitting a quarterly Risk briefing, which will be prepared by VP Governance and Risk Adviser. In the absence of VP Governance, Quaestor will assume responsibility for ARC reporting.
3.2 Papers will normally be circulated to members of the RMG at least five working days in advance of the meeting although late papers may be issued up to and including the day of the meeting.
3.3 Four members of the RMG shall be a quorum, one of whom shall be appointed Chair by those present for the meeting should a permanent Chair not be present (see 2.2 above).
3.4 A formal minute of each meeting will be prepared by the Risk Adviser, and ratified by VP Governance and Quaestor, prior to submission for approval at the next meeting of the RMG.
3.5 The RMG may also function between meetings through correspondence and any decisions or issues arising should be notified at the next meeting of the RMG.

Date: 07/09/2015
Approving body: Audit and Risk Committee
Version number: 2015.01
Steward: Brian Kennedy, Risk Adviser