

## EDINBURGH NAPIER UNIVERSITY RISK MANAGEMENT POLICY

### Purpose

1. Risk Management is a fundamental aspect of good corporate governance and key to the successful delivery of business objectives. This Risk Management Policy forms part of the University's internal control and corporate governance arrangements.
2. Risk management informs strategic development through the identification and treatment of risk so that strategic objectives are more likely to be achieved, damaging events are avoided and opportunities are maximised. Good risk management increases the probability of success, and reduces the probability of failure and uncertainty of achieving the University's objectives.
3. The purpose of this risk management policy is therefore to set out the University's underlying approach to risk management and to document the roles and responsibilities of Court and its sub-committees, the University Leadership Team (ULT) and other key parties. It also outlines the main aspects of the risk management process, and identifies the main reporting procedures. It applies to Institutional, School, Professional Services Directorates and project risk management.
4. This policy will be reviewed annually and any changes to roles, titles or responsibilities will be updated as required.

### Scope

5. Risk Management can be defined as, *"a process which provides assurance that objectives are more likely to be achieved; damaging things will not happen or are less likely to happen, and beneficial things are more likely to be achieved"*.
6. Risk is commonly defined as the possibility that an action, event or set of circumstances will adversely or beneficially affect an organisation's ability to achieve its objectives. Risk exists as a consequence of uncertainty and is present in all University activities. The exposure is normally expressed in terms of failure to reach an objective and the operational, reputational and financial damage that may be incurred as a result.
7. Risk Management involves the planned and systematic approach to the identification, evaluation and control of risk. It is concerned with evaluating the measures an

organisation has in place already to manage identified risk and then suggesting actions that the organisation should take to control these risks more effectively. For threats, the outcome of risk management is the reduced likelihood (probability) of a risk occurring, or limiting the consequences (impact) should the risk occur, by implementing appropriate methods of control (risk mitigations).

8. At an institutional level, risks can affect either positively or negatively the University's ability to achieve its long term strategic aims and objectives, as outlined in both Strategy 2020 and the University's Corporate Plan.
9. At an operational level (Schools & Professional Services Directorates), risks can affect the successful delivery of operational plans and the subsequent achievement of academic and financial priorities which contribute to the delivery of the Corporate Plan and Strategy.
10. At a project level, risks can affect the successful delivery of the project's stated benefits by impacting the cost, timing and/or quality of outputs.
11. It should be noted that risk management is the responsibility of everyone at the University, and not just a small number of named individuals. The University maintains a register of top strategic risks, and all academic schools and service areas maintain operational risk registers that are integrated into the annual planning and budgeting process.

### **Overview of Approach**

12. The University's approach to risk management is guided by the following principles:
  - (i) The University Court has responsibility for the effectiveness of internal controls based on information and assurance provided by the Audit & Risk Committee;
  - (ii) Risk management is implemented as an integral part of University activities at all levels and is monitored by the Audit & Risk Committee;
  - (iii) Risks are identified, analysed and recorded as appropriate, normally within a risk register which scores the likelihood and impact of risks;
  - (iv) The management of risk will involve user-friendly language and University processes will be kept as simple and effective and possible;
  - (v) Deans of Schools and Service Directors are responsible for encouraging good risk management practice within their area. This includes the accurate and effective identification, mitigation and monitoring of operational risks;
  - (vi) The top corporate risks will be identified on an annual basis and will be closely monitored by ULT, the Audit & Risk Committee and University Court.

13. Risk management is undertaken as an integral part of both strategic and operational management:

- (i) At a strategic level, those risks considered to present the greatest threat to the University's attainment of its strategic and corporate objectives, will be considered, reviewed, identified and scored annually, and as part of the overarching planning and budgeting process. The Top Risks so identified will be recommended for approval by the Audit & Risk Committee to University Court. The Top Risk Register for the forthcoming academic year will be submitted for approval by University Court in June. Monitoring reports which track the effectiveness of internal controls and mitigating actions against the Top Risks are prepared by ULT and presented to the Audit & Risk Committee and University Court three times a year (December, March & May), with relevant risks also presented to Academic Board and Finance & Property Committee;
- (ii) Operational plans will include an assessment of the risks and mitigating actions associated with key planning objectives. These risks are collated, aggregated and form the University's operational risk register. Operational risks require to be reviewed regularly by local management teams (bi-monthly), and are reviewed bi-monthly at School Board meetings. Operational risks are formally reviewed bi-annually in February and November and reviewed by the Risk & Resilience Committee, which reports to ULT. There is a clear process for escalation as a result of this monitoring which is outlined under the "Management of Risk" section below.
- (iii) Risks must be identified and assessed as part of the business case for all new schemes, investments and projects informed by the risk appetite statement and tolerances approved by Court; once approved, risks must be reviewed regularly by the project board or similar governance committee.

### **Responsibilities and Accountabilities**

14. It is essential that all participants in risk management are aware of their roles in the overall process and their own responsibilities. The key responsibilities of each group/individual are outlined below:

#### *University Court*

15. The University Court has a fundamental role to play in the management of risk and in setting the overall tone and culture of risk management within the University. Their responsibilities include:

- (i) Approving the top corporate risks register on an annual basis;
- (ii) Determining the overall risk appetite of the University
- (iii) Determining what types of risk are acceptable and what are not;

- (iv) Approving major decisions affecting the institution's risk profile or exposure
- (v) Providing a strategic focus to the management of risk, ensuring that the identification of risk is integrated and aligned to key strategic objectives;
- (vi) Setting the standards and expectations of staff with respect to conduct and probity;

*Audit & Risk Committee*

Acting on behalf of Court, the Audit & Risk Committee will:

- (i) Recommend for approval to Court, the Top Risk Register;
- (ii) Monitor the management and mitigation of the Top Risk Register;
- (iii) Develop and recommend to Court appropriate statements of risk appetite;
- (iv) Review the integrity and effectiveness of the University's risk management framework, alerting Court to any emerging issues;
- (v) Satisfy itself that less significant risks are being actively managed, with the appropriate controls in place and working effectively;
- (vi) Annually review the University's approach to risk management and approve changes or improvements to key elements of its processes and procedures;
- (vii) Approve the internal audit plan, which is linked to the Top Risk Register;
- (viii) Review and advise the Court on the adequacy and effectiveness of risk management arrangements
- (ix) Produce an annual report for Court on the adequacy and effectiveness of the institution's risk management, control and governance arrangements.

*University Leadership Team (ULT)*

16. The role of the University Leadership Team is to:

- (i) Identify and evaluate significant risks faced by the University for consideration by Court via the Audit & Risk Committee, including escalating of Risks from the operational risk register as appropriate;
- (ii) Implement policies on risk management and internal control;
- (iii) Work with the University's appointed internal audit provider to develop the annual internal audit plan;
- (iv) Provide adequate information in a timely manner to Court, via the Audit & Risk Committee on the status of risks and control measures;
- (v) Regularly review the effectiveness of internal controls;
- (vi) Identifying and acting as risk owner for appropriate strategic risks;

*Senior Leadership Team (SLT)*

17. Deans of School and Service Directors are responsible for identifying, assessing and monitoring risks at a school and service level. They will:

- (i) Disseminate good and appropriate risk practice within their School/ Service;
- (ii) Identify, monitor and assess risk issues within their School/ Service;

- (iii) Report on risk and control issues in their annual Plan and monitor according to defined processes and frequencies;
- (iv) Escalate any risks which may have increased to a level where they may have strategic importance.

### **Risk Appetite Statement**

18. The overall appetite for risk has been defined by Court. It constitutes overarching, high level guidance from Court to staff indicating the amount and type of risk the University is prepared to tolerate in order to achieve its strategic objectives, outlining the areas where the University expects a conservative, compliance focussed approach to risk and areas where our strategy requires an innovative approach embracing a degree of risk to deliver the aspirations set out in the strategy. The statement is reviewed and approved by Court annually and is available on the risk management intranet site. [insert link]

### **Risk Management Framework**

19. The management of risk is supported by a system of internal control, and is closely related to the planning and budgeting process. This enables the University to respond to a variety of operational, financial, reputational and commercial risks. The elements of this system include:

#### *Risk Appetite Statement*

20. Overarching, high level guidance from Court to staff indicating the amount and type of risk the University is prepared to tolerate in order to achieve its strategic objectives, outlining the areas where the University expects a conservative, compliance focussed approach to risk and areas where our strategy requires an innovative approach embracing a degree of risk to deliver the aspirations set out in the strategy.

#### *Policies and Procedures*

21. Attached to significant risks are a series of policies that underpin the internal control process. The policies are agreed at the appropriate level of authority and are implemented and communicated by senior management to staff. Written procedures support the policies where appropriate.

#### *Planning and Budgeting*

22. The annual planning and budgeting process is used to set objectives, agree plans and allocate resources. Accurate risk identification and reporting forms an integral part of the operational planning and budgeting process where operational risk registers are created in conjunction with the development of School and Professional Service area plans.

### *Top Risks Register*

23. The University's register of top corporate risks, being those considered to present the greatest threat to the University's attainment of its strategic and corporate objectives, is compiled and developed by the University Leadership Team based on a review of aggregated operational risks and broader assessment of the risk environment concerning the University. This is reviewed and approved annually by the University Court, on the recommendation of the Audit & Risk Committee. Emerging risks which have been escalated from the operational risk register or have appeared in-year can be added throughout the year where necessary, upon recommendation of the Audit & Risk Committee in accordance with the monitoring and escalation process outlined later in this policy.
24. Monitoring reports on the University's Top Risks Register are submitted to both the Audit & Risk Committee and University Court three times a year (in December, March and May). Reports are also submitted to Academic Board and Finance & Property Committee for risks appropriate to their remits. Risks may also be reported on an exceptional basis, as required. For example, on risks associated with new projects or on emergent external risks.

### *Operational Risk Register*

25. Responsibility for risk identification, monitoring and reporting is devolved to Deans, Directors and Heads of Department who create operational risk registers in conjunction with the development of School and Professional Service area plans. In so doing will they will take account of the parameters and tolerances specified in the risk appetite statement.
26. Detailed Risk Guidance has been produced on the required approach to the definition (in terms of risk, cause and impact), classification, assessment, mitigation, monitoring and escalation of risks which identifies risk categories, provides an assessment likelihood and impact criteria matrix, scoring matrix and rating matrix to be used in conjunction with a standard Risk Matrix template. This guidance is reviewed and updated annually and circulated along with the Matrix.

### *Aggregation, Monitoring and Review of Operational Risks*

27. Schools and Departments are required to monitor and report on the management of their operational risks across the year which are aggregated and reviewed through the following mechanism:
- February/March: Operational risks identified and register entry completed in conjunction with the development of annual plans, through the planning and

budgeting process. Identified risks are aggregated, considered and reviewed by Risk & Resilience Committee and considered for referral to ULT/Audit & Risk Committee as appropriate.

- Bi-Monthly throughout year: Operational risks are included within regular finance and performance reporting packs and reviewed and monitored as part of ongoing planning/budgeting review activity through inclusion as a standing item on School Board agendas, and by senior management of Professional Service directorates through regular management meetings to same frequency.
- October/November: Schools/Department review, re-assess and re-submit their operational risks, aggregated for consideration and review by Risk & Resilience Committee and considered for referral to ULT/Audit & Risk Committee as appropriate.

#### *Escalation of Operational/Emerging Risks*

28. The mechanism for identifying and escalating increasing operational risks or emerging new risks is as follows:

- Each time the operational risk register is reviewed as per the monitoring and review process above, scores will be adjusted as appropriate and monitoring trend information created.
- Any significant increases in risk, where risks have moved to a high/very high rating, identified at the bi-monthly School Board and Service review monitoring points (or at any other point between where an increase in risk has become apparent), and/or where a risk appears to be moving beyond the tolerance parameters and thresholds contained in the risk appetite statement, should be escalated by notifying the University Secretary (Convenor or Risk & Resilience Committee), who can refer to ULT and Audit & Risk Committee for action as appropriate, including consideration for inclusion on the Top Risks register.
- Emerging risks not currently captured on operational risk registers, which are residually high/very high and/or appear to exceed the tolerance parameters and thresholds contained in the risk appetite statement, may also be identified at any time by SLT/ULT and escalated through the above process.

#### *Internal Audit*

29. Internal audit helps the University achieve its strategic objectives by evaluating the management of risk. It also provides reassurance to senior management and other key stakeholders that important risks have been evaluated and highlights where any improvements may be necessary. The internal audit function is a critical part of the

top level governance of any organisation and helps senior management to demonstrate that they are managing the organisation effectively.

30. Internal audit is an important element of the internal control process. Apart from its normal programme of work, internal audit is responsible for aspects of the annual review of the effectiveness of the internal control systems within the University.

#### *External Audit*

31. External audit provides feedback to the Audit & Risk Committee on the operation of the internal financial controls reviewed as part of the annual audit.

#### *Third party reports*

32. From time to time, the use of external consultants will be necessary in areas such as Health & Safety and Human Resources. The use of specialist third parties for consulting and reporting can increase the reliability of the internal control system.

### **Review of Control Effectiveness**

33. The Audit & Risk Committee under delegated authority from University Court is responsible for reviewing the effectiveness of the University's systems of internal control, based on information provided by the University Leadership Team and internal and external audit.

34. On an annual basis and following a formal determination, the Audit & Risk Committee will present to Court their assessment of the adequacy of the systems of internal control based on the findings of both internal and external auditors.

**Governance & Compliance  
November 2019**

#### **Document Control**

|                  |                         |
|------------------|-------------------------|
| Author           | Governance & Compliance |
| Status           | Final                   |
| Approved         | 5 November 2019 (RRC)   |
| Review Frequency | 2 years                 |

Key changes 2019: Incorporate recommendations from IA report Dec 2018:

- Risk appetite statement
- Formalising reporting/monitoring of risk through School/Dept financial and performance reporting packs.
- Clearly defining mechanism for aggregation, review and escalation of operational risks.