FNU Risk Management Framework

1. Introduction

1.1 Risk is the threat that an event or action will adversely affect an organisation's ability to achieve its objectives and successfully execute its strategies. Risk management is the identification, analysis and control of threats to the achievement of an organisation's strategies and operational objectives. The purpose of risk management is not to remove all risk. Rather, risk management is about ensuring that risks are recognised and their potential to cause financial loss or other impact fully understood. Based on this information, action can be taken to direct appropriate levels of resource to controlling risk or minimising the effect of potential damage.

1.2 Effective risk management forms an important element of good corporate governance and management. It allows an organisation to:

- Increase confidence in achieving its priorities and outcomes
- Agree levels of acceptable risk and how these will be handled
- Reduce the potential for lost opportunities

2. FNU's risk management strategy

2.1 FNU's risk management strategy is designed to ensure that the University maximises its opportunities and minimises the impact of the risks it faces, thereby improving its ability to achieve its objectives within its governance framework. Setting and promulgating this overall approach to risk management is the responsibility of the FNU Council, but must be implemented by everyone.

2.2 FNU's approach to risk management involves a structured and systematic process for the identification, evaluation, prioritisation and management of risk at strategic and operational levels.

2.3 Corporate risks are those that could have an adverse impact on the medium- and long-term objectives of the University; managing them is responsibility of the University's senior management. Operational risks are those that could have an adverse impact on Colleges and/or Divisions, leading to service failure and under-performance; managing these risks is the responsibility of managers and staff who manage them on a day-to-day basis in the course of their work. FNU will adopt a combination of 'top down' (corporate) and 'bottom up' (operational) risk identification, assessment and analysis, to ensure coverage of the whole of the University.

3. FNU's risk management process

3.1 Risks may arise because of the general operating environment or in relation to specific decisions being made or options being considered. The template for SMG papers includes a mandatory requirement to tie decisions to the University's corporate risks.

3.2 A High-Level (corporate) Risk Register is maintained and updated every six months by SMG; individual risks and sub-risks are assigned to individual SMG members. At a local level Deans and Directors undertake a risk analysis based on their strategic priorities, including any risks assigned by SMG. This process results in the production of local level risk registers.

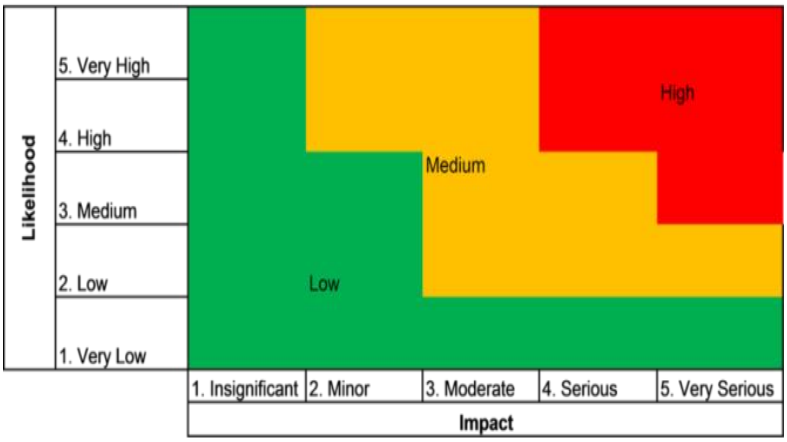
3.3 Project owners are required to maintain and keep up-to-date risk registers for specific projects, for regular reporting to the appropriate Project Steering Group/Board.

3.4 Risk assessment and mitigation is an integral part of developing partnerships with external bodies. Partners will also need to produce their own risk assessments, recorded accordingly.

3.5 All employees will use risk management training and this guidance to help manage risk on a day-to-day basis. These risks will not be recorded formally, unless the manager feels that they are significant, in which case they will be added to the existing College and Division risk registers.

3.6 Once risks have been identified, they are assessed systematically using a common framework, based on likelihood (the probability of a risk eventuating) and impact (the potential severity of the consequences should a risk eventuate), on a scale of 1 to 5 (with 1 signifying low likelihood and/or impact, 5 signifying high likelihood and/or impact). For risks with a financial impact, a monetary value is ascribed to each risk category. Each risk is assessed according to these criteria and categorised as low, medium or high, using the risk tolerance matrix shown below. The risk management process looks at the inherent assessment of each risk, as well as its residual assessment (taking key controls and improvement actions into account). Each risk and sub-risk is categorised using the RAG (red-amber-green) rating according to its residual score.

Risk Tolerance Matrix



Likelihood	1. Insignificant	2. Minor	3. Moderate	4. Serious	5. Very Serious
5. Very High	Low	Medium	Medium	High	High
4. High	Low	Medium	Medium	High	High
3. Medium	Low	Low	Medium	Medium	High
2. Low	Low	Low	Medium	Medium	Medium
1. Very Low	Low	Low	Low	Low	Low
	Impact				

3.7 A cyclical process of risk reporting and escalation includes a twice-yearly review of risks by SMG and dissemination of relevant outcomes to staff. The following process will be used:

- SMG reviews the High-Level Risk Register twice a year.
- The revised High-Level Risk Register is disseminated to local-level risk owners who review their local registers, taking into account the high-level risks as well as local operational risks.
- Deans and Directors are required to review their risk registers twice a year. Following review, local-level risk registers are sent to the Department of Risk and Compliance. If appropriate, individual Deans or Directors will be contacted to review their operational risks.
- Any risks considered for inclusion on the High-Level Risk Register will be taken to SMG.

4. Risk appetite and assessment

4.1 Risk appetite can be defined as the amount of risk that an organisation is prepared to accept in the pursuit of its strategic objectives. It may be helpful for the FNU Council to adopt an agreed statement on risk appetite, in line with international best practice.

4.2 Assessing whether to transfer, tolerate, treat or terminate a risk is based on the University's agreed appetite for risk and the availability of resources.

- **Transfer** involves transferring risk to a third party or by insurance. It is not always possible to transfer risks completely: in many cases, the University will retain corporate responsibility.
- **Tolerate** - In the event that the ability to transfer a risk is limited or the cost of taking action outweighs the potential benefits, risks may be tolerated.
- **Treat** - Most risks will fall into this category. The aim of treatment is to contain the risk to an acceptable level through a series of internal controls.

- **Terminate** - In extreme cases, terminating an activity may be the only way of managing the associated risk. This may not be possible if the activity forms part of the University's core activities.

4.3 If it is determined that a risk should be treated, controls (in the form of systems, policies and procedures) will be put in place to manage the risk. Key controls, with SMART improvement actions to strengthen them, will be reviewed twice a year by SMG.

5. FNU's risk management policy

5.1 Purpose

5.1.1 FNU has a Risk Management Policy ('the Policy') which forms part of the University's risk and compliance and corporate governance arrangements.

5.1.2 The Policy explains the University's approach to risk management, documents the roles and responsibilities of the FNU Council, the Audit and Risk Committee, Senior Management Group (SMG), and other key parties. It also outlines key aspects of the risk management process, and identifies the main reporting procedures.

5.1.3 The Policy describes the process the FNU Council will use to evaluate the effectiveness of the University's internal control procedures.

5.2 Objectives

5.2.1. The objectives of the Policy are to:

- Actively assess and manage risk
- Provide a consistent framework for identifying, evaluating, controlling, reviewing and reporting risks across the University
- Manage corporate risk in accordance with best practice, as part of good corporate governance
- Raise the profile of risk management across the University, integrating risk management into the culture of the University and making it a routine part of the decision-making process
- Create effective processes that allow the University to make risk management assurance statements annually
- Communicate to stakeholders the University's approach to risk management and its alignment with strategic planning

5.3 Institutional approach to risk management

5.3.1 The following principles outline the University's institutional approach to risk management:

- The FNU Council has responsibility for overseeing risk management holistically across the institution
- The Vice-Chancellor and SMG support, advise and implement policies approved by the FNU Council
- The University, advised by its external auditors, makes conservative and prudent recognition and disclosure of the financial and non-financial implications of risks
- Deans are responsible for encouraging good risk management practice within their College with Heads of School being responsible for good risk management within their own areas.
- Directors and Heads of Departments are responsible for encouraging good risk management practice within their divisions and departments
- Key risks will be identified and monitored on a regular basis

5.4 Resources

5.4.1 The Department of Risk and Compliance (under the Office of the Vice-Chancellor) will maintain hands-on oversight of risk management.

5.4.2 Risk plan owners will be nominated by Colleges and Divisions to ensure that the University minimises exposure to unidentified risks and threats.

5.5 Role of the FNU Council

- Sets the tone and influences the culture of risk management within the University

- Determines the appropriate risk appetite or level of exposure for the University
- Approves major decisions affecting the University's risk profile or exposure
- Annually reviews the institution's approach to risk management and approves changes or improvements to key elements of its processes and procedures

5.6 Role of the Audit and Risk Committee

5.6.1 The Audit and Risk Committee is required to report to the FNU Council that they have assurance that risk is being actively managed across the University and that appropriate mechanisms and internal controls are in place. The Audit and Risk Committee alerts the FNU Council to any emerging issues. In addition, the Audit and Risk Committee oversees internal audit, external audit and management as required in its review of internal controls. The Audit and Risk Committee is therefore well placed to provide advice to the FNU Council on the effectiveness of the internal control system, including the University's system for risk management.

5.6.2 Inter alia, the Audit and Risk Committee:

- Monitors the management of significant risks
- Satisfies itself that risks are being actively managed, with the appropriate controls in place and working effectively

5.7 Role of SMG

- Provides institutional oversight and sets the University's risk direction through the implementation of the University's risk management policy
- Ensures that the University manages its risks by appropriately identifying, evaluating and monitoring risks and ensuring that appropriate controls are in place to achieve this
- Manages corporate risk in accordance with best practice, as part of good corporate governance.
- Ensures that risks are identified and presented to the Audit and Risk Committee for consideration in an appropriate and timely manner
- Ensures that the University's risk management policy and internal controls are implemented across the University
- Ensures that there is appropriate consideration of local-level risks and that new risks identified from local risk registers are considered for escalation on to the high-level risk register where appropriate
- Directs local risk owners to include mandatory risks on local-level risk registers as appropriate
- Regularly reviews the University's risk management policy

5.8 Role of Deans and Directors

- Create and maintain up-to-date local risk registers
- Create and maintain up-to-date local risk action plans
- Promote risk awareness within their area of responsibility
- Actively participate with the Department of Risk and Compliance to ensure effective synergy between local and high-level risk registers
- Actively participate with the Department of Risk and Compliance in support of continuous improvement
- Actively participate with the Department of Risk and Compliance to ensure consistency of approach in line with the FNU risk management strategy

5.9 Role of the Department of Risk and Compliance

- Promotes the strategy and Policy throughout the University
- Reports on the risk management process and the system of internal control to SMG and the Audit and Risk Committee
- Oversees implementation of risk management ensuring alignment with the University's Strategic Plan, the Risk Management Strategy and Policy

- Tracks risk events by maintaining a database and ensuring that risk events are captured and mitigated, and that timely and up-to-date risk information is provided to the Vice-Chancellor, SMG and the Audit and Risk Committee

5.10 Role of Internal Audit

5.10.1 There is a professional requirement for Internal Audit to work independently and objectively. The role of Internal Audit therefore is not to be responsible or accountable for risk management across the University or for managing risks on management’s behalf. Rather, the key tasks of Internal Audit are:

- to provide guidance and advice on all matters of risk management
- to provide managers with practical techniques for identifying and assessing risks and review control and mitigation strategies
- to provide management with an assessment, through internal audit reviews, of whether controls in place to manage risks are appropriately designed and operating as intended
- to assess the adequacy of the mechanisms for identifying, analysing and mitigating key risks
- to provide assurance on the effectiveness of controls
- to provide feedback to the Audit and Risk Committee on the operation of the internal risk management controls reviewed as part of the annual audit

5.11 Compliance with the Policy

5.11.1 Consistent compliance with this Policy is essential to its effectiveness. All FNU employees with risk responsibilities are expected to adhere to this Policy and to follow it consistently.

5.11.2 Internal Audit, as part of its work programme, will review the risk registers periodically to ensure compliance with the overall risk programme.

5.12 Training

5.12.1 The Department of Risk and Compliance will ensure that all individuals with direct risk responsibilities receive appropriate training in order to carry out their duties effectively.

5.13 Review of the Policy

5.13.1 The Department of Risk and Compliance is responsible for the implementation and maintenance of this Policy.

5.13.2 This Policy will be reviewed annually. When significant changes are required, amendments to the Policy will be presented to SMG and the Audit and Risk Committee for approval.