



# **Scottish Universities Sport**

## **Risk Management Policy**

August 2009

## **1. Introduction**

Scottish Universities Sport (SUS) manages numerous risks. These risks have the potential to disrupt achievement of SUS strategic and operational objectives. SUS aims to use risk management to take better informed decisions and improve the probability of achieving its strategic and operational objectives.

### **Corporate Governance**

SUS follows broad principles of governance and the following have been applied:

- The identification and management of risk should be a continuous process and linked to the strategy and action plans.
- Control should be risk based including valuation of the likelihood and impact of risks becoming a reality. (Risk Register)
- Review of SUS procedures must cover business, operational and compliance as well as financing risk.
- Risk assessment and internal control should be embedded in ongoing operational procedures.
- The executive committee should receive regular reports during the year on internal control and risk.
- The principal results of risk identification, evaluation and management review of its effectiveness should be reported to, and reviewed by, the executive committee.
- The executive committee acknowledges that it is responsible for ensuring that a sound system of control is maintained and that it has reviewed the effectiveness of the above process.
- Where appropriate, set out details of actions taken or proposed, to deal with significant internal control issues and risk.

### **Purpose of this policy**

This policy is a formal acknowledgement of the commitment of SUS to risk management. The aim of the policy is not to have risk eliminated completely from SUS activities, but rather to ensure that every effort is made by SUS to manage risk appropriately to maximise potential opportunities and minimise the adverse effects of risk.

### **Policy Objectives**

1. To confirm and communicate the commitment to risk management, ensuring its assistance in achieving the strategic and operational goals and objectives of SUS.

2. To formalise and communicate a consistent approach to managing risk for all SUS activities.
3. To ensure that all significant risks to SUS are identified, assessed and where necessary treated and reported to the executive.
4. To assign accountability to all staff for the management of risks within their areas of control.
5. To provide a commitment to staff that risk management is a priority area for SUS.

### **Policy Statement**

SUS considers risk management to be fundamental to good management practice and a significant aspect of the effective governance of SUS. Effective management of risk will provide an essential contribution towards the achievement of the strategic and operational objectives and goals of SUS.

Risk management must be an integral part of the SUS decision making and routine management, and must be incorporated within the strategic and operational planning processes.

Risk assessments must be conducted on new ventures and activities, including projects, processes, systems and commercial activities to ensure that these are aligned with the SUS objectives and goals. Any risks or opportunities arising from these assessments will be identified, analysed and reported to the executive committee.

SUS will maintain a strategic and operational risk register. SUS will regularly review and monitor the implementation and effectiveness of the risk management process, including the development of an appropriate risk management culture.

### **Scope of the policy**

Risk is an inherent aspect of the work of SUS. Sound risk management principles must become part of routine management of SUS activity. The key objective of this policy is to ensure SUS has a consistent basis for measuring, controlling, monitoring and reporting risk.

### **The policy details the following:**

- What is risk?
- The SUS approach
- Risk Responsibilities and Risk Owners
- How is risk assessed?

The appendixes provide:

- Categories of risk

### **What is Risk?**

Risk exists as a consequence of uncertainty and is present in all activities whatever the size or complexity and whatever industry or business sector. It is important to understand that risk is a broader concept than the traditional view of merely a threat. It also recognises the risks of taking or not taking opportunities.

### **Risk includes:**

Threats (damaging events) which could lead to failure to achieve objectives.

Opportunities (challenges) which if exploited could offer an improved way of achieving the desired objectives but which could potentially have negative impacts.

SUS considers all types of risk it faces, strategic, operational, financial, reputational and regulatory and compliance risks. Appendix 1 gives a list of the different categories of risks.

### **The SUS Approach**

The SUS approach to risk management follows several key principles:

- The Risk Management process will be as user friendly as possible and add value. For this reason considerable effort has been put into keeping the process as simple as possible.
- SUS seeks to embed risk management across all of its operations and activities
- SUS will use a consistent and transparent approach to risk, ensuring an agreed and widely understood method and language.
- A key focus of the risk management process is the concentration on control improvements to mitigate significant risks, however there is a need to balance the cost and the effectiveness of the controls; for example where marginal improvements in control require substantial costs, the proposal may be unviable.
- Upward reporting of risk ensures that significant risks are reported and closely monitored on a regular basis at the appropriate level.

### **Risk Responsibilities**

#### **SUS Executive Committee**

The Executive Committee has responsibility for the total risk exposure of the SUS and approves the risk tolerance line annually.

## **Staff**

Effective risk management depends on the commitment and co-operation of all staff. All staff have a significant role in the management of risk, particularly within their own areas of control. Consequently all staff are responsible for and have accountability for adherence to the principles outlined in this policy.

## **Project Managers and Project Teams**

Project managers and project teams are responsible for managing project specific risk and complete a project risk register to demonstrate that this is being done.

## **Risk Management Strategy**

There are five steps to management of risks identified in the risk register which consists of:

1. Identifying the risks to achieving strategic and operational objectives
2. Determining the owner of the risk
3. Determining and assessing the existing controls in place
4. Assessing the impact and likelihood of the risk after taking account of existing controls to derive the net risk
5. Determining further control improvements to mitigate the risk and indicate what their impact on net risk will be when they are fully implemented.

Risk can be assessed using brainstorming sessions, SWOT analysis or risk assessment user groups. The executive and staff should carry out an annual review of the linkages between strategic objectives and risks to ensure that focus is maintained on priority activities.

SUS uses a risk matrix to define likelihood and impact. Impact is the potential severity or effect of the risk. Likelihood is the frequency or probability of a risk occurring. The ratings given to impact and likelihood produce an evaluation of net risk. Both the adequacy of existing controls and net risk are denoted by a traffic light system. Any risks in the red will require explicit review and approval by the executive committee.

A formal risk review should take place at least twice a year with a review of progress on control improvements for red risks every six weeks. In the case of projects there should be a risk review at each project team meeting. During the risk review, thought should be given to each risk to ensure that the risk is still relevant and applicable and that the risk register is complete (new risks should be considered at this point). It is good practice for It is important that the number of risks under active management does not exceed a manageable number (10-20) and where the net risk is considered very low the risk can be removed from the risk register.

## **Reporting significant risk**

The normal reporting regime will include publication of a revised risk register for any red risks that require reporting to that level of authority or any existing controls that have

been scored as red. The risk map shows the level of likelihood and impact of the net risk and the adequacy of controls.

The register should be reviewed at least twice a year (including consideration of new risks) by the risk owners. An annual report should be presented to the executive and include the risk register.

Any red risks and any risk where existing controls are assessed as inadequate should be reported to the executive.

## APPENDIX 1

### Categories of Risk

This appendix provides a prompt which can be used to aid risk discussions. These can be used as a guide, a starting point or as a checklist for existing registers

#### Strategic Risk – Major Threats

Sources of threat that may give rise to significant strategic risk includes:

- Budgeting (relates to availability or allocation of resources)
- Fraud or Theft
- Unethical dealings
- Product and or services failure (resulting in lack of support to business process)
- Public perception and reputation
- Exploitation of workers and or suppliers (availability and retention of suitable staff)
- Environmental (mismanagement issues relating to fuel consumption, pollution etc)
- Occupational health and safety mismanagement and or liability
- Failure to comply with legal and regulatory obligations and or contractual aspect (can you sue or be sued)
- Civil Action
- Failure of the infrastructure (including utility supplies, computer networks etc)
- Failure to address economic factors (such as interest rates, inflation)
- Political and market factors (for management of risk, security etc)
- Operational procedures – adequate and appropriate
- Capability to innovate (to exploit opportunities)
- Failure to control intellectual property (as a result of abuse or industrial espionage)
- Failure to take account of widespread disease or illness among the workforce
- Failure to complete to published deadlines or timescales
- Failure to take on new technology where appropriate to achieve objectives
- Failure to invest appropriately
- Failure to control IT effectively
- Failure to establish a positive culture following business change
- Vulnerability of resources (material and people)
- Failure to establish effective continuity arrangements in the event of disaster
- Inadequate insurance/contingency provision for disasters such as fire, floods and bomb incidents.

### **Strategic/Commercial Risks**

Examples of commercial risks includes

- Under performance of service relative to specification
- Management will under perform against expectations
- Collapse of contractors
- Insolvency of promoter
- Failure of suppliers to meet contractual commitments (this could be in terms of quality, quantity, and timescales on their own exposures to risk)
- Insufficient capital investment, shortfall in revenue expected / planned
- Fraud/Theft
- Partnerships failing to deliver desired outcome
- An event being non insurable or cost of insurance outweighs the benefit

### **Economical/Financial/Market**

- Interest rate instability
- Inflation
- Shortage of working capital
- Failure to meet project revenue targets
- Market developments will adversely affect plans

### **Legal and Regulatory**

- New or changed legislation may invalidate assumptions upon which the activity is based
- Failure to obtain appropriate approval (e.g. planning consent)
- Unforeseen inclusion or contingent liabilities
- Loss of intellectual property rights
- Failure to achieve satisfactory contractual arrangements
- Unexpected regulatory controls of licensing requirements
- Changes in tax structure

### **Organisation/Management/Human Factors**

- Management incompetence
- Inadequate corporate policies
- Inadequate adoption of management practices
- Poor leadership
- Key personnel have inadequate authority to fulfil roles
- Poor staff selection procedures
- Lack of clarity over roles and responsibilities
- Vested interest creating conflict and compromising the overall aims
- Individual or group interests given unwarranted priority
- Personality clashes
- Indecisions or inaccurate information
- Health and safety constraints

### **Political**

- Change of government policy
- Change of government
- War and disorder
- Adverse public opinion/media intervention

### **Environmental**

- Natural disasters
- Storms, flooding
- Pollution incidents
- Transport problems

### **Technical/Operational/Infrastructure**

- Inadequate design
- Professional negligence
- Human error/incompetence
- Infrastructure failure
- Operation lifetime lower than expected
- Increased dismantling/decommissioning costs
- Safety being compromised
- Performance failure
- Residual maintenance problems
- Unclear expectations
- Breaches in statutory/information security
- Lack or inadequacy of business continuity

### **Operational Risks**

- Lack of clarity of service requirements
- Inadequate infrastructure to provide required operational services
- Inadequate or inappropriate people available to support the required service provision
- Inappropriate contract in place and or inadequate contract management to support the required level of service provision
- Changing requirements, enabled in an uncontrolled way
- Products passed to operational teams without due consideration to implementation, handover, subsequent maintenance and decommissioning
- Unexpected or inappropriate expectations of service users
- Inadequate incident handling
- Lack or inadequacy of business continuity or contingency measures with regard to maintaining critical business services
- Failing to meet legal or contractual obligations

Extracted from Management of Risk: Guidance for practitioners