**Fèisean nan Gàidheal**
**Risk Management and Policies**

**Date: 15 June 2010.**

**Policy: Risk Management Policy**

**This policy forms part of the Fèisean nan Gàidheal Policy Portfolio**

**Related Policies:** All policies

**Purpose of Policy:** To ensure adequate consideration and mitigation of risks to the organisation, its personnel, its participants and visitors.

**Summary of Policy:** Strategy and objectives for operational risk management and the approach and processes by which Fèisean nan Gàidheal achieves those objectives. Fèisean nan Gàidheal defines operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."

**Policy drafted by:** Iona MacDonald, Training & Policy Officer

**Submitted to Executive Group (date):** 01 February 2010.

**Approved by Board (date):** 18 February 2010.

**Last Reviewed (date):** February 2013.

**This policy should be reviewed by (date):** February 2014.

**Catriona MacIntyre – 18 February 2010.**

**Fèisean nan Gàidheal**
**Risk Management Policy**

## Business and Operational Risk Policy

### Purpose & Scope of Policy

This policy statement outlines Fèisean nan Gàidheal's strategy and objectives for operational risk management and the approach and processes by which Fèisean nan Gàidheal achieves those objectives.

The policy takes account of, and is consistent with, operational risk policy guidance issued by government and national bodies in connection with youth arts organisations, and with current business practice in voluntary organisations.

This policy has been approved by the Board of Directors and is applicable to all Fèisean nan Gàidheal offices and to local Fèisean where appropriate, including directors, staff, tutors, local committees and volunteers.

The purpose of risk management for Fèisean nan Gàidheal is to help ensure that the organisation's strategic aims are achieved with the maximum benefit to those concerned and the minimum of delay of progress or undermining of public esteem, the latter being crucial to the continuance of the organisation. The system of internal control is intended to manage, rather than to eliminate, the risk of failure to achieve policies, aims and objectives. The strategy is based on identification of the benefits that the organisation wishes to achieve, and assessment of the level of exposure that is regarded as appropriate to take in particular areas, taking into account a cost-benefit analysis.

### Definition and categorisation

Fèisean nan Gàidheal has adopted the following definition of operational risk:

"the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events"

Operational risk presents significant exposures to Fèisean nan Gàidheal which may threaten its survival and capital adequacy.

Fèisean nan Gàidheal has established a common risk language to provide a consistent framework for the definition and categorisation of risk and the organisation of its risk management activities.

Within this framework, Fèisean nan Gàidheal categorises operational risk into 7 sub-categories, as summarised below. Fèisean nan Gàidheal's detailed risk categorisation is set out in the Fèisean nan Gàidheal risk register.

| Category | Example of event |
|---|---|
| **People** | • manual input errors<br>• inadequate management decision making<br>• inadequate staff training<br>• inadequate staffing levels<br>• processes / procedures not followed<br>• lack of escalation to management<br>• internal theft or fraud<br>• recruitment screening failure<br>• miscommunication – internal / external |
| **Processes** | • inadequate processing control – funding / claims<br>• inadequate control over outsourced activities – eg IT / finance<br>• failure of outsource provider<br>• inadequate segregation of duties<br>• inaccurate / incomplete management information<br>• inadequate supporting software<br>• inadequate / inappropriate policies<br>• inaccurate / incomplete trading data<br>• failure in corporate governance |
| **Systems** | • hardware failure<br>• software failure<br>• network / telecommunications failure<br>• third party IT provider failure<br>• inadequate virus protection<br>• inadequate system security / information management<br>• insufficient processing capacity<br>• insufficient / untested disaster recovery processes<br>• inadequate system upgrade management |
| **External events** | • failure to secure core funding<br>• natural disaster / catastrophic loss<br>• man made disaster / catastrophic loss<br>• third party / supplier failure<br>• external theft or fraud<br>• external breach of system security<br>• terrorist attack / denial of access to building<br>• power outage |
| **Reputational** | • identity theft / abuse of brand<br>• corruption, intimidation or coercion of staff<br>• failure to comply with UK legislation<br>• regulatory breach, fine, bad press<br>• downturn in popularity |

| Category | Example of event |
|---|---|
| **Legal** | • insurance policy dispute<br>• dispute over service level agreements<br>• public and employers' liability<br>• breach of public duty/trust<br>• change in law / failure to interpret law correctly |
| **Strategic** | • adverse political developments<br>• adverse developments in the wider economy<br>• failure to manage change<br>• failure to deliver business strategy |

**Risk Management Strategy**
In determining acceptable levels of exposure, the Board of Fèisean nan Gàidheal plays a decisive role. The Fèisean nan Gàidheal Board is advised on the effectiveness of the establishment and implementation of risk management by the Executive Group, which reports on a quarterly basis to the Board.

**Risk Register**
The Risk Register focuses on high level risks. Each of these relates to at least one of the strategic aims of the organisation, and focuses on those risks which could adversely affect its capacity to achieve its purposes.

**High level risks**
The high level risks are those which in the opinion of the Executive Group could critically, or seriously, affect the operation of the organisation as a whole. Their inclusion in the organisation's Risk Register indicates that they have been agreed as such with the Board.

**Strategic aims**
The strategic aims have been set out in the organisation's Five Year Development Plan. They are reproduced in full at the beginning of the Register (pages **), and then, in order to clarify the alignment of risks with aims, aims are inserted against the items in the Register which relate to them. (Five Year Plan currently under review.)

**Procedures**
Fèisean nan Gàidheal's risk management procedures involve:
- an annual Review conducted by the Senior Management Team, in consultation with the managers responsible for areas where high level risks are identified, which is presented in written form to the Executive Group of Fèisean nan Gàidheal for detailed discussion, and reported to the Board
- the linking of personal objectives for senior managers to the responsibility for the management of specific risks
- quarterly review by the Senior Management Team of the record of risks facing the organisation, and regular discussion of emerging risks and the system of risk indicators
- follow-up and reporting on actions recommended by internal audit

On at least an annual basis the organisation formally assesses whether sufficient is being done to manage each risk effectively. The Executive Group, to which the responsibility for detailed review of Fèisean nan Gàidheal's risk management arrangements is delegated, considers the recommendations of the Senior Management Team, as to which of these risks should be classified as 'high exposure', 'medium exposure' or 'low exposure', and whether the proposed approach is appropriate in the circumstances.

**Key controls**
The organisation has in place the following controls:
- an established organisational structure with identified reporting lines and responsibilities
- Financial Regulations, specifying authorisation and approval levels
- written policies for key areas of activity
- a formal structure for the governance of the organisation
- formal terms of reference, membership and periods of office for the governing body (the Board) and Committees
    - annual review of attendance at Board meetings
    - formal agendas and minutes for all Board meetings

- regular agenda items on risk management for Board, Executive and Staff meetings
- annual strategic planning and review exercises

**Risk owners**

The organisation's risk management procedures identify 'the linking of personal objectives for senior managers to the responsibility for the management of specific risks' as one of four interlinked elements in the organisation's approach to risk management. Each risk is 'owned' by a member of the Senior Management Team or delegated to an officer. Within the framework of Fèisean nan Gàidheal's risk management policy and procedures, an individual 'risk owner' is expected to take responsibility for:

- Monitoring the organisation's level of exposure to the identified risk, on a continuing basis
- Drawing the attention of the CEO and other senior managers to the need for review of and/or changes to institutional practice/activity, at any time, if:
  - The level of risk appears to be increasing
  - New approaches to risk mitigation need to be adopted
  - The level of risk appears to have been wrongly estimated
- Leading the Senior Management Team's regular review of the relevant section of the risk register
- Ensuring that issues of concern are reported to the Executive Group, as part of the regular reporting on risk management made to the Executive Group

While the ownership of risks requires regular support and advice from colleagues throughout the organisation, within Fèisean nan Gàidheal's risk management procedures, the ownership of the 9 identified 'high level' risks which comprise the Risk Register rests with the members of the Senior Management Team. It is only with the formal approval of the Chief Executive that a Senior Management Team risk 'owner' may delegate the ownership of a particular risk, or element of a risk. If this is agreed, all members of the Senior Management Team will be informed, the change will be documented, and the arrangement will be reported to the Executive Group.

Job descriptions, appraisal discussions and the setting of personal objectives will take account of the risks for which an individual member of the Senior Management Team is responsible.

**Risk rating method**

The Fèisean nan Gàidheal Risk Register currently uses the following method of risk rating:
Hazard Severity - Low-medium-high (for rating purposes, 1 - 5)
Likelihood Low-medium-high (for rating purposes, 1 - 5)
The risk rating has been calculated by multiplying these figures, to produce a 'risk score'
On the basis of the risk score, items are categorised in terms of exposure, either high, medium or low
High exposure is 17 - 25
Medium exposure is 9 -16
Low exposure is 1 – 8
Acceptable risk for activities involving children is <6.