Imperial College Union
Board of Trustees / 09 December 2020

Risk Management Policy

Author(s): Tom Flynn (Managing Director)

Purpose: To consider and approve the proposed risk management policy.

1. Context & Purpose

Risk Management Frameworks are well established in the charity sector, with the Charity Commission itself issuing guidance on the topic in the form of CC26 *Charities and Risk Management* in 2010 (updated in 2017).

Their aim is simple – to help organisations understand the factors that might prevent their ability to deliver their charitable objectives, and to take appropriate action to mitigate this. The *defensive* approach to the issue posits this as something akin to harm reduction. What might negatively impact upon our services and activities, and what can an organisation do to prevent this. But there is also an *offensive* case to make. Ensuring that we are aware and mindful of our risks will help us plan better and ensure that we are delivering maximum impact with work.

The Union's historic approach has conflated *strategic* and *operational* risk management, and there has been a lack of clarity over reporting and accountability.

2. Risk Management Frameworks

The most often cited model applied in the sector is the three lines of defence approach developed by the Institute of Internal Auditors (IIA 2013)[1] and refined specifically for charities by the Institute of Risk Management (IoRM 2015).[2] Broadly, this requires organisations to articulate their framework under three different levels, and to consider how these are related as part of a broader coherent plan.

i. First line of defence: operational risk management, for example a detailed risk register for a department or a specific project or activity, that sets out concrete steps for staff to take. Often based on the following headings: financial, legal, health & safety, reputational and operational.

ii. Second line of defence: governance and oversight of risk, for example a policy or framework that clearly identifies how risks are reported, and who is overall responsible for what. This often includes a *strategic risk register* for charities, to ensure trustees have sufficient grasp over factors impacting on the charity.

iii. Third line of defence: independent audit and assurance, for example the use of quality marks, accreditation schemes or formal benchmarking to give confidence to trustees that risks are being managed.

[1] Institute of Internal Auditors (IIA) (2013) *The three lines of defence in effective risk management and control*, Institute of Internal Auditors
[2] Institute of Risk Management (IoRM) (2015) *Risk management for charities: getting started*, IRM

3. Outputs, Monitoring & Reporting

If the three lines of approach model is adopted as our formal risk management framework, the following outputs, monitoring and reporting would be appropriate.

Line of Defence	Outputs	Monitoring & Reporting
First Line of Defence	Annual Operational Plans / Departmental Risk Registers Other policies such as: risk assessment policy, financial procedures manual.	These should be developed on an annual basis and reviewed termly by the senior manager and at Leadership Group. These should be reviewed on a triannual basis as part of a formal process.
Second Line of Defence	Strategic Risk Register Scheme of Delegation Reserves Policy	These should be formally reviewed annual each September by the full Board of Trustees. The Strategic Risk Register should be a standing item on the Finance & Risk Subcommittee. The Strategic Risk Register should integrate with the College's risk framework.
Third Line of Defence	Annual External Audit Annual Imperial College Internal Audit External Accreditation Schemes (TBC)	These should take place annually and be reported to the full Board of Trustees.