



POLICY:	Risk Management Policy
FIRST DRAFT:	ET 2015#10, (amendments, FRC 2014#04)
ADOPTED:	BR 2014#04 (Pro tem) BR 2015#01
AMENDMENTS:	
REVIEW:	June 2019

1 PURPOSE OF MIC RISK MANAGEMENT POLICY

All policies, guidelines and protocols of Mary Immaculate College, will reflect the Colleges commitment to the promotion of equality and will be fully compliant with the provisions of prevailing equality legislation.

- 1.1 Risk identification and management is necessary to maximise the likelihood of achieving the College's mission, strategic objectives and operational goals by seeking to limit, through mitigating actions, the occurrence of risks that can be foreseen through regular, systematised situational awareness and analysis.
- 1.2 It is, primarily, the responsibility of An tÚdarás Rialaithe to ensure that a robust system of risk management is in place at the College and it is the purpose of this policy to set out the framework for this system. An tÚdarás Rialaithe seeks to ensure that the risk assessment and management process is integrated into existing management systems across the College as a whole. It is the aim of An tÚdarás Rialaithe that while the Risk Management Policy and related processes are reflective of best practice, they should be kept as easy to understand and implement as possible in order to ensure that all employees of the College gain a familiarity with this essential aspect of internal control and implement risk management processes in their work, as appropriate.
- 1.3 *An tÚdarás Rialaithe* recognises that the benefits of a Risk Management Policy also include:
- Transparent processes and good practice;
 - Support for management decisions;
 - Provision of competitive advantage by adapting to new circumstances;
 - Improved public accountability;
 - Increased quality and efficiency in processes;
 - Immediate risk prioritisation;
 - Positive attitude to implementing risk controls.
- 1.4 *In summary*, purpose of the Risk Management Policy is to provide a framework for the identification, assessment and rating of risks, and for the development of strategies to deal with risks so as to provide reasonable assurance that the College's mission and strategic objectives are achieved. In practice, the Risk Management Policy establishes a framework to identify potential circumstances or events that may expose the College to risk, to manage this risk to an extent that it remains within the range of the College's 'risk appetite,' and to strengthen the College's system of internal control.

- In the sections below, this document sets out: Key Definitions (Section 2)
- Roles & Responsibilities (Section 3)
- Risk Management Framework (Section 4), comprising ---
 - Risk Identification and Assessment
 - Risk Monitoring and Reporting;
 - Risk Appetite;
 - Management of Risk

2.1 KEY DEFINITIONS

2.2 Risk:

Risk can be described as *'a possible loss or other adverse consequence that has the potential to interfere with the Colleges ability to achieve its objectives and fulfil its mission.'* Risk may entail the possibility of failure by the College to benefit from opportunities available or to achieve its objectives due to an internal or external event.

2.2.1 Risks, by their very nature, may or may not occur and fall into a variety of categories, some of the most common being:

Strategic Risks:	The inability to achieve the College's strategic and operational objectives as set out in the institutional Strategic Plan and also, fail to exploit strategic opportunities when they arise;
Operational Risks:	The inability to prevent a loss resulting from inadequate internal processes and systems;
Financial Risks:	Exposure to losses arising as a result of the need to improve the management of the College's financial assets;
Reputational Risks:	Exposure to losses arising as a result of negative publicity or public image and failure to manage stakeholder relationships effectively.

2.2.2 In addition, risks can exist at different levels:

- Institutional (Corporate) Level (i.e. 'Fundamental Risks' residing within the Institutional Risk Register)
- Faculty / Functional Service level (local risk)
- Departmental / Office level (local risk)

- Project level (local risk)

2.3 **Risk Management**

Risk management is a process of linking clearly defined steps which, operated in a cyclical fashion, support better decision-making by contributing a greater insight into risks and their impacts. Risk management is not a stand-alone activity that requires special skills and resources that add to the administrative burden. The focus of risk management will be on successfully managing risk rather than on the system of risk management alone. The College integrates risk management practices into its governance framework rather than conducting risk management as an isolated operation.

2.4 **Risk Identification:**

Risk identification is the process of determining what negative circumstances or consequences are likely to emerge and impact on institutional mission or activity.

2.5 **Risk Analysis:**

Risk analysis is the systematic usage of available information to evaluate the likelihood of specific events occurring and the magnitude of their consequences/impact on the College.

2.6 **Risk Assessment:**

Risk assessment is the process of measuring and prioritising identified risks on the combined basis of their likelihood of occurrence and the resulting impact should they materialise.

2.7 **Risk Register:**

A risk register is a list that identifies current risks and is a monitoring tool for the management of the College that offers the rationale for individual risks, their current 'rating,' their categorisation (strategic, operational etc.) and the mitigating actions linked to them.

2.8 **Risk Mitigation:**

Risk mitigation is the action(s) taken, following identification and assessment of a risk, to ameliorate or eliminate the effects of that risk. The outcome from risk mitigation is monitored by the College through regular review of the Risk Register, and mitigating actions are linked directly to the College's Annual Operating Plan (AOP). Risk mitigation may result in the removal or de-escalation of a risk within the Institutional Risk Register or its re-positioning in a local risk register if that is more appropriate following mitigating action.

2.9 Risk Appetite:

Risk appetite is the amount of risk an organisation is prepared to accept based on the expected return arising from the development/activity in question. The College can be risk-tolerant or risk-averse and different levels of risk appetite can apply to different activities. In managing its risk appetite the College will decide the threshold beyond which risk is no longer acceptable.

3.1 ROLES & RESPONSIBILITIES

3.2 Trustees

The role of the MIC Trustees, as defined under the Scheme of Incorporation and the current Instrument of Government is to grant *An tÚdarás Rialaithe* (Governing Body) with the authority to manage the governance of the institution, including its risk management and broader internal control framework. The Trustees meet quarterly and are kept apprised of the current status of risk management through quarterly reports by the College President.

3.3 *An tÚdarás Rialaithe* (ABR / Governing Body):

In line with the Scheme of Incorporation and the measures put in place by the Trustees for the governance of the College under the Instrument of Government, overall responsibility for the management of risk within the College lies with *An tÚdarás Rialaithe*. *An tÚdarás Rialaithe*, which meets quarterly, approves the College's Risk Management Policy and satisfies itself (through its Audit & Risk Management Committee) that an adequate Risk Management Framework is in place at the College, and that fundamental risks are being managed effectively by the Executive Team.

3.4 Audit & Risk Committee (ARC)

The role of the Audit & Risk Committee, which meets quarterly, is to assure *An tÚdarás Rialaithe* that an adequate Risk Management Framework is in place at the College. In providing the required level of assurance, the Audit & Risk Management Committee will:

- Keep under review, and advise on, the operation and effectiveness of the College's Risk Management Framework;
- Ensure that assurance provided by management and external/internal auditors is appropriate;
- Monitor the effectiveness of Risk Management in relation to risks

identified as fundamental to the success or failure of the College's strategic objectives;

- Report to *An tÚdarás Rialaithe* on its findings in relation to fundamental risk management and the adequacy of the Risk Management Framework on an annual basis.

3.5 Executive Team (ET)

ET, which meets at three week intervals, is responsible for:

- Implementing the College's Risk Management Policy;
- Identifying and monitoring fundamental institutional risks and for ensuring that mitigating controls are in place and linked, as appropriate, to the Annual Operating Plan (AOP) of the College;
- Ensuring that each fundamental risk has a 'Risk Owner' responsible for its management;
- Ensuring that individuals understand what level of risk they are empowered to take on behalf of the College;
- Ensuring local risks are appropriately managed through review of reports on Local Risk Registers;
- Taking particular note of risks identified in local risk registers that should be escalated to the Institutional Risk Register;
- Tracking the status of the Institutional Risk Register at three week intervals and highlighting new areas of potential risk in light of reports on local risk registers and other relevant circumstances;
- Monitoring the assessment and management of fundamental risks that could impact on the achievement of the College's objectives;
- Encouraging a risk management culture throughout the College so that risk is embedded as part of the College's decision making and operation;
- Critically reviewing the effectiveness of risk management processes;
- Ensuring that all substantial projects or new programmes undergo prior risk assessment and that such assessment is included in the project/ programme proposal

3.6 Strategic Planning Group (SPG)

The SPG, which meets quarterly, is responsible for the following in relation to risk management:

- The identification, assessment, rating, management, mitigation and ownership of risk within members' individual areas of responsibility;

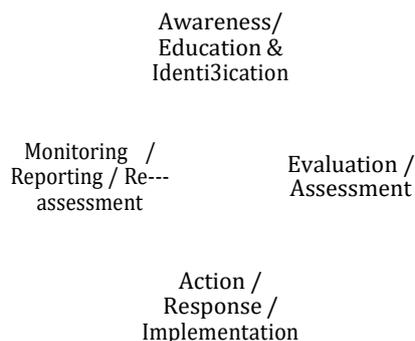
- The establishment and regular review of a Local Risk Register by members in their areas of responsibility and their transmission to their respective Line Managers (who are members of ET) bi-annually or as required
- The identification of new and emerging risks that cannot be managed locally and agreement that such risk is of a fundamental character and should be escalated to the Institutional Risk Register
- Supporting the embedding of risk management in members' individual areas of responsibility and the development of a risk-aware culture at all operational levels within the College

3.7 Internal Audit

A system of independent internal audit is in place in order to carry out ongoing review of internal controls within the College. In developing its Annual Internal Audit Plan, in consultation with the Audit & Risk Committee and the President, cognisance will be taken by the Internal Auditors appointed by the College of the current status of the Institutional Risk Register and local risk registers. Internal audits of College functions/units will include an assessment of the effectiveness of their respective risk management processes and will provide independent assurance to *An tÚdarás Rialaithe*, through its Audit & Risk Committee, that risks are being managed appropriately.

4.0 RISK MANAGEMENT FRAMEWORK

4.1 The Risk Management Framework is an iterative process consisting of steps which, taken in sequence, enable continuous improvement in decision-making. It constitutes a logical and systematic method of identifying, analysing, evaluating, managing, monitoring, communicating and mitigating risks associated with any activity, function or process such that the College is positioned to minimise loss and maximise opportunity. This iterative process may be expressed as the following cyclical work-flow:



4.1.1 The MIC Risk Management Framework provides assurance from Academic and Professional Service functions to the senior management team (ET and SPG) and, through the team, to the Audit & Risk Committee and *An tÚdarás Rialaithe*. Effective risk management focuses on understanding, measuring and mitigating for risk rather than necessarily avoiding or totally eliminating it and comprises the following components:

4.1.2 **Risk Identification:**

The purpose of risk identification is to produce a list of the potential risks that could impact on the College achieving its strategic and/or operational objectives. Risks will be identified (commonly under four pre---defined categories as set out in Section 2.1.1) and prioritised using a variety of techniques. A formal risk identification and review exercise will be undertaken on a quarterly basis in order to update both the Fundamental Risk Register and local risk registers as required.

4.1.4 **Risk Assessment:**

Risk assessment is completed by examining the consequences of the risk materialising, the vulnerabilities associated with each risk and the existing controls in place to mitigate each risk, where 'consequences' will be taken to mean **negative or positive outcomes** and 'vulnerabilities' will be taken to mean **weaknesses in existing work practices, processes, systems or personnel**. During the risk assessment stage, appropriate quantification of risk is critical to an effective Risk Management Framework. Not all risks are of equal weighting and effective risk management is only possible if risks are a) measured and b) prioritised appropriately.

4.1.4.1 **A) Measurement**

The size (rating) of any risk will be measured using two factors of occurrence: likelihood of occurrence and business impact of occurrence. Each factor incorporates a separate scale which, in order to ensure consistency across the various levels of risk management, must always be applied during the risk assessment stage of the process. These scales are as follows:

Business Impact Rating Scale:

- 1 No significant impact
- 2 Minor impact
- 3 Significant but containable impact
- 4 High impact
- 5 Extremely detrimental impact

Likelihood of Occurrence Rating Scale

1	Rarely, if ever	Not likely to occur in a 10---year time period
2	Possible	Likely to occur in a 10 year time period.
3	Likely	Likely to occur in a two year time period.
4	Very likely	Likely to occur in a 3---12 month time period
5	Almost unavoidable / already occurring	Likely to occur in next 3 months.

Calculation of Risk Rating

A rating metric for each risk that is identified is arrived at by multiplying the business impact score by the likelihood of occurrence, with the spectrum of risk extending between a score of 1 and 25. Within this spectrum, the following bands of risk will apply:

Low:	1 --- 7.99
Medium:	8 – 19.99
High:	20 --- 25

4.1.4.2 B) Prioritisation

Risks should be prioritised according to their ability to prevent the College from achieving its continuum of objectives. Once the risk identification and measurement process has taken place, individual risks should be located within either the Fundamental Risk Register or a local risk register by assessing the extent to which the risk is biased towards the core institution---level objectives of the College (or local goals) and falls toward the one end of the spectrum of impact or the other, as shown in the table attached at Appendix A, below (which illustrates risk effect according to the four categories of risk and the extent of their impact using the Business Impact Rating Scale)

4.1.5 Risk Mitigation:

An effective Risk Management Framework depends on the presence of a risk mitigation stage in the risk management process. Mitigation occurs once a risk has been identified, rated (measured and prioritised) and assigned an 'owner' (staff

member with overall responsibility for the area of College strategy or operations within which the risk falls). The risk is then off-set by an agreed mitigating action that has the effect of reducing the impact of the risk or diminishing or eliminating the possibility that it will occur. Mitigating actions must be contained in the risk register (Institutional Risk Register or local risk register) and, ideally, should be linked to the institutional Annual Operating Plan (AOP) or local AOP. Each mitigating action listed in a risk register must lead to an implementation report which presents sufficient evidence for the controllers of the risk register, ET, An tÚdarás Rialaithe and the Internal Auditor to be satisfied that risk has been reduced in terms of its occurrence likelihood and/or potential impact. This process takes place during the Monitoring & Reporting phase of the Risk Management Framework.

4.1.6 Risk Management & Reporting

4.1.6.1 Fundamental Risk Register

The Fundamental Risk Register will be monitored by the Executive Team on a three weekly basis. The purpose of this monitoring cycle is to situate ET in a position to track risk mitigation against implementation of the institutional AOP as well as to act upon the emergence of new risks between scheduled meetings of the Strategic Planning Group (SPG). At quarterly intervals, the SPG will convene to review the Risk Register in detail and this process will involve identification of new risks (as appropriate), reports by risk owners on the implementation status of mitigating actions, consideration of the current ratings in respect of listed risks, and agreement as to whether current risks should be re-rated, de-escalated, devolved to local risk registers (as relevant) or eliminated.

Following each meeting of the SPG, a risk management status report (inclusive of the current iteration of the Institutional Risk Register) will be presented to the Audit and Risk Committee which will consider the appropriateness and effectiveness of controls in place in respect of the institutional risks. Following each meeting of the Audit & Risk Committee a report, on its behalf, will be presented to An tÚdarás Rialaithe by the chair of the Audit & Risk Committee. Additionally, the President will provide a report to each meeting of the College Trustees which includes a statement of An tÚdarás Rialaithe's most recent deliberations in respect of the Institutional Risk Register.

4.1.6.2 Local Risk Registers

Each Academic unit (Faculty and Department), together with each Professional Services functional unit (Department/Office) will develop a local risk register immediate to their specific individual remit. Responsibility for development of such local risk registers lies with those members of the SPG to whom the

Academic and Professional Service units report. Local risks will be identified and rated according to the same metrics as above and mitigating actions will be selected and implemented, and linked to the operational plans of units with direct responsibility for the area covered by the risk. Each member of the SPG will be responsible for ensuring that this linkage occurs and that a coordinated response takes place where more than one Academic or functional unit has responsibility for a risk and its mitigation.

Formal review of local risk registers will take place as follows:

- During internal audit of any area or service to which a local risk register is linked directly (in which case the Internal Auditor will conduct the review in consultation with the Audit & Risk Committee and the SPG member with oversight of the risk register in question);
- Following any major changes to the structure, funding or strategic direction of the Academic / Professional Service department or unit with ownership of the risk register (in which case the SPG member with overall responsibility for the Academic / Professional Service department will present the local risk register, together with revisions proposed, to the SPG for consideration);
- Following a specific request by ET for presentation of a local risk register to the SPG, for review, via the SPG member with overall responsibility for the Academic / Professional Service department within which the local risk register is maintained

4.1.7 **Risk Appetite**

The College's tolerance of risk, or 'risk appetite' is characterised by how it accepts and manages risk. Risk elements arising from proposed or actual developments/activities within the College may fall into three categories:

- Risks that are trivial and therefore acceptable and do not need to be managed;
- Risks that are acceptable and routinely arise in certain types of activity and that will need to be managed;
- Risks that are found to be unacceptable and therefore the development/activity should not proceed.

4.1.8 **Management of Risk**

Upon completion of a given risk assessment and taking account of the institutional risk appetite, the College will decide to:

- Treat the risk by application of internal controls, including the incorporation of the risk and its corresponding mitigation within the Institutional Risk Register (or a local risk register if the risk is of such character that its placement at this remove is more appropriate;

- Tolerate the risk by incorporation of the risk within the Institutional Risk Register, absent any mitigating action which would serve to reduce or eliminate the risk significantly;
- Terminate the risk by ceasing or otherwise reconfiguring the progenitor activity or development such that the risk is reduced or eliminated;
- Transfer the risk (e.g. by inviting insurers or sub-contracting parties to adopt the risk)

5.0 REVIEW OF POLICY

This policy will be reviewed every five years normally, except as circumstances necessitate earlier review.