



Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Inspiring Generations

The Campaign for Trinity College Dublin

RISK MANAGEMENT POLICY TRINITY DEVELOPMENT & ALUMNI



Version Control Risk Management Policy

Version	Reviewed / Approved by	Date
June-19	Audit & Risk Committee	19 June 2019
June-19	Board of Trustees	23 October 2019
October 2020	Director of Operations	September 2020
October 2020	Audit and Risk Committee	1 October 2020
October 2020	Board of Trustees	5 November 2020



1. Purpose of this policy

1.1 The purpose of this document is to;

- Provide a framework to support TD&A in formally identifying, assessing, managing and reporting on risk
- Provide a framework for TD&A to measure likelihood and impact of risks to it in a dynamic and progressive manner
- Establish responsibilities for overseeing the effectiveness of risk management
- Establish responsibilities for managing and participating in the formal risk management processes
- increase overall awareness of risk throughout the organisation and to enable managers and those responsible for risk reporting, to better identify, assess and control risks within their areas. It seeks to enforce ownership

2. Scope

2.1 This Policy applies across all divisions of TD&A to all staff and across all activities and all areas.

3. Risk Management Objectives

3.1 TD&A recognises that the application of risk management is an important element of good governance and assists the TD&A in achieving its stated objectives. Effective risk management provides the Board of Trustees, management and staff with assurance regarding the effective management of risks that may threaten the achievement of stated objectives. Specifically, the rigorous analysis and management of uncertainty surrounding these objectives will assist TDA in ensuring that threats are mitigated whilst opportunities are advanced.

4. Risk Management Framework

4.1 Proactive risk management provides the Board, management and staff with assurance regarding the effective management of risks that may threaten the achievement of stated objectives.

4.2 The Risk Management Framework is developed with the capacity to effectively adapt to the changing environment in which TD&A finds itself. It strives to align itself with the TD&A Strategic Plan supported by agreed risk management principles derived from both the experience of the TD&A and the risks it seeks to manage.

4.3 The Risk Management Framework outlines the process of measurement of risk or opportunities resulting in one of the following risk ratings:

- i) Green is defined as a low risk
- ii) Amber is defined as a medium risk
- iii) Red is defined as a high risk



These ratings have defined limits of measurement and are assessed based on experience, incident and other environmental factors deemed relevant.

- 4.4 The process of measuring the risk of likelihood and impact is considered between the ratings of 1 to 5.
- 4.5 Inherent risk is defined as the risk without controls whilst residual risk is assessed against the effectiveness of the controls managing the risk.

5. Risk Appetite

- 5.1 Risk appetite refers to “the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time” (The Orange Book: The Management of Risk – Principles and Concepts). TD&A has a responsible approach to risk management, seeking to recognise and manage exposure to risks.
- 5.2 TD&A recognises that to successfully deliver on its mission and objectives it must be prepared to avail of opportunities where the potential reward justifies the acceptance of certain risks. TD&A seeks to minimise its exposure to reputational, compliance and financial and reputational risk, whilst accepting and encouraging an increased degree of risk in pursuit of its mission and objectives.
- 5.3 TD&A will review its risk appetite annually in light of changing circumstances in its wider environment and in its capacity to bear risk.

6. Risk Management Responsibilities

- 6.1 All TD&A staff have a responsibility to engage in effective risk management. Directors will be responsible for encouraging good risk management practice within their area.
- 6.2 The governance of TD&A lies ultimately with the Board of Trustees. Governance is the system by which TD&A is directed and controlled in order to achieve its objectives and meet the necessary standards of accountability, probity and compliance. Risk management is an essential element of the process of governance.
- 6.3 The Board has responsibility for overseeing the management of risk within the College as a whole. The Board:
 - Approves the risk management policy and monitors the effectiveness of risk management processes
 - Sets the risk appetite, and approves the TD&A wide risk register at least annually



- Reviews material risk incidents and notes or approves management's actions, as appropriate
 - Includes risk management as a specific item for discussion on the agenda at least annually, and as an agenda item throughout the year as the need arises
 - Considers the formal risk assessment and management actions when considering all major proposals brought to Board for approval
 - Receives and considers reports from the Audit & Risk Committee on the effectiveness of the systems of Risk Management
 - Includes risk management experience/expertise in the competencies of at least one Member
 - Reviews management reporting on risk management and note/approve actions as appropriate
 - Require independent review of effectiveness of risk management on a periodic basis
- 6.4 The Director of Advancement is responsible for the executive management of TD&A and its day-to-day direction. The Director of Advancement is supported by the Senior Management Team which has responsibility for overseeing the operational running of TD&A including risk management. The Director of Advancement is responsible for ensuring that the Senior Management Team effectively execute their responsibilities and for drawing to the immediate attention of Board to any instances where risks are being incurred which exceed the risk appetite or if a major breakdown in the system occurs.
- 6.5 The Senior Management Team (SMT) are responsible for monitoring and recording risk. They are responsible for identifying and implementing appropriate and effective mitigating actions to reduce or eliminate risks subject to direction by the Director of Advancement and Board as appropriate. SMT are responsible for ensuring that risk management is embedded throughout the organisation, that TDA staff have sufficient awareness of this Risk Management Policy and the Risk Appetite Statement and that staff receive the necessary training to ensure risk is managed in an effective manner.
The Senior Management Team will include risk management as a standing agenda item at its meetings.
Responsibilities of the Senior Management Team include:
- Guide and oversee the development of the risk management policy
 - Embedding risk awareness and management throughout the organisation
 - Oversee the development and implementation of processes to support the identification, assessment, management and reporting of risk
 - Review the risk register(s) produced to ensure that risk management policy and guidance have been consistently adhered to in all TD&A functions
 - Report to the Board and Audit & Risk Committee
 - Monitor the effectiveness of risk management
 - Promote the ongoing enhancement of risk management processes
- 6.6 The Director of Operations has overall responsibility for Risk Management.
Responsibilities include;
- Report directly to the Board (and Audit & Risk Committee) at least bi-annually



- Ensure the implementation of the risk management policy
 - Coordinate the formal risk management process
 - Ensure all individuals with responsibility for risk management are provided with guidance appropriate to their responsibilities.
- 6.7 As heads of function, each Director is responsible for overseeing the formal risk management processes in their respective functions.
Responsibility include:
- Review and approving risk register in their areas of responsibility
 - Escalate significant risks to the Senior Management Team as the need arises
 - Ensure that risk registers are prepared to the appropriate standard and on a timely basis
- 6.8 The Operations Manage Team (OMT) have an important role in risk management within TDA. Their responsibilities include:
- coordinating the preparation and updating of local risk registers
 - agreeing the appropriateness and effectiveness of current controls
 - reviewing the risk rating for each risk on the register
 - agreeing the action plan and timelines to put in place mitigants to reduce or eliminate the risk
 - assigning responsibility for each action
- ongoing monitoring of the action plan
- The OMT will review and approve TDA's full risk register at least every 6 months and present to SMT for comment and approval
- 6.9 All TD&A staff have responsibility for risk management. Responsibilities in this regard may include;
- Own and manage risks delegated in the risk registers
 - Be aware of TDA's risk management framework and policy
 - Comply with controls as stated in risk registers
 - Escalate control gaps / weaknesses
 - Participate in the formal risk management process as required by those charged with overseeing and managing the risk management function
 - Report systematically and promptly to the Director of Operations any perceived new risks or failures of existing control measures
- 6.10 The Audit & Risk Committee should review and monitor at a high level the effectiveness of processes for managing risk. The Committee should have risk management as a periodic standing agenda item at its meetings and should exchange information with the Board and the Director of Advancement regarding the effectiveness of the risk management system. The Audit Committee should:
- Review and challenge the TDA-wide Risk Register



- Review and monitor the action plans included with the Risk Register and report to the Board of Trustees accordingly
- Review and monitor the effectiveness of the system of risk management
- Approve the Risk Based Internal Audit Plan
- Provide guidance to the externally contracted Internal Audit function focusing on key areas for review

6.11 The Internal Auditors should

- Provide objective assurance to the Audit Committee and Board on the effectiveness of the organisation risk management system
- Assess if key business risks are being managed appropriately and that the system of internal control is operating effectively

7. Risk Management Process

7.1 The risk management processes will be developed, monitored and enhanced under the guidance of the Senior Management Team taking account of the following principles:

- The risk process and enhancements will be communicated and rolled out with appropriate support to all levels of TD&A
- Risk management will be embedded within normal management processes so that risk issues are owned and managed by those involved in the day to day running of TD&A at all levels. This will entail the coordination of operational strategic and business planning with risk identification, assessment and management at unit level across TD&A as well as a top down assessment of risk
- In identifying risks regard will be had to all possible internal and external sources of risk including strategic objectives, compliance obligations, governance risks and cover all activities
- In assessing risk levels, the effectiveness of existing controls in place will be assessed
- A common system for assessing risk will be established across all areas
- All risks will have named individuals as risk owners
- All actions will be regularly monitored by OMT, and progress reported to the Senior Management Team by risk owners
- The Director of Operations will monitor and report at regular intervals throughout the year to Senior Management Team on actions to manage risks and changes in risks identified and will report to the Board and Audit & Risk Committee at least bi-annually

7.2 Risk Management is a process to identify, assess, manage and control potential events or situations in order to manage the impact or likelihood of unfortunate events or support the realisation of opportunities

7.3 Risks should be recorded on the Risk Register in a way to be clear to all readers/stakeholders. Risks should be clearly expressed and the structure of the risk should clearly separate the:



- Vulnerability;
- Cause; and
- Consequence;

In summary, the “Risk that X occurs due to Y”

- 7.4 The risk process considers and documents what controls are in place and implemented to mitigate the identified risk
- 7.5 Controls may be defined as “any action taken to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organises and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved
- 7.6 Controls should be easily understandable and should clearly demonstrate the checks or safeguards in place to manage risk. Controls are only to be included if they are currently in place
- 7.7 Each individual risk should be assessed by analysing both the impact and likelihood of the risk occurring; this is achieved by use of the following scoring based criteria:

Impact	Likelihood
1 = Little or no impact	1 = Rarely, if ever
2 = Insignificant	2= Possible
3 = Minor Impact	3 = Likely
4 = Significant but containable impact	4= Very Likely
5 = High Impact	5 = Almost Certain

- 7.8 This risk assessment is performed on a “net” or “residual risk” basis i.e. after consideration of the effectiveness of controls to reduce the identified risk
- 7.9 The resulting risk assessment is recorded in the risk register, which is derived from multiplying the Impact x Likelihood, may be classified as follows:
- Low (0 – 7)** - This is on track but with some concerns that need to be addressed, should not require much attention but should be reviewed annually.
- Medium (8 – 15)** - some significant concerns which could be damaging if not addressed; should be monitored and reviewed on a periodic basis and actioned when possible.
- High (16+)** - problematic; serious concerns, high risk to overall performance, serious impact on ability to organisation to deliver key KPIs, should be on senior management agenda, monitored frequently, and actioned where possible.
- 7.10 Following the performance of risk assessment, additional checks of safeguards (actions) that are required to manage the risk, but are not currently in place should be documented in the risk register



- 7.11 The owners of each action along with a timeline for completion should also be included
- 7.12 The risk registers once drafted should be reviewed by the Operations Management Team before being sent for review and approval to the Senior Management Team at least twice a year
- 7.13 The Risk Register should be reviewed on a half yearly basis and updated for:
 - Any new risks
 - Any updates to the risk assessment (High, Medium, Low)
 - Any updates to completed actions
 - Any identification of new actions to be undertaken
- 7.14 The Director of Operations will present the Risk Register and associated Action Plan to the Audit & Risk Committee and Board at least twice per year
- 7.15 The Director of Operations will liaise with the University's Chief Risk Officer to ensure TDA's risk register is included within the University's Corporate Risk Register