Trinity Development & Alumni

Risk Management Policy

Version No: 1.3
Issue Date: October 2019
Last Review Date: May 2024

1. Purpose

The purpose of this policy is to:

1.1 Provide a Structured & Systematic Risk Framework

- to identify, assess and manage risk
- to enable prioritization of risks based on their potential impact and likelihood
- to provide a foundation for developing and implementing effective mitigation strategies and controls.

1.2 Promote Risk Awareness, Understanding & Ownership

Facilitate clear communications about TDA's risk tolerance and risk management strategies to increase awareness and understanding of risks and promote ownership among all stakeholders, employees and decision makers.

1.3 Ensure Strategic Objective Alignment

Ensure that risk management efforts are aligned with TDA's Strategic Objectives.

1.4 Governance and Compliance

Ensure compliance with relevant laws, regulations, and industry standards related to risk management, enhancing overall governance and accountability.

1.5 Decision Support

Serve as a tool for decision-makers by providing relevant information about risk appetite, identification and assessment of potential risks, allowing for more informed and strategic decision-making.

1.6 Financial Stability

Contribute to financial stability by helping to identify and manage risks that could have financial implications, ensuring the organization's long-term sustainability.

1.7 Continuous Improvement

Establish a foundation for continuous improvement by regularly reviewing and updating risk management practices to adapt to changes in the business environment.

2. Scope

2.1 This Policy applies across all divisions of TDA to all staff and across all activities and all areas.

3. Risk Management Objectives

3.1   The existence of a robust risk management framework is an integral part of good governance and assists TDA in achieving its strategic objectives. Specifically, the identification, analysis and management of uncertainty surrounding these objectives will assist TDA in ensuring that threats are mitigated whilst opportunities are advanced.
The risk management framework provides management and staff guidance regarding the risk appetite of the Board of Trustee and expectations regarding the mitigation of risks that potentially threaten the achievement of stated objectives.

4. Risk Management Framework

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

4.2   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.

4.3   The process of measuring the risk of likelihood and impact is considered between the ratings of 1 to 5.

4.4   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). TDA has a responsible approach to risk management, seeking to recognise and manage exposure to risks.

5.2   TDA 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. TDA seeks to minimise its exposure to reputational, compliance, financial and reputational risk, whilst accepting and encouraging an increased degree of risk in pursuit of its mission and objectives.

5.3   TDA 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 Roles & Responsibilities

6.1   The governance of TDA lies ultimately with the Board of Trustees. Governance is the system by which TDA 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.

6.2   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 TDA 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

6.3   The Chief Advancement Officer (CAO) is responsible for the executive management of TDA and its day-to-day direction. The CAO is supported by the Senior Management Team which has responsibility for overseeing the operational running of TDA including risk management. The CAO 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.

6.4   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 CAO 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.

SMT will include risk management as a standing agenda item at its meetings at least twice per year to review and approve the risk register.
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 TDA functions
- Report to the Board and Audit & Risk Committee
- Monitor the effectiveness of risk management
- Promote the ongoing enhancement of risk management processes

6.5 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.

6.6 As heads of function, each Director is responsible for overseeing the formal risk management processes in their respective functions.
Responsibility includes:
- 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.
- Ensure that a risk assessment is undertaken prior to the commencement of any new project or significant new process

6.7 The Operations Manage Team (OMT) have an important role in risk management within TDA. Its 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.

6.8 All TDA 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

6.9 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 CAO regarding the effectiveness of the risk management system. The Audit Committee should:
- Review and challenge the TDA 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

6.10 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 Profile

7.1 TDA is exposed to several risk categories which are reflected in the Risk Appetite Statement. Risks in the Risk Register will be classified against one of the categories set out below accepting that some risks may apply to more than one category:
a) Fundraising and Alumni Engagement
b) Reputation
c) Compliance
d) Financial
e) People & Culture
f) Operations
g) Information Technology Risk
h) Environment, Social and Governance

TDA must ensure that it can adequately address these risks as the arise and ensure a contingency is in place.

8. Risk Management Process
8.1 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 TDA
- 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 TDA at all levels. This will entail the coordination of operational strategic and business planning with risk identification, assessment and management at unit level across TDA 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

8.2   Risks should be recorded in a clear, comprehensible format highlighting the Vulnerability, Cause and Consequence. 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"*

8.3   The risk process considers and documents what controls are in place and implemented to mitigate the identified risk.

8.4   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

8.5   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

8.6   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

8.7   This risk assessment is performed twice, firstly an assessment of the 'Inherent' risk, i.e. an assessment of the risk before any existing mitigants are taken into account and then on a "net" or "residual risk" basis i.e. after consideration of the effectiveness of controls to reduce the identified risk.

8.8   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.

8.9   Following completion of the risk assessment, any additional, required mitigating actions to further manage the risk will be recorded on the risk register.The owners of each action along with a timeline for completion should also be included.

8.10   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.

8.11   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

8.12   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.

8.13   The register presented to the Audit & Risk Committee will include those risks which management deem should be removed or which have been fully mitigated against however Risks will only be removed from the Register once the Committee has reviewed and approved.

8.14   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 Risk Register.

8.15   TDA will collaborate with the University Risk Management Office and utilise the Trinity College online Risk Management System to record the final risk register.

POLICY VERSION HISTORY

Version	Date	Brief Summary of Change	Owner's Name
V1.0	19/06/2019	Initial Document approved by TF ARC Committee	David O'Shea
V1.0	23/10/2019	Reviewed and approved by trustees	David O' Shea
V1.1	05/11/2020	Reviewed and approved by TF ARC and trustees	David O' Shea
V1.2	25/11/2021	Reviewed and approved by TF ARC and trustees	David O' Shea
V1.3	18/06/2024	Reviewed and approved by TF ARC and trustees	David O' Shea

CONSULTATION PROCESS DETAILS

REVIEW AND CONSULTATION PROCESS	The policy owner will implement a two-tier review process which involves both an annual scan of the policy and supporting processes to ensure alignment with relevant University policies and any legal updates; and a deep dive review of the policy and supporting processes every three years to ensure alignment, relevance, and implementation measures are in place. Reviews to be approved by TDA Director of Operations.
ASSOCIATED DOCUMENTATION	**Legal Framework:** Charities Act 2009, Charites Governance Code **Trinity Policies:** University Risk Management Policy May 2022 https://www.tcd.ie/about/policies/assets/pdf/Risk-Management-Policy-May2022.pdf

RESPONSIBILITIES & DISTRIBUTION

IMPLEMENTATION & TRAINING:	Implementation: Initial training and Statement issued to all new staff at induction; Annual all staff training; OMT review bi-annually prior to review of Risk Register Training: Director of Operations
DISTRIBUTION METHODS:	• Soft Copy distributed to all staff on induction. • Available on Staff Bamboo HR system.
FOR FURTHER INOFRMATION ON THIS POLICY	Name: David O' Shea E-mail: OSHEADA@tcd.ie