Technological University of the Shannon:
Midlands Midwest

Ollscoil Teicneolaíochta na Sionainne:
Lár Tíre Iarthar Láir

Risk Management Policy

October 2021

www.tus.ie

Contents

1.0 Purpose

The Technological University is committed to establishing and maintaining a systematic approach to the identification assessment and management of risk. The purpose of this policy is to ensure that risks to the Technological University are identified, assessed and managed to enable the Technological University to operate within an acceptable level that has been defined and approved. In order to achieve this objective, the Technological University will be required to identify risks and determine how they may be tolerated, treated, transferred or terminated on an ongoing basis.

2.0 Scope

This policy sets out the Technological University's risk management process, risk appetite statement and how the success of the policy is to be measured. This policy applies to all [Faculties / Departments] and Functions within the Technological University, both academic and support, and includes campus companies and research centres. These functions are collectively referred to hereinafter in this policy as the 'Technological University'. Appendix A provides definitions of key terms used throughout the document.

3.0 Risk appetite

The Technological University's appetite for risk varies according to the activity undertaken. Table 1 below outlines the Technological University's risk appetite across its primary activities. This risk appetite should be utilised when making decisions that affect the Technological University in pursuit of its mission and objectives. It recognises that its appetite for risk varies according to the activity undertaken,and that its acceptance of risk is subject always to ensuring that potential benefits and risks are fully understood before developments are authorised, and that sensible measures to mitigate risk are established.

The Technological University's appetite for risk across its activities is provided in the following statements, and is illustrated diagrammatically. Activities are expected to be calibrated by each Technological University. Table 1 For Illustrative purposes only at this stage.

TABLE 1 – *Indicative activities*	Indicative Low Appetite — Indicative High Appetite
Reputation	
Compliance	<>
Financial Performance and sustainability	< >
Research	< >
Education and Student Experience	< >
Knowledge Exchange	< >
International Development	< >
Organisation Change	< >
TU objective	< >
Environment and social responsibility	< >
People and culture	< >
Health and Safety	<>
IT resilience and business continuity	< >
Data and management information	< >

The below statements are illustrative and should be updated for each Technological University and for each line item in the table above as per the examples below:

Reputation – It is regarded as critical that the Technological University preserves its reputation at all times. The Technological University therefore has no appetite for risk in the conduct of any of its activities that puts its reputation in jeopardy, could lead to undue adverse local or national publicity, or could lead to loss of confidence by the Irish political establishment or local stakeholders.

Compliance – The Technological University places great importance on compliance, and has no appetite for any breaches in statute, regulation, professional standards, ethics, bribery or fraud. It wishes to maintain accreditations related to courses or standards of operation, and has low appetite for risk relating to actions that may put accreditations in jeopardy.

Financial Performance and sustainability – The Technological University aims to maintain its long-term financial viability and its overall financial strength. Minimum criteria to be updated per Technological University: For example;

Achieve a target surplus of a minimum of an average of 2% of gross income per annum over any 3-year period.

(An alternative Risk Appetite statement approach is located below within Appendix D)

4.0 Risk management process

Risk management is the systematic application of management policies, procedures and practices to identify, assess and manage risk effectively while reporting to the relevant stakeholders of the Technological University. There are six phases to the process as follows:

4.1 Risk analysis

Risk analysis is performed at least [each quarter / each semester / twice yearly] to facilitate the analysis of new and existing risks facing the Technological University. The risk analysis is conducted using a combination of bottom up and top down reporting across the following risk categories:

- Strategic risk
- Reputational risk
- Compliance risk
- Financial risk
- Operational risk (including Health and Safety).

A risk detailed on the Risk Register should be concise, self-explanatory, and should deal with only one risk.

Each [Faculty / Department] and Function is required to maintain an up to date Risk register detailing the key risks specific to their area.

The *Technological University Senior Team* are responsible for maintaining an up to date Technological University Risk Register which contains high level risks to the Technological University along with any relevant risks identified within the [Faculty /Departmental] and Functional Risk Registers.

Maintenance of the Technological University Risk Register is facilitated by the VP Finance & Corporate Governance who is responsible for compiling the key risks from each [Faculty / Department] and Function Risk Register and updating the Technological University Risk Register to reflect changes in the key risks across theTechnological University as agreed by the Technological University Senior Team. Individual managers remain responsible for managing risks in their respective areas.

The process of updating of the Technological University Risk Register may also be triggered by the Audit &Risk Committee, the Technological University Senior Team or the VP Finance & Corporate Governance at any stage during the year if a new risk is identified that warrants immediate attention.

4.2 Gross risk assessment

Following the risk analysis, the gross (inherent) risk rating of each risk within the risk register is assessed. The impact and likelihood of the gross risk is assessed prior to the consideration of any controls or actions taken by the Technological University to manage the risk. Impact and likelihood are assessed on the scale as outlined within Appendix C. An overall gross risk rating is assigned based on the product of the impact and likelihood scores. The assessment of gross risk is recorded on the risk register. This step is applicable to the [Faculty / Departmental] and Functional Risk Register as well as the Technological University Risk Register.

4.3 Identification of controls

Following the Gross risk assessment, the controls in place to manage each risk are assessed. Each control is designed to reduce exposure to the risk by preventing a negative outcome from occurring or detecting that it has occurred and ensuring corrective actions are taken. Controls reduce exposure to risk but cannot eliminate it in full. As good practice, the assessors should seek to identify a mix of preventative and detective controls. Controls identified are recorded on the risk register. The controls in place should be assessed to determine if they remain relevant and to determine if new controls could also be included.

This step is applicable to the [Faculty / Departmental] and Functional Risk Register as well as the Technological University Risk Register.

4.4 Net risk assessment

Following identification of controls, the net (residual) risk rating of each risk is assessed. The impact and likelihood of the net risk is assessed after consideration has been given to the effect of controls identified in 3.3 on impact and likelihood. Impact and likelihood are assessed on a [four/five] point scale as outlined within Appendix C. An overall net risk rating is assigned based on the product of the impact and likelihood scores. Where controls have been identified as having changed since the last review it is likely that there may be a change in the net risk assessment.

The assessment of net risk is recorded on the risk register. This step is applicable to the [Faculty / Departmental] and Functional Risk Register as well as the Technological University Risk Register.

4.5 Identification of mitigating actions (to reduce risk)

The net risk identified during the net risk assessment can either be tolerated, treated, terminated or transferred.

Tolerating the risk is a formal acceptance of the net risk, the acceptance and capacity to manage the net risk in the event of a risk failure and acknowledgement that no further action is required.

The **treatment** of risk requires management to identify mitigating actions which will further reduce the risk to an acceptable level.

Risk may also be **transferred** through the use of insurance or similar instruments.

Actions taken to treat or transfer risk are recorded on the risk register as 'mitigating actions. Best practice recommends that actions are Specific, Measureable, Achievable, Realistic, and Time-bound ("SMART").

If the net risk is deemed excessive to the Technological University the activity giving rise to the risk should not be undertaken, **terminating** the risk. This decision should be made in the context of the Technological University's risk appetite outlined in section 4.0.

Contingency actions may be included per the second example risk register template in Appendix D. These outline actions that may be anticipated to be taken should the risk materialise.

This step is applicable to the [Faculty / Departmental] and Functional Risk Register as well asthe Technological University Risk Register.

4.6 Monitoring and reporting of the Risk Management Plan

Risk monitoring and reporting procedures are required to ensure an effective risk management plan and process is maintained on an ongoing basis.

4.6.1) Each [quarter / semester /twice yearly period], on completion of steps outlined in 3.1-3.5 the [Faculty / Departmental] and Functional risk registers and a report detailing the trajectory of any changes in the top 10 risks are submitted to the VP Finance & Corporate Governance by the Dean of [Faculty / Department] or Function within 30 days of the review period end.
4.6.2) The VP Finance & Corporate Governance considers which risks from the [Faculty / Departmental] and functional risk registers warrant inclusion in the Technological University register and presents an updated Technological University Risk Register to the Senior Team for review and sign off. A "Risk Committee" may be established to assist the VP Finance & Corporate Governance fulfil their duties in this process.

All risks with a net risk rating of above [12 (for 4x4 model) /15 (for 5x5 model)] must be included in the register and the VP Finance & Corporate Governance may also use their discretion to include other risks or raise a risk for inclusion where it is observed that a lower risk item is trending within a number of [Faculties / Departments] or Functions but not rated greater than a net riskrating of [12 (for 4x4 model) /15 (for 5x5 model)].

The net risk rating reporting threshold of [12 (for 4x4 model) /15 (for 5x5 model)] can only be changed with the approval of the Audit & Risk Committee.

The updated Technological University Register and the [Faculty / Departmental] and Functional risk registers(if requested) facilitate the Technological University Senior Team completing steps 3.1 to 3.5 above for the Technological University Risk Register.

The Senior Team are responsible for approving the Technological University Risk Register each review period.

4.6.3) Annually the Risk Management Policy including risk appetite, the Technological University Risk Register and the Risk Management Plan are reviewed and recommended by the Audit & Risk Committee to the Governing Body for approval.

4.6.4) Key Performance Indictors on risk are provided to the Audit & Risk Committee once per review period detailing:

- The top 15 risks to the Technological University and changes to the trajectory of each of those risks;
- Significant control failures identified during the review period; and
- Updates on mitigating actions within the Technological University Risk Register which have missed their deadlines.

Annually the Audit & Risk Committee will report to Governing Body in relation to the effectiveness of the Technological University's risk management process. The Audit & Risk Committee may also update Governing Body of any critical risk management developments during the remainder of the year.

5.0 Measuring success

The Technological University measures and reports upon the success of the overall risk management process annually.

Success is measured by tracking actions taken to address key risk areas and the achievement of reduced risk across the Technological University.

6.0 Review of policy

The Technological University policy is reviewed by the Audit & Risk Committee and approved by theGoverning Body annually.

Appendix A – Definitions & Localisation Glossary

Definitions

Risk: Any uncertain event that could significantly impede or enhance the ability to achieve objectives.

Risk Appetite: This is the level of risk that an organisation is prepared to accept in pursuit of its objectives, and before action is deemed necessary to reduce the risk. It represents a balance between the potential benefits of innovation and the threats that change inevitably brings.

Risk Management: the systematic process of identifying, assessing and managing risk to acceptable levels.

Technological University Risk Register: This is a risk recording and monitoring tool for the management of the Technological University. The register acts as a repository for all key risks identified and includes details of the risk rating assigned to the risk as well as details of the mitigating controls and actions which manage the risk.

Impact: The risk impact is assessed by examining the consequences of the risk materialising.

Likelihood: The likelihood should be assessed by considering the vulnerabilities associated with the risk which exist within the Technological University's internal and external environment.

Consequences: Negative or positive outcomes.

Vulnerabilities: Weaknesses in existing work practices, processes, systems or people.

Gross Risk: The level of risk before mitigating controls are considered.

Net Risk: The level of risk remaining after considering mitigating controls.

Strategic Risk can be defined as the inability to achieve the Technological University's strategic goals or objectives as set out in the Strategic Plan and risk of not availing of opportunities when they arise.

Reputational Risk is defined as exposure to losses arising as a result of bad press, negative public image and the need to improve stakeholder relationship management.

Compliance Risk is defined as the risk of legal sanctions, material financial loss, or reputation loss the organisation may suffer as a result of its failure to comply with laws, its own regulations, code of conduct, and standards of best/good practice.

Financial Risk can be defined as the exposure to losses arising as a result of the need to improve the management of the Technological University's financial assets.

Operational Risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

Control activity: An action taken to minimise the negative consequences of a risk. A control differs from a process activity as a well-designed control should either prevent a negative consequence from occurring in the first place or detect that the negative consequence has occurred and initiate corrective actions. Control wording should be very clear regarding:

- Who is responsible
- What action is performed
- When is it performed

Mitigating actions: A mitigation action is a specific action, project, activity, or process taken to reduce or eliminate long-term risk. Mitigating actions may be 'one off' in nature rather than reoccurring and may involve changes to operating procedures such as the introduction of a new control.

Localisation Glossary:

The following term requires update within the Policy to reflect the circumstances of the individual Technological University:

ST –Senior Team

Appendix B - Roles & Responsibilities

Group / Function	Roles & Responsibilities
Governing Body	• Oversee responsibility for risk management within the Technological University. • Confirmation in the annual report that the Governing Body has carried out an assessment of the Technological University's principal risks, including a description of these risks, where appropriate, and associated mitigation measures or strategies. • Review management reporting on risk management and note/approve actions as appropriate; • Provide final approval of the Technological University Risk Management Policy and any amendments thereto at least annually. • Provide final approval of the Institutional Risk Register and any risk tolerances / risk management plans identified within at least annually. • Approve the Technological University's risk appetite and risk management plans (via approval of the Risk Management Policy) at least annually. • Establish an Audit and Risk Committee to give an independent view in relation to risks and risk management systems. • Make risk management a standing item on the Governing Body meeting agenda. • Require periodic external review of effectiveness of risk management framework. • Advising the relevant Minister of the need to include risk management experience/expertise in the competencies of at least one Governing Body member. Where composition of the Board does not allow for this, expert advice should be sought externally.
Audit & Risk Committee	• Coordinate with the Governing Body in respect of its oversight of the Technological University's risk management function including : ○ Approval of the Technological University Risk Management Policy and any amendments thereto. ○ Approval of the Technological University Risk Register and any risk tolerances identified within. ○ Approval of the Technological University s risk appetite (via approval of the Risk Management Policy).

Group / Function	Roles & Responsibilities
	• Ensure ongoing review of the operation and effectiveness of the Technological University's Risk Management process. • Meet with the VP Finance & Corporate Governance to discuss contents of risk reporting as required. • Report to the Governing Body in relation to the effectiveness of the Technological University s risk management process on anannual basis.
President	• Ensure processes and procedures are in place within the Technological University to facilitate adherence to the Risk ManagementPolicy.
Technological University VP Finance & Corporate Governance	• Identify, measure and manage risk across the Technological University. • Ensure provision of adequate training across the Technological University. • Ensure adequate communication of the Risk Management process across the Technological University. • Promote a risk management culture. • Submit a risk management report and up to date Technological University Risk Register to the Senior Team each review period. • Attend Audit & Risk Committee meetings to report on risk as required.
Technological University Senior Team (including President)	• Maintain an up to date Technological University Risk Register. • Implement the Risk Management policy and advocate a Risk Management culture. • Communication of Strategic/ Technological University level development affecting functional risk management practice.
Heads of Faculty / Departments & Support	• Prepare and maintain [Faculty / Departmental] or Functional risk registers in line with the Technological University s RiskManagement Policy.

Group / Function	Roles & Responsibilities
Functions, Directors of Research Centres	• Monitor the effectiveness of controls and action status on an ongoing basis. • Coordinate with the VP Finance & Corporate Governance in risk management reporting each review period.
All staff / employees	• Ensure cooperation with all parties in the implementation of the Technological University risk management process and policy. • Raise risks to Heads of Faculty & Support Functions, Directors of Research Centres for inclusion within Functional / Departmental risk registers

Appendix C - Risk assessment tools

To ensure consistency across the Technological University the following method will be used in assessing risk [examples which may be customised are provided below]. Two options available; Option A, using a 4x4 score model and Option B, using a 5x5 score model.

1. Risk Impact Criteria - Option A - Risk Impact Criteria for a 4x4 score model

1. Risk Impact Criteria						
Description	**Strategic risk**	**Reputational risk**	**Compliance risk**	**Operational risk**	**Financial Impact**	**Score**
Extreme	Non-completion of capital project. Non-recruitment of key personnel.	Prominent coverage of Technological University in national media and /or political reaction	Breach in laws and regulations e.g. resulting in material fines, penalties being levied on the Technological University or funding being withheld	Serious impact on objectives e.g. closure of Technological University for >2days	>€1m or X% of Turnover	4
Serious	Failure to meet quality standards	Embarrassment within a department/function leading to adverse media or a significant number of student complaints	Breach in laws and regulations e.g. resulting in substantial fines and consequences	Significant impact on objectives Short to medium damage. e.g. unavailability of a faculty/service for >2 days	<€500-€1m or X% of Turnover	3
Moderate	Significant delay in the delivery of new programmes. Significant delay in the completion of capital project	Reputational impact in local/specialist area covered in the media or some student complaints	Breach in laws and regulations with no fine, and no regulatory investigation	Moderate impact on objectives. Some short term damage. e.g. disruption to a number of departments for a day	<€100-€500k or X% of Turnover	2
Minor	Minor delay in achievement of departmental goals	Potential damage evident to those close to the event/area of interest	Breach in laws and regulations noted but no consequences identified	Minimal impact on objectives. Minor Damage e.g. non-delivery of several classes during one day	<€100k or X% of Turnover	1

Option B - Risk Impact Criteria for a 5x5 score model

Description	Strategic Risk	Reputational risk	Compliance Risk	Operational Risk	Financial Risk	Score
Extreme	Non-completion of capital project. Non-recruitment of key personnel.	Prominent coverage of Technological University in national media and/or political reaction	Breach in laws and regulations e.g. resulting in material fines, penalties being levied on the Technological University or funding being withheld	Serious impact on objectives e.g. closure of Technological University for >2days. Serious debilitating injury/loss of life.	>€1m or X% of Turnover	5
Major	Failure to meet quality standards	Embarrassment within a department/function leading to adverse media or a significant number of student complaints	Breach in laws and regulations e.g. resulting in substantial fines and consequences	Significant impact on objectives Short to medium damage. e.g. unavailability of a department /function for up to 2 days. Injury requiring hospitalisation.	<€500-€1m or X% of Turnover	4
Moderate	Significant delay in the delivery of new programmes. Significant delay in the completion of capital project	Reputational impact in local/specialist area covered in the media or some student complaints	Breach in laws and regulations with no fine, and no regulatory investigation	Moderate impact on objectives. Some short term damage. e.g. disruption to departments / function for a day. Injury requiring attendance at medical facility	<€100-€500k or X% of Turnover	3
Minor	Minor delay in achievement of departmental goals	Potential damage evident to those close to the event/area of interest	Breach in laws and regulations noted but no consequences identified	Minimal impact on objectives. Minor Damage e.g. non delivery of several classes during one day.	<€100k or X% of Turnover	2
Insignificant	No impact	No impact on reputation	No impact on compliance	Consequences can be absorbed under normal operating conditions	<€5k or X% of Turnover	1

2. Risk Likelihood Criteria

Option A - Risk likelihood criteria for a 4x4 Score Model

Assessed likelihood	Description	Score
Very Probable	Estimated >90% chance of occurrence one year	4
Probable	Estimated 90%-50% chance of occurrence one year	3
Improbable	Estimated 50%-10% chance of occurrence one year	2
Very Improbable	Estimated <10% chance of occurrence one year	1

The use of historical data may guide the definition of likelihood

- Option B - Risk likelihood criteria for a 5x5 Score Model

Assessed likelihood	Description	Score
Very Probable	Estimated >90% chance of occurence one year. Almost certain to occur.	5
Probable	Estimated 60%-89% chance of occurrence one year. Probable or likely to occur.	4
Possible	Estimated 30% - 59% chance of occurrence one year. Potential to occur.	3
Improbable	Estimated 10%-29% chance of occurrence one year. Improbable but not impossible to occur.	2
Very Improbable	Estimated <10% chance of occurrence one year. Remote chance of occurrence.	1

3. Risk Rating Criteria

Option A - Risk Rating Criteria for 4x4 score model

		Likelihood			
		Very Improbable (1)	*Improbable (2)*	*Probable (3)*	*Very Probable (4)*
Impact	*Extreme (4)*	4	8	12	16
	Serious (3)	3	6	9	12
	Moderate (2)	2	4	6	8
	Minor(1)	1	2	3	4

Option B - Risk Rating Criteria for 5x5 score model

		Likelihood				
		Very Improbable (1)	*Improbable (2)*	*Possible (3)*	*Probable (4)*	*Very Probable (5)*
Impact	*Extreme (5)*	5	10	15	20	25
	Major (4)	4	8	12	16	20
	Moderate (3)	3	6	9	12	15
	Minor (2)	2	4	6	8	10
	Insignificant (1)	1	2	3	4	5

4. Risk Register Examples

		Gross risk assessment				Net risk assessment				
Risk ref	Description of risk	Impact	Likelihood	Gross risk rating	Mitigating controls - link to ICF where appropriate	Impact	Likelihood	Net risk rating	Mitigating actions	Risk Owner
1	Loss arising from ransomware scam	Major	Probable	16	1. Ransomware detection tool employed by the Technological University 2. Cyber security attack response outlines response	Major	Improbable	8	1. IT security staff to run awareness programme for one weekeach semester during 2017/18 year.	Secretary Financial Controller

Or

				Current Score					Target Score						
Dept	Risk	Risk Type	Controls in Place	Impact	Likelihood	Score	Mitigating actions (to reduce the risk)	Contingency actions (if the risk is realised)	Impact	Likelihood	Target Score	Action Owner	Status	Implementation Date	Escalation
IT	Loss arising from ransomware scam	Operational	1. Ransomware detection tool employed by the Technological University 2. Cyber security attack response outlines response once detected/reported.	Major	Probable	16	1. IT security staff to run awareness programme for one week each semester during 2017/18 year. 2. Penetration testing scheduled for April 2018 to assess the strength of the Technological University network.	1. Cyber security attack response outlines response once detected/reported. 2. Disaster recovery plan (last updated in Jan 2018), to be put in place.	Moderate	Possible	9	IT Manager	Open	30/06/2018	Secretary Financial Controller

Appendix D – Alternative Risk Appetite Statement

This Risk appetite should be utilised when making decisions that affect the Technological University in pursuit of its mission or Strategic objectives.
An approach may be to set the overall Technological University guidelines for each of the four choices above rather than breaking it down into specific areas

	RISK APPETITE (How much risk, on a broad sense, we are willing to take to achieve objectives within the Technological University			
	Philosophy	Tolerance	Choice	Trade-Off
	Overall risk-taking philosophy	Willingness to accept uncertain outcomes or period-on-period variation	When faced with multiple options, willingness to select an option which puts strategic objectives at risk	Willingness to trade against achievement of other objectives
Open	Will take justified risks	Fully anticipated	Will chose option with the highest risk-adjusted return; accept possibility of failure	Willing
Flexible	Will take strongly justified risks	Expect some	Will chose to put at risk, but will manage impact	Willing under the right conditions
Cautious	Preference for safe delivery	Limited	Will accept if limited, and heavily outweighed by benefits	Prefer to avoid
Minimalist	Extremely conservative	Low	Will accept only if essential, and limited possibility / extent of failure	With extreme caution
Averse	Avoidance of risk is a core objective	Extremely low	Will always select the lowest risk option	Never

Document Information

1. Document Details

Title:	Risk Management Policy
Owner:	Vice President Finance & Corporate Governance
This Version Number:	Version 1.0
Location:	www.tus.ie

2. Relevant Existing/Related Documents

Title	**Status**	**Relevance to this Document**
Code	Approved	THEA Code of Governance September 2019

3. Approvals

This document requires following approvals (in order where applicable):

Name	**Date**	**Details of Approval Required**
TUS Governing Body	12/10/2021	