Risk Management Policy

Purpose:	This document outlines the Dundalk Institute of Technology's policy for the identification, assessment and management of risk.
Circulation:	This document is available for all to review and will be published on the Institute's website
Policy author:	Chief Risk Officer & Vice President for Finance, Resources & Diversity
Policy Owner:	Finance, Audit & Risk Committee Governing Body

Reference	Details	Page No.
1	Introduction	3
2	Purpose	3
3	Scope	3
4	Key stakeholders	3
5	Risk categories	5
6	Risk appetite	5
7	Risk scoring	6
8	Risk matrix, rating & legend	7
9	Process for identifying, accessing and managing risk	8
10	Monitoring and reporting risk management	9
11	Review of policy	10
12	Approval history	10
N/A	Appendix A – Risk Register	11
N/A	Appendix B – Risk Acceptance Form	12

1. Introduction

Risk management is on on-going process of identifying, assessing and mitigating against risks or threats that may prevent Dundalk Institute of Technology ("DkIT") from achieving its objectives. Section 7 of the THEA Code of Governance specifically notes the importance of a robust risk management policy.

> *Risk management and internal control are important and integral parts of a performance management system and crucial to the achievement of outcomes. They consist of an ongoing process designed to identify and address significant risk involved in achieving an entity's outcomes.*

Risk management also refers to the tracking of risks over a period of time to identify those factors that were successful in the mitigation against the effects of such risk and those that require additional review.

2. Purpose

The purpose of this policy is to provide guidance to those tasked with identifying, assessing and managing risk within DkIT and consequentially:

- support the achievement of the strategic objectives
- protect the Institute's students, staff and assets
- ensure financial stability
- protect the Institute's reputation
- comply with the THEA Code of Conduct
- transparent processes and good practice
- support for management decisions
- increase the wider stakeholder's understanding and attitudes towards risk management

Based on the guidance of this policy risk should be managed to a level that has been defined and accepted by Governing Body. This policy does not attempt to encompass other legislative registers such as those required under health & safety etc.

3. Scope

This policy sets out DkIT's risk management policy across the entire Institute to include all schools, department and functions. Its scope extends to subsidiaries, research centres and indeed any academic or support function under the remit of the Institute.

4. Key Stakeholders

Each member of DkIT's stakeholders have an important role to play in risk management. The following are some specific roles:

i. <u>Governing Body</u>
The overall responsibility for managing risk within the Institute rests with the Governing Body. The Governing Body will approve the Institute's Risk Management Policy and will satisfy itself through the work of the Finance, Audit & Risk Committee ("FAR").

ii. <u>Finance Audit & Risk Committee</u>
The role of FAR is to ensure an adequate risk framework is in place, supported by this policy and a risk register. The committee will review the risk register and monitor the progress towards managing risks identified. It will also report its findings to the Governing Body.

iii. President

The President of the Institute has overall responsibility to ensure adherence to this risk management policy. Although an appropriately qualified individual can be nominated to the role of Chief Risk Officer to the Governing Body the President retains ultimate responsibility for risk within the Institute.

iv. Chief Risk Officer

The Chief Risk Officer (CRO) is responsible for:

- Preparing & reviewing the risk management policy
- Ensuring adequate training is in place across the Institute
- Assisting the Leadership Team in promoting a risk management culture
- Collating and consolidating risk registers provided by each member of the Leadership Team for their relevant area
- Providing FAR with an updated risk register at agreed intervals

This role may be filled by the President or the activities delegated to another member of staff.

v. Leadership Team

This team includes:

- President
- Head of School of Business & Humanities
- Head of School of Engineering
- Head of School of Health & Sciences
- Head of School of Informatics & Creative Arts
- Head of Research & Graduate Studies
- Vice President for Academic Affairs and Registrar
- Vice President for Finance, Resources & Diversity
- Vice President for Strategic Planning, Communications & Development
- Human Resources Manager

The above have a responsibility to implement the risk management policy and advocate an appropriate risk management culture. This team is also tasked with bringing forward, at intervals determined by FAR or the Chief Risk Officer, local risk registers that are prepared by their teams for collation by the Leadership Team.

vi. Management Teams

These teams include Heads of Departments or Heads of Function and their support teams across each of the schools or functions. Their key deliverable is to provide input, by working alongside the relevant member of the Leadership Team, to a local risk register in conjunction with their own individual teams. This risk register should be extended to the wider members of their team for additional feedback and input. These teams may be referred to as 'local teams'.

vii. Risk owner

A risk owner is responsible for managing a risk that has been identified and should manage the controls in place to mitigate against the risk crystallising or the impact of the risk itself.

viii. All staff / employees

All staff are expected to be familiar with the contents of the risk management policy and communicated identified perceived risks to Heads of Department or Heads of Function for further consideration.

5. Risk Categories

Risks are identified across the following categories through a bottom up and top down approach:

- Strategic risk
  - Risks associated with achieving the Institutes strategic aims as identified in the Institute's Strategic Plan
- Reputational risk
  - Those risks in relation to stakeholders (staff, students, etc.) and other public bodies' perception of DkIT
- Compliance risk
  - Compliance and governance risks along with legislative requirements as laid down by statute
- Financial risk
  - Any risks that may cause harm to the Institute resulting in financial loss or misstatement
- Operational risk
  - Risks involved with the Institutes core activities along with support functions such as, for example, the continuity of IT systems
- Capital risks
  - Any risk associated with capital projects, be it infrastructural or the roll out of new software.

6. Risk Appetite

Risk appetite (or risk tolerance) guides the various stakeholders as to the level and type of risk that the Institute believes is acceptable in the pursuit of their objectives. The risk appetite is specific to the activity being undertaken. The following table outlines the various levels of risk the Institute are willing to accept:

Risk appetite	Engagement with risk (overall risk taking philosophy)	Tolerance towards risk (willingness to accept uncertain outcomes)	Choice towards risk (when choosing different options)
Risk seeking	Aggressive risk taking is justified	Risk is full anticipated & acknowledged	Greatest benefit is the desired outcome
Risk tolerant	Balanced approach when considering risk	Risk is expected	Risk must be manageable
Risk neutral	Preference for safe delivery	Limited risk is involved	Benefits need to heavily outweigh risks
Risk cautious	Extremely conservative	Risks are low and not expected	Only proceed if risk is unlikely to occur
Risk adverse	Avoidance of risk is a core objective	There is no risk involved	Lowest risk is the desired outcome

The above risk appetites overlaid on the risk categories to reflect the Institutes approach to risk:

Risk appetite	Risk Category	Notes
Risk seeking	None	None
Risk tolerant	Strategic risk Capital risk	For both these categories DkIT acknowledge there is a level of risk involved which can be managed by continuous review and robust controls
Risk neutral	Operational risk	The Institute acknowledge that innovative and creative learning environments pose a risk however the benefits must heavily outweigh such risks
Risk cautious	Reputational risk Compliance risk Financial risk	The Institute is risk cautious for all areas in relation to reputation, compliance and financial. Robust governance and financial controls are valued.
Risk adverse	None	None

7. Risk Scoring

In order to ensure there is a standardised process for scoring the likelihood and impact of risks the following structures have been developed:

i. Likelihood of risk occurring

The occurrence of a risk crystallising needs to be determined by the risk owner in addition to the relevant member of the Leadership Team. The following scale should be used when measuring the likelihood of the risk:

Assessed Likelihood	Description	Score
Very likely	> 80% change of occurrence	5
Likely	60% - 80% change of occurrence	4
Possible	30% - 60% change of occurrence	3
Unlikely	10 % - 30% chance of occurrence	2
Very unlikely	< 10% chance of occurrence	1

ii. Impact of risk

The impact of each risk needs again to be determined by the risk owner in conjunction with the relevant member of the Leadership Team. The following scale, relevant to the category of risk, should be used when measuring the likelihood of the risk:

Strategic Risk

Impact	Description / examples	Score
Extreme	Strategic objectives will not be achieved	5
Serious	Strategic objectives will be significantly delayed	4
Moderate	Strategic objectives may be delayed but will be achieved	3
Minor	Different course of action required to meet objectives	2
Negligible	Minor delay, will not affect overall plan to meet objectives	1

Reputational Risk

Impact	Description / examples	Score
Extreme	Lack of confidence noted by majority of key stakeholders	5
Serious	Lack of confidence by some key stakeholders	4
Moderate	Negative wider public perception	3
Minor	Small number of complaints by stakeholders	2
Negligible	Minor disturbance to a small cohort	1

Compliance Risk

Impact	Description / examples	Score
Extreme	Breach of laws resulting in prosecution / fines	5
Serious	Breach of laws with no prosecution / fines	4
Moderate	Numerous instances of poor compliance with laws / governance	3
Minor	Isolated instances of poor compliance with laws / governance	2
Negligible	Good practice not being implemented	1

Financial Risk

Impact	Description / examples	Score
Extreme	Financial loss in excess of €75,001	5
Serious	Financial loss of between €35,001 & €75,000	4
Moderate	Financial loss of between €15,001 & €35,000	3
Minor	Financial loss of between €5,001 & €15,000	2
Negligible	Financial loss of no more than €5,000	1

Operational Risk

Impact	Description / examples	Score
Extreme	Inabilty to delivery lectures and other core support services	5
Serious	Fragmented delivery of lecture and other core services	4
Moderate	Some disruption to lectures & services	3
Minor	Minor disruption affecting a small cohort no more than a week	2
Negligible	Little or no disturbance lasting no more than a day	1

Capital Risk

Impact	Description / examples	Score
Extreme	Inability to complete a large capital project	5
Serious	Project delayed significantly	4
Moderate	Project delayed but will be delivered within an agreed timeframe	3
Minor	Minor delay that will not affect the final delivery	2
Negligible	Additional misc. resources required to keep the project on track	1

8. Risk Matrix, Rating and Legend

Once the likelihood and impact of a risk can be identified the rating of the risk can be judged using the following risk matrix:

Risk Matrix			Likelihood (b)				
			Very unlikely	Unlikely	Possible	Likely	Very likely
	Impact	Score	1	2	3	4	5
Impact (a)	Negligible	1	1	2	3	4	5
	Minor	2	2	4	6	8	10
	Moderate	3	3	6	9	12	15
	Serious	4	4	8	12	16	20
	Extreme	5	5	10	15	20	25

The output of (a) x (b) provides a risk rating which can then be classified being the risk legend:

Risk Legend	Risk rating	
	From	To
Extreme	20	25
Serious	15	19
Moderate	10	14
Minor	5	9
Negligible	1	4

9. Process for Identifying, Accessing and Managing Risk

Risk management is a systematic and continuous process of identifying, accessing and managing risk. The following steps should be followed in sequence by each member of the Leadership Team when reviewing risks with their teams:

i. Risk identification

Risk identification should take place at least three times per annum by each relevant function or school. Each risk identified should have an owner who shall be responsible for the management of that risk by implementing relevant controls to minimise the impact should it crystallise.

In order to ensure risks are identified at a sufficiently granular level each school or function should maintain an up to date risk register specific to the area they are responsible for (i.e. a local risk register). This local risk register is the responsibility of the relevant member of the Leadership Team and should not be delegated to any other party.

These local risk registers will form an important component of the Institute risk register which will contain a combination of specific and high level risks. Individual risk owners retains the responsibility in managing the risk specific to their area irrelevant of the risk being included on the Institute risk register or not.

All staff have an important role to play in the effective risk management and it is important staff are encouraged to contribute and have input into risk registers. Given a risk register is a 'live document' it is envisaged it should be under continuous review and updated in line with any developments. Sufficient consideration should be provided to changes in the environment the Institute operates and what risks any changes in this environment might create.

The relevant member of the Leadership Team will have final review and primary responsibility of the register applicable for their school / functions.

ii. Gross risk assessment

Following the risk identification the gross risk rating of each risk should be noted on the risk register. The gross risk rating is that before any controls or actions are put in place to manage the risk. The impact and likelihood should be considered by using the tables provided in sections 7 & 8 above. Each and every risk should have a gross risk assessment applied to it.

iii. Identification of controls

Following the gross risk assessment controls should be designed to prevent the risk from occurring or reduce the impact of the risk. Given the nature of some risks it may

not be possible to eliminate the risk in full. Controls should be a both preventative and detective. Any controls that are currently in place should also be recorded. It is the responsibility of the Risk Owner to ensure they controls are inforce. Controls should be reviewed regularly to ensure they are sufficiently addressing the risk.

iv. Net risk assessment

After applying controls to the risk the net or residual risk is assessed. The purpose of this step is to consider what the updated risk rating might be (impact x likelihood) after the application of the identified controls. This assessment is also recorded on the risk register.

v. Identification of mitigating actions

The net risk above can be treated in one of three areas:

- Tolerated

  The net risk, after the implementation of controls identified at step (iv), is accepted and no further mitigating actions can be undertaken internally the risk is deemed tolerated.

  If a risk is being tolerated and the net risk is classed moderate or above a risk tolerance form must be prepared by the Risk Owner. The purpose of this form is to provide both the Leadership Team & FAR with additional details on the risk and how it will be managed going forward.

  A copy of the risk tolerance form can be found in Appendix B

- Transferred

  A partial transfer of the consequences or prevention of some risks may be migrated to a third party; insurers or the use of specialised consultants or third parties for example. A risk should only be transferred if it is required under legislation, governance or all internal possibilities have been exhausted.

  Although a risk can be partially transferred all risks remain the primary responsibly of the DkIT team.

- Terminated

  Should the net risk be deemed excessive, based on the category specific appetite, the activity giving rise to the risk should be terminated. The risk appetite by category is detailed in section 6 of this policy.

10. Monitoring and Reporting of Risk Management

Each member of the Leadership Team should undertake a formal review of their Risk Register three times per annum. In order to complete this review they should follow steps (i) to (v) as detailed in Section 9 of this document. Within four weeks of the formal risk review taking place the updated risk register, in addition to the completed risk tolerance forms, should be forwarded to the CRO for their review.

The previous net risk rating (i.e. the net risk rating from the previous risk register) needs also to be documented on the risk register in order to identify any risk movements e.g. a risk that may have been rated as serious previously but is not being rated as moderate or vice versa. The purpose of this exercise is to monitor the effectiveness of controls previously put in place.

Based on the updated risk register the CRO will collate any risk identified as moderate or above on the main Institute risk register along with, at their discretion, a sample of other risks. This

additional sample may be based on trends the CRO has identified across other local risk registers or other such risks as they see fit.

The Leadership Team are responsible for approving the Institute risk register and may raise queries to Local Teams on specific risks as they see fit.

Once approved by the Leadership Team the risk register will be presented to FAR outlining:

- The top 15 risks to the Institute based on net risk assessment
- Details of any risk that has progressed from moderate to serious or serious to extreme
- Any control weaknesses that have been identified / reported on to the Leadership Team

FAR will then report their findings to the Governing Body.

The following summarises the timelines involved for academic years 2022 /2023 onwards:

Period end	Updated Risk Register forward to CRO	Reviewed by Leadership	FAR & Governing Boy
30 August	28 September	28 October	Next available scheduled meeting
30 December	28 January	28 February	
30 May	28 June	28 July	

The following timelines will apply **solely** for the academic year 2021 /2022:

Period end	Updated Risk Register forward to CRO	Reviewed by Leadership	FAR & Governing Boy
30 September	14 November	28 December	Next available scheduled meeting
30 March	28 April	28 May	

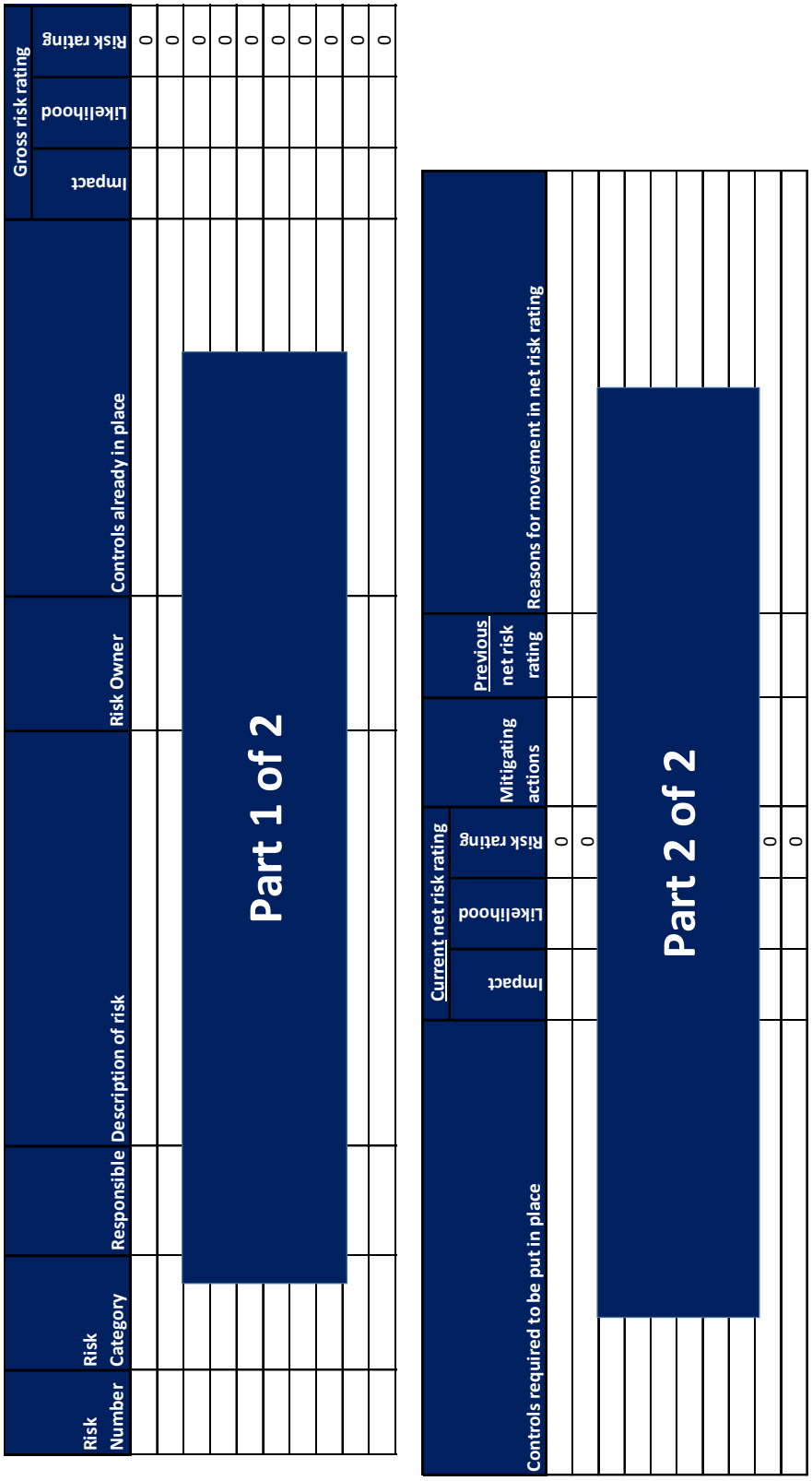
11. Review of Policy

This policy will be reviewed on an annual basis before being presented to FAR, and subsequently Governing Body, for their review and approval.

12. Detailed Approval History

Version number	Version date	Reviewed & approved by Leadership	Reviewed & approved by FAR	Reviewed & approved by Governing Body
1	8 August 2015			
2	12 August 2021	8 September 2021	21 September 2021	26 October 2021

Appendix A: Risk Register



Appendix B: Risk Acceptance Form

DkIT Risk Acceptance Form

(to be completed by the risk owner for any risk identified as moderate or above)

Risk title:	
Risk category	
Risk owner:	
Risk rating:	
Date raised:	
Risk reference number:	
Risk register (school, function, etc.)	

Detailed description of risk:
How was the risk identified?
Describe the expected likelihood of the risk (what might cause it to occur etc.):
Describe the expected impact of the risk (what can be expected to occur.):

List all controls and measures that are in place to manage this risk:
How was the chose mitigation action chosen (e.g. tolerated, terminated or transferred)?
What steps are available to the institute long term to better manage this risk? Will this require financial investment? If so, had this been quantified?
When will the controls surrounding this risk be reviewed again to ensure they are sufficient in stabilising or mitigating the risk?
Other comments or information:

Recommendation to accept risk:			
Title	**Name**	**Signature**	**Date**
Risk Owner			
Leadership Team member			
President / Chief Risk Officer			

Noted at FAR (if required)	
Date	**Meeting Reference**