**Risk Management Policy**

**Version 6 – January 2026**

| | |
|---|---|
| Purpose: | This purpose of this policy is to outline the process for identifying, assessing and managing risk in Dundalk Institute of Technology. |
| Circulation: | This document is available for all to review and will be published on the Institute's website |
| Policy author: | Vice President for Finance & Corporate Affairs |
| Policy Owner: | Chief Risk Officer |
| Approval Date: | Executive Board: 10 February 2026<br>Audit, Risk and Compliance: 17 February 2026<br>Governing Body: 24 February 2026 |
| Review Date: | As required or based on the request of the Audit & Risk, Compliance Committee or Chief Risk Officer. |

**Revision History:**

| | |
|---|---|
| **Date of Revision** | 17 September 2025 |
| **Version Number** | 5 |
| **Summary of Changes** | Section 6 re-worded to better explain the relationship between Risk Appetite and Risk Tolerance - they are not interchangeable terms |
| **Changes Marked** | Section 6 (Pages 6 & 7) Risk Tolerance<br>Section 10 (page 13) Timelines for Risk Register Review |

| Reference | Details | Page No. |
|---|---|---|
| 1 | Introduction | 3 |
| 2 | Purpose | 3 |
| 3 | Scope | 3 |
| 4 | Key stakeholders | 3 |
| 5 | Risk categories | 5 |
| 6 | Risk appetite and Risk tolerance | 6 |
| 7 | Risk scoring | 7 |
| 8 | Risk matrix, rating & legend | 9 |
| 9 | Process for identifying, accessing and managing risk | 9 |
| 10 | Monitoring and reporting risk management | 11 |
| 11 | Review of policy | 12 |
| 12 | Approval history | 12 |
| N/A | Appendix A – Risk Register | 13 |
| N/A | Appendix B – Risk Acceptance Form | 14 |

## 1. Introduction

Risk management is on on-going process of identifying, assessing and managing 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 and reporting on risks over a period of time. Such tracking assists in identifying those factors that were successful in managing various risks and those that may 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 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:

| Stakeholder | Role |
|---|---|
| Governing Body | 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 Audit, Risk and Compliance Committee (ARC). |

| | |
|---|---|
| | Whilst the Governing Body may delegate the various activities for risk management to the ARC it shall retain final oversight and responsibility. |
| Audit, Risk and Compliance Committee (ARC) | The role of ARC is to ensure an adequate risk framework is in place. This is achieved via a Risk Management Policy and Risk Registers.<br><br>The Committee will review the Institute Risk Register and monitor the progress towards managing those risks identified. The committee will also report its findings and recommendations to the Governing Body. |
| President | The President of the Institute has overall responsibility to ensure adherence to this Risk Management Policy. Although the activities of Chief Risk Officer can be delegated to another member of staff the President retains ultimate responsibility for risk within the Institute. |
| Chief Risk Officer | The Chief Risk Officer (CRO) is responsible for:<br><br>• Preparing & reviewing the risk management policy<br>• Assisting the Executive Board in promoting a risk management culture<br>• Collating and consolidating risk registers submitted by each member of the Executive Board for their schools / departments / functions<br>• Providing ARC with an updated risk register at agreed intervals<br><br>This role may be filled by the President or the activities delegated to another member of staff. |
| Executive Board | The executive Board are responsible for:<br><br>• Embedding a culture of Risk Management, including horizon scanning, identification of new and emerging risks, and scenario planning, throughout the Institute so that risk is embedded as part of the Institute's decision-making processes.<br>• Supporting the Chief Risk Officer / President in monitoring the assessment and management of risks that could impact on the Institute achieving its objectives.<br>• Ensuring that Institute employees have a good understanding of this policy to include the Risk Appetite and Risk Tolerance as set out.<br>• Ensuring risks are appropriately identified, managed and monitored in line with the Risk Management Policy<br>• Taking particular note of any risks identified that should be escalated to the Institute's Risk Register<br>• Bringing forward, at intervals determined by ARC or the Chief Risk Officer, local risk registers that are prepared by their teams for review by the Executive Board. |
| 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 into 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'. |

| | |
|---|---|
| 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. The Risk Owner is not responsible for the consequences of the risk crystallising but instead is tasked with managing agreed controls and escalating to the relevant Executive Board member should these controls not be effective in managing the risk. |
| Staff / Employees | All staff are expected to be familiar with the contents of the Risk Management Policy. Staff should also escalate identified perceived risks to Heads of Department or Heads of Function for further consideration. |
| Internal Audit | Internal Audit reviews the Institute Risk Register in developing the Annual Internal Audit Plan, in consultation with the Audit, Risk and Compliance Committee and the President. |

## 5. Risk Categories

Risks are identified across the following categories:

- 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, regulatory bodies, etc.) and other public bodies' perception of DkIT.
- Compliance risk
  - Risk associated with non-compliance with legislation or inadequate governance and / or accurate reporting.
- 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. This includes both the delivery of teaching, support functions etc. (including risk associated with IT).
- Capital risks
  - Any risk associated with capital projects, be it infrastructural or the roll out of new software.

Categories of risk can be subjective and some risks could potentially be suited to more than one category. It is important to consider the category of risk in line with the impact of the risk (refer to section 7 of this policy). Users may decide to list the risk twice, under both categories, or instead list it under the category with the greatest impact.

## 6. Risk Appetite and Risk Tolerance

Risk is an inherent part of running any organisation. Risk appetite provides stakeholders guidance 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.

Risk tolerance is defined as the acceptable deviation from the level set by the risk appetite. Risk appetite is about "taking risk" and risk tolerance is about "controlling risk". For risk

appetite to be adopted successfully in decision making, it must be integrated with the control environment of the Institute through risk tolerance, as noted in the following quote:

*"The risk appetite statement is generally considered the hardest part of any Enterprise Risk Management implementation. However, without clearly defined, measurable tolerances, the whole risk cycle and any risk framework is arguably at a halt."* - Institute of Risk Management

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 fully anticipated & acknowledged | Greatest benefit is the desired outcome |
| Risk tolerant | Balanced approach when considering risk | Risk is expected / inherent to the process | Risk must be manageable |
| Risk neutral | Preference for safe delivery | Limited risk is involved | Benefits need to heavily outweigh risks |
| Risk cautious | Very 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 risk appetite (refer to section 6) overlaid on the risk categories (refer to section 5) define the appetite for the various risks identified:

| Risk appetite | Risk Category | Notes |
|---|---|---|
| Risk seeking | None | None |
| Risk tolerant | Strategic risk<br>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<br>Compliance risk<br>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 |

The Risk Appetite is reviewed on regular intervals and will form part of the ARC and Governing Body's annual review of the Statement of Internal Controls. This review of the Risk Appetite may result in a review of this policy being required.

## 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 probability of a risk crystallising needs to be determined by the Risk Owner in conjunction with the relevant members of the Executive Board. 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 again needs to be determined by the Risk Owner in conjunction with the relevant member of the Executive Board. 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 |
|---|---|---|
| Critical | Significant strategic objectives will not be achieved within the term of the Institute's Strategic Plan. | 5 |
| Serious | Significant strategic objectives will be materially delayed however agreed alternatives are in progress. | 4 |
| Moderate | Strategic objectives may be delayed but will be achieved within the lifetime of the Strategic Plan. | 3 |
| Minor | Different course of action required to achieve objectives / goals within the original timeframe. | 2 |
| Negligible | Minor delay, will not affect overall plan to meet objectives by agreed timelines. | 1 |

**Reputational Risk:**

| Impact | Description / examples | Score |
|---|---|---|
| Critical | Lack of confidence by majority of key stakeholders with nationally adverse publicity. | 5 |
| Serious | Lack of confidence by some key stakeholders with extensive local adverse publicity. | 4 |
| Moderate | Negative wider public perception and some local adverse publicity. | 3 |
| Minor | Small number of complaints by stakeholders with very minor publicity. | 2 |
| Negligible | Minor disturbance to a small cohort with no publicity. | 1 |

**Compliance Risk:**

| Impact | Description / examples | Score |
|---|---|---|
| Critical | Breach of laws resulting in regulatory action against the Institute. | 5 |
| Serious | Breach of laws with (without regulatory action) or material non-compliance with the Code of Conduct. | 4 |
| Moderate | Numerous instances of poor compliance with legislation / good governance standards. | 3 |
| Minor | Isolated instances of poor compliance with laws / governance without remedial action. | 2 |
| Negligible | Good practice not being implemented. | 1 |

**Financial Risk:**

| Impact | Description / examples | Score |
|---|---|---|
| Critical | Financial loss in excess of €1 million or anything in excess of 1.50% of the annual budget. | 5 |
| Serious | Financial loss of between €600,000 and €1 million or between 1.00% and 1.50% of the annual budget. | 4 |
| Moderate | Financial loss of between €150,000 and €600,000 or between 0.25% and 1.00% of the annual budget. | 3 |
| Minor | Financial loss of between €50,000 and €150,000 or between 0.10% and 0.25% of the annual budget | 2 |
| Negligible | Financial loss of no more than €50,000 or in excess of 0.10% of the annual budget | 1 |

**Operational Risk (including IT Risk):**

| Impact | Description / examples | Score |
|---|---|---|
| Critical | Inability to delivery lectures and other core support services to all stakeholders for more than 3 consecutive days | 5 |
| Serious | Fragmented delivery of lectures and other core services for 3 consecutive days. | 4 |
| Moderate | Some disruption to lectures and services lasting no more than 3 days. | 3 |
| Minor | Minor disruption affecting a small cohort no more than a week | 2 |
| Negligible | Little or no disturbance lasting no more than 1 day | 1 |

**Capital Risk:**

| Impact | Description / examples | Score |
|---|---|---|
| Critical | Inability to complete a large core capital project / project delayed with no revised completion date. | 5 |
| Serious | Core project delayed significantly but will be completed within 12 months of the delay becoming apparent. | 4 |
| Moderate | Project delayed but will be delivered within an agreed timeframe. | 3 |
| Minor | Minor delay that will not affect the final delivery of the project. | 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 |
| | Critical | 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 |
| Critical | 20 | 25 |
| Serious | 15 | 19 |
| Moderate | 10 | 14 |
| Minor | 5 | 9 |
| Negligible | 1 | 4 |

## 9. Risk Management Framework / Process for Identifying, Accessing and Managing Risk

Effective risk management focuses on understanding, measuring and controlling risk rather than necessarily avoiding or totally eliminating it. The Risk Management Framework is an iterative process consisting of steps, when taken in sequence, enable continual improvement in the Institute's decision-making.

It constitutes a logical and systematic method of identifying, assessing, managing and reporting risks associated with any activity, function or process in a way that will enable the Institute to minimise potential losses, disruptions, damages etc. while maximising opportunities.

The following steps should be followed in sequence by each member of the Executive Board when reviewing risks with their teams:

i. Risk Identification

Risk identification should take place at least twice per annum by each relevant function or school. Each risk identified should have an owner (Risk Owner) who shall be responsible for the management of that risk by implementing agreed controls to prevent the risk from crystallising or minimise the impact should it actually 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 Executive 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 retain the responsibility in managing the risk specific to their area.

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 such changes might create.

The relevant member of the Executive Board will have final review and primary responsibility of the Risk Register applicable for their school / functions (aka their Local Risk Register).

ii. Gross risk assessment

Following the risk identification, the gross risk rating of each risk should be recorded on the risk register. The gross risk rating is that before any controls or actions are put in place to manage the risk (i.e., what would happen if there were no controls or management). 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. Controls already in place

Following the gross risk assessment, controls currently in place to manage the risk should be documented. These may include items such as; subcommittees already in place, strategies already devised and being implemented, projects underway etc. Given the nature of some risks these controls, already in place, may not be possible to eliminate the risk in full. It is the responsibility of the Risk Owner to ensure they controls are enforced and to escalate to the relevant member of the Executive Board should they not be operating efficiently.

iv. Net risk assessment

After applying the existing controls to the gross risk, the net or residual risk is calculated. The net risk assessment determines how efficient the current controls are and how these controls are reducing the likelihood and impact of the risk crystallising.

v. Controls required to be put in place

Risk Owners, in conjunction with the relevant member of the Executive Board, may then decide to implement additional controls to reduce the net risk rating further. These controls may be particularly important if the current controls have not been successful in reducing the net risk rating from that of the gross risk rating. Additional controls should reflect the seriousness of the risk and any changes to the risk since the last review of the Risk Register.

For example, if the gross risk rating is equal to the net risk rating (i.e., both are 20) it would suggest the current controls are not operating effectively. Ideally the controls already in place (refer to paragraph iii above) should reduce the net risk rating to a level equal to or less than the Risk Appetite for the category of risk under review.

It may not be possible to reduce the net risk rating to that of the Risk Appetite or lower. Such risks should be escalated to the Executive Board and a Risk Acceptance Form should be completed.

Again, it is the responsibility of the Risk Owner to ensure additional controls are actioned. Controls should be reviewed regularly to ensure they are sufficiently addressing the risk.

vi. Identification of mitigating actions

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

- Tolerated

  If the net risk, after the implementation of controls identified at paragraph (iv) above, 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 above the Risk Appetite a Risk Acceptance Form must be prepared by the Risk Owner in conjunction with the Chief Risk Officer. The purpose of this form is to provide both the Executive Board and ARC with additional details on the risk and how it will be managed going forward.

  A copy of the Risk Acceptance 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 / 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 Institute.

- Terminated

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

## 10. Monitoring and Reporting of Risk Management

Each member of the Executive Board should undertake a formal review of their Risk Register twice per annum. In order to complete this review they should follow steps (i) to (vi) as detailed in section 9 of this document. After this formal risk review taking place the updated Local Risk Register (in addition to the completed Risk Acceptance Forms, if applicable) should be forwarded to the Chief Risk Officer 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 to assist in identifying any risk movements. The purpose of this exercise is to monitor the effectiveness of controls previously put in place.

Based on the updated Local Risk Registers the Chief Risk Officer will collate the main Institute Risk Register.

The Executive Team are responsible for reviewing and approving the Institute Risk Register and may raise queries to Local Teams on specific risks as they see fit.

Once approved by the Executive Board the risk register will be presented to ARC outlining:

- The most pertinent risks to the Institute based on net risk assessment
- A Risk Acceptance Form for any risk whose net risk rating is in excess of the Risk Appetite
- Any control weaknesses that have been identified / reported on to the Executive Board

ARC will then report their findings to the Governing Body.

The following summarises the timelines involved.

| Period end | Updated Risk Register forward to CRO | Reviewed by Executive Board | ARC & Governing Body |
|---|---|---|---|
| 31 May | 30 June | 30 September | Next available scheduled meeting |
| 31 December | 31 January | 04 February | |

## 11. Review of Policy

This policy will be reviewed as required by the Chief Risk Officer or the ARC Committee.

## 12. Approval History

| Version number | Version date | Reviewed & approved by Executive Board | Reviewed & approved by ARC | Reviewed & approved by Governing Body |
|---|---|---|---|---|
| 1 | 8 August 2015 | | | |
| 2 | 12 August 2021 | 8 September 2021 | 21 September 2021 | 26 October 2021 |
| 3 | 31 August 2023 | 20 September 2023 | 26 September 2023 | 3 October 2023 |
| 4 | 28 May 2025 | 28 May 2025 | Reviewed 3 June 2025 | |
| 5 | 15 September 2025 | | | |
| 6 | 26 January 2026 | | | |

## Appendix A: Risk Register

| Risk Number | Risk Category | Executive Board Member Responsible | Description of risk | Risk Owner | Gross risk rating | | | Controls already in place | Current net risk rating | | | Previous Net Risk rating | Controls required to be put in place | Mitigating actions | Reasons for movement in net risk rating |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Impact | Likelihood | Risk rating | | Impact | Likelihood | Risk rating | | | | |
| | | | | | | | 0 | | | | 0 | | | | |
| | | | | | | | 0 | | | | 0 | | | | |
| | | | | | | | 0 | | | | 0 | | | | |
| | | | | | | | 0 | | | | 0 | | | | |

**Appendix B: Risk Acceptance Form**

## DkIT Risk Acceptance Form

| | |
|---|---|
| **Risk title:** | |
| **Risk category** | |
| **Risk owner:** | |
| **Current Net Risk rating:** | |
| **Previous Net Risk rating:** | |
| **Risk reference number:** | |

| **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** |
| **President / Chief Risk Officer** | | | |

| **Noted at ARC (if required)** | |
|---|---|
| **Date** | **Meeting Reference** |
| | |