DCU Risk Register

Guide
Table of Contents

Introduction ........................................................................................................................................... 2
Risk Management Theory .................................................................................................................. 2
Definition of Key Terms .................................................................................................................. 2
Categories of Risks .......................................................................................................................... 4
Risk Register Steps .......................................................................................................................... 5
Risk Management Roles ................................................................................................................. 8
Reporting of Urgent Risks ................................................................................................................ 9
Conclusion ........................................................................................................................................... 9
Appendix 1 – Risk examples in a university context ........................................................................ 10
Appendix 2 – Impact assessment Criteria at a Unit level .................................................................. 12
Appendix 3 – Overview of the University’s Risk Management Structure ........................................ 13

Version Control

<table>
<thead>
<tr>
<th>Document Name</th>
<th>DCU Risk Register Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version Reference</td>
<td>V2.0</td>
</tr>
<tr>
<td>Document Owner</td>
<td>Risk &amp; Compliance Officer</td>
</tr>
<tr>
<td>Approved by</td>
<td>Chief Operations Officer</td>
</tr>
<tr>
<td>Date</td>
<td>November 19th 2021</td>
</tr>
</tbody>
</table>
**Introduction**

Risk management, within the context of Dublin City University, can be defined as the ongoing process to identify, assess, manage and control potential events or situations that may prevent the University from achieving its goals.

The purpose of this guide is to assist with the preparation of new risk registers, or the updating of existing registers. Risk management theory is briefly explained and the guide is intended to be used by Heads of Units and Senior Managers across the University (including its Campus Companies).

**Risk Management Theory**

Risk management is a process that is used to identify risks, to evaluate their potential consequences, to consider how likely they are to occur and to then rank them so that the resources to manage them can be efficiently allocated. A risk is managed by taking action to either reduce the likelihood of its occurrence and/or to reduce its impact.

The University's risk management process is not intended to limit potential for growth or improvement. It aims to manage risks, both negative and positive, in an acceptable and appropriate manner.

The risk management process requires an annual cycle of risk reviews. Each cycle has a number of steps and a separate guide on how that process is implemented in practice across the University can be obtained from the Risk Officer.

This guide focuses on the recommended steps to be taken by a Head of Unit, or a member of Senior Management, when they are preparing or updating a Risk Register as part of the annual risk cycle.

**Definition of Key Terms**

**Risk**

A risk is the possibility of an uncertain event occurring in the future that may prevent or delay the achievement of an organisation’s goals. As they are uncertain, risks are generally measured in terms of their potential impact and likelihood.

A risk should not always be thought of in a negative sense, for example as an obstacle to be overcome. Risks can also present an opportunity to succeed or to attain stated goals and so a degree of risk may be acceptable and even desired. In doing so risk management seeks to ensure that risks are identified and managed in such a way as to reduce their negative effects while also allowing for the possible positive effects of managed risk taking.
Issue
An issue, as distinct from a risk, is a current situation, event or set of circumstances that an organisation is currently dealing with that is already affecting its ability to achieve its aims.

Risk Register
A risk register is a formal way of documenting the important relevant details of risks. The layout of risk registers will vary from one organisation to another but there are certain elements common to all. These are:

1) description of the risk and its potential impact;
2) an indication of the controls or measures which are, or can be, put in place to reduce the likelihood of a risk materialising or, if it does materialise, to reduce its potential negative impact;
3) prediction of the risk's likelihood;
4) prediction of the risk's impact;
5) method to rank risks; and
6) named Risk Owner (i.e. the individual or group within the organisation that is responsible for the management of the risk).

There are three types of risk register that are created and used at different stages within the University's risk process.

1) **Unit Level Risk Registers** (aka. 'Operational Risk Registers') are risk registers maintained at a local level in Units across the University (e.g. Schools / Faculties / Research Centres / Support Functions / Campus Companies). In general, Unit Level Registers tend to focus on operational risks that can affect the unit but they may also contain risks that impact upon the University as a whole.

2) **Functional Area Risk Registers (FARR)** are intermediary level registers that are prepared in each risk cycle by the individual members of the University's Senior Management Group (SMG). They are based upon risks from unit level registers but they may also list additional novel risks as put forward by the author.

3) **Strategic Risk Register (SRR)** is the highest level of risk register for the University as a whole and is the prime documentary output of the University's annual risk cycle. It lists the most serious risks that can, or in the case of issues already are, affecting the University. In general, the risks contained in the SRR are strategic in nature but they can also be operational.

Controls
Controls are actions or measures that will reduce the likelihood of a risk occurring or, if it does occur, will reduce its potential negative impact. There are two categories of controls.
1. **Current controls / measures already in place** - These can take the form of either policies, procedures, initiatives or other tailored measures.

2. **Further controls / measures required** - Those that could, or will, be put in place at some point in the future to manage the risk.

Controls should be appropriate to the risk and should address its root cause. However, care must also be taken to ensure that there is a balance between the amount of effort required to implement a control and the benefit to be obtained from doing so.

**Residual Risk**
The University’s risk management process assesses the relative seriousness of a risk in terms of its likelihood and impact. It applies a ‘Residual Risk Model’ which means that it estimates the likelihood and impact of a risk after taking into account the effect of the current measures already in place to manage the risk. It is the residual risk value that will determine whether a risk is categorised as either being high, medium or low. An example of residual risk in practice is given below.

**Serious Fire**
The impact of a fire on campus may, in some instances, lead to serious injuries or even death. Therefore, the impact value assigned to such a fire risk will be ‘5’ after applying the impact assessment criteria set out in **Appendix 2**.

If there were no effective fire safety measures in place the likelihood of such a fire occurring would be either 4 (Likely) or 5 (Certain). However, the residual risk of such a fire event is estimated after taking into account the actual fire safety measures that are in place to reduce its likelihood (e.g. fire safety training) or, if it were to occur, the measures that seek to limit its impact (e.g. fire alarms, fire safety equipment etc).

While the potential impact of such a risk will always be rated high, its likelihood should be low and hence its residual risk rating will also be low.

**Categories of Risks**
Risks can generally be allocated to one or more of the following categories:

- Operational
- Financial
- Reputational
- Strategic
Examples of typical risks in each category that may arise in a university context are listed in Appendix 1.

These categories will cover the majority of risks but there may be some that do not naturally belong to any one category. Where this occurs, it is best practice to allocate the risk to the category in which it has the largest impact and then estimate its likelihood using the impact assessment criteria in Appendix 2.

Risk Register Steps
The preparation of both Unit Level Registers and Functional Area Risk Registers are an essential part of the University's annual risk process. The steps to either to prepare an entirely new register, or update an existing one, are essentially the same and are described in this section of the guide.

Step 1 – Confirm Goals
As already noted a risk is the possibility of an uncertain event occurring in the future that may prevent the achievement of an organisation's goals. Therefore, the first step, in the context of a University Unit, is to identify the operational and strategic goals of the Unit.

Operational goals are the day-to-day tasks of the Unit. For an academic unit one of its operational goals would be the provision of lectures. For a research unit it would be conducting research and for a professional support unit it would be the efficient provision of admin support.

Strategic goals tend to be of a medium to long-term in nature. They may involve the remodelling of how a Unit performs its existing tasks or how it might take on an entirely new task (e.g. the implementation of a new student information system).

Step 2 – Identify Risks
For each goal identified, a list of potential risks or threats towards achieving that goal should then be identified. One should ask the question - 'What can go wrong?' Once a risk is identified, it should then be considered as a possible entry on the Unit’s risk register.

Sources of risks can arise from many areas, for example from the final report on foot of a recent DCU Quality Promotions Office review, or from a ‘brainstorming’ session with the staff of the Unit. Alternatively, you could consult with the relevant members of the Unit’s staff who are in the best position to identify and provide details on risks.

When explaining the context to a risk it is important that the risk's description be concise and clear and that it separates out the elements of the risk into both its root cause and effect. Successfully identifying a risks cause will assist in identifying the appropriate controls or measures to effectively manage it.
Step 3 – Identify the Current Controls / Measures
For each risk identified and included on the register, the controls or measures that seek to limit its adverse impact, or reduce the likelihood of its occurrence, should be recorded on the register. Controls are to be split into two categories; those which are currently in place and actively managing the risk (i.e. ‘Current Controls’) and those controls which may be put in place at some point in the future assuming sufficient time and resources are available and where there is a necessity to do so (i.e. ‘Future Controls’).

Controls can take many forms but their essential characteristic is that they mitigate risk in some manner. Current controls are only effective if they are in place and have a positive effect in mitigating the risk. A control that is not already in place cannot be defined as a current control. In such cases, it is more appropriate to place the control under the Future Controls section of the risk register.

Heads of Units and Senior Managers should also satisfy themselves that the current controls shown against each risk are being actively applied in practice.

Step 4 – Assess the Residual Risk Likelihood & Impact
Once a risk, along with its current controls, is identified and included on the register the next step is to assess how serious it is by applying the ‘Residual Risk’ model referred to earlier. This is calculated by assigning numeric values to both the risk’s likelihood and impact and then multiplying both to give a score. The higher the score, the more serious the risk.

The likelihood and impact of risks are both rated on a scale of 1 to 5 with the possible combined score for any particular risk being a value between 1 and 25. After calculating the score, the risk is then allocated to one of the three categories as indicated on the following table.

<table>
<thead>
<tr>
<th>Range Band</th>
<th>Colour</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Level Risks</td>
<td>Green</td>
<td>1 – 7</td>
</tr>
<tr>
<td>Medium Level Risks</td>
<td>Amber</td>
<td>8 – 15</td>
</tr>
<tr>
<td>High Level Risks</td>
<td>Red</td>
<td>16 - 25</td>
</tr>
</tbody>
</table>

Estimating the likelihood of a risk is very subjective as it is rarely possible to predict the future with any certainty. However, some indication of how likely it is that a risk may materialise is required and this can be made by applying the following guidelines.
The next task is to assess a risk’s potential impact. The assessment of a risk’s impact depends to a large extent upon the context, as a risk’s impact at unit level is unlikely, in most cases, to be the same when it is assessed at a University level. The criteria for assessing a risks impact at a unit level is shown in Appendix 2 and is used to guide the selection of the appropriate impact level from the following table.

<table>
<thead>
<tr>
<th>Level</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rare or very remote (20 years and over)</td>
</tr>
<tr>
<td>2</td>
<td>Unlikely (10 to 20 years)</td>
</tr>
<tr>
<td>3</td>
<td>Possible (5 to 10 years)</td>
</tr>
<tr>
<td>4</td>
<td>Likely (1 to 5 years)</td>
</tr>
<tr>
<td>5</td>
<td>Certain to occur / already happening / or within one year</td>
</tr>
</tbody>
</table>

Please note that the University’s risk process provides for a different set impact criteria from those in Appendix 2 when a risk is being considered for inclusion in the Strategic Risk Register.

**Step 5 – Take Action – Identify Future Controls**
Where the residual risk rating for a risk is deemed too high then additional actions are to be implemented to reduce the residual risk to an acceptable level. Risks whose residual risk ratings are low are unlikely to be a priority. As resources are always limited and Risk Management endorses the application of limited resources to those risks that require the most attention.
In addition, on reviewing risks managers may find that the controls or measures being applied to manage a particular risk are ineffective or, in some cases, entirely absent. If that is the case then further additional measures should be taken if the residual risk rating is too high.

Where further action is deemed necessary the type of action will depend upon the circumstances. Examples of the different types of action that might be applied are provided below.

1. **Treat the risk** - apply specific controls that reduce the risk’s likelihood and/or limit its potential impact. An example would be the measures outlined above for the management of a serious fire.

2. **Substitute the risk** - transfer the risk to another organisation or body. An example of this would be the taking out of an insurance policy for the risk of flooding on campus.

3. **Terminate the risk** - where the residual risk is deemed unacceptable, or there are no controls that can be put in place to effectively manage the risk, the only way of reducing the risk may be to cease the activity that gives rise to it.

**Step 6 – Allocate a Risk Owner**
Where possible, a risk owner should be allocated to each risk on the register. The owner will be the individual or group who has the task of managing the risk by ensuring that the current controls are implemented and/or by developing future controls where necessary.

The allocated risk owner must have the authority and capacity to address the risk and they also need to be made aware of their responsibility for its management.

**Step 7 – Monitor and Report**
Ideally, over time the negative risks should be reduced. To effectively monitor and report on this aspect of risk management a process of regular reviews is required. Where it is noted that medium and high level risks are not being reduced from one review cycle to another then an assessment of whether the current controls are effective should be completed by management. The substitution of the existing controls, or the development of new ones, may be needed.

**Risk Management Roles**
The roles of all parties in implementing risk management across the DCU Community are described in detail in the University's Risk Management Policy as published on its website.
Everyone has a role to play in risk management; it is not the exclusive responsibility of any one group or individual.

**Reporting of Urgent Risks**

Unit level risk registers are generally reviewed and updated regularly, usually at least once a year. However, there may be instances where a new risk materialises which, by its nature is urgent and/or serious and will not have been logged on a unit level risk register to date. In such circumstances, staff members should inform the Risk & Compliance Officer of the existence of the risk after first discussing it with their Unit manager. A decision can then be taken as to how to treat the risk depending on the circumstances in each case.

**Conclusion**

Unit risk registers are updated as part of each risk review cycle by the Unit’s management and are then fed into a process that culminates with the preparation of a SRR. There are a number of steps involved in developing the SRR that are primarily the role of senior management across the University, with oversight of that process being provided by the Governing Authority Risk Committee (GARC). See [Appendix 3](#) for an overview of the various parties involved.

As stated in the introduction, the purpose of this guide is to assist managers across the University with the preparation of new risk registers, or the updating of existing registers. Any queries on the process should be directed to the University Risk and Compliance Officer who reports directly to the Chief Operations Officer.

As a final point, it is worth reiterating that all members of the DCU community have a role to play in risk management generally; it is not the sole responsibility of any one individual or group.

**End.**
Appendix 1 – Risk examples in a university context

Please note:
   a) the list is indicative only;
   b) it is not exhaustive;
   c) risks can fall into more than one risk category;
   d) there may be other risks that do not fall into one of the categories set out below; nevertheless, the risk should be recorded on the Unit’s risk register.

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Typical Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational</td>
<td>• Any event that prevents or disrupts the normal activity of a university unit, e.g. flood damage, relocation, refurbishment of offices, staff disputes, poor staff morale etc.</td>
</tr>
<tr>
<td></td>
<td>• Any event posing a threat to the health and safety of individuals or groups on campus.</td>
</tr>
<tr>
<td></td>
<td>• IT issues which affect the delivery of services e.g. these could be related to hardware, software, storage, the general IT infrastructure, network resilience etc.</td>
</tr>
<tr>
<td></td>
<td>• Dependence on key staff.</td>
</tr>
<tr>
<td></td>
<td>• Absence of formal succession planning.</td>
</tr>
<tr>
<td></td>
<td>• Pressures on service delivery caused by the external environment e.g. government policy, education sector constraints, competition from other institutions.</td>
</tr>
<tr>
<td></td>
<td>• Capacity / quality / ability of the built environment to provide for the delivery of services.</td>
</tr>
<tr>
<td></td>
<td>• Capacity / ability of staff to deliver on Unit and University goals.</td>
</tr>
<tr>
<td></td>
<td>• Obsolete or near end of life specialist equipment or facilities.</td>
</tr>
<tr>
<td></td>
<td>• Outdated or absent crisis continuity plans.</td>
</tr>
<tr>
<td></td>
<td>• Failure to comply with legal or contractual obligations.</td>
</tr>
<tr>
<td></td>
<td>• Poor contract management processes.</td>
</tr>
<tr>
<td></td>
<td>• Unclear or poor understanding of the Unit’s service delivery obligations or aims.</td>
</tr>
<tr>
<td></td>
<td>• Human error and/or staff performance issues.</td>
</tr>
</tbody>
</table>
| Financial          | • Insufficient funding to maintain or increase the level of service delivery.  
|                   | • Increasing costs versus decreasing income.  
|                   | • Threats to the University’s research funding model.  
|                   | • Inability to meet budget or performance targets.  
|                   | • Constraints on the ability to increase income on a Unit or University level.  
|                   | • Static central government funding being spread across a greater number of sector wide institutions.  
|                   | • An unsustainable funding model.  
|                   | • Absent or unsuitable funding source for capital or current expenditure commitments.  
|                   | • Onerous financial liability clauses in contractual relationships (research collaborations, employee contracts, pension fund obligations).  
|                   | • Difficulties in obtaining sufficient funding from external providers (e.g. government, research agencies, philanthropists etc).  
|                   | • Adverse changes in international currency exchange rates that expose the University to a financial loss.  
| Reputational      | • Any event or incident that may potentially damage the University’s reputation.  
|                   | • Dishonest or unethical actions of staff, researchers or students.  
|                   | • Damage to our reputation through association with third parties who act in a dishonest or unethical manner.  
|                   | • Misconduct of staff or students.  
|                   | • Unintentional leakage of Intellectual Property.  
|                   | • Breach of partner confidentiality.  
|                   | • Adverse media attention.  
|                   | • Adverse relationship with media entities.  
| Strategic         | • Competition in core and sought after markets (particular sectors or geographical areas etc.).  
|                   | • Adverse Government or EU policy that is not conducive to the University’s strategic goals.  
|                   | • Possible deficiencies in the human talent and infrastructural assets available for the pursuit of |
institutional and unit goals.

- Increasing demands for services through growth without a similar increase in support to deliver those services (e.g. funding, staffing, change in work practices and management framework).
- Targets for undergraduate / postgraduate student numbers that cannot be met.
- Challenges in attracting international students, staff and researchers in sufficient numbers.
- Difficulties in retaining staff.
- Non-alignment of operational processes across the institution.

### Appendix 2 – Impact assessment Criteria at a Unit level

<table>
<thead>
<tr>
<th>Impact Category</th>
<th>1 Minor</th>
<th>2 Limited</th>
<th>3 Serious</th>
<th>4 Very Serious</th>
<th>5 Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Constituent Strategy</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1) Research &amp; Innovation</td>
<td>Negligible delay in achieving a strategic objective or initiative of the unit.</td>
<td>Some delay with implementing a strategic objective or initiative at unit level.</td>
<td>Significant delay with implementing a strategic objective or initiative at unit level.</td>
<td>Failure to deliver on one or more of the unit’s strategic objectives or initiatives.</td>
<td>Failure to deliver one or more of the unit’s mission critical activities and / or strategic objectives.</td>
</tr>
<tr>
<td>2) Teaching &amp; Learning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3) International</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4) Student Experience</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5) Engagement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Operational</strong></td>
<td>Students/staff aware of problem but impact on them is limited.</td>
<td>Short term disruption to a critical unit activity.</td>
<td>Short term significant disruption to critical unit activities.</td>
<td>On-going &amp; significant disruption to critical unit activities.</td>
<td>Complete shutdown of critical unit activities for an extended period.</td>
</tr>
<tr>
<td>1) Physical Infrastructure</td>
<td>Up to 3% of the unit’s annual budget</td>
<td>4% to 10% of unit’s annual budget</td>
<td>11% to 15% of unit’s annual budget</td>
<td>16% to 20% of unit’s annual budget</td>
<td>Greater than 20% of unit’s annual budget</td>
</tr>
<tr>
<td>2) Unit Effectiveness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3) Health &amp; Safety***</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Financial</strong></td>
<td>Unit’s reputation not affected</td>
<td>Some negative comments in local press / media about the unit</td>
<td>Critical article in local media or criticism from within DCU senior management regarding the unit.</td>
<td>Continuing &amp; significant negative publicity in local or national media regarding the unit. DCU managerial concern.</td>
<td>Unit loses confidence of the public and / or DCU management.</td>
</tr>
<tr>
<td><strong>Reputational</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*** Due regard is to be given to the Unit’s Occupational Health & Safety Hazard and Risk Assessment
Appendix 3 – Overview of the University’s Risk Management Structure

END.