



RISK MANAGEMENT POLICY

Version: March 2026

Glasgow Caledonian University
Risk Management Policy

- 1 Introduction**
- 2 Objectives of the Policy**
- 3 Risk Management in GCU**
- 4 Risk Appetite**
 - 4.1 Definition**
 - 4.2 Benefits**
 - 4.3 Risk Types & Appetite**
 - 4.4 Executive Board Escalation**
- 5 Risk Registers**
 - 5.1 Identification**
 - 5.2 Evaluation**
 - 5.3 Managing Risk**
 - 5.4 Monitoring & Reviewing**
- 6 Risk Event Log**
- 7 Risk Management Forum**
- 8 Accountabilities, Roles & Responsibilities**
- 9 Project Planning**
- 10 Partnerships & Contracts**
- 11 Decision Making**
- 12 Business Continuity & Disaster Recovery Planning**

- Appendix 1 Risk Appetite Framework**
- Appendix 2 Corporate Risk Register Template**
- Appendix 3 School and PSD Risk Register Template**
- Appendix 4 Project Risk Register Template**

1 Introduction

Risk is a part of everyday life and successful organisations manage their risks effectively. High quality risk management is a positive process which supports and enhances business management.

The University recognises the responsibility to identify, evaluate and manage internal and external risks as a key component of good corporate governance and is committed to embedding risk management to help achieve the University's strategic and operational objectives.

The Risk Management Policy outlines GCU's approach to risk and details the Risk Appetite Framework to be applied. It helps ensure risks are properly identified and then either eliminated or reduced to an acceptable level. This approach is to protect the university and ensure risks are managed effectively. The policy also aims to emphasise the opportunities afforded by positive risk management, which is important to support the successful delivery of the University's Strategy. To ensure that the focus is on a meaningful, high quality output, the University's risk management process has been kept as straightforward as possible.

Good organisational risk management will lead to organisational **resilience**. Resilience means being able to thrive in an uncertain environment; it means being able to withstand shocks; and it means coming through uncertainty in a stronger position.

2 Objectives of the policy

The principal objectives of this policy are:

- To further embed risk management within the University as a valuable and positive business management tool, helping GCU identify and evaluate opportunities as well as threats
- To assure the University's resilience and ability to thrive in an uncertain environment
- To raise awareness of the principles and benefits involved in the risk management process and to obtain staff commitment to the principles of risk control.
- To ensure and facilitate compliance with best practice in corporate governance, ensuring that the appropriate disclosure statement can be issued within the annual Financial Statements

3 Risk Management in GCU

Risk Management in GCU is summarised in the diagram below.



GCU has developed a Risk Appetite Framework to support the delivery of the University's Policy. Nine principal risk types have been identified by GCU and these are detailed in the Table in Section 4 below, with the associated appetite for each type of risk. Each type of risk is supported by a Risk Statement and Tolerance Metrics. These are presented in full at [Appendix 1](#).

The University's Risk Appetite underpins everything that is undertaken by the University and must be considered when reviewing new business propositions and projects.

All University Executive Team and Committee Papers include a Cover Sheet Section outlining the impact of the proposal presented on risk and detailing the risks and mitigations inherent in the proposal. All proposals generating risks are considered in line with the University's Risk Appetite tolerances.

On a day to day basis, risk is managed via the ongoing active monitoring and review of the Corporate Risk Register, School and Department Risk Registers, as well as project risk registers where appropriate.

University Risk is overseen by the University Executive Team, which has put in place a Risk Management Forum (RMF). RMF reports to the University Executive Team and is authorised to make recommendations regarding the management of risk in the University. The Forum reports to University Executive Team after each meeting and provides a detailed annual progress report to University Executive Team for noting.

In addition, following University Executive Team approval, the live Corporate Risk Register, together with a note on amendments from the previous version, are made available on Teams/Convene, for all members of Court.

Glasgow Caledonian University

Risk Management Policy

The Corporate Risk Register will be an agenda item once per annum at Court for a full detailed review. At all Court meetings either the Principal or COO & DVC update to Court will outline any material changes made to the Risk Register since the previous Court update.

In addition to the Court papers outlined above, there will be an annual opportunity for Court to reflect on the key organisational risks linked to the wider delivery of Strategy 2030.

The Risk Register will be presented, twice per annum at Finance and General Purposes Committee and Audit Committee. All sub Committees of Court will use the live Corporate Risk Register to inform their agenda, with focus on risks which pertain to the sub Committees area of responsibility.

Risk papers presented at each Court and Committee meeting will reflect the most recent Corporate Risk Register available on Teams/Convene, highlighting key movements from the previous version.

The Risk Management system is covered in detail below.

4 Risk Appetite

4.1 Definition

Risk appetite is defined as:

“The amount or type of risk the University is prepared to tolerate in order to achieve its strategic aims and objectives”

A Risk Appetite Framework provides direction over the level of risk the University is prepared to accept.

In the case of threats, it describes the level of exposure which is considered tolerable and justifiable should the threat materialise.

In the case of opportunities, it defines how much should be put at risk to realise the benefits of the opportunity.

In both cases, it is informed by an assessment of the costs (financial, reputational or otherwise) of managing the risks alongside the impact or benefits that may result from them.

The University has identified eight risk types and defined the maximum level of risk it is willing to accept against each type. Each risk type is supported by a Risk Statement and Tolerance Metrics.

Risk Statements describe the University’s attitude towards each type of risk, while the metrics define how GCU will judge if it is acting in accordance with the stated attitude to risk. It is not designed to limit or stop activity but rather to guide the levels of governance applied to decision making.

The reputation of the University and risk to it through any type of activity or action is considered to be embedded and integral within each of the eight risk types covered by the risk appetite statement.

4.2 Benefits

Defining an organisation’s risk appetite can help in a number of ways, outlined below:

- It ensures the organisation is only taking a level of risk and the type of risk that it is comfortable with
- It ensures the risks you are exposed to are commensurate to the opportunity or reward to be gained
- It provides a framework for decision making: significant decisions can be taken with consideration to how it will affect the level of risk the organisation is exposed to, and if this is acceptable or not
- It assists staff to make judgements about which risks are acceptable & which are not
- It ensures that the response to risk is proportionate, and helps to avoid over the top or lax reactions to risk
- It requires reporting or escalation where there is an exceeding of the organisation’s appetite for risk.

4.3 Risk Types & Appetite

Eight risk types have been identified and associated risk appetites articulated as outlined in the Table below. The complete Risk Appetite Framework, with Risk Statements, is attached at [Appendix 1](#). Although live and amendable by University Court at any time, the Risk Appetite Framework and Risk Statements will be formally reviewed and updated by University Court every two years. Risk Appetite Statements will be presented to University Court on an annual basis as part of an annual Risk Management Update.

Risk Type & Tolerance Range	Appetite									
	Unacceptable to take risks				Higher willingness to take risks					
	1	2	3	4	5	6	7	8	9	10
1 – Education										
2 – Research										
3 - International										
4 - Business Enterprise & Innovation										
5 - People and Culture										
6 - Legal & Regulatory Compliance										
7 - Finance										
8 - Sustainability & Infrastructure										
Operational Impact	Minimal change in operational performance and delivery.			Some change to operational performance and delivery.				Step change in operational performance and delivery.		
Financial Impact	Impact up to £250k			Impact £250k to £750k.				Impact over £750k.		

Note: light grey indicates the level of risk the University finds acceptable.

4.4 University Executive Team Escalation

Where an activity will result in a level of risk exposure greater than the University's risk appetite, then the matter must be escalated to University Executive Team.

Referral to University Executive Team is also required where:

Glasgow Caledonian University Risk Management Policy

- A project or activity has risks which result in conflicting Risk Appetites, e.g. a Transnational Education project - International risk score of 8 and a Reputational risk score of 4, or
- Accumulated risk breaches total Risk Appetite for that Risk Type, i.e. where a number of small projects add together to incrementally create a level of risk which exceeds GCU appetite for that type of risk.

5 Risk Registers

A risk register is the document containing the relevant information about the risks facing an organisation, a department, a project or an activity. These are collated using the four stage risk management process which is detailed below. GCU's risk register templates are attached at [Appendices 2, 3 & 4](#).

The University maintains a Corporate Risk Register of all significant risks that may affect GCU's ability to achieve its strategy and objectives, and records the measures in place for dealing with them. Schools, Support Departments and Projects maintain their own Risk Registers.

A Project Risk Register must be completed for all commercial and research projects. An approved Risk Register forms part of the Project Approval Process for Research and Commercial Risk Registers. The Associate Deans of Research have authority to approve Project Risk Registers for projects within their Schools with total value less than £50k. For projects with values above £50k, Dean or Vice-Dean approval is required.

A Project Risk Register should also be completed for any transnational education project or strategic area or project that is not covered elsewhere.

The four key stages of Risk Management, explained below, are:

- [Identifying risks](#)
- [Evaluating risks](#)
- [Managing risks](#)
- [Monitoring & reviewing risks](#)

5.1 Identification

The first stage is to identify the significant barriers, problems, issues, concerns, challenges, **risks** that could stop you from achieving your strategic and operational objectives.

This should be done by the relevant management team, i.e. by the managers who are responsible for delivering the objectives of either the University, School or support service.

Before identifying risks, the group should be clear on what their objectives are. Risks come in many different types. Consideration should be given to the wide range of different types of risks, such as financial, operational, reputational, and technological and stakeholder risks. When

Glasgow Caledonian University Risk Management Policy

identifying risks it is important to consider the associated opportunity if any afforded by this risk, which may help with evaluation and management in the next stages of the process.

Risks can be identified in a number of ways, for example:

- *Workshops, e.g. A 'brainstorming' session*
- *Increased staff awareness – so they know how to feed in to the process*
- *During a review of current performance*
- *Using previous experience*
- *SWOT Analysis, or something similar*
- *Experience of other organisations (what can you learn from others success, or mistakes?)*
- *Exchange of information with stakeholders*
- *Perceived areas of weakness*
- *Stakeholders surveys, such as students and staff, perceive the University*
- *Internal or external reports and horizon spotting – press, etc.*

5.2 Evaluation

Once the risks have been identified they need to be evaluated. Not all risks faced by the University will be of the same magnitude or significance. The purpose of the evaluation stage is to filter out the risks that need to be managed from the risks that simply need to be monitored.

Each risk is assessed for the **likelihood** it will happen and the **impact** if it does happen.

GCU evaluates risks using a 4x4 evaluation matrix – see below. Risk Criteria to support evaluation of Impact and Likelihood are also provided below.

		Impact			
		Minor	Significant	Serious	Major
Likelihood	Certain	4	8	12	16
	Probable	3	6	9	12
	Possible	2	4	6	8
	Unlikely	1	2	3	6

Risk Criteria - Likelihood

Score	Factor	THREATS - DESCRIPTION	THREATS - INDICATORS	OPPORTUNITIES - DESCRIPTION	OPPORTUNITIES - INDICATORS
4	Certain	More than 75% chance of occurrence	Regular occurrence. Circumstances frequently encountered – daily / weekly / monthly.	Favourable outcome is likely to be achieved in one year or better than 75% chance of occurrence.	Clear opportunity which can be relied upon with reasonable certainty, to be achieved in the short term based on current management processes.

Glasgow Caledonian University Risk Management Policy

3	Probable/ Likely	40% - 75% chance of occurrence	Likely to happen at some point within the next 1-2 years. Circumstances occasionally encountered (few times a year).	Reasonable prospects of favourable results in one year. 40% to 75% chance of occurrence.	Opportunities that may be achievable but which require careful management. Opportunities that arise over and above the plan.
2	Possible/ Could happen	10% - 40% chance of occurrence	Only likely to happen 3 or more years.	Some chance of favourable outcome in the medium term or less than 40% chance of occurrence.	Possible opportunity which has yet to be fully investigated by management. Opportunity for which the likelihood is low on the basis of management resources currently being applied.
1	Unlikely	Less than 10% chance of occurrence	Has happened rarely /never before.	Less than 10% chance of occurrence.	Has happened rarely/never before

Risk Criteria - Impact

Score	Factor	Effect on Service	Effect on Reputation	Effect on Activity
4	Major	Major loss of service, including several important areas of service areas for protracted period. Service Disruption 5+ Days.	Adverse and persistent national media coverage. Adverse central government response, involving (threat of) removal of delegated powers. Officer(s) and/or Members forced to resign. Major impact on student experience with likelihood of negative impact on student survey results and potential impact on future student recruitment.	Complete failure of activity. Delay – 3 months or more.
3	Serious	Serious loss of an important service area for a short period. Serious effect to services in one or more areas for a period of weeks. Service Disruption 3-5 Days.	Adverse publicity in professional and/or municipal press, affecting perception and/or standing in professional and/or local and/or government community. Adverse local publicity of a serious and persistent nature. Significant impact on student satisfaction with potential impact on future student survey results.	Serious impact on activity. Most of expected benefits fail. Delay – 2-3 months.
2	Significant	Significant effect on an important service area for a short period. Adverse effect to services in one or more areas for a period of weeks Service. Disruption 2-3 Days.	Adverse local publicity and/or local public opinion. Statutory prosecution of a non-serious nature. Disruption caused to a large group of students or student complaint with merit which requires escalation	Significant effect on activity. Delay – 3 weeks – 2 months.

Glasgow Caledonian University Risk Management Policy

1	Minor	Minor disruption of important service area. Minor effect on non-crucial service area. Service Disruption 1 Day.	Contained within section/Unit or Directorate. Complaint from individual student/small group of students, of arguable merit.	Minor impact on activity. Delay less than 2 weeks.
----------	-------	---	--	---

5.3 Managing Risk

In broad terms any risk can be addressed (or managed) using one of the four methods below - the 4 T's.

Tolerate	Accept the risk, either because it is insignificant or it would not be of benefit to do any more.
Treat	Take cost effective actions to reduce either the likelihood of the risk happening, the impact, or both.
Transfer	Let someone else take the risk (eg. by insurance or passing responsibility or the risk to a contractor), however, some level of risk is likely to be retained by the University.
Terminate	Agree that the risk is too high and do not proceed with the project or activity

Each risk identified should have a 'risk owner'. The risk owner should be responsible for co-ordinating any activity required to manage the risk, or for simply monitoring the situation to see if the level of risk changes.

If further action is required to manage a risk it should be for the risk owner to propose what action is appropriate. This can then either be agreed or amended by the relevant group of managers.

5.4 Monitoring and Reviewing

Monitoring of risks is often best done as part of reviewing performance. There is a clear link between how an organisation (or a part of an organisation) is performing and how it is managing the risks it faces.

To ensure that the monitoring a review of risk is carried out effectively, the following approach must be followed:

- 1 Risk must be a standing Agenda item on all School/Department Management Meetings, with a formal review of the School/Department Risk Register each quarter, with updates more frequently if circumstances change.

Glasgow Caledonian University

Risk Management Policy

- 2 New risks identified through the decision making process must be identified for inclusion in the Risk Register.
- 3 Red/High risks from School and departmental Risk Registers must be escalated to Finance and the appropriate Executive Lead for consideration by the Risk Management Forum to determine whether the risk has a corporate impact.
- 4 School and Support department Risk Registers will be maintained on Teams as a live document and will be reviewed twice per annum by RMF.

The review of risk will provide comfort to managers that the significant barriers to success are being appropriately addressed, and as part of this process the following should be considered:

- 1 The existing or proposed wording for each specific risk
- 2 Are the “Impact” and “Likelihood” scores for each risk reasonable?
- 3 Are the mitigation actions for each risk appropriate?
- 4 Is the residual risk score reasonable in each case?
- 5 Are the early warnings and planned actions appropriate?
- 6 Are risk owners and co-owners valid?
- 7 Agree timelines for each risk
- 8 Are there any risks that are not covered that should be included or any further actions or controls that should be added?

6 Risk Event Log

A Risk Event Log will be maintained by the Risk Management Forum so that the University can benefit from lessons learned due to significant and unexpected events.

A Risk Event Log entry must be completed for any incidence where a risk has or is expected to materialise and:

- The reputation of the University has been impacted in an adverse way;
- There has been significant adverse impact on the operations of the University; or
- There has been significant financial loss to the University (If an event has not adversely impacted the reputation or operations of the University then Risk Event Log entries should be limited to those where the financial impact was greater than £50k.)

There will be a Risk Event Paper presented at each RMF to inform the decision on adding any Risk Events to the Risk Event Log

The Risk Event Paper and new entries on the Risk Event Log will be presented at all Audit Committee meetings.

Glasgow Caledonian University

Risk Management Policy

Each Risk Event Entry will include Actions to be undertaken and there will be regular review of status of the Actions included in the Risk Event entries.

7 Risk Management Forum

The Risk Management Forum (RMF), reporting to the University Executive Team (UET), is responsible for overseeing the successful implementation of the University's Risk Management Policy. This will include responsibility for the co-ordination of risk management activity. The RMF will ensure that the necessary processes are in place to manage University risk and achieve compliance with governance requirements.

The RMF will meet every quarter, with additional meetings arranged if necessary. It will report to the University Executive Team quarterly and provide an annual progress report, which summarises the GCU risk management activity overseen by RMF in discharging its responsibilities during that period.

The RMF will be chaired by the Chief Operating Officer & DVC (or nominee) and membership will include:

- Chief Operating Officer and Deputy Vice Chancellor (Chair)
- Chief Financial Officer (Vice Chair)
- UET members with a risk assigned to them
- Representative from each School (at least one Dean)
- Representative of GCU London
- Director of IT
- Director of Student Life
- Director of People
- Director of Strategy & Planning
- Director of Estates
- Director of Future Students, Marketing & Communications
- Director of Governance & Legal
- Head of Security
- Representative from Finance

8 Accountabilities, Roles & Responsibilities

The University Executive Team has overall responsibility for developing the University's approach to risk management. Responsibility for the day to day management of specific risks lies with the managers and staff, as they are the people directly responsible for different business activities.

The different roles and responsibilities for risk management are shown below:

Group	Role
-------	------

Glasgow Caledonian University Risk Management Policy

Court	Legally responsible for ensuring that systems are in place for the assessment and management of risk and approves the University Risk Management. Delegate's authority to manage risk to the Principal, as Accounting Officer, who, in turn, delegates day-to-day responsibility to the University Executive Team.
Audit Committee	Sub Committee of Court with responsibility for monitoring and reviewing the effectiveness of the University's risk management arrangements on behalf of Court and advising Court concerning the internal and external auditors' assessments of the effectiveness of the University's risk identification and mitigation procedures.
University Executive Team (UET)	To formally approve the University's Risk Management Policy before presentation to Court and to consider risk as part of all decisions. Review the University's arrangements for risk management annually.
Risk Management Forum (RMF)	Reporting to the University Executive Team (UET), the RMF ensures the University manages risk effectively through successful implementation of the Risk Management Policy. The RMF reports to UET and Audit Committee quarterly and Finance & General Purposes Committee twice per annum. RMF will provide an detailed Corporate Risk Register paper to University Court annually. In addition there will be a brief update paper, highlighting material changes to the Risk Register since last reviewed by University Court, provided by RMF for each Court meeting where the annual detailed paper is not presented. In addition to reviewing School, Department and the Corporate Risk Register, the group will consider strategic risks affecting the organisation and make recommendations to the Board as appropriate.

Group	Role
Managers	Ensure risk is managed effectively in line with the University's Risk Management Policy and this is reviewed and reported appropriately. Risks should be recorded in the School/department Risk Register and managers should highlight risk matters to their Executive member as required. Formally review all arrangements for risk management affecting their activity each quarter, with updates more frequently if circumstances change.

Glasgow Caledonian University Risk Management Policy

Project Managers & Principal Investigators	Ensure project risk is managed effectively in line with the University's risk management policy and this is reviewed and reported appropriately. Where material, project risks should be recorded in the School/department Risk Register.
All Employees	Undertake their job within risk management guidelines, including compliance with all control measures that have been identified. Report any risks to their Managers.
Internal Audit	Comment on the adequacy of the process in place to identify risk and the effectiveness of the control measures in place. Make recommendations to Management, the University Executive Team and Audit Committee as necessary.
External Audit	External Audit based around key areas of financial risk to GCU highlighted on the Corporate Risk Register.

9 Project/Initiative Planning

Managing risks within projects, and new initiatives, is part of running a successful activity. Risk should be considered before the start of the activity, as part of the initial project/solution design and in overcoming the barriers to delivering a successful outcome.

A detailed Project Risk Register must be prepared using the template at [Appendix 4](#).

A Project Risk Register must be completed for commercial, transnational education and research projects.

A Project Risk Register should also be completed for any change management initiative that is not covered elsewhere but which will impact Risk to the University.

10 Partnerships and Contracts

Where the University provides services in partnership with others or through a contractor, risks need to be considered as if GCU were providing those services itself. Whilst these risks may be managed through formal contracts and partnership agreements that clearly allocate risks to the appropriate parties, failure by either or any one of those parties to manage their risks effectively can have serious consequences for the other(s).

Before entering into partnership, joint working or business contract arrangements, the prospective partners and contractors should be asked to provide evidence of their approach to Risk Management.

Depending on the scale of the partnership or contract, a detailed Project Risk Register must be prepared – see [Appendix 4](#).

11 Decision Making

Where the University Executive Team or University Court is being asked to make decisions they should be advised of the risks associated with the recommendations being made.

The standard GCU Business Case Template contains a Risk and Impact section, but where the decision is material a detailed Project Risk Register must be attached – see [Appendix 4](#).

All GCU University Executive Team and Committee papers include a Risk section on the front cover which requires confirmation of the mitigation to existing risks that are provided by the proposal, together with details of any additional risks created by the proposal. A detailed project Risk Register to be included in the submission for any proposal with material risks attached.

12 Business Continuity and Disaster Recovery Planning

Some risks could impact upon the University business running during times of change or disruption. These risks will feed into the business continuity planning cycle. Consideration should be given to having business continuity plans in place should these risks happen.

Certain risks emerge which could mean major disruption to our business, senior management teams, employees or accommodation. These risks will be dealt with as part of the University's disaster recovery planning cycle.

13 Fraud Risk

The University is committed to preventing fraud and maintaining strong standards of integrity across all of its activities. The recent introduction of the Failure to Prevent Fraud offence under the Economic and Corporate Transparency Act 2023 (ECTTA) requires large organisations – including universities – to put in place reasonable fraud prevention measures based around six principles of:

1. Top-level commitment
2. Risk Assessment
3. Proportionate risk-based prevention procedures
4. Due Diligence
5. Communication (including training)
6. Monitoring and Review

There is no specific Fraud risk maintained on the Corporate Risk Register, instead the assessment of and measures to manage fraud are included within the assessment and documentation of the specific risks on the Corporate Risk register and in operational Risk registers.

There is a specific Fraud risk included within the Finance operational risk register.

Glasgow Caledonian University Risk Management Policy

There is a suite of counter fraud policies currently in place at the university which are in place to mitigate against fraud risk, including:

Policy	Owner
Financial Regulations & Procedures	Finance
Financial Misconduct	Finance
Anti-Money Laundering	Finance
Delegated Authority	Finance
Criminal Facilitation of Tax Evasion Statement	Finance
Public Interest Disclosure	People Services
Anti-Bribery	Governance & Legal
Gifts & Hospitality	Governance & Legal