Risk Management Framework

Document Control Information	
Reviewed by the Audit & Risk Committee:	**November 2021**
Date of Next Review:	**December 2024**
Approved by the Board of Management:	**December 2021**

The Board of Management (or any person/group with delegated authority from the Board) reserves the right to amend this document at any time should the need arise following consultation with employee representatives.

1. Introduction

Risk is a part of everyday life and successful organisations manage their risks effectively. High quality risk management is a key process which supports and enhances business management. In this context a risk is defined as an event which can affect, positively or negatively, the delivery of the agreed outcomes and objectives of the organisation.

The College recognises that it has a responsibility to manage internal and external risks as a key component of good corporate governance and is committed to embedding risk management to help achieve its strategic and operational objectives.

Risk Management is a key aspect of the College strategic planning, governance and management framework and the Board of Management sets its appetite for risk as a basis for the management of the College.

This Risk Management Framework outlines the College's approach to risk and how it should be managed. It helps ensure risks are properly identified and then either eliminated or mitigated to an acceptable level. This approach is to protect the College and ensure risks are managed effectively. The Framework also aims to emphasise the opportunities afforded by positive risk management, which is important to support the successful delivery of the College's strategic objectives.

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

The Vice Principal Operations has responsibility for ensuring that the Risk Management Framework is implemented.

2. Objectives of the Framework

The principal objectives of this Framework are:

- To implement and embed risk management across the College in line with the best practice in Risk Management, thereby creating a valuable and positive, proactive business management tool, which will help the College identify and evaluate opportunities as well as threats.
- To assist the College develop resilience, supporting the organisation in anticipating and responding to changing risks and thereby 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 as well as raising awareness of risk in all involved in Learning & Teaching and delivery of the College Support Services.
- To ensure organisational time and resources are aligned appropriately to the risks the College faces.
- To prevent injury, damage and losses, and reduce the cost of risk and protect the College's reputation through strengthened governance, accountability and decision making.

- To ensure and facilitate compliance with best practice in corporate governance, ensuring that theappropriate disclosure statement can be issued within the Annual Report and Financial Statements.
- To provide assurance to, and work collaboratively with key stakeholders, to ensure significant risks are being managed appropriately.

3. Risk Management Governance in the College

The Board of Management is responsible for Risk Management within the College. The Board will approve the Risk Management Framework, the Risk Appetite Statement and the Risk Register at least twice per year.

The Audit & Risk Committee have a level of delegated responsibility for reviewing the system of Risk Management within the College, ensuring it is appropriately scrutinised and audited, and for recommending changes to the register or the system of risk management to the Board of Management. Risk Management will therefore be a formal agenda item at each meeting of the Audit & Risk Committee.

Risk Management will also feature on the agenda of all Board, Board Sub-Committee and formal College Committee meetings for consideration.

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

College Risk is overseen by the Senior Management Team (SMT), who has put in place a Risk Management Committee (RMC) to consider the operational management of risk. The RMC reports to the SMT and is authorised to make recommendations regarding the management of risk in the College. The RMC reports to SMT after each meeting will provide a detailed annual progress report to SMT for noting. In addition, Risk activities are reported to each Audit & Risk Committee and to the main Board a minimum of twice per annum.

The RMC will meet a minimum of four times per year and the purpose and function of the RMC is set out in its' Terms of Reference, a copy of which is attached at Appendix 1.

4. Risk Appetite

The Board of Management will set a Risk Appetite. This statement specifies the Risk Appetite or willingness of the Board of Management to accept or tolerate different levels of Risk in relation to specific aspects of the College's activities. The Board is responsible for the overall management of risk and opportunity. It must set the risk appetite and ensure there is an appropriate balance between risk and opportunity and that this is communicated to the management team.

Risk Appetite was fully reviewed in November 2021 and is presented below.

	Risk Appetite				
Risk Category	**Averse**	**Minimalist**	**Cautious**	**Open**	**Hungry**
1. Policy					
2. Reputation					
3. Financial					
4. Digital					
5. Workforce					
6. Student Experience					
7. Legal & Compliance (including Health & Safety risks)					
8. Environmental Sustainability					

The Board's Risk Appetite Statement is an integral part of the Risk Register and will be re-considered by the Board at least twice per year. The College SMT will then manage the College on the basis of the Risk Appetite Statement.

The table below details the behaviors associated with each Appetite.

Risk Appetite	Example Organisational Behaviours
1. Averse	• Preference is for ultra-safe actions; stick to tried & tested methods • Innovation / change is avoided unless it's forced upon us • All reasonable steps will be taken to manage the risk; we are prepared to be bureaucratic and tightly control processes • Only prepared to accept only insignificant or very minor losses if the risk happens
2. Minimalist	• Preference is for low risk actions that have worked well in the past • Innovation / change is avoided if possible or only taken to make incremental improvements • All reasonable steps will be taken to manage the risk; prepared to be bureaucratic and tightly control processes • Prepared to accept minor losses if the risk happens
3. Cautious	• Preference is for actions that are unlikely to result in any loss • Innovation / change is generally avoided, and will only be entered into if all stakeholders are committed, and success is almost guaranteed • Open to new ways of working, if they have been proven elsewhere • Prepared to accept the possibility of moderate losses if the risk happens
4. Open	• Willing to take bold decisions where benefits outweigh the risks, but only if steps have been taken to reduce / mitigate risks • Innovation is supported, but only if clear benefits are demonstrated and we are reasonably confident in our success • Open to new ways of working, even if they are not fully proven • Prepared to accept major losses are possible if the risk happens
5. Hungry	• Willing to accept increased scrutiny from stakeholders and a loss of credibility if things go wrong • Innovation is pursued, we are willing to break the mould to deliver organisational goals even if failure is a possibility • Eager to 'break the mould' and be disruptive compared to peers or competitors • Prepared to accept catastrophic outcomes are possible if the risk happens

The Audit & Risk Committee will seek to review the Risk Register and identify areas where the actual level of perceived risk differs from the appetite for that Risk. In such circumstances it would then be expected that management would put additional mitigations in place. The Scottish Public Finance Manual (SPFM) requires the College to have a Risk Appetite Statement and appropriate Risk Management processes in place.

5. College Risk Register

The Risk Register is a well-established document which identifies and ranks risks and outlines mitigation strategies for the risks identified. This is the main tool for recording risks and is a live document which is updated on a regular basis. The format of the Risk Register is based on Charted Institute of Public Finance and Accountancy (CIPFA) risk management guidance. It identifies the risks and scores them in relation to probability and materiality. This enables the College to identify those risks which could have a material impact and are likely to occur. The Risk Register is considered at every meeting of the Audit & Risk Committee, Risk Management Committee and is considered twice per year by the Board of Management and once per year by each of the other formal Sub Committees of the Board.

The risk register is the key risk management tool for managing risk effectively. The register supports the capture, assessment and monitoring of risk facing an organisation, providing useful reporting on risk trends, action planning and the sharing of lessons learned across the College.

The Risk Register is compiled in Excel and is attached at Appendix 2. The same format is used for all Team Risk Registers as well as for the overall College Risk Register and includes: a reference number, status, date identified, risk title, risk description, strategic plan alignment, risk owner, responsible officer, evaluation of the inherent (Gross) risk, risk treatment approach, detail of the mitigating actions and controls in place, evaluation of the residual risk, risk appetite category/ impact, actions planned, warning mechanisms, date reviewed and the movement in the period. This format was introduced in November 2021 and is best practice.

The risk register will be used as the basis for monitoring risk throughout the College. Key teams will be responsible for identifying the risks in their service area and will record these using the attached risk register format.

These Registers, together with any Project Risk Registers will feed into the overall College Risk Register, which will contain all significant risks that may affect the achievement of strategy and objectives, recording the measures in place for dealing with them.

A Project Risk Register must be completed for all major projects where funding is in excess of £250,000, or where required by management.

The Risk Register is considered at every meeting of the Audit & Risk Committee, the RMC, the SMT and twice per year by the Board of Management.

Risk Registers are collated using the five stage Risk Management process below.

5.1 Identification and Recording of Risk
5.2 Evaluation of Risk
5.3 Management of Risk
5.4 Monitoring & Reviewing of Risks

5.1 Identification and Recording of Risk

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 team or Project Manager, i.e. by those who are responsible for delivering the objectives of the area.

Before identifying risks, the group should be clear on what their objectives are. Risks come in manydifferent types. Consideration should be given to the wide range of different types of risks, such as operational, financial and reputational. When 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 group discussion session/Horizon scanning*
- *Increased staff awareness – so they know how to feed into 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 or trend analysis from complaints data*
- *Internal or external reports and horizon spotting – press, etc*
- *Trends or risks identified in operational risk assessments or site surveys*

Risk identification is an ongoing activity, with individual risks and the impact and/or likelihood of risk changing regularly. Risk identification is the process of determining what outcomes you are seeking to achieve and identifying what can threaten the achievements of these objectives.

The process for describing risks is set out below. All risks should be crafted to detail the risk, cause and effect:

Risk:	A brief description of the event or the potential threat (or opportunity).
Cause:	The drivers or triggers that may lead to the realisation of the risks / uncertainty.
Effect:	The consequences that may arise from the risk / uncertainty materialising.

Risk descriptions themselves are often prefaced with:

"Loss of…."	*"Lack of…."*	*"Failure to…."*	*"Inappropriate…."*
"Inability to…."	*"Reduction of…."*	*"Disruption to…."*	

Describing Risk Example:

Risk:	Failure to deliver major change projects on time and on budget.
Cause:	Lack of, or ineffective, project management; under-estimation of resource requirements; lack of appropriate resources; conflicting priorities.
Effect:	Financial pressure; detrimental impact to deliverability of other parts of the programme; increase in temporary staffing costs.

5.2 Evaluation of Risk

Once the risks have been identified they need to be evaluated. This involves evaluation of the likelihood of a risk occurring and impact if it does. This is done using the scoring matrices below at two stages. The inherent risk is assessed as the risk if there were no controls or mitigating actions. Once these are taken into account the residual risk is then evaluated.

Not all risks faced by the organisation will be of the same magnitude or significance. Neither does the College have the resources or will to manage every single risk it faces. 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.

The College evaluates risks using a 5x5 Risk Evaluation Matrix – see below.

Risk Criteria – Likelihood Assessed on a 1 to 5 scoring basis

TITLE	DESCRIPTION	SCALE
Almost Certain	Very high chance, or even certainty, that this will happen	5
Likely	Likely to happen	4
Possible	Possible chance of happening	3
Unlikely	Small chance of happening	2
Rare	Very unlikely. Assumption is that it will never occur	1

Risk Criteria – Impact Assessed on a 1 to 5 scoring basis

The impact category is decided by taking the highest impact of the risk, for example if a risk scores a '5' for reputational impact but a '4' in all other categories the risk should be considered to have an overall rating of '5'. However, it should be noted this is guidance and teams are free to use their professional judgement when prioritising risks.

For Team Risk Registers, the likelihood of the risk is assessed as the possibility of the risk occurring in the next 12 months, whereas for the College Risk Register, which focuses on Strategic Risks, this can be for up to three years.

Impact

TITLE	DESCRIPTION	SCALE
Catastrophic	Death, total systems loss, unacceptable outcome	5
Major	“Major” injury/illness, major damage or impact	4
Moderate	Loss time injury/illness, serious damage or impact	3
Minor	Minor impact or outcome	2
Insignificant	Very minor. Little consequence	1

Risk Evaluation Matrix – 5x5

This is a ‘5x5’ matrix and the assessed scores of impact and probability are multiplied together to determine the overall risk score, to a maximum of 25. Based on the score allocated for likelihood and the impact score, a total risk will be calculated.

Likelihood x Impact

13 - 25	Critical risk – should be eliminated or moved to a lower level
8 - 12	Undesirable – must be avoided if reasonably practicable
3 - 7	Acceptable – can be accepted provided risk is managed
1 - 2	Low -no further consideration required

5.3 Management of Risk

Each risk, based on its score, will be rated as either LOW, ACCEPTABLE, UNDESIRABLE OR CRITICAL and will be colour-coded according to the Risk Assessment Table above. This rating will determine the broad approach to be taken to the management of each risk, as set out below. This rating reflects the level of risk that the College is willing to accept or tolerate, which then dictates the level and intensity of response required.

	Risk remains above acceptable level
	Risk remains undesirable
	Risk is acceptable or can be managed

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

Each risk identified should have a Risk Owner and Responsible Person where different. 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 Responsible

Person to propose what action is appropriate. This can then either be agreed or amended by the relevant group of managers.

The Risk Owner is considered to be accountable for the risk and is the person who co-ordinates any activity to manage the risk within the College. The Responsible Person may have accountability or responsibility for specific tasks or actions that help control the risk in question.

Tolerate	Accept the risk because: • It is relatively insignificant • It would not be of benefit to do any more, ie where the cost of avoidingor treating the risk is considered to outweigh the potential benefits. • The risk at the current time is acceptable to the College and resources shouldbe invested elsewhere.
Treat	Take cost effective actions to reduce either the likelihood of the risk happening,the impact, or both. ***Examples of actions to reduce likelihood:*** • Introducing procedure manuals and controls with which all staff mustcomply. • Documented authorisation procedures and limits. • Regular review and compliance checking to evidence procedures beingfollowed. • Specification of contract conditions to mitigate potential College exposure. • Staff training to raise awareness of the risk and controls required. ***Examples of actions to reduce impact:*** • Business Continuity and emergency planning. • Public relations and media handling. • IT back up arrangements in case of systems failure. After treatment a risk may still remain. A decision will then be taken as towhether the remaining risk is at a tolerable level or further action is still required.
Transfer	Let someone else take the risk (eg. by insurance or passing operationalresponsibility for the risk to a contractor or partner). When a risk is transferred some level of risk is invariably retained by theCollege, such as the reputational consequences of a service failure
Terminate	Agree that the level of risk is too high and do not proceed with the project oractivity (or carry out the activity in a different way).

5.4 Monitoring & Reviewing of Risks

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 and reviewing of risk is carried out effectively, the following approach should be followed:

1. Risk should be a standing Agenda item on all Meetings, with a formal

review of all College Risk Registers each quarter, with updates more frequently if circumstances change. If necessary SMT will seek assurance from the individual Risk Owners that the risk they are responsible for is being effectively monitored and action is being taken as agreed in formal action plans.

2. New risks identified through the decision making process should be identified for inclusion in the Risk Register.

3. All Team Risk Registers will be collected centrally twice per annum. Red/High risks from Team Risk Registers will be presented to the RMC twice per annum together a summary of the movements in these Registers. Any issues or concerns should be flagged to the RMC Chair or another member of the RMC, for consideration by the RMC, in order to determine whether the risk has an impact on the College Risk Register.

The review of risk should 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 are any risks that are not covered that should be included or any further actions or controlsthat should be added?

6. Structure for Managing Risk in the College

The College has a number of processes and procedures in place to manage risk effectively, detailed below.

6.1 Risk Management Committee

The College has a Risk Management Committee (RMC). This Committee meets a minimum of 4 times per academic year and consists of members of the Senior Management Team and a wide range of Operational Managers. The Terms of Reference for the RMC is provided in **Appendix 1.** This Committee is the main operational group with responsibility for discussing Risk Management issues and it considers the Risk Register at each meeting and recommends changes to it. The Committee is chaired by the Director of Corporate Services.

6.2 Meeting Agendas

All meetings of the Board of Management, its standing committees and all formal internal meetings have Risk Management as a standard agenda item. This ensures that any new risk management issues are identified by members of the committee and if appropriate included in the Risk Register. In respect of formal, internal College meetings it is the responsibility of the Chair to inform the Chair of the Risk Management Committee of any new risks identified.

6.3 Board of Management Reports

All formal reports to the Board of Management and its Standing Committees include a section on Risk Management implications. The author of the report is required to consider and highlight any risk implications arising as a consequence of the contents of the report.

6.4 Board Development

Risk Management will be considered as a Board development topic and forms part of the induction process for all new members of the Board of Management.

6.5 Audit & Risk Committee

The Audit & Risk Committee has a specific role in the review and management of risk. It considers the Risk Register and Risk Appetite Statement at each meeting as a standing agenda item. The Committee will make recommendations for changes to the Risk Register, Risk Management Framework and Risk Appetite Statement to the Board of Management. The Audit & Risk Committee also has responsibility for the oversight of College Internal and External Audit arrangements. The Committee are required to ensure that audit programmes include Risk Management as a topic for regular independent audit review and to ensure that the audit plans take appropriate cognisance of perceived risk.

6.6 Assurance Framework

The College will maintain an assurance framework which will be regularly reviewed by the Audit & Risk Committee and presented to the Board of Management annually. The Vice Principal Operations will be responsible for maintaining a mapping of all sources of assurance which are available routinely to the Board of Management and its Standing Committees. The objective of this exercise is to review the full range of the sources of assurance which aim to provide the Board with assurance that the College is being managed and operated in a way which is consistent with its Mission, Vision, and Strategic Plan. The sources of assurance will also seek to provide evidence that the processes and procedures in place to ensure that the College is well controlled and managed are being adhered to. The Assurance Framework and its regular review will also ensure that the College is compliant with the Scottish Government Audit and Assurance Committee Handbook.

6.7 Insurance

The College ensures that it has an appropriate level of insurance in place as a key risk management Framework. The Director of Corporate Services is responsible ensuring procurement and arrangement of insurance cover. Details of the cover in place are reported annually to the Finance and Resources Committee, The Audit & Risk Committee and to the Risk Management Committee.

6.8 Health and Safety Management

Health and Safety Management at the College is a further element of the Risk Management Framework. A separate Health and Safety Policy and management process operates within Glasgow Kelvin College. The minutes of the Health and Safety Committee are considered by the Risk Management Committee at each meeting. The Board of Management approves the Health and Safety Policy annually and also considers an annual report on Health and Safety.

6.9 Strategic and Operational Planning

The College Strategic and Operational processes include consideration of the wider context facing the College and its local partners. This includes a review of the operational environment in which the College operates to ensure that the both the Senior and Operational Management Teams give full consideration to internal/external risks and challenges.

6.10 Financial Planning

The budget preparation and monitoring processes include explicit reference to the financial risks associated with the strategic and operational plans on an annual basis. The Finance and Resources Committee has responsibility for the oversight of financial management. The Vice Principal Operations also has responsibility for medium term financial planning, associated scenario planning and for ensuring that Risk Management is integrated into these planning and modelling processes.

6.11 Business Continuity Planning and Disaster Recovery

It is the responsibility of the Director of Corporate Services and the Director of Digital Services to ensure that the College has appropriate disaster recovery documentation, processes and procedures in place which are subject to regular review and testing. This will help ensure the College has the capacity and plans in place which will enable it to recover quickly in the event of a major incident. This is aimed at minimising the risk that the College will be unable to deliver is operational objectives as a result of an unforeseen incident.

7. Review

The Risk Management Framework will be reviewed every three years, unless changes require to be made during this period.