Capital City College Group

Risk Management Policy 2020/2021

Author:	**Stewart Cross**	**Approved by:**	GLT, Audit Committee and the Board
Version:	1.0	**Date of approval**:	08/07/2020
Equality Impact Assessed	Yes	**Review date:**	Annual: June 2021

Contents

1. Purpose

1.1. Capital City College Group is committed to the highest standards of accountability and probity throughout its operation, ensuring responsible use of resourses to maximise the benefits to our students, business clients and communities in which we work. This policy outlines its approach to risk in order to guide decision making and promote an organisational culture in which risks are identified, assessed and managed effectively.

1.2. This document sets out the policy for managing risk at the Capital City College Group ("the Group"), and the procedures by which that policy is put into effect.

1.3. It has been designed to provide a framework for managing the risks the Group faces, ensuring that risk management is embedded in all group activities and enabling the Group's risk management objectives to be achieved in the most effective way. It documents the roles and responsibilities of the Board and members of staff including the Group Leadership Team in managing risk.

2. Scope

2.1. The policy applies to all college activities, and at all levels within the organisation. The oversight, identification and management of risk is a key responsibility of the Group's Board, the Group Leadership Team and College management. All staff within the organisation are integral to the identification and management of risk.

2.2. This document forms part of the Group's internal control and governance arrangements.

3. The Nature and Purpose of Risk Management

3.1. The Group adopts the ISO31000 definition of risk and risk management. **Risk** is defined as the effect of uncertainty on objectives. **Risk Management** is defined as coordinated activities to direct and control an organisation with regard to risk. This is carried out by:

- Methodically identifying, categorising and evaluating each risk.
- Identifying links between different risks.
- Establishing controls to mitigate risks.
- Assessing the effectiveness of these controls and the remaining risk.
- Identifying further work needed.
- Providing corporate oversight of risk.

3.2. The risks to be managed can be risks of omission as well as commission. Failure to take action which could benefit the Group, and taking action which could harm the Group, are both treated in the same way.

3.3. Risk Management forms part of the Group's system of internal control. This system encompasses a number of elements that together facilitate an effective and efficient operation, enabling the Group to respond to a variety of operational, financial, and commercial risks. It is designed to identify and prioritise the risks to the achievement of Group policies, aims and objectives, to evaluate the likelihood of those risks being realised and the impact should they be realised, and to manage them efficiently, effectively and economically. Its elements include:

a. *Policies and procedures.*
Attached to significant risks are a series of policies that underpin the internal control process. The policies are set by the Board of Governors and implemented and communicated by senior management to staff. Written procedures support the policies where appropriate.

b. *Regular reporting*
Comprehensive reporting systems to the Group Leadership Team (GLT) and Board are designed to monitor key risks and their controls. Decisions to rectify problems are made at regular meetings of the GLT and the Board where appropriate.

c. *Business planning and budgeting*
The Business Planning and budgeting process is used to set objectives, agree action plans, and allocate resources. Progress towards meeting Business Plan objectives is monitored regularly.

d. *Group Risk Register*
A Group Risk Register is prepared by GLT and approved by the Board. This is a framework which helps to facilitate the identification, assessment and ongoing monitoring of risks significant to the Group. A separate project Risk Register may be set up for a major Group initiative.

e. *College, CCCT and Directorate Risk Registers.*
Colleges, CCCT and corporate directorates will develop and use this framework to ensure that their significant risks are identified, assessed and monitored. The documents will be formally appraised annually but emerging risks will be added as required, and improvement actions and risk indicators will be monitored regularly. Colleges will report on risk to their College Education Boards.

f. *Financial Controls*
The Group has a comprehensive set of financial controls; including a comprehensive annual budgeting system, regular reviews by the Board of financial performance against forecasts, target setting & monitoring, capital investment guidelines and formal project management disciplines.

g. *Audit Committee*
The Audit Committee is required to report to the Board on internal controls and alert them to any emerging issues. In addition, the committee oversees internal audit, external audit and management as required in its review of internal controls. The committee is therefore well-placed to provide advice to the Board on the effectiveness of the internal control system, including the Group's system for the management of risk.

h. *Internal audit programme*
Internal audit is an important element of the internal control process. Apart from its normal programme of work, internal audit is responsible for aspects of the annual review of the effectiveness of the internal control system within the organisation. It operates within the ESFA's *Post 16 Audit Code of Practice*.

i. *External audit*
External audit provides feedback to the Audit Committee on the operation of the internal financial controls reviewed as part of the annual audit.

j. *Third party reports.*
From time to time, the use of external consultants will be necessary in areas such as health and safety, and human resources. The use of specialist third parties for consulting and reporting can increase the reliability of the internal control system.

4. Risk Management Policy and Objectives

4.1. Risk Management aims to ensure that Group resources are directed efficiently and effectively to minimise the overall risk to the organisation. The following policy statement sets out the Group's approach to risk management:

- The Group is a risk aware organisation and seeks to manage risks actively, particularly those with a potentially negative impact.
- The Group adopts an open and receptive approach to risk identification and management; it promotes a culture where risks can be discussed freely and will be escalated effectively.
- The Group will seek to learn from the risk management processes with the aim of continual improvement.

- Key risks will be identified and closely monitored on a regular basis.
- Risk appetite will be determined by the Board on an annual basis taking into account the business strategy context, risk management culture, risk management processes and its risk management systems.

4.2. The Group's overall Risk Management plan is aimed at:

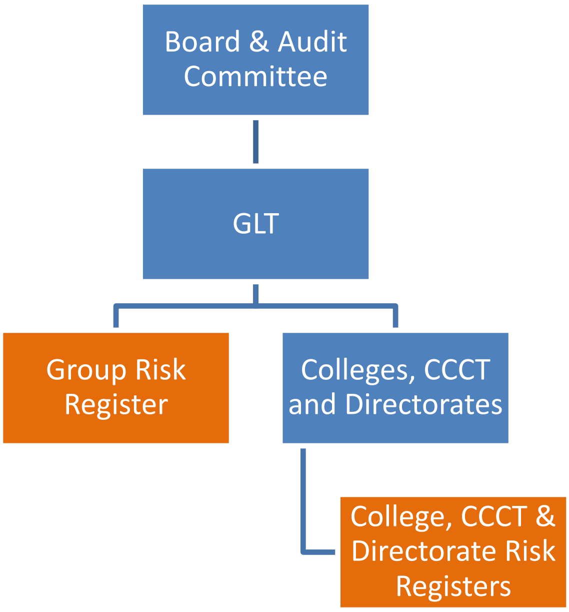
- Protecting its students, staff and assets.
- Managing risk in accordance with best practice and reducing the cost of risk.
- Anticipating and responding to changing social, environmental and legislative requirements.
- Raising awareness of the need for Risk Management.
- Integrating Risk Management into the culture of the Group.
- Adopting legal compliance as a minimum standard.

4.3. Effective Risk Management protects and adds value to the Group and its stakeholders through supporting the Group's objectives by:

- Improving decision making, business planning and prioritisation by comprehensive and structured understanding of the wider business environment.
- Enhancing communication between departments and services.
- Protecting and enhancing Group assets and image.
- Developing and supporting staff and the Group's knowledge base.
- Helping to focus the internal audit plan.

5. Risk Management Framework

5.1. Risk is managed within each of the colleges, CCCT and corporate directorates and the within the Group, and recorded in their separate Risk Registers, which in the case of the colleges are reported to their Education Boards. Risks that arise from activity that flows between the Colleges/CCCT and the Group, plus systemic and high level strategic risks will be recorded and reviewed at Group level. The Group Risk Register is reported to the Board of Governors, and scrutinised by the Audit Committee on their behalf.


Board & Audit Committee
GLT
Group Risk Register
Colleges, CCCT and Directorates
College, CCCT & Directorate Risk Registers

5.2. The Board has oversight of the risk management strategy and the common approach to the management of risk throughout the institution, through the development, implementation and embedding within the organisation of a formal, structured risk management policy and associated procedures. On behalf of the Board, the Audit Committee has the responsibility to consider and advise on the adequacy and effectiveness of the system of internal control and to adopt a risk based approach to assessing it.

6. Identifying Risks

6.1. As the first step in the risk identification process it is necessary to understand the Group's corporate objectives and the legal and regulatory environment in which it operates.

6.2. The second step is the translation of these objectives into operating aims in the form of detailed business plans and performance indicators for each area of activity. This should be an ongoing annual exercise with regular updating of the aims.

6.3. The next step is to identify what would stop each area, or the organisation as a whole, being as successful as it should. Risks can readily be identified through either mind mapping or a more structured approach. What is most important is the completeness of the lists of risks. Some risks will cross 'functional' boundaries; many may not fit neatly into pockets. Generally risks evolve, and new ones are identified as old ones disappear.

6.4. There are many methods for grouping risks, starting from either categorising risk or analysing it using a functional approach. Consideration by category, for example, would include:

- *Strategic risks* – concern the long-term strategic objectives of the Group. They can be affected by such areas as capital availability, legal and regulatory changes, reputation and changes in the physical environment.
- *Operational risks* – concern the day-to-day issues that the organisation is confronted with as it strives to deliver its strategic objectives. For example, relationships with subsidiaries and subcontractors and failure to maintain timely and accurate learner data.
- *Financial risks* – concern the effective management and control of the finances of the Group and the effects of external factors such as funding and market exposures. For example, failure to achieve a balanced budget.
- *Compliance risks* – concern legal or funding compliance issues such as health & safety, environmental, trade descriptions, consumer protection, data protection, employment practices and regulatory issues.
- *Reputational risks* – concern potential damage to the Group by association, for example with local events or the behaviour of linked organisations; from the press, word-of-mouth and its on-line presence.

7. Assessing Risks

7.1. Having identified the risks that the Group is facing, they need to be prioritised into a manageable order so that action can be focused on the most significant risks.

7.2. The risk before any controls are applied (called the **gross risk**) should be considered in terms of its likelihood and impact. Not all risks will affect the Group with the same impact, and some are far more likely to occur within the Group than others. There is perhaps a low likelihood of fire in a large teaching centre, but there would be a significant disruption if a large part of the centre becomes unusable.

7.3. Likelihood and impact should be scored as follows. The assessed gross risk is the product of the likelihood and impact scores:

Assessment of Likelihood (in the next 12 months):

5 = Highly probable
4 = More than likely
3 = Evens chance
2 = Less than likely
1 = Highly improbable

Assessment of Impact (on the Group as a whole):

5 = Catastrophic
4 = Substantial
3 = Significant
2 = Moderate
1 = Minor

Risk calculation (Likelihood x Impact):

Likelihood	**5**	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	**2**	**3**	**4**	**5**
	Impact					

Colour coding:

🟥	High Risk >10
🟧	Medium Risk 5-10
🟩	Low Risk <5

7.4. Impact is the harder to evaluate. The impact score should be based on the potential effect on the Group as a whole. If in doubt, financial impact should be used. So, for example, a financial crisis in a partner organisation may have a very serious impact on that relationship, but if we can be assured that the reputation of the Group is unaffected and the financial consequence for the Group is limited, the impact should be scored low.

8. Controlling Risks

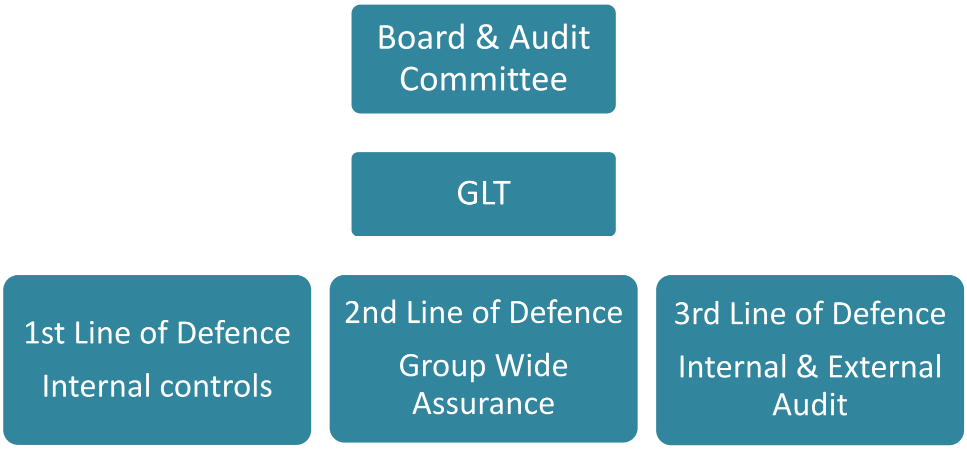
8.1. Once risks have been identified and prioritised, it is necessary to decide how the Group will address them. There are four main options:

- Do nothing, i.e. accept the risk. This is acceptable where the likelihood and impact of the risk are both low.
- Avoid the risk by withdrawing from that area of activity.
- Transfer all or part of the risk to a third party such as a subcontractor, business partner or insurer.
- **Mitigate** the risk.

8.2. In most cases of significant risk, mitigation will be the preferred action. This is achieved by putting in place **controls** which reduce either the likelihood or the impact of the risk. Some controls will address the whole of the Group, and some will be confined to the areas where the risks have been identified.

8.3. In each case a control needs to be evidenced. The **evidence** is a document, electronic record or process check that provides a persistent record that the control has been successfully applied.

8.4. The Group recognises three levels of controls and their associated evidence. This forms a standard model of Three Lines of Defence, as illustrated below:



- The first line of defence is provided through College, CCCT or directorate level assurance in the day to day operation of the organisation and supported by our policies and procedures, for example:
  "Evidence of application of the Learner Disciplinary process where required."

- The second line of defence is group-wide internal controls. Examples of the group's second line of defence include the quality assurance framework, financial regulations, health and safety and safeguarding procedures. Their deliverables provide group-wide assurance, for example:
  "Business Planning meetings and budget report to Board"

- The third line of defence is external assurance, for example that provided by the internal and external auditors, who are independently appointed by the Board and report directly to the Audit Committee:
  "Internal Audit reviewed Business Planning in 2018-19 and provided 'Substantial Assurance'".

8.5. College, CCCT or directorate controls are the simplest to put in place, followed by group-wide controls and then external controls. Colleges may implement controls within their individual academic directorates. These controls are often part of the business process and can therefore be evidenced continuously. Group-wide controls often produce monitoring reports periodically, for example to GLT meetings, Audit Committee or Board. External controls such as audits are undertaken at most annually. However, external controls provide the greatest level of corporate assurance. In practice, a balanced set of controls should include examples of all three.

8.6. The risk after all the controls are applied (called the **net risk**) should then be calculated in terms of its likelihood and impact. Not all risks can be equally well controlled. Some risks have a high controllability: the effect of well-designed controls is strong and the net risk is much lower than the gross risk. Conversely, some risks, for example government policy, have a low controllability and the gross and net risks will be very similar.

Controllability is assessed in terms of net risk / gross risk:

H	The Group itself can largely control this risk or influence the environment. Net Risk / Gross Risk < 70%
M	The Group and others can partially control this risk or influence the environment. Net Risk / Gross Risk >= 70%, < 100%
L	The Group can only marginally control this risk or influence the environment Net Risk / Gross Risk = 100%

8.7. The likelihood or impact of an identified risk can change for a number of reasons including:

- The nature of the risk has changed or is changing.
- Existing controls are inadequate or not functioning.
- Existing controls are enhanced.
- New controls are introduced.

8.8. If the net risk score reaches a level that remains a red risk after mitigation, the Audit Committee will consider whether further action needs to be taken to enhance the range of controls.

9. Risk Registers

9.1. Group-wide risks are recorded in a group **Risk Register**, which lists the risks in a structured format approved by the Audit Committee, together with their controls, evidence, gross and net risks. Additional information is included where appropriate, including information on exceptional risks, linkages between risks and further action identified.

9.2. A revised group Risk Register is drawn up termly by a special meeting of the Group Leadership Team. Its preparation is the responsibility of the Director of Information & Integration. The draft group Risk Register is then discussed, amended and approved by Audit Committee.

9.3. The Board may approve a separate project **Risk Register** for a major Group initiative.

9.4. The Group's requires **College, CCCT and Directorate Risk Registers** to be prepared and maintained at least annually. These are the responsibility of Principals and Directors. They are assessed and approved by the relevant Senior Management teams where appropriate. Key risks are then fed into the group Risk Register and shared annually with the Audit Committee.

10. Responsibilities

10.1.The Board and Audit Committee

The Board of Governors has responsibility for overseeing risk management within the Group as a whole. The Board of Governors will:

- Set the tone and influence the culture of risk management within the Group, including risk appetite and expectations of members of staff with respect to conduct and probity.
- Approve major decisions affecting the Group's risk profile and exposure.
- Monitor the management of significant risks to reduce the likelihood of unwelcome surprises or impact.

- Seek assurance that the less significant risks are being actively managed, with the appropriate controls in place and working effectively.
- Review risks on a regular basis through the Audit Committee.
- Annually review the Group's approach to risk management and approve changes or improvements to key elements of its processes and procedures.
- Appoint internal auditors to provide assurance on key risks and as the third line of defence.

Regular monitoring of risk management sits with the Audit Committee, which will act on behalf of the Board to:

- Consider and advise on the adequacy and effectiveness of the system of internal control and the risk based approach to assessing it.
- Provide oversight of the policy and related implementation actions on behalf of the Board.
- Review and recommend adoption of the Risk Management Policy to the Board at least annually.
- Receive reports from auditors and monitor management actions to address the risks identified.
- Agree the format of the Group Risk Register at least annually.
- Consider and approve the Group Risk Register at least three times per year.
- Review the risks in the Risk Register together with their controls to determine if the risks are appropriate and whether further action is necessary to enhance the range of controls.

10.2.The Group Leadership Team must:

- Support and implement policies approved by the Board.
- Review key performance indicators and progress towards group objectives.
- Take necessary action to address adverse departures from objectives.
- Agree actions to deal with any perceived new risks or failures of existing control measures.
- Focus and co-ordinate Risk Management activities throughout the Group.
- Develop risk response processes, including contingency and business continuity programmes.
- Raise the level of management awareness and accountability for the business risks experienced by the Group.
- Develop risk management as part of the culture and provide a mechanism for risk management issues to be discussed and disseminated to all areas of the Group.
- Consider the risk implications of GLT decisions.
- Review the group Risk Register before each Audit Committee meeting, ensuring that key risks identified at college/directorate level are included.
- Set out explicitly the risks contained within papers proposed to Board and its Committees.

10.3.The Director of Information and Integration must:

- Update the group Risk Register and policy and present them to Audit Committee for approval.
- Feed key risks from College, CCCT and Directorate Risk Registers into the group Risk Register and share them annually with the Audit Committee.
- Provide guidance, interpretation and understanding of Risk Management principles, strategy and systems.

10.4.College Principals, Senior Management Teams and CCCT and Corporate Directors must:

- Support and implement policies approved by the Board.
- Review key performance indicators and progress towards group objectives, as agreed by the GLT.
- Take necessary action to address adverse departures from objectives.
- Agree actions to deal with any perceived new risks or failures of existing control measures.
- Focus and co-ordinate Risk Management activities throughout the College/Directorate.
- Develop risk response processes, including contingency and business continuity programmes.
- Raise the level of management awareness and accountability for the business risks experienced by the College/Directorate.
- Develop risk management as part of the culture and provide a mechanism for risk management issues to be discussed and disseminated to all areas of the College/Directorate.
- Consider the risk implications of their decisions.
- Prepare and maintain a College, CCCT or Directorate Risk Register and review it termly.
- Escalate significant risks to the Group.
- Consider whether separate risk registers are required at lower levels within their organisation (depending on its size and complexity), and if so, set out responsibilities, procedures, timelines and review mechanisms for them.
- Colleges will report on risk at least annually to their College Education Boards.

10.5.All managers must:

- Take primary responsibility for managing risk on a day-to-day basis.
- Take responsibility for promoting risk awareness within their operations; introduce Risk Management objectives into their businesses.
- Keep under regular review the risks which fall into their area of responsibility, the possible impacts these have on other areas and the consequences other areas may have on them.
- Use performance indicators to monitor the key business and financial activities, progress towards objectives and identify developments which require intervention, as agreed with their Director.
- Identify and evaluate the significant risks faced by their operations and report them to their Director.
- Report early warning indicators systematically and promptly to directors, to allow action to be taken. The frequency of reporting should be related to how quickly a risk can materialise and its likely impact.
- Ensure that Risk Management is incorporated at the conceptual stage of projects as well as throughout a project.
- Ensure that Risk Management is a regular management meeting item to allow consideration of exposure and to prioritise work in the light of effective risk analysis.
- Comply fully with group policies and procedures to ensure key controls are maintained.

10.6.All staff must:

- Understand their accountability for individual risks.
- Understand that Risk Management and risk awareness are a key part of the Group's culture.
- Understand how they can enable continuous improvement.
- Report systematically and promptly to senior management any perceived new risks or failures of existing controls.

11. Policy Review

11.1. The Board, on the advice of the Audit Committee, shall review and approve the Risk Management Policy at least annually. In so doing, it shall consider the effectiveness of the Policy, with particular focus on:

- The Group's objectives and its financial and non-financial targets.
- The organisational structure and calibre of the Group Leadership Team.
- The culture, approach, and resources with respect to the management of risk.
- The effectiveness of delegation of authority.
- Public reporting.
- Timely identification and assessment of significant risks.
- Prioritisation of risks and the allocation of resources to address areas of high exposure.
- Quality and timeliness of information on significant risks.
- The time it takes for control breakdowns to be recognised or new risks to be identified.
- The ability of the Group to learn from its problems.
- The commitment and speed with which corrective actions are implemented.

12. Implications

12.1. *Financial Implications*
This policy has no direct costs. However, proper implementation of the policy is essential to the Group's system of internal control, which enables it to respond to a variety of operational, financial, and commercial risks.

12.2. Equality Implications
The impact of risk management on the employment, delivery or use of services by individuals with protected characteristics is varied, depending on nature of the risks and the methods of mitigation used. Risks relating to Equality and Diversity are included within the Group's Risk Register, but many other risks (e.g. financial, quality of teaching and learning, health & safety, safeguarding) play important roles too.