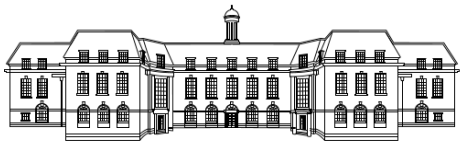


STRANMILLIS UNIVERSITY COLLEGE

A College of Queen's University Belfast

RISK MANAGEMENT POLICY AND STRATEGY

Version No:	Reason for Update	Date of Update	Updated By
1	Review Timeframe	September 2014	Governance Manager
2	Review	June 2017	Governance Manager
3			
4			
5			
6			
7			
8			

Introduction

The purpose of this document is to set out for staff, the University College's policy and strategy for the effective management of Risk and its association with good governance.

Risk Policy

Stranmillis University College's Mission is *'to sustain a vibrant, inclusive learning community, educating, shaping and enriching society through excellence in teaching, scholarship and research.'*

Much of our work is innovative and ground-breaking – and as such involves a certain amount of conscious risk taking.

The Governing Body of Stranmillis University College is committed to ensuring good governance in the delivery of the College's mission and strategic objectives, including the effective and efficient management of its resources and the high quality of the College's projects and activities. We will minimize – and were appropriate eliminate,

where cost effective and reasonable to do so -risks to the achievement of objectives through an appropriate system of controls – so that residual risk, after mitigating actions, can be borne without serious or permanent damage to the College.

Through this policy, the aim is to ensure that all risks associated with the delivery and provision of the College's activities and services are minimized, and wherever possible and practical – eliminated. The University College recognises both its **strategic (corporate) risks** – which will be monitored by the Governing Body and its sub-committees, and the **operational and project risks**, which will be monitored by the Senior Leadership Team and Academic Committees, and reported to the Governing Body on a regular basis.

It is the responsibility of the Governing Body:

- to hold the Principal of the University College to account for maintaining a sound system of internal control that supports the achievement of policies, aims and objectives while safeguarding the public and other funds and assets for which it is responsible in accordance with statutes and ordinances and the Financial Memorandum with the Department for the Economy (DfE);

- to set the tone and influence the culture of risk management within the University College;

- to ensure that risks are managed effectively; and that risks are assessed before they are taken;

- to determine which risks are acceptable and which are not;

- to set the standards and expectations of staff with respect to conduct and probity;

- to determine the appropriate risk appetite or level of exposure for the University College;

- to approve major decisions affecting the Institution's risk profile or risk exposure;

- to monitor the management of fundamental strategic (Corporate) risks;

- to satisfy itself that (less fundamental) Operational/Project risks are being actively managed with appropriate and effective controls in place. Most risks can be effectively managed or even eliminated if dealt with systematically.

This policy sets out the principles that will apply to the management of risks by the University College. The Governing Body will review the Policy bi-annually and approve changes or improvements to key elements of its processes and procedures.

Specific Commitments

In managing risk, the University College commits to:

a. satisfying all mandatory and statutory responsibilities and duties in line with legislation, established good practice, and its own policies and procedures.

b. ensuring the health, safety and wellbeing of those who provide and/or use its services.

c. promoting community relations and good relations in all of its activities – ensuring that they are inclusive and accessible to the best of its abilities.

d. promoting safe working practices – aimed at the reduction and/or elimination of risk.

e. promoting awareness and management of risks through communication and training.

f. establishing and regularly reviewing a systematic and consistent approach to risk assessment and risk reduction/elimination.

g. prioritising risks – and ensuring that their management and reduction is appropriately and proportionately resourced.

h. implementing this policy in line with the Risk Management Strategy – approved and regularly reviewed by the Board.

Risk Appetite

In setting its risk appetite, the Governing Body acknowledges that there is a certain amount of risk in all of the University College's activities and that it may not be possible or desirable to completely eliminate such risks. There are also opportunities to take measured risks, for example, in the area of innovation in curriculum and research, where there is a potential high risk of failure. The Governing Body must be assured that such 'opportunity' risks are carefully managed with robust controls and that where necessary, contingency arrangements are put in place.

The Board also acknowledges that project risk appetite may need to differ from the risk appetite applied to routine business and therefore this will be considered on a project by project basis. Risk appetite in these circumstances will also inform decisions by the Governing Body on whether to proceed with a project.

However, for routine business, the Governing Body will not tolerate any action or inaction that would seriously impact the achievement of objectives whether knowingly or unknowingly. Neither will the Governing Body tolerate any action or inaction that would have a negative impact on the good governance of the University College or any action or inaction that would bring the University College into disrepute. The University College is also risk averse in relation to legal and statutory compliance areas, for example in relation to the Health, Safety and Well-Being of staff and students and others who visit the Stranmillis Campus.

This policy is accompanied by a **Risk Management Strategy**, and a **Risk Register format** which has been approved by the Governing Body and which will be regularly assessed, reviewed and updated by the Governing Body.

Approved by the Governing Body on 13 June 2017

Risk Management Strategy

Definition of Risk

Risk is defined as: The uncertainty of outcome, whether positive opportunity or negative threat, of action, inaction, or events. Risk to the achievement of objectives will be assessed in respect of the combination of the likelihood of something happening, and the scale of potential impact.

Effective Risk Management:

- covers all risks, including governance, management, fraud, quality, reputational and financial, focusing on the most important risks;
- produces a balanced portfolio of risk exposure;
- is based on a clearly articulated policy and approach;
- requires regular monitoring and review, giving rise to action where appropriate;
- needs to be managed by an identified individual and involve the demonstrable commitment of Governors, Academics and other staff;
- is integrated into normal business processes and aligned to the strategic objectives of the Institution.

Benefits

The process of identifying risks and the introduction of internal controls to help mitigate such risks helps to support effective business planning, avoids excessive risk taking and helps to improve the Institution's ability to respond quickly and effectively to opportunities and threats in the internal and external environment. Risk Management is central to the achievement of objectives, whether at strategic, operational or project level.

Compliance and Reporting

Under the terms of the Financial Memorandum with the Department for the Economy (DfE), the University College must ensure that there are appropriate arrangements in

place to promote effective Risk Management, Control and Governance. This is a condition of the award of Grant.

The Code of Good Practice for Audit and Risk Assurance Committees sets out the minimum reporting requirements. Audit and Risk Assurance Committees must produce an Annual Report to the Governing Body, including an opinion on the adequacy and effectiveness of the system of Risk Management, Control and Governance.

The Accounts Direction from DfE also requires the University College to issue a Governance Statement as part of the audited financial statements. This statement must include an account of the Risk Management arrangements in place and how risk assessment and internal control is embedded in the Institution's operations.

Risk Management Principles

1 The University College will not commit to any new project or activity until a thorough and effective risk assessment has been carried out.

2. The University College will maintain an effective control framework, designed to contain risks where cost-effective to do so – and to manage risks effectively.

3. All staff in the University College will have commensurate responsibility for identifying and managing risk to the achievement of objectives.

4. The authority to take decisions involving risk will be commensurate with the level of risk – and will be clearly defined and communicated by management.

5. Major external risks or threats to the University College will be identified and monitored on a regular basis – and contingency plans made to effectively and proportionately respond in the event of such threats materialising.

6. Where appropriate, risks should be minimized by the securing of appropriate insurances or indemnity from third parties with whom the College is collaborating, including those with whom there is a contract to provide services.

7. As part of the assessment of risks, dates and timelines for review will be established and adhered to and there will be clearly identified Risk Owners.

8. Risk will be a standing item on the agenda of the Governing Body, its sub-committees and all Academic Governance Committees.

9. In keeping with the University College's wider policies, risk assessment will include wherever possible – consideration of the views of stakeholders.

Risk Management Process

The Risk Management process is aligned to the Planning Process because of the linkage to the achievement of objectives. All objectives, corporate or otherwise, including project objectives must be assessed by management for risk to the achievement of objectives.

A format for recording risks is attached at **Annex 1** and includes summary analysis formats as part of the presentation of risks. The Risk Register, follows the Risk Management process as described below, and has been designed with reference to the HM Treasury Orange Book - Management of Risk - Principles and Concepts.

Step 1: Identifying and Defining the Risk

Identifying risks is the first step in the process of building the University College's risk profile. This should be a continuous process, routinely generated through discussion with staff at Team/Committee meetings and when reviewing progress against business plans. Risks should be directly related to objectives, corporate or otherwise and a certain amount of horizon scanning may also be necessary to identify upcoming risks.

It is important that the essence of the risk is clearly articulated in a Risk Statement to ensure that the management of the risk is focused in the right area. The statement should be stated in terms of the cause of the risk and its impact and not simply the converse of the objective. An example risk statement is provided in **Annex 1.**

Step 2: Assessing the Inherent Risk

The inherent risk assessment is the level of risk before any controls have been put in place. It is important that this assessment is undertaken so that the University College knows what the exposure would be if controls were to fail. The inherent risk should be assessed in respect of the combination of the likelihood of something happening, and the impact if it does actually materialize. Guidance on assessing the level of inherent risk is attached at **Annex 2.**

Step 3: Controlling the Risk

This stage of the process is about identifying the controls that are currently in place to manage the risk. Such controls should give reasonable assurance of confining the risk within the Risk Appetite agreed by the Governing Body. The purpose of controls is normally to constrain the risk rather than to eliminate it.

Step 4: Assessing the Residual Risk

The residual risk assessment, takes account of the controls that are already in place to manage the risk. In the same way as the inherent risk assessment this assessment will consider the combination of the likelihood of something happening, and the impact if it does actually materialize.

Step 5: Considering What Further Actions are Necessary to Manage the Residual Risk

The adequacy of the controls can only be considered once the residual risk is identified. At this stage it is important to consider what further actions, if any can be taken, to manage the residual risk to an acceptable level. This should be viewed in the context of the risk appetite and tolerability levels decided by the Governing Body as set out in the Risk Policy. Specific details and target dates for implementing such actions and the name of the person responsible for taking this/these forward should be recorded on the Risk Register.

It should be noted that some risk is unavoidable and it is not within the College's ability to manage the risk to a tolerable level, in which case this should be clearly identified in the Risk Register. The need for contingency arrangements should also be considered in the event of the Risk materialising.

It should also be noted that some risks may not be the responsibility of the University College, in which case ownership for such risks should be transferred. Nevertheless, we will wish to seek assurance form the other party, for example in a contract situation that they have processes in place to manage those risks.

Terminating the risk will be a last resort. For example in a project management situation if it becomes clear that the project cost/benefit relationship is in jeopardy a decision may be taken to cease the project. This will be a matter for the Project Board and the Governing Body to consider.

Escalating Risks

All risks which, following a combined residual assessment scoring 12 or above on the Impact/Likelihood Matrix at **Annex 3**, should be brought to the attention of the Principal for consideration of escalation from Operational /Divisional Risk Registers to the Corporate Risk Register. Irrespective of whether the risk is escalated, the risk should remain on the Operational/Divisional Risk Register for continued monitoring and action as required.

Roles and Responsibilities

Audit and Risk Assurance Committee and the Governing Body

The Corporate Risk Register will be reviewed at all Audit and Risk Assurance Committee and Governing Body meetings throughout the year at which assurance will be sought that all necessary controls are in place and these are operating effectively and that, where appropriate further action is being taken in a timely manner to manage risks to an acceptable level. Similarly, the Education Committee, Finance and General Purposes Committee and HR and Remuneration Committee will consider the Operational/Divisional Risk Registers in relation to the key areas reporting to the respective Committees on a regular basis. A record will be contained within the Minutes.

The Principal and Directors

The Principal with the support of the Directors will be responsible for ensuring that the Risk Management Policy is implemented across the University College and that it is embedded and operating effectively. Discussion on Risks will feature on the Agenda of all Committees and will be recorded in the Minutes.

Directors with cross-cutting responsibilities, may decide to maintain a Directorate Risk Register rather than individual Risk Registers within their area of responsibility, to ensure proper oversight of risks across different areas, while ensuring that risks continue to be managed at the appropriate level.

Departmental Heads

All Departmental Heads will be responsible for engaging with their staff to identify, assess and review risks on a regular basis and to ensure that the Operational/Divisional Risk Registers are up-to-date and used to inform discussion. A record will be kept of these discussions.

They will also be responsible for reporting those risks to the Principal via the Director that may require entry to the Corporate Risk Register. An audit trail of discussions in relation to this will be maintained.

Internal Audit

Internal Audit will, as part of its programme of reviews, provide annual assurance to the Governing Body on Risk Management and its effective implementation. As part of the consultancy arrangements with Internal Audit, training for staff will be provided.

Corporate Governance Manager

The Corporate Governance Manager will provide ongoing support to Directors and Departmental Heads and guidance to staff in the University College in implementing these Risk Management arrangements. The Governance Manager will also facilitate reviews of the arrangements as required for the Governing Body.

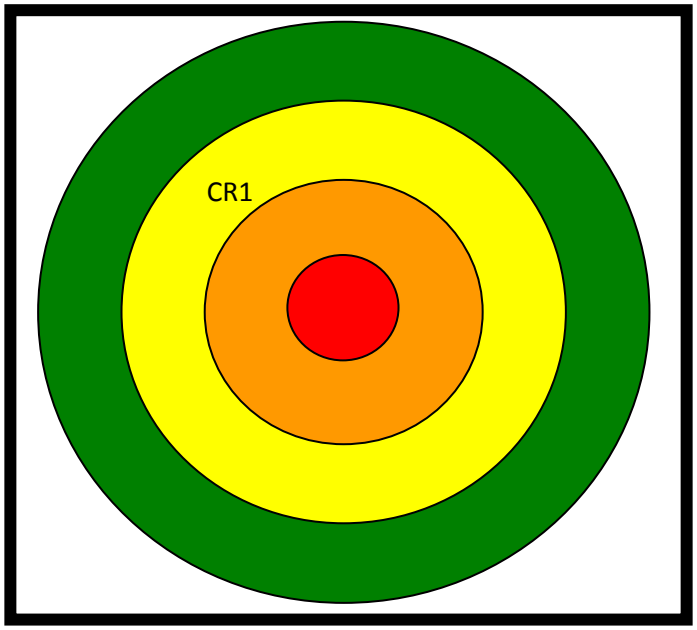
Annex 1

*Divisional/Corporate Risk Register

Risk Movement

LIKELIHOOD	IMPACT				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
5 Almost Certain	M (5)	H (10)	H (15)	E (20)	E (25)
4 Likely	M (4)	M (8)	H (12)	H (16)	E (20)
3 Possible	L (3)	M (6)	M (9)	H (12)	E (15)
2 Unlikely	L (2)	M (4)	M (6)	M (8)	H (10)
1 Rare	L (1)	L (2)	M (3)	M (4)	H (5)

Risk Assessment Matrix



QUARTERLY RISK SUMMARY

Worked Example

Risk No.	Summary	Inherent Assessment	Residual Assessment	In Quarter Change
R 1	Theft of intellectual property, including fabrication or plagiarism of research or scholarly work could lead to loss of data, publications, funding and reputation.	9	6	New Risk

Worked Example:

1	2	3	4		5	6		7	8
Risk No	**Objective(s)**	**Risk**	**Assessment** Inherent		**Controls in Place**	**Assessment** Residual		**Action Planned and Responsibility** **Target Date**	**Risk Owner**
			Impact	Likelihood		Impact	Likelihood		
R2	**Aim 2:** to produce research publications of world-leading and internationally excellent standard	Theft of intellectual property, including fabrication or plagiarism of research or scholarly work could lead to loss of data, publications, funding and reputation.	**3**	**3**	- Regulations Governing the Allegation and Investigation of Misconduct in Research - Code of Ethics in Research - Research Office - Data Protection Policy - Disciplinary Procedure - Regular review of Risk Register	**3**	**2**	• Policy Scoping Exercise • Training • Establishment of Working Group to develop policy and guidelines on Intellectual Property During 2017- 18 Dr N Purdy	**Dr N Purdy**

Sources of Assurance **Research and Scholarship Committee provides end of year assurance.**

Key points to Note

- It is important to keep Risk Registers up-to-date in order to reflect the current control environment and further management actions being taken to manage the risks to an acceptable level.

- Risks with an inherent score falling within the 'green zone' do not need to be included in the Risk Register.

- Risks with a residual score of zero should be removed from the Risk Register if management is content that such risks have been dealt with. If circumstances change, the risk may be included again in the Risk Register as appropriate.

- Do not confuse activities with the key controls that are in place to manage the risks. It is also important to include both preventative and reactive controls. Preventative *Controls* include any policy, procedure, practice, process, technology, technique, method, or device that modifies or manages risk. Reactive controls relate to contingency measures in the event of the risk materialising.

- Risk treatments or further actions being taken to manage the risk eventually become controls or modify existing controls, once they have been implemented.

- Where a target date is missed – the reason for slippage should be recorded.

- Sources of assurance relate to how you are informed/how you know that the controls that are in place are working effectively. Identification of assurance provision for key controls helps to reinforce management's responsibility for the design and operating effectiveness of controls within the University College – particularly in relation to identified risks thereby providing greater assurance to the Principal regarding the overall management of the specific risks.

Annex 2

Risk Type (with associated impact)

Impact	Impact on individual(s) – staff or public.	Statutory Duty.	Business / Operational	Buildings/ Engineering/ Environmental	Quality of Service	Finance
5 Catastrophic:	• Irreversible multiple injury or Death	• Multiple breach of statutory legislation and prosecution.	• Litigation > £500k expected. • National Media Interest • Severe loss of confidence and reputation	• Critical Environmental Impact. • Service closed for unacceptable period.	• Severe impact on customer satisfaction. • Gross failure to meet professional / national standards	• Significant financial impact (over 5% of total directorate budget) • Theft / loss >£250k
4 Major	• Major injury/ill health (reportable) • Major clinical intervention • Permanent incapacity	• Multiple breach of statutory legislation and improvement notice issued.	• Litigation >£250k to <£500k expected. • Adverse publicity • Impact on reputation	• Major/significant environmental impact • Severe disruption to service	• Major impact on customer satisfaction. • Failure to meet professional / national standards	• Major financial impact (between 2% - 5% of total directorate budget. • Theft / loss between £100k - £250k
3 Moderate	• Temporary Incapacity • Short term monitoring • Additional medical treatment up to 1 year • Extended hospital stay.	• Single breach of statutory legislation and Improvement Notice issued.	• Litigation >£50k - <£250k possible. • Potential for adverse publicity, avoidable with careful handling • Potential to impact on reputation.	• Moderate environmental impact • Moderate disruption to services	• Formal complaint expected. • Failure to meet internal standard	• Moderate financial impact (between 1% and 2% of total directorate budget) • Fraud/Theft / loss between £50k - £100k
2 Minor	• First Aid/ self-treatment • Minor injury • Minor ill health up to 1 month • Near miss (small cluster)	• Breach of statutory legislation.	• Litigation <£50k • Impact on reputation – internal awareness,	• Localised environmental impact • Disruption to service perceived as inconvenient	• Possible complaint. • Single failure to meet internal standard.	• Minor financial impact (up to 1% of total directorate budget) • Fraud/Theft / loss between £1k - £50k
1. Insignificant	• Near miss (single) • No adverse outcome • No injury or ill health	• Near breach of statutory legislation. • Minor breach of guidance or legislation.	• Possible litigation due to settlement is <£5k.	• Minimal impact to environment. • Minimal disruption.	• Customer initially unhappy. • Minor non-compliance with internal standard.	• Theft / loss up to £1k.

Likelihood Descriptor	**Probability /** Likelihood (of event or incident occurring over lifetime of Corporate Plan)
5 Almost Certain	The event is more likely than not to occur.
4 Likely	The event is likely to occur.
3 Possible	There is a reasonable chance of the event occurring.
2 Unlikely	There event is unlikely to occur.
1 Rare	The event will occur only in exceptional circumstances.

Annex 2

Prioritisation		
Colour	**Timescale for action**	**Timescale for review**
RED (Extreme)	Action immediately	Review within 1 month
AMBER (High)	Complete Action within 3 months where possible	Review within 3 months
YELLOW (Medium)	Complete Action within 6 months where possible	Review within 6 months
GREEN (Low)	Complete Action within 12 months where possible or accept risk	Review controls within period of corporate plan

Annex 3

LIKELIHOOD	IMPACT				
	Insignificant	Minor	Moderate	Major	Catastrophic
	1	2	3	4	5
5 Almost Certain	M (5)	H (10)	H (15)	E (20)	E (25)
4 Likely	M (4)	M (8)	H (12)	H (16)	E (20)
3 Possible	L (3)	M (6)	M (9)	H (12)	E (15)
2 Unlikely	L (2)	M (4)	M (6)	M (8)	H (10)
1 Rare	L (1)	L (2)	M (3)	M (4)	H (5)