St George's, University of London

Risk Management Policy
September 2018

1. Purpose of this Document

This risk management policy forms part of St George's, University of London (the "Institution") corporate governance arrangements. The purpose of this policy is to define the Institution's approach to risk management, outline the risk management process and reporting procedures and detail the roles and responsibilities of key individuals and committees.

A risk is a possible action or event that would affect an organisation's ability to meet its business objectives and deliver on its strategy. Risk Management is a systematic, structured approach to the continual identification, evaluation and management of these risks.

2. Benefits of Risk Management

Establishing and embedding effective risk management can bring the following benefits to an organisation:

- Regular reporting of major risks provide a clear picture of the organisation's weaknesses. This allows for action to be taken to improve the organisation's position and increase the likelihood of achieving the organisation's objectives.
- Ensuring a wide overview of issues promotes more effective prioritisation of resources and focus on significant issues.
- Regular consideration of risks minimises the likelihood of problems occurring that have not been planned for or mitigated against.

3. Risk Management Process and Procedure

3.1 The Risk Registers

The Institution holds a central "Strategic Risk Register" which holds the most significant risks to the Institution and the achievement of its business objectives. The strategic risk register comprises;

- the strategic risks summary table, (template in appendix 1)
- narrative tables on key changes, (template in appendix 2)
- each individual strategic risk, (Strategic Risk Template in appendix 3)
- a strategic risk summary matrix, (template in appendix 4)
- risk scoring and classification guidance (appendix 5)

The Strategic Risk Register is maintained by the Risk Management Co-ordinator (a member of Governance, Legal and Assurance Services, GLAS), however the individual risk owners are responsible for ensuring that their risks are accurately reflected in the register and kept up-to-date. The register is reported in full to Risk, Audit and Efficiency Committee (RAEC) on a quarterly basis for their review and approval, as well as being reported to Audit Committee and Council. The latest version of the Strategic Risk Register is also published on the SGUL portal to facilitate downward reporting of the strategic risks to all staff.

If there are significant changes to a risk between the quarterly reports to RAEC, the risk owner should update the record of their strategic risk and report this to the Risk Management Co-ordinator, who will report these changes in risk to the Executive Board if their immediate attention is required.

In addition to the Strategic Risk Register, there are "local" Management and Project Risk Registers which hold the local risks for each Institute, Directorate, Unit and Project. These registers are produced in a standardised table format (template in appendix 6) to ensure adequate monitoring and reporting of risks.

Any significant new activities or projects submitted to the Executive Board must have an accompanying risk register in order to be considered.

The individual Management and Project Risk Registers are owned and maintained by the relevant Head of Institute/ Professional Services Directorate/ Unit or Project Manager and it is their responsibility to ensure that the register is kept up-to-date. These registers are reported on a quarterly basis to the Risk Management Co-ordinator who provides a selection of these registers in full (pre-determined on a rotational basis) and a monitoring report on all the registers to each RAEC.

3.2 Risk Appetite

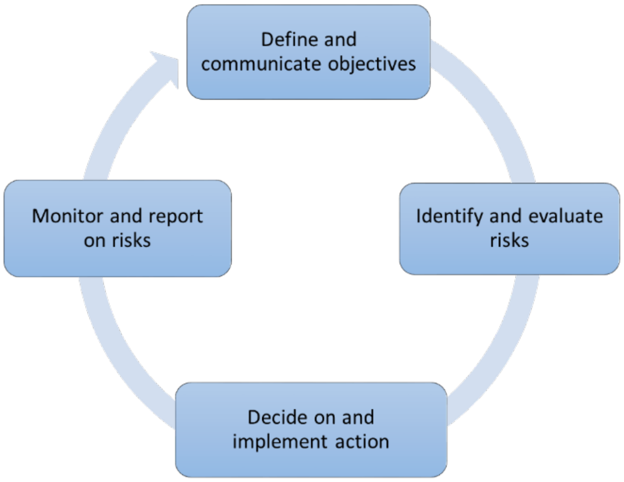
Risk appetite is the amount of risk that an organisation is willing to tolerate. The Institution's risk appetite varies across areas and context as it recognises that to achieve its objectives it is sometimes necessary to accept a degree of risk. Generally speaking:

- In areas of compliance, core business and values, the Institution is risk averse and seeks to minimise exposure to risks. This is described as having a "low" risk appetite.
- The Institution looks to responsibly support innovation and so for some activities or projects it is willing to tolerate some level of risk and is described as having a "medium" risk appetite.

For strategic risks, the risk appetite is agreed by RAEC and the strategic risk scoring and classification system guidance (appendix 5) is used to score with reference to the designated appetite. For risks on locally owned registers, it is expected that the risk owners will tolerate risks in line with the Institution's risk appetite, as described above.

3.3 Process

The Institution's risk management is coordinated by GLAS, namely by the appointed Risk Management Co-ordinator. The illustration below shows the fundamental risk management process which remains the same across the Institution's various Institutes, Professional Services Directorates, Units and Projects.


Define and communicate objectives
Identify and evaluate risks
Decide on and implement action
Monitor and report on risks

3.3.1 Define and communicate objectives

A risk is something that would hinder an organisation from meeting its objectives and so the Institution's risk management process is integrated with its strategic planning process. Objectives should be regularly reviewed (and if necessary, redefined) to ensure that they remain aligned to the Institution's overall objectives and are still appropriate.

3.3.2 Identify and evaluate risks

Once the objectives have been defined, the risks can be identified and there are a number of ways to do this. Involving people from across the Institution (for strategic objectives) or across the team (for local management/ project objectives) can help to give a broader and more representative identification of risks. The number of risks identified should be limited to enable them to be adequately monitored and reported on.

As a minimum, risks are evaluated according to their *likelihood* and *impact* and scored using the strategic risk scoring and classification system guidance (appendix 5). Strategic risks should be further evaluated, as per the guidance, in order to cover all fields of the Strategic Risk Template (appendix 3).

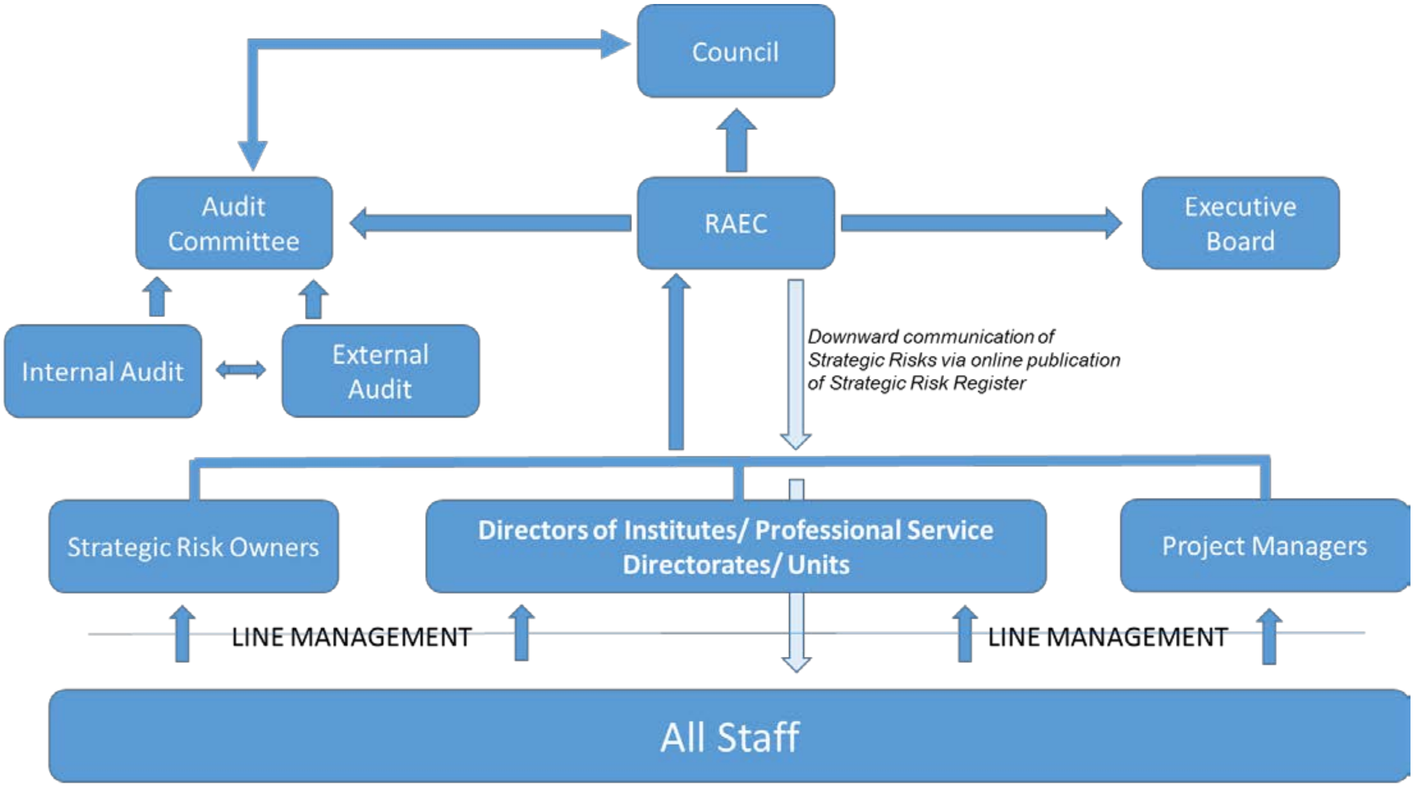
3.3.3 Decide on and implement action

The risk scores and evaluations will guide the decision on how much or which action should be taken in order to minimise the likelihood and/or impact of the risk. The risk's tolerability should be evaluated in reference to the risk appetite in order to further guide decision on action i.e. if a risk is outside of the risk appetite, more resource may be needed to implement mitigating action and bring the risk within tolerable range.

For any actions to be implemented, an individual should be named as responsible for this and a deadline should be established.

3.3.4 Monitor and report on risks

The risk registers are the key mechanisms in the monitoring and reporting of risks. Risks should be reported within these registers and the risk scoring and classification guidance (appendix 5) used to ensure that risk scores can be monitored over time and are comparable both across and within registers. The diagram below shows the communication flow of risk reporting across the Institution and the roles and responsibilities of individuals and groups in relation to the monitoring and reporting of risks are detailed after this, in section 4.


Council
Audit Committee
RAEC
Executive Board
Internal Audit
External Audit
Downward communication of Strategic Risks via online publication of Strategic Risk Register
Strategic Risk Owners
Directors of Institutes/ Professional Service Directorates/ Units
Project Managers
LINE MANAGEMENT
LINE MANAGEMENT
All Staff

4. Roles and Responsibilities

4.1 The Principal

The Principal has the ultimate responsibility for management of the Institution's risk.

4.2 Council

Council has responsibility for:

- Monitoring the management of significant risks to ensure that appropriate controls are in place
- Ensuring that less significant risks are actively managed
- Taking the Institution's risk profile and exposure in to account when considering major decisions
- Annually reviewing the Institution's approach to risk management

4.3 Audit Committee

Audit Committee is required to:

- Consider risk at each meeting by reviewing Strategic Risk Register and related reports presented by the Chair of the Risk, Audit and Efficiency Committee
- Satisfy itself that there are effective risk management procedures in place within the institution
- Raise any concerns it has over risk management and internal control with Council
- Approve a Strategic Audit Plan which is consistent with the Institution's Strategic Risk Register and establishes confidence in the risk management process

4.4 The Executive Board

The Executive Board has overall responsibility for:

- Ensuring the implementation of the Institution's risk management policy and processes
- Ensuring the appropriate availability and allocation of resource to support risk management

4.5 Risk Audit and Efficiency Committee (RAEC)

RAEC are responsible for:

- Implementing the Institution's risk management policy and processes and reviewing the Risk Management Policy on an annual basis
- Providing reports (from the Chair) for each Council and Audit Committee meeting and by exception, reporting risk matters to the Executive Board that require their immediate attention
- Ensuring the Strategic Risk Register is reviewed and maintained on a quarterly basis, reviewing and approving proposed changes to strategic risk scores as they occur.
- Reporting key changes to the Executive Board, for information
- Ensuring the current business of the institution is adequately represented in the local management and project risk registers and reviewing these in full on a rotational basis.
- Review and approval of SGUL's Whistleblowing and Public Interest policy on an annual basis.

4.6 Risk Management Coordinator

The risk management coordinator has responsibility for summarising and collating risk data and is clerk to the RAEC. This function lies with a member of the Governance, Legal and Assurance Service. The risk management coordinator is also responsible for the downward reporting and communication of risks, ensuring that the SGUL portal contains up-to-date versions of risk management documentation, including the strategic risk register.

4.6 Directors of Institutes/ Professional Service Directorates/ Units and Project Managers

These individuals have responsibilities to:

- Produce and maintain management and/ or project risk registers. These should be updated quarterly and this action confirmed to each RAEC meeting.
- Ensure that their area's objectives, and thus risk frameworks, are aligned to and informed by the objectives of the Institution as a whole.
- Report by exception to RAEC on any risks that hold a high residual risk score (20 or above).

4.7 Risk Owners

Individual risk owners have responsibility for:

- Ensuring that the record of their risk is kept up-to-date and that changes are passed on to; the Risk Management Co-ordinator for strategic risks; the management/ project risk register owner for local risks, in a timely fashion
- Ensuring implementation of the appropriate actions, controls and monitoring of their risk, including consideration at appropriate institutional committees and groups
- Exception reporting to RAEC when risks that require immediate attention arise
- Sponsoring good risk management practices within their Institute/ Directorate/ Unit/ Project

4.8 All Staff

All staff hold the shared responsibility of reporting identified risks that they do not perceive to be reflected in the relevant local risk register, or in the Institution's Strategic Risk Register. Staff should report these risks to their line managers in the first instance and, if the risk jeopardises the achievement of the Institution's business objectives, reported also to the Risk Management Coordinator for the attention of the RAEC.

4.9 Internal Audit

The Institution commissions a yearly internal audit to act as an impartial adviser on risk management, reporting on the adequacy and effectiveness of institutional risk management, control and governance arrangements.

4.10 External Audit

The Institution's external auditors provide feedback to the Audit Committee on the operation of the internal financial controls reviewed as part of the annual audit. They also look at the internal auditors report and are at liberty to request sight of the risk registers.

5. Whistleblowing

Whistleblowing scenarios can represent a big risk to individuals and organisations however it is not the same as risk management. It is the term used to describe when an individual raises concerns about an organisation's activities, usually to the organisation or their regulator. Activities that might typically raise concern are:

- a criminal offence
- someone's health and safety is in danger
- risk or actual damage to the environment
- a miscarriage of justice
- the company is breaking the law
- attempts to conceal any of the above

St George's "Whistleblowing and public interest disclosure Policy and Procedure" details how individuals can raise concerns for protection under the Public Interest and Disclosure Act 1998, and can be found on the SGUL Portal, under GLAS.

Appendix 1 – Strategic Risks Summary Table

Strategic Risks Summary Table (template)

L =	Likelihood
I =	Impact
RR =	Residual Risk
RA =	Risk Appetite
VRA =	Variance to RA

		01/02/2017	17/05/2017	18/09/2017	26/10/2017	08/02/2018	Current Scores 17/05/2018						
Risk	**Risk**	RR	RR	RR	RR	RR	L	I	RR	RA	VRA	Change in RR?	
1												⬇	Narrative 1
2													
3												⬆	Narrative 2
4													
5													
6													
7													
8													
9													
10													
11													
…													

Appendix 2 – Strategic Risks Narrative Table

Narrative Table (template)

<table>
<tr><td colspan="1"><b>Risk Area :</b> <i>(from strategic themes)</i></td><td><b>Risk ID:</b></td><td colspan="6"><b>Risk Owner/ Deputy:</b></td></tr>
<tr><td colspan="2" rowspan="3"><b>Risk: Risk 1</b>
<i>Here the risk should be described as succinctly as possible.</i></td><td rowspan="3"><b>Risk App.</b></td><td></td><td><b>L</b></td><td><b>I</b></td><td><b>RR</b></td><td><b>VRA</b></td></tr>
<tr><td><b>XPrevious DateX score</b></td><td></td><td></td><td></td><td></td></tr>
<tr><td><b>XCurrent DateX score</b></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="8"><b>Narrative on Change:</b>
<i>Insert Narrative Here e.g.</i>
<i>XYZ mitigating actions have reduced Likelihood to 1 from 5 due to A.</i>
<i>Impact has been reduced to 2 from 3 due to B.</i>
<i>The Residual Risk Score is now very low and comfortably within risk appetite. RMEC agreed that this should no longer be considered a strategic risk and should be removed from Principal Strategic Risk Register going forwards.</i>
<i>See minutes of RMEC meeting XXXX</i></td></tr>
</table>

Appendix 3 – Strategic Risk Template

Strategic Risk (template)

<table>
<tr><td><b>Risk Area :</b> <i>(from strategic themes)</i></td><td><b>Risk ID:</b></td><td colspan="6"><b>Risk Owner/ Deputy:</b></td></tr>
<tr><td colspan="2" rowspan="4"><b>Risk:</b>
<i>Here the risk should be described as succinctly as possible.</i></td><td rowspan="4"><b>Risk App.</b></td><td></td><td><b>L</b></td><td><b>I</b></td><td><b>RR</b></td><td><b>VRA</b></td></tr>
<tr><td><b>Pre- mitigation score</b></td><td></td><td></td><td></td><td></td></tr>
<tr><td><b>Post- mitigation score</b></td><td></td><td></td><td></td><td></td></tr>
<tr><td><b>Target score</b></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2"><b>Causes:</b>
<i>Possible causes or contributors to the risk occurring should be listed here, but the list should be limited to those most likely as multiple causes will inhibit the targeting of actions</i></td><td colspan="6"><b>Consequence:</b>
<i>Detail what the consequence would be if the risk occurred.</i>
<i>Consider the knock-on consequences for other departments.</i></td></tr>
<tr><td colspan="2"><b><u>Mitigating Action:</u></b>
<i>Outline current or upcoming activity that will mitigate this risk</i></td><td colspan="6"><b><u>Effect:</u> Prevention, Impact Reduction or detection?</b>
<i>Detail the desired effect of this action</i>
<i>Prevention – reduce the likelihood of risk or consequence</i>
<i>Impact reduction – reduce negative effect of consequence</i>
<i>Detection – mechanism to provide early warning or timely detection resulting in additional time for response.</i></td></tr>
<tr><td colspan="3" rowspan="3"><b>Activity/ Outcome Trail</b>
<i>Bullet point key activities or actions from the last 6 months</i></td><td><b>Council KPI</b></td><td colspan="4"><b>Target</b></td></tr>
<tr><td><i>KPI #</i></td><td colspan="4"><i>KPI Target</i></td></tr>
<tr><td colspan="2"><i>Last reported Status (RAG)</i></td><td colspan="3"><i>Current Status (RAG)</i></td></tr>
<tr><td><b>Internal Accountable Group:</b> <i>give monitoring Board/ committee accountable for this risk</i></td><td colspan="7"><b>External Monitoring:</b> <i>list monitoring / regulatory body</i></td></tr>
<tr><td colspan="8"><b>Index Tags:</b> list related words from the index</td></tr>
</table>

Appendix 4 – Strategic Risk Summary Matrix

Strategic Risk Summary Matrix

Likelihood (L)
1 = Very Unlikely
2 = Unlikely
3 = Possible
4 = Likely
5 = Very Likely

X

Impact (I)
1 = Insignificant
2 = Small and local
3 = Will disrupt some of the Institution
4 = Will disrupt all of the Institution
5 = Serious imminent crisis

= Residual Risk (RR)

RR score	Level of Risk
1 - 6	🟩 Low Risk
7 - 12	🟨 Medium Low Risk
13 - 19	🟧 Medium High Risk
20 - 25	🟥 High Risk

The below matrix plots all of St George's Strategic Risks, as according to their current "pre-mitigation" risk scores.

Likelihood					
5	🟩	🟨	🟧	🟥	🟥
4	🟩	🟨	🟨	🟧	🟥
3	🟩	🟩	🟨	🟨	🟧
2	🟩	🟩	🟩	🟨	🟨
1	🟩	🟩	🟩	🟩	🟩
	1	2	3	4	5

Impact

Appendix 5 – Risk Scoring and Guidance

Risk Scoring and Guidance

Each identified risk is scored and classified as follows:

Likelihood (L)
1 = Very Unlikely
2 = Unlikely
3 = Possible
4 = Likely
5 = Very Likely

X

Impact (I)
1 = Insignificant
2 = Small and local
3 = Will disrupt some of the Institution
4 = Will disrupt all of the Institution
5 = Serious imminent crisis

= Residual Risk (RR)

RR score	Level of Risk
1 - 6	Low Risk
7 - 12	Medium Low Risk
13 - 19	Medium High Risk
20 - 25	High Risk

For each identified risk, a Risk Appetite is established. The Risk Appetite is the level of Residual Risk (RR) that St George's is willing to accept for each identified risk.

Acceptable level of Residual Risk	Risk Appetite
1 – 8	Low
9 - 16	Medium
17 - 25	High

The Variance to Risk Appetite (VRA) is calculated for Strategic Risks and this indicates the variance between what the Residual Risk score is, and what the Risk Appetite permits as an acceptable Residual Risk score. Risk owners should work to ensure that the Residual Risk score for their identified risk is within (or below) the acceptable level as per the Risk Appetite. The VRA score is then rated as red, amber or green to indicate attainment of this.

The VRA score is calculated and rated as below:

	Calculation
For Low risk appetite items	VRA = Residual Risk score - 8
For Medium risk appetite items	VRA = Residual Risk score - 16
For High risk appetite items	VRA = Residual Risk score - 25

VRA	Rating
0 or below	Green
1 - 4	Amber
5 +	Red

For each Strategic Risk, the Likelihood, Impact, Residual Risk and Variance to Risk Appetite scores are calculated for pre-mitigation (the current level of risk), post mitigation (the theorised level of risk after mitigating actions have been put in place), and the target score given (the level of risk that the owner aspires to ultimately achieve) . The risk appetite remains the same.

Appendix 6 – Local Risk Register (template)

XXX Management Risk Register		Last Updated:	
Owned by:		Version Number:	
Internal Monitoring Group:			

Each identified risk is scored and classified as follows:

Likelihood (L)	X	Impact (I)
1 = Very Unlikely		1 = Insignificant
2 = Unlikely		2 = Small and local
3 = Possible		3 = Will disrupt some of the Institution
4 = Likely		4 = Will disrupt all of the Institution
5 = Very Likely		5 = Serious imminent crisis

= Residual Risk

RR Score	Level of Risk
1-6	Low Risk
7-12	Medium Low Risk
13-19	Medium High Risk
20-25	High Risk

Any risk with a Residual Risk score of 20 or above must be reported to the Risk Management Coordinator for referral to the Executive Board.

No.	Key Risks	Early Warning Mechanisms	Current Mitigating Actions	L	I	RR	Planned Further Improvement Actions	Responsible person