Operational Risk Management Procedure

Responsible Officer:	SVP - Operations
Responsible Office:	Business Resilience
Related Procedures:	Enterprise Risk Management Procedure
	Procurement procedures
	Business Continuity procedures
Related College Policies:	Risk Management Policy
	Business Continuity Policy
Effective Date:	9 February 2023
Supersedes:	Not applicable
Next Review:	February 2026

I. Purpose & Scope

The purpose of this procedure is to provide a framework for the management and monitoring of operational risk within the university. This procedure should be read in conjunction with the Integrated Risk Management Policy and forms part of the overall Integrated Risk Management Framework for King's.

Ensuring that all risks that may impact the operations of the university are captured, understood and effectively mitigated in order to minimize disruption to the core business of teaching and research is the responsibility of all staff who engage in the management of operations within the university. This also extends to ensuring that services and operations delivered or conducted by third parties have an effective risk management policy, to reduce the risk to university operations.

II. Definitions

Risk management – co-ordinated activities, systems and processes for managing risk in the context of the university's vision, strategy, objectives and targets.

Issue – something that has happened or is happening.

Risk – in accordance with the ISO31000 (2018) definition, King's College London defines risk as the potential "effect of uncertainty on objectives", where an effect is a deviation from an intended or expected outcome.

Integrated Risk Management Framework – a framework which articulates the whole system by which the university manages risk.

- The Framework encompasses this Risk Management Policy, a number of procedures on the process and responsibilities for managing the various types of risk across the university, our enterprise risk register and risk appetite statement.
- The integrated risk management considers 'top down' strategic risk, 'bottom up' operational, partnership, project and programme and other risks and the capture and monitoring of emerging risks

Enterprise Risk – risks that are institutionally significant and relate to the achievement of the ambitions of the university.

- These risks may emerge from both external and internal influences:
    - External influences are those which occur outside of the organisation but have a direct impact on university business.

- Internal influences are a combination of business planning round and operational risks, where the combination of such threats would significantly impact the financial, legal and/or reputation standing of the university.

Strategic Risk – risks to being able to deliver the strategic objectives set out in our current Vision and Strategy. By their nature strategic risks are institutionally significant and therefore are also captured in the Enterprise Risk Register. The Integrated Risk Management Framework uses the term 'strategic' risk, however 'corporate' risk is occasionally used synonymously in the organisation.

Partnership Risk – risks that arise from partnership activity.

Operational Risk – risks relating to delivery of the core operations of the university. Core operations are those operations, procedures and processes that support the delivery of teaching and research.

Project & Programme risk - risks relating to projects and programmes.

Emerging Risk – potential risks that do not yet pose a clear threat to the institution but should be closely monitored. Emerging risks are captured and monitored through external horizon scanning, risk review points, and via the Integrated Planning Process.

Risk Appetite – the level of risk that the university is willing to tolerate or accept in the pursuit of its strategic aims. When considering threats, risk appetite defines the acceptable level of exposure deemed tolerable or justifiable by the institution; when considering opportunities, risk appetite defines how much the university is prepared to actively put at risk in order to realise the potential or expected benefits.

Risk Owner – the risk owner is the person(s) *accountable* for the effective management of risk – both monitoring any changes on likelihood and impact, and initiating, adapting and overseeing mitigating actions as appropriate.

Risk Manager – the risk manager is the person(s) who is *responsible* for the effective management of a risk.

Key Operational Risks – a risk that if realised will disrupt the service or processes that are essential for delivering an excellent student and staff experience or significantly impact financial or business operations.

Issue Management – where a risk has been realised and is currently happening (impacting the university), it is an issue and needs further mitigations to reduce the threat to the organisation. It is no longer a risk when it has been dealt with and the level of impact to the university is within its risk tolerance as defined in the local and overarching risk appetite statements.

III. Roles and Responsibilities

College Council

- As the university's governing body, Council has the ultimate responsibility for the Integrated Risk Management Framework and the management of risk at the university.
- Council delegates the responsibility for ensuring that the university is complying with its policy on risk management to the Audit, Risk and Compliance Committee.
- The President & Principal is responsible on behalf of the Council for ensuring that integrated risk management is undertaken effectively across King's and in accordance with the policy.
- The University Executive supports the President & Principal with this and acts as the main risk management committee of the University.
- On-going risk management forms part of the day-to-day operational resilience planning and service delivery in faculties, directorates and business units and is the responsibility of the relevant Executive Dean/Head of Directorate/Programme Manager.

The Audit, Risk and Compliance Committee (ARCC)

- The Audit, Risk and Compliance Committee (ARCC), a sub-committee of Council, is responsible for regularly assessing the effectiveness of the Integrated Risk Management Framework, along with its constituent parts, and advising Council accordingly.
- The ARCC may also monitor the management of significant and/or complex enterprise risks to provide assurance to itself and Council that unwelcome consequences are effectively managed.

President and Principal

- The President and Principal is accountable to Council for the Integrated Risk Management Framework.

University Executive

- The University Executive, chaired by the President &Principal, acts as the university's Risk Management Committee, and oversees the day-to-day management of enterprise risks across the university ensuring that the Integrated Risk Management Framework is fit for purpose and applied
- Individual members of University Executive are responsible for the management of individual enterprise level risks (they are the Risk Owners).
- University Executive will be supported in the management of particular risk categories (e.g., partnership, project & programme) by relevant advisory committees

Senior Vice President (Operations)

- The Senior Vice President (Operations) is responsible to the President and Principal for the effective implementation and operation of the Integrated Risk Management Framework.
- The Director of Business Resilience is responsible to the Senior Vice President (Operations) for the ensuring the framework <u>operational risk management</u> is in place, effectively implemented and reported on through agreed channels on a regular basis.

Senior Leaders

- Senior Leaders (including those leading Academic Faculties and Departments, Institutes and Professional Service Directorates) are responsible for the management of strategic and operational risks in their areas of responsibility. They are accountable for the effective management of risk in their areas of responsibility, for reporting new risks, and substantial changes to known risks to the University Executive through either the Senior Leadership Forum, individual members of the University Executive and/or business plan submissions and in-year reviews.

Local Operational teams

- Senior Leaders should ensure that they have sufficient local resources in place to support operational risk management. There should be a role holder who is responsible to the Senior Leader for managing the process and reporting any concerns or areas for development.

Business Assurance Team

- Business Assurance are responsible for working with the ARCC, Senior Vice Principal (Operations) and the Director of Strategy, Planning and Analytics to ensure the Integrated Risk Management Framework is fit for purpose as well as undertaking regular reviews relating to risk management on behalf of Council and ARCC for assurance and continuous improvement purposes.

- The university's internal audit function will use local risk registers alongside copies of processes and procedures to formally provide assurance on the university's arrangements for risk management, control and governance, Value for Money and the production of data for public bodies.

III. Procedure

Identifying Operational Risks

The responsibility for managing and mitigating operational risks sits with the operation or service owner. All key risks should be captured in a local risk register using the university format available Here

All services should have one business owner, who is also the risk owner. Risk mitigations may be distributed across a number of teams. Where there is disagreement on the risk owner, this should be escalated to the Business Resilience team in the first instance for clarification.

Teams should identify key activities and procedures as they relate to the operational risks of the university. This may also include projects or third-party contracts which are delivering an aspect of the operational risk universe i.e., delivery of a new suite of labs. Teams can make use of the Business Impact Analysis process to identify key activities and processes as the basis for identifying the risks. Click Here for link to BIA Document

Risks v. Issues

Where a risk is realised and is impacting the operations of the organisation to the extent that it is impacting the effective and efficient operations of the university is should be treated as an issue and be dealt with in a timely fashion in line with BAU Operations. Once the issues has been managed and the threat reduced, the risk should be revised on the risk registers, if the risk is still a potential threat.

Operational risks can be considered under the following headings.

- **Risks relating to people** (e.g. Loss of key staff, workplace health and wellbeing, employment practices)
- **Risks to processes** (e.g. human error, lack of written processes, Fraud, loss of third party provider, supply chain)
- **Risks to premises** (e.g. Loss of premises due to internal or external influences, lack of appropriate premises to deliver the core activities, failure of maintenance standards)
- **Risks to systems** (e.g. IT system failure, blackouts, power loss)
- **Risks relating to compliance or regulatory activities** (e.g. failure to meet H&S workplace safety, failure to report to external bodies, statutory data reporting)

Risk Relating to People

All organisations are vulnerable when staff levels are inadequate in either number or quality. The success of organisations can usually be ascribed not only to the quality of senior management, but the effectiveness of procedures put in place for recruiting, training, supporting and retaining good staff.

In assessing how well King's manages operational risks relating to people, the following should be considered:

- What is the staff turnover rate (rate of leavers per staff complement per annum) and how does it compare with the organisation's peer group? (information available from HR)
- What is the rate of absenteeism and how does it compare with the peer group? (information available from HR)
- What procedures does the organisation have for the induction of new staff and for training staff and what is the completion rate?
- What percentage of staff positions is vacant and how does this compare with the peer group?
- Is there a succession plan in place for all key staff?

High staff turnover, high absenteeism, weak training and development processes, high levels of staff vacancies and vulnerability to the departure of key staff will impact the operations of the university. Understanding where risks relating to people can be treated to improve the operational resilience of the team is key to reducing risk.

Risk Relating to Process

To deliver high quality teaching and research, the underpinning processes must be effective, efficient and appropriate. In assessing risks to process effectiveness, the following should be considered:

- Are all the key processes used by your business unit written down and made available to staff?
- Are all the processes understood and implement consistently across teams?
- Do all the processes have a clear process owner? if the process has a number of contributors cross college, is that understood and do all teams work effectively together to achieve the process outcome?
- Does the process get reviewed regularly and does it have performance targets to monitor effectiveness?

Poorly understood processes without a clear owner directly impacts the delivery of core operations. When considering core processes, it may be helpful to review the Service Excellence Standards for the processes in your area.

Risks relating to Premises

Risks relating to the university's overall plans for the development of the Estate in line with Vision 2029 are captured in the Corporate Risk Register. These risks, if realised would significantly inhibit Kings' ability to delivery world leading teaching and research, causing financial and reputational damage. In terms of operational risk in relation to premises, the following should be considered:

- Are the current premises fit for purpose for the delivery of the core activities?
- Are existing spaces being always used efficiently (i.e. at full or near full capacity?)
- Where space is limited, are WoW principled being applied or could be applied to ensure space is used efficiently

Space should be fit for the purpose that takes place within those spaces and must be used effectively in order to support the core activities. Unused or under-used spaces and those that do not meet legal or structural requirements to delivery the core activities will negatively impact operations.

Risks relating to Systems

Failure of systems will interrupt business activity and can result in large costs being incurred. In assessing the exposure to operational risk arising from inadequate systems, the following should be considered:

- How often are systems out of operation (or 'down')?
- What proportion of activities is supported by existing systems? Is there a high proportion of manual 'work arounds' – for example, analysis and record keeping using 'homemade' spreadsheets?
- What back-ups exist for existing systems?
- Are all new systems thoroughly tested and run on a parallel basis with existing systems during their launch period?

Systems that are unreliable or require a number of manual workarounds either because of system unreliability or system operational complexity, or time available v. system input demands, effect the delivery of the core activities, often causing additional work and pressures to local teams. Poor systems also impact the quality of data available for planning and delivery of core activities.

Risks relating to compliance or regulatory activities

The university is a regulated organisation requiring compliance in a wide range of activities in to maintain approval and deliver safe and innovative teaching and research. Operations that are carried out, that do not meet the regulatory requires will impact research, teaching, the financial and reputational standing of the university. When considering the risks posed through failure to meet and monitor regulatory or compliance requirements, the following should be considered:

- Are the regulatory requirements understood and embedded in current operational practice?
- Are those engaged with the regulated activities or activities requiring compliance standards trained and a record kept and monitored?
- Are the spaces where regulated or standards of compliance are required maintained and monitored to ensure standards are sustained?
- How often have standards not been met/regulatory breaches?

Ensuring that the university is able to meet and maintain is regulatory requirements and compliance standards allows the university to delivery high quality research derived teaching. The loss of licences and operations due to breaches in regulation significantly damage the university's ability of operate.

Appendix A illustrates the core activities of the university. Faculties and Directorates should consider how their operations and services contribute to the delivery of the overall mission under the areas outlined in the chart, and any risks to the underpinning processes and procedures that may negatively impact operations. When identifying operational risks, faculties should consider any locally owned operations that may impact their delivery of business plans, staff and student experience and research outputs. Where the faculties rely on activities that are owned by Directorates, they should be sighted on risks and mitigations to reduce the impact on faculty delivery. (see section on Risk Reporting).

Directorates should refer to the Service Excellence Catalogue to ensure that risks relating to their core operations are clearly articulated and effectively mitigated to reduce any negative impact to the KPI's set within that framework in support of "Simple, Nimble and Effective". Additionally, Directorates will have locally owned activities that may not be reflected in the Service Excellence framework, but should be included in local registers where threats to those activities would impact downstream processes and outcomes.

Project and Portfolio Risks

The Portfolio Director, through the King's Portfolio Office (KPO), maintains a core set of project and programme information (the Enterprise Portfolio) on key university initiatives either planned or in train across portfolio's such as E&F, IT, SED, HR, Finance, RMID and SPA. Projects are categorised as:

- Develop and Transform
- Replacement and Continuity
- Compliance and Regulation

Projects are also flagged as to whether they directly contribute to delivering our Strategy 2026 objectives.

Enterprise Portfolio projects

These are projects that support the Strategic Vision for the University in continuing to be a world leader in Research and Education. These projects will improve the Student Experience, Research Capacity and Quality and deliver substantial Estates developments. These projects carry significant risks for the university in terms of Financial, Reputational and National/International standing and are overseen by the Senior Leadership of the University with significant budget and staff time commitments over an extended period. Risk Management for these projects is overseen by the King's Portfolio Office. Active risk management remains the responsibility of the individual project boards to monitor and actively mitigate.

BAU Projects/ Operational Projects

These are projects that renew, improve or replace existing processes, systems or spaces are part of the ongoing maintenance and updating of the university operating model. Whilst these projects may carry some financial or reputational risks, with budget implications to a lesser extent than a Enterprise Portfolio project, they are lead and managed by a Faculty or Directorate Lead, who takes responsibility as the project sponsor. Risks relating to these projects should be reported into the Faculty/Directorate of the Project Sponsor and be reported alongside all other operational risks in their area.

For the purpose of this process, projects considered BAU should follow this operational risk management process. If you are unclear as to whether a project is BAU or under the King's Portfolio Office, please contact the Director of Business Resilience in the first instance.

Collating and evaluating risks

- Identified risks should be framed in the form of "Failure to…….caused by……leading to"
- The likelihood and impact should then be scored using the university's risk template which can be found as a tab in the risk register template. This is the Initial Risk Rating. Assistance in determining this rating, please refer to the impact table following this link
- Each Faculty/Directorate/ Business Unit should have a Risk Appetite Statement in relation to the delivery of their main activities. A risk appetite statement is a measure of how much risk can be accepted in order to ensure effective delivery of an activity to the required standards and/or allow opportunities for development that leads to further improvement. The Operational Risk Appetite Framework is in Appendix C
- Compare the initial risk rating to the risk appetite score. If the risk rating is higher than the risk appetite, then action needs to be agreed to mitigate the likelihood and/or the impact. Mitigations that are already in place should be considered and the residual risk rating calculated. If the residual risk is still higher than the risk appetite further action is required. [Examples are included in Appendix D]

- Where a process is shared between more than one Directorate or Faculty, teams should work together to clearly identify the risks and agree appropriate mitigations, with clear mitigation owners and timelines for completion.
- If Teams decide to use one risk register to collate both Project Risk, Business Planning Risks and operational Risks, these should be allocated a grading. T2 for Business Planning Risks and T3 for Operational and BAU Project Risks.

Risk Treatment

When considering risk mitigations, there are four accepted approaches to reduce risk.

a. **Treat** – take action to reduce *either* the probability of the risk occurring *or* the severity of the impact were it to occur.

b. **Tolerate** – accept the risk and do not attempt to reduce it. This response is appropriate when the risk score is below the risk appetite, or occasionally when the risk is above the appetite but the costs of treating it outweigh the potential benefits.

c. **Transfer** – transfer the risk to a third party, e.g. through insurance.

d. **Terminate** – eliminate the risk, e.g. by changing the objective or the approach being taken to achieve it, or by abandoning the objective entirely.

The risk profile can change and therefore the risk treatment may need to be amended to ensure the risk remains within the risk appetite.

Risk Reporting

Operational risks should be discussed and monitored on a regular basis at local level and decisions around risk management and mitigation should be recorded. Updates to the risk registers following those meetings, should be updated into the Power BI dashboard on a quarterly basis, which will be shared with SVP Ops and SOG for review as part of the process of ensuring service excellence.

Business Unit leaders should also report any significant changes to the SVP Operations as part of their normal management processes.

Risk Escalation

Where a risk is identified as having the potential to significantly impact the operations of the university or pose a threat to its Financial or reputational position, risks must be escalated for review

Faculties should escalate operational risks in the first instance to the DVP – Operations. Directorates should escalate operational risks to the SVP – Operations. Project risks should be escalated to the Portfolio Director. Equally, ongoing significant issues should also be reported through the same escalation process. See Appendix B

Risk Escalation - Project Risks.

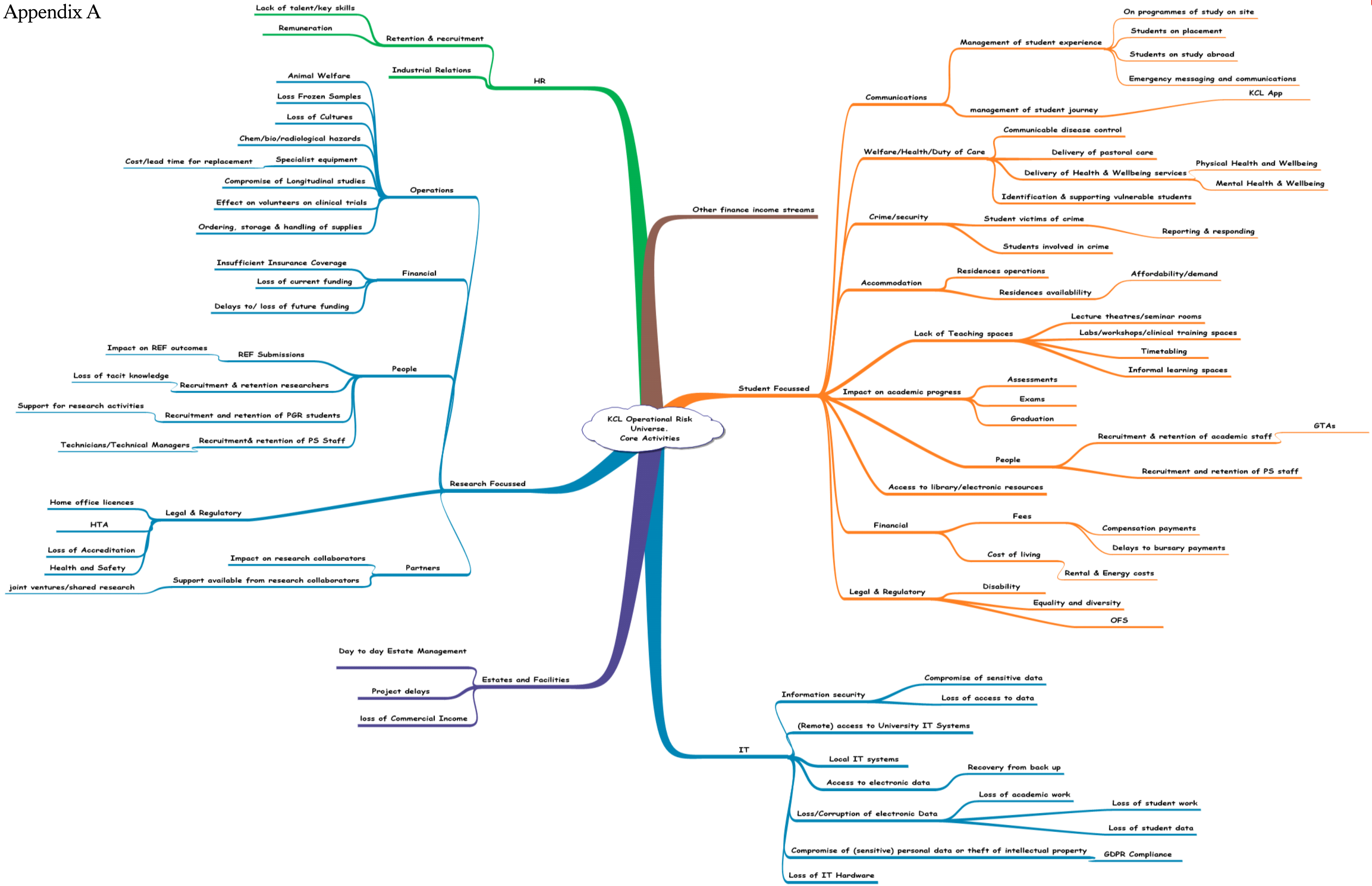
The King's Portfolio Office will track changes in risk profile. In addition, if the risk profile of a project increases either during the pre-project planning or whilst the project is in flight, this should be escalated directly by the Project Sponsor to the King's Portfolio Office for review. If the Portfolio Director considers the risks relating to the project have increased and may significantly impact the financial or reputational standing of the university, the project may be referred to the Portfolio Oversight and Benefits Assurance Sub-Committee (PSC) for detailed discussion on recovery plans. Otherwise, BAU/ Operational Projects risks will be reported alongside Operational Risks as part of this process.

Business continuity

Risks to key operations should have a continuity plan in place in the event the risk is realised at a key point in the academic year, to reduce the impact to the university and return it to normal operations as soon as possible. Information on Business Impact Analysis and Business Continuity Planning can be found here.

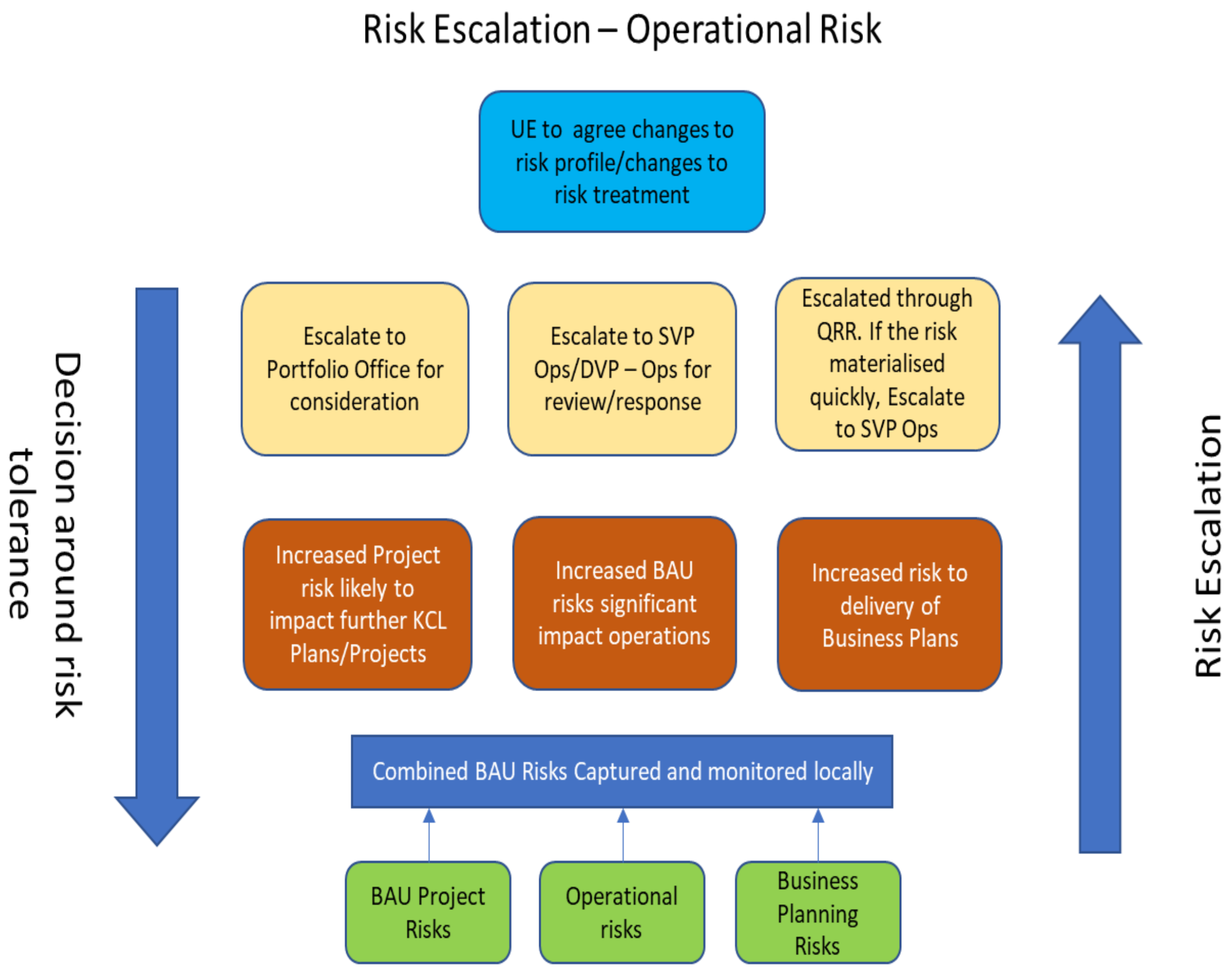
Version V1.1 21/09/22 S.Rowe

Appendix A



KCL Operational Risk Universe. Core Activities
HR
Retention & recruitment
Lack of talent/key skills
Remuneration
Industrial Relations
Other finance income streams
Research Focussed
Operations
Animal Welfare
Loss Frozen Samples
Loss of Cultures
Chem/bio/radiological hazards
Specialist equipment
Cost/lead time for replacement
Compromise of Longitudinal studies
Effect on volunteers on clinical trials
Ordering, storage & handling of supplies
Financial
Insufficient Insurance Coverage
Loss of current funding
Delays to/ loss of future funding
People
REF Submissions
Impact on REF outcomes
Recruitment & retention researchers
Loss of tacit knowledge
Recruitment and retention of PGR students
Support for research activities
Recruitment& retention of PS Staff
Technicians/Technical Managers
Legal & Regulatory
Home office licences
HTA
Loss of Accreditation
Health and Safety
Partners
Impact on research collaborators
Support available from research collaborators
joint ventures/shared research
Estates and Facilities
Day to day Estate Management
Project delays
loss of Commercial Income
Student Focussed
Communications
Management of student experience
On programmes of study on site
Students on placement
Students on study abroad
Emergency messaging and communications
management of student journey
KCL App
Welfare/Health/Duty of Care
Communicable disease control
Delivery of pastoral care
Delivery of Health & Wellbeing services
Physical Health and Wellbeing
Mental Health & Wellbeing
Identification & supporting vulnerable students
Crime/security
Student victims of crime
Reporting & responding
Students involved in crime
Accommodation
Residences operations
Residences availablility
Affordability/demand
Lack of Teaching spaces
Lecture theatres/seminar rooms
Labs/workshops/clinical training spaces
Timetabling
Informal learning spaces
Impact on academic progress
Assessments
Exams
Graduation
People
Recruitment & retention of academic staff
GTAs
Recruitment and retention of PS staff
Access to library/electronic resources
Financial
Fees
Compensation payments
Delays to bursary payments
Cost of living
Rental & Energy costs
Legal & Regulatory
Disability
Equality and diversity
OFS
IT
Information security
Compromise of sensitive data
Loss of access to data
(Remote) access to University IT Systems
Local IT systems
Access to electronic data
Recovery from back up
Loss/Corruption of electronic Data
Loss of academic work
Loss of student work
Loss of student data
Compromise of (sensitive) personal data or theft of intellectual property
GDPR Compliance
Loss of IT Hardware

Appendix B



Risk Escalation – Operational Risk
UE to agree changes to risk profile/changes to risk treatment
Escalate to Portfolio Office for consideration
Escalate to SVP Ops/DVP – Ops for review/response
Escalated through QRR. If the risk materialised quickly, Escalate to SVP Ops
Increased Project risk likely to impact further KCL Plans/Projects
Increased BAU risks significant impact operations
Increased risk to delivery of Business Plans
Combined BAU Risks Captured and monitored locally
BAU Project Risks
Operational risks
Business Planning Risks
Decision around risk tolerance
Risk Escalation

Appendix C

Operational Risk Appetite Framework		Date: October 2022	Review Date: Jan 2024			
Appetite	**Definition**	**Financial Risks**	**Service Delivery**	**Compliance**	**Systems/Technology**	**BAU Projects**
Avoid	Avoidance of risk and uncertainty in achievement of key deliverables or initiatives is key objective. Activities undertaken will only be those considered to carry virtually no inherent risk.	Our operations will avoid any risk to income and expenditure in line with planning round agreements. Recurrent expenditure on core activities continues unchallenged to protect exiting activities. Only willing to accept low cost options. New market opportunities not pursued	We will aim to maintain or protect existing processes and services rather than create or innovate new processes that may add risk to existing arrangements. Activities only undertaken with existing levels of staff capacity and capability	We will avoids anything which could be challenged, even unsuccessfully. There is no appetite for any breaches of external regulations	General avoidance of systems/technology developments and rollout. We would avoid changing existing processes and systems that may impact current operations	Avoidance of any new projects that may negatively impact the existing operations of the university.
Cautious	Preference for very safe business delivery options that have a low degree of inherent risk with the potential for benefit/return not a key driver. Activities will only be undertaken where they have a low degree of inherent risk.	Value for Money(VfM) is a primary concern. Limited willingness to challenge recurrent expenditure on existing activities. Resources generally restricted to core activities. Investment in strategic change is limited to clearly defined opportunities with minimal exposure to risk	Innovations in approaches to supporting the delivery of teaching, student support and research are avoided unless essential. Ongoing development of existing staff	Compliance is key, however where it is necessary to make a short term change to the processes that underpin compliance requirements, this may be undertaking, but the owner has to be very sure KCL would win any challenge. Prefer to avoid any action that could result in a regulatory challenge	We are only making essential changes to systems/technology to protect current operations.	Project outcomes require little or no organisational change and the organisation is prepared and equipped for the change. The project has a high confidence of success with a low inherent risk profile.
Moderate	Preference for safe options that have low degree of inherent risk and only limited potential for benefit. Willing to tolerate a degree of risk in selecting which activities to undertake to achieve key deliverables or initiatives, where we have identified scope to achieve significant benefit and/or realise an opportunity. Activities undertaken may carry a high degree of inherent risk that is deemed controllable to a large extent.	VfM and maintenance of core services still the priority but willing to consider the benefits of redistribution of resourcing. Prepared to pursue opportunities with the possibility of some limited financial loss, where the expected outcome would improve the student experience	There is a preference to stick to the status quo in terms of service delivery operations, innovations are undertaken, but only in discrete areas. We have a commitment to develop the skills and capabilities of staff and recruit additional talent in new areas. Robust assurance around implementation of new innovations with tolerance of only minor short-term negative impact on the quality of service delivery for a small number of students to achieve next improvement in service.	We want to be reasonably sure KCL would win any challenge. Limited tolerance for any action that could result in a regulatory challenge	Systems/technology changes are limited to the improvement of current operations. We are keen to ensure that existing systems and technology is working to the most current version and we are using the full suite of tools to the maximum advantage.	Projects are undertaken with clear requirements and a well defined scope. There will be some cross functional working supported by a clear PM structure and reporting lines. Project outcomes are clear and unlikely to change delivering measured improvements to existing services/facilities, with limited disruption
Open	Willing to consider all options and choose one most likely to result in successful delivery while providing an acceptable level of benefit. Seek to achieve a balance between a high likelihood of successful delivery and a high degree of benefit and value for money. Activities themselves may potentially carry, or contribute to, a high degree of residual risk	Recurrent expenditure actively reviewed and challenged with the value and benefits of reducing/restructuring the cost base considered. Prepared to invest for reward in terms of new opportunities that support the strategic vision and minimise the possibility of financial loss by managing the risks to a tolerable level that has been approved by Finance and UE	Service innovations are supported with demonstration of benefits to ensure Service Excellence standards maintained equal to or above the agreed KPI's. Willingness to consider new approaches to secure the best staff talent and to develop existing staff skills and capability. Responsibility for non-critical decisions may be devolved within the local management structures	Challenge will be problematic but we are likely to win it the gain will outweigh the adverse consequences. Regulatory challenge would be problematic but the gain will outweigh the adverse. Taking compliance risks at this level require sign off of the mitigation approach by UE via the SVP Operations	Support for systems/technology changes to enable operational delivery. Appetite for innovative developments which may involve a risk of negative impact on larger numbers of students to achieve long-term benefits.	Projects are undertaken where the expected outcome will delivery new processes and systems to improve operations. These projects are may be overseen by the King's Portfolio Office or may be moved from BAU or Portfolio Office if the risk profile changes leading to potential impacts on the strategic plans/Service Delivery standards
Hungry	Eager to be innovative and to choose options based on maximising opportunities and potential higher benefit even if those activities carry a very high residual risk.	Prepared to make significant changes to the cost base without firm guarantee that projected benefits could be realised. Prepared to invest for the best possible rewards and accept the possibility of financial loss (although controls may be in place) Resources allocated without firm guarantee of return. Supported by PST	Prepared to actively pursue innovative operational change in our desire to "break the mould" and challenge current working practices. Prepared to change operations that have a high inherent risk and may result in significant gain or loss. Accept high levels of devolved authority – management by trust rather than tight control.	Chances of an adverse regulatory finding are likely and consequences are serious but the gains are significant in the long term. Taking compliance risks at this level require sign off of the mitigation approach by PST via the SVP Operations	New technologies viewed as a key enabler of operational delivery. Actively pursue new solutions to become a sector lead in service operations and delivery. Significant risk and disruption is likely in order realise the gains.	Projects are undertaken where the expected outcome will delivery new processes and systems to improve operations. These projects are likely to be overseen by the King's Portfolio Office where the risk of failure would significantly impact staff and student experience, regulatory or financial operations

Appendix D

Examples of Managing Operational Risks

Example One

Risk Register - Example One													
No.	**Risk description**	**likelihood (Score 1 - 5)**	**Impact (Score 1-5)**	**Net Risk**	**Risk Owner(s)**	**Mitigating actions. Free text box. Please include link to any web materials**	**Named owner of Mitigations**	**Residual likelihood (Score 1 - 5)**	**Residual Impact (Score 1-5)**	**Net Risk**	**Critical Dependencies**	**Initial Risk Rating**	**Residual Risk Rating**
1	Failure to comply with statutory obligations caused by gaps in maintenance procedures and document processes and owners, leads to a statutory or legal breach.	4	5	20	Assurance Lead	1. Completion of an updated H&S processes. 2. Completing Safety gap analysis. 3. Reinstate the reviews of compliance information on a monthly basis 4. Completing a Competence Matrix.	Director of Operations	4	5	20	Aligned processes with building users.		

The Directorate has set its risk appetite as follows;

• Finance Moderate	• Service Delivery Open	• Compliance Cautious	• Systems/Technology Moderate	• BAU Projects Moderate

The above risk relates to compliance. The Directorate has agreed that it is only prepared to accept a cautious approach to compliance risk. The residual risk in this example is significant and therefore outside the tolerable risk level the Directorate has set. In this case, the mitigations do not provide an effective reduction in the risk and further mitigations should be agreed to reduce the risks.

Where there is nothing more that can be done that will reduce the risk to an acceptable level, in line with the risk appetite statement, this risk should be escalated in line with the escalation table, for review and further consideration of ways in which the residual risk can be reduced or effectively managed should it be realised.

Example Two

Risk Register - Example Two													
No.	Risk description	likelihood (Score 1 - 5)	Impact (Score 1-5)	Net Risk	Risk Owner(s)	Mitigating actions. Free text box. Please include link to any web materials	Named owner of Mitigations	Residual likelihood (Score 1 - 5)	Residual Impact (Score 1-5)	Net Risk	Critical Dependencies	Initial Risk Rating	Residual Risk Rating
2	Failure to ensure that sufficient staff are available to cover caused by sickness absence and or staff turnover leads to gaps in service coverage at key points in the academic year resulting is loss of service.	4	3	12	Director of Staff	1. Core processes to be identified against academic calendar 2. Training on core processes to be rolled out to teams to ensure cross support within teams. 3. Review staff absence records with OD/HR to identify any core issues and address.	Directorate Lead	4	2	8	Support for HR/OD		

The Directorate has set its risk appetite as follows;

• Finance Moderate	• Service Delivery Moderate	• Compliance Cautious	• Systems/Technology Cautious	• BAU Projects Moderate

In this example, the risks relate to staffing and service delivery. With a Moderate appetite for service delivery, the initial risk rating is higher than the tolerance set in the appetite statement. However, once the mitigations have been applied, the risk rating reduces. This example would also need a clear timeline for the completion of the mitigations to ensure the level of risk is in line with the appetite statement, accepting short term, negative impacts, whilst the mitigations are implemented. If the timeline is not met, the residual risk rating would need to be increased and the mitigations reviewed and amended.