Enterprise Risk Management Procedure

Responsible Officer:	Director of Strategy
Responsible Office:	Strategy, Planning and Analytics
Related Procedures:	Operational Risk Management Procedure
Related College Policies:	Integrated Risk Management Policy
	Procurement Policy
	Business Continuity Policy
Effective Date:	9 February 2023
Supersedes:	Not applicable
Next Review:	February 2026

---

1. Purpose & Scope

The purpose of this procedure is to provide guidance on the management and monitoring of enterprise risk across 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.

2. 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.

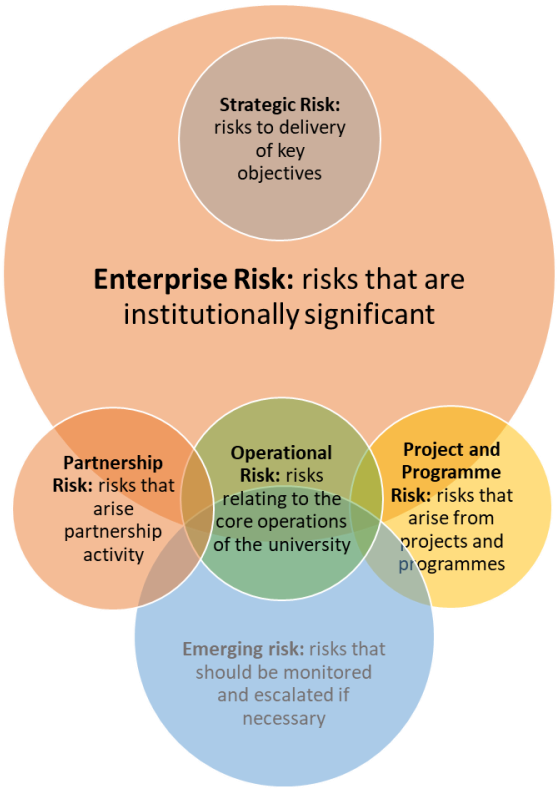

Figure 1: Enterprise Risks

3. Procedure

3.1. Risk Appetite

The Risk Appetite Statement specifies the level of risk that the university is willing to tolerate or accept in the pursuit of its strategic aims. It is linked to the university's strategy, and any strategic decisions should reflect the tolerance specified in the statement. The Risk Appetite is agreed with the Principal's Senior Team and the University Executive. It is reviewed every 12-18 months, and updated in line with changes to the university's strategy and vision.

3.2. Identifying Enterprise Risks

The responsibility for managing and mitigating enterprise risks sits with the University Executive. Enterprise risk encompasses strategic, operational and partnership risks and are of a magnitude that would significantly impact the financial, legal and/or reputational standing of the university. Risks identified in these categories are captured on the Enterprise Risk Register and are allocated a specific risk owner who is accountable to University Executive for the management and mitigation of the risk.

Risks are identified through horizon scanning, the integrated planning process, assessment of project, programme and partnership risk, and an annual review of the Enterprise Risk Register in line with the Strategy and Vision.

Any emerging risks are reviewed by University Executive to assess whether they are significant enough to feature on the Enterprise Risk Register.

3.3. Managing Enterprise Risks

3.3.1 Responsibilities

Managing strategic risks

The Integrated Risk Management Framework includes the management of strategic risks. These are risks to being able to deliver on the strategic objectives of the university strategy, identified through a process of horizon scanning and review in line with our Vision and Strategy. Strategic risks are always considered enterprise risks and are found in the Enterprise Risk Register.

Managing operational risk

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 standardised template. Local risk registers will be reviewed at quarterly review meetings. Further information can be found in the Operational Risk Procedure [link].

Managing partnership risk

The responsibility for managing and mitigating partnership risks sits with the Partnership Committee.

Risk Owners

Risk Owners are members of University Executive and are *accountable* for the effective management of risk – both monitoring any changes on likelihood and impact, and initiating, adapting and overseeing mitigating actions as appropriate.

3.3.3 Processes

Risk Scorecards

Risks scorecards are used as a tool to support the management and reporting of risk and show greater detail than the Enterprise Risk Register. Risk scorecards should:

Identify risk

1. Identify the risk in the context of the university's Vision, strategic objectives and BAU operations.
2. Risks should be framed in the form of "Failure to...caused by…leading to".
3. Identify the areas of the university that may be impacted by the risk event, should it occur.
4. Identify the type of risk.
    - Operational
    - Financial
    - Reputational
    - Legal (including legislative changes)
5. Identify if the risk is a threat or an opportunity

Assess risk

6. Assess the risk, determining a pre-mitigation score and associated RAG rating, using the 5x5 matrix (as seen below), which ranks risks from 'rare' to 'almost certain' for likelihood and from 'very little impact on operations' to 'catastrophic impact on business delivery' for impact.

7. Consider the likelihood of the risk event occurring.
8. Assess and determine the response (avoid, accept, mitigate, transfer). Risk responses will determine the type and level of action required to manage the risk.
9. Clearly describe a response action plan based on the above.
10. Assess the risk, to determine a post-response action plan score and associated RAG rating using the 5x5 matrix.

			IMPACT				
LIKELIHOOD			Very Little Impact on operations	Some service impact	Services will be impacted to an extent	Significant impact	Catastrophic impact on business delivery
			1	2	3	4	5
	Almost Certain	5					
	Highly Likely	4					
	Likely	3					
	Possible	2					
	Rare	1					

Figure 2: 5x5 Risk Matrix

Define short term and long-term mitigation/action plans

11. Once risks have been identified and assessed, set out in the scorecard the actions which are being taken to either reduce the likelihood of the event taking place or to lessen its impact if it should happen (in the case of a threat).
12. In the case of a risk opportunity, response action plans should set out how the risk event will be taken advantage of should it occur.
13. Response action plans should be SMART (specific, measurable, achievable, realistic, time-bound). Risk owners will be accountable for specified actions and risk managers will be responsible for the effective management.
14. The setting out of these response action plans allows management to make a judgement on the efficacy of the actions which are being put in place to manage risk and to identify any gaps in the approaches adopted.

Monitor and report

15. Risks should be reviewed by risk owners at regular intervals (see schedule in section 4.5) to assess for the continued relevance of the risk, RAG status, mitigation action plans, and whether any escalation is necessary.
16. Changes in the internal and/or external environment may affect the mitigation action plans and therefore change the risk rating for the activity.

3.4. Recording Risk

All enterprise risks are captured on the Enterprise Risk Register, which is held by SPA and updated with risk owners once every quarter.

Whilst risk scorecards hold the detail of each individual enterprise risk the Enterprise Risk Register provides the summary. Any updates to risk scorecards are mirrored in the Enterprise Risk Register.

3.5. Monitoring, Review and Sign Off

The Enterprise Risk Register is a live document and is monitored by SPA. Review of risks takes place at frequent intervals and to varying degrees of depth:

1. An extensive review every 12 months – this looks at the Enterprise Risk Register in line with King's Strategy and Vision to ensure it is comprehensive. It will conduct an external horizon scan for potential risks to UK Higher Education and King's specifically, assess for key delivery risks to goals and objectives, and review risks arising from the Integrated Planning Process.
2. A 6-month light touch review – this will work with each risk owner to update mitigation action planning and assess any changes to RAG status.
3. Quarterly request to risk owners to update risks – this will serve as a reminder to risk owners to check and update risks in line with quarterly accountability meetings.

University Executive has oversight and reviews and approves any changes periodically. Alongside review points at UE, ARCC is also sighted on the risk register at termly intervals.

3.6. Induction and support for risk owners

3.6.1 Risk owners will be inducted to their role through appropriate training which will outline key responsibilities alongside how to complete a risk scorecard.

3.6.2 At each annual extensive review point, risk owners will be sent a self-assessment survey which will enable Business Assurance and SPA to evaluate for any knowledge gaps in managing risk and to provide targeted support as needed.