Risk Management Guidance

1.0 Introduction

1.1 A risk can be defined as uncertainty, which could affect our objectives. A risk is something which might happen as opposed to an incident which is something that has happened (or is happening).

1.2 Exposure to risks is inevitable, in fact we will need to take risks to be successful, so it is important to acknowledge and monitor them, and allocate resources in order to manage their impacts upon the University.

1.3 The perception of risk can vary widely across individuals and across cultures. Risk management can help us to be more objective in our assessment of risk and more consistent in how we treat them.

1.4 The University has a Risk Management Policy which describes its approach to risk management and this Framework has been developed to explain the procedures involved and to raise awareness among staff.

1.5 A consistent approach to risk management can help us to be prepared for challenges and harness opportunities by identifying and treating risks in a timely way, establishing our risk appetite to enable effective decision-making and to prioritise resources appropriately.

2.0 Risk Management - Assessment

2.1 For each type of risk the University's standard approach will be to:

- **Identify** risks which threaten the fulfilment of the University's objectives;
- **Assess** the impact of a risk would have upon the University and the likelihood of it occurring;
- **Consider** who should own the risk and how it should be managed (e.g. tolerated or treated);
- **Confirm** any controls that are already in place and assess whether they are sufficient;
- **Reduce** the risk through taking further mitigating action if necessary;
- **Define** a tolerable residual risk rating, which should be reached if mitigation is successful;
- **Monitor** the risk to ensure mitigating activity is sufficient and on-track
- **Record** incidents and near misses that have occurred to learn lessons; and
- **Review** risks that have been controlled to feed back into the process.

2.2 The University's Risk Scoring Matrix assigns ratings to risks in terms of their likelihood and impact:

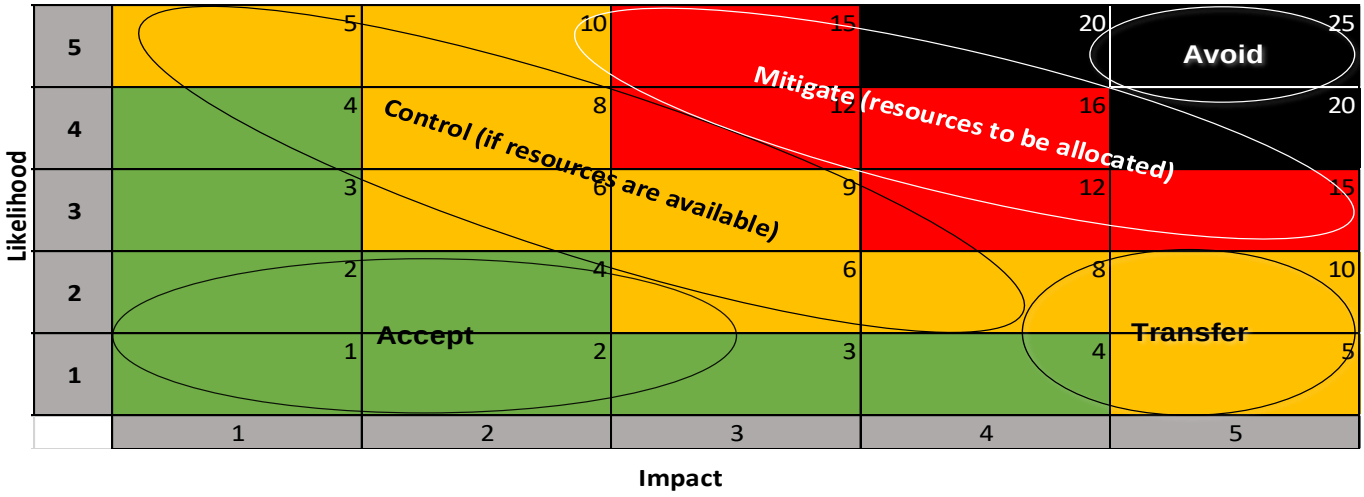
Fig.1 – University of Sussex Risk Scoring Matrix

LIKELIHOOD										
	Event is **expected** to occur imminently	>90%	**Almost Certain**	**5**	5	10	15	20	25
	Event will **probably** occur at some point	50-90%	**Likely**	**4**	4	8	12	16	20
	Event **could** occur in the future	30-50%	**Possible**	**3**	3	6	9	12	15
	Event is **not expected** to occur	10-30%	**Unlikely**	**2**	2	4	6	8	10
	Event would only occur in **exceptional** circumstances	<10%	**Rare**	**1**	1	2	3	4	5
					1	**2**	**3**	**4**	**5**
					Minor	**Moderate**	**Significant**	**Major**	**Severe**
	US UNIVERSITY OF SUSSEX		**Oversight**		Resolution would be achieved through normal activity	Resolution would require input from Head of School or Director	Resolution would require action approved by UEG	Resolution would require direction from Council	Intervention by Council and possibly external bodies (e.g. OfS)
			Cost		Under £50k	£0.05m to £0.5m	£0.5m to £5m	£5m to £25m	Over £25m
			Reputation		Negligible reputational damage, reputational building	Reputation damage unlikely, potential to build reputation	Some adverse publicity, but short-lived reputational damage	Some adverse publicity, but short-lived reputational damage	Substantial and prolonged reputational damage
			Achievement of Objectives		Negligible impact of School/Divisional objectives	School/Divisional objectives compromised	Some impact upon the University's strategic objectives	Major impact upon the University's strategic objectives	Failure of strategic objectives, requiring fundamental revision
	IMPACT								

3.0 Risk Treatment

3.1 The diagram below indicates how the rating of risks may influence their treatment.

Fig. 2 - Risk Rating and Potential Treatment Options to be Considered



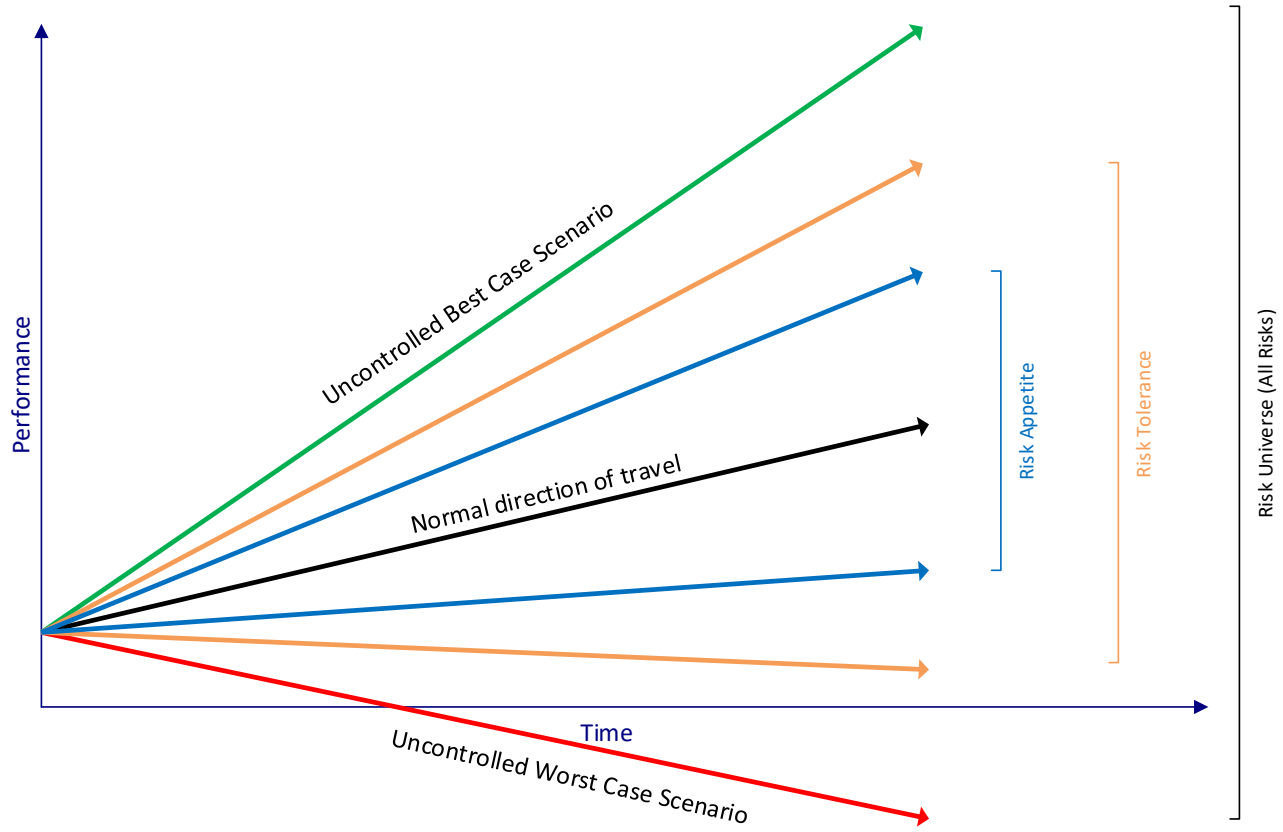
4.0 Risk Appetite

4.1 Risk appetite refers to the amount and type of risk that the University will take in order to achieve its objectives.

4.2 Even in the most challenging times, the University must remain open to risk taking in order to remain competitive and achieve its objectives. It is acknowledged that certain strategies, programmes or mitigating activities may expose the University to higher levels of risk at certain points in time and this may be entirely appropriate given the beneficial outcomes, which may be derived from taking such risks.

4.3 Figure 3 below indicates how the University will be exposed to risk as it seeks to improve performance.

Fig. 3 - Risk and Performance



4.4 Given the environment in which the University operates, it is expected that the University's risk appetite may be subject to change over time.

4.5 Consideration will be given to the following factors when determining the University's risk appetite:

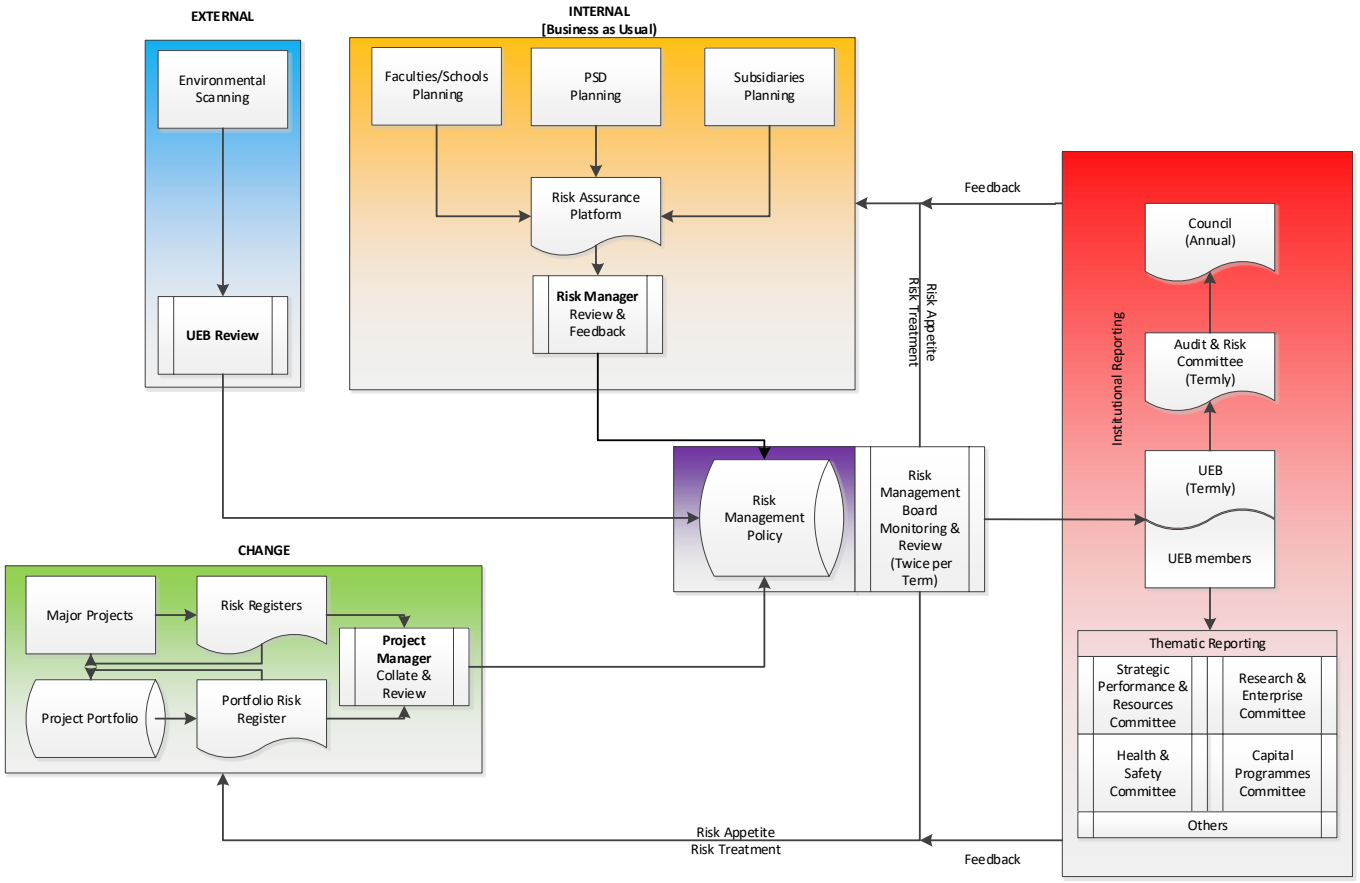
- external factors which alter the University's operating environment;
- any significant change in the University's strategic objectives and mission;
- the University embarks on a major transformation programme;
- the overall effectiveness of the University's Risk Management Policy; and
- a major incident affects the University's reputation and/or financial sustainability.

4.6 The University's Risk Appetite Statement is available on the GCGC Risk Management web pages. The Risk Appetite Statement will be reviewed by the Risk Management Board at regular intervals and in line with strategy development.

5.0 Communication of Risk

5.1 Figure 4 below indicates how risk management information should be communicated through the University.

Fig. 4 - Communication of Risk Management information within the University of Sussex.



5.2 Risk Identification

5.2.1 Risks will be identified in one of the following ways:

- External scanning of what's happening in the environment in which the University operates (e.g. political, economic or regulatory change within the higher education sector);
- Internal reporting of operational risks (e.g. financial sustainability, league tables);
- Risks identified during Major Projects (e.g. delivery timelines and budget); and
- Local Risks (e.g. space, condition of buildings and infrastructure, safety and wellbeing, staff engagement, student recruitment etc.).

5.3 External risks may emerge at any time and the University is unlikely to directly control the likelihood of them occurring. However, by giving due consideration to the foreseeable outcomes of such risks, it should be possible to attend to them and if necessary, allocate resources which serve to manage their impact upon the University.

5.4 The University Executive Board will conduct routine environmental scanning as part of their normal business and institutional risks will be considered at Risk Management Board meetings.

5.5 However, if a significant risk is identified or emerges from elsewhere in the University, the relevant Executive Dean or Director should inform their line manager (usually the Provost or COO respectively) and the General Counsel and Director for Governance and Compliance. If necessary, the Senior Risk and Resilience Manager will provide advice to the risk owner to undertake an initial assessment, consider the most appropriate method of recording and reporting (see section 6.0), discuss strategies for treating the risk and monitor the progress towards mitigation.

6.0 Risk Recording, Monitoring and Reporting

6.1 Institutional Risk Register (IRR)

6.1.1 The Institutional Risk Register contains a record of the key strategic risks which are being prioritised by the University at a given point in time. The IRR is reviewed by the Risk Management Board (RMB) twice per term, before being reported to the Audit and Risk Committee (ARC). Risk Management Board members will discuss which risks should be included in the IRR, agree ownership and how they should be rated using the University's approved Risk Scoring Matrix (see Fig. 1 in Section 2.2).

6.1.2 The IRR will be accompanied by a highlight report, which enables Risk Management Board members to consider the University's key risks and monitor the progress being made towards mitigation.

6.1.3 Each version of the IRR will be collated by the Senior Risk and Resilience Manager (in consultation with the General Counsel and Director of Governance and Compliance) who will request regular updates from risk owners. Ownership of IRR risks will be assigned to the relevant member of UEB. Reports will ask members to note the current contents of the IRR and consider any other risks that may need to be added, removed or re-articulated. Any risks which have been removed from the IRR will be recorded and subsequently reported to ARC.

6.1.4 ARC will provide assurance to Council on the overall effectiveness of risk management within the University. ARC will review the contents of the IRR at each of their meetings and will seek assurance that sufficiently resourced mitigation plans are in place and on track to manage the University's most significant risks. Occasionally, ARC may also request more detailed 'deep dive' reports from the relevant risk owners to investigate how such risks are being managed.

6.2 Local Risk Registers – Maintained via the Risk Assurance Platform (RAP)

6.2.1 The Risk Assurance Platform (RAP) is a system for recording, monitoring and reporting local risk information from within the University's Faculties, Schools, Professional Services and subsidiaries.

6.2.2 Executive Deans, Heads of Schools and Directors are required to discuss their local risks with their Management Teams and update their information on the RAP at least twice per year. Schools, Divisions and subsidiaries with higher risk profiles are advised to undertake reviews more regularly, at intervals to be agreed between the risk owners, in consultation with the Senior Risk and Resilience Manager.

6.2.3 Local risks recorded on the RAP will be reviewed by the Senior Risk and Resilience Manager twice per year with progress reported periodically to the Risk Management Board.

6.2.4 The Senior Risk and Resilience Manager will provide support to enable the relevant colleagues to identify, monitor and escalate their local risks and to develop and implement appropriate SMART mitigation plans within reasonable timeframes. Risk and action owners will receive automated reminders from the RAP system when risk actions need to be reviewed. Additional Guidance Notes for using the RAP can be found on the Risk and Business Continuity web pages.

6.2.5 In most cases, individual local risks are unlikely to have an institutional impact, although there are some notable exceptions. For example, in a larger School, the failure to meet certain student recruitment targets may have a significant financial impact for the University.

6.3 Escalation and Removal

6.3.1 Risks can be escalated from local risk registers to the institutional level to in the following ways:

- Identification (Internal) – a new risk is identified by UEB and requires attention;
- Emergence (External) – environmental factors (e.g. regulatory change) cause an institutional risk to emerge and be brought to the attention of UEB;
- Escalation - A local risk escalates from within a Faculty, School, Professional Service or applicable subsidiary of the University, which has the potential to have an institutional impact; and
- Accumulation - Numerous similar local risks combine to create an institutional risk.

6.3.2 Risks will be removed from the IRR when they have been treated sufficiently so that their ratings reach acceptable levels (within risk appetite and tolerance), or if they are no longer prioritised at an institutional level.

6.4 Incident and Near-miss Reporting

6.4.1 Whilst risk registers are intended to be forward-looking records, risk owners are responsible for reporting any local risks which have materialised and impacted upon the University. Initially, such incidents must be reported by the Risk Owner to the General Counsel and Director for Governance and Compliance. Major incidents (e.g. those which are likely to have a severe impact upon the operation of the University) will be escalated via the Chief Operating Officer and or the Provost to the Vice Chancellor.

6.4.2 Local risks that have materialised will be marked as 'Issues' on the Risk Assurance Platform and these will be monitored by the risk owner in liaison with the Senior Risk and Resilience Manager. Near misses (where a significant incident may have been close to occurring but the full impact was fortunately avoided) should be reported in the same way, so that lessons can be learned and mitigation strategies can be reviewed.

6.4.3 In some cases, mitigation measures may themselves expose the University to additional risks and therefore, those responsible for implementing them will be required to regularly evaluate their risk control strategies in order to support the overall achievement of objectives.

7.0 Risk Assurance

7.1 The University adopts the "Three Lines of Defence" model in order to provide assurance that risks are being managed effectively with roles, responsibilities and accountabilities as shown in Fig. 5 below:

Fig. 5 The Three Lines of Defence Approach to Risk Management

1st Line - Management Faculties/Divisions/Subsidiaries	•involved in day-to-day risk management •follow the approved risk recording and reporting process •assign ownership of risks and actions necessary to treat them
2nd Line - Oversight Governance and Competence	•develop and maintain Risk Management Policy and Guidance •confirm monitoring responsibilities of senior leaders and committees •provide support and guidance on articulation of risks •promote consistency and good practice in risk management
3rd Line - Audit Compliance	•monitor and report on activities in the 1st and 2nd lines •provide an independent perspective and challenge the process •objective reporting to provide assurance

7.2 - 1st Line of Defence – Managing Risk

7.2.1 The University aims to create an environment where risk management becomes established as a routine part of normal operations. This first line of defence provides assurance by identifying local and institutional risks, assigning ownership, instigating effective treatment and monitoring progress.

7.3 - 2nd Line of Defence – Internal Oversight

7.3.1 The second line of defence involves mechanisms that provide standards, oversight and direction, which are in line with accepted good practice, such as the University's Risk Management Policy. The Senior Risk and Resilience Manager will be responsible for maintaining suitable procedures and guidance, in order to support those who manage risk. In addition, the University's Executive Board and relevant Committees will be suitably informed to undertake their monitoring and assurance roles.

7.4 - 3rd Line of Defence - Independent Assurance

7.4.1 The third line of defence refers to the numerous approaches that provide assurance to the University, such as our Internal/External Audit functions. Additional assurance mechanisms may also apply and will have their own monitoring and oversight functions, such as those which are regulated by the Office for Students or the Health & Safety Executive.

7.5 - Risk Controls and Assurance

7.5.1 Risk assurance mechanisms should be proportionate to the potential exposure, to ensure that clearly defined controls are identified and implemented. Such actions might include:

- development of business case(s) to initiate mitigating activities, projects and programmes;
- recruitment of technical expertise into a function;
- professional training for existing staff to improve competence;
- reviewing the terms of reference of an existing oversight committee; and
- the need for an internal audit of a particular area of activity.

8.0 – Training and Awareness

8.1 The Senior Risk and Resilience Manager will deliver a programme of activity to raise awareness of Risk Management among University staff. This will include the development and provision of appropriate guidance and training materials for all staff, liaising with key staff who are routinely involved in the Risk Management process and facilitating training where required.

8.2 The intention of Risk Management training will be to enhance understanding of the University's approach to Risk Management and to promote consistency and compliance. The Senior Risk and Resilience Manager will facilitate training (either directly or in partnership with external providers) to develop competence among staff who play a role in Risk Management, such as:

- Induction for those with responsibility for risk management;
- Understanding risk appetite;
- Identifying, describing and assessing risks;
- Good practice in maintaining risk registers; and
- Using the University's Risk Assurance Platform.

8.3 The Senior Risk and Resilience Manager will maintain information on the University website to enhance the understanding of all staff of the benefits of risk management and to embed a culture of risk awareness.