University of Aberdeen

Risk Management Framework

Version 2.0

Status – *Approved*

Update Due: 02/2023

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

This document is the University's Risk Management Framework. The Framework is comprised of two key components: the University's Risk Management Policy, and the University's Risk Management Process, which gives a detailed overview of the processes, tools and reporting structures in place for the effective management of risk.

The Framework applies across the University at all levels, including strategic organisational level, Schools, Directorates and on projects; risk management is an important part of the institutional Project Management Methodology. At organisational level, overarching accountability for the management of risk lies with the University Court, with additional oversight provided by the University's Audit and Risk Committee (ARC). ARC undertakes an assurance role, designed to help ensure the effectiveness of the University's risk management arrangements. Within this wider Framework, the University also has a Strategic Risk Register designed to support delivery of strategic institutional objectives, with a particular focus on the commitments made via Aberdeen 2040.

The Risk Management Framework was developed and is owned by the University's Directorate of Planning. It aligns with best practice and internationally recognised standards for risk management, such as the ISO31000 Risk Management Principals and Guidelines document.

2. RISK MANAGEMENT - KEY TERMS AND DEFINITIONS

The following definitions are provided for key terms. These definitions are recognised and accepted by the University and are applicable to the University's Risk Management Framework, encompassing all risk related policies and processes. All stated definitions are based on those given in the BS ISO3100:2018 Standard, and are therefore widely recognised across different sectors.

- **Risk**: In accordance with the ISO3100 (2018) definition, the University defines risk as the potential "effect of uncertainty on objectives". An "effect" is a deviation from an intended or expected outcome, which can be positive, negative or both, and which can address, create or result in opportunities or threats.

  A risk will be considered as either a threat (negative) to the University's ability to achieve any given objective, or as uncertainty resulting from an opportunity (positive) which offers potential benefits to the institution.

  An objective can have different aspects or categories; such as financial or regulatory, as examples, and can apply at different levels, within different contexts. For example, risks can be strategic or operational, and can apply to projects, processes and "business as usual" activities.

  A risk will usually be referred to in terms of risk *sources*, such as cost uncertainty; potential *events*, such as a cyber-attack or a pandemic; the *likelihood* that they will occur, and their *consequences* in the event that they do unfold.

  NOTE: it is important to recognise the difference between a risk and an issue. A risk is something that *might* happen, and therefore the outcome is uncertain. With an issue, there is no uncertainty; an issue is something that *has* happened or *is* happening.

- **Risk Management**: is defined as the "coordinated activities, systems and processes in place to direct and control the University with regard to the management of risk."

- **Stakeholder:** this is defined as a person, group or organisation that can affect or be affected by a decision or activity, or have the perception that they can affect or be affected. Alternatively, a "stakeholder" can also be referred to as an "interested party".

- **Risk Source**: this is an element which either on its own, or in combination with others, can potentially give rise to risk; for example, cost, schedule, user satisfaction.

- **Risk Event**: this is an occurrence or a change in circumstances, which can have several causes and a range of consequences. An event might be something that is expected but does not happen, or something unexpected which does happen. Brexit and the Coronavirus pandemic are both examples of events.

- **Consequence**: this is the outcome of an event which will affect objectives. This can be certain or uncertain, positive or negative, and can have direct or indirect impacts. As an example, consequences of an event like Brexit within a University context might be a decline in student numbers and a drop in tuition fee income.

- **Likelihood**: this is the chance that something will happen, noting it can be defined, measured or determined in quantitative or qualitative terms, objectively or subjectively.

- **Control**: this is a measure or measures that maintain or modify any given risk, and can include actions, initiatives, processes, policies or practices.

- **Risk Appetite**: this refers to the level of risk the University is willing to tolerate or accept in the pursuit of its objectives. 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 potential or expected benefits.

Risk Appetite is directly linked to Risk Tolerance; an organisation with a higher Risk Appetite will tolerate a higher level of risk, meaning its risk tolerance threshold - the point at which the level of risk exposure becomes intolerable or unacceptable - will also be higher.

- **Risk Owner**: this is the person, persons or entity in authority accountable for the effective management of a risk.

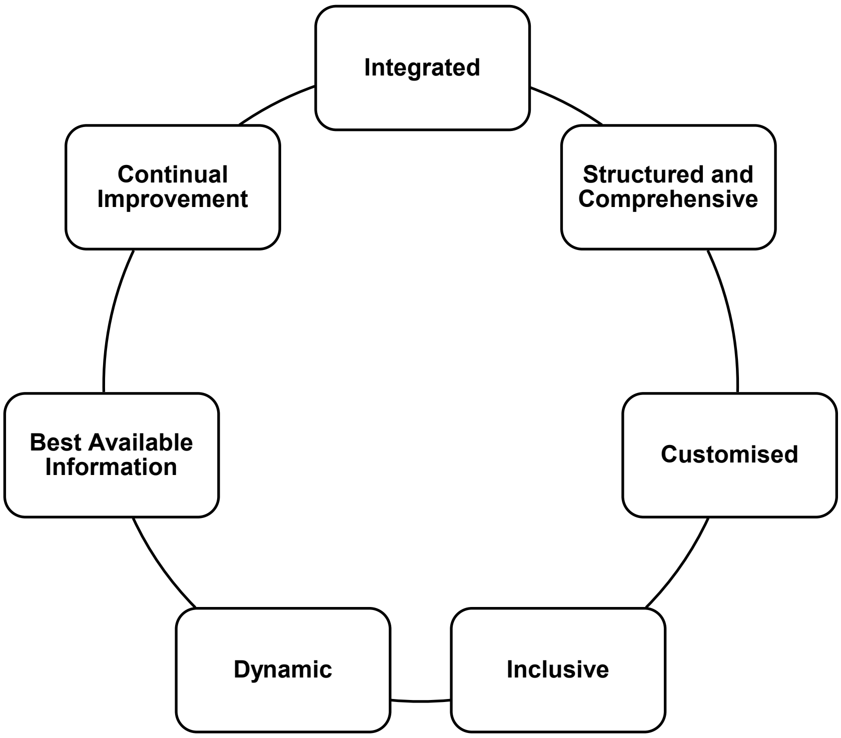
- **Risk Manager**: this is the person, persons or entity with delegated responsibility for the effective management of a risk.

  It should be noted that while Risk Owners and Risk Managers may be directly accountable and responsible for the management of specific risks, in practice, all stakeholders and University employees have a responsibility for good risk management.

3. PRINCIPLES OF RISK MANAGEMENT

The University subscribes to the principles set out below for effective and efficient risk management, based on those included in the ISO 31000:2018 standard. These principles underpin this Framework document, and they will inform the continuous development and improvement of all institutional risk management arrangements.

FIGURE 1: RISK MANAGEMENT PRINCIPLES



1. **Integrated**: risk management is a central part of the University's activities and its wider management arrangements, applicable institutionally, across Schools and Professional Services, and on projects.
2. **Structured and Comprehensive**: the risk management arrangements in place are structured and comprehensive, ensuring consistency of use across the University at different levels, and where applicable, ease of comparison.
3. **Customised**: the Framework and processes in place should be customised and proportionate, taking account of context and the environment, internally and externally, as well as relevant institutional aims and objectives.
4. **Inclusive**: risk management will include timely involvement of key stakeholders, ensuring that all relevant knowledge, views and perceptions are considered as and when appropriate.
5. **Dynamic**: risk management provides the ability to dynamically anticipate, define and respond to changes or events timeously and effectively; noting risks will emerge, change and disappear in different areas under different circumstances over varying timelines.
6. **Best available information**: risk management should at all times be informed by the best available information. This is crucial for identifying and defining risks accurately; for determining the likelihood and scale of any consequences posted, and for informing the nature of the required response.
7. **Continual Improvement**: risk management arrangements are continually improved through learning and experience, underpinned by a process of continuous reviews.

4. RISK MANAGEMENT POLICY FRAMEWORK

4.1. UNIVERSITY POSITION STATEMENT ON RISK MANAGEMENT

The University operates in a sector and wider environment where different sources, influences and events create uncertainty. Uncertainty manifests itself as "risk", and risk can affect the University's ability to achieve its aims and objectives across all areas of the organisation. Risk will take the form of a threat or may come with opportunities, but either way, risk management is key to addressing the uncertainty created by reducing the likelihood that risks might be realised, and the resultant consequences in the event that they are. It is the University's position, therefore, that the use of risk management should be a cultural norm, inherent in its governance arrangements, and key to both driving performance and informing decision-making at all levels.

The University's commitment to risk management, and the implementation of this framework, brings with it a number of high-level **benefits** which include, but are not limited to:

- Ensuring that risks are adequately identified, understood and considered when setting aims and objectives at different levels of the organisation, thereby enhancing the likelihood of successful outcomes.
- Similarly, ensuring that risks are adequately identified, understood and considered as part of decision-making processes, particularly where they concern capital investment decisions, the pursuit of opportunities or managing the impact of external issues like Brexit or Covid-19;
- In all cases, ensuring that the level of risk or the severity of potential consequences is minimised.
- Enabling a more proactive approach to management, which underpins better planning, enhances effectiveness and improves outcomes.
- Ensuring that the amount and types of risks taken across the University reflect its appetite for risk in any given area, and its wider strategic aims.
- Ensuring that information relating to such risks and their management is effectively communicated to key stakeholder groups, thereby providing increased confidence and assurance when decisions are made.
- Ensuring that the systems and processes articulated herein are followed and are operated successfully, as part of an ongoing process of continuous improvement.

The Framework is owned by the Directorate of Planning, and endorsed and promoted by the Senior Management Team. It applies across the University at all levels, including at institutional level, and at the level of Schools and Professional Services directorates. Risk management should be integrated as an important governance and management function in each of these areas, making it part of daily business considerations, and a key factor which drives decision-making, as above. Risk management is also an integral part of the institutional Project Management Methodology, which is applied to all major projects undertaken by the University, including major change initiatives, strategic projects, international partnerships, and projects which require significant capital investment, such as those under estates and digital.

4.2. UNIVERSITY RISK APPETITE STATEMENT

The University acknowledges that in different areas, the nature of risks it faces will vary; normally arising from either threats posed, or as a consequence of pursuing opportunities. In turn, the level of exposure carried by different activities will vary, and its threshold for accepting varying levels of risk will change depending on the risk area under consideration, along with the specific objectives involved, the subsequent activities undertaken, and the projected benefits.

As above, the University defines risk appetite as the level of risk it is willing to tolerate or accept in pursuing opportunities. On this basis, it informs how much the University is prepared to actively put at risk in order to realise potential or expected benefits. When considering threats, risk appetite informs the levels of risk the University will tolerate before thresholds are breached and escalation is required.

At a strategic level, the University will apply risk appetite ratings and statements to those risk areas under which the predominant ethos is to pursue opportunities in line with strategic objectives. This will be an ongoing and iterative process, noting that the University's appetite for risk across such areas will evolve over time. In turn, the University's application and use of risk appetite will likewise evolve as it goes through different stages of maturity.

For those risk areas which are more focused on mitigating threats, the University will develop and apply tolerance thresholds. In either case, the application of risk appetite ratings and tolerance thresholds will be used as a valuable tool to inform decision making.

4.3. Risk Management and University Strategy – Aberdeen 2040

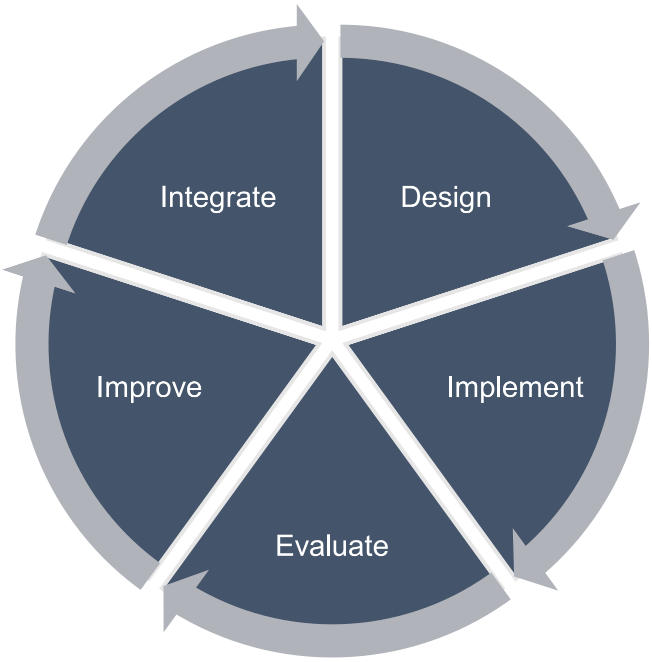
The University's risk management function interfaces directly with its strategic planning arrangements at institutional level; it is a key tool used to mitigate and control risks which might affect the University's ability to achieve the overarching strategic aims and commitments mapped out in the Aberdeen 2040 strategy. This is reflected in the composition of the Strategic Risk Register, against which all priorities outlined in Aberdeen 2040 can be mapped.

4.4. University Approach to Risk Management – Continuous Improvement

The Risk Management Framework is a live document that will evolve over time, as the University continues to advance and mature its risk management arrangements, under an ethos of continuous improvement. The University will follow a cyclical continuous improvement model based on the following steps:

- **Design** risk management systems and processes, as part of a wider framework.
- **Implementation** of the framework at different levels of the organisation.
- **Evaluation** of the framework and its constituent policy and processes to ensure best practice and ongoing effectiveness.
- **Improvement** of the framework where areas or relative weakness or poor practice are identified.
- **Integration** of risk management into management of the University at all levels.

Figure 2: Continuous Improvement Approach to Risk Management



The University will evaluate and review the Framework annually via the Directorate of Planning. This will ensure that the Framework remains aligned to best practice and that the arrangements in place remain effective.

4.5. Risk Management: Accountability and Responsibility

Accountability and responsibility for risk management sits at all levels of the organisation:

- **At an individual level**, all risks identified under the Risk Management Process, will be assigned a **risk owner** and **risk manager**. The risk owner is accountable for managing their risk(s), supported by one or more risk managers, who will normally be key stakeholders working in a relevant or associated function. The risk managers will be *responsible* for managing their risks on a more operational, day-to-day basis. Risk owners and managers will also be required to ensure that all risks under their remit are subject to scrutiny at the appropriate fora across the University's committee structures (*more on this under 5.3*).

- **At University level**, as part of the institutional corporate governance structure, accountability for risk management lies with the University Court and with the Audit and Risk Committee (ARC). Within this context, Court has a remit to ensure the establishment and monitoring of systems of control and accountability for risk assessment and management; the remit for ARC can be accessed here. SMT has delegated responsibility, as a core function, for oversight of the University's risk management arrangements, which includes management of all strategic risks via the SRR. SMT is also required to ensure that authority is delegated to manage risk at different levels of the University, as follows:

- **At School level**, every School should have a risk register in place, and School Executive Committees should have overarching responsibility for the management of all risks which might affect the School's ability to achieve its strategic aims and objectives. Heads of School will normally undertake the risk owner role, and will be responsible for appointing risk managers.

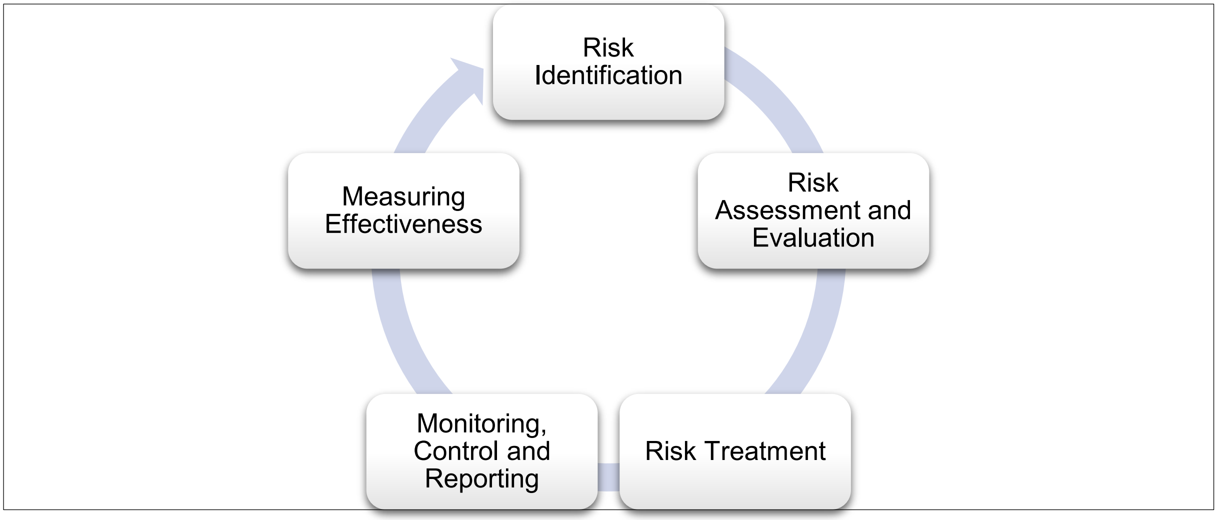
- **Within Professional Services Directorates**, each Directorate should have a risk register, with the Director normally assigned as risk owner for all major risks identified. Risk managers will be appointed accordingly. Directors will also commonly act as risk manager for risks under the SRR in areas relevant to them, supporting the SMT lead designated as risk owner.

- **For institutional projects of strategic importance**, including Digital, Estate-based and International projects, the Project Board will have overarching responsibility for ensuring that key risks are identified, monitored and controlled throughout the project lifecycle. Accountability for ensuring effective risk management takes place will normally sit with the Project Sponsor, with day-to-day responsibility falling to the project manager. The Project Board will normally report on risk as part of regular reports submitted to the appropriate authority; for example, the Digital Strategy Committee for Digital projects. Further information on risk management within a project context can be found within the University's Project Management Methodology.

5. RISK MANAGEMENT PROCESS

The following gives a detailed overview of the University's Risk Management Process, which is based on the cyclical workflow as below under Figure 3.

Figure 3: Risk Management Process


Risk Identification
Risk Assessment and Evaluation
Risk Treatment
Monitoring, Control and Reporting
Measuring Effectiveness

5.1 RISK IDENTIFICATION

The first step in the risk management process is risk identification. A variety of methods can be used for identifying risks, including brainstorming sessions with key stakeholders; formal or informal workshops; benchmarking exercises; horizon scanning; formal consideration by management groups, committees, boards or equivalents. When looking to identify uncertainties, a number of factors should be considered, noting these are often interlinked:

- Aims and objectives;
- threats and opportunities;
- vulnerabilities and capabilities;
- changes in the internal and external environment;
- the nature and value of assets or resources, for example buildings and finance;
- potential consequences and their impacts on objectives;
- limitations of knowledge and reliability of information;
- time-related factors.

The process of risk identification will vary depending on context and the level at which risks are being assessed. For example, at organisational level, strategic risks should be identified for ongoing management at the start of any major planning period to ensure that the strategic priorities outlined in any new strategy, like Aberdeen 2040, are taken account of. Consequently, risk identification at this level should be part of wider strategic planning arrangements. Similarly, at School or Directorate level, risks should align with the strategic priorities articulated in School or Directorate plans, and should therefore be identified early as part of the respective planning process.

Within a project setting, key risks should be identified at the start of a project, and managed throughout the project lifecycle. This should be done in accordance with the University's Project Management Methodology.

All identified risks should be recorded using the University's standardised risk register template, which comes with a supporting technical guide. These documents are available here via the University website.

5.2 Risk Assessment and Evaluation

When analysing risks, the purpose is to consider the risk source, potential consequences, likelihood, events, scenarios, controls and their effectiveness. The potential impacts should also be considered against multiple objectives, particularly where consequences are likely to be widespread. In particular, the following factors should be considered:

- the likelihood of events and consequences;
- the nature and magnitude of consequences, i.e. impact;
- complexity and connectivity;
- time-related factors and volatility;
- the effectiveness of current controls.

From this exercise, a <u>risk score</u> can be produced. Risk Scoring provides an important function through which the severity of potential risks facing the University can be established according to set criteria. This enables categorisation of risk by severity, and enables determination on whether the level of risk incurred is in line with the University's appetite for risk in that area, or whether it sits relative to agreed tolerance thresholds. It is also thus used to inform the prioritisation of risks, and to inform decision making on how to respond.

Risk scoring takes account of the ***likelihood*** that a risk will occur and then the expected consequences or ***impact*** in the event that it does. The risk score is determined using a matrix under which levels of likelihood and impact are given a numeric value, as below.

Likelihood - is graded by the University at four levels:

Table 1: Measuring Likelihood

Score	Definition
4	High likelihood of occurring
3	Realistic likelihood of occurring
2	Moderate likelihood of occurring
1	Unlikely to occur

Impact - is also graded at four levels:

Table 2: Measuring Impact

Score	Definition
4	Severe
3	Significant
2	Moderate
1	Measurable

This scoring system is applied via a standard scoring matrix. The matrix provides a visual representation of the risk score by applying RAG ratings to match the severity of risk posed. Those risks RAG rated lowest will be coloured green, and those highest coloured red. A copy of the matrix is included below under Figure 4 for information. The matrix is also included with more detailed criteria in the risk register template, along with the technical guide, available here.

Figure 4: Risk Scoring Matrix

		Impact			
		Low (1)	Moderate (2)	High (3)	Critical (4)
Likelihood	Highly Likely (4)	🟨 **4**	🟧 **8**	🟥 **12**	🟥 **16**
	Likely (3)	🟩 **3**	🟨 **6**	🟧 **9**	🟥 **12**
	Feasible (2)	🟩 **2**	🟨 **4**	🟨 **6**	🟧 **8**
	Unlikely (1)	🟩 **1**	🟩 **2**	🟩 **3**	🟨 **4**

Each Risk should be allocated two risk scores, as follows:

- **Unmitigated Risk Score –** often referred to as an inherent or gross risk score. This refers to the level of risk an activity would pose if no controls or mitigating actions were put in place.

- **Mitigated Risk Score** - often referred to as a residual or net risk score; this refers to the level of risk remaining after controls and mitigating actions are taken into account. The Mitigated Risk Score should ideally reflect the applicable risk appetite, and/or should fall within any agreed tolerance threshold.

Given that the mitigated risk score is applied taking account of actions designed to mitigate the risk, it should always be lower than the initial risk score (either in terms of impact, likelihood, or both).

5.3. Risk Treatment

When an initial risk score is determined, a decision should be made on how to respond to the risk. This is referred to as **risk treatment**. There are four main options:

- **Avoid**: this means avoid taking the risk by not starting the relevant activity, or terminating the risk by discontinuing and thereby removing the risk source. This will not always be possible, particularly where risks are posed by external events outwith the University’s control, such as Brexit or Covid-19.

- **Treat**: this means adding controls and/or taking mitigating actions to reduce the likelihood of a risk occurring, or its consequences if it does. Unless a decision is made to avoid a risk, almost all risks should undergo some form of treatment if possible.

- **Tolerate**: this means accepting risk where this is an option, usually in pursuit of an opportunity. This should always be an informed decision that takes account of the expected cost-benefit trade-off. This might apply to opening an overseas campus, as an example.

- **Transfer** (the risk): this is normally done via insurance or through contractual arrangements; for example, on a capital construction project in Estates, the risk of cost overrun could be transferred to the contractor by agreeing a fixed price contract.

All controls applied to any risk, and all mitigating actions agreed, should be recorded in the risk register. This will then be used as a key tool for monitoring and controlling progress, which will include appraising the effectiveness of different treatments, and their impact on risk scores.

5.4 MONITORING, CONTROL AND REPORTING

5.4.1. Monitoring and Control

Risks should be monitored and controlled on an ongoing basis. At an individual level, responsibility for monitoring and control lies with the risk owner and risk manager, in consultation with key stakeholders. This includes individual stakeholders and more collectively, stakeholder groups; for example, any relevant committee, project boards, or School Executive Committees (within Schools).

For the SRR, risk owners should ensure that their risk areas are routinely reviewed outwith any formal reporting structure, via the relevant committee (or equivalent). Table 3 maps each strategic risk area, as included in the SSR, to the appropriate for undertaking this function.

Table 3: Mapping Strategic Risk Areas to Committees

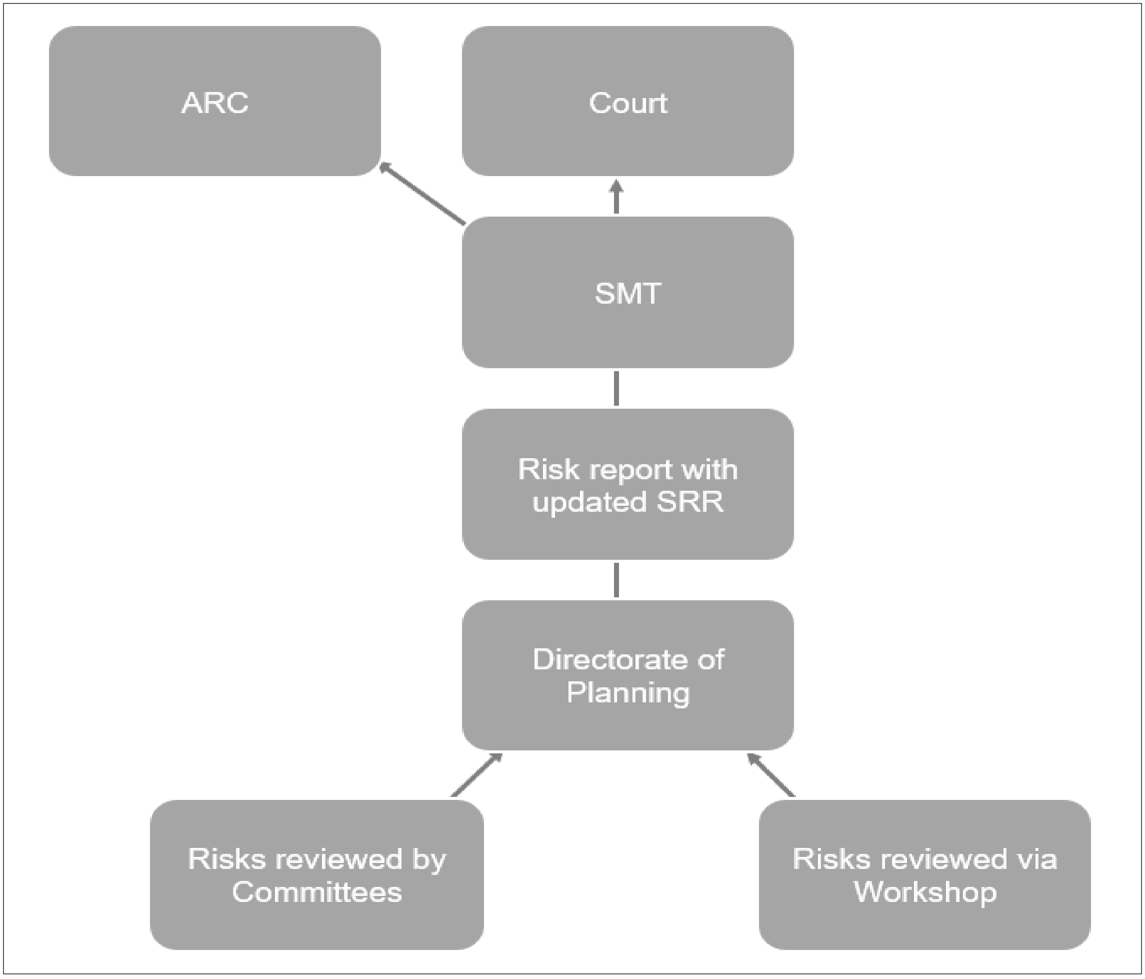
	STRATEGIC RISK AREA	COMMITTEES
1	Financial Sustainability	• SMT • Policy and Resources Committee
2	Estates and Facilities	• Estates Committee
3	Student Recruitment (UG, PGT and PGR)	• Student Recruitment Committee
4	Education (UG and PGT)	• Education Committee
5	Research and PGR	• Research Policy Committee
6	Digital and Information Services	• Digital Strategy Committee • Information Governance Committee
7	People	• SMT • Policy and Resources Committee
8	Health, Safety and Wellbeing (Staff and Students)	• Health and Safety Committee • Policy and Resources Committee
9	International Partnerships	• International Partnership Committee
10	Reputation	• SMT
11	External Environment	• SMT
12	Environmental Sustainability	• Sustainable Development Committee
13	Leadership and Governance	• Governance and Nominations Committee
14	AUSA and other Third Parties	• SMT

When monitoring and reviewing risks, they should be revised according to any changes affecting the risk status, the risk score or progress made in completing mitigating actions; updates should then be made accordingly. This may include the addition of new mitigating actions or enhancing the measures already in place; either way with a view to bringing the risk score down to an acceptable level.

5.4.2. Reporting

Reporting arrangements will also provide an additional level of monitoring and control. At University level, ARC and Court will receive a high-level report on risk twice per year in May/June and November/December, as part of a bi-annual reporting process. Each of these reporting rounds will involve a workshop with key stakeholders, coordinated by the Directorate of Planning. These reports will provide summary updates on management of the risk areas which comprise the SRR, with a particular focus on those areas which pose the most significant risks at that time. In this way, a monitoring and control function is being exercised at the highest level. Additionally, these reports will also provide assurance to ARC and Court that the University's risk management processes are being followed, and that they continue to function well. A visual representation of the institutional reporting structure for the SRR is given below.

Figure 5: Strategic Risk Management - Reporting Structure


ARC
Court
SMT
Risk report with updated SRR
Directorate of Planning
Risks reviewed by Committees
Risks reviewed via Workshop

More generally, and as above under 5.4.1, reporting on risk management will also take place at different levels across the University, and should include reporting to University committees as and where appropriate, to School Executive Committees, to Project Boards and so forth.

5.5 MEASURING THE EFFECTIVENESS OF THE RISK MANAGEMENT PROCESS

5.5.1 Internal Assurance

The Directorate of Planning has responsibility for ensuring that the Risk Management Framework is kept up to date, in line with best practice, and that it remains effective. On this basis, the Framework will be reviewed in full on an annual basis by the Directorate of Planning, in consultation with internal auditors if or where appropriate. Each review will take account of external risk management standards, with the overarching purpose of driving continuous improvement and enhancing maturity. On completion, a statement on the review outcomes should be made to both ARC and Court as part of the established reporting process.

Additionally, by reporting to ARC biannually, as above, ARC will undertake an assurance function designed not only to ensure that all major risks facing the University are being effectively managed, but also to provide assurance that the University's wider risk management arrangements are being properly implemented, and that they remain fit for purpose. This ensures that the Framework and its constituent processes are subject to scrutiny by an objective third party, albeit one internal to the University.

5.5.2 Internal Audit

The University's risk management arrangements will also be subject to review as part of the internal audit process, carried out by auditors appointed at institutional level; currently PwC. Audits will take place on an ad-hoc basis; the last audit on risk management took place in 2019. This is an important assurance function carried out by an external authority on risk management.