RISK MANAGEMENT POLICY AND PROCEDURE

i. Purpose

This Risk Management Policy and Procedure forms part of the University's internal control and corporate governance arrangements.

The Policy explains the University's underlying approach to risk management, documents the roles and responsibilities of the Board of Governors, the senior staff, and other key parties.

The Procedure outlines key aspects of the risk management process, and identifies the main reporting procedures.

In addition, it describes the process the Board of Governors will use to evaluate the effectiveness of the institution's internal control procedures.

ii. Scope

The Risk Management policy and procedure applies to all University officers, staff, contractors, visitors and students. It applies to all current and future activities and opportunities.

1. Risk Management Policy

1.1 Policy statement

Taking sensible, calculated risks is essential for St Mary's to achieve its strategic aims and academic mission. The University has a responsible approach to risk management, seeking to recognise and manage exposure to risks, while accepting a degree of risk in line with potential reward.

1.2 Key principles

The following key principles outline the University's underlying approach to risk management and internal control:

- Risk management planning is considered an intrinsic part of the financial and strategic planning process across all departments at the University

- the Board of Governors has responsibility for overseeing risk management within the University as a whole

- there is an open and receptive approach to solving risk problems which is adopted by the Board of Governors

- the Vice-Chancellor and the senior staff team supports, advises and implements policies approved by the Board of Governors

- the University makes conservative and prudent recognition and disclosure of the financial and non-financial implications of risks

- all Heads of Faculty/Institutes and Departments (both academic and support services) are responsible for encouraging good risk management practice within their departments, and

- key risk indicators are identified and closely monitored on a regular basis, aided by the identification of early warning indicators.

2. Risk Management Procedure

2.1 Roles and responsibilities

The University adheres to Office for Students guidance on the role of the Board of Governors and senior staff regarding risk management.

Position/role	Responsibility
Board of Governors	Sets the tone and influences the culture of risk management within the University: • Determine the University's appetite for risk as a whole or on any relevant individual issue • Determine what types of risk are acceptable and which are not • Setting the standards and expectations of staff with respect to conduct and probity • Determine the appropriate risk appetite or level of exposure for the University • Approve major decisions affecting the University's risk profile or exposure • Monitor the management of significant risks to reduce the likelihood of unwelcome surprises • Establish the University Audit Committee, delegating authority for risk management and monitoring to the committee and satisfying itself that the less significant risks are being actively managed, with the appropriate controls in place and working effectively • Periodically review the University's approach to risk management and approve changes or improvements to key elements of its processes and procedures and • Report annually on the institution's approach to risk management, with a description of the key elements of its processes and procedures.

Position/role	Responsibility
Senior Leadership Team (SLT)	• Implementing risk management policy (including approving this Policy and Procedure) and internal control. A member of SLT, namely the Chief Financial Officer, Chairs the Risk Management Group • Identify and evaluate on a regular basis the significant risks faced by the University, and review risks identified on the Strategic Risk Register, for consideration by the Board of Governors • Provide adequate information in a timely manner to the Board of Governors and its committees on the status of risks and controls and • Undertake periodic reviews of the effectiveness of the system of internal control and provide a report to the Board of Governors
Director Strategic Planning	The Director Strategic Planning is the staff member with overall responsibility for the risk management process, including: • providing impetus and drive to the process to ensure the implementation timetable is achieved • ensuring Risk Management is embedded throughout the University • the administration and coordination of the risk management process, including acting as the main conduit of risk reporting between staff and the Risk Management Group, and • ensuring University staff receive appropriate training on risk management as and when required.
University Executive Committee	• Operationally manages the University's strategic risks • Maintains the University Strategic Risk Register

Position/role	Responsibility
Risk Management Group (RMG)	• The Risk Management Group (RMG) is responsible for the implementation of the risk management process, including: • On behalf of the University Executive Committee, the operational management of the University's risks in accordance with this policy, particularly those on the University Strategic Risk Register, identifying and implementing (if possible) coordinated actions to improve risk management • the assessment and management of other risks as they arise, escalating risks and opportunities to SLT as appropriate • monitoring the adequacy of risk management at the University, including of this policy and procedure and Departmental and Strategic Risk Registers (and the mitigating actions listed for each Strategic Risk), and making recommendations for improvement to SLT as and when required • communicating messages related to risk management to group members' respective areas as and when required supporting and advising the SLT and the Audit Committee on the progress of risk management across the University
Audit Committee	• A Committee of the Board of Governors, having delegated authority to monitor and report to the Board on internal risk controls, alerting Governors to any emerging issues • Oversees internal audit, external audit and management as required in its review of internal controls and Provides advice to the Board on the effectiveness of the internal control system, including the University's system for the management of risk.
Strategic Risk owners	• Are responsible for the high-level management of each of the risks on the Strategic Risk register, including ensuring risk profiles are up-to-date and reflect the current environment, and designing and managing the mitigating actions. • Provide the RMG a report on the status of the Strategic Risk, particularly if the risk event has actually occurred. • Provide the RMG a report on progress of the mitigating actions for each Strategic Risk, particularly noting any completed actions.
All University staff	• Are responsible for managing risk proportionate to their own work and area of authority • Familiarise themselves and comply with University policies and procedures • Report any risks arising in their work areas to their line management/RMG member as appropriate, and • Are responsible for ensuring they fully understand their risk management-related roles and responsibilities.

2.2 University risk appetite

In order to achieve its strategic aims and mission the University will have to accept a degree of risk. The risk that the University is willing to take should be within agreed tolerances for risk appetite. The risk appetite defined by the University, and agreed with the Board of Governors, may vary across different risk areas.

The Audit Committee must receive details of the University's risk appetite on an annual basis so that they are able to assure themselves of the University's level of risk exposure.

For definitions of the University's risk appetite thresholds and current risk appetite against each of the key risk areas, see Appendix 1.

2.3 Risk Registers

The Strategic Risk Register, Emerging Risk Register and Opportunities Register are stored centrally by the Strategic Planning team.

All Departments (Faculty/Institutes and Services) should develop a risk register using the template at Appendix 2 as a guide which encompasses the major risks to their area of business as part of the annual business planning process. All projects, programmes and area objectives outlined in the Delivery Plan should manage or mitigate the risks outlined in the Department risk register.

2.3.1 IT projects

A risk and issues log should be developed and maintained for all IT projects which identify critical issues, mitigating actions and timeframes, and which is regularly reviewed and updated as appropriate by the project manager.

2.4 Identifying risks

The following steps should be taken to identify and document risks and mitigating actions:

1. Identify risks to achieving the project/programme objectives. See "Risk identifiers" below for examples of sources of risk.
2. Analyse the risk. Gain an understanding of the risk by completing the risk register template at Appendix 4. Determine the risk owner. Examine the causes of the risk and the consequences if the risk should eventuate. Also consider the controls (ie mitigating actions), if any, which are already in place to mitigate or manage the risk.
3. Rate the risk. Determine the impact and probability of the risk based on the assessment in step 3. Allocate a rating of 1-5 for each of probability and impact, based on the assessments outlined in the matrices (see Appendix 3). An overall score is then calculated (the gross risk) using these ratings which, when considered against the University's risk appetite for the category of risk, determines the level and urgency of the mitigation and monitoring activities to be undertaken.
4. Determine any further mitigating actions that will be taken to manage or treat the risk. These should include programmes and projects in the Delivery Plan. Any high-priority actions should be highlighted (see note).

5. Rate the probability and impact of the risk once the mitigating actions identified in step 4 have been implemented (the net risk).

Note: Progress against the mitigating actions will be monitored at Risk Management Group meetings. Risk owners will provide an update on the mitigations, with any completed actions logged by RMG Secretariat.

An annual meeting of the University Executive Committee (see Appendix 4) is attended by members of the SLT/risk owners to consider and re-evaluate the Strategic Risk Register, with changes made as appropriate. New risks will also be considered.

2.4.1 Risk identifiers

The following are example sources of risk which may be considered when identifying risks involved in programmes or projects.

- SWOT/PESTLE analyses at Department and University level:
  - New/changed legislation
  - Political environment
  - Market conditions
  - Infrastructure (including physical and IT infrastructure)
  - Reputation and public perception
  - Organisational culture
  - Resources available
  - Contractual arrangements
  - Audit outcomes.
- Reviews of policies/procedures, business plans, risk registers, assurance maps etc.
- Management/subject matter expert assessments.

Potential risks should be categorised according to key risk areas as defined by the University:

- Financial Health and Investments
- Strategic Investments (ie projects)
- Education and Student Experience
- Research and Enterprise
- Development and Commercial Activity
- Partnership and External Collaboration.

2.5 Risk reviews

In addition to the annual cycle outlined in Appendix 3 the practice of risk management is implied within the agenda of SLT weekly meetings. A formal review of the Strategic Risk Register takes place quarterly at a meeting of the SLT.

Risk should be a standing agenda item at Faculty/Institutes and Services meetings. Directors/Heads of Area should regularly monitor and manage risks at a local level and review their area's risk registers at least every 6 months, making updates as required. Individual management reviews by project managers of risks associated with particular projects are ongoing and communicated appropriately.

The SLT manages the University's strategic risks and undertakes regular reviews of the Strategic Risk Register, making changes and updates as required. A formal review of the register as a whole takes place at the University Executive Committee annually (see *2.4 Identifying risks*).

The RMG monitors and maintains the Strategic risk register, Emerging risk register and Opportunities register at each meeting, escalating issues where required (see "Risk escalation" below).

2.6 Risk escalation

St Mary's management below SLT level (ie Directors/Heads of Faculty/Institutes and below) are able to refer operational risks which have been identified as being beyond its authority or ability to manage to the attention of their line management or the RMG. RMG are then able to escalate risks which they view as requiring additional high level management attention and action to SLT.

If SLT view the escalated risk as being of sufficient severity and relevance to the University as a whole it will be added to the Strategic Risk Register for ongoing management and monitoring.

2.7 Removing risks from Risk Registers

2.7.1 Departmental Risk Registers

Departmental Heads are able to make the decision to remove a risk from their Departmental Risk Register if they feel that the risk is no longer relevant to the operation of their area or has been mitigated sufficiently to warrant removal. This decision is to be discussed with the relevant member of the SLT for their approval.

2.7.2 Strategic Risk Register

SLT may decide to remove a risk from the Strategic Risk Register as a result of mutual consent from SLT members or a submission from the relevant risk owner.

2.8 Risk management as part of the system of internal control

The system of internal control incorporates risk management. This system encompasses a number of elements, listed below, that together facilitate an effective and efficient operation, enabling the University to respond to a variety of operational, financial, and commercial risks.

For details on roles and responsibilities of University staff (including the Board of Governors) regarding risk management, see *2.1 Roles and responsibilities*.

2.8.1 Policies and procedures

Attached to significant risks are a series of policies that underpin the internal control process. The policies are set by the Board of Governors and implemented and communicated by University management to staff. Written procedures support the policies where appropriate.

2.8.2 Risk Management Group (RMG)

The Risk Management Group (RMG) consists of staff from across the Faculty/Institutes and Services, providing a detailed level of scrutiny of the Strategic Risk register and risk management across the university. Any issues requiring decision or action are escalated to the University Executive Committee (UEC). RMG's detailed reporting lines are outlined below.

<u>Audit Committee</u>
- RMG Chair reports to Audit Committee on proceedings after all RMG meetings, and provides a high level update on the status of each strategic risk
- RMG reports to the Audit Committee on risk management from a compliance perspective eg on compliance issues it has identified and a comparison of the current residual risk to the risk appetite. It also provides the full set of papers from the previous meeting (strategic risk register, emerging risk register, and opportunities register) for the Committee's information.

<u>UEC</u>
- RMG Chair reports to UEC on proceedings after all meetings, and tables an UEC Committee Summary sheet outlining recommendations and items for UEC consideration after each meeting
- UEC is updated via the RMG Chair to the RMG on the progress of action implementation.

<u>SLT</u>
- RMG and/or UEC makes recommendations to the UEC on any areas where it deems higher-level management action is required to make improvements to risk management or to capitalise on opportunities as they arise.

Members are required to attend at least 4 of 5 scheduled RMG meetings annually. A delegate should be nominated in cases where members cannot attend. The group monitors and reports on attendance on an annual basis.

2.8.3 Regular reporting

Comprehensive regular reporting is designed to monitor key risks and their controls. Decisions to rectify problems are made at regular meetings of the RMG, SLT and the Board of Governors, as appropriate.

2.8.4 Planning and budgeting

The planning and budgeting process is used to agree objectives, action plans, and allocate resources. Progress towards meeting Faculty/departmental objectives is monitored regularly.

2.8.5 Strategic Risk Register

The Strategic Risk Register is compiled by the SLT and identifies and assesses risks significant to the University. The document is formally appraised annually with emerging risks added as required, and mitigating actions and risk indicators are monitored regularly through the SLT and the University Executive Committee.

2.8.6 Emerging Risks Register

Risk Management Group formally identifies and documents emerging risks on an Emerging Risk Register to enable the proactive management of future issues as part of an active, pre-emptive approach to risk management across the institution.

The emerging risks identified and documented in the registers will be reviewed by RMG at each future meeting. The trajectory of each emerging risk will also be discussed by the group.

Below are the criteria for rating emerging risks, including for inclusion on the main risk register.

Criteria for rating emerging risks

Criteria	Rating and Priority		
a. Likelihood of risk occurring	Possible	Unlikely	Unlikely
b. Level of exposure to risk	High	Moderate	Low
c. Ability to respond to risk	Unable/very limited	Limited	Good
d. Timeframe	Short (under 1 year)	Medium term (12 months – 2 years)	Long-term (2+ years)
Rating	High (Priority – 1)	Medium (Priority – 2)	Low (Priority – 3)

Threshold definitions

Rating	Definition
Low	Review to ensure continued relevance, consider removal from register
Medium	Keep on "emerging risks" register and continue to review for future changes
High	Consider a move from emerging to main risk register for active management/mitigation

2.8.7 Emerging Opportunities Register

RMG will identify current and future opportunities and formally document them on an Opportunities Register in order for the University to benefit from them. These opportunities will then be flagged with the University Executive Group and taken forward as appropriate.

The opportunities identified and documented in the registers will be reviewed by RMG at each future meeting.

Below are the criteria for rating and prioritising emerging opportunities.

Emerging Opportunities
Criteria for rating emerging opportunities

Criteria	Rating and Priority		
a. Likelihood of opportunity crystallising	Likely	Possible	Unlikely
b. Advantage to institution	High	Moderate	Low
c. Ability to respond to opportunity	Able	Limited	Unable/very limited
d. Timeframe	Short term (under 1 year)	Medium term (12 months – 2 years)	Long term (2+ years)
Rating	High (Priority – 1)	Medium (Priority – 2)	Low (Priority – 3)

Rating definitions

Rating	Definition
High	Consider taking action/developing action plan to make the most of the opportunity
Medium	Keep on register for noting/observation and revisit for future changes (particularly to timeframe)
Low	Review to ensure continued relevance, consider removal from register

2.8.8 Faculty/Departmental Risk Register

Heads of Faculty/Institutes and Departments, both academic and support services, develop and use this Register to ensure that significant risks in their areas of responsibility are identified, assessed and monitored. The emerging risks are added as required, and mitigating actions and risk indicators are monitored regularly by departments.

2.8.9 Assurance map

The assurance map, coordinated by Strategic Planning and confirmed by the SLT, is used to assess the effectiveness of all activities, systems and processes ("sources of assurance") in place

within the University at mitigating identified Strategic Risks. It identifies areas which require additional management attention or which may be over-covered. The map is regularly monitored by RMG with recommendations made to SLT to address any issues identified. See Appendix 3 for more information and examples of sources of assurance.

2.8.10 Internal audit programme

Internal audit is an important element of the internal control process. Apart from its normal programme of work, internal audit is responsible for aspects of the annual review of the effectiveness of the internal control system within the organisation. The Risk Register informs the internal audit plan.

2.8.11 External audit

External audit provides some feedback to the Audit Committee on the operation of the internal financial controls reviewed as part of the annual audit.

2.8.12 Third party reports

From time to time, the use of external consultants may be necessary. The appropriate use of specialist third parties for consulting and reporting can increase the reliability of the internal control systems.

2.9 Periodic review of effectiveness

Risk owners
If the risk event has actually occurred, a review of the risk profile and analysis of the approach to managing the risk (eg whether the mitigations were in place and effective) by the risk owner is triggered. See 2.9.2 *Testing mitigating actions and raising issues* below for the process to be followed in this instance.

Risk Management Group

The RMG has the ability to commission a review of departmental risk registers by calling upon appropriate risk owners to present their risk management approach and test the mitigation actions in place.

Project managers of "major" projects may also be called upon by RMG to report on risk management in the project. If one or more of the following criteria are met (apart from criteria 4, which should be in combination with one or more of the other criteria), the project is considered a "major" project and is reportable to RMG.

Note: this is indicative guidance for reporting project-related risks. The appropriateness of using this guidance for some projects (depending on project size, cost and timeframes) may require further discussion between the Project Manager and Strategic Planning.

2.9.1 "Major"/reportable project criteria

1. Total project budget is £250 000 or above

2. Innovative or contentious, with a potential high impact on University reputation or staff and/or student morale. See the risk rating matrices at Appendix 3 for the University's definition of "high impact"
3. High level of complexity, involving:
    a. Two or more different departments, and/or
    b. New technology which may require integration with existing systems, and/or
    c. New or changed business-critical technology, and/or
    d. Major changes to current work practices.
4. Urgent/timing (in combination with one or more of the other criteria):
    a. Delivery is required to meet a statutory/legislative deadline, or
    b. Project will require a year or more to complete, or
    c. Is time-critical for other reasons.

2.9.2 Testing mitigating actions and raising issues

The following steps will be taken to test mitigating actions and raise concerns:

1. Risk owners identify the key mitigating actions from the register, including milestones and due dates (there may be mitigating actions which are less effective than others at mitigating risks, or that are out of risk owner's control)
2. Risk owners provide the RMG a report on the following if called on to do so, or if the risk event has actually occurred:
    - The status of each key mitigating action and how effectively it is working to address the risk eg. number of students recruited as a result of implementing a Clearing strategy
    - Any factors which are preventing the mitigating action progressing, if relevant, and what is or could be done to address these issues

RMG is able to provide feedback on report and assistance if necessary. If RMG deems it necessary, concerns may be reported to SLT via RMG Chair/Lead Officer.

If the operational/strategic risk owner or a delegate has not attended the RMG meeting this prevents discussion involving the risk owner and it is not appropriate or possible for RMG to approve the risk in this instance. The relevant risk profiles will be submitted as draft to UEC with the note that final approval is pending these discussions.

Audit Committee

The Audit Committee receives reports on risk management at each meeting which it communicates to the Board through its report and minutes, identifying significant risks as they arise. The Board receives the Annual Risk Management Monitoring Report together with the final progress report on the Annual Delivery Plan, typically at its summer meeting each year.

Board of Governors

The Board of Governors is responsible for reviewing the effectiveness of internal control of the institution, based on information provided by the senior staff. Its approach is outlined below.

In reviewing the effectiveness of the internal control of the University the Board will consider the following aspects:
Control environment:

- the University objectives as set out in its Corporate Plan and Annual Operating Statement and its financial and non-financial targets

- organisational structure and calibre of the University management at all levels

- culture, approach, and resources with respect to the management of risk

- delegation of authority and

- public reporting.

On-going identification and evaluation of significant risks:

- timely identification and assessment of significant risks

- prioritisation of risks and the allocation of resources to address areas of high exposure.

Information and communication:

A Risk Management Communication Strategy is set out in *Appendix 2.*

- quality and timeliness of information on significant risks and

- time it takes for control breakdowns to be recognised or new risks to be identified.

Monitoring and corrective action:

- ability of the University to learn from its problems
- commitment and speed with which corrective actions are implemented

Document Title	**Risk Management Policy**
Version	4.0
Person Responsible	Director Strategic Planning
Author	Elizabeth Bell
Committee review	Risk Management Group University Executive Committee Senior Leadership Team
Circulation	Audit Committee
Document date	March 2008
Last amended	23 May 2022
Effective from	1 December 2015
Review date	1 December 2022
History	See Appendix 7. History of changes

3. Glossary

Assessment Criteria	The criteria used to make sense of the risks identified; the quasi-probability under which the significance of risks is ranked in terms or likelihood of occurrence and the impact upon the organisation.
Controls	Management processes and techniques developed to control or regulate activity or processes that cause risk; such as how activities will or will not be done.
Early Warning System for Risk Indicators	A system for early warning of changing conditions which could affect the risk profile of the organisation (such as the likelihood of an opportunity or exposure becoming manifest).
Emerging Risk	A new or familiar factor, action or event which would adversely affect the institution's ability to achieve its strategic objectives, but which has not yet materialised.
Impact	The effect or consequence of a risk manifesting.
Inherent Risk (or Gross Risk)	The assessment of risk before the application of any controls, transfer or management responses.
Likelihood	The probability that a risk will now occur.
Operational Risk	An operational risk is the crystallisation of a factor, action or event that would adversely impact operational delivery of strategic objectives, such as a failure of or flaw in policies, procedures or systems. Such risks will normally be considered by Executive management.
Opportunity	A favourable factor, action or event which would allow the institution to move towards achieving its strategic objectives.
Residual Risk (or Net Risk)	The risk remaining after the effect of mitigating actions have been assessed on the inherent (gross) risk.
Risk Appetite	The degree of risk that the University is prepared to accept when conducting its business in order to achieve its strategic aims and academic mission.
Risk Assessment	The means of arriving at an understanding of what risks are important to the organisation.
Risk Assurance	Audit of both the management system of checks and balance and the process by which risks are forecast and monitored.
Risk Management	Ensuring all relevant risks are understood and prioritised; and ensuring information on risk is organised as to be useful for management purposes.
Risk Profile	The unique array of opportunities and exposures to the organisation.
Source of assurance	An activity, document (plan, policy, procedure etc), process etc that helps manage or mitigate a risk.
Strategic Risk	A strategic risk is the crystallisation of an internal or external factor, action or event that would adversely affect the institution's ability to achieve its strategic objectives. Such risks will normally be considered by the Board of Governors.

Appendix 1. Risk Appetite

Appetite Threshold	Description
Low Risk Appetite	The University is willing to proceed with a portfolio of activities providing that the exposure is not greater than either: - Financial Loss: 0%-1% of turnover as an investment or liability Or two of the following: - Staff resource: No more than 10 days of senior staff time (Spine point 46 and above) over and above everyday operational business or· - Reputation: Likely to have some negative local / regional damage to reputation or· - Finite land resource: Consider change of use for existing infrastructure but not new development
Medium Risk Appetite	The University is willing to proceed with a portfolio of activities in pursuit of achieving strategic aims providing that the exposure is not greater than either: - Financial Loss: 1%-5% of turnover as an investment or liability Or two of the following: - Staff resource: No more than 25 days of senior staff time (Spine point 46 and above) over and above everyday operational business or - Reputation: Likely to have significant negative local / regional damage and or some national damage to reputation or· - Finite land resource: Consider change of use for existing infrastructure and limited new development on areas of the estate where it is permitted
High Risk Appetite	The University is willing to proceed with a portfolio of activities in pursuit of achieving strategic aims providing that the exposure is not greater than either; - Financial Loss: 5% - 10% of turnover as an investment or liability Or two of the following: - Staff resource: No more than 45 days of senior staff time (Spine point 46 and above) over and above everyday operational business or· - Reputation: Likely to have significant regional or national damage to reputation or· - Finite land resource: Consider change of use for existing infrastructure and significant new development on areas of the estate where it is permitted that may impact on heritage areas of campus

St Mary's Risk Appetite

Key Risk Area	Rationale for Risk Appetite	Risk Appetite Threshold
Financial Health & Investments	- Performance against HEFCE financial PIs - Financial reserves - Performance of investments; - Pension and other liabilities. - Investments intended to bring secure long-term financial return - High risk investments are more likely to result in losses to the capital sum - Losses have to be recognised within the accounts and the measures required to compensate for these could jeopardise core activities	Medium
Strategic Investments (i.e. projects)	- Investment intended to support key strategic aims - Risk of under-investment may lead to loss of competitive position within the sector. (Examples include, investment in student accommodation, investment in a new student record system)	High
Education and student experience	- Key strategic aims associated with future financial security and academic mission/ Distinctiveness relates to this area; - Core business of the University so appetite should be higher than for other non-core activities – an approach taken by other Universities.	Medium
Research and Enterprise	- Growing area of business of the University accounting for small percentage of income (direct and indirect income). - Spread of activity across the University means the risk is spread along with the potential impact of relatively higher risk projects.	Medium
Development and Commercial Activity	- Current exposure & possible volatility in commercial environment. - Scale and scope of potential projects currently under consideration means that the appetite should be set lower to ensure the collective risk is limited for this area.	Medium
Partnership and external collaboration	- St Mary's mission in terms of the community means some risk should be taken for the greater public good; - Volatility of local partnership organisations and structures, as well as limited financial and staff resources at the disposal of the University means that some caution should be taken to limit risk appetite.	Medium

Completed by:	[name, title]	[date]
Approved by:	[name, title]	[date]

Appendix 2. Risk Register template

Risk	Risk owner	Risk category	Causes	Consequences	Early warning indicators	Probability	Impact	Risk score	Rating	Risk appetite	Mitigating actions	Residual probability	Residual impact	Residual risk score	Residual risk rating

Appendix 3. Risk rating matrices

	Impact	Financial Loss	Health & Safety	Business Interruption	Reputation	Regulatory	Service Delivery
1	*Insignificant*	Negligible (less than £50k)	Incident requiring no more than minor medical treatment	Negligible; Critical systems unavailable for less than one hour	Will not or unlikely to damage reputation	No legal or regulatory implications	Low impact on service delivery. Minimal disruption to one part of the organisation
2	*Minor*	50k to £500k or less than 1% of expenditure	Minor injury requiring medical treatment & some days lost	Inconvenient; Critical systems unavailable for several hours	Adverse local media coverage. Short term damage to reputation	Minor legal or regulatory concerns raised	Minor disruption. Significant disruption to one part of the organisation. Reprioritisation needed to ensure continuity of services.
3	*Moderate*	500k to £2m or 1-5% of expenditure	Likely to lead to reportable injury; possible hospitalisation & numerous days lost	Client dissatisfaction; Critical systems unavailable for less than 1 day.	Adverse regional media coverage.	Moderate legal or regulatory concerns raised	Major disruption. Significant disruption to more than one part of the organisation. Significant management action needed to recover.
4	*Major*	£2m to £9m or 5-25% of expenditure	Single death, serious injury or permanent disability to an individual.	Critical systems unavailable for 1 day or a series of prolonged outages	Adverse and extended national media coverage. Long term damage to reputation	Potentially serious legal or regulatory implications	Major disruption. Significant disruption to several parts of the organisation. Significant management action needed to recover.
5	*Catastrophic*	In excess of £9m or 25% of expenditure	Multiple fatalities or permanent disability/ill health. Possible prosecution by the HSE	Critical systems unavailable for more than a day (at a crucial time)	Sustained adverse media coverage at various levels. Long term damage to reputation and loss of confidence in the University. Possible inquiry.	Very serious legal or regulatory concerns	Significant disruption of the whole organisation. Serious disruption with impact on the strategic and operational activities of the University.

Likelihood		
1	*Rare*	May occur under exceptional circumstances. It could happen but probably never will.
2	*Unlikely*	Has not occurred before but could occur at some time in the next 10 years. 25% chance of occurring.
3	*Possible*	May occur at some point over 3 year period. History of occurrence at this/another similar University 25-50% chance of occurring.
4	*Likely*	Very difficult to control. Will probably occur more than once in the next 3 year period. 50-75% chance of occurring.
5	*Almost Certain*	Has recently occurred. Will occur this year. May occur at frequent intervals over the next 3 year period. More than 75% chance of occurring.

	Low	Acceptable	Unlikely to require specific application of resources; Manage by routine procedures. Monitor and review.
	Moderate	*Acceptable*	Unlikely to cause much damage and/or threaten the efficiency and effectiveness of the programme/activity. Treatment plans to be developed and implemented by operational managers. Manage by specific monitoring or response procedures.
	High	*Generally not acceptable*	Likely to cause some damage, disruption or breach of controls. Senior management attention needed and management responsibility specified; Treatment plans to be developed and reported to SLT
	Extreme	*Not acceptable*	Likely to threaten the survival or continued effective functioning of the programme or the organisation, either financially or politically. Immediate action required; Must be managed by senior management with a detailed treatment plan.

		Impact				
		1	2	3	4	5
Probability	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Appendix 4. Risk Management Communication Strategy

The strategy summarises how information about risk management at St Mary's University is communicated, using a typical annual cycle to demonstrate:

Date	Process	Stakeholders and communication method
Summer	The Strategic Risk Register is the subject of annual review at an annual University Executive Committee meeting, in conjunction with the approval of the Corporate Delivery Plan, Corporate Plan and Financial Forecasts	Board of Governors at summer meeting
Autumn	The revised Risk Register is published	To Heads of Faculty and Heads of Service and available to all staff via the intranet; to relevant external stakeholders (i.e. OfS)
November	Review by Audit Committee	Audit Committee meeting
February	Annual Planning Meetings, with each Head of Faculty and Head of Service: 'bottom up' risk assessment by operations, projects and functions	Each Head of Faculty and each Head of Service meeting with Senior Staff team using prescribed agenda including risk assessment
March	Review by Audit Committee, incorporating mid-year review of Risk Register	Audit Committee meeting
June	Review by Audit Committee, incorporating preparation for year-end review by Board of Governors	Audit Committee meeting

Appendix 5. Risk Assurance mapping

<u>Layout of the Risk Assurance Map</u>
The Risk Assurance Map lists the following elements:
- All Strategic Risks as per the University's Risk Register
- Strategic Risk owners and
- University risk appetite for each risk
- All the sources of assurance of risk management that are relevant to the University in 3 "lines of defence":

  1. <u>Business management (first line)</u> which includes all the activities that constitute day-to-day planning, operational tasks and management controls and outputs.
  2. <u>Functional/corporate oversight (second line)</u> which includes reviews of compliance with relevant legislation, management structures and management review, and
  3. <u>Independent sources of assurance (third line)</u>.

There are two complementary ways to set out this information. Both versions should be maintained to inform management decisions:

Version 1: lists by type/category of assurance (eg data and reporting, systems, management controls etc) which provides a high level snapshot (heat map) of broader areas which may require additional resources, and those which may be over covered.

Version 2: feeds into version 1. Individual sources of assurance are listed and rated against the relevant risks. This provides a picture of how relevant each source is to a risk and identifies specific areas for improvement.

<u>Example sources of assurance</u>
- <u>First line: business management:</u> delivery plans, project delivery, systems (eg. HR, Finance), data/reporting, procedures and special projects.
- <u>Second line: functional/corporate oversight:</u> PCBs, upper management committees/meetings, It system controls and policies.
- <u>Third line: independent sources of assurance.</u> Examples include internal and external audit, governance structures, and external regulation.

<u>Assurance ratings</u>
Each type of assurance is RAG rated according to the effectiveness of the cover it provides.
- Green: source of assurance assessed as adequate
- Yellow: some concerns over adequacy of source of assurance
- Red: serious/significant concerns over the adequacy of source of assurance
- Purple: source applicable and but does not exist or is under development, but not yet completed/functional
- White: source of assurance not applicable to risk.

The assurance level of each source of assurance and the overall level of assurance are RAG rated using the system below as guidance, although risk owners are able to adjust the rating outcome if required.

Risk appetite	Red (significant concern over assurance)	Amber/yellow (some concern over assurance)	Green (adequate assurance)
Low	<70% total adequate (green) sources of assurance per type	70-90%	>90%
Medium	<60%	60-80%	>80%
High	<50%	50-70%	>70%

Risk Appetite

The University's risk appetite is used to determine whether the level of assurance is adequate. Actions to improve the assurance can then be identified eg. increasing project funding, new areas of focus for projects, additional internal audit activity, reviews of compliance, production of additional data/information required etc.

Review of Risk Assurance Map

The Risk Assurance Map is regularly reviewed and updated by the University's Risk Management Group.

Appendix 6. Risk Management Checklist for Project Managers

Section A. This section provides a checklist of one-time risk management activities which should be undertaken during the project planning phase.

1. The Project Manager has considered risk appropriately during project planning by undertaking the following tasks:	☐
a) Confirmed whether the project meets the criteria of a major/reportable project (see point 2.9 of the Risk Management Procedure)	☐
b) Identified relevant risk factors (preferably in consultation with project team)	☐
c) Completed the risk register template for the project (Appendix 2 of the Risk Management Procedure) to ensure understanding of the risk, causes, consequences, severity and potential impact	☐
d) Prioritised the identified risks according to severity and potential impact	☐
e) Developed a risk management plan which outlines appropriate mitigating actions for each of the identified risks, including responsible officers, milestones and due dates, and defines trigger for implementing mitigating actions	☐
f) Updated the project plan/schedule to include mitigating actions and additional reporting requirements for a major/reportable project if necessary (see 1a)	☐
g) Identified project team member responsible for maintaining the project risk register	☐
h) Has submitted the risk register for review and signoff by the relevant party (Head of Department, SLT or SLT member)	☐
2. Project team has been trained on risk management (optional)	☐
3. The risk register has been circulated to all project team members	☐
4. The risk register is available to all project team members	☐

Section B. This section provides a checklist of risk management activities which should be undertaken on a regular basis throughout the life of the project.

Review and update the project risk register on a regular basis	☐
Ensure sufficient information is documented to allow understanding of project risks and mitigating actions	☐
Reprioritise risks as required	☐
Update the project plan to reflect any impact on resources, timing etc arising from risk management	☐
Implement actions to mitigate any new risks which meet defined trigger (see 1e)	☐

Appendix 7. History of changes

Version	Date	Section	Changes/updates
4.0	23/08/22	Procedure	Version history • Changes made as per the recommendations of the internal audit into the governance of Risk Management • Updated Responsible Officer • Made corrections to version history (corrected page numbers etc) • Updated Committee Review and Circulation
			2.1 Roles and responsibilities • Added details on the roles and responsibilities of Strategic Risk owners, including on providing updates on progress of mitigating actions for Strategic Risks • Clarified the role of the Board of Governors in risk management at the university
			2.4 Identifying risks • Clarified the process to identify and monitor mitigating actions, including requirement of risk owners to provide progress updates at RMG meetings and for Secretariat to log completed actions.
			2.8 Risk management as part of the system of internal control • Added detail on the Risk Management Group's reporting lines to University Executive Committee and Audit Committee • Clarified role of UEC and SLT as it relates to the Risk Management Group's reporting lines • Corrected RMG meeting attendance requirements
			2.8.2
			2.8.6 Emerging Risk Register • Changed rating "system" for emerging risks to "High/Medium/Low" as per agreement at RMG (April 2022)
			2.8.7 Emerging Opportunities Register • Changed rating "system" for emerging opportunities to "High/Medium/Low" as per agreement at RMG (April 2022)
3.5	31/01/22	Procedure	2.8 Risk management as part of the system of internal control • Added detail on the role of the Risk Management Group and meeting attendance requirements for RMG members • Added further detail on the process of identifying and documenting emerging risks and opportunities

	10/12/21	Procedure	2.9 Periodic review of effectiveness
			• Added points of procedure in relation to:
			   ○ Triggering review of mitigating actions in case where risk has occurred
			   ○ Submitting profile to UEC as draft where risk owner is not present to lead discussion at RMG meeting

3.4	01/09/21	General	• Updated references to Faculties, UEC and other governance arrangements to reflect current management structures
		Procedure	• 2.3.1 Risk Register ○ Addition of policy related to issues and risk logs for IT projects
			• 2.9 Major Project descriptors ○ Note added for guidance to descriptors
3.3	29/11/18	General	• Removed references to HEFCE, updated to Office for Students (OfS) where appropriate
		Procedure	• 3. Glossary ○ Addition of new, separate "operational" and "strategic" risk definitions

3.2	09/09/17	Procedure	• 2.4.1 Risk identifiers
			   ○ Addition of "audit outcomes" as a risk identifier
			• 2.9.1 "Major"/reportable project criteria
			   ○ Addition of reference to "high impact" definition in Appendix 3
			• Replaced term "areas" with "departments"

3.1	10/07/17	Policy	• 1.2 Key principles • Addition of key principle on risk management being an intrinsic part of the planning process

		Procedure	• 2.1 Roles and responsibilities
			   ○ Reference to Board of Governors' delegated risk management authority to Audit Committee
			   ○ Addition of role of Chief Operating Officer as Chair of RMG
			   ○ Addition of Director Strategic Planning responsibility to act as main conduit for risk reporting between staff and RMG
			   ○ Change to RMG responsibility re risk registers – management and maintenance of University Strategic Risk Register (rather than departmental risk registers)
			   ○ Addition of RMG members' responsibility to communicate messages related to

			risk management as required
			○ Addition of section on Directors Forum responsibilities regarding risk management
			○ Addition of section on responsibilities of all staff regarding risk management
			• 2.4 Identifying risks
			○ Addition of detail regarding an annual meeting of the Directors Forum to formally review Strategic Risk Register
			• 2.5 Risk reviews
			○ Addition of line that risk should be standing item at Schools/Services meetings
			○ Addition of Directors Forum role in conducting risk reviews
			○ Change to RMG role from responsibility for "departmental" to "Strategic" risk register
			• 2.9 Periodic review of effectiveness
			○ Addition of RMG role in testing mitigating actions and process to test these
			○ Addition of "major" or reportable project criteria
			• Appendix 4 Risk Management Communication Strategy
			○ Addition of detail regarding Strategic Risk Register review at annual Directors Forum meeting
			○ Addition of Appendix 6. Risk Management Checklist for Project Managers
3.0	31/03/17	General	• Formatting – addition of table of contents, other general reformatting (headings etc)
			• Separation of Policy statement and Procedure document
			• Addition of Scope statement for Policy and Procedure
		Policy	• Addition of general policy statement on risk management to underpin the Key Principles
			• Removed paragraph on "residual risk" definition (this is already defined in section 3. Glossary)
			• Removed "Benefits of Risk Management" –

			general points only
			• Formatting – addition of headings and section numbers
		Procedure	• Formatting – headings, new section titles and renumbering (removed paragraph numbering), tables
			• 2.1 Roles and responsibilities:
			o Renamed from "Role of the senior staff" and renumbered
			o Formatted into tables
			o Addition of statement on adherence to HEFCE guidance on role of Board of Governors
			o Reworded "senior staff" to "Senior Management Team" to reflect current management arrangements
			o Clarification of role of Chief Operating Officer, Head of Corporate Planning, Risk Management Group (RMG) and Audit Committee
			• 2.2 University risk appetite
			o Addition of statement on University's risk appetite
			o Addition of associated appendix (Appendix 1) with current risk appetite thresholds and risk appetite
			• 2.3 Risk registers
			o New procedure on development of risk registers and role of Strategic Planning team in managing risk registers
			• 2.4 Identifying risks
			o New section outlining procedure to undertake to identify and document risks
			o New section outlining sources of risk (risk identifiers) and University's risk categories
			• 2.5 Risk reviews
			o New section outlining process for risk register reviews at all management levels
			• 2.6 Risk escalation
			o New section outlining process to escalate newly identified risks for more senior management if and when

			required
			• 2.7 Removing risks from Risk Registers
			o New section outlining process for removal of risks from risk registers as and when appropriate, including authority required to do so
			• 2.8 Risk management as part of the system of internal control
			o Renumbered
			o Addition of references to SMT (replacing "senior staff") and RMG
			o 2.8.4 renamed to "Strategic Risk Register"
			o New subsection on University Assurance Map
			• 2.9 Periodic review of effectiveness
			o Paragraph on role of Audit Committee moved to beginning of section; Board of Governors paragraph moved underneath
			• 3. Glossary
			o Renumbered
			o Renamed from "Risk definitions and glossary of terms"

			o New definitions added:
			        ▪ Risk appetite
			        ▪ Source of assurance

			o Definition of "residual risk" updated
			o Definition of "risk" updated to align to HEFCE definition
		Appendices	• University Risk Appetite guidance (as tabled at SMT) added as Appendix 1
			• Risk Register template inserted as Appendix 2
			• Risk rating matrices added at Appendix 3
			• "Risk management communication strategy" renumbered to Appendix 4
			• Guidance to risk assurance mapping added as Appendix 5.

2.0	02/09/16	**Role of the Senior Staff**	• Updates to role of Head of Corporate Planning
1.0	30/10/15		• Original document