

## RISK MANAGEMENT POLICY AND PROCEDURE

i. Purpose .....	3
ii. Scope .....	3
1. Risk Management Policy.....	3
1.1 Policy statement .....	3
1.2 Key principles .....	3
2. Risk Management Procedure.....	5
2.1 Roles and responsibilities .....	5
3.1 Risk management as part of the system of internal control.....	8
3.1.1 Planning and budgeting .....	8
3.1.2 Faculty/Departmental-level Risks .....	8
3.1.3 Strategic Risk Register.....	8
3.1.4 Policies and procedures .....	8
3.1.5 Risk Management Group (RMG).....	9
3.1.6 Regular reporting .....	9
3.1.7 Emerging Risk Register .....	9
3.1.8 Emerging Opportunities Register .....	10
3.1.9 Internal audit programme .....	10
3.1.10 External audit.....	10
3.1.11 Third party reports.....	10
4.1 University risk appetite .....	10
5.1 Risk Registers .....	11
5.1.1 IT projects .....	11
6.1 Identifying and analysing risks .....	11
6.1.1 University risk appetite .....	12
6.1.2 Risk identifiers.....	12
7.1 Risk reviews .....	12
8.1 Risk escalation .....	13
9.1 Removing risks from Risk Registers .....	13
9.1.1 Strategic Risk Register.....	13
10.1 Periodic review of effectiveness.....	13
10.1.1 "Major"/reportable project criteria .....	14
10.1.2 Testing mitigating actions and raising issues.....	14
11. Glossary .....	17
Appendix 1. Risk Appetite .....	17
Appendix 2. Risk Register template.....	21
Appendix 3. Risk rating matrices .....	22
Appendix 4. Criteria for assessing emerging risks and opportunities .....	24

Appendix 5 . Risk Management Communication Strategy .....	25
Appendix 6. Risk Management Checklist for Project Managers.....	27
Appendix 7. History of changes .....	29

## **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, key committees, 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**

The University is required to have in place adequate and effective management arrangements to ensure compliance with the Office for Students' Conditions of Registration and to deliver the public interest governance principles applicable to it, as defined by the OfS. This includes adequate management of financial, strategic and operational risks, and monitoring and reporting of changes and emerging risks.

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 University manages the risks it faces effectively in order to ensure that statutory obligations are met, and to safeguard its students, staff and others to whom it has a duty of care.

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

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

- To align risk management with the University's objectives set out in the annual operating plan and Vision 2030.
- the Board of Governors has responsibility for ensuring proactive and effective 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 University learns from previous threats, opportunities, successes and failures to inform the future management of risks
- the University makes conservative and prudent recognition and disclosure of the financial and non-financial implications of risks
- all Deans and Directors (both academic and professional 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
- the University encourages a proactive approach to risk which supports transparency, open discussion and learning from past risks and opportunities to inform future management.

## 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.

<b>Position/role</b>	<b>Responsibility</b>
Board of Governors	<p>Sets the tone and influences the culture of risk management within the University:</p> <ul style="list-style-type: none"><li>• Determine what types of risk are acceptable and which are not, the likelihood of unacceptable risks occurring, and how unacceptable risks should be managed</li><li>• Setting the standards and expectations of staff with respect to conduct and probity</li><li>• Determine the appropriate risk appetite or level of exposure for the University</li><li>• Approve major decisions affecting the University's risk profile or exposure</li><li>• Monitor the management of significant risks to reduce the likelihood of unwelcome surprises</li><li>• Establish the University Audit and Risk Committee (ARC), delegating authority for risk management and monitoring to the committee and satisfying itself that the significant risks are being actively managed, with the appropriate controls in place and working effectively</li><li>• Periodically review the University's approach to risk management and approve changes or improvements to key elements of its processes and procedures and</li><li>• Report annually on the institution's approach to risk management, with a description of the key elements of its processes and procedures.</li></ul>

<b>Position/role</b>	<b>Responsibility</b>
Senior Leadership Team (SLT)	<ul style="list-style-type: none"> <li>• Implementing risk management policy (including approving this Policy and Procedure) and internal control. A member of SLT, namely the Pro Vice-Chancellor (Enterprise) &amp; Chief Financial Officer (PVC), Chairs the Risk Management Group</li> <li>• 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</li> <li>• Provide adequate information in a timely manner to the Board of Governors and its committees on the status of risks and controls and</li> <li>• Undertake periodic reviews of the effectiveness of the system of internal control and provide a report to the Board of Governors</li> </ul>
University Secretary & Director Strategic Planning	<p>The University Secretary is the staff member with overall responsibility for the risk management process, including:</p> <ul style="list-style-type: none"> <li>• providing impetus and drive to the process to ensure the implementation timetable is achieved</li> <li>• ensuring Risk Management is embedded throughout the University</li> <li>• 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</li> <li>• ensuring University staff receive appropriate training on risk management as and when required.</li> </ul>
University Executive Committee	<ul style="list-style-type: none"> <li>• Operationally manages the University's strategic risks</li> <li>• Maintains the University Strategic Risk Register</li> </ul>

<b>Position/role</b>	<b>Responsibility</b>
Risk Management Group (RMG)	<ul style="list-style-type: none"> <li>• The Risk Management Group (RMG) is responsible for the implementation of the risk management process, including:</li> <li>• On behalf of the Senior Leadership Team, responsible for the identification, oversight and monitoring of the University's risks in accordance with this policy, particularly those on the University Strategic Risk Register, identifying and monitoring the implementation of coordinated actions to improve risk management</li> <li>• the assessment and management of other risks as they arise, escalating risks and opportunities to SLT as appropriate</li> <li>• monitoring the adequacy of risk management at the University, including of this policy and procedure and project and Strategic Risk Registers (and the mitigating actions listed for each Strategic Risk), and making recommendations for improvement to SLT as and when required</li> <li>• communicating messages related to risk management to group members' respective areas as and when required</li> <li>• supporting and advising the SLT and the Audit and Risk Committee on the progress of risk management across the University</li> </ul>
Audit and Risk Committee	<ul style="list-style-type: none"> <li>• A Committee of the Board of Governors, having delegated authority to monitor and report to the Board on internal risk controls. Receives the risk register and internal audit reports at each meeting and alerts Governors to any emerging issues Oversees internal audit, external audit and management as required in its review of internal controls andCritically challenges and reviews the risk management framework and the adequacy and effectiveness of controls to evaluate how well the arrangements are working</li> <li>• Provides advice to the Board on the effectiveness of the internal control system, including the University's system for the management of risk.</li> </ul>
Strategic Risk owners	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Provide the RMG a report on the status of the Strategic Risk, particularly if the risk event has actually occurred.</li> <li>• Provide the RMG a report on progress of the mitigating actions for each Strategic Risk, particularly noting any completed actions.</li> </ul>
All University staff	<ul style="list-style-type: none"> <li>• Are responsible for managing risk proportionate to their own work and area of authority</li> <li>• Familiarise themselves and comply with University policies and procedures</li> <li>• Report any risks arising in their work areas to their line management/RMG member as appropriate, and</li> <li>• Are responsible for ensuring they fully understand their risk management-related roles and responsibilities.</li> </ul>

### **3.1 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, outlined 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*.

#### *3.1.1 Three lines of assurance*

The University's risk management framework is structured around the "three lines of assurance" model which ensures roles and responsibilities for risk management are defined across all functions of the University.

1. Business management (first line) which includes all the activities that constitute day-to-day planning, operational tasks and management controls and outputs. This includes delivery plans, project delivery, systems (eg. HR, Finance), data/reporting, procedures and special projects.
2. Functional/corporate oversight (second line) which includes the University's strategic risk register, reviews of compliance with relevant legislation, management structures and management review. This includes Project Control Boards, upper management committees/meetings, IT system controls and policies.
3. Independent sources of assurance (third line). This includes internal and external audit, governance structures, and external regulation.

#### *3.1.2 Planning and budgeting*

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

#### *3.1.3 Faculty/Departmental-level Risks*

Local risks are expected to be managed by local managers, with Heads of Faculties and Departments ensuring that significant risks in their areas of responsibility are identified, assessed and monitored, and that issues are raised and escalated through relevant channels as necessary.

#### *3.1.4 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 reviewed annually with emerging risks added as required, and mitigating actions and risk indicators are monitored regularly through Risk Management Group (see 3.1.6), the SLT and the University Executive Committee.

#### *3.1.5 Policies and procedures*

Attached to significant risks are the University's policies which underpin the internal control process. The policies are set by University senior management and implemented and

communicated by University management to staff. Written procedures support the policies where appropriate.

### *3.1.6 Risk Management Group (RMG)*

The Risk Management Group (RMG) consists of staff from across the Faculties and Services, providing a detailed level of scrutiny of the Strategic Risk register, emerging risks and opportunities, and risk management across the university.

Deans and Directors sit on RMG and monitor the effectiveness of the risk management framework, and provide updates on the progress of mitigating actions at each meeting.

Any issues requiring decision or action are escalated to the University Executive Committee (UEC) and SLT. RMG's detailed reporting lines are outlined below.

#### Audit and Risk Committee

- RMG Chair reports to ARC on proceedings after all RMG meetings, and provides a high level update on the status of each strategic risk
- RMG reports to the ARC 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.

#### UEC

- 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.

#### SLT

- RMG and/or UEC makes recommendations to the SLT 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 80% (3 of 4) of scheduled RMG meetings annually. A delegate should be nominated in cases where members cannot attend. The group monitors attendance at each meeting.

### *3.1.7 Regular reporting*

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

### *3.1.8 Emerging Risk 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. Departments identify emerging risks as part of the planning process, and via RMG representation.

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.

The criteria for rating emerging risks, including for inclusion on the main risk register, are at appendix 4.

### *3.1.9 Emerging Opportunities Register*

RMG identifies current and future opportunities and formally documents them on an Opportunities Register in order for the University to benefit from them. Departments identify emerging opportunities as part of the planning process, and via RMG representation. These opportunities are then flagged with the University Executive Committee and taken forward as appropriate. They may also be integrated into departmental and University-wide planning to ensure they are aligned with resource planning and planning priorities.

The "high" and "medium" rated opportunities identified and documented in the register will be reviewed by RMG at each future meeting. "Low" rated items will be reviewed and included in RMG and other papers less frequently (for example, at every second meeting of RMG).

The criteria for rating and prioritising emerging opportunities are at appendix 4.

### *3.1.10 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 Strategic Risk Register informs the internal audit plan. Progress against the annual internal audit plan is monitored by the ARC at each meeting.

### *3.1.11 External audit*

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

### *3.1.12 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.

## **4.1 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 and Risk 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.

## 5.1 Risk Registers

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

All Departments should ensure that their risks are considered and evaluated as part of their annual planning, delivery and appraisal processes whether this be for business as usual, or a once-off project, particularly those meeting the criteria of a “major project” (see 10.1 *Periodic review of effectiveness*). Departments are encouraged to hold their own risk registers: 2.4 below outlines the process to identify and analyse the Department’s or project risks, and the risk register template at appendix 4 can be used to formally document them.

### 5.1.1 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.

## 6.1 Identifying and analysing risks

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

1. List the key risks to achieving the project/programme objectives. See “Risk identifiers” below for examples of sources of risk.
2. Analyse the key risks:
  - a. Determine the risk owner.
  - b. Identify the key risk area in the University’s risk appetite statement that the risk falls into (see 2.4.1 below). The risk appetite defines the extent to which the University is willing to take risks in that area.
  - c. Examine the causes of the risk.
  - d. Consider the consequences if the risk should eventuate.
  - e. Also consider the controls (ie mitigating actions), if any, which are already in place or underway to mitigate or manage the risk.
3. Use the risk rating matrices (appendix 3) to determine the probability of the risk occurring, and the impact it would have if it did, if no further action was taken to address it (ie the initial, or gross risk rating). The risk appetite definitions can also be used to guide the Department/team’s next steps ie whether to treat, tolerate (accept), transfer (for example via contracts, insurance, collaborations) or terminate (not begin or stop an activity) the risk.
4. Identify any further mitigating actions that will be taken to manage or treat the risk, including 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 (ie the residual/net risk). This rating reflects the level of confidence about the treatment of the risk.

Note: Progress against the mitigating actions will be monitored at Risk Management Group meetings where they are also mitigations for the University’s strategic risks. Risk owners or Deans/Directors will provide an update on the mitigations, with any completed actions recorded by RMG Secretariat.

### 6.1.1 University risk appetite

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

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

The results of the risk analysis should be compared with the risk appetite (the type and extent of risks that the University is willing to take) to determine the areas in which additional action is needed. For example, if a risk is assessed as exceeding the University's defined risk appetite, it may require additional mitigations to reduce its likelihood or impact, or a decision may be needed on whether to tolerate, transfer, or terminate the risk.

### 6.1.2 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 and other compliance requirements
  - Political environment
  - Market/sector conditions (demographics, demand, funding changes)
  - Infrastructure (including physical and IT infrastructure)
  - Reputation and public perception
  - Organisational culture
  - Resources available
  - Contractual arrangements
  - Audit outcomes
  - Supply chain/costs
  - Partnerships
  - Environment and sustainability
  - Knowledge management (eg staffing single point of failure, intellectual property, system malfunctions).
- Reviews of policies/procedures, business plans, risk registers (ie project risk registers, other HEIs' registers, the National Risk Register etc), assurance maps etc.
- Management/subject matter expert assessments.

## 7.1 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.

Risk should be a consideration at Faculty and Services meetings. Directors/Deans should regularly monitor and manage their area's risks at a local level. Individual management reviews by project managers of risks associated with particular projects are ongoing and communicated appropriately. Heads of Department and project managers report to Risk Management Group on the progress of mitigations and any emerging issues.

The SLT manages the University's strategic risks and undertakes regular reviews of the Strategic Risk Register, making changes and updates as required. An annual meeting of the SLT considers and re-evaluate the Strategic Risk Register, with changes made as appropriate. New risks will also be considered. The outcomes of this meeting are taken to UEC and Board.

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).

## **8.1 Risk escalation**

St Mary's management below SLT level (ie Heads of Department/Faculty and below) can refer critical issues or 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.

Governors via the Audit and Risk Committee receive reports on any escalated risks and issues at RAC meetings during the year.

## **9.1 Removing risks from Risk Registers**

### *9.1.1 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.

The RMG as a group may decide to recommend the removal of a strategic risk from the register, which will then be submitted to SLT for a final decision.

## **10.1 Periodic review of effectiveness**

### Risk management framework

The University's Risk Management framework is subject to a comprehensive review annually to ensure it remains effective, relevant, and aligned with institutional objectives and external regulatory requirements. The review takes place alongside the review of the Strategic Risk Register in September each year.

### 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

RMG's role is to ensure effective oversight and assurance that project risks are being appropriately managed. RMG receives risk updates from major projects but considers these by exception to avoid duplicating the work of Project Boards.

The RMG has the ability to commission a review of the Strategic risk register 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.*

#### 10.1.1 "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.

#### 10.1.2 *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 may provide feedback and assistance if required. 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 SLT/UEC with the note that final approval is pending these discussions.

### Audit and Risk Committee

The Audit and Risk 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 either its summer or early Autumn 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 4*.

- 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	<b>Risk Management Policy</b>
Version	4.3
Person Responsible	Director Strategic Planning
Author	Elizabeth Bell
Committee review	Risk Management Group University Executive Committee Senior Leadership Team
Circulation	Audit and Risk Committee
Document date	March 2008
Last amended	10 December 2024
Effective from	1 December 2015
Review date	1 December 2025
History	See Appendix 7. History of changes

## 11. Glossary

<b>Assessment Criteria</b>	The criteria used to make sense of the risks identified; the quasi-probability under which the significance of risks is ranked in terms of likelihood of occurrence and the impact upon the organisation.
<b>Controls</b>	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.
<b>Early Warning System for Risk Indicators</b>	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).
<b>Emerging Risk</b>	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.
<b>Impact</b>	The effect or consequence of a risk manifesting.
<b>Inherent Risk (or Gross Risk)</b>	The assessment of risk before the application of any controls, transfer or management responses.
<b>Likelihood</b>	The probability that a risk will now occur.
<b>Operational Risk</b>	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.
<b>Opportunity</b>	A favourable factor, action or event which would allow the institution to move towards achieving its strategic objectives.
<b>Residual Risk (or Net Risk)</b>	The risk remaining after the effect of mitigating actions have been assessed on the inherent (gross) risk.
<b>Risk Appetite</b>	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.
<b>Risk Assessment</b>	The means of arriving at an understanding of what risks are important to the organisation.
<b>Risk Assurance</b>	Audit of both the management system of checks and balance and the process by which risks are forecast and monitored.
<b>Risk Management</b>	Ensuring all relevant risks are understood and prioritised; and ensuring information on risk is organised as to be useful for management purposes.
<b>Risk Profile</b>	The unique array of opportunities and exposures to the organisation.
<b>Source of assurance</b>	An activity, document (plan, policy, procedure etc), process etc that helps manage or mitigate a risk.
<b>Strategic Risk</b>	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

<b>Appetite Threshold</b>	<b>Description</b>
<b>Low Risk Appetite</b>	<p>The University is willing to proceed with a portfolio of activities providing that the exposure is not greater than either:</p> <ul style="list-style-type: none"> <li>• Financial Loss: 0%-5% of turnover as an investment or liability</li> </ul> <p>Or two of the following:</p> <ul style="list-style-type: none"> <li>• Staff resource: No more than 10 days of senior staff time (Spine point 46 and above) over and above everyday operational business or</li> <li>• Reputation: Likely to have some negative local / regional damage to reputation or</li> <li>• Consider change of land use for existing infrastructure but not new development</li> </ul>
<b>Medium Risk Appetite</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• Financial Loss: 5-10% of turnover as an investment or liability</li> </ul> <p>Or two of the following:</p> <ul style="list-style-type: none"> <li>• Staff resource: No more than 25 days of senior staff time (Spine point 46 and above) over and above everyday operational business or</li> <li>• Reputation: Likely to have significant negative local / regional damage and or some national damage to reputation or</li> <li>• Consider change of use for existing infrastructure and limited new development on areas of the estate where it is permitted</li> </ul>
<b>High Risk Appetite</b>	<p>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;</p> <ul style="list-style-type: none"> <li>• Financial Loss: between 10% and no more than 20% of turnover as an investment or liability</li> </ul> <p>Or two of the following:</p> <ul style="list-style-type: none"> <li>• Staff resource: No more than 45 days of senior staff time (Spine point 46 and above) over and above everyday operational business or</li> <li>• Reputation: Likely to have significant regional or national damage to reputation or</li> <li>• 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</li> </ul>

## St Mary's Risk Appetite

Key Risk Area	Rationale for Risk Appetite	Risk Appetite Threshold
People and Culture	<ul style="list-style-type: none"> <li>SMU's staff are its most valuable asset: they are the driving force behind the University fulfilling its strategic objectives and achieving Vision 2030.</li> <li>SMU wants to empower its staff to reach their full potential by developing a supportive, inclusive, collaborative and inspiring work environment</li> <li>To ensure that the right people are in place at the right time, and that the University's employment model is flexible enough to adapt to emerging risks</li> </ul>	Medium
Financial Health & Investments	<ul style="list-style-type: none"> <li>Performance against HESA Key Financial Indicators</li> <li>Financial reserves</li> <li>Performance of investments</li> <li>Pension and other liabilities.</li> <li>Investments intended to bring secure long-term financial return</li> <li>High risk investments are more likely to result in losses to the capital sum</li> <li>Losses have to be recognised within the accounts and the measures required to compensate for these could jeopardise core activities</li> </ul>	Medium
Strategic Investments (i.e. projects)	<ul style="list-style-type: none"> <li>Investment intended to support key strategic aims</li> <li>Risk of under-investment may lead to loss of competitive position within the sector.</li> <li>(Examples include investment in student accommodation, investment in continued improvements to the SRS, new Medical School)</li> </ul>	High
Education and student experience	<ul style="list-style-type: none"> <li>Key strategic aims associated with future financial security and academic mission/distinctiveness/value proposition relates to this area;</li> <li>Core business of the University so appetite should be higher than for other non-core activities - an approach taken by other Universities.</li> </ul>	Medium
Research and Enterprise	<ul style="list-style-type: none"> <li>Growing area of business of the University accounting for small percentage of income (direct and indirect income).</li> <li>Spread of activity across the University means the risk is spread along with the potential impact of relatively higher risk projects.</li> </ul>	Medium
Development and Commercial Activity	<ul style="list-style-type: none"> <li>Current exposure &amp; possible volatility in commercial environment.</li> <li>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.</li> </ul>	Medium

Partnerships and external collaboration	<ul style="list-style-type: none"> <li>• St Mary's mission in terms of the community means some risk should be taken for the greater public good;</li> <li>• 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.</li> <li>• Increasing importance of developing robust Partnerships to diversify the University's sources of income</li> </ul>	Medium
Regulation and compliance	<ul style="list-style-type: none"> <li>• New regulatory criteria imposed following the introduction of the Office for Students which are subject to change.</li> <li>• A failure to meet these responsibilities could result in penalties, compromise the integrity of academic programmes, and damage the University's reputation among staff, students and other stakeholders</li> </ul>	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	<i>Insignificant</i>	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	<i>Minor</i>	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	<i>Moderate</i>	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	<i>Major</i>	£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	<i>Catastrophic</i>	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	<i>Rare</i>	May occur under exceptional circumstances. It could happen but probably never will.
2	<i>Unlikely</i>	Has not occurred before but could occur at some time in the next 10 years. 25% chance of occurring.
3	<i>Possible</i>	May occur at some point over 3 year period. History of occurrence at this/another similar University 25-50% chance of occurring.
4	<i>Likely</i>	Very difficult to control. Will probably occur more than once in the next 3 year period. 50-75% chance of occurring.
5	<i>Almost Certain</i>	Has recently occurred. Will occur this year. May occur at frequent intervals over the next 3 year period. More than 75% chance of occurring.

	<b>Low</b>	<b>Acceptable</b>	Unlikely to require specific application of resources; Manage by routine procedures. Monitor and review.
	<b>Moderate</b>	<b>Acceptable</b>	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.
	<b>High</b>	<b>Generally not acceptable</b>	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
	<b>Extreme</b>	<b>Not acceptable</b>	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	8	12	16	20
	4	5	10	15	20	25
	5					

## Appendix 4. Criteria for assessing emerging risks and opportunities

### Criteria for rating emerging risks

Criteria	Rating and Priority	
a. Likelihood of risk occurring	Possible	Unlikely
b. Level of exposure to risk	Moderate – High	Low
c. Ability to respond to risk	Limited	Good
d. Timeframe	Short – Medium term (1 month – 2 years)	Long-term (2+ years)
	<b>Manage (Priority – 1)</b>	<b>Monitor (Priority – 2)</b>

### Threshold definitions

Rating	Definition
<b>Monitor</b>	Keep on “emerging risks” register and continue to review for future changes
<b>Manage</b>	Consider a move from emerging to main risk register for active management/mitigation

### Criteria for rating emerging opportunities

Criteria	Rating and Priority		
a. Likelihood of opportunity crystallising	Likely (favourable outcome likely in one year, or better than 75% chance of occurrence)	Possible (reasonable prospects of favourable results in one year or 25%-75% chance of occurrence)	Unlikely (some chance of favourable outcome in medium term or less than 25% chance of occurrence)
b. Advantage to institution	High	Moderate	Low
c. Ability to respond to opportunity (eg resourcing)	Able	Some	Limited
d. Timeframe	Short term (1 month – 1 year)	Medium term (2 years)	Long term (2+ years)
	<b>Exploit (Priority – 1)</b>	<b>Explore (Priority – 2)</b>	<b>Observe (Priority – 3)</b>

### Rating definitions

Rating	Definition
<b>Exploit</b>	Consider taking action to make the most of the opportunity
<b>Explore</b>	Explore opportunity further including possible development of action plan to ensure readiness to take advantage of opportunity within limited timeframe
<b>Observe</b>	Keep on register for noting/observation and revisit for future changes (particularly to timeframe)

## Appendix 5 . 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 to relevant external stakeholders (i.e. OfS)
November	Review by Audit <u>and Risk</u> Committee	Audit <u>and Risk</u> 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 <u>and Risk</u> Committee, incorporating mid-year review of Risk Register	Audit <u>and Risk</u> Committee meeting
June	Review by Audit <u>and Risk</u> Committee, incorporating preparation for year-end review by Board of Governors	Audit <u>and Risk</u> Committee meeting



## 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:	<input type="checkbox"/>
a) Confirmed whether the project meets the criteria of a major/reportable project (see point 2.9 of the Risk Management Procedure)	<input type="checkbox"/>
b) Identified relevant risk factors (preferably in consultation with project team)	<input type="checkbox"/>
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	<input type="checkbox"/>
d) Prioritised the identified risks according to severity and potential impact	<input type="checkbox"/>
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	<input type="checkbox"/>
f) Updated the project plan/schedule to include mitigating actions and additional reporting requirements for a major/reportable project if necessary (see 1a)	<input type="checkbox"/>
g) Identified project team member responsible for maintaining the project risk register	<input type="checkbox"/>
h) Has submitted the risk register for review and signoff by the relevant party (Head of Department, SLT or SLT member)	<input type="checkbox"/>
2. Project team has been trained on risk management (optional)	<input type="checkbox"/>
3. The risk register has been circulated to all project team members	<input type="checkbox"/>
4. The risk register is available to all project team members	<input type="checkbox"/>

**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	<input type="checkbox"/>
Ensure sufficient information is documented to allow understanding of project risks and mitigating actions	<input type="checkbox"/>
Reprioritise risks as required	<input type="checkbox"/>
Update the project plan to reflect any impact on resources, timing etc arising from risk management	<input type="checkbox"/>
Implement actions to mitigate any new risks which meet defined trigger (see 1e)	<input type="checkbox"/>

## Appendix 7. History of changes

Version	Date	Section	Changes/updates
5	1/12/25	<b>General</b>	<ul style="list-style-type: none"> <li>• General update to align with RM standards (LGA Must Know Guide Risk Management, IRM 2002, HMT Orange Book)</li> <li>• Rearrangement/retitling sections to improve document flow</li> </ul>
		<b>Policy</b>	<ul style="list-style-type: none"> <li>• Updates to policy statement and key principles to encompass obligations re public interest governance principles, safeguarding etc as per LGA Must Know Guide Risk Management</li> </ul>
		<b>Procedure</b>	<p>2.1 Roles and responsibilities</p> <ul style="list-style-type: none"> <li>• Updates to align with R&amp;Rs as outlined in IRM 2002 (BoG) and HMT Orange Book p45 (ARC)</li> <li>• University Secretary (+ Director SPO) with overall responsibility for RM process</li> </ul> <p>3.1 Risk management as part of the system of internal control</p> <ul style="list-style-type: none"> <li>• 3.1.3 no longer mandates development of Departmental risk registers but outlines expectations of Depts to manage their risks</li> <li>• 3.1.8 Added definition of Departments' role in identifying emerging risks</li> <li>• 3.1.9 Added definition of Departments' role in identifying emerging opportunities. Added detail around "low" rated items for efficiency</li> <li>• 3.1.11 External audit (previously 2.8.11)</li> <li>• 3.2.12 Third party reports (previously 2.8.12)</li> </ul> <p>5.1 Risk Registers</p> <ul style="list-style-type: none"> <li>• Risk planning as part of annual planning process (as per D2-6 and section 91 of HMT Orange Book)</li> <li>• Removed para around using risk register templates as 3.1.3 no longer mandates development of Dept risk registers</li> </ul> <p>6.1 Identifying and analysing risks</p> <ul style="list-style-type: none"> <li>• Rewrite to simplify and align with LGA Must Know Guide Risk Management</li> <li>• 6.1.1 new section: University risk appetite, analysis of risk as per HMT Orange Book section D6</li> <li>• 6.1.2 new section Risk identifiers: added "knowledge management" as per IRM 2002</li> </ul> <p>7.1 Risk reviews (previously 2.5)</p> <ul style="list-style-type: none"> <li>• New section on annual formal review process</li> </ul> <p>8.1 Risk escalation (previously 2.6)</p> <p>9.1 Removing risks from Risk Registers (previously 2.7)</p> <ul style="list-style-type: none"> <li>• Removed section on Departmental Risk Registers (no longer mandated)</li> <li>• Added RMG's ability to remove risk</li> <li>• Removed section on Assurance Map</li> </ul>

			10.1 Periodic review of effectiveness (previously 2.9) <ul style="list-style-type: none"> <li>Added requirement to review RM framework at least annually, as per HMT Orange Book</li> <li>Added role of RMG in oversight, removed reference to “departmental register”</li> </ul>
		<b>Appendix 5</b>	Removed. Reference to “lines of assurance” moved to section 3.1
		<b>Appendix 7</b>	History of changes pre-version 4 moved to separate document
4.3	10/12/24	General	Updates to titles, committee names etc
		Procedure	2.8.6, 2.8.7 Emerging risks, Opportunities <ul style="list-style-type: none"> <li>Added correct criteria for assessing emerging risks and opportunities</li> </ul>
4.2	30/04/24	Procedure	Appendix 1. Risk appetite <ul style="list-style-type: none"> <li>Updated version as per RMG changes</li> </ul>
4.1	03/07/23	General	Updates to titles etc
4.0	23/08/22	Procedure	Version history <ul style="list-style-type: none"> <li>Changes made as per the recommendations of the internal audit into the governance of Risk Management</li> <li>Updated Responsible Officer</li> <li>Made corrections to version history (corrected page numbers etc)</li> <li>Updated Committee Review and Circulation</li> </ul>
			2.1 Roles and responsibilities <ul style="list-style-type: none"> <li>Added details on the roles and responsibilities of Strategic Risk owners, including on providing updates on progress of mitigating actions for Strategic Risks</li> <li>Clarified the role of the Board of Governors in risk management at the university</li> </ul>
			2.4 Identifying risks <ul style="list-style-type: none"> <li>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.</li> </ul>
			2.8 Risk management as part of the system of internal control <ul style="list-style-type: none"> <li>Added detail on the Risk Management Group’s reporting lines to University Executive Committee and Risk and Audit Committee</li> <li>Clarified role of UEC and SLT as it relates to the Risk Management Group’s reporting lines</li> <li>Corrected RMG meeting attendance requirements</li> </ul>
			2.8.2
			2.8.6 Emerging Risk Register <ul style="list-style-type: none"> <li>Changed rating “system” for emerging risks to “High/Medium/Low” as per agreement at RMG (April 2022)</li> </ul>

			<p>2.8.7 Emerging Opportunities Register</p> <ul style="list-style-type: none"><li>• Changed rating “system” for emerging opportunities to “High/Medium/Low” as per agreement at RMG (April 2022)</li></ul>
--	--	--	---