APPROVED: 3rd July 2017 **APPROVAL BODY:** Board of Governors **REVIEW DATE:** July 2021
MPLEMENTATION DATE: Summer 2018 onwards

University of Worcester

Risk Management Policy

1. Purpose and definitions

1.1 The purpose of the risk management policy is to explain the University's underlying approach to risk management and to document the roles and responsibilities of the Board and its sub-committees, the University's senior leadership and other staff with executive responsibilities. It also outlines key aspects of the risk management process, and identifies the main reporting procedures.

1.2 Corporate risks are recorded in the University Risk Register. This records opportunities or threats that may affect the University's future success and ability to deliver its strategic plan. The Register is a dynamic and 'living document' that is populated and updated through the University's regular risk assessment and management work. It provides an assessment of the potential magnitude or scale and likelihood of a given risk and details of how individual risks will be treated, the controls in place to mitigate the risk and plans to strengthen the controls.

1.3 A departmental-level risk can be defined as a risk that may affect the ability of an Institute or professional services team of delivering successfully operational plans or key activities.

2. Scope and approach to risk management

2.1 This risk management policy forms part of the University's governance and internal control arrangements.

2.2 The University has a responsible approach to risk management, seeking to recognise and manage appropriately its exposure to risks. In pursuit of achieving its strategic aims and academic mission the University will, therefore, accept a degree of risk, commensurate with the potential reward.

2.3 Risk management is embedded into the management practice of the University's senior leadership. This approach is championed by the Vice Chancellor and is reflected in the Vice Chancellor's reports, presented at each meeting of key University committees and meetings, namely: The Board, the Vice Chancellor's Advisory Group, the University Executive and briefing meetings for all staff.

3. Risk Appetite

3.1 The risk appetite framework, describes the level of risk that the University is willing to accept in the pursuit of its strategic aims, and will inform formal strategic decision-making by the Board. Therefore, risk appetite seeks to articulate and prioritise institutional effort and balance the institutional risk profile in key strategic areas, to ensure that the University's resources and creativity are focused on key areas (known as 'Key Risk Areas'). In order to facilitate innovation, to enable the University to be sector-leading, to develop new models of working and/or to embrace new opportunities in areas central to its mission and strategy, the University is willing to tolerate more risk-taking, with appropriate mitigating action. In other areas of activity, the University will be more cautious and less willing to take risks.

3.2 The University's Key Risk Areas in the risk appetite framework are:

- Learning and Teaching
- Student Experience
- Inclusive practice

- Financial investments in targeted long-term strategic developments (with approved business plans).
- Community engagement and outreach
- Research and Enterprise
- Development and Commercial Activity
- Partnership and external collaboration
- Overall Financial Health

These will be reviewed regularly to ensure they remain aligned with the University's strategic plan.

3.3 The risk appetite thresholds are of relative rather than absolute measures. The thresholds are as follows:

- ***Prepared:*** willing to take calculated risks from prepared ground, to innovate, pioneer and maximise opportunities related to the delivery of the University's strategy
- ***Moderate:*** open to taking some risks
- ***Prudent:*** cautious and in some cases avoiding risk so that effort can be focused in other risk areas.

3.4 The Key Risk Areas and Risk Appetite Thresholds are reviewed and approved on at least an annual basis at times, when the Board is reviewing the delivery of the Strategic Plan and setting priorities for the academic year.

4. Responsibilities

4.1. The **Board** is responsible for:

- Approving the Risk Management Policy
- Reviewing annually the University's approach to risk management and risk appetite
- Approving changes or enhancements to key element of its processes or reporting, except those decisions for which the Audit Committee has delegated powers (see 3.2 below).
- Seeking assurance (via Audit Committee) of the successful implementation of the Risk Management policy and related processes
- Reviewing the University Risk Register at least three times per annum and approving as appropriate changes proposed to the Register
- Monitoring the management of all corporate risks by the University's senior leadership
- Approval of major decisions affecting the University's risk profile or exposure.

4.2 In accordance with sector-wide requirements, the **Audit Committee** is responsible for:

- Reviewing the effectiveness of the risk management, control and governance arrangements on behalf of the Board.
- Reporting to the Board on internal controls and alerting members to any emerging issues.
- Monitoring, on behalf of the Board, the management of corporate and department-level risks, by receiving and reviewing risk management reports (including the full University Risk Register) at least three times per annum. The Reports shall summarise the review process associated with the local registers and any key themes that have been identified.
- Authorising remedial action where necessary to enhance the University's risk management arrangements.
- Providing comment on new risks.

4.3 Led by the Vice-Chancellor and Chief Executive, **University's Senior Leadership** team (known as the Vice Chancellor's Advisory Group) is responsible for:

- Identifying, evaluating and reporting the significant corporate risks faced by the University, and ensuring that appropriate mitigating action is taken. The team is responsible for monitoring and reporting changes in the status of corporate risks, in risk management reports and the University Risk Register for consideration by the Board and the Audit Committee.
- Providing adequate information in a timely manner on the status of risks, controls and planned action.

- Undertaking training and development activities associated with risk management, as appropriate.

4.4 Individual **members of the University's Senior Leadership team** are responsible for:

- Effective risk management in their areas of responsibility, in accordance with the University's Risk Management Policy and procedures.
- Undertaking regular reviews and assessment of key risks within their areas of operation as part of routine management arrangements. These shall be recorded in a local risk register (see below para. 6.1).
- Overseeing the implementation of risk management controls and planned development work in their area of responsibility.
- Submitting on a six monthly basis the current version of the local risk register to the University Risk Manager.
- Escalating any significant changes in terms of existing or new risks to the University's Risk Manager
- Reviewing Departmental Information Security Risk Registers for the departments/Institutes for which they have direct leadership responsibility.

4.5 The **Head of Information Assurance** is responsible for maintaining the following registers:

- the University Information Security Register
- Local risk registers for the University's subsidiary companies
- Project risk registers.

These are reviewed routinely on at least a six-monthly basis. Any major changes should be reported immediately to the University Risk Manager.

4.6 The **University's Risk Manager** is responsible for ensuring that the University operates effective procedures relating to risk management and for undertaking formal reviews on behalf of the Board of the risk management policy. The University Risk Manager will provide on-going training to risk owners in order to facilitate the effective operation of risk management and prepare risk management reports on behalf of the University's senior leadership for consideration by both the Board and the Audit Committee. This responsibility currently resides with the Clerk to the Board.

5. Risk Identification and Assessment

5.1 The methodology used to assess Corporate Risks in the University Risk Register is based on the use of a nine-point scale risk rating mechanism to assess the impact and likelihood of risk, based on the following definitions:

Impact				
	H	🟧	🟥	🟥
	M	🟩	🟧	🟥
	L	🟩	🟩	🟧
		3	**2**	**1**

Likelihood

H1: High impact, high likelihood
H2: High impact, medium likelihood
H3: High impact, low likelihood
M1: Medium impact, high likelihood
M2: Medium impact, medium likelihood
M3: Medium impact, low likelihood
L1: Low impact, high likelihood
L2: Low impact, medium likelihood
L3: Low impact, low likelihood.

5.2 Classifications of high, medium and low impact and likelihood are provided below:

	High (H or 1)	Medium (M or 2)	Low (L or 3)

Impact	Result in failure to achieve one or more strategic aims, objectives or key targets	Restrict ability to achieve one or more strategic aims, objectives or key targets	Impact on some aspects of one or more strategic aims, objectives or key targets
Likelihood	Greater than 70% chance of the risk materialising in the next 2 years	Between 30% to 70% chance of the risk materialising in the next 2 years	Less than 30% chance of the risk materialising in the next 2 years

5.3 A similar risk assessment matrix is used in Local Risk Registers and departmental Information Security Registers. A twelve-point scale is used. An additional category has been added relating to risk impact to highlight and potentially escalate risks that may affect the overall University. The definitions for high, medium and low impact have also been adjusted to reflect the departmental context in which local registers are created. Intelligence gathered from local information security registers will be used to review and update the University's Information Security Risk Register. The University's Risk Manager will review the University Information Security Risk Register and be informed of all local information security risks with a net risk rating of UW1, UW2, H1, H2. This review may result in changes being made to the overall University Risk Register.

Impact

UW	🟨	🟥	🟥
H	🟩	🟧	🟥
M	🟩	🟨	🟧
L	🟩	🟩	🟨
	3	**2**	**1**

Likelihood

UW: Institutional Impact that is likely to affect the reputation or operation of more than one key corporate business process, system or institute/department of the University
H: High impact that likely to prevent more than one business process or system from operating or will impact part of the University's work.
M: Medium impact that may affect the operation of part of the Department's/Institute's business.
L: Low impact that may affect the work of individuals or groups of staff in terms of service delivery.
1: Likely, with a 70%+ chance of the risk occurring.
2: medium Likely, with a 30-70% chance of the risk occurring
3: Lower likelihood, with a 0-30% chance of the risk occurring.

5.4 Gross and Net Risk Rating: In identifying and assessing risk, two types of risk are recorded on all risk registers:

- **Gross Risk** refers to the initial assessment of a risk without any controls or response from the University/department to help mitigate either the likelihood of the risk occurring and/or the impact on the operation of the University/department.
- **Residual Risk or Net Risk** is the risk rating remaining after the implementation of a control or response/actions which are recorded in the risk register. The residual risk rating does not take into account planned actions.

6. Risk Reporting

6.1 The University has three types of risk register:

- **University Risk Register**: this Register is intrinsically linked to the University Strategic Plan. It identifies risks that have a fundamental impact on the University's ability to operate as a business and/or deliver its Strategic Plan. Risk management is incorporated into the strategic planning process to ensure that the University is able to monitor risks to achieving the University's objectives and determine which risks have the most significant impact.

- **Local Risk Registers***:* The high level strategic risks identified in the University Risk Register, are underpinned and informed by risk registers managed at the local operational level and include:

Registers for the Institutes and academic support departments (reporting to the Deputy Vice Chancellor) professional services departments (reporting to members of the Vice Chancellor's Advisory Group, subsidiary companies and registers for major University projects.

- **Information Security Registers**: owned by each Institute and professional services department, these document risks and risk management activity associated with information security, which includes the handling and storage of data (including personal data) and the use of Information Communications Systems. The intelligence gathered from these Registers is reviewed and informs the risk identification, assessment and management in the University Information Security Register.

6.2 Format of Risk Registers

6.2.1 The University Risk Register and Local Risk Registers share common features to ensure a consistent approach to risk identification and risk management across all areas. Each register incorporates the following criteria:

CRITERIA	**DETAIL**
Risk ID	Provides the risk with a unique identifier
Strategic Ref	Aligns the risk identified with relevant area(s) of the Strategic Plan
Risk Appetite Category (University Risk Register only)	Identifying at least one of the nine Key Risk Areas associated with Risk Appetite provided in para 3.2 above.
Risk Title	A short sub-heading summarising the risk
Risk Description	A detailed risk description provided under the Risk Title
Risk Ownership	Assigns ownership of the risk to relevant member of the Senior Management Team (see below)
Gross Risk rating & movement	Initial rating of a risk without any controls or response. The risk movement indicates whether the rating has changed since the previous report i.e. whether it is the same, has increased or has decreased.
Risk Type	Identifies whether the risk is an emerging, enduring or diminishing risk
Risk Response	Identifies whether the risk should be: tolerates, transferred, treated or terminated.
Risk Management Control	Describes controls and management actions already in place to mitigate against the risk
Residual Risk rating & movement	The net risk remaining after the implementation of controls or actions. The risk movement indicates whether the rating has changed since the previous report i.e. whether it is the same, has increased or has decreased.
Planned Actions	Identifies action(s) to be implemented in order to mitigate the risk. When planned actions are completed, they are then documented in the 'Risk management controls' section.
Planned Action Lead	Assigns ownership of the planned action to an appropriate member of the University Executive Committee
Planned Action Due Date	Sets due date for implementation of the planned action
Progress since previous review	Provides an update on progress since the previous report in terms of mitigating the risk, denoted by the following flag: unchanged (⇔**)**, improving position (⇑**)**, progress is stalling (⇓**)**.

6.2.2 In addition to the above criteria, the University Risk Register also includes a section to describe the principal category for each corporate risk. This information is displayed in a diagrammatic form on the University Risk Heat Map, which is provided at the beginning of each risk management report. There are four categories:

- Strategic
- Operational (including risks associated with change management, effectiveness and efficiency)
- Financial

- Legal, Regulatory or Compliance

6.2.3 The Information Security Risk Registers include the key fields used in the University and Local Registers (cited in para 6.2.1 above), with two exceptions:

- The reference to the University strategic plan is omitted
- The Risk Title field is replaced by Risk Scenario, which is based on descriptions provided by the UCISA toolkit on Information Security which is a Higher Education sector resource.

7. Risk Assurance Map

7.1 The Risk Assurance Map identifies how the risk management controls are being monitored in terms of their successful operation and effectiveness. For each risk three lines of assurance are mapped:

- First line: ongoing management responsibilities, relevant policies, procedures, and processes and/or management information reports
- Second line: internal structures and post-holders without direct management responsibilities in the specific business area that have a review/monitoring role, such as governance committees and senior manager with oversight responsibilities and success measures (where possible benchmarked with other Universities), associated with specific aims and objectives in the Strategic Plan 2018-23, which will be monitored by the Board
- Third line: independent reviews within the past three years by internal or external auditors (denoted by IA and EA respectively in table below) and external reviewer by designated sector bodies, regulators and professional accreditation bodies.

8. Internal and External Audit Procedures (as they relate to risk)

8.1 ***Internal Audit:*** Internal audit is an important part of the internal control process for risk. The University's internal auditors use a risk-based methodology, which is informed by the risks included in the risk register and a review of the Risk Assurance Map. Reviews of the University's approach to risk management (including the benefits that are derived) are undertaken on an annual basis and informed by a dedicated review of risk management every three years.

8.2 ***External Audit:*** External audit provides feedback to the Audit Committee on the operation of the risk management process.

8.3 ***Annual Review of Effectiveness***

The Board is responsible for reviewing the effectiveness of the internal control of the University, based on information provided by the senior management team. This is done at the meeting when the University's financial accounts are received and formally approved. For each significant risk identified, the Board will:

- review the previous year and examine the institution's track record on risk management and internal control
- consider the internal and external risk profile of the coming year and consider if current internal control arrangements are likely to be effective.