Risk Management Policy

1. Purpose of Policy

This policy sets out the University's approach to risk management of strategic and operational risks and details how employees are expected to assess and manage risk alongside their day-to-day activities, ensuring that well-informed decisions are made and that the University's activities are compliant with this policy. This policy forms part of the University's internal control framework and governance arrangements.

This policy applies to:

All employees within Cardiff University's Colleges, Schools, Institutes, Departments, Professional Services Departments and Sites in the management of strategic and operational risks.

This policy provides guidance and accountability to:

All joint ventures, subsidiaries and partnerships of Cardiff University.

1.1 Scope of Policy

This policy:

a. Provides definitions of risk terminology agreed by the University.
b. Details the agreed risk appetite classifications and the University's statement of risk appetite and tolerance.
c. Defines the University's approach to agreed risk thresholds, risk register hierarchy and risk reporting frequency.
d. Defines the University's agreed risk scoring criteria.
e. Describes the agreed arrangements for risk governance.
f. Defines the agreed approach to risk maturity and culture.
g. Communicates the agreed roles and responsibilities for managing risk.
h. Details the agreed approach to risk assurance and mapping.
i. Sets out the agreed arrangements for monitoring this policy.
j. Details any related policies and procedures.

2. Policy

2.1 Definitions

The University uses the following terminology relating to risk and risk management:

- A Risk is defined as a threat, an uncertain, future event that could adversely affect the achievement of objectives. Unlike an issue where the event has materialized a risk is a potential event that *could* materialize.

- Risk Owner is defined as the accountable person for the risk.

- Risk Lead is defined as the person who manages the local day to day management of the risk and reports risk activity to the risk owner.

- Secondary Risk Lead(s) is defined as the person(s) who provides input into the risk and reports risk activity to the risk lead.

- Risk Action Owner(s) is defined as the person(s) who is assigned a future action to treat the risk.

- An Issue is defined as something that has occurred or is currently happening and is viewed as an ongoing problem/issue. Potentially, an issue is an identified risk that has materialized and has been escalated from a risk register to local reactive response management.

- An Incident is defined as any situation that might be or could lead to, an interruption or disruption of core activities, loss, emergency or crisis and which requires special measures to restore matters back to business as usual. When responding to an incident, members should refer to local incident management protocols or the University's Major Incident plan for guidance. This includes any event that has or has the potential to:
  - threaten people.
  - threaten buildings.
  - threaten the environment.
  - threaten the organisation's credibility/reputation.

  Or,
  - Requires the attendance of local or national law enforcement officers, for example, police or regulatory government enforcement bodies such as HSE, FSA, EHA, HMRC etc.

- Risk Management is defined as the process by which risks are identified, assessed, prioritised and managed in order to support well-informed decision-making and maximise the realisation of opportunities across the University.

- Risk Management Software enables the Institution to have a complete picture of the risk universe, controls and treatment plans, assurance and risk environment in real time. See section 5 to view guidance on 4Risk Management Software.

- Risk Maturity is defined as the measure of how well an organisation understands and manages its risk position.

- Assurance Mapping is defined as a risk management framework that defines 3 levels of assurance for strategic risks. In summary; 1st line is operated by managers and staff, 2nd line is the review and management of 1st line and details control functions, 3rd line is independent assurance from for example internal and external audit.

- Risk Universe is defined as a universal list of risks across all levels within the institution.

- Strategic & Operational Risk Management Guidance is defined as a guidance document to compliment the use of the risk management policy and assist in the risk management processes of; risk identification, assessment, analysis, management and treatment of risk(s).

- Inherent Risk Score (Gross) is defined as the amount of risk before any controls (its raw/untreated state). Note, it is expected that the Inherent risk score will only change when the internal or external environment surrounding the risk changes.

- Residual Risk Score (Net) is defined as the amount of risk that remains after implemented controls. Note, the residual risk score does not include future actions.

- Target Risk Score is defined as the expected risk score considering implemented controls and all future actions. Scoring the risk at target level enables the Risk Owner to identify if further controls are required. The target score should aim to be within the assigned risk tolerance scoring range. Note, when all future actions have been implemented the residual risk score should mirror the target score.

- Future Actions are defined as controls that require action to implement. They are assigned to a Risk Action Owner and a target date is set for completion of action. Once future actions have been completed they are listed within implemented controls and the risk is re-scored at residual level.

- Risk Appetite is defined as the amount of residual risk that the University is prepared to accept, tolerate or be exposed to at any point in time.
- Risk Tolerance is defined as the level of residual risk an entity is willing to accept in order to achieve objectives. Residual risk scores that sit above tolerance ranges require action, with risks below requiring discussion on risk response.
- 4 T's is defined as a set of responses to risk being; Treat (Take action to control the risk either by reducing the likelihood of the risk developing or limiting the impact should the risk materialize), Terminate (Do things differently and thus avoid the risk), Tolerate (If this risk is unable to be treated or nothing can be done at a reasonable cost to mitigate the risk at a reasonable level consideration is needed to whether the risk can be tolerated by the institution) and Transfer (Can some parts of the risk be transferred/shared via insurance, contractual arrangements or accepted by third parties)
- A Risk Matrix is defined as a visual representation of the risk analysis process and categorises risks based on their level of likelihood and severity of impact.
- Risk Threshold is defined as the level of exposure or uncertainty that triggers action or avoidance.
- A Strategic Risk Register is defined as a register that records risks that could affect the implementation or achievements of objectives within the Strategic Plan (the five Critical Success Factors and/or KPI's) or could impact the entire organisation.
- A Professional Service, Operational Risk Register is defined as a register that records the identification of risks to key operational activities at professional service, and the delivery and achievement of the operational delivery plan.
- A School Risk Register is defined as a register that records the identification of risks relating to the delivery and achievement of operational objectives.
- A College Risk Register is defined as a register that records the identification of risks relating to the delivery and achievement of operational and strategic objectives.

2.2 Approach to Risk Classifications, Appetite, Tolerance, Thresholds, Reporting Frequency, Risk Scoring Criteria, Risk Register Hierarchy and Risk Governance Levels

As part of the risk identification process the Risk Owner is to identify the uncertain event or action (the threat), risk causes (internal and external) and potential impacts. The Risk Owner is to then identify the most significant impact from the list of potential impacts and assign it to one of the 'Most Significant Impact Category' detailed within the Institution's Risk Appetite and Tolerance Statements. All impact categories are aligned to an appetite classification and residual risk tolerance range. For an identified risk that is scored at residual level (scored on likelihood and impact using the risk scoring criteria) which is above the tolerance range the risk is to be recorded on a register and response discussed in response to the (4 T's). Risk(s) with a residual risk score below tolerance do not require inclusion on a risk register. Trigger points in the form of risk thresholds provide guidance on when a risk is to be escalated, de-escalated, closed or included within specific governance channels.

Annually the Vice-Chancellor (VC), determines (following advice from University Executive Board (UEB)) the nature and extent of the following classifications and statements.

The VC, confirmed that the University sits comfortably in the following position:

- Residual Risk Appetite Classifications & Risk Tolerance Ranges (detailed in Table 1)
- Residual Risk Appetite and Tolerance Statements (detailed in Table 2)
- Residual Risk Thresholds for Risk Escalation (detailed in Image 1)
- Residual Risk Monitoring and Updating of Register Frequency (detailed in Table 3)
- Risk Matrix and Scoring Criteria (detailed in Table 4)
- Risk Register Hierarchy (detailed in Image 2)
- Residual Risk Governance Levels (detailed in Table 5)

Table 1: Residual Risk Appetite Classifications & Risk Tolerance Ranges

Risk Appetite Classifications	Description (summarised from the Orange Book)	Residual Risk Tolerance Scores
Averse (Very Low)	Avoidance of risk and uncertainty in achievement of key deliverables or initiatives is a key objective.	The University will accept risk with a residual score of **1 – 2**
Minimalist (Low)	Preference for the very safe business delivery options that have a low degree of risk with the potential for benefit/return not a key driver.	The University will accept risk with a residual score of **3 – 5 or below**
Cautious (Medium)	Preference for safe options that have low degree of risk and only limited potential for benefit. Willing to tolerate a degree of risk in selecting which activities to undertake to achieve key deliverables or initiatives, where we have identified scope to achieve significant benefit and/or realise an opportunity.	The University will accept risk with a residual score of **6 - 10 or below**
Open (High)	Willing to consider all options and choose one most likely to result in successful delivery while providing an acceptable level of benefit. Seek to achieve a balance between a high likelihood of successful delivery and a high degree of benefit and value of money. Activities themselves may potentially carry, or contribute to, a high degree of residual risk.	The University will accept risk with a residual score of **11 – 16 or below**
Eager (Very High)	Eager to be innovative and to choose options based on maximising opportunities and potential higher benefits even if those activities carry a very high residual risk.	The University will accept risk with a residual score of **17 – 20 or below**

Table 2 Institution Risk Appetite and Tolerance Statements (aligned to residual risk scores)

	Residual Risk Appetite and Tolerance Statements					
Most Significant Impact Category	Very Low Averse	Low Minimalist	Medium Cautious	High Open	Very High Eager	RATIONALE
Reputation and Credibility		Tolerance 3-5				It is regarded as critical that the University preserves its high reputation and credibility. The University therefore has low appetite for risk in the conduct of any of its activities that puts its reputation in jeopardy, could lead to undue adverse publicity, or could lead to loss of confidence by the Welsh and UK political establishment, and funders of its activities.
Compliance		Tolerance 3-5				The University places great importance on compliance, and has no appetite for any breaches in statute, regulation, professional standards, research or medical ethics/ ethical considerations, bribery or fraud. It wishes to maintain accreditations related to courses or standards of operation and has low appetite for risk relating to actions that may put accreditations in jeopardy.
Financial			Tolerance 6-10			The University aims to maintain its long-term financial viability and its overall financial strength. Whilst targets for financial achievement will be higher, the University will aim to manage its financial risk by not breaching a number of minimum criteria which are being developed by the Chief Finance Officer.
Research				Tolerance 11-16		The University wishes to be at the leading edge in the creation of knowledge and making a difference to society. It wishes to grow its research activities and improve its performance in each REF assessment compared to the previous assessment. It recognises that that this will involve an increased degree of risk in developing research activities and is comfortable in accepting this risk subject to ensuring that potential benefits and risks are fully understood before developments are authorised and that sensible measures to mitigate risk are established.
Education and Student Experience				Tolerance 11-16		The University wishes to stimulate students to develop a lifelong thirst for knowledge and learning and encourage a pioneering innovative and independent attitude and an aspiration to achieve success. It expects as a minimum to be in the top quartile of surveys related to student experience. It recognises that this should involve an increased degree of risk in developing education and the student experience and is comfortable in accepting this risk subject always to ensuring that potential benefits and risks are fully understood before developments are authorised and that sensible measures to mitigate risk are established.
Innovation and Engagement				Tolerance 11-16		The University wishes to be amongst the leaders in transforming knowledge, ideas, skills, and expertise into advice, innovation, intellectual property, and enterprise, thereby enriching society. It recognises that developing this may involve an increased degree of risk and is comfortable in accepting this risk subject always to ensuring that potential benefits and risks are fully understood before developments are authorised and that sensible measures to mitigate risk are established.

International Development		Campus Development outside of UK Tolerance 3-5	Investments Overseas Tolerance 6-10	Developing Networks Tolerance 11-16		The University aims to achieve global impact in its activities and to promote research and other collaborations and staff/student exchanges with leading institutions across the world. It has an open appetite for developing such networks to the extent that they support the mission and reputation of the University but a cautious appetite for investing in research facilities overseas, and a minimalist appetite for investing in the development of student campuses outside of the UK.
Environment & Social Responsibility				Tolerance 11-16		The University aims to make a significant, sustainable, and socially responsible contribution to Wales, the UK and the world through its research, education, knowledge exchange and operational activities. It recognises that this should involve an increased degree of risk and is comfortable in accepting this risk subject always to ensuring that potential benefits and risks are fully understood before developments are authorised and that sensible measures to mitigate risk are established.
People & Culture		Tolerance 3-5				The University aims to value, support, develop and utilise the full potential of our staff to make the University a stimulating and safe place to work. It places importance on a culture of academic freedom, equality, diversity and inclusion, dignity and respect, collegiality, annual reviews, the development of staff, and the health and safety of staff, students and visitors. It has minimalist appetite for any deviation from its standards in these areas.

Image 1: Residual Risk Thresholds for Strategic and Operational Risk Escalations & Governance

Impact						
	Very High Severe 5	Low 5	Medium 10	High 15	Major 20	Major 25
	High Significant 4	Low 4	Medium 8	High 12	High 16	Major 20
	Medium Moderate 3	Low 3	Medium 6	Medium 9	High 12	High 15
	Low Minor 2	Very Low 2	Low 4	Medium 6	Medium 8	Medium 10
	Very Low Insignificant 1	Very Low 1	Very Low 2	Low 3	Low 4	Low 5
		Very Low Rare 1	Low Unlikely 2	Medium Possible 3	High Likely 4	Very High Almost Certain 5
		Likelihood				

- **Residual Risk Threshold >16**

Automatic escalation to Strategic Risk Register and removal of risk from other previous register.
Risk Owner to liaise with Chief Operating Officer with regards to the benefits of forming a contingency planning group.

- **Residual Risk Threshold 12 – 16**

Professional Service, School and College risks are included in summary within the Annual Risk Management Report and reviewed at Corporate Governance Compliance & Risk Group.

- **Residual Risk Threshold 15 – 16**

School risks to be escalated to College level register.

- **Residual Risk Threshold <2**.

Risk is not required to be recorded on a risk register

- **Any operational or strategic risks at residual level that are within or below tolerance range**

can be requested by the Risk Owner for closure with approval required from VC (as advised by UEB) for strategic risk closures and Heads of Departments/School/Colleges for operational risk closures (as advised by Risk Owner).

- **Operational or strategic risks that materialize**

should no longer be detailed on a risk register nor managed through risk management processes. See Strategic and Operational Risk Management Guidance document for further information on risks versus issues and incidents.

Table 3 Residual Risk Monitoring and Updating of Register Frequency

Very Low (1-2)	Low (3-4)	Medium (5-10)	High (12-16)	Major (20-25)
No reporting of risk required. **Maintain watching brief.**	Reviewed and updated **every 4 months**	Reviewed and updated **every quarter**	Reviewed and updated **every quarter**	Requires Immediate attention and action and is to be reviewed and updated **every quarter**

Image 2 – Risk Register Hierarchy and Levels of Risk Governance

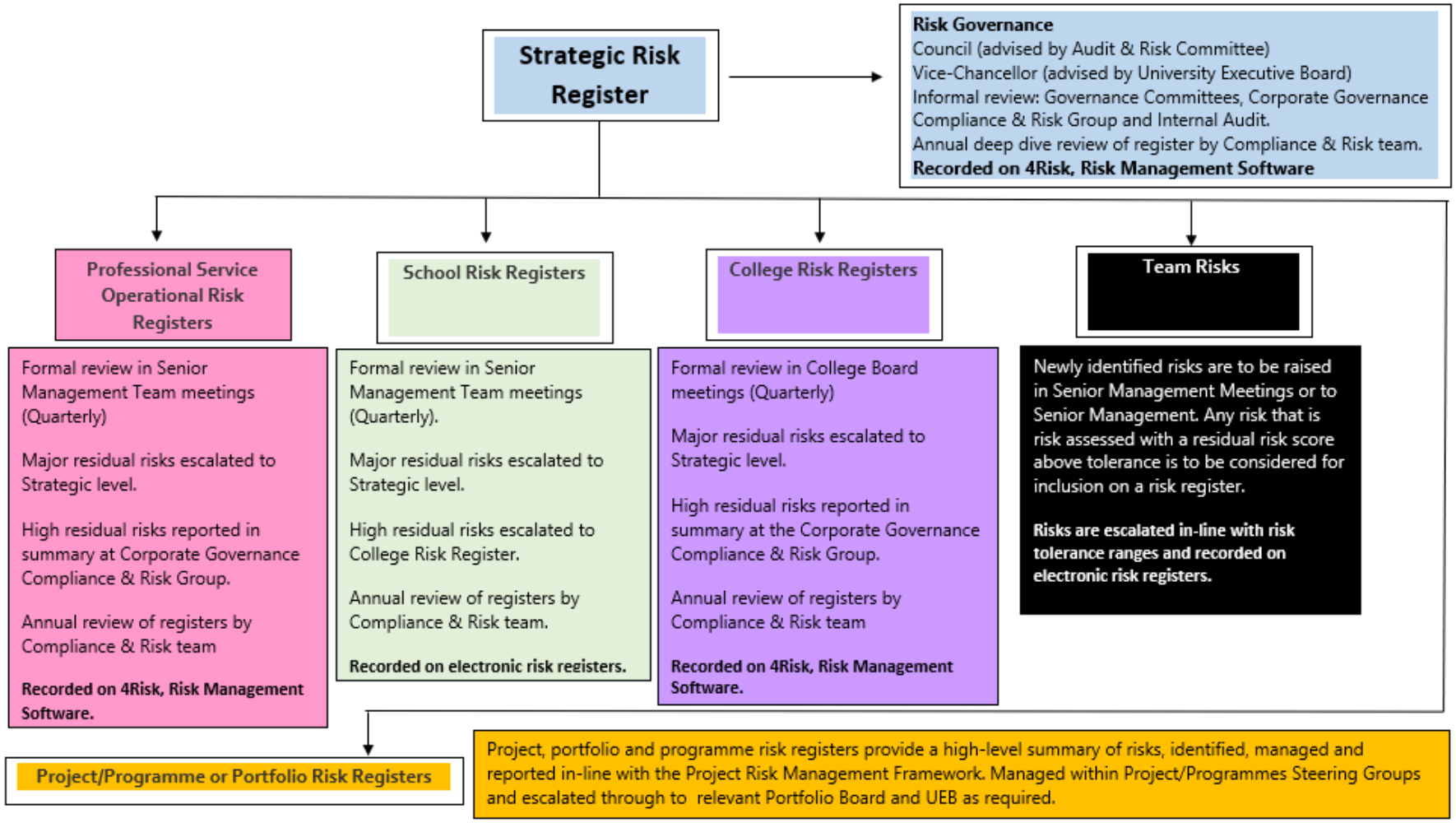

Table 4 Risk Matrix and Scoring Criteria (Threats)

Impact						
	Very High Severe 5	Low 5	Medium 10	High 15	Major 20	Major 25
	High Significant 4	Low 4	Medium 8	High 12	High 16	Major 20
	Medium Moderate 3	Low 3	Medium 6	Medium 9	High 12	High 15
	Low Minor 2	Very Low 2	Low 4	Medium 6	Medium 8	Medium 10
	Very Low Insignificant 1	Very Low 1	Very Low 2	Low 3	Low 4	Low 5
		Very Low Rare 1	Low Unlikely 2	Medium Possible 3	High Likely 4	Very High Almost Certain 5
		Likelihood				

Likelihood Assessment Criteria

Likelihood	1 - Very Low, Rare Likelihood	2 – Low, Unlikely Likelihood	3 – Medium, Possible Likelihood	4 – High, Likely Likelihood	5 – Very High, Almost Certain Likelihood
	1% to 5% chance of happening; there is not much likelihood this will happen	6% to 25% chance of happening; we don't think this will happen	26% to 50% chance of happening; we don't know if this will happen (50/50)	51% to 75% chance of happening; we are reasonably sure this will happen	76% to 99% chance of happening; we are almost certain this will happen

Impact Assessment Criteria

Impact Categories	Impact Scoring				
	1 **Very Low, Insignificant Impact**	**2** **Low, Minor Impact**	**3** **Medium, Moderate Impact**	**4** **High, Significant Impact**	**5** **Very High, Severe Impact**
Reputation & Credibility	Highly unlikely to cause adverse publicity	Unlikely to cause adverse publicity	Needs careful PR/Diverse local publicity	Local and National publicity/limited damage to University brand	Significant national and international publicity/sustained damage to University brand
Compliance	Regulations breach that results in minimal or no damage or loss.	Fines or claims brought.	Case referred by complainant to regulatory authorities and potential for regulatory action with more than localised effect or fines.	Formal external regulatory investigation into organisational practices with potential for suspension of significant elements of University operations or fines	Formal external regulatory investigation involving high profile criminal allegations against management and threat of imprisonment or withdrawal of status or imposition of sanctions resulting in forced termination of mission critical activities.
Financial	Financial impact =<£50k	Financial impact =>50k and <£250k	Financial impact => £250K < £1M.	Financial impact => £1M <£5M	The financial impact would cost the University => £5M
Research	Minor impact on research activity	Short-term impact on research activity	Significant impact on research activity	Major impact on research activity; significant impact on a school; short term damage to research funding	Unsustainable impact on research activity; significant impact on a College; irreparable damage to research funding
Education & Student Experience	No noticeable impact on student experience	No impact to teaching; would lead to individual students raising concerns; no impact on NSS scores	Minor disruption to teaching; would lead to a group of students raising concerns; low impact (1-2) years on NSS scores	Significant disruption to teaching; would lead to individual students raising a formal complaint or leaving the University; medium impact (2-3 years) on NSS scores	Teaching stopped in one or more School; would lead to a group of students raising formal complaints or leaving the University; long term impact (more than 3 years) on NSS scores
Innovation & Engagement	Minor impact on our Innovation Strategy	Would have a small impact on our ability to take advantage of commercialisation opportunities	Would have a major impact on the Innovation Strategy objectives	Would have a significant impact on our ability to take advantage of commercialisation opportunities	Would result in us unable to achieve our Innovation Strategy

			Opportunities may result in some commercialisation opportunities		Opportunities would result in significant commercialisation opportunities
International Development	Minor impact on international activity which does not have widespread consequences for international strategy	Short-term impact on international activity; minor impact on recruitment, research, reputation and partnership activity – contained to small region	Significant impact on international activity; loss of significant income and detrimental to partnership activities, research and reputation in one region	Major impact on international activity; major impact on a partnership activity, research, reputation and recruitment in key geographical region or several regions.	Unsustainable impact on international activity impacting several key regions. Would result in inability to achieve our International Strategy or meet institutional targets.
Environment & Social Responsibility	Overall success in meeting targets and fulfilling actions; a small number of actions not achieved within expected timescale	Overall success in meeting targets and fulfilling actions; some targets missed and some actions not achieved within expected timescale	Mixed success in meeting targets and fulfilling actions; significant revision required to strategy and action plan	Some successes in implementing sustainability strategy but overall failure to achieve goals, resulting in negative publicity	General failure to achieve strategy resulting in widespread condemnation and reputational damage to University
People & Culture	Minimal impact to student and/or staff wellbeing. No visible impact on capacity and capability, service delivery and operations.	An increase in wellbeing cases. Key roles are being impacted. Visible impact on capacity and capability, service delivery and operations.	Major impact to student and/or staff wellbeing and moral. Short term loss of key roles. Moderate impact to capacity and capability. Moderate impact on service delivery and operations.	Significant Impact to student and/or staff wellbeing. Threat of staff industrial action. Long term loss of key roles. Significant impact to capacity and capability. Highest impact on service delivery and operations	Severe Impact to student and/or staff wellbeing. Widespread and sustained industrial action. Long term impact to capacity and capability. Complete loss of service delivery and operations

Table 5 Risk Governance Channels, Terms of Reference Summarised

Council	Council is the accountable body for risk management at the University. Council seeks assurance that associated policy and processes remain effective. Council takes an opportunity during each risk cycle, to review the risk report and feedback to the VC on any amendments to direction of travel for specific risks, or with the risk management process itself. Council is advised by the Audit & Risk Committee on the internal risk management arrangements, including the efficacy of the strategic risk register, the risk policy and guidance, appetite, control and governance arrangements. Council receives the risk report from the Chair of the Audit and Risk Committee at three out of four meetings.
Vice-Chancellor (VC)	The VC has overall responsibility for the institutional management of risk, with Council having oversight of risk management as the accountable body. The VC monitors institutional risks, new and emerging risks and ensure that risks are being managed effectively with a clear system of accountability and responsibility in place. The VC agrees (following advice from University Executive Board (UEB)) the processes for managing risk and brings forward proposals to Audit and Risk Committee for recommendation to Council for final sign off. The VC, approves the implementation of policies and procedures, which set out how risk will be managed and reviews the annual Risk Management Report which provides a summary of risk activity from within that year across the institution.

University Executive Board (UEB)	UEB advises the VC in the performance of her/his duties as the University's chief executive officer, including; Management of risk in the institution; Ensuring the control, co-ordination and monitoring within the University of risk and internal controls, and ensuring compliance with relevant legislation and regulations; Recognising information as a strategic asset of the University, ensuring that the value to the organisation is understood and actualised, and that measures are in place to protect against risk; Developing and implementing the Risk Management policy.
University Committee(s)	Nominated committee(s) with responsibility for having oversight of a particular risk(s), relating to its area of business. Each committee should: Review thoroughly those University risks for which it has oversight and monitor implemented controls and future actions for the risks it has oversight of, and make recommendations to the senior leadership team and Risk Owners as and when necessary.
Audit & Risk Committee (ARC)	The Audit and Risk Committee holds responsibility to scrutinise the University's performance, and to advise and/or recommend proposals to the Council, regarding internal risk management arrangements, including the efficacy of the strategic risk register, the risk strategy and appetite, control and governance arrangements. This includes compliance with the legal and regulatory framework that the institution operates within. This shall include consideration of the culture and behaviour that is prevalent within the university and arrangements that can affect reputation, such as the management of conflicts of interest. The Audit & Risk Committee receives the risk register at each of its four meetings.
Corporate Governance Compliance & Risk Group (CGCRG)	Providing direction and oversight in respect of Institutional risks to support the Vice Chancellor in the role of development, maintenance and review of systems and processes for monitoring and reviewing the effectiveness of internal controls to manage risks, and the effectiveness of the consideration of risks. Overseeing the Risk Assurance Map to support UEB's role in development, maintenance and review of systems and processes for monitoring and reviewing the effectiveness of internal controls to manage risks, and the effectiveness of the consideration of risks.
College Board	The Board members shall take responsibility for: The assessment and control of risk.
Senior Management Team Meetings	Risk to be a standing agenda item, quarterly. Opportunity to discuss and risk assess any new or emerging risk(s) identified by service area. For any new or emerging risk above tolerance (as per section 2.3 of this policy and the Institutions Risk Appetite and Tolerance Statements) risk(s) are to be recorded on a risk register, with department acting in accordance with Institutional risk threshold guidance (see section 2.3 of this policy). Formal review of risk register and verbal updates from Risk Owners, Risk Leads and Risk Action Owners on residual risks medium to major with residual green risks reviewed annually (September).

2.3 Risk Maturity

The University's Risk Maturity will be assessed annually by Internal Audit in consultation with the Compliance and Risk team using the Chartered Institute of Internal Auditors (CIIA) criteria for assessing organisational risk maturity across a continuum from risk naïve to risk embedded as detailed in Table 6.

Table 6 Chartered Institute of Internal Auditors (CIIA) criteria

Maturity	Risk Management Controls	Definition
Naïve	Unreliable	Adequate control activities are not designed or are not fully operational
Aware	Informal	Control activities are designed and in place but not fully documented
Defined	Standardised	Control activities are designed, in place, consistently applied and are adequately documented
Managed	Monitored	Standardised controls with periodic testing for effective design and operation with reporting to management
Enabled	Optimised	Integrated controls with real-time monitoring by management and continuous improvement

2.4 Risk Management Improvement Plan

The Risk Management Improvement Plan is informed by the risk management maturity assessment and is monitored and actioned by the Compliance and Risk team in the University Secretary's Office.

It is the role and responsibility of the Risk Manager to set target dates against identified actions and update the central version, housed in the Compliance and Risk team. The Improvement plan is to be revised annually in-line with future risk maturity assessment recommendations and Internal and External Audit recommendations and priorities.

The improvement plan is to be included within the Risk Management Report which is submitted annually to the VC, UEB, Audit & Risk Committee and Council for oversight.

2.5 Risk Culture within the University

Embedding a risk management culture that recognises the importance of risk management is critical to the successful implementation of this policy. The University strives to embed a culture where risk management is a key component in all decision-making processes. This enables decision making to take place in an informed manner and aligns with recognised good practice set out by the Institute of Risk Management.

This Risk Policy aims to:

Tone at the Top	Communicate a consistent tone from Council and VC in respect of risk taking and avoidance.
Accountability and Ownership	Highlight the importance of continuous risk management, including clear accountability for and ownership of specific risk and risk areas, implemented controls and future actions

Transparency and Timeliness	Promote transparent and timely risk information flowing up, down and across the University.
Lessons Learned	Actively seeks to learn from experiences, mistakes and near misses.
Encouragement and Consequences	Recognise the importance of appropriate risk-taking behaviours and encourages the challenge and sanction of inappropriate behaviour.
Diversity and Challenge	Promote consideration of diversity of perspectives, values and beliefs to ensure that the status quo is rigorously challenged when appropriate

3. Roles and Responsibilities

Any person appointed to a role and is on leave (officially excused from work) has the right to delegate their role for a duration of time. Notification is to be made to the complianeandrisk@cardiff.ac.uk team.

3.1 Vice-Chancellor (VC)

The Vice-Chancellor's role as Executive can be summarised as the following;

- Accountable to Council for implementing and enforcing an appropriate Risk Management Policy and Guidance document and allocating responsibilities to individuals within that policy.
- Setting the tone and influencing the culture of risk management across the University.
- Review of the Strategic Risk Register quarterly for;
  - Progress made in mitigating strategic risks;
  - Robustness of mitigations of strategic risks; and
  - Ensuring that risks are aligned to risk appetites, tolerances and thresholds.
- Agree (as advised by UEB) requests for new strategic risks, strategic risk escalations, de-escalations and/or risk closures.
- Ensure that strategic risks recorded within the risk register reflect the institutions' joint ventures, subsidiaries and partnerships.
- Report and present the Strategic Risk Register at Audit & Risk Committee and Council (if not delegated).
- Review annually the University's approach to risk management to ensure guidance documents and policy remain fit-for -purpose.
- Approve changes or improvements to the risk management policy and guidance documents.
- Actively monitor the internal and external environment to identify new or emerging risks through horizon scanning.

3.2 Risk Owner(s)

Risk Owners have the following responsibilities:

- Responsibility for the management, control, reporting, updating of risk register and communication of all aspects of the risk, including implementation of future actions to address threats and maximize opportunities. Note, day to day monitoring, managing and reporting of risk may be delegated to a Risk Lead if deemed necessary for *local* management.
- It is the responsibility of Risk Owners to operate in accordance with risk management processes outlined in the Strategic and Operational Risk Management Guidance document.
- Risk Owners must ensure risks are monitored and the risk register is updated in-line with the residual risk reporting frequency as detailed in section 2.3 of this policy (Table 3).
- For operational risks (residual score medium or above) verbal updates are to be provided

quarterly in senior management team meetings/College Board by Risk Owner or by appointed Risk Lead.

- Risk escalations, de-escalations and closures are to be in-line with the University's risk thresholds as detailed in section 2.3 of this policy (Image 1).
- For residual risks scored as major, Risk Owners are to liaise with the Chief Operating Officer with regards to the benefits of forming a contingency planning group.
- Risk Owners are to have a holistic approach to risk identification with all related entities considered within the risk universe.
- Attendance as required at relevant committees, such as Audit and Risk Committee, where in-depth reviews have been requested and representation is required
- Assist with the annual review of their assigned risk(s), conducted by the Compliance and Risk team.
- Attend annual risk management training sessions as requested by the Compliance and Risk team.
- Appointment of delegated Risk Lead and Risk Action Owners to manage risk at local level if deemed necessary.
- Ensure clear responsibilities and channels of communication exist that enable delegated Risk Lead to monitor and report on risk on behalf of the Risk Owner who holds overall risk accountability.
- Risk Owners of strategic risks are to contribute to the risk management assurance map which identifies the relevant lines of defence to each risk and assurance coverage.
- For strategic Risk Owners they are to actively engage with the Microsoft Teams platform and have regular communication with the Risk Manager.
- Active monitoring of internal and external environment to identify new or emerging risks through horizon scanning.

3.3 Risk Lead(s)

The Risk Lead (if appointed) acts on behalf of the Risk Owner who has delegated responsibility for monitoring, managing and reporting on the risk at local level.

Key responsibilities include;

- Operate in accordance with the risk management processes outlined in the Strategic and Operational Risk Management Guidance document.
- Ensure risks are monitored, managed and reported on in-line with the residual risk reporting frequency as detailed in section 2.3 of this policy (Table 3).
- Attendance at annual risk management training sessions as requested by the Compliance and Risk team.
- Holistic approach to risk identification with all related entities considered within the risk universe.
- Attendance at relevant committees (as required), such as Audit and Risk Committee, where in-depth reviews have been requested and representation is required.
- Assist the Risk Owner with the annual review of their assigned risk(s), conducted by the Compliance and Risk team.
- Liaise with appointed Risk Action Owners in-line with risk reporting frequency as per section 2.3 of this policy and update risk register accordingly.
- For strategic risks assist the Risk Owner in completion of the risk management assurance map which identifies the relevant lines of defence to each risk, and assurance coverage.
- For strategic Risk Lead's they are to actively engage with the Microsoft Teams platform and have regular communication with the Risk Manager.
- Active monitoring of internal and external environment to identify new or emerging risks through horizon scanning.

3.4 Risk Action Owner(s)

Risk Action Owners are senior officer(s) with operational responsibility for delivering against the future actions that have been identified, to bring the risk within the University's risk appetite and tolerance.

Key responsibilities include;

- Operate in accordance with the risk management processes outlined in the Strategic and Operational Risk Management Guidance document.
- Risk Action Owner is to ensure risk actions are monitored and the risk register is updated in-line with the residual risk reporting frequency as detailed in section 2.3 of this policy (Table 3).
- Attend annual risk management training sessions as requested by the Compliance and Risk team.
- Assist the Risk Owner or/and the Risk Lead with the annual review of their assigned risk(s), conducted by the Compliance and Risk team.
- For operational risks (residual score medium or above) verbal updates on assigned actions are to be provided quarterly in Senior Management Team meetings/College Board.
- For strategic Risk Action Owners they are to actively engage with the Microsoft Teams platform and have regular communication with the Risk Manager.
- Active monitoring of internal and external environment to identify new or emerging risks through horizon scanning.

3.5 Heads of Professional Service Departments, School and College Registrar

Each Area is responsible for:

- Risk Identification and management of risks inside own areas of accountability and maintenance of a Risk Register which is aligned to this policy and processes within the Strategic & Operational Risk Management Guidance document.
- Operate in accordance with the risk management processes outlined in the Strategic and Operational Risk Management Guidance document.
- Risk registers are to be updated on in-line with the residual risk reporting frequency as detailed in section 2.3 of this policy (Table 3).
- Risk escalations, de-escalations and closures are to be reported in-line with risk thresholds as per section 2.3 of this policy (Image 1)
- Agree (as advised by Risk Owner) requests for new risks (and review of new risk enquiry forms), risk escalations, de-escalations and/or risk closures.
- Operate in accordance with risk governance and register hierarchy as per section 2.3 of this policy (Image 2)
- Assist the Compliance and Risk team in the Annual Risk Management Report and in performance reviews which evaluates risk registers and their alignment to the risk management policy and guidance and adherence to roles and responsibilities as detailed within this policy.
- Ensure that senior level management attend risk management training sessions and workshops annually, delivered by the Compliance and Risk team.
- Ensure that (where possible) Risk Registers reflect the institutions' joint ventures, subsidiaries and partnerships.
- Ensure that all audit recommendations are reflected in risk registers.
- Act as a Risk Steward and nominate Risk Steward Deputy (see role definition in section 3.6/3.7).
- Lead on the formal review of risk register on a quarterly basis in senior management team meetings or at College Board.
- Active monitoring of internal and external environment to identify new or emerging risks through horizon scanning.

3.6 Risk Steward(s)

Each Risk Steward is responsible for:

- Championing the aims of this policy and promoting adherence to working to the institutions approach to risk management detailed in the Strategic and Operational Risk Management Guidance document.
- Be a point of contact to respond to any local risk queries.
- Actively engage with risk training workshops and Microsoft Teams platform as requested by the Compliance and Risk team and have regular communication with the Risk Manager.

3.7 Risk Steward Deputy

- Act as a delegate to the Risk Steward in periods of absence. Assist with risk register administrative duties as requested.

3.8 University Secretary's Office (Compliance and Risk Team)

The Compliance and Risk team is responsible for:

- Providing advice, guidance and support to staff on risk management.
- Ensuring that this policy and guidance is communicated, maintained, updated annually and that appropriate support and training is provided.
- Delivery of the Internal Communications Plan.
- To request and review copies of Operational, School and College Risk Registers annually to ensure that there is a central repository and a consistent approach to risk management, identifying any risks or trends from across the institution that may require escalation, de-escalation or closure.
- Annual review of risks detailed within the Strategic Risk Register.
- Monitor the effectiveness and consistency of the Risk Management Policy and guidance across all departments.
- Work in consultation with Internal Audit in the annual assessment of the University's risk maturity.
- Development, maintenance, actioning and monitoring of the Risk Management Improvement Plan.
- Perform risk management performance reviews.
- Producing and maintaining the Strategic Risk Register and reports (to include requests for new risks, escalations, de-escalations and risk closures) to VC, UEB, Audit & Risk Committee and Council.
- Create, deliver and facilitate risk training as described in this policy and maintain a staff training schedule and record of attendance at risk management training sessions.
- Develop risk management resources and provide advice on the risk management process.
- Perform an annual review of risk management processes and deliver report of findings from across the institution in the form of an Annual Risk Management Report, submitted to VC, UEB, Audit & Risk Committee and Council for oversight.
- Active monitoring of internal and external environment to identify new or emerging risks through horizon scanning.
- Engagement with external entities to enable benchmarking and horizon scanning.

3.9 Chief Risk Officer

The Chief Risk Officer is performed by the University Secretary and key responsibilities include:

- Promoting effective risk management across the institution and at a senior level on a day-to-day basis.
- Chairing and reporting the risk element at the Corporate Governance Compliance & Risk Group.
- Active monitoring of internal and external environment to identify new or emerging risks through horizon scanning.
- To undertake delegated responsibilities as directed by the VC and to provide the VC with oversight and direction on the management of risk across the University.

3.10 Leads for Major Projects/Portfolios/Programmes Risks

- Responsible for ensuring that project, portfolio, programme risk registers provide a high-level summary of risks, identified, managed and reported in-line with the Project Risk Management Framework.
- Risks in Projects/Programmes are managed within Project/Programmes Steering Groups and escalated through to the relevant Portfolio Board and UEB as required.

3.11 Internal and External Audit

Internal Auditors undertake audit work sufficient to allow them to provide an annual opinion to the Audit and Risk Committee on the adequacy and effectiveness of the University's arrangements for risk management.

External Auditors provide feedback to the Audit and Risk Committee on the operation of internal financial controls reviewed as part of the annual audit.

3.12 All Joint Ventures, Subsidiaries and Partnerships of Cardiff University

All joint ventures, subsidiaries and partnerships of Cardiff University are responsible for:

- Ensuring there is open communication between parties on any risk that could impact Cardiff University and its achievement of its strategic objectives.

4 Monitoring and Review

4.1 Risk Management Assurance and Mapping

Risk management assurance will provide a framework for Risk Owners to consider the evidence gained from a review of the effectiveness of the University's management of risk. Having acted or put controls in place, these should be monitored for effectiveness at a frequency that is suited to the risk exposure. This will mean that Risk Owners will need to carry out a review of internal controls to report on their effectiveness as part of the risk management process. A risk assurance process can be used to independently test whether the risk policies, procedures and related controls are functioning as intended.

Developing a Risk Assurance Framework will assist the University to ensure that there is assurance across the University's strategy, strategic risks and legislative/statutory requirements and that this is captured and reported appropriately to relevant Committees.

An assurance map, detailing the 3 lines of defence will be produced to accompany each iteration of the Strategic Risk Register and will be reported concurrently with the Strategic Risk Register.

The purpose of the assurance map is to provide additional assurance that all risks identified in the Strategic Risk Register are being managed effectively and efficiently.

An assurance map identifies the relevant lines of defence that relate to each risk, and plots assurance coverage against risk controls. It enables the University to determine whether assurance activities are sufficient for risks, whether assurance activities are being duplicated or whether additional assurance activities are necessary for risks with inadequate coverage.

The University's Risk Assurance Map will be a living document and subject to ongoing review as risks are developed and controls put in place.

4.2 Policy Monitoring

To supplement the annual Internal Audit of Risk Management, the Compliance & Risk team will formally review the Risk Management Policy annually.

The following areas of activity will support the embedding of the Risk Management Policy and guidance.

1. Maintain a staff training schedule and record of attendance at risk management training sessions.

2. Perform a periodic review of the active management of risks and adherence to this policy;
   - Quality and content of risk assessments, risk registers and reports
   - Role of Risk Owners, Risk Leads and Risk Action Owners and frequency/quality of risk updates provided
   - Assurance mapping process
   - The role of Risk Stewards

The findings of the risk management policy monitoring will be reported periodically to the Corporate Governance Compliance & Risk Group with a zero tolerance to non-adherence to this policy. Any non-conformance will be reported in the first instance to the Corporate Governance Compliance & Risk Group and escalated (if deemed necessary) to VC, UEB and Audit and Risk Committee governance channels.

5. Related Policies and Procedures

This policy is to be read in conjunction with the Strategic and Operational Risk Management Guidance document.

For Portfolio, Programme or Project guidance please refer to the Project Risk Management Framework.

To view information on the Risk Management Software 4Risk click here

To view the Major Incident Plan click here

If you have any queries around the content provided within this document and how to interpret it, please contact the Compliance and Risk Team via complianceandrisk@cardiff.ac.uk

6. Version Control Information

If you require a copy of this policy in large print or another format, please contact the Compliance and Risk Team: complianceandrisk@cardiff.ac.uk."

The Policy states that a Welsh language version is available.

Mae'r ddogfen yma hefyd ar gael yn Gymraeg

Document Name	Risk Management Policy	
UEB Policy Sponsor	Claire Sanders, Chief Operating Officer, USO	
Policy Owner	Claire Sanders, Chief Operating Officer, USO	
Policy Author(s)	Daisy Gandy, Senior Risk Manager, USO	
Version Number	*1.3*	
Equality Impact Outcome and Form Submission Date	TBC	

Privacy Impact Assessment outcome (where applicable)	N/A	
Approval Date	07/November/2023	
Approved By	Vice-Chancellor (UEB)	
Date of Implementation	*08/01/2024*	
Date of Last Review	*November 2023*	
Date for Next Review	*November 2024*	
For Office Use – Keywords for search function		

7. Change History Record

The table below should be completed by the Author each time a change is made to the policy

Version amended	Description of Change	Version created
2017	New policy template used. Revised risk terminology agreed by the University. Reviewed risk appetite classifications and the University's statement of risk appetite Tolerance ranges introduced. Risk thresholds introduced Revised risk register hierarchy and risk reporting frequency. Revised risk scoring criteria. Revised risk governance. Revised roles and responsibilities for managing risk. Revised information on risk assurance and mapping. New monitoring procedure for policy. New related policies and procedures included.	19/07/2023
04/04/2024	Table 3 Residual Risk Monitoring and Updating of Register Frequency updated for Major and High risks from every month to every quarter.	04/04/2024
22/04/2024	Risk Steward Deputy role added to section 3.5 and 3.7, risk management performance reviews added to sections 3.5 and 3.8 and section 3.5 updated to include ask; Ensure that all audit recommendations are reflected in risk registers and responsibility to review new risk enquiry forms.	23/04/2024