Strategic & Operational Risk Management Guidance

The following guidance is in adherence with ISO31000's approach to risk management and compliments the institution's Risk Management Policy.

Step 1: Scope, Content & Criteria

The purpose of establishing the risk scope, the context and criteria is to customize the risk management process, enabling an effective risk assessment and tailored risk treatment.

You need to be thinking about whether this is a new risk that has been risk assessed, an escalated risk, a closed risk, a risk identified from an issue or incident or a risk that requires assessment.

Does this risk relate to strategic, professional service, project or portfolio, school or college objectives?

Is it an opportunity or a threat? And what constraints, limitations or assumptions need to be discussed/documented?

Step 2: Risk Identification

Make sure that what you are identifying is actually a 'risk' and not an impact or cause OR something that has already happened or is happening now (this is an issue or incident) **See Appendix A on guidance on Risks versus Issues and Incidents**

A 'risk' is: something that might happen which, if it occurred, could prevent the University from fulfilling its objectives.

Key things to remember:

Contributing factors (causes) can be both internal and external.

Causes can be hypothetical; even if a contributing factor is unlikely to materialize, if there would be a notable impact on the department should it occur, it's probably worth including.

Be brief – try and keep each factor down to one bullet point.

The risk register should include the headlines, not the detail.

Event, Cause, Impact, Objective

Once you have identified the risk event, it is helpful to use the following approach:

'If [uncertain event]…. Due to (Causes) Then this could result in [most significant impacts]….meaning the (un-achievement of which objectives)

Step 3: Risk Analysis - Score Risk at Inherent level

Now you have your risk articulated you need to score the risk at inherent stage which involves rating the likelihood and impact of the risk in the absence of all controls, its raw state.

Ensure at this stage that you are rating the most significant impact. **Refer to Appendix B to review the impact categories and scoring criteria for likelihood and impact**.

Note, it is expected that the Inherent risk score will only change when the internal or external environment surrounding the risk changes.

Step 4: Identification of Implemented Controls

Once scoring at inherent stage has been completed the Risk Owner is asked to review what implemented controls are in place for the identified risk.

If the risk is entered onto the 4Risk Management software Risk Owners will be asked to link controls to identified risk causes and impacts. This will enable the Risk Owner and Risk Manager to clearly identify worth of controls and view any gaps in mitigation.

Tools such as the Fishbone and Risk Bow Tie method are support tools which can be requested from the Risk Manager if required.

Step 5: Re-Score Risk at Residual Level

Residual is the status of the risk at the present time, considering the implemented controls identified in step 4.
Risk Owners are asked to refer to Appendix B once more to re-score risk but now considering implemented controls.
Key things to remember:
If the overall risk status has remained the same as the inherent score (either in terms of likelihood or impact) then you need to consider *why* your implemented controls are not effective.
The residual risk score should never be higher than the inherent risk score.
It is expected that the residual risk score will change over the lifetime of the risk and completed future actions will be added to the list of implemented controls and the residual scoring will reflect this.
If the risk is outside of tolerance the Risk Owner is asked to consider the 4 T's (Treat, Tolerate, Terminate, Transfer) in their response to the risk.
Further guidance on the 4T's can be found within **Appendix D Risk Response Guidance.**
Once all future actions have been completed the residual risk score should match the target score as the target score includes implemented controls and future actions.
The goal is for the target score to be within or below the risk appetite score and once the residual risk score meets tolerance the risk can be considered for closure.

Step 6: Risk Evaluation Stage

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis (inherent and residual risk scores) with the established risk criteria (Risk Appetite and Tolerance Classifications and Statements) to determine where additional action is required.

Risk Owners are asked to view **Appendix C Residual Risk Appetite Classifications & Risk Tolerance Ranges** to identify if the residual risk score is within the acceptable tolerance range. Note, the tolerance range is assigned to the most significant impact category of the risk.

Step 7: Treat Risk - Risk Treatment Stage

The purpose of risk treatment is to select and implement options for addressing risk. As a Risk Owner if you are to Treat the risk you need to identify future actions to enable the achievement of the residual risk being within or below the assigned risk tolerance scoring range.

<u>Key things to remember</u>:

Set realistic and achievable target dates for the completion of actions.

You should have future actions identified and if you do not you need to ask yourself why. Is it that there are no future controls possible for the risk? If that is the case you need to consider whether the risk can be tolerated or activity terminated or shared (the 4T's).

Remember, any completed future actions get moved to the implemented controls list and a review of the residual risk score is required at that stage.

The target score is a score that considered all implemented and future actions so if you add any new future actions you need to ensure that the target score considers any new future actions.

For future actions that require further resource to implement actions are to include details on route of request.

Will there be a single Risk Owner identified to manage, report and monitor this risk or in addition to the Risk Owner who holds overall risk accountability will there be a Risk Lead who will manage the risk at local level.

Have you assigned Risk Action Owners for all future actions?

For risks detailed on the 4Risk management software ensure each future action is assigned a rate of priority (High, Medium or Low) in terms of its completion.

Step 8: Scoring Risk at Target Level

It is at this stage where the risk is scored for the third time but this time taking into account <u>all implemented controls and all future actions.</u> **Refer to Appendix B to review the impact categories and scoring criteria for likelihood and impact.**

<u>Key things to remember:</u>

The target score will give the Risk Owner an indication of where the risk sits fully mitigated and will allow the Risk Owner to compare the target risk score with the assigned risk tolerance score.

Should the target score not be within or below the risk tolerance category this will indicate to the Risk Owner that more work is required to mitigate this risk and additional future actions are to be considered in the treatment of the risk.
All risks whether recorded at University level cannot be closed unless the residual risk score is on par or below the assigned risk tolerance score.

Step 9: Risk Assurance

Once a strategic risk entry is entered onto the risk management software (4Risk) Risk Owners work in consultation with the Risk Manager to detail the 3 lines of defence and assign assurance ratings on all implemented controls.

See Appendix E for guidance on the 3 lines of defence framework.

Risk Monitoring, Governance, De-escalation, Escalation or Closure and Process for Updating Risk Register

See Appendix F to view roles and responsibilities of risk contacts.

See Appendix G to view Residual Risk Monitoring and Updating of Register Frequency

For risks recorded on the 4risk, risk management software: To request a risk escalation to strategic level, de-escalation to operational level or risk closure Risk Owners are asked to review and edit the risk entry on the 4Risk Management system by clicking on the relevant analysis code, either:

- Request Escalation to Strategic Register
- Request De-escalation to Operational Register
- Request Risk Closure

Once the analysis code has been selected either the Risk Manager, Head of Professional Service Area, College Registrar or PVC will review the request in their risk dashboard. In addition to selecting the relevant analysis code the Risk Owner is asked to provide a rational for escalation, de-escalation or closure within the risk update section of the risk entry.

On receipt of request for strategic requests the Risk Manager will review the rational and include the risk within the necessary governance channel for approval to be sought from the Vice Chancellor. Decision to be communicated to the appointed Risk Owner and Risk Manager to update the 4Risk, risk management system in-line with decision. For Professional Service or College level risks decisions are to be made in-line with the institutions roles and responsibilities, with decision communicated to the Risk Owner and software updated with new analysis code. Note, requests for risk escalation, de-escalations and risk closures are to be aligned with the risk management policy risk thresholds with School and Team/Departmental requests to be made in senior management team meetings.
See Appendix H to view Risk Thresholds and Risk Register Hierarchy.

Risk Management Training

The aim of the tiered risk management training is to enable all staff and members to meet their Risk Management responsibilities outlined in the Risk Management Policy:

Level One – **Risk Management Awareness - General.** This will be provided to all staff on induction, as part of the in-person 'Welcome to Cardiff University' Induction. The intended learning outcomes are to understand what risk is, what risk management is, how a risk is reported and how the organisation's risk appetite and culture operates.

Level Two – **Practical Risk Management – Targeted.** This level of training is available to all staff but is targeted towards staff with a risk facing role, senior management, appointed risk owners, risk leads, secondary risk leads, future action owners, action owner assignees or risk stewards. Level Two training is available on the staff Intranet page under Supporting your work - Your work environment – Strategic & Operational Risk Management and does not require repetition, though this does not mean that additional risk related training and education should not be identified through PDR. This training will be in four parts:

- **Part 1**. To understand the key principles within the Risk Management Policy, Guidance & New Risk Enquiry Form the 'An Introduction to Risk Management Processes' video (20 minutes) informs the viewer on our Institutional approach to risk.
- **Part 2**. To test your level of understanding on the risk management process by completing the 'How much do you know about Risk' quiz (10 minutes).
- **Part 3.** Attendance as requested at bespoke, ad hoc training sessions facilitated and delivered by the Compliance and Risk Team on an individual/department/group or University Executive Board need's basis on key themes such as; the use of 4risk/electronic risk registers and risk assessment process/tools to include; identification techniques, scoring and analysis, evaluation and treatment and assurance mapping.
- **Part 4.** Staff are invited to attend the internal risk management course on 'Risk Management, The Basics' delivered through Staff Development.

Level Three – **Audit & Risk Committee, Finance & Resource Committee and Council.** Level three is divided into 2 parts: Awareness of risk management processes and practical experience.

- **Part 1. Awareness:** At induction members are signposted to the Risk Management Policy, Guidance document, the latest Annual Risk Management Report and Strategic Risk Register.

- **Part 2. Practical:** Members will be advised on ad-hoc, theme specific risk management courses/tutorials delivered to support risk management activity and member's needs. Example themes are, understanding risk appetite and tolerance, horizon scanning of risk environment and risk analysis techniques in practice.

To request risk management workshops or 1-1 training please contact the Compliance and Risk team at Complianceandrisk@cardiff.ac.uk

Appendix A Guidance Note on Risks versus Issues and Major Incidents

Introduction

This note has been created based on feedback from those responsible for risk management activity across the University and sets out the difference between risks, issues and major incidents and their management.

High level overview – what's the difference?

Figure 1 below details the definitions on risks, issues and major incidents.

Figure 1 – risks versus issues

Risk	Issue	Major Incident
A Risk is defined as a threat, an uncertain, Future event that could adversely affect the achievement of objectives. A risk can **be mitigated against** to prevent the risk from becoming an issue.	**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. Prevention is not possible due to the level of certainty that the event will occur/has occurred so unlike a risk an issue can not be mitigated.	**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

Differences in treatment

A **risk** is identified, assessed, analyzed, evaluated, recorded and reported on a risk register. Risks can be planned for based on the anticipated likelihood and impact and the introduction of treatment plans/future actions to mitigate them to acceptable levels.

Risk responses include:

a) Treat

b) Tolerate
c) Transfer
d) Terminate

An **issue** is a problem that has occurred and has a material impact on objectives.
Issues are not managed through risk management processes with risks materializing into an issue removed from risk register monitoring and reactive response management at local level required. If deemed necessary the issue can be recorded and monitored through the use of an Issue tracker. To request a template please contact the Risk Manager (Gandyd@cardiff.ac.uk)

An **incident** is R.A.G. rated and depending on the level of incident this can be managed by either a local or major incident team in accordance with the University's Major Incident Plan and Local Business Continuity Plans.

Appendix B 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 Opportunities may result in some commercialisation opportunities	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 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

Appendix C: Residual Risk Appetite Classifications & Risk Tolerance Ranges

Risk Appetite Classifications	**Description (summarized 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**

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		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

				11-16		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 authorized 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 authorized 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 authorized 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.

Appendix D Risk Response Guidance

Terminate (avoid / eliminate)	Do things differently and thus avoid the risk.
Treat (control / reduce)	Take action to control the risk either by reducing the likelihood of the risk developing or limiting the impact should the risk materialize.
Transfer (Insurance / contract)	Can some parts of the risk be transferred/shared via insurance, contractual arrangements or accepted by third parties.
Tolerate (accept / retain)	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.

Appendix E: Three Lines of Defence Framework

The Risk Management Process is part of the University's internal control system, which can be considered under the "Three Lines of Defence" framework. The three lines of defence model sets out how the different parts and levels of the University play important roles in effectively managing risk.

The First Line of Defence

In the first line of defence are managers and those who are responsible for operationally identifying, owning and managing risks, following approved policies, procedures and guidelines set by Cardiff University to manage risk. In the first line of defence, they are responsible for:

- **Compliance with all relevant policies and procedures -** those who manage risk should be fully conversant with policy requirements that are required within their area of responsibility, implementing those requirements, monitoring that policy requirements are being fulfilled.
- **Risk Assessment -** ensuring that risks are identified and assessed within their management areas.
- **Implementing risk treatment –** As per the 4 T's to risk response.
- **Risk monitoring** - comprehensive and regular monitoring of risks and controls via the risk register. The updates provided by risk owners to the formal risk reporting cycle should evidence that risks have continued to be managed between the reports within the cycle and highlight any changes in score

and/or actions. Future Actions to improve existing or implement additional controls should be monitored to completion by the risk owner, with any resulting impact on the risk profile reflected in the scoring. Risk monitoring should include an assessment of new information that changes the risk profile, in addition to reviewing controls in place and action plans already in progress.

- **Risk based decision-making** Risk assessment is built into various committee-reporting templates to enable committees to consider the risks of any proposals being made.
- **Business Continuity planning** sets out how the University (or departments thereof) would continue to manage key operations should a major event or situation occur.
- **Business planning and budgeting** - set objectives, agree action plans, and allocate resources considering risk. Progress towards meeting objectives is monitored regularly.

The Second Line of Defence

The provision of effective policies, frameworks, tools, techniques and support to enable risk and compliance to be managed in the first line. Second line of defence is interested in ensuring there is sufficient training and skill in the first line to identify risk, ensuring monitoring is carried out to judge how effectively policies are being implemented in practice, and ensuring effective tools are in place enabling risks are being assessed and managed.

The types of controls within this defence line are (not exhaustive):

- **Communication and training on internal controls** – All new staff are required to carry out mandatory training. Local inductions are in place to appraise staff of the risks in the work environment. Training and development in the management of risk topics, policies and procedures is widely available.
- **Competent Advisors** – the University employs a number of competent advisors across various subject matter, who set policy, give advice, support and training to those in the first line, on the management of risk. From time to time, the use of external consultants to review risk controls in specific areas may prove necessary, the engagement from specialist third parties for consulting and evaluating may be required.
- **University policies and procedures** – University policies set out how core and regulated activities of the University must be carried out. Written procedures support the policies where appropriate.
- **University Compliance Framework and Monitoring**- The Compliance Framework is the University register of all legislative, regulatory and policy requirements that the University is obligated to, or has chosen to, comply with.

The Third Line of Defence

The third line of defence is in place to assess and evaluate, on behalf of the governing body and UEB that the controls in place within the first and second lines of defence are working effectively and provide recommendations on any areas that can be improved. The third level can also be used to give independent assurance to regulators that appropriate controls and processes are in place and operating effectively.

- **Internal Audit** – appointed by Council, the Internal Auditor will review key processes, evaluating risk controls and report findings to the Audit and Risk Committee. This include highlighting where findings indicate an increased level of risk. Audit and Risk Committee provide UEB with the final audit reports and its opinion on the management of the risks identified.
- **External audit** – appointed by Council, this focuses specifically on the effectiveness and accuracy of financial controls and provides feedback to the Audit and Risk Committee as part of the annual audit review. The External Auditor also provides sector benchmarking information to inform Audit and Risk Committee's assurance that the University has identified the relevant risks.

Appendix F: Roles and Responsibilities of Risk Contacts

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.

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.

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 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.

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 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 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.

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 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.

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 policy (Table 3).
- Risk escalations, de-escalations and closures are to be reported in-line with risk thresholds as per section 2.3 of 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 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 of policy).
- 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.

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.

Risk Steward Deputy

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

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.

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.

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.

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.

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.

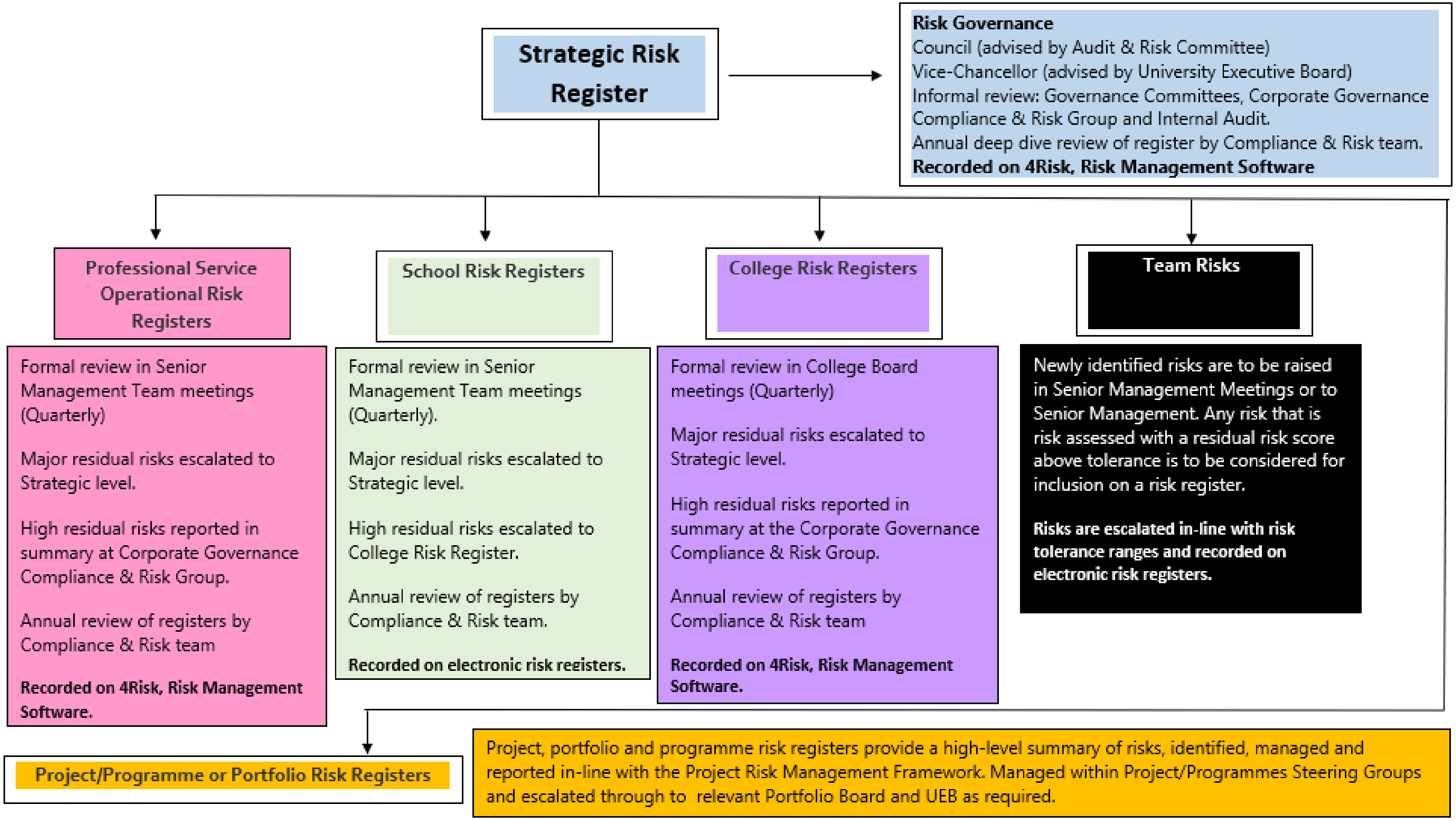
Appendix G to view Residual Risk Monitoring and Updating of Register Frequency

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**

Appendix H Risk Thresholds and Risk Register Hierarchy

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.



Strategic Risk Register

Risk Governance
Council (advised by Audit & Risk Committee)
Vice-Chancellor (advised by University Executive Board)
Informal review: Governance Committees, Corporate Governance Compliance & Risk Group and Internal Audit.
Annual deep dive review of register by Compliance & Risk team.
Recorded on 4Risk, Risk Management Software

Professional Service Operational Risk Registers

Formal review in Senior Management Team meetings (Quarterly)

Major residual risks escalated to Strategic level.

High residual risks reported in summary at Corporate Governance Compliance & Risk Group.

Annual review of registers by Compliance & Risk team

Recorded on 4Risk, Risk Management Software.

School Risk Registers

Formal review in Senior Management Team meetings (Quarterly).

Major residual risks escalated to Strategic level.

High residual risks escalated to College Risk Register.

Annual review of registers by Compliance & Risk team.

Recorded on electronic risk reeisters.

College Risk Registers

Formal review in College Board meetings (Quarterly)

Major residual risks escalated to Strategic level.

High residual risks reported in summary at the Corporate Governance Compliance & Risk Group.

Annual review of registers by Compliance & Risk team

Recorded on 4Risk, Risk Management Software.

Team Risks

Newly identified risks are to be raised in Senior Management Meetings or to Senior Management. Any risk that is risk assessed with a residual risk score above tolerance is to be considered for inclusion on a risk register.

Risks are escalated in-line with risk tolerance ranges and recorded on electronic risk registers.

Project/Programme or Portfolio Risk Registers

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