Risk Management Procedure	
Enabling Policy Statement; Executive Owner; Approval Route:	Our Operations - Chief Operating Officer - Operations Committee
Is the Procedure for internal use only (Non-disclosable)?	Disclosable
Associated Policy Statements:	n/a
Authorised Owner:	University Secretary and General Counsel
Authorised Co-ordinator:	Head of Governance Services
Effective date:	1 December 2023
Due date for full review:	October 2026
Sub documentation:	-

Approval History

Version	Reason for review	Approval Route	Date
1.0	Move to new template and regular update due	Operations Committee Executive Board Audit and Assurance Committee by electronic resolution	13/09/2023 26/10/2023 12/12/2023

1. Purpose

In accordance with the Terms and Conditions of funding for higher education institutions (OfS), this procedure ensures that there are effective arrangements for providing assurance to the governing body that the University has a robust and comprehensive system of risk management. The Procedure defines the strategy, principles and governance structure to support Risk Management consistently throughout the University of Surrey. The purpose of this document is to:

1.1 Set out a common approach and minimum requirements for risk management activities within the University of Surrey for use by all staff, as appropriate to their roles;
1.2 Provide guidance to support the risk management approach;
1.3 Enable the University to meet the expectation of Council with regard to risk management; and
1.4 Enable effective risk management in order to benefit the University through operational improvement and informed strategic decision making.

2. Scope and Exceptions to the Procedure

Compliance with the Risk Management Procedure is mandatory for all staff, contractors and staff in subsidiary companies.

3. Definitions and Terminology

Action Owners
Members of staff responsible for ensuring mitigating actions against identified risks are completed within specified timescales.

Gap to (risk) appetite
The difference between the net and the target risk score for a risk. For example, if the net score is 20 and the target score is 12, there will be a gap to appetite of 8.

GOAT
The Corporate Risk Management system currently in use.

Gross (inherent) risk score
Risk score (likelihood x impact) if no controls were in place.

Impact
How great an impact would this risk have if it were to occur. Impact could be in many areas, including financial, reputation, human resources, market valuation, etc. Scored from 1 (low) to 5 (serious).

Likelihood
The probability or frequency that the risk will crystallise. Scored from 1 (rare) to 5 (almost certain).

Net (residual) risk score
Risk score (likelihood x impact) once existing controls have been taken into account.

Risk
An uncertain event or situation which, should it occur, would have an adverse effect on the University's ability to achieve its goals and objectives.

Risk appetite
Council's expression of the types and amounts of risk it is willing to take or accept in pursuit of its objectives.

Risk Champions
Members of staff who act as conduits for senior managers to input changes to risk information on the risk management system and can be contacted to offer advice on risk methodology.

Risk Owners
Members of staff who have been assigned the responsibility for identifying and assessing risks in a designated area.

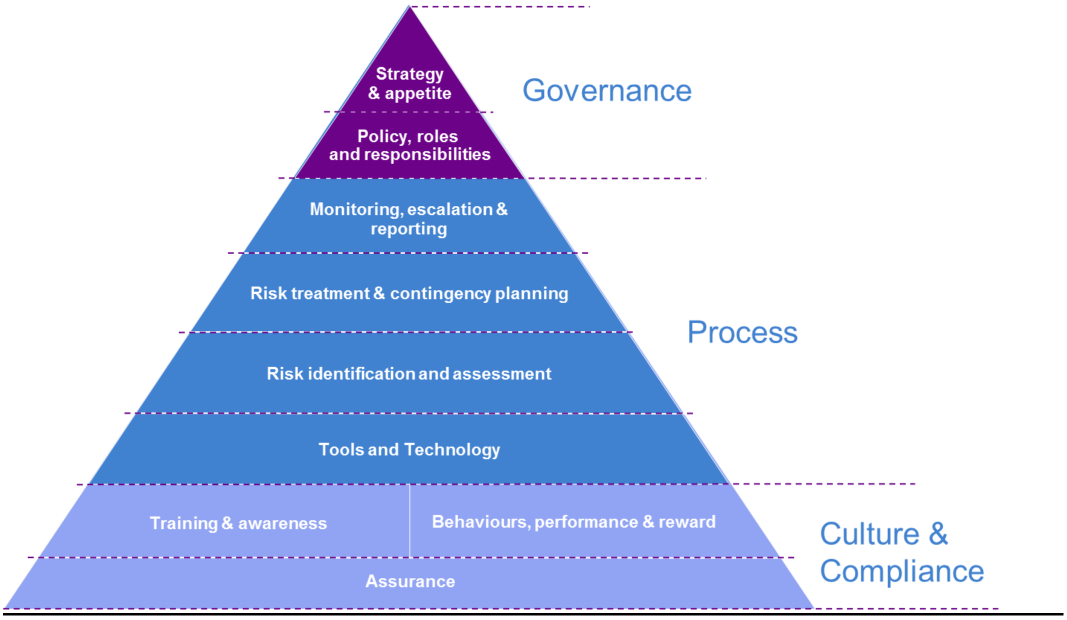
Target risk score
A reflection of risk appetite at a granular level. Outstanding actions are designed to take the risk down to the target level.

4. Procedural Principles

4.1 What is Risk Management?

Risk management is the set of activities that enables the identification, assessment and management of risks throughout the University. The University of Surrey's risk management framework, which comprises the governance, process, culture and compliance activities that support robust, embedded and consistent risk management, is depicted below.

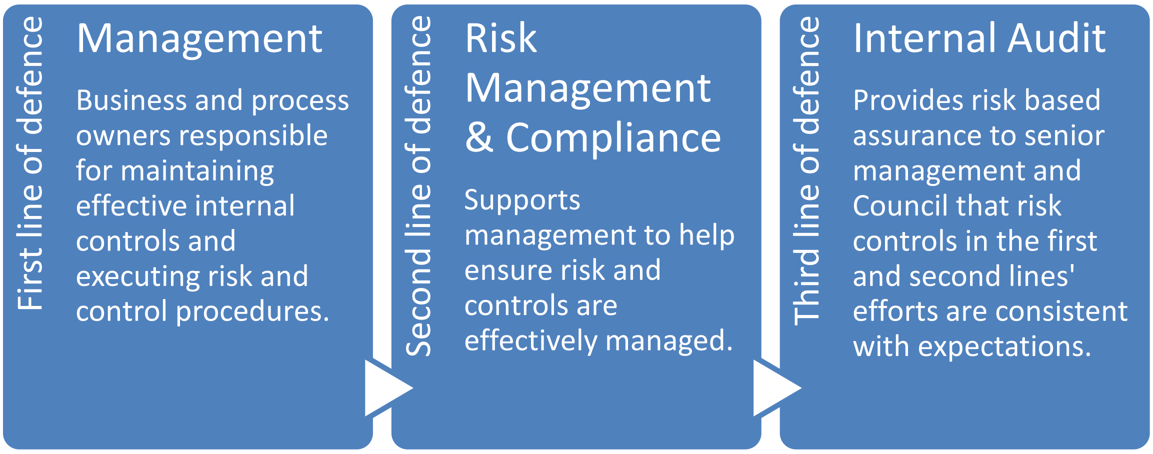
Risk management is a core component of the University of Surrey's wider governance and internal control framework, including the committee structure and the Scheme of Delegation, which provides the overarching structure through which the University is managed to achieve its objectives.


Strategy & appetite
Policy, roles and responsibilities
Governance
Monitoring, escalation & reporting
Risk treatment & contingency planning
Risk identification and assessment
Tools and Technology
Process
Training & awareness
Behaviours, performance & reward
Assurance
Culture & Compliance

An effective system of Risk Management provides the University of Surrey with many benefits, including:

- Informed risk decision making to help deliver consistent and improved business performance by the avoidance of unwanted surprises and the realisation of opportunities.
- Identification and mitigation of key risks that could have a material impact on the achievement of business objectives.
- Consistency and clarity in accountability and ownership for managing risks, enhancing governance.
- An improved view of key controls, their effectiveness and gaps in the control environment, enabling optimisation.
- A clear path to raise significant risks to senior management and the Council.
- A proactive, risk aware culture across the University.
- Assurance to Council and Audit and Assurance Committee that processes and behaviours are embedded to ensure significant risks are routinely and consistently identified, understood and effectively managed.

Risk Management is part of the 'Three lines of Defence' model:



First line of defence

Management

Business and process owners responsible for maintaining effective internal controls and executing risk and control procedures.

Second line of defence

Risk Management & Compliance

Supports management to help ensure risk and controls are effectively managed.

Third line of defence

Internal Audit

Provides risk based assurance to senior management and Council that risk controls in the first and second lines' efforts are consistent with expectations.

4.2 Risk Management strategy

The University of Surrey strategy for Risk Management is that all significant risks to the achievement of our objectives are identified, assessed and managed within Risk Appetites. To achieve this, Council and management promote a culture that encourages routine consideration of risk in key decisions and supports integration of risk management with our critical processes and ways of working.

The purpose of risk management is **NOT** to eliminate risk, or to make the University of Surrey risk averse – controlled risk taking is something we must continue to do in order to achieve our objectives and be successful. Its purpose is to support better decisions through an improved understanding of risk, which means taking the right risks for the right benefits and returns.

The objectives of our Risk Management strategy are to:

- Identify and understand all the significant risks that we face;
- Select and proactively take the risks that give us the right returns, and understand their potential impact on the University;
- Take action to manage the risks we do not want to be exposed to, ensuring our resources are effectively and efficiently prioritised and used; and
- Monitor and report the risks we are taking against our desired risk appetite.

Every employee is responsible for helping us to effectively manage our risk exposures making us a more resilient organisation, able to successfully respond to our changing environment. The

Governance and Risk Assurance department will support the business as outlined in section 4.6, in meeting the requirements of this Procedure to consistently and effectively manage all the key risks the University faces.

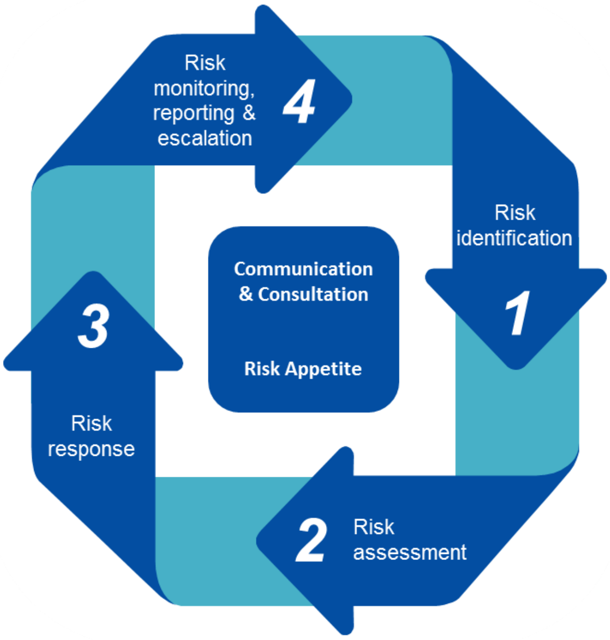
4.3 Principles

The key principles of our Risk Management approach are outlined below:

- It is the responsibility of all staff (as appropriate to their roles) to ensure they understand and comply with this Procedure.
- Our approach to identifying and managing risks, including the use of common risk management terminology, shall be consistently applied across the University. Note that this Procedure does not aim to replace specialist risk management techniques used in certain areas of our business such as Health and Safety but aims to establish a common language for risk and achievement of minimum standards of practice and rigor in risk management throughout the whole organisation.
- Risk management shall be embedded in all key processes and decision points (e.g. business planning, maintenance, stakeholder engagement etc.) as well as day-to-day operations.
- A clear risk management governance structure exists that defines accountability and supports direction and control of risk management across the University and its subsidiaries. All risks are individually assigned a Risk Owner who acts as a single point of accountability for its management.
- Our desired risk-taking approach (i.e. the amount of risk we are comfortable taking) is defined via Risk Appetites and our key risk exposures are being managed in accordance with it.
- The reporting and escalation of risk information should be timely and accurate and cover all key risks to support management decision making at relevant levels of the University. The reporting and escalation of a risk does not, however, pass on risk ownership.
- Risk Owners are responsible for identifying and managing the risks to their respective business areas and gaining assurance that the Risk Management framework is operating effectively.
- Risk Management awareness and training will be provided to all staff as appropriate to their roles and responsibilities.
- All corporate risks identified will be recorded in GOAT.

4.4 The Risk Management Process

The four main stages of the University of Surrey’s risk management process are set out in the diagram below.


Risk monitoring, reporting & escalation
4
Risk identification
1
Communication & Consultation
Risk Appetite
3
Risk response
2
Risk assessment

1. Risk identification

The first stage in the risk management process involves the identification and description of all risks that could affect business objectives and includes establishing the context and environment of the business area under review and agreeing appropriate risk ownership and categorisation.

To ensure that the University of Surrey's risk profile is complete, the Executive Board conducts a "top down" (looking across or down from the top of the University) strategic risk identification exercise on an annual basis. This supplements the Directorates' "bottom up" (identifying risks at operational levels of the University and working up) risk evaluation that is performed monthly / quarterly. In addition, consideration of risk is also embedded into key processes including budgeting, business planning and performance management.

All identified risks are captured in GOAT. Risk descriptions include details of the event, the risk's root causes, and the potential consequences should that risk crystallise (which aids in deciding actions to take and necessary controls).

2. Risk assessment

Once risks have been identified, an estimation of their potential likelihood and business impact is needed to determine whether they are of concern and require a management response with, for example, implementation of controls and mitigation; this is called risk assessment.

All risks are assessed from three perspectives:

- a Residual or Net basis, assuming controls and mitigating activities already in place work as intended;
- an Inherent or Gross basis, assuming the controls and mitigating activities do not exist or do not work as intended; and
- a Target basis, capturing the desired level of risk exposure based on Risk Appetite.

Assessing risks in this way supports understanding of the reliance placed on existing controls and mitigation, the worst-case scenario for the risk, and how acceptable current levels of exposure are compared to Target positions i.e. the 'Gap to Appetite'. This helps to inform the focus of management oversight and challenge as well as prioritisation of responses.

The impact and likelihood values of risks are assessed over an annual time horizon, using the University of Surrey scoring criteria, which consist of five-point severity scales. This allows reliable and consistent measurement and comparison of risks on a like-for-like basis.

The Risk Owner is responsible for agreeing the assessed size of each risk.

3. Risk response

Where the Residual/net severity of a risk exceeds acceptable levels (i.e. is not aligned with Target levels) then appropriate actions may need to be selected and implemented to bring the Net risk position in line with the Target risk position and close the gap to appetite.

Options to respond to a risk can typically include:

- Reduction, with controls and mitigation;
- Transfer, with insurance and contracts;
- Avoidance, by stopping or changing the activity that gives rise to the risk; and
- Acceptance, if the benefit of taking the risk justifies the potential downside exposure or further responses are not feasible or cost-effective.

The Risk Owner retains overall accountability for the management of the risk, though Action Owners can be assigned to have responsibility for the implementation of specific response activities.

Details of all planned activities and delivery milestones shall be detailed in Risk Response Plans and recorded in the corporate risk system.

4. Risk monitoring, reporting & escalation

Risk monitoring and reporting involves the timely tracking, capture and sharing of risk information to enable review and notification of changes in risk exposure by management. It supports understanding and decisions on risk responses to be made, including potential management interventions to avoid a risk occurring or reduce its impact should it occur.

In addition to monitoring of individual risks, the Audit and Assurance Committee, on behalf of Council, also undertakes on-going performance monitoring of the systems of risk management and internal control to assure they are effective and performing as expected. A Risk Update Report is issued to, and reviewed by, the Audit and Assurance Committee at each of their four meetings every year.

The University of Surrey have implemented a 2-level taxonomy with which to report and rank their corporate risks.

Risks at Level 1 are made of 12 categories with which to capture risks from all parts of the business. The risks at Level 1 are selected for our 'Principal risks'. The principal risks we face are annually approved and disclosed in The University of Surrey's Annual Report.

Principal risks are those risks that are considered by the Executive Board and Council to have the greatest potential to affect the achievement of our strategic objectives, inherently derived from the nature of our activities as a University or as specific risks to the University priorities.

Level 1 risks are used for reporting and ranking purposes to the Executive Board and Audit and Assurance Committee. All risks on level 1 will have a risk appetite statement prepared for them.

Risks at Level 2 are those risks that are recorded on the corporate risk register. These are aligned to the respective level 1 risks and represent all the risks (at an enterprise level) that areas of the University manage as part of their activities.

Level 2 Risks that exceed the escalation thresholds (significant Gap to Appetite or net score of 15 or higher) are reported to, and reviewed by, the Executive Board sub committees with oversight responsibilities, as well as at Executive Board prior to the Audit and Assurance Committee's quarterly meetings. Key strategic risks are reviewed by the directorates monthly or quarterly, and significant changes are communicated to Executive Board and/or its sub-committees.

The thresholds for risk escalation, based on the scoring criteria where a risk rating of 25 is the most severe and 1 is the least, are:

- Risks with a significant differential between residual/net score and target score i.e. a large gap to appetite as agreed by the relevant committee.
- Risks with residual/net score of 15 or greater; and
- Risks that have an inherent/gross and residual/net impact score of 5 that have been separately identified as a 'HILL' (High Impact Low Likelihood).

Outside of monthly risk reporting, any new risks that are identified from ongoing business activities and analysis, or risks that have been detected via monitoring to have changed in severity, that meet the escalation criteria, should be immediately communicated to the Chair of Executive Board or the relevant sub-committee. In turn, these risks will be escalated to the Executive Board and Audit and Assurance Committee in line with the agreed escalation process.

4.5 Communication, Consultation and Appetite

Communication and consultation are key factors in all stages of the risk management process, ensuring appropriate individuals are engaged who can, for example, contribute to a better understanding of the nature and details of a risk, as well as those who could be specifically affected by it. It is also critical to ensuring that accountable decision makers and management receive the right types of information at the right time and are engaged to provide their views and share their experiences.

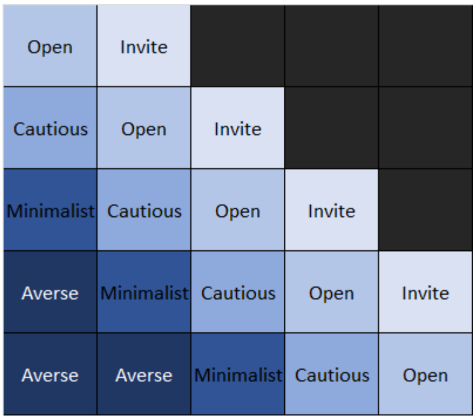
Risk appetite, which is Council's expression of the types and amounts of risk it is willing to take or accept in pursuit of its objectives, is also a key consideration throughout the risk management process, helping inform the University’s understanding of the levels of risk that is deemed to produce required returns, and those risks that are not acceptable and require management responses, escalation and reporting.

Executive Board has developed risk appetite statements for each Level 1 Principal risk of the University. These are reviewed by Executive Board, Audit and Assurance Committee and Council on an annual basis. These contain a formal classification of the appetite, a high-level summary of the statement, and the key drivers associated with the principal risk over which we can implement controls. The degree of mitigation implemented is a clear expression of the University’s risk appetite. Risk appetite statements will be cascaded to risk owners and champions on an annual basis.

Our appetite scales are defined in the following table:

	Averse	Minimalist	Cautious	Open	Invite
Appetite scale	Avoidance of risk and uncertainty is a key organisational objective	Preference for ultra-safe business delivery options that have a low degree of gross risk and only have a potential for limited reward	Preference for safe delivery options that have a low degree of gross risk and may only have limited potential for reward	Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward.	Eager to be innovative and to choose options offering potentially higher business rewards.

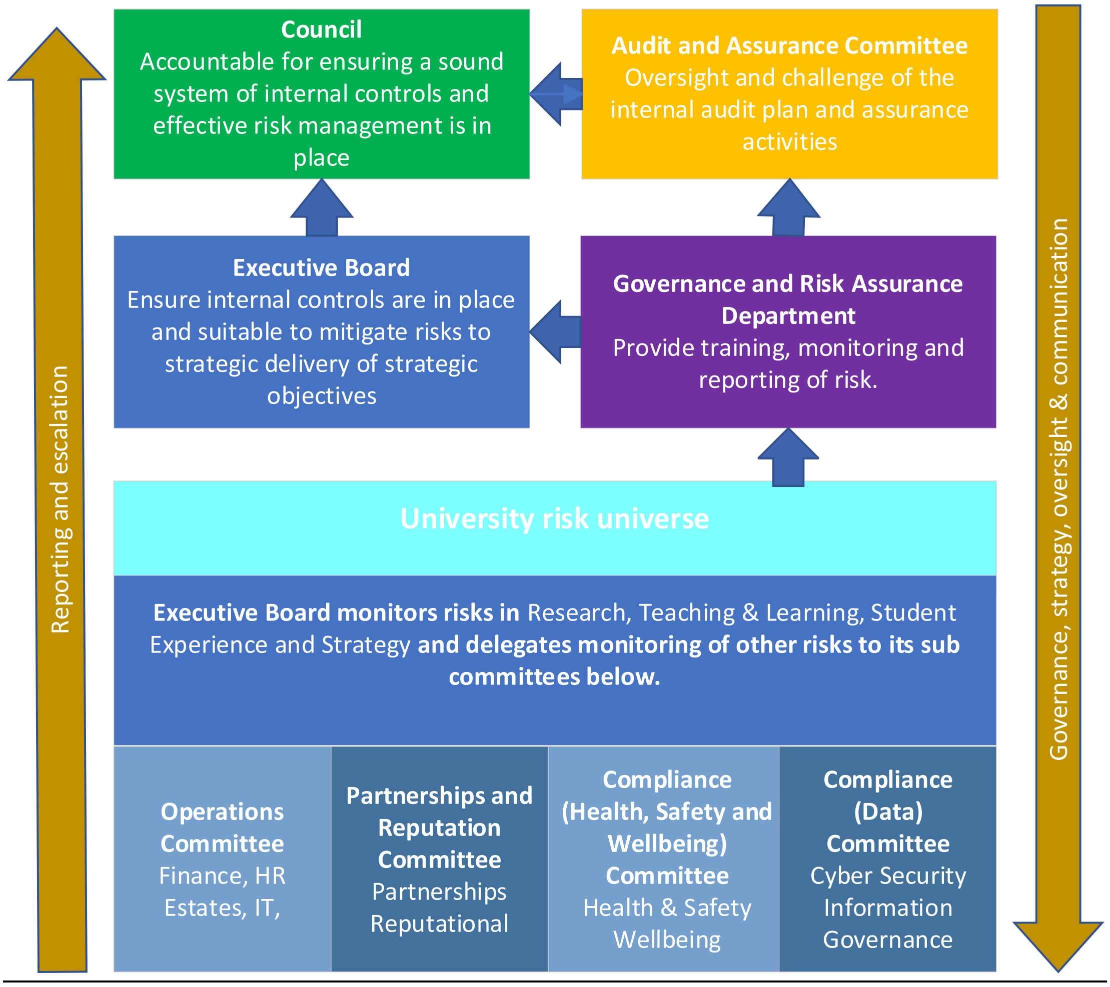
Target risk: The determination of a target risk is, in practice, a reflection of risk appetite at a granular level. For example, where the Residual/net risk is higher than the Target risk, the risk may be considered to be unacceptable, and a risk reduction plan is required. Once the Residual/net risk aligns with the Target risk level, the risk would then be considered to be acceptable and within appetite. The setting of target risk levels will be informed by Council’s risk appetite, policies and procedures, and management plans and objectives.



Open	Invite			
Cautious	Open	Invite		
Minimalist	Cautious	Open	Invite	
Averse	Minimalist	Cautious	Open	Invite
Averse	Averse	Minimalist	Cautious	Open

4.6 Roles & Responsibilities

To successfully embed risk management across the University, the risk management process is supported by a governance structure that defines roles and responsibilities at each level, outlined below.



Council
Accountable for ensuring a sound system of internal controls and effective risk management is in place

Audit and Assurance Committee
Oversight and challenge of the internal audit plan and assurance activities

Executive Board
Ensure internal controls are in place and suitable to mitigate risks to strategic delivery of strategic objectives

Governance and Risk Assurance Department
Provide training, monitoring and reporting of risk.

University risk universe

Executive Board monitors risks in Research, Teaching & Learning, Student Experience and Strategy **and delegates monitoring of other risks to its sub committees below.**

Operations Committee
Finance, HR
Estates, IT,

Partnerships and Reputation Committee
Partnerships
Reputational

Compliance (Health, Safety and Wellbeing) Committee
Health & Safety
Wellbeing

Compliance (Data) Committee
Cyber Security
Information Governance

Council

Council is ultimately accountable for ensuring risks are managed effectively across the University of Surrey. Key responsibilities include:

- Agreeing the University's Risk management approach and appetite.
- Providing oversight, challenge and approval of the management of the University of Surrey's principal risks (Level 1 Risks) and defining the monitoring process required for the on-going scrutiny of the risk management and internal control systems.

Audit and Assurance Committee

The Audit and Assurance Committee is responsible for overseeing and challenging the effectiveness of the University of Surrey's Risk Management (though Council retains ultimate accountability for risk management in the University). The Audit and Assurance Committee, on behalf of Council, monitors and assesses effectiveness of the risk management approach to satisfy itself that the implementation is aligned with the delivery of University's purpose and priorities. Where it finds areas of weakness or opportunities to improve it takes corrective action.

Key responsibilities include:

- Ensuring Council receives appropriate assurance that the systems of risk management and internal control are operating effectively, and that all significant failings and weaknesses and principal risks have suitable management activities in place to rectify and/or remain within defined risk appetite;
- Advising Council on the University's overall risk appetite, tolerance and strategy, taking into account the current and prospective regulatory, legal, political, macroeconomic and financial

environment, noting that Council must retain ownership and approval of the University's overall risk appetite, tolerance and strategy;

- Overseeing and advising Council on the current risk exposures of the University and future risk strategy;
- In relation to risk assessment:
    - Keeping under review the University's overall risk assessment processes that inform Council's decision making, ensuring both qualitative and quantitative metrics are used;
    - Reviewing regularly and approving the parameters used in these measures and the methodology adopted;
    - Setting a standard for the accurate and timely monitoring of large exposures and certain risk types of critical importance.
- Reviewing the University's capability to identify and manage new risk types;
- Reviewing reports on any material breaches of risk limits and the adequacy of proposed action.

Executive Board

Executive Board (EB) is responsible for ensuring Risk Management is effective and embedded in the business. Key responsibilities include:

- Leading a strategic 'top-down' risk assessment exercise on an annual basis, aligned to the strategic planning and budgeting cycle.
- Quarterly review, challenge and approval of all significant 'bottom-up' risks that have been escalated to the Executive Board through sub committees.
- Individual ownership of principal risks and proposal of the principal risk list to Council.
- Actively sponsoring and supporting the practice of risk management and procedure compliance by promoting the right tone from the top.
- Defining desired appetite levels for key risk areas for Council review and acceptance.
- Challenging Directorate/Faculty/Department management during performance reviews as to the effectiveness of their risk management performance.

Executive Board sub committees

The sub committees of Executive Board are responsible for monitoring the risks and risk management in their areas. Key responsibilities include:

- Receiving a summary report on the relevant risk environment, identifying emerging trends or risks out of appetite and holding individual areas to account on their management of risk.
- Receiving matters escalated to the committee from other sub-committees or Executive Board.
- Escalating to EB any risk outside risk appetite that cannot be treated, tolerated, transferred or terminated.
- Reviewing internal audits and other assurance activity against areas under the remit of the committee including monitoring progress with addressing significant findings.
- Identifying risks.

Directorate /Faculty/Department Management

Responsible for implementing this procedure in their Directorate /Faculty/Department and ensuring that appropriate risk management governance structures, processes and activities are in place. Key responsibilities include:

- Identifying risks in their area;
- Effective management of risks within their Directorate /Faculty/Department, including the high-level strategic risk(s) for reporting upwards to the Executive Board, sub committees and Council;
- Reviewing and challenging the scope, quality, completeness and validity of risk information reported by their area;
- Escalating risks in accordance with the defined scoring criteria.

Risk champions

Risk champions are employees that are experienced and trained in good practice risk management and provide local guidance and support in their respective Directorate /Faculty/Department on risk management activities. A risk champion will be appointed by each Directorate /Faculty/Department to have responsibility for liaising with the senior managers and updating their risks on the system on their behalf. (This role is commonly delegated to the administrator for the Directorate/Faculty/Department).

Key responsibilities include:

- Leading, coordinating and supporting the performance of effective risk management in their Directorate /Faculty/Department and supporting compliance with this procedure, acting to provide advice, support and motivation to management and staff.
- Reporting the Directorate /Faculty/Department 's key risk information on a monthly / quarterly basis.
- Liaising with the Governance and Risk Assurance Department to ensure that good practice risk management activities are shared across the University.

Cervus+

Cervus+ is a subsidiary of the University and audits the effectiveness of risk management at the University and provides some training and workshops.

Governance and Risk Assurance (GRA) Department

GRA is responsible for supporting the operation of the University of Surrey's Risk Management and the University's compliance with this procedure. Key responsibilities include:

- Coordinating and supporting Directorate /Faculty/Department risk reporting.
- Facilitating strategic risk assessment by the Executive Board.
- Producing University-wide risk reporting for submission to the Executive Board sub committees, Executive Board, Audit and Assurance Committee and Council.
- Facilitating knowledge sharing across the Directorate /Faculty/Departments and acting as a centre of excellence for good practice risk management.
- Providing training on GOAT.

Risk Owner

A named individual shall be allocated as the Risk Owner for each risk identified, who will be the single point of accountability and responsible for its effective management. The Risk Owner shall:

- Identify new risks
- Take overall responsibility for ensuring the risk is reduced to agreed target appetite levels.
- Be familiar with the risk and have the required authority to ensure its effective management.
- Be responsible for assessing and agreeing the severity of the risk.
- Be accountable for monitoring the risk to identify any material changes or issues.
- Ensure that all escalations e.g. where defined thresholds are breached, are made as required.

Note: Where a risk is identified that would more appropriately be owned and managed by another area, it should be notified to their respective management and the Risk Champion so they can appoint a suitable Risk Owner.

Action Owner

Action Owners have delegated responsibility from Risk Owners and are responsible for the implementation of specific risk response activities.

5. Governance Requirements

5.1. **Implementation: Communication Plan**

The Procedure will be placed on the Policies and Procedures web page and on the GRA web pages on Surrey Net.

It will be emailed to all Risk Owners, Risk Champions and other interested parties.

A Microsoft Team will be established for risk owners and champions and other interested parties.

5.2. Implementation: Training Plan

Training is provided to new Risk Owners and Risk Champions, on risk management in general and on the University's corporate risk management system.

5.3. **Review**

This procedure will be reviewed every three years.

5.4. **Legislative Context and Higher Education Sector Guidance or Requirements**

The University is answerable to the OfS (Office for Students, formerly HEFCE) for the proper use of the funding they provide. The "Terms and conditions of funding for higher education institutions", currently prescribes that "In accordance with the HEI's own statutes and constitution, there should be effective arrangements for providing assurance to the governing body that the HEI has a robust and comprehensive system of risk management, control and corporate governance."

The following bodies provide useful guidance on risk management:

- ISO Guide 73:2009 and ISO 31000
- Institute of Risk Management
- HM Treasury Orange Book

5.5. **Sustainability**

This procedure does not have any sustainability implications.

6. Stakeholder Engagement and Equality Impact Assessment

6.1. An Equality Impact Assessment was completed on 29/09/2023 and is held by the Authorised Co-ordinator.

6.2. Stakeholder Consultation was completed, as follows:

Stakeholder	**Nature of Engagement**	**Request EB Approval (Y/N)**	**Date**	**Name of Contact**
Governance	Shared document	Y	25/09/2023	Andrea Langley
H&S	Emailed document	n	20/9/2023	Matt Purcell
Sustainability	Emailed document	n	22/9/2023	Martin Wiles
Cervus+	Shared document	n	25/09/2023	Mat Cooling and James Pointer