Risk Management Framework

Effective from October 2021

Document purpose

This document explains the University of Kent's (**the University**) underlying approach to risk management and the standards for risk management which are to be applied consistently across the University. This framework forms part of the University's corporate governance arrangements.

Document Control

Properties

Document Title	Risk management framework
Document Scope	University of Kent
Document Owner	Council
Accountable Executive	Director of Governance and Assurance
Document Location	
Frequency of Review	Annual
Document last Approval Date	26th November 2021

Change Control

Version	Date	Description of Change
1.0	26/11/2021	Original Version

Document Distribution & Approval

Governing Body	Role	Date Completed
Executive Group	Review and recommend	27/09/2021
Audit Committee	Review and recommend	12/10/2021
Council	Approval	26/11/2021

Contents

1 Principles 4
2 Governance 5
3 Responsibilities and accountabilities 6
4 Risk identification 7
5 Risk objective setting 8
6 Risk assessment 9
6.1 Current risk assessment 9
6.2 Forward-looking risk assessment 9
6.3 Use of risk assessment in management of business resilience 10
6.5 Use of risk assessment in strategic decision making 11
6.6 Use of risk assessment in proportional internal control management 11
7 Risk control 13
8 Risk monitoring 14
9 Risk management reporting 15

1 Principles

Risk management should facilitate the identification, assessment, and prioritisation of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. The following principles have been established for risk management.

1. **Robust governance:** Robust governance arrangements should be implemented to oversee the effectiveness of risk management and internal control arrangements.

2. **Clarity of accountabilities and responsibilities: -**The responsibilities and accountabilities for risks and controls should be unambiguous and should be articulated at all levels of the organisation.

3. **Completeness of scope:** The scope of risk management should cover the management of potential losses caused by external events that threaten the business model such as COVID, BREXIT; or caused by failures in internal operational systems, policies, and processes such as failures in health and safety or data protection controls.

4. **Transparency and measurability of risk management strategy:** The risk management strategy should make explicit the choices made in terms of risks taken in the pursuit of the University's ongoing viability. The attitude towards risk should be transparent and measurable.

5. **Integrity of assessment:** The assessment of risk should have integrity to enable comparison between risks and to enable tracking of movements between assessment periods. Assessment should include both qualitative and quantitative information.

6. **Farsighted assessment:** The assessment of risks should include a forward-looking assessment. This should include consideration of the impact of material external events that might cause risks to crystalise.

7. **Use of risk assessment in managing business resilience:** The assessment of risks should inform the application of resources to manage business resilience to minimise the impact of unfortunate events or to maximise opportunities.

8. **Use of risk assessment in business decision making:** The assessment of risks should include a rigorous assessment (due diligence) of the impact from strategic projects.

9. **Use of risk assessment in determining a proportional approach to internal control:** The robustness of internal control arrangements should be proportional to the assessed level of risk exposure and the defined attitude towards the risk.

10. **Transparency and measurability of internal control arrangements:** The internal control documentation should make explicit the choices made in terms of controls enforced in day-2-day operational management of the risks. The effectiveness of controls should be measurable.

11. **Integrity and timeliness of monitoring:** The monitoring of risks should be dynamic. Data quality standards should be maintained.

12. **Effective reporting:** Reporting should provide the Council with assurance that there are effective systems of control and risk management in place to support delivery of the University's strategic aims.

The remaining sections of this document provide standards to facilitate delivery against these principles in an efficient manner with minimal administrative burden.

2 Governance

Robust governance: Robust governance arrangements should be implemented to oversee the effectiveness of risk management and internal control arrangements.

1) **Council: -** The Council is responsible for ensuring that the University has a robust and comprehensive system of risk management and as such is responsible for the approval of the risk management framework. In determining its opinion on the effectiveness of risk management, Council is informed and advised by Executive Group and the Audit Committee on the effectiveness of the framework and its operation. The Council has specific responsibility for: setting the tone and influencing of the culture of risk management; determining the appropriate risk management strategy and providing the direction for co-ordinated and economical application of resources (financial and otherwise). The council has responsibility to set risk appetite and agree how risk is measured

2) **Audit Committee:** -The Audit Committee is responsible for monitoring the effectiveness of the University's risk management system. This committee is led by a lay member of Council and receives termly reports from the University's internal auditors on the effectiveness of risk management. The Audit Committee is responsible for reviewing the University's risk management framework and for recommending it for approval by the Council. This committee, on behalf of Council, keeps under review the integrity and effectiveness of the University's risk management framework, it alerts Council to any actual or anticipated movements in risk profile and any changes to risk management arrangements. The Committee prepares an annual report for Council and expresses an opinion on the adequacy and effectiveness of the institution's risk management, internal control, and governance arrangements.

3) **Executive Group: -** The Executive Group has responsibility for developing the University's approach to risk management and for implementing arrangements that deliver effective risk management. It develops the University's risk management framework and monitors the implementation of the Council's risk management strategy. This group has responsibility for escalating decisions regarding the application of resources to minimise, monitor and control risks to Council as appropriate. The Group considers and makes recommendations to Senate and Council regarding internal control arrangements and other matters as appropriate.

Full terms of reference are available for all governing bodies. These provide in full the duties of the various governing bodies.

3 Responsibilities and accountabilities

Clarity of accountabilities and responsibilities: -The responsibilities and accountabilities for risks and controls should be unambiguous and should be articulated at all levels of the organisation.

1) **First line of defence: -** The first line of defence is responsible for the way risks are managed and controlled day-to-day. The Vice Chancellor and President (**VC**) is accountable for the implementation of the risk management framework and the internal control system. To assist her in her duties the VC has delegated accountability to members of the Executive Group. The executive with allocated accountability for a risk category is called the executive risk owner. The delegated responsibility can be further cascaded to members of the executive's office at the executive's discretion. An individual with allocated responsibility for a risk category is called a risk owner.

2) **Second line of defence: -** The second line of defence is responsible for the development of the risk management and internal control systems and the coordination of governance, risk management and internal control activities.

    a) The Director of Governance and Assurance (**DG&A**), with the support of their office, is responsible for the ongoing development and enhancement of the risk management and internal control systems.

    b) The DG&A is responsible for coordinating the reporting of assurance information. This includes information on the adequacy of the governance system including the risk management and internal control systems.

    c) The DG&A, with the support of their office, is accountable to the Council for providing an opinion on the ongoing suitability of the risk management strategy and its alignment to the overarching university strategy.

    d) The DG&A, with the support of their office, is responsible for coordinating the University implementation of institutional change consistent with developments in legislation and regulation and can evidence compliance through maintenance of a comprehensive policy framework.

    e) The DG&A, with the support of their office, is responsible for coordinating independent auditing of the adequacy of the governance, risk management and internal control arrangements.

3) **Third line of defence:** -The third line of defence is responsible for undertaking independent assessments of the governance, risk management and internal control systems.

    a) The University has appointed third parties who are considered to have the necessary expertise to provide an opinion. The external and the internal auditors' appointments are periodically reviewed by the Audit Committee.

    b) External auditors provide an independent examination of the financial statements prepared by the organisation. The role of external audit is to determine whether, in the auditor's opinion, the financial statements present fairly in all material respects. In expressing an opinion as to accuracy of the financial statements, they will likely express a view and be explicit as to any deficiencies in the control environment which might lead them to be unable to rely on the Universities records presented to them.

    c) Internal auditors provide independent assurance that the University's governance, risk management and internal control arrangements are operating effectively. Internal auditors provide an unbiased and objective view, and they must be independent from the operations that they evaluate. They report to the highest level in an organisation:

senior managers and governors. They must have access to all relevant information and resources.

4 Risk identification

Completeness of scope: The scope of risk management should cover the management of potential losses caused by external events that threaten the business model such as COVID, BREXIT; or caused by failures in internal operational systems, policies, and processes such as failures in health and safety or data protection controls.

Identification of all risks to the business model is undertaken by creating a corporate risk categorisation and subcategorization hierarchy with application at different levels of the organisation.

1) **Corporate risk category definition: -** A categorisation of corporate risks should be maintained to facilitate complete coverage of risks pertinent to the University's business model, ensuring that risks that impact upon strategic aims are managed in full. This should include financial risks, conduct risks and operational risks. Each risk category has a clear unambiguous definition for consistent application across the university. Ownership of each risk category is allocated.

2) **Sub-categorisation by risk owners: -** Further subcategories of risk can be defined as appropriate at the discretion of risk owners. (For example, educational services risks could be broken down by division/school, information technology risks could be broken down by application, organisation risks could be broken down by department). This forms a hierarchy of risk categories enabling: (i) risks to be aggregated or interrogated at different levels; (ii) enablers to be developed for ongoing assessment, monitoring, and internal control or the risks; (iii) allocation of responsibility and accountability for a risk; (iv) application of specialist expertise.

3) **Application at different levels:** - The categorisation model can be applied, at the discretion of the VC, to various levels of the organisation (from the entire group to a division). Each entity selects the risks which are pertinent to it providing justification if a risk is not pertinent.

The corporate risks together with definition and ownership are documented in the risk universe. The appropriateness of the risk universe is reviewed at least annually. In addition, it is reviewed following significant changes to the business model.

5 Risk objective setting

Transparency and measurability of risk management strategy: The risk management strategy should make explicit the choices made in terms of risks taken in the pursuit of the University's ongoing viability. The attitude towards risk should be transparent and measurable.

The risk management strategy should act as a planning and organisational tool, facilitating the University's coordinated and economic application of resources. It should contain the following: -

1) **Risk appetite statement: -** The risk appetite statement provides the primary risk objective of the University. The primary objective is linked to (i)financial strength and hence to ongoing viability, (ii) conduct and hence reputation, (iii) operation and hence continuous delivery.

2) **Financial management framework: -** Principles for financial management of liquidity and cash flow are set out in the Financial Framework. The principles for the management of reserves and cash flow provide the definition of the minimal surplus of the University in line with the risk appetite statement. They define the mitigating actions that will be taken in the event of a breach with this threshold. Mitigating actions may include liquidity management of working capital and enforced spend reductions. Financial management principles also include rules for how any surplus is subsequently invested within the University and the level of cash reserves that should be maintained at any one time.

3) **Attitude to risk: -** For each category of risks the Council determines whether it is willing to accept the risk or wishes to reject the risk. For each of the risks that the Council is willing to accept the risk preferences are defined. These articulate whether the Council is willing to take on more risk or less risk than currently. They therefore define the anticipated direction of travel of a risk.

4) **Risk tolerances**: - Risk tolerances (discretionary limits) are defined that provide maximum and minimum exposure to the risk categories. Risk tolerances provide boundaries to the exposure of the risk that the Council is willing to accept. Risk tolerances are monitored on a regular basis. The monitoring enables mitigating action to be taken when potentially too much or too little risk is being taken.

5) **Prudent management principles: -** Prudent management principles are official instructions that is given by the Council without dictating the means of implementing the instruction. The Council establishes principles for the prudent management of each risk category. These should strike the reasonable balance between the potential benefits of exposure to a risk and the cost of impacts of mitigation of such exposure.

The strategic approach to risk management is documented within the risk management strategy which is owned and approved by the Council following recommendation by the Audit Committee. the appropriateness of the risk management strategy is reviewed annually.

6 Risk assessment

6.1 Current risk assessment

Integrity of assessment: The assessment of risk should have integrity to enable comparison between risks and to enable tracking of movements between assessment periods. Assessment should include both qualitative and quantitative information.

The risk assessment process is the process for assessing the entire risk profile of the University on a current (T=0) basis. The current risk assessment process includes the following steps:

1) **Quantitative assessment:** For each corporate risk category, a stress is defined for (i) a worst-case loss event; and (ii) and expected loss event, within this category. The impact on financial sustainability is then assessed (net financial loss) for these events according to a defined formula based on parameters for impact and likelihood, or if necessary, using scenario analysis. The model is documented and is subject to validation.

2) **Qualitative assessment:** The quantitative assessment is supplemented by a qualitative assessment of risks which includes information on the size of the exposure and the level of internal control. Movements over the reporting period should be explained in the qualitative assessment.

3) **Overall assessment of impact on financial sustainability:** Correlations are applied between risk categories to determine an overall assessment of the impact on financial sustainability to cover all the risk categories defined in the risk universe. Reverse stress testing is carried out to identify the combinations of events that could lead to non-viability.

4) **Determination of adequacy of surplus**: Current level of reserves is measured against the requirement to cover normal operating requirements and a buffer for the aggregate financial impact of risks.

5) **Financial mitigation planning:** Should the surplus be negative then liquidity management mitigations are required. A financial recovery plan should be established for approval by the Board of Governors on the recommendation of the Audit Committee.

The assessment of risks is carried out at least annually. Additional ad-hoc assessments may be undertaken at points of significant change.

6.2 Forward-looking risk assessment

Farsighted assessment: -The assessment of risks should include a forward-looking assessment. This should include consideration of the impact of material external events that might cause risks to crystalise.

The forward-looking risk analysis is the process for assessing the movements in risk profile caused by emerging external events. The forward-looking risk assessment process includes the following steps:

1) **Horizon scanning: -** Emerging external events that could threaten the business model are identified. This should include consideration of: (i) Political events; (ii) Economic events; (iii) Sociocultural events; (iv) Technological events; (v) environmental events; (vi) Legislative events. The level of threat is tracked over time considering the proximity of the threat.

2) **Business impact analysis: -** Business impact analysis is undertaken considering the impact on all corporate risk categories based upon defined scenarios for the external event (best case, worst case, expected case).

6.3 Use of risk assessment in management of business resilience

Use of risk assessment in managing business resilience: The assessment of risks should inform the application of resources to manage business resilience to minimise the impact of unfortunate events or to maximise opportunities.

Resources should be applied to resilience management proportionately to the level of threat to the strategic aims.

1) **Trigger for resilience planning/ mitigation planning:** Where (a) the risk assessment exceeds defined tolerance levels; or (b) when the impact assessment undertaken of an emerging external event highlights a significant threat; then mitigation planning should be triggered. A crisis management team should be established.

2) **Resilience planning/ Mitigation planning: -** Resilience plans should represent a proportionate response according to the level of the threat and the proximity of the threat. Proposed plans should be submitted by the Executive Group for approval by the Council and to obtain a commitment of resources. Resilience plans should include at least the following: -

    a) Objectives for (i) overall assessment of risk; (ii) the residual overall level of financial loss incurred due to the event; (iii) the residual level of impact on each risk category.

    b) A phasing for the mitigations considering the proximity of the threat. Consideration should be made to: -

        i) Preventative measures: - Implementation of new institutional arrangements to prevent the impact of the event including, but not limited to, implementation of new insurance arrangements.

        ii) Emergency response measures: - Emergency response is enacted immediately on the occurrence of the event to reduce the impact of the event. It is the handling of the initial emergency. For example, this may include management of evacuations and engagement and cooperation with emergency services, management of crisis communications.

        iii) Business recovery measures: - Business recovery facilitates a return to business-as-usual activity within an acceptable time frame to reduce the impact of the event by limiting the duration of the impact. It may involve the implementation of alternative facilities, staff, technology or involve the adoption of different methods to resume normal service.

    c) Roles and responsibilities for preventative, emergency response and business recovery measures.

3) **Implementation of resilience measures/ mitigative measures**: - Implementation of resilience measures should be tracked. Any deviations with timelines for implementation should be highlighted with explanations provided.

6.5 Use of risk assessment in strategic decision making

Use of risk assessment in business decision making: The assessment of risks should include a rigorous assessment (due diligence) of the impact from strategic business decisions.

The due diligence process ensures that there are no unforeseen impacts from strategic business decisions. Strategic decisions include, but are not limited to, proposals for new lines of business; new collaborative arrangements; acquisitions and divestments; material new technology system; changes of pricing model; changes to the product portfolio. (Strategic decisions do not include day-2-day operational decisions.) The due diligence process includes the following steps:

1) **Project definition and scope: -** Create clear definitions for the project and the project scope. This should include a clear outline of the need for the project and a summary of the changes in corporate arrangements required. It should also outline the scope of affected University entities.

2) **Business case development: -** Establish the business case for change with definition of the benefits over a 5-year period on a best case, worst case and expected case basis.

3) **Business impact analysis: -** Conduct business impact analysis considering the impact on all corporate risk categories based upon defined scenarios. Mitigations should be defined for all adverse impacts where possible.

4) **Feasibility analysis: -** Assess the resources necessary for the project to be completed and compare them to what the University has available.

The definition and scope, business case, business impact assessment and the feasibility analysis should be submitted as part of the project initiation documentation. The Executive Group should consider whether the change is the right option for the University and represents value for money. Approval of the project initiation and commitment of resources follows delegated authority limits. The proposal should not be implemented the necessary approval.

Due Diligence is undertaken at least annually in line with the business planning process and ad-hoc due diligence may be undertaken at points when strategic change is proposed in the course of a year.

6.6 Use of risk assessment in proportional internal control management

Use of risk assessment in determining a proportional approach to internal control: The robustness of internal control arrangements should be proportional to the assessed level of risk exposure and the defined attitude towards the risk.

Development of internal control arrangements can be proposed by management following self-assessment activity or in response to an internal audit finding. All developments have cost implications, so consideration needs to be made on the optimisation of use of resources. Proposals can be accepted, rejected, or deferred. To assist in the selection and prioritisation of activity and subsequent allocation of resources, all proposals/ recommendations should include sections for: scope and definition; business case; business context; feasibility:

1) **Scope and definition: -** Proposals should be scoped by the risks that they are intended to address and defined by clear statements of areas of control effectiveness or efficiency that the proposal is intended to address.

2) **Business context:** - It is important that all proposals are made with full consideration of other controls for the same risk. All control arrangements for a risk should be considered to ensure that the measures work coherently together and to eliminate business

inefficiency through implementation of multiple disparate activities aimed at producing the same outcome.

3) **Business case: -** Proposals can be made for (a) addition of controls; (b) enhancement of controls; or (c) removal of controls. It is important that all proposals have a clear business case for change in terms of (a) reduction of impact or likelihood of a risk; (b) enhancement in efficiency of the organisation. Any proposal should be economically justifiable. Any proposal for a new control should be accompanied by a clear statement of the control's objective.

4) **Feasibility analysis: -** Feasibility analysis should be undertaken for the proposal of any new control. This is used to determine the viability of the proposal, such as ensuring it is legally and technically feasible as well as can be adequately resources and supported.

Developments of internal control arrangements should be documented appropriately in university policies.

.

7 Risk control

Transparency and measurability of internal control arrangements: The internal control documentation should make explicit the choices made in terms of controls enforced in in day-2-day operational management of risks. The effectiveness of controls should be measurable.

Internal control arrangements are documented, deployed, and periodically assessed.

1) **Documentation: -** Internal control arrangements are aligned to risks and their prudent management principles. They are documented in university policies, control standards and procedures.
   a) **Policies**: -A policy is a set of standards setting out how the University will attain its strategic aims and comply with the regulations established by the Council. Policies should outline minimum internal control requirements and roles and responsibilities for each risk. Policies are mandatory documents and are approved by governing bodies according to their delegated authorities. Policies should contain the following sections: Introduction; Objective statement; Governance; Roles and responsibilities; Minimum standards of control, Management information and reporting,
   b) **Control standards: -**A standard is a detailed method/ protocol for the operation of a control that is required by a policy. Control standards may be aligned to industry standards if appropriate. Standards are not mandatory documents and are created at the discretion of the policy owner. Control standards may be documented but do not need approval of a governing body.
   c) **Process/ Procedures**: - A process/ procedure is a fixed, step-by-step sequence of activities or course of action (with definite start and end points) that must be followed in the same order to correctly perform a task. Processes/ Procedures should be designed in a manner to be compliant with policies and, if applicable, control standards. Processes/ Procedures are not mandatory documents and do not need approval by a governing body.

2) **Deployment: -** Deployment of internal control arrangements ensure awareness and understanding of all affected parties. This is achieved through publication and training.
   a) **Publication:** All approved regulations, policies, control standards and processes must be published on the Universities Intranet site. Publication of internal control documentation is coordinated by the Governance and Assurance Office
   b) **Training:** Training should be provided to affected parties to ensure understanding of the purpose of controls and their application.

3) **Assessment: -** Internal control arrangements are assessed and scored periodically for ongoing adequacy.
   a) **Internal audit activity: -** Internal audit provides independent assurance regarding the adequacy of internal control arrangements. Internal audit activity is prioritised by the assessed level of risks and anticipated movements in risk (due to external events, due to impacts of business decisions, or due to changes in the internal control environment). Reports from audit activity should highlight any findings in respect to control weaknesses and their relative importance in terms of controlling the likelihood or impact of a risk. An overall rating of adequacy is provided.
   b) **Management self-assessment: -** Management self-assessment is undertaken on an annual basis and should cover all risk categories. It results in an assessment of operational compliance and an assessment of design effectiveness of controls for each risk category. Executives are required to attest regarding the adequacy of controls on an annual basis.

8 Risk monitoring

Integrity and timeliness of monitoring: -The monitoring of risks should be dynamic and track lead, actual and lag metrics. Data quality standards should be maintained.

The monitoring process is the process for reviewing information regarding risks to strategic aims over time. It enables breaches to risk tolerances to be flagged. The risk monitoring procedure includes consideration of probability and impact indicators:

1) Probability indicators:
For each category of risk, where empirical data is available, the probability distribution is tracked. This shows the probability of loss events at different degrees of severity and is based on historical data. The mean, standard deviation and 95th percentile of losses within the category is also tracked. For all categories of risk, the level of assurance of internal control arrangements is tracked. This includes both internal audit ratings and self-assessment ratings.

2) Impact indicators:
For each category of risk, the actual worse case assessment (T=0 assessment) of the risk should be captured and tracked in terms of net financial impact. Breaches to risk tolerances should be flagged. Justifications of movements should be provided. For each category of risk actual losses (on a rolling 12-month basis) should be tracked. All crystallised risk events (incidents) should be recorded with information on the loss incurred, the cause of the incident, the date of the incident and the response to the incident.

All indicators should be reviewed periodically to maintain standards of accuracy, completeness, consistency, currency, precision, privacy, reasonableness, integrity, timeliness, uniqueness, and validity

The risk monitoring process is undertaken continuously. Frequency of data collection should reflect the volatility of the risk. The period for tracking indicators should be at least equivalent to the business planning horizon.

9 Risk management reporting

Effective reporting: Reporting should provide the Council with assurance that there are effective systems of control and risk management in place to support delivery of the University's strategic aims.

Risk management reporting provides assurance of (a) the adequacy of control of the corporate risks; (b) that appropriate steps are being taken regarding external events with significant, institutional-level financial or reputational risks; (c) that robust due diligence is being undertaken in respect of business decisions. Risk management reports include the following:

1) **Audit Committees annual report:** - The audit committee annual report is submitted by the Audit Committee to the Council. It should contain the following: -

    a) A summary of the activity undertaken by the audit committee in the reporting period
    b) A summary of the risk profile of the University
    c) A summary of the adequacy of the control environment of the University
    d) An opinion of the adequacy of the risk management strategy
    e) A summary of material changes in governance, risk management and internal control arrangements.

2) **Annual risk assessment report**: - The annual risk assessment report is submitted by the DG&A to the Audit Committee and should include: -
    a) The qualitative and quantitative results of the risk assessment and the conclusions drawn from the results.
    b) The method and main assumptions used in the assessment and any changes in approach.
    c) Qualitative information on where significant deviations have been made with the stated Council approved risk management strategy.
    d) The effect of external events on a qualitative and quantitative basis over the business planning horizon
    e) The effect of material decisions on a qualitative and quantitative basis over the business planning horizon.

3) **Annual internal audit report**: - The annual internal audit report is submitted by the internal auditors to the A&R Committee. The internal audit report should include: -
    a) A breakdown of work undertaken in the auditing period
    b) A summary of material findings
    c) An annual audit opinion.
    d) Planned activity for the next auditing period.

4) **Termly internal audit report(s**): -The termly internal audit report(s) is submitted by the Internal Auditors to the A&R Committee. The termly internal audit reports should include:
    a) Auditors' opinion
    b) Auditors' recommendations

5) **Hypergene strategic monitoring dashboards**: - Dynamic dashboards for review by Council and executive members. Includes:
    a) Risk categories and definition
    b) Risk impact indicators
    c) Risk probability indicators
    d) Mitigating actions definition and status