**BISHOP GROSSETESTE UNIVERSITY**

**Document Administration**

| | |
|---|---|
| **Document Title:** | BGU Risk Policy |
| **Document Category:** | Policy |
| **Version Number:** | 2.2 |
| **Status:** | *Approved* |
| **Reason for development:** | To enable the organisation to achieve its objectives, triangulating strategy with risk and performance (informed decision making through 'active management') |
| **Scope:** | This procedure applies to staff |
| **Author / developer:** | Director of Strategy and Planning |
| **Owner** | Director of Strategy and Planning |
| **Assessment:** (where relevant) | ☐ Equality Assessment<br>☐ Legal<br>☐ Information Governance<br>☐ Academic Governance |
| **Consultation:** (where relevant) | ☐ Staff Trade Unions via HR<br>☐ Students via Bishop Grosseteste University Students' Union<br>☐ Any relevant external statutory bodies |
| **Authorised by (Board):** | University Council |
| **Date first authorised:** | 3 July 2018 |
| **Date current version authorized:** | 3 July 2018 |
| **Date current version effective from:** | September 2018 |
| **Date next review due to commence*:** | September 2021 (with interim annual reviews) |
| **Document location:** | University Website |
| **Document dissemination / communications plan** | University website, Staff Portal |
| **Document control:** | All printed versions of this document are classified as uncontrolled. A controlled version is available from the *University website*. |
| **Alternative format:** | If you require this document in an alternative format, please contact governance@bishopg.ac.uk. |

*Please note, this document remains valid until formally replaced or revoked by the University.

# Table of Contents

## 1. Introduction

Like every business the University faces numerous risks. These risks have the potential to disrupt achievement of the University's strategic and operational objectives. The University aims to use risk management to take better-informed decisions and improve the probability of achieving its strategic and operational objectives.

## 2. Corporate Governance

The University has a responsibility to fulfil its corporate governance role in demonstrating appropriate and prudent financial control.

This includes demonstrating that the organisation has a healthy risk culture, aligned to the Universities Strategic Objectives and business model by demonstrating a systematic approach to the themes and aspects outlined below:

| Theme | Aspect |
|---|---|
| Tone at the top | Risk Leadership: clarity of direction<br>• Senior management set clear and consistent expectations for managing risks<br>• Leaders role model risk management thinking and actively discuss tolerance to risk issues |
| | Responding to bad news: welcoming disclosure<br>• Senior management actively seek out information about risk events<br>• Those that are open and honest about risks are recognised |
| Governance | Risk Governance: taking accountability<br>• Management are clear about their accountability for managing business risks<br>• Role descriptions and targets include risk accountabilities |
| | Risk Transparency: risk information flowing<br>• Timely communication of risk information across the organisation<br>• Risk events are seen as an opportunity to learn |
| Competency | Risk Resources: empowered risk function<br>• The risk function has a defined remit and has the support of leaders<br>• It is able to challenge how risks are managed |
| | Risk Competence: embedded risk skills<br>• A structure of risk champions support those managing risks<br>• Training programmes are in place for all staff |
| Decision Making | Risk Decisions: informed risk decisions<br>• Leaders seek out risk information in supporting decisions<br>• The business's willingness to take on risks is understood and communicated |
| | Rewarding appropriate risk taking<br>• Performance management linked to risk taking<br>• Leaders are supportive of those actively seeking to understand and manage risks |

*IRM Risk Culture Aspects Model*

In practice, this means creating a culture of risk management that is part of everyday decision making linked to the governance and management of the organisation through its structures, roles and responsibilities. This means:

- The identification and management of risk should be a continuous process linked to the achievement of the University's strategic, corporate and operational objectives.
- The approach to internal control should be risk and event based assessing the likelihood and impact of risks becoming a reality.
- Review procedures must cover all risk areas not just financial risk.
- Risk assessment and internal control should be embedded in ongoing operational procedures.
- The governing body or relevant committee should receive regular reports during the year on internal control and risk.
- Risk identification, evaluation, management and monitoring should be systematic throughout the organisation and a review of the systems effectiveness should be reported to, and reviewed by, the governing body.
- The governing body acknowledges that it is responsible for ensuring that a sound system of control is maintained and that it has reviewed the effectiveness of the above process.
- The governing body is, where appropriate, expected to set out details of actions taken or proposed, to deal with significant internal control issues.

## 3. Purpose of this policy

This policy is a formal acknowledgement of the commitment of the University to risk management. The aim of the policy is not to have risk eliminated completely from University activities, but rather to ensure that every effort is made by the University to manage risk appropriately to maximise potential opportunities and minimise the adverse effects of risk.

### 3.1 Policy Objectives

- To confirm and communicate the University's commitment to risk management to assist in achieving its strategic, corporate and operational goals and objectives.
- Where possible to align risk with delivery (activity) and performance (KPIs) to provide a triangulated approach to managing the delivery of the strategic, corporate and operational objectives.
- To formalise and communicate a consistent approach to managing risk for all University activities and to establish a reporting protocol.
- To ensure that all significant risks to the University are identified, assessed and where necessary treated and reported to the University governing body in a timely manner through the University's audit committee.
- To assign accountability to relevant committees and staff for the management of risks within their areas of control.
- To provide a commitment to staff that risk management is a core management capability.

### 3.2 Policy Statement

The University considers risk management fundamental to good management practice and a significant aspect of corporate governance. Effective management of risk will provide an essential contribution towards the achievement of the University's strategic, corporate and operational objectives and goals.

Risk management must be an integral part of the University's decision-making and routine management, and must be incorporated within all areas of the planning processes at all levels across the University.

Risk assessments must be carried out on new ventures and activities, including projects, processes, systems and commercial activities to ensure that these are aligned with the University's objectives and goals. Any risks or opportunities arising from these assessments will be identified, analysed and reported to the appropriate management level.

The University will maintain a risk register that categorises risk at strategic, corporate and operational level. The University's Leadership Team, the Vice Chancellors Executive Group (VCEG) will monitor strategic and corporate risk as part of the Strategic Planning Framework. The Senior Management Group will monitor operational risk as part of the University's Operational Plan. Departmental action plans should contribute to the management and treatment of risk through the actions taken.

The University is committed to ensuring that all staff, particularly Heads of Departments and *Service Managers* are provided with adequate guidance and training on the principles of risk management and their responsibilities to implement risk management effectively.

The University will regularly review and monitor the implementation and effectiveness of the risk management process, including the development and embedding of an appropriate risk management culture (see above) across the University.

### 3.3 Scope of the policy

Risk is an inherent aspect of all business (academic and administrative) activities. Sound risk management principles must become part of routine management activity across the University.

The key objective of this policy is to ensure the University has a consistent basis for identifying, assessing, monitoring, managing, controlling, and reporting risk across the University at all levels.

### 3.4 The policy details the following:

The policy outlines the different aspects of the way in which the University will effectively manage risk.

#### 3.4.1. What is Risk?

Risk exists because of uncertainty and is present in all activities whatever the size or complexity and whatever industry or business sector. It is important to understand that risk is a broader concept than the traditional view of merely a threat. It also recognises the risks of taking or not taking opportunities. Risk includes threats (damaging events) which could lead to failure to achieve objectives. Opportunities (challenges) which if exploited could offer an improved way of achieving the desired objectives but which could potentially have negative impacts.

The University considers all types of risk including strategic, corporate, operational, financial, reputational, regulatory and compliance. Different possible types or categories of risks is shown in Appendix 2. These may assist with pre-determining risk appetite or tolerance.

#### 3.4.2 The University's Approach

The University's approach to risk management follows several key principles:

- ❖ The Risk Management process will be as user friendly as possible and add value. For this reason, considerable effort has been put into keeping the process as simple as possible.
- ❖ The University seeks to embed risk management across all departments including commercial ventures and programmes and projects delivered by separate arms of the Universities organisational arrangements, where they contribute to the strategic objectives. Its immediate aim is to ensure that effective risk management is embedded in the University's leadership and management group(s).
- ❖ The aim is to marry top down and bottom up assessments to produce a comprehensive picture of risk across all University activities.
- ❖ All departments will use a consistent and transparent approach to risk, ensuring an agreed and widely understood method and language.
- ❖ A key focus of the risk management process is the concentration on control improvements to treat significant risks, however there is a need to balance the cost and the effectiveness of the controls; for example where marginal improvements in control require substantial costs, the proposal may be unviable.
- ❖ Escalation reporting of risk ensures that significant risks are reported and closely monitored on a regular basis at the appropriate level.

### 3.4.3 Risk Roles and Responsibilities

Please see Appendix 1.

### 3.4.4 Risk Management Approach and Process

There are five steps to management of risks identified in the risk register. The process consists of:

1. Risk identification and ownership: Identifying the risks to achieving strategic and operational objectives and name the risk owner.
2. Analysing the risk: What is the actual risk and what is the likelihood and impact?
3. Evaluate and rank the risk: Based on the risk assessment, including the calculation model and guidance, what is the risk score (gross risk and expected net risk after treatment)?
4. Treat the risk: Determining the course of action and the way we want to treat the risk. Then assessing the controls either in place, or which need to be put in place, and what level of risk will be tolerated, including expected risk tolerance.
5. Monitor and review: How and where risk will be monitored and reviewed.

Note: The five steps apply to all new ventures and activities, including projects, processes, systems and commercial activities.

### 3.4.5 Risk identification and ownership

Risk can be identified anywhere and by anyone, using a number of mechanisms and timescales. For example during the planning cycle, setting new operational objectives for the University's Two Year Plan will result in risks being identified. However, new risks can be identified at any time.

As part of their Terms of Reference, Committees and Boards in the Strategic Planning Framework are responsible for treating risk in their Strategic objective area, through their actions. They will identify new external and internal risks or threats through their shared knowledge of the sector and their

knowledge of operational issues, this information will inform the identification of new risks, and any escalation required through the above process.

VCEG, SMG and relevant Committees and Management Groups should regularly review the linkages between strategic objectives and risks to ensure that focus is maintained on priority activities.

Risk ownership will be elected at the point the risk is identified. If the risk is strategic or corporate, a member of the Leadership Team (VCEG) should own it. If the risk is operational, it should be owned at Head of Department level (SMG), however, there may be a need for the level of expertise to dictate the owner of a risk rather than the inclusion in either VCEG or SMG.

Risk ownership is different to responsibility for reporting on risk and for delivering the mitigating action(s), however, the risk owner could report and deliver mitigating actions, they do not have to be different people.

### 3.4.6 Analysing the risk

Risk assessment is the process to ensure that, before a risk is placed on the register, the risk is appropriately articulated. For risk to be managed it is critical to ensure that reviewers fully understand the actual risk to the organisation. This also helps to ensure appropriate scores and mitigating actions are associated with the risk.

Once the risk is fully understood, the likelihood and impact scores can be considered. This will provide and overall gross risk score before any treatment is considered. Risks that are scored at the highest level or have significant likelihood and impact should be brought to the relevant leadership or management group's attention at the earliest opportunity. Note: VCEG meets twice monthly and SMG once a month.

### 3.4.7 Treating the risk

Once a risk has been assessed and understood, owners can determine the actions required to treat risk using five principles: avoidance; reduction; transfer; accept; share. Avoidance of risk may prove too costly (financial or otherwise) but this option should always be considered at this stage. Treatment and the actions identified may be 'business as usual' activity or specific initiatives that will improve the likelihood of achieving the strategic objectives. The risk owners should ensure clarity over which actions what are business as usual (no additional cost) and what are new actions, so that the cost of these can be accurately calculated and considered against the benefit.

Depending on the level of risk, strategic, corporate or operational, mitigating actions should be shared with the relevant committee or group. This should preferably take place before they are added to the risk register, so that appropriate challenge is applied prior to further scrutiny from the relevant governing body.

### 3.4.8 Risk tolerance/appetite

Council are responsible for setting the overall tolerance (or appetite) for strategic risk. Having considered how to treat the risk, and the level of tolerance, an expected net risk score should be considered. Risk Owners should expect to receive challenge where the residual risk, once mitigation action is complete, is higher than any agreed tolerance. This challenge should come from VCEG for

Operational Risk and Council and/or Audit Committee for Strategic and Operational risk as high levels of operational risk can lead to strategic risk. The risk target or net risk that is acceptable may therefore change depending on the challenge received from the relevant group or committee.

### 3.4.9 Monitoring and review

The process for monitoring the risk register includes the Risk Owner or responsible officer updating the register with progress on mitigating actions, including any changes to timescales, and providing an updated risk score where risk is increasing or reducing. The original risk score remains throughout the life of the risk, but for monitoring purposes ongoing risk scores, whether they stay the same or change, will be shown as action taken impacts on the risk on a monthly/quarterly/bi-annual/annual basis. This allows a comparison between the impact of the actions taken and the actual risk level as a result and the original expectation of tolerance.

The Risk Office will produce a report based on the monitoring updates on a monthly basis, providing there are risks that are being monitored to this regularity. Regularity will be decided at the risk assessment point. The report will highlight any improvement and/or deterioration of risk relevant to the monitoring period (monthly/quarterly etc). Exception reports will be required from Risk Owners where risk mitigation is seen to be ineffective or where risk levels are not reducing to meet the tolerances.

### 3.4.10 Programme/Project Risk

Programmes and project leads that are responsible for delivering University Strategic Aims through their projects will be expected to produce a risk register. Where strategic or corporate risk develops because of a programme or project not delivering the expected benefit or results, this should be escalated to the Leadership Team (VCEG). The risk should be evaluated and a decision taken for the risk to be added to the risk register following the approved process and five steps.

### 3.4.11 Risk Reviews

A formal risk review should take place at least twice a year with a review of progress on control improvements for red risks every four to six weeks. In the case of programmes or projects there should be a risk review at each Board meeting. During the risk review, thought should be given to each risk to ensure that the risk is still relevant and applicable and that the risk register is complete (new risks should be considered at this point). It is good practice for the Senior Management Team (SMG) to note emerging risks for consideration and review during their regular monthly meetings.

It is important that the number of risks under active management are kept to a manageable number, suggested between 15 to 20 in total. Where the residual risk is considered very low (1 probabilility and 1 impact), the risk can be removed from the risk register. Risk reviews should consider the following questions and these should be recorded in the minutes or notes from the meeting:

1. Is the risk still relevant?
2. Is the risk owner still appropriate?
3. Has the risk reduced to an extent where de-escalation and delegation of the management of the risk can be completed, and the risk removed from the register?
4. Has the risk increased to an extent where escalation needs to take place to the next management level and a reassessment of the risk needs to take place?

5. What are the circumstances around the changes to risk levels, what is the explanation and evidence?
6. What opportunities do the changes present?
7. What are the recommendations from the group?

### 3.4.12 Annual Risk Reviews

The University should prepare an annual report that provides an overview of how effective the risk management process is working – its effectiveness. This should include:

- The lessons learned from the process, approaches and models for continuous improvement;
- the risk register and exception reports for each red or significant risk so that those risks are considered as part of the planning cycle;
- An update on risks where the mitigating actions treated the risk;
- Where opportunities were created because of effective risk management.

### 3.4.13 Risk Management Procedures and Models

The University uses a risk model (Appendix 1) to define probability/likelihood and impact. Impact is the potential severity or effect of the risk. Probability is the frequency or likelihood of a risk occurring. The ratings given to impact and probability produce an evaluation of gross risk. Both the adequacy of existing controls and gross risk is denoted by a traffic light system. Any risks in the red will require explicit review and approval by the Leadership Team (VCEG).

The University's risk scoring model should be used where risk is considered Strategic, Corporate or Operational. Programme and Project Leads should also use the University model and risks reported to the Programme or Project Board. Significant or red risks for programmes and projects should be reported to the Leadership Team (VCEG) who will consider whether they should feature in the University Risk Register.

### 3.4.14 Levels of risk can be defined as:

**Strategic**: A risk that will impact on the delivery of the strategic objectives or the strategy itself.
**Corporate**: A risk that could impact on the effectiveness of the organisation as a whole but is not directly related to the strategic objectives.
**Operational**: A risk that relates to the efficiency of the University's systems and their components (people, processes, IT systems or infrastructure) that if unmanaged would impact or undermine the delivery of the strategic objectives or the organisation as a whole.

### 3.4.15 Major or catastrophic risks

Major and catastrophic red risks and any risks with inadequate existing controls must be reported to the Vice Chancellor.

As mitigation action plans are developed, VCEG will take a view as to whether the actions being taken to treat the risk are adequate or whether more, or something different, could be done. As a result of this exercise, VCEG will either recommend or decide whether the level of residual risk is acceptable or whether the risk should be terminated (for example ending the activity where the risk originates). In many instances, the termination of the risk may not be possible because of the cost or other factors.

## 4. Risk Management Process – Roll Out

The risk process including the risk approach, processes and procedures should be rolled out before the start of the new Academic Year 2018. The risk register is to be fully established with the transfer of existing, or adding of new, risks being completed by end June 2018. During Spring/Summer 2018 this will be rolled out at Leadership and Management level to VCEG and then to SMG. Risk will be a standing item on Committees included in the Strategic Planning Framework and other key committees and groups such as the Equality and Inclusion Committee.

Note: During the initial roll out there will be a review and any variation, needed for the effective running of the risk process will be made. Specifically the appropriate escalation and de-escalation levels will be reviewed. This will be based on the review from Audit Committee and will take into account any operational issues that occurred during the year. VCEG will also be consulted on the new Policy and any feedback incorporated into the approach and documentation.

Each year the University Risk Manager will review the risk registers. The policy will be updated annually to reflect any changes. Otherwise, the policy will be reviewed every three years. The next review date is March 2019 and then March 2022.

Please contact the University Risk Manager should you have any questions regarding this policy or the application of the risk management process across the University.

**APPENDIX 1: Roles and Responsibilities**

**University Governing Body (Council)**

University Council has responsibility for the total risk exposure of the University and approves the risk tolerance line annually. They will be assured that the management of the organisation is effective enough to manage risks in accordance with their set tolerances.

Council has responsibility for the total risk exposure of the University by:

- Setting the tone and influence of the culture of risk management across the University
- Determining the extent to which the University is "risk taking" or "risk averse" as a whole sets the University's risk tolerance line
- Approving major decisions affecting the University's risk profile or exposure
- Determining what types of risk are acceptable/not acceptable and monitoring significant risks and control improvements to mitigate risks
- Annually reviewing the University's approach to risk management and approving changes or improvements to key elements of the process and procedures

**To aid this Council will receive**

An annual report from Internal Audit on the effectiveness of the risk management process in the University, making recommendations when necessary.

A regular update on the Risk Register together with a report that details any significant changes to risk and assurance on the effectiveness of the risk management policy and processes.

**Vice Chancellor**

The Vice Chancellor, advised by VCEG, is responsible for the effective management of strategic and corporate risks. The Vice Chancellor is responsible for escalating increasing or significant risk to Council.

**Leadership Team - Vice Chancellors Executive Group**

VCEG advised by the University Risk Manager, is responsible for corporate risks by:

- Identifying and evaluating the significant risks faced by the University
- Providing adequate information in a timely manner to Council on the status of risks and controls
- Participating biannually in a risk review and reporting the outcomes to Council
- Implementing policies on risk management and internal control
- Participating in the annual review of effectiveness of the system of internal control and risk management by internal audit
- Delegate risks to SMG/other where they are no longer considered strategic but may be corporate or operational

**Audit Committee**

The responsibilities of the Audit Committee are outlined separately in their terms of reference and will keep under review the effectiveness of the risk management, control and governance arrangements,

and in particular, to review the external auditors' management letter, the internal auditors' annual report, and management responses.

**Senior Management Group (SMG) and Heads of Departments**

SMG and Heads of Departments are responsible for the management and monitoring of risk in line with this policy within their areas of responsibility. SMG is responsible for the effective management of risk identified in the Operational Plan and for escalating increasing or significant risk to VCEG including:

- Reviewing risks associated with the Operational Plan and any action plans produced by their departments, including programme and project risks
- Escalate any high or red risks to VCEG

**Staff and students**

Effective risk management depends on the commitment and co-operation of all staff and students. All staff have a significant role in the management of risk, particularly within their own areas of control. Consequently, all staff are responsible for and have accountability for adherence to the principles outlined in this policy.

**Programme/Project Managers and Project Teams**

Project managers and project teams are responsible for managing programme and project specific risk and complete a programme/project risk register to demonstrate that this is being done. Where programme or project risks significantly increase the escalation reporting process should be applied relevant to the risk impact (strategic, corporate or operational).

**University Risk Manager (Director of Strategy and Planning)**

The University Risk Manager reviews the risk management process annually and reports on this annually to the Audit Committee. The internal audit programme is mainly based on the risk register(s) of the University and recommended reviews will arise from this and from VCEG requirements.

**University Risk Manager and the Director of Finance**

The University Risk Manager and the Director of Finance will work together to ensure the overall policy, approach, process and procedures are working effectively and the systems for managing risk are protecting the organisation from any unnecessary failures, negative events or impact. The University Risk Manager, as the risk process owner, ensures that risk is managed effectively at all levels and that risk registers are reported at an appropriate level.

**University Risk Office (Planning Team and Governance Team)**

The Risk Office is responsible for co-ordinating the risk management programme and will provide advice and guidance, including the development of standard templates and tools to assist the University in managing risk.

The Risk Office will develop and conduct training on the principles of risk management, risk identification and assessment and on how to implement risk management effectively.

Where necessary, the Risk Office will assist departments and leads to conduct risk assessments on new ventures and activities.

The Risk Office will maintain the University's risk register.

The Risk Office, working with the Finance Office, will develop a reporting system and maintain information on losses or adverse events when risks eventuate.

The Finance Office will manage the insurance and risk financing requirements of the University.

**APPENDIX 2: Types and Categories of Risk**

**Types and categories of risk**

This appendix provides a prompt that can be used to aid risk discussions. These can be used as a guide, a starting point or as a checklist for existing registers and for Audit Committee to consider the level of risk that will be tolerated for each threat.

**Strategic Risk – Major Threats**

Sources of threat that may give rise to significant strategic risk includes:

- ✓ Budgeting (relates to availability or allocation of resources)
- ✓ Fraud or Theft
- ✓ Unethical dealings
- ✓ Product and or services failure (resulting in lack of support to business process)
- ✓ Public perception and reputation
- ✓ Exploitation of workers and or suppliers (availability and retention of suitable staff)
- ✓ Environmental (mismanagement issues relating to fuel consumption, pollution etc)
- ✓ Occupational health and safety mismanagement and or liability
- ✓ Failure to comply with legal and regulatory obligations and or contractual aspect (can you sue or be sued)
- ✓ Civil Action
- ✓ Failure of the infrastructure (including utility supplies, computer networks etc)
- ✓ Failure to address economic factors (such as interest rates, inflation)
- ✓ Political and market factors (for management of risk, security etc)
- ✓ Operational processes and procedures – adequate and appropriate
- ✓ Capability to innovate (to exploit opportunities)
- ✓ Failure to control intellectual property (as a result of abuse or industrial espionage)
- ✓ Failure to take account of widespread disease or illness among the workforce
- ✓ Failure to complete to published deadlines or timescales
- ✓ Failure to take on new technology where appropriate to achieve objectives
- ✓ Failure to invest appropriately
- ✓ Failure to control IT effectively
- ✓ Failure to establish a positive culture following business change
- ✓ Vulnerability of resources (material and people)
- ✓ Failure to establish effective continuity arrangements in the event of disaster
- ✓ Inadequate insurance/contingency provision for disasters such as fire, floods and bomb incidents.

**Strategic/Commercial Risks**

Examples of commercial risks includes

- ✓ Under performance of service relative to specification
- ✓ Management will underperform against expectations
- ✓ Collapse of contractors
- ✓ Insolvency of promoter

- ✓ Failure of suppliers to meet contractual commitments (this could be in terms of quality, quantity, and timescales on their own exposures to risk)
- ✓ Insufficient capital investment, shortfall in revenue expected / planned
- ✓ Fraud/Theft
- ✓ Partnerships failing to deliver desired outcomes or outputs
- ✓ An event being non insurable or cost of insurance outweighs the benefit

**Economical/Financial/Market**

- ✓ Exchange rate fluctuation
- ✓ Interest rate instability
- ✓ Inflation
- ✓ Shortage of working capital
- ✓ Failure to meet project revenue targets
- ✓ Market developments will adversely affect plans

**Legal and Regulatory**

- ✓ New or changed legislation may invalidate assumptions upon which the activity is based
- ✓ Failure to register with any new regulatory body, such as OfS
- ✓ Failure to obtain appropriate approval (e.g. planning consent)
- ✓ Unforeseen inclusion or contingent liabilities
- ✓ Loss of intellectual property rights
- ✓ Failure to achieve satisfactory contractual arrangements
- ✓ Unexpected regulatory controls of licensing requirements
- ✓ Changes in tax structure

**Organisation/Management/Human Factors**

- ✓ Management incompetence
- ✓ Inadequate corporate policies
- ✓ Inadequate adoption of management practices
- ✓ Poor leadership
- ✓ Key personnel have inadequate authority to fulfil roles
- ✓ Poor staff selection procedures
- ✓ Lack of clarity over roles and responsibilities
- ✓ Vested interest creating conflict and compromising the overall aims
- ✓ Individual or group interests given unwarranted priority
- ✓ Personality clashes
- ✓ Indecisions or inaccurate information
- ✓ Health and safety constraints

**Political**

- ✓ Change of government policy
- ✓ Change of government
- ✓ War and disorder
- ✓ Adverse public opinion/media intervention

**Environmental**

- ✓ Natural disasters
- ✓ Storms, flooding
- ✓ Pollution incidents
- ✓ Transport problems

**Technical/Operational/Infrastructure**

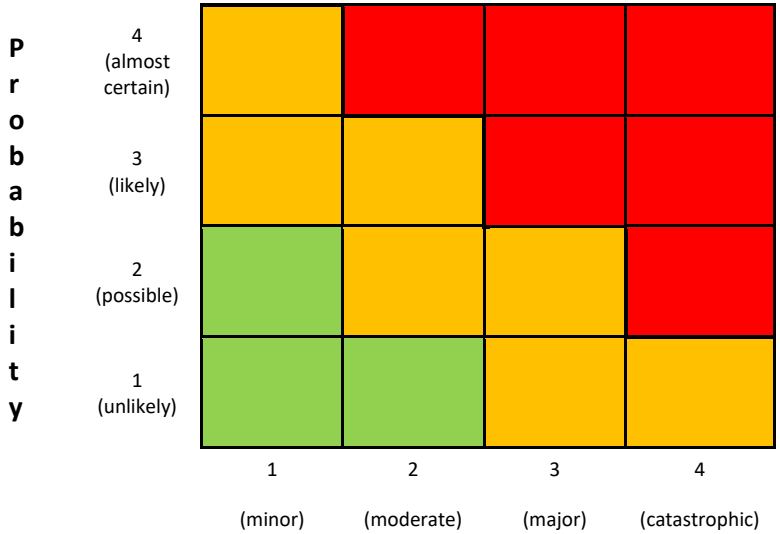
- ✓ Inadequate design
- ✓ Professional negligence
- ✓ Human error/incompetence
- ✓ Infrastructure failure
- ✓ Operation lifetime lower than expected
- ✓ Increased dismantling/decommissioning costs
- ✓ Safety being compromised
- ✓ Performance failure
- ✓ Residual maintenance problems
- ✓ Unclear expectations
- ✓ Breaches in statutory/information security
- ✓ Lack or inadequacy of business continuity

**Operational Risks**

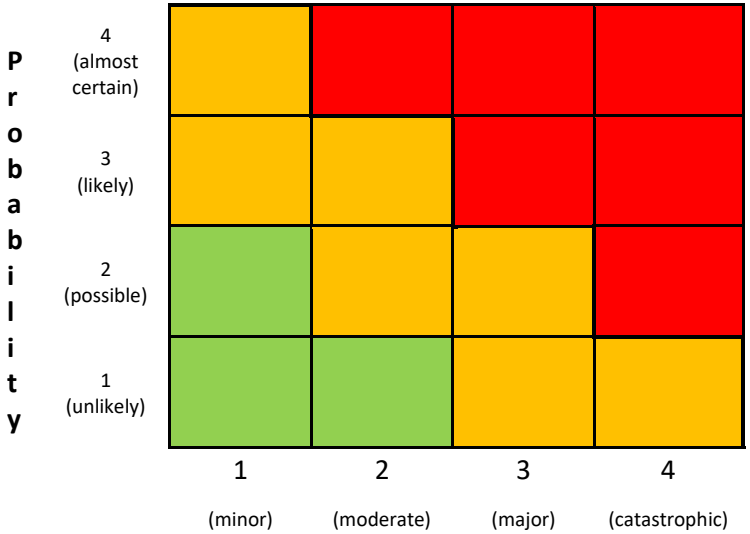
- ✓ Lack of clarity of service requirements
- ✓ Inadequate infrastructure to provide required operational services
- ✓ Inadequate or inappropriate people available to support the required service provision
- ✓ Inappropriate contract in place and or inadequate contract management to support the required level of service provision
- ✓ Changing requirements, enabled in an uncontrolled way
- ✓ Products passed to operational teams without due consideration to implementation, handover, subsequent maintenance and decommissioning
- ✓ Unexpected or inappropriate expectations of service users
- ✓ Inadequate incident handling
- ✓ Lack or inadequacy of business continuity or contingency measures with regard to maintaining critical business services
- ✓ Failing to meet legal or contractual obligations

**APPENDIX 3: Analysing Risk - Gross/Net Risk Model**

Using the 'analysing risk' process, consider the type of risk in Appendix 2 and the appropriate treatment of risk to provide the gross and net risk scores.




**Gross Risk Score**




**Net Risk Score**