



**ACCRA
TECHNICAL
UNIVERSITY**

RISK MANAGEMENT AND GUIDELINE POLICY

2022

TABLE OF CONTENTS

SECTION ONE: RISK MANAGEMENT POLICY

1.0 INTRODUCTION	5
1.1 Vision, mission and Share Values.....	5
1.2 Purpose of the Risk Management Policy.....	6
1.3 Objectives of the Policy.....	7
1.4 Statement of Commitment.....	7
1.5 Scope of the Policy.....	8
1.6 Current Status of ATU's ERM Implementation.....	9
2.0 KEY TERMS AND DEFINITIONS	10
3.0 RISK MANAGEMENT FRAMEWORK	17
3.1 Risk Management Principles.....	18
3.2 Risk Management Process.....	20
3.3 Risk Assurance and Reporting.....	21
3.4 Risk Monitoring.....	23
4.0 LINKING RISK MANAGEMENT WITH THE UNIVERSITY STRATEGY	25
5.0 THE UNIVERSITY'S STATEMENT ON RISK APPETITE	26
6.0 THE UNIVERSITY'S STRATEGIC RISK CATEGORIES	29
7.0 RISK MANAGEMENT HIERARCHY AND INSTITUTIONAL RESPONSIBILITY FOR MANAGING RISK	32
8.0 REVIEW OF THE RISK MANAGEMENT POLICY	39
9.0 APPROVAL	40

SECTION TWO: RISK MANAGEMENT POLICY GUIDELINES

Appendix One: Risk Management Process.....	41
Appendix Two: Template for Assessing Risk.....	53
Appendix Three: Strategic Risk Register Template.....	63
Appendix Four: Departmental Risk Register Template.....	64
Appendix Five: Sample University Risk Register.....	65
Appendix Six: Sample Risk Assessment Table.....	67
Appendix Seven: A walk through Risk Management Process Template.....	66



FOREWORD BY THE GOVERNING COUNCIL

The Governing Council takes overall responsibility for Accra Technical University's (ATU) success. Our role is to exercise leadership and sound judgment in directing ATU to achieve sustainable growth and act in the best interests of all our stakeholders. The Governing Council shall continue to maintain an oversight role and monitor the effectiveness of internal controls and risk management activities.

ATU's strategic plan realization and the development of the University depend on our ability to take calculated risks in a way that does not jeopardize the direct interests of stakeholders. Sound management of risk will enable us to anticipate and respond to changes in our work environment, as well as make informed decisions under conditions of uncertainty.

This policy will serve as a guide to Management and Staff in integrating risk management into ATU's operations in a more structured way.

It is expected that the policy provides a systematic way of assessing and managing both our strategic and operational risks at all the University Structure. This, in the view of the Governing Council, is an important stride in our quest to ensure compliance with relevant statutes and to build ATU to a model status in the Public Sector of Ghana.

Sequel, the Governing Council has the pleasure to present this Risk Management Policy to guide management in establishing and implementing the necessary infrastructure required for sound Enterprise Risk Management within ATU.

.....
CHAIRPERSON, GOVERNING COUNCIL



1.0 INTRODUCTION

Risk management forms part of Accra Technical University's (ATU's) internal control and corporate governance arrangement has become a regulatory requirement for all public sector institutions. The Public Financial Management Act, 2016, Act 921 Section 7(2) requires Principal Spending Officers to operate a comprehensive corporate risk management and internal control arrangements. Also, the Internal Audit Agency Act, 2003, Act 658 stipulates in section 3 (2F) that the agency, as part of its regulatory role shall ensure that risks are adequately managed in covered entities.

Furthermore, the previous g Accra Polytechnic Strategic Plan 2013-18 and the current ATU's Strategic Plan 2021-2025 continues on a trajectory towards Vision 2025 in an increasingly competitive higher education sector in the face of rapidly changing external regulatory, financial, operating, and teaching environment.

The Risk Management Policy and Guideline (RMP & G) captures ATU's response to uncertainties and a clear understanding of the University's Strategy, and the risks involved in adopting and executing it. These risks may originate from within or outside the University and must be mitigated. This means that they can only be managed and sometimes minimized, but rarely eliminated once understood and evaluated. Risk management is about carrying out our activities fully prepared, with vigilance on the current and future impact that decisions taken will have on the University and its students, staff and stakeholders with an ability to adapt to prevailing circumstances, while remaining focused on the University's Vision.

1.1.1 Vision Mission and Share values

To be recognized as the Top Technical University in Ghana, with Strong Regional Influence.

1.1.2 Mission

To Advance Technical Knowledge by Creating Conducive Environment for Applied Research, Quality Teaching and Competency-Based Training with High Impact on Industry and Creation.

1.1.3 Shared values

Our shared values of Integrity, Creativity and Excellence embody our essence as staff and students of Accra Technical University.

1.2 PURPOSE OF THE RISK MANAGEMENT POLICY

The purpose of this Policy is to provide a clear and consistent risk management methodology and approach for the effective management of risk across the University in the pursuit of its mission, vision and strategic goals as enshrined in the ATU 2021-2025 Strategic Plan and other policy documents of the University. It summarizes how risk management supports the University's planning activities and further aims at providing ATU Senior Management, Directors, Deans, Heads of Departments, Heads of Sections and Units and other staff with a guide to assist in managing the strategic and operational risks faced by the University.

The Governing Council, as part of delivering on its oversight responsibilities, will hold Management accountable for this policy and the management of strategic risk.

1.3 Objectives of the Policy

The objectives of the policy are:

- To commit the University in formalizing its approach to Risk Management
- To continuously develop risk management and profile across the University
- To integrate risk management into the culture and decision-making process of the University and ensure accountability at all levels of the risk management process
- Manage risks through the determination of the University's risk appetite and monitor its risk profile in accordance with best practices
- Create effective risk management processes that will allow the University to make annual risk management assurance statements with confidence.

1.4 Statement of Commitment

As a public tertiary institution, Accra Technical University (ATU) is committed to adopting best practices in the management of risks at all levels of operations and this can be achieved through the identification, evaluation and control of risks to ensure that they are reduced to an acceptable level or eliminated in the delivery of its mandate under the Technical University Act, 2016 (Act 922). The University is also committed to maximizing opportunities to achieve its strategic and operational objectives and deliver effective services across all spheres of the University - local, national and international. It is acknowledged that some risks will always exist and will never be eliminated.

All employees must understand the nature of risk and accept responsibility for risks associated with their area of work. Employees will receive the necessary support, assistance and commitment from the Governing Council and the University Management Team.

The University, as a corporate body, has an obligation to provide for the health and safety of its staff, students, customers, and visitors. The University is also obliged to protect its material assets and to minimize its losses and liabilities. The Governing Council is also committed to ensuring that ATU has and maintains an effective, efficient and transparent system of risk management in accordance with ISO 31000: 2018 as reviewed.

Risks or opportunities will be identified, analyzed and reported to the appropriate Management level. The University will maintain a strategic risk register. All Faculties, Directorates, Departments, Sections and Units will maintain operational risk registers. As mentioned earlier, the University is committed to ensuring that all staff, particularly Deans, Directors, Heads of Departments, Sections and Units are provided with adequate guidance and training on the principles of risk management and their responsibilities to implement risk management effectively.

1.5 Scope of the Policy

This Policy provides a guideline on managing risks faced by ATU in the pursuit of its strategic and operational goals. The policy addresses a broad range of potential exposure to risks across the entire operations of the University which include core activities and enabling activities in Faculties, Academic and Administrative Departments and Directorates, Satellite Campuses and temporary set-ups in the name of the University. Below are some of the risks associated with the core activities and enabling activities that the policy seeks to address:

CORE ACTIVITIES

- Governance and Compliance Risk
- Teaching and Learning Risks
- Engagement Risks
- Research Risk
- Reputational Risk

ENABLING ACTIVITIES

- Human Resources Risks
- Financial and Commercial Risks
- Information Technology Risks
- Assets Management Risks
- Environmental and Sanitation Risks
- Estate and Infrastructure Risks
- Health, Safety and Security Risks
- Audit and Investigation Risks

1.6 CURRENT STATUS OF ATU'S ENTREPRISE RISK MANAGEMENT (ERM) IMPLEMENTATION

Currently, the University manages risk formally or informally to varying degrees in many processes including:

- Strategic and operational planning
- Business continuity planning
- IT back up plans
- Financial and assets management

- Facility emergency response plans
- Standard operating procedures
- Emergency management planning
- Occupational health and safety practices
- Projects and policy development and implementation
- Agreements and contracts

This policy therefore aims at formalizing risk management in Accra Technical University by initiating the changes needed to manage risk in an aligned and coordinated manner across the University.

2.0 KEY TERMS AND EXPLANATIONS

Risk

Organizations face uncertainties as a result of internal and external factors that influence whether and they will achieve their objectives. The effect this uncertainty has on the achievement of an organization's objectives or intended outcomes is Risk. Risk is the chance of something happening that will have an effect on objectives. Risk is defined by ISO 31000 (2009) as the "effect of uncertainties on objectives", where an "effect" is a deviation from an intended or expected outcome.

ISO 31000

The Government of Ghana has adopted ISO 31000:2009 (ISO 31000-2018 Revised) as the risk management standard for managing strategic,

operational and program risks. ISO 31000 is a risk management standard developed by the International Organization for Standardization. The purpose of ISO 31000 is to provide principles and guidelines on risk management that can be applied to any type of risk. The ISO 31000 is not intended to promote uniformity of risk management across organizations, but rather, harmonize risk management within a given organization by being scalable and adaptable to add value for the organization. The design and implementation of risk management in an organization needs to take into account the varying requirements of a specific organization, its particular objectives, context, structure, operations, processes, functions, services, assets and specific practices employed.

Adoption of the ISO 31000 standard involves developing and implementing a risk management framework based on a set of principles and using a risk management process to systematically identify, assess and treat risks.

Risk Measurement

Risk is measured in terms of consequence and likelihood. It is the exposure to such things as economic or financial loss or gain, physical damage, injury or delay as a consequence of pursuing a particular course of action. The concept of risk has three elements:

- The perception that something could happen;
- The likelihood of something happening;
- The consequence/impact if it happens.

Risks might include but are not limited to:

- A breach of security
- A threat of physical safety
- A client dissatisfaction
- Deficiencies in financial controls and reporting
- Failure of a project to achieve its objective
- Failure of equipment or computer systems
- Failure to recognize and take advantage of opportunities
- Fraud
- A breach of legal or contractual responsibility
- Mismanagement
- Unfavourable publicity

Risks may further be categorized as follows:

Strategic Risks:

These are defined as risks that could affect or influence the University's ability to achieve its vision, mission and strategic objectives. They are mainly external risks that could threaten the overall success of the University. Any risk (program and policy risk or corporate service risk) that is deemed to have a significant and overarching effect on the University can be termed a strategic risk. Unmitigated strategic risks can affect the delivery of long-term outcomes in the University and may impact the University's reputation. The University Council will conduct an in-depth review of individual strategic risks at successive meetings.

Examples of these are:

- Political - Change of government or cross cutting policy decisions.
- Economic- Effects of global economy on Ghana's economy e.g. the effects of the economic downturn.
- Socio cultural - Demographic psychological changes that affects demand for services.
- Technological - Obsolescence of current systems; cost of procuring best technology available.
- Regulatory/Legal – changes in legislations and Statute requirements.

Programme and Project Risks

These are operational level risks that could impact or influence the achievement of business objectives. They are the risks to individual programmes and projects, and the responsibility of Senior Responsible Officers (SRO) - typically Pro-vice chancellor, Deans and Directors. These risks should be contained in Programme and Project risks registers. They are also included in Faculty / Directorate Risk Registers if material to the Faculty or Directorate achieving its business objectives. Programme project risk registers should be updated on an ongoing basis as the projects progress.

- New Projects -prioritizing between projects which are competing for Resources; ensure making optimal delivery decisions.

- Project Delivery - failure to deliver projects on time/to budget specification
- Clear Objectives - lack of clarity of the purpose and objectives of project

Corporate Service Risks

These are risks that could affect the delivery of the University's programmes and services. They include finance, human resource, and Information and Technology emergency management risks

Business Risks

These are the risks to the effective operation of the University, Faculty and its component units or a Directorate. Named Heads are responsible for managing these risks, as set out in the Faculty or Directorate Risk Registers this are held within Directorate's or Faculty Business Plans. These risks should also be updated on an ongoing basis.

- Service failure - failure to deliver our services to students with agreed/set terms
- Resources - financial risks such as insufficient funding, poor budget management, fraud; Information (adequacy for decision making; loss personal data resulting in loss of reputation); Physical asset (loss/damage/theft).
- Resilience - Capacity of systems/processes and IT to withstand adverse impacts and crises. Disaster recovery/continuity planning.

Joint delivery partner(s)

This is in recognition that the University may be affected by risks that our delivery partners are exposed to e.g. reputation or top delivery partner risk. These risks are managed by the delivery partner but we need to be aware of them by working closely with them in monitoring those top risks. Our delivery partners should report quarterly on these risks to the University Council or the appropriate committee

- Relationships - threats to commitment of relationship/clarity of role Accountability (particularly to Central Government).
- Operations - overall capacity and capability to deliver.
- Governance - Regularity and propriety/compliance with relevant requirements/ethical considerations.

Risk Management

It is the coordinated activities which come together to optimize the management of potential opportunities and minimize adverse effects. In other words, Accra Technical University defines risk management as the coordinated activities, systems and processes in place to direct and control the University with regard to the management of eventualities.

Risk Management Framework

This is the set of components that provide the foundations and institutional arrangements for the design, implementation, monitoring and control of risks and for the review and continual improvement of the University's risk management function.

Risk Appetite

This refers to the level of risk the University is willing to tolerate or accept in the pursuit of its objectives. When considering threats, risk appetite defines the acceptable level of exposure deemed tolerable or justifiable by the University. When considering opportunities, risk appetite defines how much the University is prepared to actively put at risk in order to realize potential or expected benefits.

Risk Appetite is directly link to risk tolerance. An institution with a higher risk appetite will tolerate a higher level of risk. This means its risk tolerance threshold, the point at which the level of risk exposure becomes intolerable or unacceptable will also be higher.

Risk Owner

This is the person or entity in authority who is accountable for the effective management of a risk.

Risk Manager/ Chief Risk Officer

This is the person (s) or entity with delegated responsibility for the effective management of a risk.

Note: While Risk Owners and Risk Managers may be directly accountable and responsible for the management of specific risks, in practice, all University employees have a responsibility for good risk management.

3.0 RISK MANAGEMENT FRAMEWORK

The design of ATU risk management framework took into account the distinctive attributes of ATU-its objectives, context, structure, operations, services, processes, and employees. ATU's Risk Management Policy is derived from its adoption of the "ISO31000:2018 or as reviewed: Risk Management -Principles and Guidelines". The Framework provides the foundation and organizational arrangement for designing, implementing, monitoring, reviewing and continually improving risk management throughout ATU.



Figure 1: The Risk Management Framework (Source: ISO 31000:2018)

3.1 RISK MANAGEMENT PRINCIPLES

ISO 31000 states that the purpose of risk management is the creation and protection of value. The principles set out in ISO 31000 provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. There are eight principles presented in the standard as below.

- Framework and processes should be customized and proportionate.
- Appropriate and timely involvement of stakeholders is necessary.
- Structured and comprehensive approach is required.
- Risk management is an integral part of all organizational activities.
- Risk management anticipates, detects, acknowledges and responds to changes.
- Risk management explicitly considers any limitations of available information.
- Human and cultural factors influence all aspects of risk management.
- Risk management is continually improved through learning and experience.

The first five principles provide guidance on how a risk management initiative should be designed, and principles six, seven and eight relate to the operation of the risk management initiative. These latter principles confirm that the best information available should be used; human and cultural factors should be considered; and the risk management arrangements should ensure continual improvement.



Figure 2: The diagram depicting the risk management principles

3.2 RISK MANAGEMENT PROCESS

The focus of the risk management system is to identify and treat risks. It is a systematic and a continuous process of identifying and analysing risks and, where appropriate, taking adequate steps to address these risks before they can impact negatively on objectives. The process will help increase the probability of success in achieving the overall objectives of ATU.

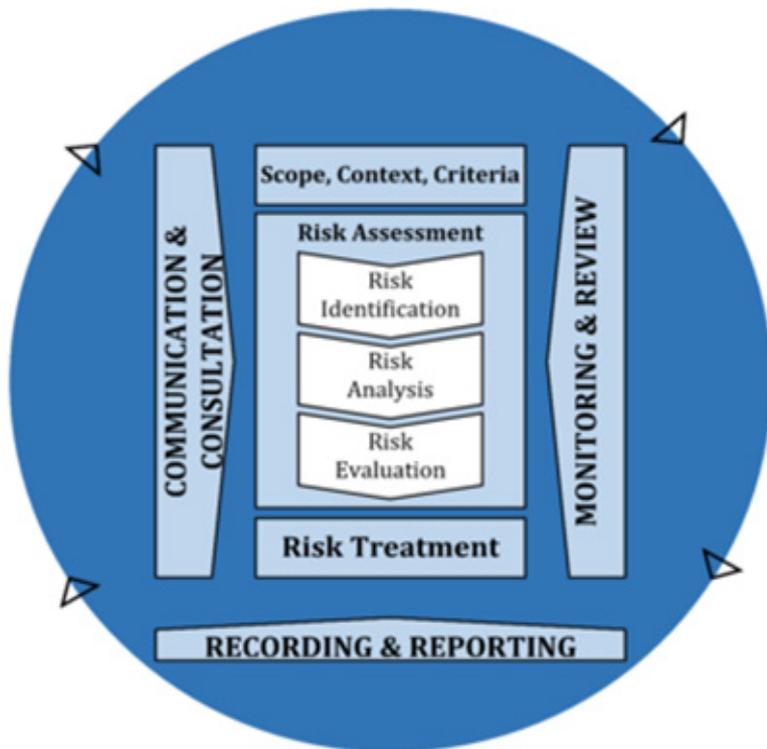


Figure 3: Diagrammatic illustration of the key stages involved in the risk management process

Detailed explanation of the process together with the relevant tools and templates are provided in the Risk Management Guidelines.

3.3 RISK ASSURANCE AND REPORTING

The Internal Audit Unit of ATU has the responsibility to provide assurance on the effectiveness and adequacy of risk management activities to assist management in improving governance and internal controls.

In order for the Governing Council to be properly informed of the status of risks facing the University, all departments are required to report regularly on risks assessed and progress with respect to their management. Departmental reports setting out ATU's major risks and actions being taken to manage them are to be consolidated. The consolidated reports are to be submitted to the Governing Council each quarter utilizing a standard format that details all identified significant risks.

3.3.1 Quarterly Risk Reporting

The Risk Management Committee will follow-up on major risks from the Risk Register and Action Plan on a quarterly basis and check the existence of newly identified material risks. This process will be undertaken within the operational planning as part of the planning process. The goal is to improve risk controlling by instituting quarterly risk follow-ups. Major risks must still be reported within ad hoc reports. The quarterly risk report should be issued to the Vice Chancellor and the Governing Council with appropriate comments from the Risk Management Committee.

The quarterly report will be reviewed by the Risk Management Committee in terms of endorsing the actions undertaken or proposed, and by the Governing Council in terms of the appropriateness of actions and compliance with the Risk Management Policy.

3.3.2 Ad Hoc Reporting of Newly Identified Major Risks

Managers at all levels of ATU will report newly recognized risks to the Risk Management Committee. Ad hoc reports can be used to address all of the risk areas defined in the Risk Matrix. The reports can also be used to highlight risks that have not been identified in the past. Ad hoc reporting thresholds should be established by the Risk Management Committee and Internal Audit Directorate.

It will be the role of risk owners/departmental or unit heads and the Risk Management Committee to regularly review progress on the achievement against the action plan. However, the Governing Council will also receive quarterly reports on achievement against the plan and on any unresolved risk issues. It will be the role of the Risk Management Committee to draw together all risk issues and make appropriate recommendations.

3.3.3 Departmental Risk Registers

As part of their regular activities, every department will be required to maintain a risk profile that provides details of all identified risks together with their assessment of likelihood and consequence (each rated on a 1-5 scale). Each Directorate, Faculty, Department, Unit within ATU shall prepare a risk register and forward it to the Risk Management Committee.

3.3.4 University Risk Register

The Risk Management Committee will keep an up-to-date register for the University, showing all the risks identified and details of how they have been disposed of or being managed. This register shall be a consolidation of all departmental risk registers and shall be available for inspection by the Governing Council and Management.

The Risk Management Committee will produce a final risk report and quarterly risk maps to Management for review and feedback.

3.4 RISK MONITORING

The presence and functioning of the components of the risk management system will be assessed over time and modifications made as necessary. Risk monitoring will be an integral part of risk treatment plans to give assurance that the measures remain effective.

The University's risk monitoring and review process encompasses all aspects of risk management for the purposes of:

- (a) Ensuring that controls are effective and efficient in both design and operation;
- (b) Obtaining further information to improve risk identification and assessment;
- (c) Analyzing and learning lessons from events (including near-misses), changes, trends, successes, and failures;
- (d) Detecting changes in the external and internal context of ATU; and

(e) Identifying emerging risks.

Monitoring will be accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Risk controlling will involve monitoring the implementation and progress of agreed actions and controls, re-evaluation, and compliance with decisions.

Directorates, Faculties, Departmental and Unit heads should undertake day-to-day monitoring of their top risks/hazards. Progress in implementing risk treatment plans provides a performance measure. The results should be incorporated into the department's overall performance management, measurement, and reporting activities.

4.0 LINKING RISK MANAGEMENT WITH THE UNIVERSITY STRATEGY

Risk Management is a key component of the University's strategic planning and performance management systems. The University's Strategic Risk Register aligns with the University's strategic objectives and institutional key performance indicators.

At the faculty and academic departmental levels, all risk registers directly correlate with, and therefore underpin management of the objectives outline in Faculty/departmental plans. Similarly, within the various administrative and Professional Directorates, Risk Registers must be in place to ensure the effective management of key risks which have the potential to affect areas of strategic importance.

As part of ATU's performance management framework, the University shall continually work towards linking risk management practices to the performance objectives of departments, teams, and individual staff to ensure achievement of their objectives.

5.0 THE UNIVERSITY'S STATEMENT ON RISK APPETITE

As noted under key terms and definitions, the University defines Risk Appetite as the level of risk it is willing to accept in the pursuit of its objectives.

The University accepts that it must take risk, to some extent, in order to achieve its aims and objectives, and to realize expected benefits. The University is committed to ensuring that all risks taken will be proactively controlled, and exposure will be kept to an acceptable level. The University acknowledges that the level of exposure carried by different activities will vary, and its threshold for accepting varying levels of risk will change depending on the risk area under consideration, the specific objectives involved, the subsequent activities undertaken and the projected benefits.

However, the University is clear that it will reject or closely manage any activity that has the potential to cause significant financial or reputational harm to the institution, most notably where this might endanger the University's viability, its ability to achieve its key strategic aims and objectives or its ability to meet its regulatory and /or legal obligations. The University defines risk appetite based on the following categories.

Table 1: Risk Appetite

Risk Appetite Category	Definition
Avoid	No appetite. Not prepared to accept any level of risk
Averse	Prepared to accept only low levels of risk, with a preference for very safe or prudent options, even if these carry potential for only very limited return
Moderate	A tendency to accept low or moderate levels of risk in order to achieve objectives; a more ambitious outlook, albeit still relatively prudent
Open	Willing to consider all options / actions/activities to achieve objectives even where there are elevated levels of associated risk
High	Eager to pursue original, creative, pioneering options activities to achieve objectives, and to accept substantial risks in order to achieve successful outcomes and significant rewards

Based on these categories, the University's institutional baseline risk appetite is defined as "moderate to open". This means that while maintaining a level of prudence, the University is generally willing to consider all options, and will accept moderate levels of risk in the pursuit of its objectives except for task with critical risks that the University will continue to maintain a low appetite.

However, while a general appetite of moderate to open is in place, it is recognized that risk appetite will vary according to the objectives pursued and the linked activities undertaken. For example, the University would give consideration to options or activities which carry elevated levels of risk, where it can be shown that the anticipated outcomes are realistically achievable and likely to deliver enhanced benefits; acceptance of risk, irrespective of risk appetite, should always take account of the likely benefits an activity will deliver. At strategic level, risk appetite is applied to the University's identified risk areas as indicated below.

6.0 ACCRA TECHNICAL UNIVERSITY'S RISK CLASSIFICATION

Once the risk has been articulated it can be classified into one of the strategic themes/pillars in the 2021-2025 strategic plan. This classification ensures that any common significant risks can be escalated and reported appropriately. The following table provide a list of the risks categories used within the University and some examples of the types of risks that could be classified under each heading

Strategic Theme	Examples include risks relating to:
1.Enhancing Student Experience	1.1 Strengthening competency- based skills development in TVET by increasing the quality of delivery and access to career relevant BTech, MTech, DTech programmes. 1.2 Instituting a scholarship scheme to support brilliant but needy students. 1.3 Increasing female participation in Science, Technology, Engineering and Mathematics Programmes (WISTEM). 1.4 Enhancing the employability skills of students through a career skill development. 1.5 Providing opportunities for skill development in innovative and emerging technologies. 1.6 Enhancing student's acquisition of high level employable and critical soft skill by forming cross disciplinary groups for problem based learning projects. 1.7 Providing opportunities for extra curriculum activities. 1.8 Improving the quality of teaching. 1.9 Improving student's Workplace Based Learning experience. 1.10 Improving security on campus for students. 1.11 Improving student's support services. 1.12 Improving Library Services 1.13 Improving the process involved in attracting, retaining and graduating top class students

<p>2.Impact Oriented Research and Innovation</p>	<p>2.1 Strengthening the directorate of Research, Innovation, Publication and Technology Transfer (DRITT) to spearhead donor engagement and staff training to improve staff skills in grants attraction, research management, and intellectual property issues.</p> <p>2.2 Aligning the research agenda of ATU to national development priorities and undertake industry and market-driven joint research to increase uptake of research findings.</p> <p>2.3 Establishing the ATU Research and Innovation Fund (ARIF) to increase support for the acceleration of innovation technology development and technology transfer by staff.</p> <p>2.4 Nurturing early – career academics to hone their skills in impact – oriented research, high impact publication, international networking and presentation.</p> <p>2.5 Improving the quality and number of facilities for applied research and technology transfer.</p> <p>2.6 Increasing publication of research outcomes</p> <p>2.7 Establishing Centres of Excellence (CoE) to undertake high level research and innovation, and to provide training to stimulate technological advancement in specific sectors of industry.</p>
<p>3. Industry and Community Engagement</p>	<p>3.1 Collaborating with industry for research development and technology transfer.</p> <p>3.2 Engaging industry experts to bridge the gap between industry and Academia.</p> <p>3.3 Enhancing University- Community engagement.</p> <p>3.4 Building community confidence in the capabilities of the University by engaging in activities that make significant contributions to the economic and social life of the communities.</p> <p>3.5 Initiate and sustain the University's community engagement activities.</p>

<p>4. Internationalization and Visibility of the University</p>	<p>4.1 Strengthening existing linkages with other international institutions</p> <p>4.2 Establishing new strategic linkages and strengthen existing ones at the national level</p> <p>4.3 Inviting leading international scholars and entrepreneurs as mentors to give international lectures at ATU and foster beneficial networking with strategic external stakeholders</p> <p>4.4 Maintaining a high quality and diverse international student profile</p> <p>4.5 Initiating and hosting students entrepreneurship competitions and national and international technology fairs to increase the visibility of ATU</p> <p>4.6 Injecting creativity into the University's communication and marketing strategies to aggressively brand the University</p> <p>4.7 Increasing the visibility of the University in the traditional Media</p> <p>4.8 Championing corporate social responsibility programmes for the benefit of society and the visibility of the University</p> <p>4.9 Effectively marketing ATU to an international audience.</p>
<p>5. ETC</p>	<p>5.1 ETC.</p>

7.0 RISK MANAGEMENT HIERARCHY AND INSTITUTIONAL RESPONSIBILITY FOR MANAGING RISK

The University's risk management consists of three management levels at which risks are managed and risk registers maintained. The three levels are Corporate Level, Faculty/Directorate and Departmental level. Under each Faculty are academic departments while under each Directorate are professional and administrative departments. All identified risks will be assigned to a risk owner and a risk champion with the former ultimately accountable and the latter responsible for ensuring effective management of each risk.

Corporate Level Risks or strategic risks are those risks that are linked to the achievement of the University's objectives and performance measures as contained in the ATU 2021-2025 Strategic Plan and other policy documents of the University. At the strategic or University level, and within the wider institutional corporate governance, framework, overarching accountability and responsibility for the management of risk lies with the University Council and with the Audit Committee through the Risk Management Committee.

The Faculty level risks refer to the key strategic and operational risks for all five (5) faculties. These risks are managed by the faculty deans and reviewed and agreed by the faculty board.

Directly linked to the faculty risks are the academic department risks. These are risks relating to the operations of each of the academic departments. These risks are linked to the objectives of the departments and are managed by the Head of Department'.

The Directorate / Professional level risks are key strategic and operational risks relating to the operations of the University's support functions and services managed by Directors.

The Professional Services Departmental Level Risks are risks relating to the operations of each of the professional and administrative departments. These are linked to the objectives of the department and managed by the Heads of Department and reviewed by the respective Deans or Directors.

Risk owners will be members of the Risk Management Committee. Underpinning risk registers also exist in support of the strategic risk register and key themes within the University's Strategic Plan (2021-2025) and other policies of the University. These include Enhancing students' experience, impact-oriented research and innovation, industry and community engagement risk registers among others. These risk registers should be managed by the Pro Vice Chancellor, appropriate Dean or Director.

At the faculty/school level, Faculty board/committee have overarching responsibility for the management of risk. Deans report on risks to the risk management committee through senior management on an annual basis as part of the institutional faculty planning process which is part of the University's wider strategic planning framework. This is an integrated approach which ensures the alignment of risk management with the strategic planning function. Deans will normally undertake the risk owner role and will be responsible for appointing risk champions.

The following structures and officers have specific roles to play in the University's risk management hierarchy:

The University Council

The Council is ultimately accountable for the risks of the University.

It requires assurance from both the Vice Chancellor and the Audit Committee that appropriate policies are in place and the risk management processes are adequate. The Council sets the University's risk appetite i.e., the level of risk considered tolerable in the absence of controls. As an integral part of its leadership role, the Council has responsibility for ensuring that the risk to the Public, the delivery of the University's objectives, and the reputation of the entire institution are all being appropriately managed. The Council assigns the risks on the Strategic Risk Register to its members to increase accountability for managing the high-level risks.

Vice – Chancellor (VC)

The Vice Chancellor (in his role as the Principal Spending Officer) has responsibility for developing and maintaining a sound system of internal controls and for reviewing its effectiveness. By signing the University's annual accountability statement, he asserts confidence that appropriate policies are in place and that the risk management process is operating properly to effectively manage the risks that may affect the achievement of objectives and operational outcomes.

The VC is accountable to the University Council and has overall responsibility for protecting the University from unacceptable costs or losses associated with its operations. The Vice Chancellor performs this function through the risk management committee.

The Audit Committee

The Audit Committee advises the VC (Principal Spending Officer) on the adequacy of risk management and internal control, through reviewing:

- the mechanism for the assessment and management of risks;
- the assurances relating to the corporate governance

requirement of the University;

- the activity of internal and external audit (planned and results)
- how effective the top risks of delivering partners are being managed, and;
- reporting annually to the University's Council summarizing its review and monitoring activities as they relate to oversight of the risk management process. The committee will also indicate, in its opinion and based on its activities, any significant business risks which remain at an unacceptable high level.

Risk Management Committee

- Responsible for the oversight of the Risk Management Policies and practices of the University
- Review the Risk Management Policy and associated frameworks, processes and practices of the University as and when needed.
- Shall ensure that the University is taking the appropriate measures to achieve prudent balance between risk and reward in both ongoing and new business activities.
- The Risk Management Committee shall evaluate significant risk exposures of the University and assess management's actions to mitigate the exposures in a timely manner (including one-off initiatives, and ongoing activities such as business continuity planning and disaster recovery planning & testing).
- The Risk Management Committee will coordinate its activities with the Audit Committee in instances where there is any overlap with audit activities (e.g. internal or external audit issue relating to risk management policy or practice).

- The Risk Management Committee may form and delegate authority to sub-committees and/ or individuals when appropriate.
- The Risk Management Committee shall make regular reports to the Council

Internal Audit

The internal audit function will support University's programmes by providing advice and support on risk management, and through an annual independent review of risk management practices and procedures, provide assurance on their effectiveness and efficiency and provide ad-hoc guidance on risk management.

Senior Management Team

The effectiveness of risk management is unavoidably linked to management competence, commitment and integrity, all of which forms the basis of sound corporate governance. Corporate governance provides a systematic framework within which the senior management team can discharge their duties in managing the University.

Senior management team are responsible for:

- Considering new and existing risks and their impact on proposed plans as part of the annual planning cycle. Risk records must be maintained up-to-date on an regular basis to reflect any changes which may occur
- Providing direction and guidance within their areas of accountability so that staff best utilize their abilities in the preservation of the University's resources
- Successfully promoting, sponsoring and coordinating the development of a risk management culture throughout the University

- Guiding the inclusion of risk management in all strategic and operational decision making
- Possessing a clear profile of major risks within their area of control incorporating both opportunity and negative risks
- Maintaining a framework to manage, monitor and report risks
- Managing risks to meet University objectives, mission and vision
- Improving corporate governance

Supporting senior management team to achieve the above objectives are directors of the various directorates and deans of the various faculties.

Heads of Departments/ Heads of Units and Section

Heads at all levels will be responsible for the adoption of robust risk management practices and will be directly responsible for the results of risk management activities relevant to their area of responsibility.

Employees.

All employees are responsible for:

- Acting at all times in a manner which does not place at risk the health and safety of themselves or any other person in the University
- Providing direction and training to persons for whom they have a supervisory responsibility or duty of care provision relating to safety
- Identifying areas where risk management policies should be adopted and advising their supervisors accordingly
- Meeting their obligations under relevant legislation including work health and safety

- Taking all practical steps to minimize the University's exposure to contractual, tortuous and professional liability

Risk Improvement Officers (RIO)

Designated staff in all Directorates, Faculties, Departments, Sections and Units will have roles in coordinating and facilitating the risk management processes.

The Risk Improvement Officers shall:

- Work with all staff to identify, document and report strategic risks from their areas that influence the University's ability to achieve its mandate and goals for inclusion in the University's strategic risk register
 - Provide risk management advice and process support to their designated area
 - Develop risk management practices and tools for their designated area, identify emerging or changing risks and assist in building risk management capacity across the University
 - Work with appropriate authorities to determine risk tolerance
 - Report the performance of risk management within their designated areas..

All identified risks must have a designated person responsible for the management of appropriate policies, procedures, activities and resources to contain the risk within acceptable limits. This designated person has direct oversight of the risk they manage. He/she must be a designated individual with the commensurate authority to manage the risk and;

- Develop a risk management plan and report on the status of the

risk and controls as per the risk management plan

- Ensure a common understanding of the risk and specify how the mitigating strategy is intended to manage the risk
- Ensure any gaps or changes in the controls and mitigating strategies are identified and communicated to the appropriate level
- Make recommendations on the risk tolerance to the appropriate authority
- Track the risk through its life-cycle to closure or sufficient reduction in likelihood and/or consequence
- Ensure risks are identified and manage as part of policy development, program planning and delivery, operational decisions and allocation of resources.

8.0 REVIEW OF THE RISK MANAGEMENT POLICY

The Risk Management Policy shall be reviewed as and when need be to ensure relevance to ATU's business and compliance with new developments in risk management. The various sections that form part of this policy shall be reviewed independently and individually whenever the need arises.

9.0 APPROVAL

That the University Council approves the Risk Management Policy and Guideline for adoption by the University.

Name: DR WILFRED KWABENA ANIM-ODAME

Signature

Designation: COUNCIL CHAIRMAN

Date:

Name: PROF. SAMUEL NII ODAI

Signature

Designation: VICE CHANCELLOR

Date:

GUIDE TO THE IMPLEMENTATION OF THE RISK MANAGEMENT POLICY

APPENDIX ONE: RISK MANAGEMENT PROCESS

The University's risk management process as referred to in the Risk Management Policy is depicted in the

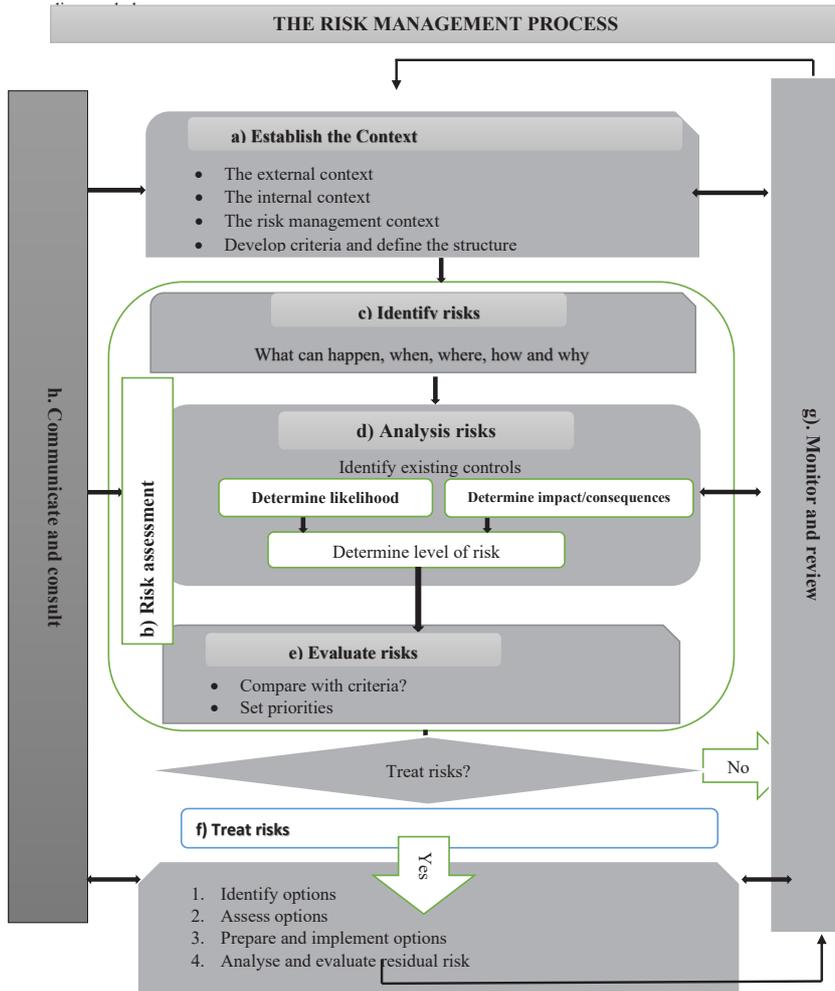


Figure 4: Risk management process diagrammatic representation

Figure 4 outlines the five components for identifying and managing risk

- Establishing the context
- Risk assessment (identification, analysis and evaluation)
- Risk treatment
- Monitoring and review
- Communication and consultation

The five components have been isolated for descriptive purposes, but in reality they overlap and blend together. In addition, risk may not progress through the components at the same rate.

a) Establish the context

Before beginning the process of managing risk, an understanding of the various interconnected elements that affect the University, program or policy must be developed. To establish the context for risk, the Risk Improvement Officer should;

- Outline the mandate and context in which the risk assessment will take place.
- Establish the scope and the duration of risk management process.
- Determine who should be involved in the risk management process.

b) Assess the risk

Assessing the risk includes identifying, analysing and evaluating the risk.

c) Identify the risk

Risk identification requires the ability to visualize how particular sets of circumstances might cause both routine and extraordinary events. The risk team should;

- Identify the risk that could affect the achievement of the university, program or project objectives.
- Identify the sources of each risk i.e. identify when, where, why and how it is likely to occur and who might be involved.

For each risk, identify the current control in place.

Controls are the processes and practices that are currently in place to manage the risk? Do the controls work fully so that the risk is sufficiently reduced? Practical example – you have a lock on the door, but the lock sticks or it is left unlocked by someone, the control is insufficient.

Assurance – are there any control where you lack the assurance they are working or not? Practical example- you have a lock on the door but no one is responsible for checking that the door is actually engaged or you have a fire extinguisher but no one is responsible for refilling

If there are gaps, then detail any action plan you might have to remove those gaps. The responsible person for implementing the action should always be detailed.

d) Analyse the Risk

Risk analysis involves identifying the positive or negative consequences and the likelihood of the risk occurring and assigning risk rating to them. This determines their severity and the relevant risk management response required. The team responsible for the risks should;

- Use 5 point scale (Rare, Unlikely, Possible, Likely, and Almost Certain) to rate each identified risk for the likelihood of its occurrence.

1 = Rare	Occurs only in exceptional circumstances
2 = Unlikely	could occur at some time if circumstances change.
3 = Possible	rarely occurs in normal circumstances.
4 = Likely	will probably occur in most circumstances.
5 = Almost certain	expected to occur in most circumstances.

Rating

Consequences/Impact

1= insignificant:	No reputation or credibility impact. Consequences are dealt with by routine operations.
2 = Minor:	Effectiveness of some aspect of University but would be dealt with internally.
3 = Moderate:	Some reputational damage or loss of credibility. Consequences would not threaten the organization but would mean there would be a significant review or changed ways of operating.
4 = Major:	Major reputational damage and loss of credibility. Consequences would threaten the effectiveness and efficiency, or survival of the programme or University.
5 = Catastrophic:	Catastrophic reputational damage and inability to continue operations for the foreseeable future.

Consequences would threaten the survival of the University.

The 5x5 risk assessment matrix (below) evaluates risks in terms of consequences (impact) and likelihood, from the University's perspective. Plotting risk on this matrix gives a risk ratio (index) which indicates the degree of severity of the risk and the associated risk management response.

Risk Assessment Matrix

LIKELIHOOD [PROBABILITY]	IMPACT [CONSEQUENCE]				
	1= Sig- nificant	2 = Minor	3= Moderate	4 = Major	5= Cata- strophic
1 = Rare	Low	Low	Low	Low	Moderate
2 = Unlikely	Low	Low	Moderate	Moder- ate	Moderate
3 = Possible	Low	Moderate	Moderate	High	High
4 = Likely	Low	Moderate	High	High	Extreme
5 = Almost Certain	Low	Moderate	High	Extreme	Extreme

Extreme Risks: are unacceptable to the University as they would significantly impact the University and its operations. For Strategic Risk, given the highest categorization of this risk, its owner will normally be at the University Council level. Mitigating actions must be considered as a first response. Council must approve a proposal to “accept” any extreme risk. Business plan must reflect action to manage the risk. A full contingency plan must be in place and a review date agreed by the risk owner and approved by Council.

High risks: will have a major impact on the University and comprehensive risk management action is required. Senior management must approve a proposal to “accept” any high risk. Business plan must reflect action plan to manage the risk. A full contingency plan must be in place and a review date agreed by the risk owner and approved by the Council.

Moderate risks: while considered a lesser threat, should be subject to mitigating action while considering other Directorate’s business plan priorities. They should be reviewed quarterly to ensure that they do not escalate to become high risks. A contingency plan may also be needed particularly for risk with medium impact/low likelihood i.e. low risk.

Low risks: are low impact and low priority and generally the University would be content to carry such a risk as existing controls are able to manage it. No immediate action is therefore required, but they should be kept under periodic review.

e) Evaluate the Risk

When evaluating risk it is important to identify areas where minimal levels of risks are permissible, as well as areas where high level of risk should be managed through mitigating strategies and controls. The objective is to separate minor acceptable risks from major risks.

Risk tolerance: will be determined by examining the risk assessment to gauge if the risk is tolerable or not. Key factors impacting risk tolerance include the internal and the external impact of the risks, the likelihood of the risk occurring, the ability of the University's mitigating strategies and controls to influence the risk, and the environment (political, stakeholders, media, etc.).

Using the initial analysis, the team responsible for the risk should:

- Review each risk against university priorities.
- Consider University's responsibilities with respect to each risk.
- Determine if the risks are within or outside University's risk tolerance.
- Assess the controls in place to manage each risk and the effectiveness of those controls.
- Decide which risks are unacceptable and rank them for the treatment (risk management). For each risk outside the University's risk tolerance, identify the risk owner.

f) Treat the Risk

Effective risk management is not about avoiding risk, but about identifying the risk and putting in measures to mitigate the likelihood and the impact of its occurrence. There are variety of responses to risk.

- Tolerate – accept the risk and be prepared to manage its consequences;
- Transfer – the risk to a third party;
- Treat - reduce the risk through the application of controls;

- Terminate – avoid the risk by deciding not to proceed with the activity; and
- Take the Opportunity- see the risk as having the ability to further business objectives while being aware of and taking action against the risk involved.

Risk treatment is ascertained by asking the following key questions:

- What action is being taken?
- Who is the person responsible for the controls?
- What are the controls and what is the process for giving assurance to the risk owner that the control works?
- What indicators do you have that help you to see if the risk is getting worse or better?
- When is the next review of this risk scheduled?

RAYG Status

How content are you with the existing controls on a Red, Amber or Green scale where:

Red	you think it's likely that the risk will happen and have adverse impact
Amber	the risk might happen and will have some impact.
Yellow	the risk may happen but the chances are slim. Impact will not affect the University in major way.
Green	the risk is almost certain not going to happen or, if it

does, there will be no impact. It may also mean that existing controls are adequate to manage the risk.

Note that for the top two the University expects that action will be taken to reduce the risk.

This action should be well detailed.

Propose a risk treatment approach for each risk.

Risk treatment options therefore include:

- Terminate exposure to the risk.
- Transferring or sharing or all of the responsibility for control of the risk to another party or parties.
- Treating the risk to reduce the likelihood of its occurrence and/or mitigate the consequences.
- Take advantage of the opportunity identified to enhance the achievement of the set objective.

When the analysis indicates that the risk is outside the University's accepted risk tolerance, the team will apply an appropriate reporting method and mechanism to ensure that the risk is appropriately understood, assessed, managed and communicated to the appropriate person or group.

Once the risk treatment option is chosen, the risk is treated and this involves:

- Developing a risk management plan that is consistent with the chosen risk treatment approach and brings or maintains the risk within the University's risk tolerance. The plans should include the controls in place to manage the risk, the risk treatment, approach, and the mitigating strategies if the approach is to treat the risk. Mitigating strategies

are by definition, new strategies undertaken to mitigate identified risk. Identifying existing controls as a way to mitigate risk will not reduce the level of risk to an acceptable level. Existing controls will need to be strengthened or new strategies identified to manage the risk.

- Implementing the risk management plan with available resources.
- Monitoring and reporting on the risk and risk treatment to ensure the treatment is working and to identify the opportunities to continually improve the risk management plan.
- Mitigating strategies are new strategies undertaken to mitigate identified risk.

g) Monitor and Review Risk

Risks need to be continuously monitored and reviewed since very few risks remain static.

Both monitoring and review of risk should be a planned part of the risk management process. It can be periodic or adhoc. The purpose of monitoring and review is to;

- Determine the effectiveness of the treatment in controlling the risk,
- See how the risk has changed overtime and
- Identify when further action is required.

The risk remaining after risk treatment is called the Residual Risk.

Risks need to be kept under ongoing review. This will need to take place at several levels,

Example;

- The University Council and the Audit Committee should regularly review the strategic risk facing the University.
- Project risk should be reviewed by Senior Responsible Owners.
- Pro VC / Deans of faculties will formally review their Faculty Risk Registers as part of the business planning and mid-year review process. They should also make regular assessments of how effectively their delivery partners manage their risks.

When monitoring and reviewing risks, the following questions should be considered;

- Are the controls effective and efficient in both design and operation?
- Have there been any changes in the external and the internal environment or new information that will affect the risk, risk analysis or risk treatment plan?
- Are there any new risk that should be assessed?
- What have we learned from the events, near-misses, changes, trends, success and failures to help manage the risk in the future?

h) Communicate and consult

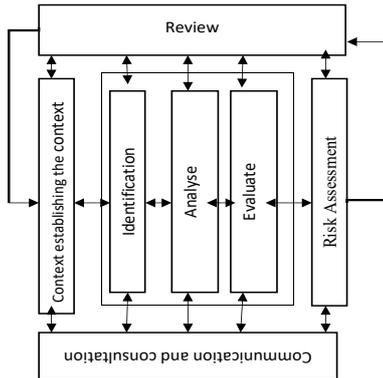
Communication and consultation is not a distinct stage in the management of risk but runs through the entire risk management process. The identification of new risks or changes in risk level or treatment is dependent on effective and timely communication and consultation. Environmental scanning for risks depends on maintaining good communication network with relevant contacts and sources of information to facilitate identification of changes, which will affect the University's risk profile.

APPENDIX TWO: TEMPLATE FOR ASSESSING RISK

Step 1 – Establish the Context

Establish the risk management, strategic, and organizational context to set the stage for the risk process and ensure a rigorous methodology.

This is a critical stage that should be done in advance of a risk workshop. When you hold a risk workshop the participants must have a common understanding of the context and assess the risks with defined criteria that reflect the risk tolerance of your organization (e.g. what constitutes an extreme impact in one organization may be considered only a minor impact in another). This will help personal bias and ensure that the process is replicable.



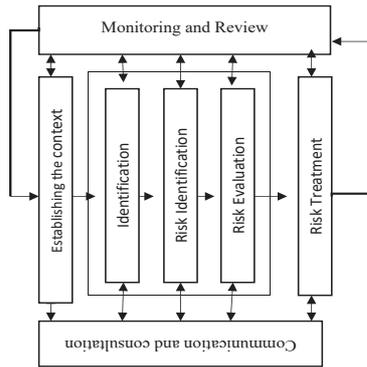
Identify	Response
1. Risk management context: <ul style="list-style-type: none"> • What is the object and the scope of the risk assessment (e.g. strategic goals, operational plans etc.?) • The risk criteria that will be used to analyse the impact and likelihood levels (e.g. 1-5 table defining impact and likelihood level) • The time frame for the risk assessment (3 years, 5 years etc.) 	
2. External context <ul style="list-style-type: none"> • What are the key external factors that impact on risks? • Who are the key stakeholders who should be consulted and / or participate? 	
3. Internal Context <ul style="list-style-type: none"> • What are the key factors from within your faculty/Department/Directorate that impact on risk? • Who are the internal staff that should participate in the risk process or be consulted or informed? 	
Question 4 Where are the strategic strengths and weaknesses of your University?	

Step 2 – Identify Risk

Consider the input from step 1 and identify what and how risk events can arise.

What are the events and treats that would have an impact upon meeting the objectives? Risk can be identified by brainstorming, survey and interviews.

Tips: seek input from a broad perspective of people.



Part 1 ID possible risks	Risk event (source + pathway consequences)
e.g. Risks to the University Clinic goal not maintaining community health by implementing a public immunization program for X disease Risk: inadequate staff capacity to inoculate dispersed population.	We do not have sufficient staff to immunize such a large population that is spread over such a large area. This could result in communities being missed leading to localized epidemics and multiple fatalities.
Risk 2 Name	
Risk 3 Name	
Risk 4 Name	

Step 3 – Analyze Risks

Identify and Assess Existing Controls

Before you can analyze the impact and likelihood of a risk occurring, you must consider existing controls that are **already in place** to prevent the risk and mitigate impacts should the risk occur.

Risk Name (from Step2)	Existing Controls to prevent risk from occurring	How effective is this control on reducing the risk? Rating (1-3) 1 = low 2 = medium 3 = high	Existing Controls to minimize impacts should risk occur	How effective is this control on reducing the risk? Rating (1-3) 1 = low 2 = medium 3 = high
e.g. Risks to implementing a community immunization program for X disease Risk Name: Inadequate Staff Capacity to immunize	a) Call in all staff, cancel leaves.	1=Low - only small numbers of staff are on leave at any one time	b. Clinics and hospitals to treat sick.	2= Medium effectiveness in the event of a major outbreak, clinics and hospitals will be over run and staff infected.
Risk 2 – Name				
Risk 3 - Name				

a) Once you have identified the existing controls, with workshop participants create a credible defined scenario that would lead to the risk event:

Example: e.g. Risks to University Hospital goal of maintaining public health by implementing a public immunization program for disease X

Risk: Inadequate Staff Capacity to inoculate dispersed population

Scenario: In the event of an outbreak of the highly contagious X disease, there will be insufficient hospital staff to immunize vulnerable people on time to prevent a major outbreak. Because the disease is so virulent, the hospital will be unable to treat the ill. Thousands of fatalities are expected.

b) Assess the likelihood and consequence of the risk event on your scenario using **the predefined risk criteria / consequence and likelihood tables** (see sample tables below). **Tip:** Assess the consequence level first, and then assess the likelihood of the scenario occurring and resulting in that level of consequence.

Consequence - outcome of an event affecting a set objective.

Note: there may be a range of possible outcomes associated with an event (financial, reputation, etc.). Rate consequence that is deemed to be the most significant

1 = No reputational or credibility impact. Consequences are dealt with by routine operations.

Insignificant:

2 = Minor

3 = Moderate

effectiveness of some aspect of the organization but would be dealt with internally.

Some reputational damage and loss of credibility. Consequences would not threaten the organization but would mean there would be a significant review or changed ways of operating.

4 = Major
Major reputational damage and loss of credibility. Consequences would threaten the effectiveness and efficiency, or survival of the program or organization.

5 = Catastrophic
Catastrophic reputational damage and inability to continue operations for the foreseeable future.

Catastrophic
Consequences would threaten the survival of the organization

Likelihood, Likelihood is the probability that the risk event will actually occur.

1 = Rare

: Occurs only in exceptional circumstances

2 = Unlikely

: Could occur at some time

3 = Possible

: Rarely occurs in normal circumstances

4 = Likely

: Will probably occur in most circumstances

5 = Almost

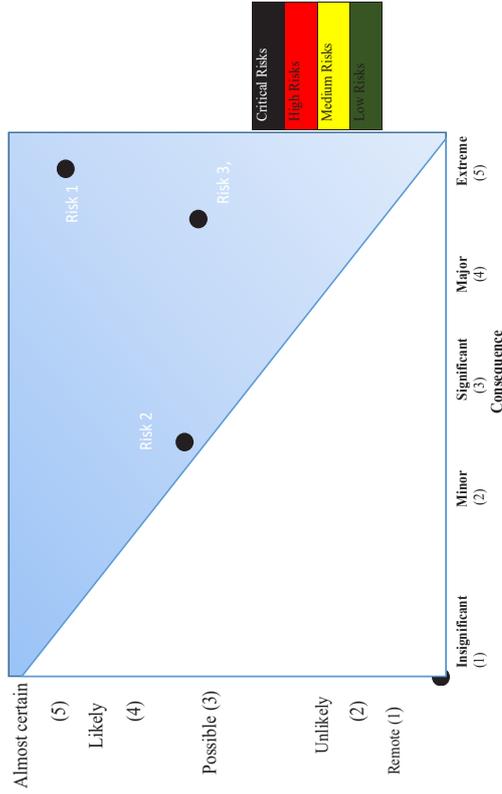
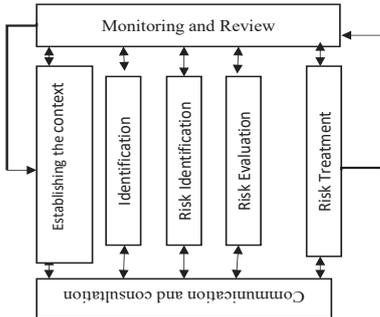
: Expected to occur in most circumstances

certain

Step 4 – Evaluate Risks

Do the risks fall within your organization's risk tolerance?

Plot consequence and likelihood ratings on a matrix to determine relative ratings and the level of risk and then enter the risk ratings into the register.

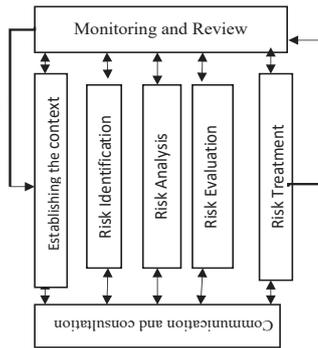


Step 4 - Analyze Risks continued
Risk Register

Description of risk and what is at risk	Risk Rating	Risk Tolerance	Risk Owner	Risk response, control and assurance	Gaps in control and assurance, including what action is being taken to close these gaps	RAG Status
<p>What is the risk category:</p> <ul style="list-style-type: none"> ➤ Strategic Programme or project ➤ Operational ➤ Joint with delivery partner(s) <p>What is the risk that will prevent us from achieving our objective? You should make clear what objective is at risk and this should be cross referenced to our business plan.</p>	Expressed in likelihood and impact	What is level of risk that you would be content with?	Individual with the authority to manage the risk	Controls in place to reduce the risks to achieving the objective. The person responsible for the controls. The process by which the risk owner is given assurance that the risks are sufficiently controlled. What action is being taken?	Control: Do the assurances identify that any of the controls are not working or are not fully implemented? Assurance: Are there controls where assurance is available? What actions are planned to close gaps? Who is the person responsible for this and when do they need to be done by?	How content are you with the existing controls? <u>Green</u> : totally no further action needed. <u>Amber-green</u> : no content but we are taking more actions to increase contentment <u>Amber-red</u> : not content, and we are taking actions. <u>Red</u> : worried and don't know what to do.

Step 5 – Evaluate Risks

Do the risk fall within your organization's risk tolerance?



Are the risks:

Acceptable – The risk is acceptable given that current risk treatments continue.

Unacceptable – The risk cannot be justified under any circumstances.

Tolerable – Further risk reduction may be impractical, but the opportunities and benefits of the proposed activity outweigh the risks.

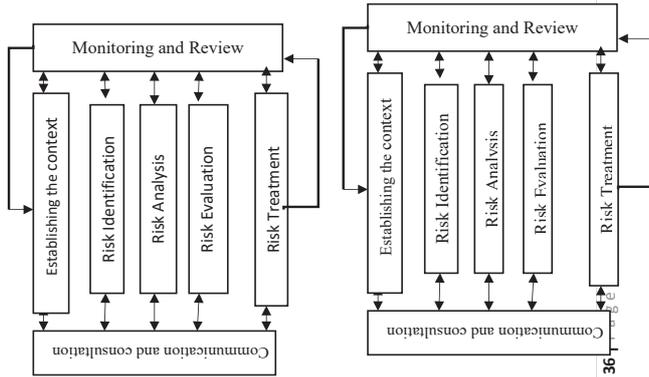
Acceptable with additional controls or treatments - Other risk controls or treatments can be added to reduce risks to acceptable levels.

Step 6 – Treat Risks

Determine risk treatment options

Step 5 – Treat Risk (Continued)

Develop and implement a specific management plan which includes consideration of funding



There are 4 risk treatment options:

1. **Accept the risk** (when there is no option but to proceed or the benefits of proceeding outweigh the potential costs – this must be a deliberate and informed decision).
2. **Avoid the risk** (get out of this area of business – governments frequently do not have this option)
3. **Share the risk** with another party. This includes 3rd party contracts and insurance. (They must be capable of and willing to assume the risk)
4. **Reduce the risk** by additional controls to reduce the likelihood, consequences, or both

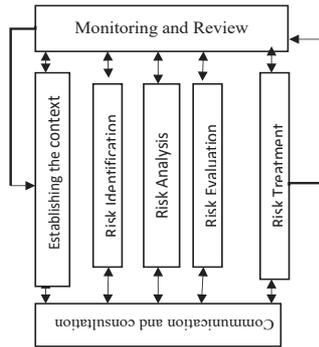
Risk Management Plan	
Risk Treatment	Proposed Action
Description:	Resource Requirements
	Timing
	Assigned Responsibility

If the proposed risk management strategies are deemed to be effective at reducing the risk and that there is adequate resources and capacity to implement it: update the risk register.

NB: Evaluate proposed risk management strategy on the basis of effectiveness at risk reduction and ease to implement. If the strategy is acceptable

Step 6 – Communicate

Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process concerning the process as a whole



Communication Thought Provoking Questions

What method of communication will you use to communicate risk information throughout your organization?

How often will you communicate on various aspects of the risk management process?

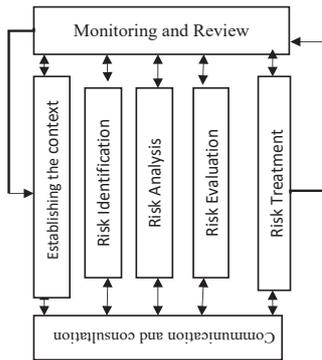
Will levels of detail on risk communication be different for the various levels within the organization?

What communication tools will you employ?

What existing communication within your organization can be used to communicate risks?

Step 7 – Report Monitor, And Review

Monitor and review the performance of the risk management process, risks and changes



Risk	Indicators of Successful Risk Treatment
Risk Name:	Indicator 1
	Indicator 2
	Indicator 3

APPENDIX FOUR: DEPARTMENTAL RISK REGISTER TEMPLATE/RISK PROFILE

DEPARTMENT:

DATE:

OBJECTIVES	RISK NAME & DESCRIPTION	Risk ID	RISK TYPE	RISK OWNER	POTENTIAL ROOT CAUSE(S)	RISK ANALYSIS			EXISTING RISK MITIGATION	CONTROL EFFECTIVENESS	RESIDUAL RISK	DESIRED RESIDUAL RISK	ADDITIONAL INITIATIVES TO FURTHER REDUCE THE RESIDUAL RISK LEVEL (TASK)	TASK OWN ER(S) & DATE (S)
						LIKELIHOOD	IMPACT	INHERENT RISK						

APPENDIX FIVE: SAMPLE UNIVERSITY RISK REGISTER

Risk	Possible Consequences	Risk Assessment before Controls	Actions And Controls	Risk Assessment with Controls	Proposed Treatment	Risk Assessment with Treatment	Responsible Person and Timeline
Strategic Direction The strategic Direction of the Company may not be achieved	ATU may not focus on what is most important to achieve business success	<u>Likelihood</u> Possible Consequences Severe <u>Inherent risk</u> High	ATU objectives have been established Business plan has been developed KPIs have been developed	<u>Likelihood</u> Possible Major Current risk High	Further develop the business plan by formulating and assigning KPIs to key people <i>Link achievement of the action to a long-term performance based incentive e scheme</i>	<u>Likelihood</u> Unlikely Consequences Major Future risk Moderate	Vice Chancellor By 31 Mar 2022
<u>Key people</u> There may be loss of key people form the University	Business plan Objectives may not be achieved Business development may be stalled	<u>Likelihood</u> Likely Consequences Severe <u>Inherent Risk</u> Extreme	Human resources Department established Human resources Policies in place Workforce plan in place	<u>Likelihood</u> Likely Consequence Major Current risk extreme	Develop and implement Measures to retain key people (e.g. long term performance based incentive scheme) Develop and implement a succession plan	<u>Likelihood</u> Unlikely Consequences Minor <u>Inherent Risk</u> Low	Director of Human Resources By 31 Mar 2022
Health, safety, environment (HSE) there may be ins sufficient focus on HSE	People may be injured or killed The University may cause	<u>Likelihood</u> Likely Consequences Severe	Safety management system in place	<u>Likelihood</u> possible Consequence Major	Establish a safety committee Commission an independent audit	<u>Likelihood</u> Likely Consequence Major	Manager HSE By 30 June 2022

	environment damage	Inherent Risk		Current risk extreme	of the safety management system Develop and implement an environmental management system and seek ISO 14000, environmental managements certificate	Current risk Extreme	
Fraud and wrongdoing There may be fraud or wrong doing at the company	There may be financial loss to the University There may be damage to the University's reputation	Likelihood Likely Consequence Major Current risk extreme	Delegations of authority in palace Internal audit Department established	Likelihood Likely Consequence Major Current risk extreme	Conduct a fraud risk assessment Developed and implement a fraud and corruption prevention plan	Likelihood Likely Consequence Major Current risk moderate	Director Internal audit By 30 June 2021

APPENDIX SIX: SAMPLE RISK ASSESSMENT TABLE

Likelihood Rating	Consequence Rating				
	1	2	3	4	5
5	M	H	H	E	E
4	L	M	H	H	E
3	L	M	M	H	H
2	L	L	M	M	H
1	L	L	L	M	H

L = LOW RISK	M = MODERATE RISK	H = HIGH RISK	E= EXTREME RISK
--------------	-------------------	---------------	-----------------

Consequence Definition	Risk Factors	Reputation/Image	Health And Safety Environment(HSE)	Project Management	Business Performance	Likelihood Definition
<p>1 Insignificant The event is of low consequence</p>	<p>1 Financial loss- Small increase in cost Not in line with budget</p>	<p>1 unsubstantiated low profile media exposure or no media attention</p>	<p>1 single minor injury to one person- No lost time or insignificant environment damage</p>	<p>1 Project close to time , budget and quality</p>	<p>1 No impact on business outcome or KPIs</p>	<p>1 Rare The event is only expected to occur in exceptional circumstances</p>
<p>2 Minor The event may threaten a part of the company</p>	<p>2 Financial loss Minor financial impact</p>	<p>2 Substantiated, low impact low media profile (not Front page news)</p>	<p>2 medically treated injury to one person, less than 5 days lost time or minor environment damage</p>	<p>2 project has minor issue with time, budget or quality</p>	<p>2 less than 10% variance in business outcomes or KPIs</p>	<p>2 Unlikely The event is not likely to occur</p>
<p>3 Moderate The event may threaten many parts of the company</p>	<p>3 Financial loss ≤ 500k</p>	<p>3 substantial public Embarrassment moderate Media profile (front page 1 day)</p>	<p>3 minor or medically treated injury to several people less than 10 days lost time</p>	<p>3 project has issue with time, budget or quality</p>	<p>3 10%-25% variance in business outcomes or KPIs</p>	<p>3 Possible The event may occur</p>

<p>4 Major The event may threaten achievement of business objectives.</p>	<p>4 Financial loss – 500k To 2 million</p>	<p>4 Substantiated public embarrassment, high impact Major media attention (National for 1 week or more)</p>	<p>4 single, death, or long term disabling injuries to one or more people or substantial environmental damage.</p>	<p>4 Project has substantial issues with time, budget or quality</p>	<p>4 Likely The event is likely to occur</p>
<p>5 severe the event may stop achievement of the University's goals</p>	<p>5 Financial loss \geq 10% revenue KPIs</p>	<p>5 Substantiated public embarrassment, multiple impacts, long lasting widespread media coverage</p>	<p>5 multiple losses of life or permanent disability, plus extensive injuries to several people or severe environmental damage.</p>	<p>5 Large project has severe issues with time, budget or quality.</p>	<p>5 Almost certain The event is already occurring or is expected to occur</p>

APPENDIX SEVEN: A WALK THROUGH RISK MANAGEMENT PROCESS TEMPLATE
(ADAPTED FROM INTERNAL AUDIT AGENCY TRAINING DOCUMENT)

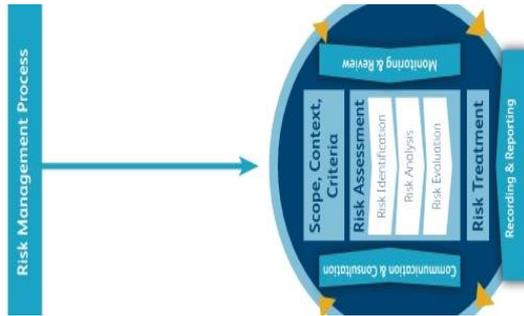
Step 1 – Establish the Context

Establish the strategic, organizational and risk management context in which the rest of the process will take place

State the Objective:

Response	
<p>Question 1 What are the key factors from outside of ATU that may impact on objective?</p>	<p>External:</p>
<p>Question 2 What are the key factors from within ATU that impact on objective?</p>	<p>Internal:</p>

<p>Question 3 What are the strategic strengths, weaknesses, threats and opportunities of your Organisation?</p>	<p>Strength:</p> <p>Weakness:</p> <p>Opportunity:</p> <p>Threat:</p>
--	--

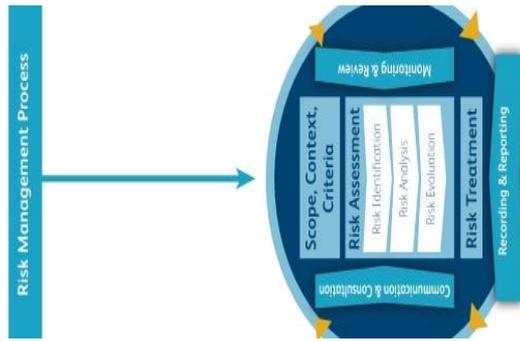


Step 2 – Identify Risks

Identify what and how risk events can arise as the basis for further analysis (What can happen, when, where, how & why)

Objective:

What are the events and threats that would have an impact upon meeting your objectives?



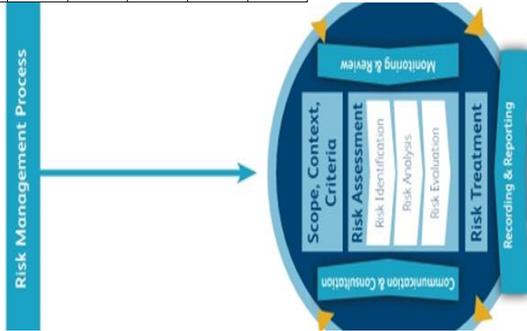
Risk	Explanation
<i>Risk 1:</i>	
<i>Risk 2:</i>	
<i>Risk 3:</i>	
<i>Risk 4:</i>	
<i>Risk 5:</i>	

Step 3 – Analyse Risks

Analyse risk in terms of likelihood and impact

1 = Rare / Insignificant 2 = Unlikely / Minor 3 = Possible / Moderate 4 = Likely / Major 5 = Certain / Catastrophic

Objective:



Risk Name	Likelihood Rating (1 to 5)	Impact Rating (1 to 5)
Risk 1:		
Risk 2:		
Risk 3:		
Risk 4:		
Risk 5:		

Likelihood – Is the probability that a risk will occur in the absence of any compensating controls to prevent the risk.

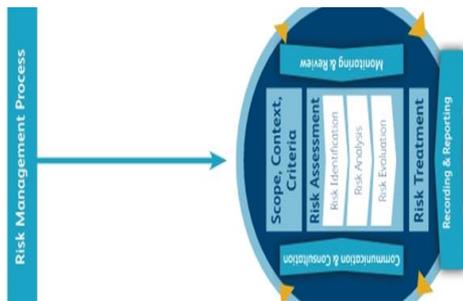
Impact – The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. It is the measure of impact the risk has on meeting our objectives.

Step 4 – Evaluate Risks

Compare estimated levels of risk against the pre-established criteria. Risk must be evaluated in the context of current controls. This enables risks to be ranked so as to identify management priorities

Risk Name	Likelihood Rating (1-5) - <i>a</i>	Impact Rating (1-5) - <i>b</i>	Inherent Risk Rating (<i>a</i> x <i>b</i>)
Risk 1:			
Risk 2:			
Risk 3:			
Risk 4:			
Risk 5:			

Objective.....



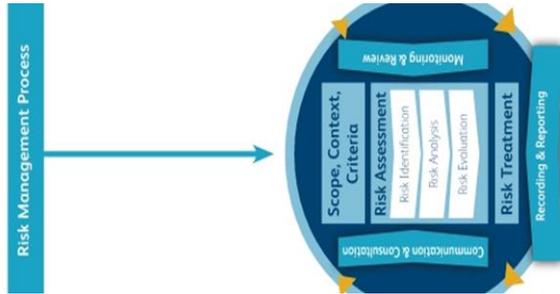
Are the Risks:

- **Acceptable** – The risk is acceptable given that current risk treatments continue
- **Unacceptable** – The risk cannot be justified under any circumstances.
- **Tolerable** – Further risk reduction may be impractical, but the opportunities and benefits of the proposed benefits outweigh the risk
- **Acceptable with additional Controls or Treatments** – Other risk controls or treatments can be added to reduce risks to acceptable levels

Step 5 – Treat Risks

Develop and implement a specific management plan which includes consideration of funding

Objective:

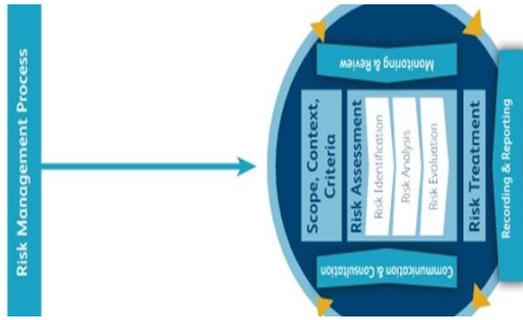


Proposed Risk Management Action Plan	
Risk 1:	
Risk 2:	
Risk 3:	
Risk 4:	
Risk 5:	
Resource Requirements	
Risk 1:	
Risk 2:	
Risk 3:	
Risk 4:	
Risk 5:	
Timing	
Risk 1:	
Risk 2:	
Risk 3:	
Risk 4:	
Risk 5:	
Assigned Responsibility	
Risk 1:	
Risk 2:	
Risk 3:	
Risk 4:	
Risk 5:	

Step 5 – Treat Risks (Continued)

Develop and implement a specific management plan which includes consideration of funding

Objective:



RISK NAME	Impact on Reducing Risk (HML)	Ease of Implementation (HML)	Options Chosen (T/RL/RC)
Risk 1			
Risk 2			
Risk 3			
Risk 4			
Risk 5			

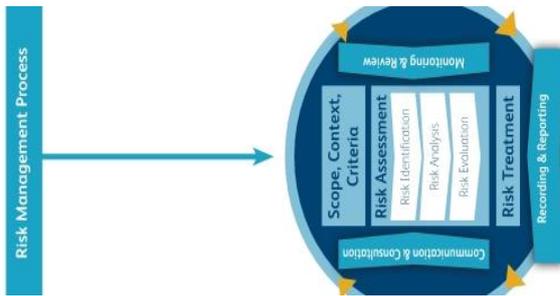
Step 6 – Record and Report

Risk management activities should be traceable. In the risk management process, records provide the foundation for improvement in methods as well as in the overall process.

Objective:

<p>Recording and Reporting Thought Provoking Questions</p> <p><i>What method will you use to Record and report on risk management activities throughout ATU?</i></p>
<p><i>Who will Document risk management activities and outcomes on risk management process?</i></p>
<p><i>Will details of risk reporting be different for the various levels within ATU?</i></p>
<p><i>How often will you Report on your risk management activities and outcomes. within ATU?</i></p>

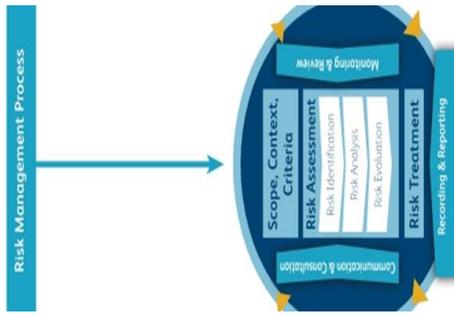
What will warrant the review of the Risk Management records?



Step 7 – Monitor and Review

Monitor and review the performance of the risk management process, risks and changes.

Objective:



Example	Risk Performance Measure
Risk Name – Human Resources A lack of requisite knowledge, skills and experiences among the ministry’s personnel threatens the execution of its business model and achievement of its objectives	Risk Performance Measures (Indicators): <ul style="list-style-type: none"> • Number of training sessions for employees • Skills assessments • Ratio of experienced personnel to less experienced

Risk Name	Risk Performance Measure (Indicators):
1	
2	
3	
4	
5	

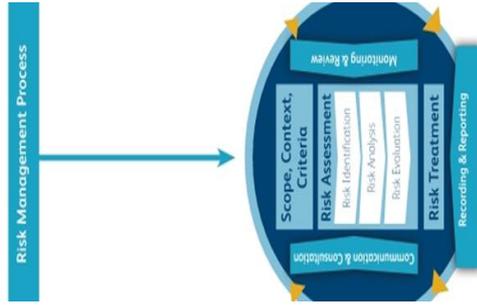
Performance indicators to measure how successful risk is being managed.

Step 8 – Communicate and Consult

Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process concerning the process as a whole

Objective:

Communication Thought Provoking Questions
<i>What method of communication will you use to communicate risk information throughout your organization?</i>
<i>How often will you communicate on various aspects of the risk management process?</i>
<i>Will levels of detail on risk communication be different for the various levels within the organization?</i>
<i>What communication tools will you employ?</i>
<i>What existing communication within your organization can be used to communicate risks?</i>



© 2023

Accra Technical University
Public Affairs Directorate

Email: info@atu.edu.gh/pr@atu.edu.gh
<https://atu.edu.gh>

Tel: 0332095371/0543264917/0544368159