Classification: Governance and University Relations
Approving Authority: President
Responsible Authority: Office of the President
Implementing Authority: Chief of Staff
Effective Date: January 2024
Review: December 2024

University Risk Management Policy & Procedures

1.0 Purpose

1.1 To Identify potential events, practices, and procedures that may significantly affect the University's ability to achieve its strategic goals and successfully maintain its operations, reputation, and legal obligations.

1.2 To respond to risks based on a comprehensive risk assessment for the purpose of ensuring that the University's mission, vision, and objectives will be achieved.

2.0 Scope

2.1 This policy applies to all units, departments, employees, students, contractors, and stakeholders associated with the University.

2.2 It encompasses all categories of risks, including but not limited to strategic, reputational, operational, safety, human capital, compliance, and financial-related risks.

3.0 Definitions

3.1 Environmental Risks - potential negative impacts on the environment stemming from the institution's operations.

3.2 Lab Risks - potential hazards associated with laboratory environments in a university. These can include chemical, biological, radiological, and physical hazards. For instance, risks might arise from handling dangerous chemicals, working with infectious agents, or operating high-powered equipment.

3.3 Occupational Risks - related to the health and safety hazards that employees may encounter as part of their work.

3.4 Risk - the potential that an event, circumstance, or action can adversely impact the University's ability to achieve its objectives.

3.5 Risk assessment - the process of evaluating and quantifying the potential impact and likelihood of identified risks.

3.6 Risk Management - the systematic process of identifying, analyzing, evaluating, and responding to risks, aiming to minimize the likelihood and impact of adverse events and maximize opportunities.

3.7 Risk Register - a comprehensive and structured document that serves as a central repository for recording and tracking identified risks within an organization. It includes essential information about each risk, such as its description, potential impact, likelihood of occurrence, risk owner, and planned or implemented response strategies.

3.8 Risk response strategies - actions and measures designed to mitigate or address identified risks, including risk avoidance, risk reduction, risk transfer, risk acceptance, and risk exploitation.

3.9 Risk matrix - a visual representation that categorizes risks based on their potential impact and likelihood, assisting in prioritizing risk response efforts.

3.10 Risk monitoring - ongoing tracking and evaluation of identified risks, their response strategies, and any changes in their impact or likelihood.

3.11 Security Risks encompass any threats to the safety and well-being of individuals on campus, as well as to the physical and digital assets of the institution.

3.12 Whistleblower is an individual who exposes information or activity within an organization that is deemed illegal, unethical, or incorrect.

4.0 Policy

4.1 The University will adopt a proactive approach to identify and address potential risks before they materialize into significant threats.

4.2 All stakeholders will be accountable for managing risks within their respective areas and shall report and communicate risks to the President's Office Chief of Staff who will oversee the Risk Management Committee.

4.3 University risk management involves:

- The establishment of a Risk Management Committee responsible for implementing the Risk Management Procedures in this policy.
- The determination of the priorities of the risk management system.
- Monitoring progress in managing risk.
- Formal identification of strategic risks that have an impact on the University's goals.
- Development and implementation of a risk register.
- The Chief of Staff reports the status of risks to the President.

4.4 The Risk Management Committee Membership

- Chief of Staff – Chair
- Secretary (Executive Assistant of Chair)
- University President
- Vice President of Administration and Finance (VPAF)
- Vice President of Academic Affairs (VPAA)
- Vice President of Enrollment Services and Student Affairs (VPESSA)
- Chief of Media and Communication Officer
- Vice President of Research (VPR)
- Vice President of Institutional Advancement and Global Engagement (VPIAGE)
- Internal Legal Counsel

4.5 University members will proactively identify and assess risks in all aspects of our operations, including security, financial, occupational, technological, legal, strategic, and compliance-related and reputational domains, to ensure comprehensive risk management.

4.6 Risks identified will be evaluated in terms of their potential impact and likelihood, and prioritized to focus on managing those that pose the greatest threat to our objectives and operations.

4.7 Appropriate risk mitigation strategies will be developed and implemented for all high-priority risks, aiming to reduce the likelihood and/or impact of these risks to an acceptable level.

4.8 Continuous monitoring of risks and the effectiveness of mitigation strategies will be conducted. Regular risk reporting will be provided to senior management and relevant stakeholders.

4.9 We are committed to fostering a risk-aware culture within the organization. Employees at all levels will receive training on risk management principles and their specific roles in supporting these efforts.

4.10 Our risk management practices will comply with all applicable laws and regulations. We will regularly review and update our policies to ensure ongoing legal and regulatory compliance.

4.11 Stakeholders, including employees, partners, and clients, will be engaged in the risk management process, ensuring diverse perspectives are considered and addressed.

4.12 Plans and procedures will be in place to ensure an effective response to emergency situations and incidents, minimizing impact and facilitating quick recovery.

4.13 Technology-related risks, including cybersecurity threats, will be systematically identified, and managed to protect our digital assets and information integrity.

4.14 Environmental risks will be managed in alignment with our commitment to sustainability, ensuring our operations contribute positively to environmental stewardship.

4.15 AUIB supports the reporting of any actions that conflict with our ethical standards, laws, or organizational policies, and as such guarantees protection from retaliation for all employees who, in good faith, report such concerns.

5.0 Procedures

5.1 Schedule annual risk assessment meetings in each department for identifying risks.

5.2 Implement a standardized risk assessment matrix to evaluate and categorize risks.

5.3 Regularly review and update the prioritization of risks using agreed upon criteria for prioritizing risks.

5.4 Develop risk mitigation plans for critical risks that define clear actionable steps for each mitigation plan, including timelines and desired outcomes. Regularly test and update these plans.

5.4.1 Develop specific emergency response plans for different types of incidents, such as natural disasters, technological failures, and security incidents.

5.4.2 Conduct regular cybersecurity assessments and penetration tests and update IT policies in response to new technological threats and trends.

5.4.3 Regularly assess environmental impact and compliance with environmental laws, setting targets for reducing environmental impact and track progress against these targets.

5.4.4 Conduct regular audits and reviews of operational processes and implement standard operating procedures (SOPs) across all departments to minimize the variability that can lead to operational risks. Develop contingency plans for critical operational failures, like supply chain disruptions or system outages.

5.4.5 Monitor financial metrics continuously to identify early warning signs of financial distress. Implement strict financial controls and auditing practices to prevent fraud and ensure accuracy in financial reporting. Regularly review and adjust financial strategies in response to changing market conditions and organizational objectives.

5.4.6 Develop a robust crisis communication plan to address potential reputational risks quickly and effectively. Monitor social media and other public forums to gauge public perception and identify emerging reputational risks.

5.4.7 Keep abreast of changes in laws and regulations that impact different areas of the organization. Conduct regular compliance audits and implement training programs to ensure staff awareness and adherence to legal requirements.

5.4.8 Align risk management strategies with the organization's long-term goals and objectives. Perform regular analyses to identify strategic risks and opportunities.

5.4.9 Implement robust Human Resource policies covering recruitment, retention, and succession planning to mitigate risks associated with workforce management.

5.4.10 Conduct regular and thorough assessments of all workplace and residence environments to identify potential health and safety hazards. This should include the development of clear, concise safety protocols and guidelines tailored to the specific hazards identified in different areas of the workplace.

5.5 A quarterly report supplemented with additional reports as needed will be forwarded to the President together with the Risk Register for notification and/or action, unless the Report includes major issues for action by the President in which case the Report will be submitted to the President as soon as possible after the required action is identified.

5.6 Conduct annual reviews of risk management practices with our internal legal counsel to ensure compliance. Stay updated on regulatory changes that may impact risk management strategies.

5.7 Establish a whistleblower policy to encourage reporting of legal and ethical violations.

5.8 The Risk Management Committee shall meet a minimum of four times per academic year and on demand to address an immediate risk.

5.8.1 The central purpose is to compile a comprehensive Risk Register (see Appendix A).

5.8.2 At the commencement of each academic year, the Chair will call the first meeting of the Committee.

5.8.3 If this is the inaugural meeting of the Committee, the Chair will require members to conduct a risk assessment exercise with faculty/staff reporting to them.

5.8.4 In the next meeting after the inaugural meeting, draft risk assessments will be agreed upon or modified, and then incorporated into a University Risk Register.

5.8.5 At meetings after the inaugural meeting, the Chair will direct members to review the Risk Register.

5.8.6 The Chair, assisted by the Secretary, will produce a draft Committee Report which will be debated and agreed upon in the Committee.

5.9 Major concerns with the Risk Register, e.g., lack of action by the Action Owner, will be referred to the appropriate Committee members for review and rectification by faculty/staff reporting to them.

5.10 The Committee will advise the Emergency Preparedness Committee of any issues that are likely to be of concern to that Committee and include a copy of the agreed upon Risk Register.

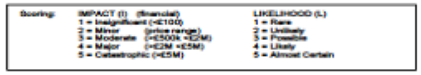
Related Policies and Documents

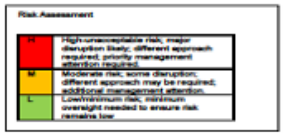
Business Continuity
Compliance and Ethics
Conflict of Interest
Crisis Communication Plan
Data Governance and Privacy policies
Environmental Policy
Emergency Management and Business Continuity
Financial Management
Gifts Policy
Human Resources policies
Information Security and Data Protection
Insurance Policies
Lab Safety
Occupational Health and Safety
Strategic Planning
Whistleblower Policy

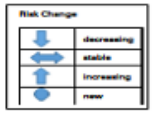
Appendices

Appendix A – Sample of a Risk Register

Annex







Strategic Risks

No	Relevant Strategic Objective	Risk Description	Risk Cause(s)	Risk Consequence	Risk Owner	Inherent Risk Assessment I	Inherent Risk Assessment L	Inherent Risk Assessment PL	Existing Controls	Remaining Risk Assessment I	Remaining Risk Assessment L	Remaining Risk Assessment PL	Actions for further control	Action Owner	Action Review Date
1															
2															
3															
4															
5															
6															
7															
8															
9															
10															