

Operations Risk Management Policy

Policy Owner	Vice Chancellor for Financial and Administrative Affairs	Responsible Office	Office of VCFAA
Approved By	Chancellor	Effective Date	October 2025
		Next Review Date	October 2028

Purpose

This policy aims at identifying the probability of having negative consequences of certain incidents that might occur during the normal course of operations and thus clarifying the set of controls, activities and actions in place to control AU's business continuity with regards to such risks. Each activity or task carries some element of risk. Therefore, it is imperative to have a proper risk management policy to identify and tackle risks that may affect the functioning and outcomes of various business operations, tasks and activities.

Scope

This policy shall cover operational risks pertaining to fiscal resources, information technology, facilities, and occupational health and safety.

Policy Statement

This operations risk management policy serves as an institutional framework that provides guidelines to monitor and track possible risk factors that might cause disruptions to the smooth functioning of business operations, and thus hinder the fulfillment of the University's mission or strategic goals. The AU risk management policy is tailored around Ministry of Education standards and the CAA requirements.

A number of risk factors can affect the proper delivery of University's key business activities and support services. All potential risk factors are grouped into one of the following risk categories:

1. Financial Risks
2. Information Technology Risks
3. Facilities and Infrastructure Risks
4. Environmental Health and Safety Risks

■ Financial Risk Management

1.1. Purpose

This section identifies, evaluates, and mitigates the negative impact of different sources of financial risks which may expose the University to potential losses of financial resources or fluctuation of financial performance. Therefore, a structured methodology is established and adopted by the University to regularly identify such risks, evaluate the negative financial impact of certain events, decide their significance and adopt the best risk mitigation strategies to deal with such risks.

1.2. Financial Risk Identification

1.2.1. Credit Risk

Credit risk is the risk that an external party to a financial instrument will fail to meet an obligation, causing the University to incur a financial loss.

1.2.2. Liquidity Risk

Liquidity risk is the risk that the University will encounter difficulties in raising funds to meet its liabilities when they become due.

1.2.3. Interest Rate Risk

Interest rate risk is the risk associated with the fluctuations in the interest rate on its interest-bearing assets and liabilities; namely fixed deposits, medium-term loan and borrowings.

1.2.4. Accounts Receivable Risk

While the University balances between the interests of all stakeholders, certain special situations faced by some students can justify granting them credit facilities by postponing the payment of due balances or accepting settlements by post-dated cheques or scheduled installments. The accounts and cheques receivable risk is identified by the overdue customer balances, cheques receivable and scheduled installments with the probability that such amounts are becoming uncollectible.

1.2.5. Compliance Risk

This is the risk of non-compliance with financial rules, regulations, standards and laws. Key areas of concern include adherence to Federal Tax Authority (FTA) regulations, General Pension and Social Security (GPSSA) requirements and financial reporting standards.

1.2.6. Financial Fraud Risk

Financial fraud risk is the potential for financial loss due to intentional deception aimed at obtaining an unlawful financial advantage. This includes offenses such as embezzlement, asset misappropriation, fraudulent financial reporting, bribery and corruption.

1.2.7. Funding or Grant Non-Compliance Risk

Failure to adhere to the specific terms, conditions, and obligations in a funding or grant agreement constitutes non-compliance. This occurs when a recipient does not meet the requirements set forth by the funding source.

1.2.8. Budget Insufficiency Risk

This risk involves the risk of running short of budget due to declining revenues related to potential drop in student enrollment/ decreasing demand on certain programs, or due to uncontrolled increases in expenditures or financial losses during the normal course of business activities which might be caused by uncontrollable circumstances such as fire, theft, claims by third parties for damages or losses, which will ultimately affect the University's ability to meet its obligations.

1.2.9. Human Resources Risk

Human resources management function is subject to various risks during the normal course of operations, including legal non-compliance, talent attrition, shortage of qualified employees, employee performance issues impacting the quality of work and achievement of goals and objectives, and the inability to adapt to recent trends in the business environment.

1.2.10. Procurement Risk

Some risks that can be associated with procurement function from financial perspective may include lack of a strategic perspective of the procurement activities; failing to maintain viable relationships with key vendors, discontinued availability of supply sources for some key products and services that add critical value to work, lack of proper and timely communications with other units related to key projects, contracts, events and activities which can cause delays in providing the necessary supplies, equipment and tools, or price disadvantages due missing the benefits of bulk buying.

1.3. Financial Risk Evaluation and Mitigation Methodology

1.3.1. Credit Risk

Financial assets, which potentially subject the University to concentration of credit risk, consist principally of the current bank accounts and deposits/ saving accounts. The University mitigates its credit risk with regard to the bank deposits throughout:

- a) Dealing with high credit quality financial institutions, in addition to conducting continuous review of the financial institution's credibility, considering the trade-off between the benefits obtained from dealing with certain financial institution and the credibility risk involved.
- b) Extra available funds are invested in short-term fixed deposits that don't exceed 1-year maturities and over several maturity dates carefully distributed throughout the year to ensure satisfying any urgent needs for cash to meet operational requirements while avoiding the liquidation of such deposits before the maturity date and thus losing the expected returns.
- c) The University's management is continuously evaluating its investment credit risk to ensure that the credit risk related to bank accounts lies within an acceptable range.

- d) To ensure that agreements with financial institutions include clear exit terms such as repurchase agreements or liquidation clauses. These exit terms can be utilized in case of an increase in the credit risk or if investment returns become unfavorable.

1.3.2. Liquidity Risk

To mitigate such risk, the management ensures the availability of diversified funding sources along with continuous monitoring of liquidity sufficiency on regular basis.

- a) Regular cash flow forecasting serves as a key indicator of future cash sufficiency, which helps providing an early alarm pertaining to any anticipated liquidity problems.
- b) Excess funds are invested in a mix of short-term and long-term fixed deposits, carefully structured across the period to meet any urgent cash needs for operational requirements without sacrificing returns. Approximately 60% of these funds will be invested in short-term deposits.
- c) Maintain a cash safety margin equivalent to a minimum of (3) times total monthly operating expenses in highly liquid deposits.
- d) Availability of easily accessible funding sources; either through equity or debt sources, which should be maintained in order to quickly raise necessary funds to meet any financial obligations and ensure smooth running of operations.
- e) Maintain reliable and sustainable relationships with banks and other financial institutions to facilitate providing the necessary funds within a short period.

1.3.3. Interest Rate Risk

To mitigate the risk of having lower rates on deposits or higher rates on term borrowing in light of the changes in interest rates prevailing in the market, the University's financial management should:

- a) Spreading investments across various financial institutions, asset classes, and maturity dates enhances flexibility to adapt to changing market conditions.
- b) This method also reduces the exposure to the risk of losing the part or the whole returns on such deposits due to potential early liquidation of the deposits to meet emerging spending requirements.
- c) In addition, the University should regularly conduct a continuous revaluation and analysis of the market rates to maximize interest revenues on deposits and minimize interest expenses on borrowings.

1.3.4. Accounts Receivable Risk

The accounts receivable risk is mainly involved with amounts due from students, sponsors, tenants and other customers. The University mitigates the accounts receivable risk through the following strategies:

- a) Development of credit and collection policies to enforce timely payments with control measures such as late payment fees and service restrictions.
- b) Accounts receivable management to continuously monitor aging balances, identify potential bad debts, and implement robust collection procedures.
- c) Implementation of clear payment terms prior to accepting cheques to settle due accounts receivable, by reducing their maturity periods to the minimum, and maintaining detailed stakeholder payment history.

- d) Automated system controls to easily track accumulated balances, generate alerts, and support efficient collections.
- e) Establish and monitor credit limits for customers, students and sponsors to prevent excessive balances.
- f) Maintain adequate allowances for doubtful debts to protect against potential losses and financial performance volatility.
- g) Explore sustainable funding sources via different fundraising options to support students facing payment difficulties, reducing default risks.
- h) Maintain an efficient cheque management system to track bounced cheques, enforce recovery, and restrict post-dated cheque acceptance to low-risk customers with short maturities.

1.3.5. Compliance Risk

- a) Avoid high-risk transactions or business activities that may lead to potential violations of regulatory requirements.
- b) Continuously monitor regulatory changes especially those related to Value Added Tax (VAT) and Corporate Tax (CT) and ensure that policies and procedures are regularly reviewed and updated.
- c) Engage with legal and compliance experts to interpret and navigate complex regulatory landscapes and to ensure alignment with current regulatory standards.
- d) Develop a structured compliance training program that encompasses regulatory requirements applicable to taxation and compliance areas.
- e) Designate a specific staff member within the Office of Finance to oversee regulatory compliance efforts and serve as a point of contact for compliance-related inquiries.
- f) Utilize technology to automate compliance processes and improve data accuracy.
- g) Regularly assess the appropriateness of accounting policies in light of changes in regulations or business operations.
- h) Promote open communication channels between finance teams, management, and external auditors to facilitate the identification and resolution of potential non-compliance issues in a timely manner.
- i) Regularly coordinate with the internal audit team to assess compliance with financial reporting standards. Internal audits can help identify areas of improvement and strengthen controls.
- j) Employ external auditors (Big-4 & Government Auditors) to conduct independent audits of financial statements to avail an unbiased review, which will help to identify and rectify any non-compliance issues before financial statements are finalized.

1.3.6. Financial Fraud Risk

- a) Implement and enforce robust internal controls, including segregation of duties, dual authorization for financial transactions, and regular audits to deter and detect fraudulent activities among Finance.
- b) Conduct a background checks on new hires for high-risk positions.
- c) Provide regular training to employees on fraud awareness, ethical behavior, and the organization's policies and procedures. Educate employees and better equip them to recognize and report

suspicious activities.

- d) Clearly define and segregate financial duties to prevent a single individual from having too much control over a particular financial process to reduce the risk of fraud going undetected.
- e) Obtain insurance to transfer the financial risk of potential losses due to fraud, such as fidelity insurance policies. This transfers the risks against losses resulting from employee dishonesty or fraudulent activities.

1.3.7. Funding or Grant Non-Compliance Risk

- a) Conduct thorough due diligence on funding opportunities, grants, and scholarships before accepting them. Ensure alignment with the university's mission, strategic goals, and operational capacity to meet the requirements and terms and conditions attached to the funding sources.
- b) Establish strong internal controls to track and verify compliance with funding conditions throughout the project or grant period.
- c) Maintain open communication with the donors to address any uncertainties or seek clarification on terms and conditions.
- d) Foster transparency in financial reporting and ensure that all financial transactions related to the funding are accurately documented and reported.
- e) Keep staff updated on any changes or updates to funding/ grants requirements through continuous training and communication.

1.3.8. Budget Insufficiency Risk

This involves the risk of running short of budget due to declining revenues due to potential drop in student enrollment, decreasing demand on certain programs, or due to uncontrolled increases in expenditures or financial losses that might be caused by uncontrollable circumstances such as fire, theft, claims by third parties for damages or losses, which will ultimately affect the financial performance and the ability to meet certain requirements to ensure smooth running of operations. To avoid falling into budget insufficiency risk, the following steps must be taken:

- a) All revenue and expense estimates shall be based on clear assumptions that reflect a systematic methodology of estimation of the main/ leading accounts.
- b) Continuing improvement of the annual budget preparation cycle to ensure its ability to predict any potential challenges in advance and take necessary remedial measures to ensure optimal allocation of resources as needed to achieve the strategic goals and objectives.
- c) Compare performance against industry standards to identify areas for improvement.
- d) Maintain a contingency fund to provide necessary funding for any unplanned or emergency spending needs. The contingency fund should be estimated as a percentage of the annual operating spending budget or as a lump sum amount that is based on certain trends or historical utilization of such fund.
- e) Develop and implement strategies to diversify revenue streams, including increasing online course offerings, establishing continuing education programs, and seeking new grant opportunities.
- f) Enhance fundraising efforts through targeted campaigns, alumni engagement, and corporate partnerships.
- g) Develop long-term financial plans that align with the University's strategic goals.

- h) Maintain positive cash flows with excess free cash flows to support all expansion projects and maintain the extra funds into short term/ low risk bank deposits, thus providing stable and sustainable source of funding to easily satisfy all short- and long-term operational spending requirements.
- i) Conduct in-depth planning and financial feasibility prior to launching any new academic program or investing into other expansion projects.
- j) Utilize the budget reallocation techniques so that in case allocated funds are insufficient to cover requested expenses, the respective unit should try to reallocate funds between different budget line items in the unit's own approved annual budget. This reflects reconsideration of priorities that might lead to postponing some less important planned activities in order to satisfy some other more demanding requirements.
- k) Consider additional budget allocations, unless it's possible to transfer between the budget line items of a specific unit or to cover the shortage from the contingency fund. Additional budget allocations can be requested, while clearly stating the reasons for such additions. Such additional budget allocations can be approved by the Office of Budget and Planning in case the requested expenses will generate additional revenue which is not budgeted for (i.e. event or activity). In case the additional expense does not result in generating additional revenue, then the request shall be approved by the Board of Trustees.
- l) Provide ongoing budget training for staff members involved in the budget process to ensure they are skilled in the latest tools and techniques.

1.3.9. Compliance Risk

The following steps can be taken to mitigate the compliance risk:

- a) Provide a continuing learning and professional development opportunities to the team directly involved in VAT and GPSSA filing, financial reporting and all related rules, regulations and standards.
- b) Adoption of proper system setup, automated processes and other internal control measures to ensure accurate calculations and reporting along with review and validation practices.
- c) Conduct regular awareness sessions for other users from Office of Finance and other units.
- d) Conduct regular consultancy and health check sessions by specialized consultants to ensure that all processes and reports are fully compliant with applicable regulations and financial reporting standards.
- e) Participation in related workshops, conferences and seminars and maintaining viable relationships with contacts from other peer institutions within the higher education sector.

1.3.10. Human Resources Risk

The following steps will be implemented to mitigate the risks associated with human resources:

Compliance Risk:

- a) Maintain up-to-date knowledge of Human Resources related laws such as UAE labor law, general pension and social securities regulations.
- b) Provide ongoing compliance training and professional development programs to familiarize staff members about applicable laws and regulations.

Talent Loss and Attrition Risk:

- a) Conduct regular staff satisfaction surveys to obtain staff feedback on different business-related matters, to identify areas for improvement.
- b) Implement comprehensive talent management programs such as succession planning, career and professional development programs, employee engagement, rewards and recognition.
- c) Provision of sufficient budget to enable conducting professional development and training programs as well as other employee engagement programs to retain talent.
- d) Prioritize employee health and safety by offering comprehensive health insurance coverage for employees and eligible dependents.
- e) Develop and execute targeted recruitment and employer branding initiatives to attract qualified talent to AU.

Performance Management Risk:

- f) Set clear objectives for staff members along with expected level of skills and competencies, and conduct regular performance appraisal to identify the achievement of such objectives and the training needs that help them meet their performance targets.
- g) Maintain accurate and up-to-date job descriptions that suit evolving business needs.
- h) Benchmark compensation to the pay scales of peer institutions.

Business Change Risk:

- i) Conduct regular industry benchmarking to identify best practices.
- j) Provide change management training to equip employees for organizational shifts.

1.3.11. Procurement Risk

The following steps shall be adopted to mitigate the risks associated with the procurement function:

- a) Conduct continuous assessment and review of procurement procedures.
- b) Gather feedback from end users on the quality of products and services, as well as the commitment of suppliers and contractors.
- c) Conduct regular surveys for suppliers to obtain their feedback about the procurement cycle and how it can be improved.
- d) Identify key suppliers of frequently needed products and services and enter into supply agreements with them to ensure continued availability of such supplies within an affordable timeframe.
- e) Maintain proper communication channels with end users to be aware of their operating plans and be able to satisfy their requirements on time.
- f) Provide continuous training and awareness sessions for Office of Procurement staff members.

■ Information Technology Risk Management

1.4. Purpose

This section identifies the different sources of information technology risks that the University is exposed to. These risks should be properly managed in order to avoid any negative consequences such as data loss or major system failure. Several control measures are regularly conducted to identify each risk source, its significance, evaluation methods, and the adoption of optimal options to mitigate it. A major damage or failure in any of the following I.T. infrastructure or services may cause a serious disruption of operations and thus represent key risk component.

1.5. IT Risk Identification

Some risks are involved in the management of information resources, operations of systems, networks, equipment, applications and other information technology functions and processes. These risks include the following:

1.5.1. Servers and Storage:

Hardware failure in a server may cause a failure in one of the core services; such as registration or finance applications.

1.5.2. Network Appliances:

Any failure or damage to some of the network appliances may imply complete or partial outage of critical services.

1.5.3. LAN, WAN, and Internet Connections:

A disruption in any of these connections may cause outage in all web services, thus interrupting the smooth running of several academic and support services.

1.6. IT Risk Component Analysis

Information Resources and the processes of using them represent vital part of University's mission, goals and objectives. The following part analyzes and describes the risks involved in managing information resources in more detail.

1.6.1. Threats and Vulnerabilities:

Threats can be both internal and external, and come in many different forms. The common element is that they work against the confidentiality, integrity, and availability of information resources. Some of the possible threats would be the alteration of data, systems, processes or release of protected information. Others can be hackers or viruses. Vulnerabilities are weaknesses or holes in information resources and processes that may cause unauthorized or unintentional change or manipulation of resources, which can affect the confidentiality, integrity, and availability of these resources. Vulnerabilities and overall impact for every information resource must be identified and evaluated and

re-evaluated on a regular basis to ensure these ongoing risks are properly managed and appropriate controls are in place.

1.6.2. Data Loss:

Data loss can occur on any device that stores data due to one of the following:

- a) Human error, accidental data deletion, modification or overwrite.
- b) File corruption, software error or virus infection.
- c) Hardware related issues; drive failure, controller or CPU failure.
- d) Site-related theft, fire, force majeure such as floods, earthquake, lightning, etc.

1.6.3. Unplanned Service Outage:

Unplanned Service Outage may occur due to one of the following:

- a) Hardware failure such as damage in server or LAN/WAN equipment.
- b) Software problem may cause failure in I.T. service/s.

1.7. IT Risk Evaluation and Prioritization

The following describe how different risks are evaluated and prioritized.

1.7.1. Threats and Vulnerabilities:

Threats and vulnerabilities are evaluated by identifying the probability, nature and extent to which confidential information can be exposed, such as student records or exam questions.

1.7.2. Data Loss:

This risk is evaluated by reviewing the type and size of data that can be lost as well as the potential negative consequences of that on operating activities.

1.7.3. Unplanned Service Outage:

This risk is evaluated by the time, period, and consequences of the service outage on different functional activities.

1.8. IT Risk Mitigation Methodology

The following describe the risk management methodology for each risk source. The Office of IT adopts the following solutions to mitigate the risks, as follows:

1.8.1. Threats and Vulnerabilities:

The Office of IT is reducing this type of risks by installing the antivirus software on all computer devices, including PC's, laptops and servers; keeping all such devices updated, and using the Firewall to isolate the servers in a healthy and protected environment

1.8.2. Data Loss:

The Office of IT has set a backup policy to protect the critical data by recovering them in case of loss (see backup policy). A disaster recovery site is used to provide high availability of the critical data and services. Furthermore, the recovery tools are used, in case needed, for individual loss of data.

1.8.3. Unplanned Service Outage:

The Office of IT is committed to ensure continuous and uninterrupted availability of all services as follows:

- a) Uninterruptible Power Supply (UPSs) and Power Generator connectivity for the most critical LAN/WAN connections and servers, which helps in avoiding the potential disruption due to power shortage.
- b) Hardware and software support agreements are maintained to provide 24X7 support services for the most critical equipment and services.
- c) The I.T. has transferred all critical services to virtual environment, which reduces the time of service recovery and increases the high availability.
- d) Backup devices and servers are provided.

1.9. IT Risk Plan Maintenance

The following part describes the different methods adopted by the Office of IT for maintaining or updating the risk plan.

1.9.1. Threats and Vulnerabilities:

Following up on the Antivirus, updating servers and monitoring them.

1.9.2. Data Loss:

Applying the Backup Policy and ensuring that the taken backups are healthy.

1.9.3. Unplanned Service Outage:

Monitoring all LAN and WAN equipment, UPS's and servers, ensuring that all equipment are functioning in a perfect manner, and maintaining all IT equipment and services under external support agreement to increase the level of high availability.

■ Facilities Risk Management

1.10. Purpose

This section identifies the different sources of risks that AU facilities and infrastructure are exposed to, that should be properly managed in order to avoid and/or mitigate any potential negative impact. This is done throughout identifying each risk source, its significance, relevant evaluation methods and the adoption of best risk mitigation options. The purpose is to outline structured methodologies that are adopted to minimize the negative consequences of future damage to AU facilities and infrastructure, and the subsequent disruption in University's operations and services.

1.11. Facilities Risk Identification

1.11.1. Technical Faults and Breakdowns:

Any equipment malfunctions or system failures that can have a direct impact on the University's operations and continuity of key services.

1.11.2. Fire:

In the event of a fire outbreak, it becomes crucial that the fire safety system and processes are instantly activated to contain the spread and thus minimize the impact and loss.

1.11.3. Utility Outages:

Electricity and water shortages can significantly disrupt the functioning of the University's various colleges, offices and other common facilities.

1.11.4. Structural Incidents:

Any structural collapse or failure in any of the University's infrastructure can have disastrous consequences.

1.11.5. Emergencies:

Any emergency such as but not limited to natural disasters (earthquake, flooding, etc.) is beyond human control and can affect AU facilities and infrastructures critically.

1.11.6. Safety and Security:

Considering the large number of students, faculty, staff and visitors attending on campus buildings and facilities, undesired situations, incidents, disturbance and violence that can erupt in the University could jeopardize the safety and security of the occupants, facilities and infrastructure.

1.11.7. Traffic Accidents:

Any traffic accident that can occur on campus grounds involving drivers, pedestrians, or vehicles.

1.11.8. Insufficient Parking Areas:

Any shortage of parking slots on campus that might cause traffic congestion and impact campus accessibility.

1.11.9. Non-compliance with Regulatory Authorities:

Failure to adhere to relevant laws, codes, or standards.

1.12. Facilities Risk Component Analysis**1.12.1. Technical Faults and Breakdowns:**

AU facilities and infrastructure should remain in perfect functional state for efficient, reliable and normal operations at all times. This requires prompt and effective repair services and periodic preventive maintenance to be carried out to minimize or prevent facilities down time or closure.

1.12.2. Fire:

Fire is an unpredictable and inherent risk in University's environment, and carries a high damage potential. The existing facilities and infrastructure possess the necessary fire safety mechanisms and processes.

1.12.3. Utility Outages:

Uninterrupted power and water supply for AU facilities is essential and of paramount importance for its functioning and operations. These basic utilities within the Emirate of Ajman are supplied by a federal government authority, and mostly seem to be stable, sustained and reliable.

1.12.4. Structural Incidents:

A safe, stable and reliable condition of the building facilities and infrastructure, which meets the relevant and required standards is a primary requirement for any educational institution. The existing infrastructure appears to be in fair and stable condition. Maintenance and repairs are undertaken regularly and when needed by an external specialized contractor.

1.12.5. Emergencies:

It is imperative that a clear, effective and tested evacuation plan is compiled, and is circulated and posted for the facility's occupants in order to be well prepared for any such emergency incidents.

1.12.6. Safety & Security:

It is of utmost importance that AU facilities and infrastructure are safe and secure at all times for the protection and comfort of all faculty, staff, students, and visitors. AU facilities possess security systems and personnel for overseeing internal safety and security.

1.12.7. Traffic Accidents:

Campus traffic accidents pose significant risks, including physical injury, property damage, operational disruptions, and financial loss. These incidents can harm individuals, damage property, disrupt campus

activities, and negatively impact the University's reputation.

1.12.8. Insufficient Parking Areas:

The shortage in parking spaces can lead to traffic congestion, increased commute times, frustration among students, faculty, and staff members, and potentially decreased attendance or productivity. Additionally, it may contribute to accidents as drivers search for parking spaces, increasing the risk of damage to vehicles and property.

1.12.9. Non-compliance with Regulatory Authorities:

This can result in severe financial penalties, legal repercussions, and reputational damage. It can also lead to operational disruptions, loss of licenses or permits, and in extreme cases, business closure. Furthermore, it can erode public trust and hinder the organization's ability to operate effectively.

1.13. Facilities Risk Evaluation and Mitigation Methodology

1.13.1. Technical Faults and Breakdowns:

This risk potential is regularly evaluated by monitoring the frequency of reported faults and breakdowns; periodic assessments of AU's facilities and infrastructure; amount of resources and personnel needed for carrying out maintenance and repairs shall be conducted. The University mitigates this risk by conducting regular inspection of all AU facilities and infrastructures; scheduling and conducting preventive maintenance of key areas of AU's facilities and infrastructure; keeping inventory of vital spare parts and backup equipment to minimize facilities downtime; ensuring the availability of sufficient maintenance personnel for immediate action and resolution at the earliest; conducting regular training for maintenance personnel to ensure prompt and effective responses to potential technical issues.

1.13.2. Fire:

Periodic review and assessment of the fire safety mechanisms, equipment and processes within AU's facilities and infrastructure; as well as the history of fire incidents represent key indicators of exposure to such risk. This is mitigated throughout the continuous evaluation and identification of potential fire hazards; inspection of the status and condition of the fire safety systems, mechanism, equipment and processes across all AU facilities and infrastructures, in addition to scheduling and conducting preventive maintenance of fire safety systems, mechanisms and equipment; compiling fire safety manual, evacuation plan and spreading awareness; conducting fire safety and evacuation drills; conducting regular training and awareness sessions for community members, including students, faculty and staff members, assigning fire marshals who can help in any potential fire emergency, and establishing communication channels and information exchange with civil defense authorities, hospitals and other relevant authorities; in addition to putting in place loss/damage insurance policy.

1.13.3. Utility Outages:

Periodic assessments of utility infrastructure of AU's facilities; communication and information exchange with the utility provider; history of utility incidents within AU's facilities represent fundamental component to enable maintaining a proper plan to control such risks. This risk is mitigated throughout the continuous evaluation of the status and condition of the utility networks across AU facilities and infrastructure; communication and regular information exchange with the utility service providers for prioritized supply restoration to AU's facilities, scheduling and conducting preventive maintenance of key utility infrastructure of AU's facilities, and backup supply provision arrangements.

1.13.4. Structural Incidents:

Regular evaluation of the status and condition of the structural reliability of AU facilities and infrastructure is conducted to ensure the maximum safety of all AU's structures, in addition to scheduling and conducting preventive maintenance of key areas of facilities and infrastructures; communication and information exchange with civil defense department, hospitals and other relevant authorities; as well as the availability of loss/ damage insurance policy.

1.13.5. Emergencies:

To best meet the requirements of controlling this type of risks, AU maintains sustainable communication and information exchange channels with relevant emergency management authorities and government bodies, in addition to maintaining comprehensive emergency plan and procedures covering all potential emergency situations and relevant responses which shall be published to all community members. Emergency Response Team (ERT) shall be assigned and trained regularly to be able to immediately respond during emergency situations. Spreading awareness among community members; conducting safety and evacuation drills; and ensuring the availability of public liability loss/ damage insurance policy serve as additional risk mitigation techniques.

1.13.6. Safety & Security:

The risks associated with safety and security systems are regularly evaluated in light of the capacity of facilities, the status of building machinery and equipment, as well as the analysis of the volume and demographics of people visiting AU facilities; to ensure the availability of all needed resources, tools, procedures and equipment, such as camera monitoring systems, sufficient security personnel, building evacuation plans, scheduled and implemented preventive maintenance of existing safety systems and equipment; effective management and control of the occupants of AU's facilities, and information exchange with relevant security authorities.

1.13.7. Traffic Accidents:

Mitigating traffic accident risk involves a comprehensive approach including infrastructure improvements, pedestrian safety measures, speed control, driver education, emergency response planning, vehicle maintenance, security personnel, promoting alternative transportation, and data-driven analysis to identify and address specific problem areas.

1.13.8. Insufficient Parking Areas

Mitigation of insufficient parking areas can be achieved through a combination of strategies including: optimizing parking space utilization, periodic review of parking usage patterns to identify peak times and high-demand areas, constructing additional parking slots, schedule shuttle service to transport students from external parking areas to the buildings, and encouraging alternative transportation modes such as public transport and carpooling.

1.13.9. Non-compliance with Regulatory Authorities:

Mitigation of non-compliance with regulatory authorities involves proactive measures such as: staying updated on regulatory changes, establishing a dedicated compliance team, conducting regular internal audits, implementing robust record-keeping systems, providing comprehensive employee training, fostering a culture of compliance, and maintaining open communication with regulatory bodies.

■ Environmental Health and Safety Risk Management

1.14. Purpose

This section outlines and identifies the different sources of risks that are related to environmental health and safety. Environmental Health and Safety Risk Management is a continuous process and a vital part of AU's processes. It shall be carried out for all activities of AU; including outsourced activities. Consultation with employees, contractors and stakeholders are conducted to ensure protection of health and safety measures at every stage of the health and safety risk management process.

The EHS risk assessment is an ongoing process and shall be undertaken at various times including:

- when planning or making a change to a work procedure and/or practice;
- when introducing new plant, equipment, materials or substances into the workplace;
- after an EHS incident (including near misses);
- introduction of new workers;
- presence of a high level of risk associated with a specific work activity (e.g. confined space);
- at regular or scheduled intervals as appropriate to the nature of the workplace and the hazards present;
- when legislative obligations change (including regulations).

Any condition with the potential to cause illness, injury or death shall be identified as a hazard and the records for the same shall be maintained in the Risk Assessment. Safety Review for clinics and labs shall be done on a regular basis by the assigned EHS Coordinator for each College.

1.15. EHS Risk Identification

The EHS Manager/ Officer in coordination with Environmental Health and Safety Committee shall conduct a comprehensive and ongoing review of the following factors to identify the different risks involved. The review and evaluation process shall include the actual and potential risks; routine and non-routine activities, such as on duty work activities, special assignments and student accommodations; facilities, machinery, equipment and material; activities of all personnel having access to campus facilities; including students, employees, parents, sub-contractors, suppliers, and visitors; human behavior; relevant legal and other requirements; facilities at the work place, whether provided by company or others; known hazards; such as hazardous material; normal, abnormal and emergency operating conditions; design of work areas; incident reports; and known near misses.

The comprehensive list of identified EHS risks will identify the list of people who can be harmed, what can be damaged and how, including employees; students; contractors; visitors; facilities/ equipment/ property damage; members of the public; and people of determination.

A standard list of all risk sources associated with Environmental Health and Safety shall be developed using the Standard Risk Register, and must be reviewed and amended on regular basis; at least 1 time during the academic year.

1.16. EHS Risk Component Analysis

1.16.1. Slip-trip-fall due to wet surfaces:

Slips, trips and falls can occur at the entry of a building, in the classrooms, in common areas, in labs/

clinics and even as you walk outside the building. More serious slips or trips together with the resulting falls may result in sprains or strains, broken bones when trying to break the fall, a back injury due to the sudden and forceful impact during a fall, burns if it occurs near hot surfaces or if the person is handling hot fluids, and cuts if it occurs near sharp objects.

1.16.2. Manual lifting of heavy/ bulky objects:

Manual handling injuries can have serious implications for the University and the person who has been injured. They can occur almost anywhere in the premises and heavy manual labor, awkward postures, repetitive movements of arms, legs and back or previous/existing injury can increase the risk.

1.16.3. Unsafe using of sharp tools and machinery:

The usage of sharp instruments and tools is essential to many kinds of work and practical study courses, but sharp or pointed objects can be hazardous and often cause painful injuries. Injuries include cuts, puncture wounds, nicks, and gashes that can lead to serious infections, cross contamination, or diseases.

1.16.4. Exposure to working in hot environment:

Exposure to extreme heat can result in occupational illnesses caused by heat stress, including heat stroke, heat exhaustion, heat cramps, heat rashes, or death.

1.16.5. Working at heights:

The safety risks of working at height are usually falling from height and dropping equipment from height. Consequences of working at heights can be catastrophic ranging from serious injury to fatality.

1.16.6. Noise from machinery, chillers and generators:

Long term exposure to high levels of noise can cause permanent hearing loss. Short term exposure to loud noise can also cause a temporary change in hearing or tinnitus.

1.16.7. Electrocution due to incorrect wiring/ from generators:

Electrical shock risk can be caused by many reasons such as inadequate wiring, exposed electrical parts, overhead powerlines, wires with bad insulation can give you a shock, electrical systems and tools that are not grounded or double-insulated, overloaded circuits, damaged power tools and equipment and more.

1.16.8. Greenhouse gas emission from AC:

The greenhouse gas effect from the usage of ACs can cause air pollution and increase the risk of global warming and ozone layer deterioration.

1.16.9. Disposal of chemical waste:

The improper disposal of chemical waste can pose a number of potential hazards both to the environment and to the safety of employees and students, such as explosion and/or sudden release of pressure (if a tank of compressed gas is punctured); reactivity (fire, explosion, or release of dangerous gases that can result from contact between particular chemicals, or from certain chemicals and air or water); health hazards (can result from over-exposure to a hazardous substance, ranging from minor effects like headaches and skin rashes to much more serious conditions such as skin burns, organ damage, allergic-type reactions, and even death); environmental/ community risks (when hazardous substances are spilled or released into water supplies or the air).

1.16.10. Waste of oil and AC coolant:

The improper disposal of oil and AC coolant resulting from maintenance activities pose a number of risks such as toxicity, flammability, asphyxiation, land contamination, and physical hazards.

1.16.11. Unsafe filling /storage of diesel:

Diesel spills are extremely dangerous since they release flammable vapors that expand into the atmosphere, and cause static electricity which is generated from the friction between dissimilar materials (e.g. the fuel and the metal fuel filler neck). When the static electricity discharges, it produces sparks which can ignite the fuel vapors.

1.16.12. Fire due to short circuits:

Improper maintenance/ lack of regular preventive maintenance of electrical equipment, wires, and machinery can lead to short circuits which may result in fires.

1.16.13. Excessive strain due to computer usage:

Prolonged usage of computers or laptops can have long term health risks on the employee or student such as back and neck pain, headaches, shoulder and arm pain, carpal tunnel syndrome, and vision related issues. Such problems can be caused or made worse by poor workstation design, bad posture and sitting for long periods of time.

1.16.14. Poor Hygiene:

Poor hygiene habits can leave community members and others exposed to germs, infections and infestation.

1.16.15. Unsafe walking on stairs:

Falls on stairs can result in severe injuries from head trauma to broken bones. The risk of falling while using the stairs is increased if there is no proper lighting in the area, no rail/ damaged rail, broken or chipped stairs.

1.16.16. Wastage of electricity:

Excessive usage of electricity can lead to a depletion in natural resources.

1.16.17. Wastage of paper:

Excessive usage of paper can lead to a depletion in natural resources.

1.16.18. Print Cartridge Disposal:

The improper disposal of ink cartridges and toner into normal waste may pose serious contamination to the environment from the dangerous substances that it can be exposed to through their disposal. More importantly, carbon black (toner) has been classified as carcinogenic by the International Agency for Research on Cancer and therefore needs to be correctly disposed of to ensure the safety of AU Community Members.

1.16.19. Contact with infected persons/ exposure to the communicable diseases within the university:

Exposure to communicable diseases may lead to infection, which can increase the risk of having adverse health problems and complications.

1.16.20. Management of confirmed cases of communicable diseases during a pandemic:

Lack of proper protocols for management of confirmed cases of communicable diseases during a pandemic and their direct/ indirect contacts may lead to the risk of increased cases on campus. Failure to follow MOE and MOH immediate isolation, contact tracing procedures increases the likelihood of exposure to the communicable disease as well as anxiety and dissent within the University community.

1.16.21. Use of Personal Protective Equipment (PPE) during a pandemic:

Incorrect use of PPE increases the risk of further infection.

1.16.22. Exposure to communicable diseases whilst using dedicated buses:

Lack of proper protocols for safety measures while using the university transportation may increase the risk of further infection.

1.16.23. Safeguarding and prevention of radicalization, extremism and violence on campus:

Safeguarding is the process of protecting vulnerable people, whether from crime, other forms of abuse or from being drawn into terrorism-related activity. Lack of protocols on safeguarding as well as training employees on these protocols may increase the risk of physical abuse and exploitation, neglect, emotional abuse, increased barriers to students reporting concerns to responsible adults, distress or anxiety related to health or welfare of family members or friends, risk of abuse or stigmatization on the basis of infection, race or nationality, and risk of peer on peer abuse. Lack of inadequate arrangements and resources in place to provide pastoral care and welfare support as required by the University may also increase the risk of violence on campus. Employees need to know what measures are available to prevent people from becoming drawn into terrorism and how to challenge the extremist ideology and understand how to support those who may need it.

1.16.24. Smoking on campus:

Smoking has adverse health effects on smokers and on non-smokers who are exposed to second-hand smoke. Smoking indoors or in non-designated smoking areas increase the risk of air pollution, second-hand smoke exposure, poor air quality, and fire.

1.17. Environmental Health and Safety Risk Monitoring

The EHS Committee shall undertake the role of conducting regular review and evaluation of risk incidents as applicable to EHS. The EHS Committee holds planned meetings at least 2 times during the academic year; to conduct the following tasks:

- Update the pre-defined risk register; by adding new risk sources, removing existing risk sources which are deemed discontinued/ irrelevant, or modifying the details of existing risk sources.
- Re-assess the different risk sources as pre-defined in the Risk Register, in terms of probability of occurrence or consequence scoring;
- Review the risk incidents during the past period;
- Ensure that the control measures in place are still relevant to control the risk;

- Discuss further controls as deemed necessary.

In addition to the planned/ regular meetings, unplanned meetings can be also held after certain situations giving rise to the need to review the risk assessments, which might include any of the following:

- Whenever key operational circumstances affecting the work environment change;
- After an incident where investigation identifies a major/ key risk source;
- After an inspection or audit report where additional key risks are identified;
- After an emergency situation;
- When new key processes or business activities are adopted.

1.18. EHS Risk Evaluation and Mitigation Methodology

1.18.1. Slip-trip-fall due to wet surfaces:

These risks can be mitigated by following good housekeeping practices, ensuring that work areas are kept tidy, no trailing cables or obstruction in walkways, and using appropriate caution and safety signs around wet floors.

1.18.2. Manual lifting of heavy/ bulky objects:

Manual handling risks can be mitigated by using a trolley to transport heavy items, providing training in lifting techniques for anyone who undertakes the lifting of heavy loads, and proper usage of safety shoes.

1.18.3. Unsafe using of sharp tools and machinery:

These risks can be mitigated by allowing only trained employees/ students to use sharp tools and instruments, by guarding all dangerous parts of machinery as per manufacturers' standards. Machinery guards need to be inspected every month and maintained in good condition. All new machinery needs to be checked before first use. Employees and students must use appropriate PPEs while using sharp tools and machinery.

1.18.4. Exposure to working in hot environment:

Exposure to extreme heat risk can be avoided by using appropriate uniforms/ jackets if necessary, doing periodic occupational health check, and restricting work during peak hours of the day.

1.18.5. Working at heights:

The safety risks of working at height can be mitigated by assessing and listing all contractor jobs involving work at height and planning a safe system of work before initiation of job, proper storage of access equipment (i.e. ladders, tower scaffold) in staff's workshop and proper inspection before use, and training staff members to use ladders and tower scaffolds safely.

1.18.6. Noise from machinery, chillers and generators:

These risks can be mitigated by regular preventive maintenance of machinery such as drills, angle grinders, electrical saws to ensure they run as quietly as possible, and usage of ear defenders/ protection.

1.18.7. Electrocution due to incorrect wiring/ from generators:

Electrical shock risk can be mitigated by performing preventive maintenance to electrical cables and

sockets and generators, immediate attention and isolation of damaged wires and sockets, checking earth resistance, applying warning signs, and the use of appropriate PPEs.

1.18.8. Greenhouse gas emission from AC:

The greenhouse gas effect risk can be mitigated by using climate-friendly refrigerants, training and certification of technicians, and proper disposal of refrigerants or AC coolants.

1.18.9. Disposal of chemical waste:

The improper disposal of chemical waste risk can be mitigated by applying a proper waste management plan to include hazardous waste and dispose chemical containers through approved waste transporter. A quarantine area to segregate expired chemical waste need to be identified and used.

1.18.10. Waste of oil and AC coolant:

The improper disposal of oil and AC coolant risk can be mitigated by applying a proper waste management plan to include hazardous waste and dispose oil, batteries and coolants through approved waste transporter/ garage.

1.18.11. Unsafe filling /storage of diesel:

Diesel related risks can be mitigated by securing the filling stations, ensure the availability of appropriate firefighting equipment near the generators, performing routine maintenance to prevent leakages, and providing awareness sessions to employees for fire prevention and safety.

1.18.12. Fire due to short circuits:

This risk can be mitigated by regular preventive maintenance of electrical equipment, wires, and machinery, checking power sockets for any possible damage, having an adequate number of fire extinguishers/ fire hose reels, installation of smoke detectors and sprinkler system, testing firefighting system and equipment every 6 months, providing awareness sessions and training to employees and students on emergency preparedness in case of fire, setting evacuation maps, and ensuring that exits are maintained available, unobstructed, and unlocked at all times.

1.18.13. Excessive strain due to computer usage:

This risk can be mitigated by scheduling regular breaks, keeping appropriate distance from monitors, and working in a good lighting condition.

1.18.14. Poor hygiene:

This risk can be mitigated by maintaining daily hygiene checkup and keep wash rooms and common areas clean.

1.18.15. Unsafe walking on stairs:

Falls on stairs risk can be mitigated by ensuring that the surface of steps is rough to prevent slipping, proper usage of safety and warning signs, adequate lighting in stairway, and provision of solid well-maintained rails or fall barriers.

1.18.16. Wastage of electricity:

This risk can be mitigated by applying a power saving plan, reducing the usage of power where applicable, closing lights after office hours, shutting down machines when not in use, and exploration and application of alternative energy sources like solar panels, LED lights, and others.

1.18.17. Wastage of paper:

This risk can be mitigated by applying a waste management plan to include paper waste and recycling through approved waste transporter, reducing printing and using e-copies, and gradual full adoption of going-green policy with zero paper waste.

1.18.18. Print Cartridge Disposal:

This risk can be mitigated by applying waste management plan to include toner waste and recycling through approved waste transporter, reducing printing by using e-copies to share documents and information, and gradual full adoption of going-green policy with zero paper waste.

1.18.19. Contact with infected persons/ exposure to communicable diseases within the university:

This risk can be mitigated by communicating and enforcing the application of communicable diseases' protocols and safety measures to AU community members.

1.18.20. Management of confirmed cases of communicable diseases during a pandemic:

This risk can be mitigated by developing a protocol for dealing with positive cases and close contacts in the community with clear division of responsibilities.

1.18.21. Use of Personal Protective Equipment (PPE) during a pandemic:

This risk can be mitigated by enforcing strict measures for usage of PPEs to prevent the spread of communicable diseases during a pandemic, and communicating the measures to all stakeholders. Disciplinary measures are enforced for violators.

1.18.22. Exposure to communicable diseases whilst using dedicated buses:

This risk can be mitigated by reducing the capacity of buses, proper usage of PPEs while on the bus, applying social distancing, and giving awareness sessions/ training to the bus drivers on communicable diseases' awareness and precautionary measures.

1.18.23. Safeguarding and prevention of radicalization, extremism and violence on campus:

Safeguarding risks can be mitigated by implementing proper protocols on safeguarding as well as training employees on these protocols, providing the necessary arrangements and resources to provide pastoral care and welfare support, developing clear policies for students and employees using IT equipment to research terrorism and counter terrorism in the course of their learning/ working process, preventing unauthorized access to campus by Access Control protocols, usage of barriers at all entry/exits, and requiring visitors to wear visitor badge.

1.18.24. Smoking on campus:

Smoking risks can be mitigated by developing and enforcing a smoking policy, communicating the policy with all Community members, assigning designated smoking areas on campus and applying disciplinary measures for violators.

Document History

Version	Date	Update Information	Author/ Reviewer
V 1.0	24/10/2010	Policy to identify different sources of financial risk	Financial Controller
V 1.1	10/03/2013	Amendment to policy to include other sources of risk such: IT services risk, Building facilities risk, and internship risk	Financial Controller
V 2.0	19/10/2017	New policy - Major changes and incorporation of Academic Risk and Teach-out Risk	Chief Operating Officer

V 3.0	01/07/2021	Major Changes - The policy has been updated and restructured to reflect only the operational risks. The academic-related risks are now incorporated in the Teach-out Policy.	Chief Operating Officer
V 4.0	01/07/2021	The policy has been updated for additional risks in the following areas: Finance, Budget, Human Resources and Facilities.	Chief Operating Officer
V 5.0	22/10/2025	The policy has been updated for additional risks/ mitigation measures in the following areas: Finance, Budget, Human Resources and Facilities.	Vice-Chancellor for Financial and Administrative Affairs