



The American University of Kurdistan

Policy of Enterprise Risk Management

Policy Number: BF013

Effective Date: June 1, 2025

CONTENT

- I. Introduction
- II. Roles and Responsibilities
- III. Definitions
- IV. Policy
- V. Procedures
- VI. Policy History

I. INTRODUCTION

- a. **Authority:** The Board of Trustees (herein referred to as “Board”) at The American University of Kurdistan (herein referred to as “AUK” or “University”) is authorized to establish rules and regulations to govern and operate the University and its programs.
- b. **Purpose:** This document outlines a systematic process for identifying, managing and monitoring uncertainties that is aimed at managing adverse effects on the University achieving its objectives, while realizing and maximizing the opportunities it provides. This ensures a standard approach to risk management and allows risks to be correctly prioritized across all of the University’s operations, which in turns means that effective controls can be put in place to ensure the University is able to manage its operations effectively now and into the future.
- c. **Scope:** This document applies to all University stakeholders.

II. ROLES AND RESPONSIBILITIES

- a. Responsible Executive: GARC
- b. Responsible Administrator: VPAF
- c. Responsible Office: Office of VPAF
- d. Policy Contact: VPAF

III. DEFINITIONS

- *Current Risk*: The level of risk after considering the controls, actions, and risk mitigation measures already implemented to reduce either the risk's likelihood or impact.
- *Enterprise Risk Management Framework*: The totality of systems, structures, policies, processes, and people that identify, measure, monitor, and mitigate risks associated with opportunities and adverse events within the University environment.
- *Inherent Risk*: Risk in the absence of any controls, actions, or risk mitigation to alter either the risk's likelihood or impact.
- *Residual Risk*: The remaining level of risk after considering controls, actions, and risk mitigation measures implemented or planned to reduce either the risk's likelihood or impact.
- *Risk*: Any event or action that may adversely affect the University's ability to achieve its strategic and operational priorities.
- *Risk Appetite*: The level of risk the University is willing to accept to meet its strategic objectives. It conveys the degree of risk the University is prepared to accept in pursuit of its objectives and strategic plan.
- *Risk Assessment*: The process is used to determine risk management priorities by evaluating and comparing the level of risk associated with an activity against predetermined tolerances or generally acceptable levels of risk, formulated in consultation with key stakeholders.
- *Risk Management*: A planned and systematic approach to identifying, evaluating, and controlling risk to maximize opportunities and minimize losses.
- *Risk Management Process*: The systematic application of risk management policies, procedures, and practices to the activities of identifying, analyzing, assessing, evaluating, treating, monitoring, and communicating risk.
- *Risk Profile*: A representation of a set of risks according to their likelihood and consequence, used to promote discussion and prioritize actions or responses to risk.
- *Risk Register*: A register of locally identified risks established and maintained by a college, unit, or external stakeholder for their operations, including projects, commercial activity, new opportunities, and changes to existing products or processes.
- *Risk Tolerance*: The willingness to accept or reject a given level of residual risk aligned with the overall risk appetite.
- *Risk Treatment*: The process of selecting and implementing measures to manage risk exposure through avoidance, reduction, transfer/sharing, or acceptance.

IV. POLICY

Purpose

The purpose of this policy is to establish a structured and systematic approach to enterprise risk management at the AUK, ensuring that risks are proactively identified, assessed, and managed in alignment with the university's mission and strategic objectives. This policy provides a framework for integrating risk management into decision-making, enhancing institutional resilience, and safeguarding the university's people, assets, and reputation.

Objectives

The objectives of this policy are to:

- Foster a strong risk-aware culture where stakeholders at all levels take active responsibility for identifying, assessing, and managing risks while maintaining agility and innovation in realizing opportunities.
- Enhance strategic planning by identifying potential threats and uncertainties that may impact the university's mission and long-term sustainability.
- Establish a consistent and systematic approach to risk management across all university functions.
- Promote a proactive risk management approach, ensuring risks that may impact the university's strategic and operational objectives are identified and mitigated in a timely manner.
- Assist in safeguarding the University's assets – people, finance, property and reputation.
- Support informed decision-making by integrating structured risk management methods into governance, resource allocation, and operational planning.

Principles

- The University adopts risk management principles and processes in accordance with the International Standard of Risk Management: ISO 31000:2018, Risk Management – Guidelines.
- The University is committed to making risk management an integral part of the University processes and embedding risk management into the key decisions and approval processes of all major business processes and functions of the University.
- The University must embrace well-managed risk-taking in pursuit of its vision and strategic objectives.
- Risk is managed in accordance with the Enterprise Risk Management Policy and Procedures developed by the Vice-President for Administration and Finance (VPAF), and approved by the General Audit and Risk Committee (GARC).
- The University will maintain and annually review its Risk Appetite Statements (RAS). The RAS will be approved by the GARC and defines the amount of risk the University is guidance on the management of risk within acceptable levels of tolerance.
- The University must provide a structure for:
 - Communicating, mitigating and escalating major risk issues.
 - Incorporating risk management principles and objectives into strategic and operational activities and processes.
- The University must:
 - Establish risk registers.
 - Evaluate its existing risk management processes and practices, evaluate any gaps and address those gaps in its revision of the Enterprise Risk Management Policies and Procedures.

- Have an ongoing program of risk assessment across the University including risk assessment associated with new opportunities.
- Have a continuous monitoring and review process over the implementation of the ERM Policy and Procedures.
- Assess maturity of the Risk Management practices across the University.

V. ROLES AND RESPONSIBILITIES

The University utilizes three lines of defense governance model to manage its Risks and identify those individuals or functions responsible for Risk ownership, Risk oversight and Risk assurance. The VPAF, the ERMC, along with the GARC, provide oversight and support to the Risk Management Process and the three lines of defense.

Governance:

General Audit and Risk Committee: The GARC is responsible for support and oversight of the implementation of the ERM process, including approval of the Risk appetite and assessment of the Risk program against the Risk appetite.

First Line of Defense – Risk Owners:

- All University employees have a role in the effective management of Risk within the context of their area responsibilities, including the identification and disclosure of potential or emerging Risks.
- Academic college deans and administrative unit heads are responsible for implementing good operational Risk management practices, foster a culture of risk awareness, report risk exposure and significant incidents to the ERMC, and maintain and oversee appropriate internal controls that support the effective management of Risk. Effective Risk management requires timely recognition and disclosure of potential Risks and should be incorporated into planning processes and management activities.

Second Line of Defense – Risk Oversight:

- The ERMC responsibilities consist of:
 - Maintaining oversight of AUK’s Risk Register and ensuring the effective implementation of the risk management plan.
 - Promoting a strong risk-aware culture across the university, ensuring that risk considerations are embedded in decision-making.
 - Assisting with defining risk management practices
 - Ensuring that risk management activities within the first line of defense are adequately resourced to facilitate effective risk identification, assessment, and mitigation.
- The VPAF: Serves as the Chief Risk Officer for the University and has specific accountability for the coordination and implementation of the Enterprise Risk Management activities, procedures and reporting. The VPAF will report to the GARC at least once annually on the execution of ERM activity at the University.

Third Line of Defense – Risk Assurance:

The activities of the University's internal audit function provide assurance to management and the Board of Governors on the effectiveness of the risk management practices.

- *Internal Auditor:* The internal audit function at the University will provide independent review and assurance of the effectiveness of the risk management framework and present audit findings and recommendations to the GARC.

External Assurance: The external auditors offer a critical check on the university's systems, ensuring the overall risk management framework remains robust, and provide objective recommendations to enhance governance, strengthen internal controls, and improve overall risk management practices.

VI. PROCEDURES

The Risk Management Process

AUK is committed to fostering a proactive risk management culture that supports informed decision-making while ensuring the university's strategic objectives are met. The university adopts a balanced approach to risk-taking, recognizing that some risks are necessary for growth and innovation, while others must be minimized to protect its financial stability, reputation, and compliance obligations.

The risk management process should be an integral part of management and decision making and integrated into the structure, operations and processes of the University. It can be applied at strategic, operational, program, or project levels. The risk management process includes communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

1. Communication and Consultation

Communication and consultation with appropriate external and internal stakeholders will take place within and throughout all steps of the risk management process.

2. Establishing the Context

- Prior to undertaking the risk assessment process, the University needs to establish the context, and will account external and internal factors that could influence the achievement of objectives.
 - Clarify the scope and purpose of the risk assessment activity.
 - Define the internal and external parameters to be considered when managing risk.
 - Identify the relevant stakeholders to communicate and consult with.
- Internal context may include, but is not limited to:
 - The University's strategy, objectives, and values.
 - Considering AUK's governance, structure, roles and accountabilities.

- Considering the available resources and capabilities.
- Understanding the University's Risk Appetite Statement.
- The external context is the environment in which AUK operates and the impact of this on achievement of AUK's objectives, including:
 - Key legislations, rules and compliance requirements
 - Social, cultural, environmental, legal, political, technological, economic and market conditions.

3. *Risk Assessment*

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. The AUK risk assessment process is designed to identify and assess a wide variety of potential risks upon which University officials may wish to focus attention. It should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders.

- The Risk assessment process starts with the risk identification. The ERMC meets on a quarterly basis, or more often as needed to find, recognize, describe risks that might help or prevent the University achieving its objectives irrespective if the sources of the risk are outside the control of the University.
- Risk Identification: Risks identified must be documented in a risk register and include a risk description that captures:
 - The source and description of risk.
 - The risk owner (s) and areas affected.
 - Causes that may result in the risk event occurring.
 - Potential consequences for the University should this risk event occur.
- Risk analysis involves the following:
 - A consideration of uncertainties, risk sources, consequences, likelihood of events and scenarios, controls and their effectiveness given that a risk event can have multiple causes and consequences.
 - Measuring the likelihood and Impact of the risk, and converting these factors into a risk score.
 - Identifying the current controls in place.
- Risk Evaluation: Risk Evaluation involves comparing the level of risk found during the risk analysis with the University's risk appetite or acceptable risk levels determined by risk owners to determine whether the risk or its magnitude are acceptable or tolerable to the University.
 - The current risk is first assessed and compared to the risk appetite to determine whether the risk level is acceptable. If the current risk exceeds the acceptable threshold defined by the risk appetite, mitigation controls are implemented to reduce the risk exposure. Once the controls are in place, the residual risk — which represents the remaining risk after mitigation measures — is re-assessed.
 - Reflecting on the residual risk rating, and the adequacy of controls to address the risk within the University's Risk Appetite, determines if additional actions are required. If the tolerable risk rating and the residual

risk ratings are the same then no further action is required. However, if the residual risk rating has a higher rating than the tolerable risk rating then the residual risk will need to be reduced through implementing a treatment plan/s.

- The acceptance of risks lying outside the Risk Appetite Statement is subject to GARC approval. This may be the case, when, for example:
 - There are no appropriate risk treatment actions available.
 - The cost of the treatment outweighs the benefit.
 - The benefits and opportunities outweigh the potential consequences of the risk.
 - The risk is being taken to pursue an opportunity in line with the University's strategy and objectives.

4. Risk Treatment

Risk treatment involves developing a range of options for mitigating the risk, assessing those options, and then preparing and implementing action plans.

- When identifying the most appropriate treatment, it is important to consider the following principles:
 - Identify and assess a range of treatment actions before selecting one or more of these options to be implemented.
 - A cost/benefit analysis may be useful in determining the most appropriate risk treatment action.
 - Treating a risk may have implications elsewhere and impact on other activities. Consequential impacts, correlations and dependencies should also be considered to ensure that in managing one risk, an unacceptable situation is not created elsewhere.
- Once a risk treatment action is identified, it should outline as:
 - Risk treatment to be implemented
 - There are different strategies for risk treatment to be implemented. Based on the risk and the risk appetite, the following can be decided:
 - Avoidance: Avoid the risk by deciding not to start or continue the activity.
 - Reduction: Treat the risk by implementing mitigating actions and controls.
 - Retention/Acceptance: AUK may decide to accept the current risk level, if the costs associated with implementing mitigation measures outweigh the perceived benefits of treating the risk.
 - Sharing: Transfer of risk to a third-party. This could include purchasing an insurance policy, or outsourcing an activity.
 - Person responsible for implementation.
 - Timeframes for completion and resources required.
- Mitigation strategies
 - Introducing new processes, structures, and controls.

- Redesigning or enhancing existing processes, structures, and controls.
- Further monitoring of existing controls.

5. *Recording and Reporting*

Risk data are recorded in designated documents to ensure structured reporting and oversight. The following documentation is created and reported to the ERMC and the GARC:

- Risk Assessment Template: A standardized template used for evaluating risks across the university, ensuring a consistent approach to identifying, analyzing, and treating risks.
- Risk Register: The enterprise risk register documents the university's current exposure to risks. It includes key details such as risk descriptions, causes, consequences, controls, current and residual risk ratings, risk appetite, and treatment plans.
 - The VPAF is responsible for maintaining the university's Enterprise Risk Register, conducting periodic risk assessments with the support of the ERMC.
 - The members of the ERMC serve as risk owners for all key risks documented in the register.
 - Risk registers must be updated quarterly in preparation for ERMC meetings or as a response to an identified risk event requiring immediate escalation.
 - Risk owners must approve all risks recorded in the register and ensure they are regularly monitored and mitigated through strategic interventions.
- Risk Appetite Statement: A document defining the university's tolerance for risk across various functions and activities. It provides guidance on acceptable risk levels and ensures alignment with the university's strategic objectives. The statement is periodically reviewed and reported to the Board of Trustees.
- Risk Report: A comprehensive report containing: The updated risk register, risk trends and key emerging risks, risk mitigation updates and action plans, summary of risk events and escalations compliance with risk appetite and policy framework

The risk report is reviewed by the GARC, ensuring continuous oversight and governance of AUK's enterprise risk management framework.

6. *Monitoring and Review*

AUK will continuously monitor and conduct periodic reviews to ensure that risks remain well-managed, controls are effective, and mitigation strategies are aligned with the university's objectives. The key components of monitoring and review include:

- Ongoing Risk Monitoring: The ERMC continuously tracks and assesses risks for changes in likelihood or impact.
- Quarterly Risk Reviews: The Enterprise Risk Register is updated quarterly before ERMC meetings to ensure active risk management and documentation, evaluate key risks, and alignment with institutional priorities.
- Annual Risk Review: Annual risk reports are submitted to GARC for review, oversight and strategic alignment.

- Incident-Based Reviews: Major risk events (e.g., financial loss, cybersecurity breach, non-compliance) trigger immediate reviews, with findings reported to ERMC for corrective action.
- Audit Reviews: Internal Audit evaluates risk processes for adherence to best practices, while External Audit provides independent assurance on controls and compliance.

VII. POLICY HISTORY

- a. **Approved by:** Board of Trustees
- b. **Adopted:** June 1, 2025