جامعة المستقبل
Mustaqbal University
أول جامعة أهلية بمنطقة القصيم

Mustaqbal University
Risk Management Department Manual

Prepared by
The Risk Management Department

1st Edition
December 2025

Manual Identification Card

Manual Name	Risk Management Department Manual
Code	UOM-RISK-RMD-GUI-001-V1
Objective	Guiding the Risk Management Department and the other university departments regarding risk management matters
Owner	Risk Management Department
Reference(s)	The Regulations for Private Universities and Colleges, issued by the Council of University Affairs, Resolution No. (3/16/45) ISO 31000:2018 Risk Management COSO ERM Framework - Enterprise Risk Management ISO/IEC 27001 - Information Security ISO 22301 - Business Continuity
Scope	All the University's academic and administrative units
Approved by	The University Council
First Release	December 2025
Recent Review	Planned to be reviewed every 2 years
Current Edition	December 2025


بسم الله الرحمن الرحيم

Table of Contents

Chapter 1
General Framework

1.1 Introduction and Preface

1.1.1 A Word from the Director of Risk Management

In the name of ALAHA, the Most Gracious, the Most Merciful
I am pleased to present to you the Risk Management Guide for Mustaqbal University, which represents a significant step in the development of our corporate governance and management

system. Risk management is not merely an administrative tool, but a comprehensive philosophy aimed at achieving sustainability and excellence in a dynamic and complex educational environment. Given the increasing challenges facing the private higher education sector in the Kingdom of Saudi Arabia, the need for effective risk management is more urgent than ever.

The university leadership's commitment to implementing global best practices in risk management stems from our deep belief that sustainable success can only be achieved through well-considered strategic planning and proactive management of challenges and opportunities. This guide is the fruit of a dedicated collective effort, drawing inspiration from global best practices and adapting them to the local context and the unique characteristics of private university work. I anticipate that this guide will serve as an essential reference for all members of the university community on our journey towards excellence and leadership. The success of this project requires the combined efforts of everyone, and I am confident in our outstanding team's ability to translate these principles and procedures into practical realities that contribute to achieving the university's vision and mission.

Dr. Ali Mohammed Al-Habib Al-Lamouchi
Director of Risk Management

1.2 The Importance of Risk Management in Private Universities

1.2.1 The Unique Characteristics of Private Universities

Private universities in the Kingdom of Saudi Arabia possess unique characteristics that distinguish them from their public counterparts. These characteristics impose various challenges and risks that require specialized and sophisticated management:

• Reliance on Self-Revenue: Private universities rely primarily on tuition fees and educational services as their main source of income, making them more sensitive to fluctuations in student numbers and economic conditions.

• Administrative Flexibility: They enjoy greater flexibility in making administrative and academic decisions, but this flexibility comes with greater responsibility for managing the risks associated with these decisions.

• Intense Competition: They operate in a competitive environment with other public and private universities, requiring continuous excellence in quality and services.

• Susceptibility to Regulatory Changes: They are subject to regular changes in government regulations and bylaws, necessitating the ability to adapt quickly.

1.2.2 Financial and Operational Challenges

Private universities face unique challenges in financial and operational management:

• Cash flow management: The need for a delicate balance between revenues and expenses to ensure the continuity of operations.

• Infrastructure investment: The necessity of continuous investment in facilities and technology to maintain competitiveness.

• Human resource management: Attracting and retaining qualified faculty and staff in a competitive market.

• Fluctuations in demand: Being affected by changes in demand for different disciplines and student preferences.

1.2.3 The Importance of Financial Sustainability

Financial sustainability is the cornerstone of the success of any private university and requires:

• Diversification of income sources: Reducing reliance on a single source of revenue.

• Operational efficiency: Improving processes and reducing costs without compromising quality.

• Long-term planning: Developing financial strategies that ensure sustainable growth.

• Financial risk management: Identifying and managing risks that may affect the financial position.

1.2.4 Competition in the Higher Education Sector

The Kingdom of Saudi Arabia is witnessing rapid growth in the private higher education sector, creating a highly competitive environment that requires:

• Academic excellence: Offering distinguished academic programs that keep pace with the labor market.

• Quality of services: Providing high-quality student services. High-Quality Academic Performance

• Innovation and Development: Investing in modern technologies and innovative teaching methods

• Academic Reputation: Building and maintaining a strong academic reputation

1.2.5 Academic Accreditation Requirements

Obtaining and maintaining academic accreditation is one of the most important challenges facing private universities:

• Quality Standards: Adhering to rigorous standards of academic and service quality

• Continuous Improvement: Continuously developing programs and services

• Transparency and Accountability: Providing accurate and transparent data to regulatory bodies

• Periodic Review: Undergoing periodic reviews by accreditation bodies

1.2.6 Stakeholder Expectations

Private universities face increasing expectations from various stakeholders:

• Students: Expecting high-quality education, outstanding services, and high employment rates

• Parents: Seeking value for money in education

• Employers: Expecting qualified and prepared graduates for the job market

• Community: Contributing to local and economic development

• Regulatory Bodies: Adhering to regulations, rules, and standards

1.3 Guide Purpose and Scope of Application

1.3.1 Main Purpose

This guide aims to provide a comprehensive and systematic framework for risk management at Mustaqbal University, enabling all administrative levels to utilize it effectively. The academy understands and applies risk management principles and practices in a consistent and effective manner.

1.3.2 Strategic Objectives of the Guide

1. Unifying Concepts: Establishing a unified understanding of risk management terminology and concepts across the university.

2. Defining Roles and Responsibilities: Clarifying the roles and responsibilities of each level in the organizational structure.

3. Providing Practical Tools: Offering models and tools that can be directly applied.
4. Ensuring Compliance: Adhering to relevant local and international standards.
5. Fostering a Risk Culture: Raising awareness of the importance of risk management throughout the university.
6. Supporting Decision-Making: Providing decision-makers with accurate and reliable information.
7. Enhancing Institutional Performance: Contributing to the achievement of the university's strategic objectives.
8. Protecting Against Risks: Reducing exposure to risks and their negative impacts.
9. Seizing Opportunities: Identifying and capitalizing on opportunities for growth and development.
10. Ensuring Sustainability: Contributing to the financial and operational sustainability of the university.

1.3.3 Scope of Application

This guide applies to all sectors and activities of Mustaqbal University without exception, and includes:

Sector	Field	Activities Covered
Academic Affairs	Teaching and Learning	Academic programs, curriculum, assessment, quality assurance
Scientific Research	Research Activities	Research projects, scientific publication, research ethics
Financial Affairs	Financial Management	Budgets, investments, cash flow
Human Resources	Human Resources Management	Recruitment, training, performance, incentives
Information Technology	Technical Systems	Infrastructure, systems, information security
Student Affairs	Student Services	Admissions, registration, activities, advising
Facilities and Services	Infrastructure	Buildings, maintenance, security, safety
External Relations	Partnerships and Communications	Partnerships, media, community service

1.3.4 Target Categories

This guide is intended for all members of Mustaqbal University, and specifically includes:
• **University Council members**: to oversee risk management governance.
• **University President**: for strategic leadership in risk management.
• **Vice Presidents:** to implement policies within their respective areas of expertise.
• **Deans and Department Directors**: to implement risk management procedures.
• **Risk Coordinators**: to apply the guide in their units.
• **All staff members:** to actively participate in identifying and managing risks.
• **Faculty members**: to manage academic and research risks.

1.4 Terminology and Definitions

This section contains the basic definitions of the terms used in this guide, which are derived

from the international standards ISO 31000 and COSO ERM, as well as best practices in university risk management.

Terminology	Definition
(Risk Management)	Coordinated activities to guide and monitor the university about risks, including identifying, analyzing, evaluating, addressing, and monitoring risks.
(Risk)	The impact of uncertainty on goals can be positive (opportunity), negative (threat), or both.
(Opportunity)	The possibility of something positive happening could help achieve goals or improve performance.
(Threat)	The possibility of something negative happening that could hinder the achievement of goals or negatively affect performance.
(Risk Identification)	The process of finding, understanding, acknowledging, and describing risks.
(Risk Analysis)	The process of understanding the nature of risks and determining the level of risk
(Risk Assessment)	The overall process of identifying, analyzing, and evaluating risks.
(Likelihood)	The possibility of something happening, which can be defined qualitatively or quantitatively.
(Impact/Consequence)[1]	The result of an event that impacts the objectives, which can be positive or negative.
(Risk Level)	The magnitude of the risk or the set of risks, expressed as a combination of consequences and their probability of occurrence.
(Residual Risk)	The risks remaining after the application of remediation measures.
(Inherent Risk)	The risks before the application of any control measures.
(Risk Appetite)	The extent and nature of the risks the university is willing to accept to achieve its objectives.
(Risk Tolerance)	The maximum acceptable deviation from achieving defined objectives.
(Risk Treatment)	The process of modifying risks by avoiding, reducing, transferring, or accepting them.
(Risk Owner)	The person or entity with the responsibility and authority to manage a specific risk.
(Risk Register)	A record of information about identified risks and their management.
(Risk Map/Matrix)	A visual tool that displays risks categorized by probability and impact.
(KRIs) Main Risk Indicators	Metrics used to provide early warning of increased risk exposure.
Main performance	Quantitative measures for assessing the effectiveness of risk

(KPIs) Indicators	management activities.
(Risk Management Framework)	A set of components that provides the organizational foundations and arrangements for designing, implementing, monitoring, and improving risk management.
(Risk Management Process)	A method for analyzing risks using descriptions or classifications to characterize the magnitude and probability of potential consequences.
(Qualitative Risk Assessment)	A method for risk analysis using descriptions or classifications to describe the magnitude and probability of potential consequences.
(Quantitative Risk Assessment)	A method for risk analysis where numerical estimates of both consequences and probability are expressed.
(Internal Context)	The internal environment in which the university seeks to achieve its goals.
(External Context)	The external environment in which the university seeks to achieve its goals.
(Stakeholders)	Individuals or groups that could influence, be affected by, or feel affected by a decision or activity
(Controls)	Procedures implemented to reduce risk to an acceptable level
(Business Continuity)	The ability to maintain essential operations during and after events that adversely affect normal activities
(Contingency Plan)	A pre-prepared plan to respond to a potential future event or situation that could have a significant impact;
(Crisis Management)	
(Root Cause Analysis)	Implementation of strategies designed to help manage a sudden and significant adverse event;
(Business Impact Analysis)	A structured methodology for identifying the root causes of problems or events;
(RTO)	A process for identifying and assessing the potential impacts of business interruption on critical operations;
(RPO)	Maximum acceptable time period for data loss due to a destructive event
(Early Warning)	An indicator or signal that warns of a potential risk or problem
(Review)	An activity conducted to determine the suitability, adequacy, or effectiveness of a subject in achieving defined objectives

1.5 Regulatory and Legal Framework

1.5.1 National Regulations and Bylaws

i- The Regulations for Private Universities and Colleges

The Regulations for Private Universities and Colleges, issued by the Council of University Affairs, Resolution No. (3/16/45) dated 14/2/1445 AH, constitute the fundamental legal

framework governing the operation of private universities in the Kingdom. These regulations include several articles directly and indirectly related to risk management**.**

ii- Ministry of Education Regulations

The Ministry of Education issues numerous regulations and circulars that affect the operation of private universities, including:

Regulation/Circular	Topic	Impact on Risk Management
Admission and Registration Guidelines	Student admission procedures	Student Number and Revenue Risk Management
Academic Program Guidelines	Program opening requirements	Academic and Competitive Risk Management
E-Learning Guidelines	Distance learning organization	Technical and Academic Risk Management

iii- Education and Training Evaluation Commission Standards

The Commission's standards are an important framework for ensuring quality and managing academic risks:

• **Institutional Accreditation Standards**: These standards encompass governance, quality, and risk management.
• **Program Accreditation Standards**: Specific standards for each specialization.
• **E-Learning Standards**: Regulations specific to distance education.
• **Scientific Research Standards**: Ethics and research quality standards.

iv- Corporate Governance Systems

These include:
• Corporate System (concerning governance)

v- Financial and Administrative Systems

• Anti-Money Laundering and Counter-Terrorism Financing System
• Value Added Tax System
• Labor and Social Insurance System
• Personal Data Protection System

1.5.2 Adopted International Standards

i- Standard: ISO 31000:2018 Risk Management

ISO 31000: This is the leading international standard in risk management, providing general principles and guidelines for managing risks in all types of organizations.
Key Benefits:
• Provides a unified and globally recognized framework
• Applicable to all types of risks
• Supports informed decision-making
• Enhances stakeholder confidence

ii- COSO ERM Framework - Enterprise Risk Management

COSO Enterprise Risk Management is a comprehensive framework that links risk management with strategy and performance. Its key features include:
• Linking risk management to strategy
• Focusing on creating and protecting value

• Enhancing governance
• Supporting strategic decision-making

iii- ISO/IEC 27001 - Information Security

An international standard for Information Security Management Systems (ISMS), providing a systematic framework for managing risks related to information and data security.

iv- ISO 22301 - Business Continuity

An international standard for Business Continuity Management Systems (BCMS), helping to develop the university's ability to respond to incidents.

Chapter II
Risk Management Department Strategic Frame

2.1 Vision of Risk Management Department

“A nationally leading department in risk management to ensure the sustainability of excellence and the quality of future competencies.”

2.2 Mission of Risk Management Department

"Applying best practices for risk management to ensure the quality of education and professional development, the sustainability of university operations, and to promote innovation and partnership through transparency, accountability, and continuous improvement."

2.3 The Strategic Objectives of the Risk Management Department

The strategic objectives of the Risk Management Department at Mustaqbal University are:

1. To foster a culture of risk management and establish professional practices that support governance and institutionalize institutional work.
2. To ensure compliance with national and international standards and institutional and program accreditation requirements.
3. To support financial sustainability through effective financial risk management, avoiding waste, and maximizing resource efficiency.
4. To protect the university's academic reputation and maintain the quality of educational and research services.
5. To enhance the quality of decision-making by providing accurate data and analyses based on risk assessment.
6. To ensure the continuity of vital operations and services to enhance the sustainability of the educational and research process.
7. To enhance the university's competitive advantage through innovative risk management that supports academic and research excellence.
8. To protect the interests of stakeholders, including students, faculty, staff, and partners.
9. To adopt innovation and digital transformation in risk management and improve operational efficiency.
10. To commit to a continuous improvement methodology to ensure the development of the quality of the risk management system.

6.2. To enhance transparency and accountability in all risk management processes to contribute to building institutional trust.

12. Achieving full integration with the university's strategic plan to ensure that risk management priorities are aligned with the university's strategic objectives.

2.4 Performance Indicators for the Strategic Objectives

No.	Goal	Description	Performance Indicator (KPIs)
1	Strengthening the risk management culture	Raising awareness and adopting risk management practices among all departments, faculty, and students to ensure a proactive and prepared environment.	Percentage of participants in risk awareness workshops

2	Ensuring compliance with national and international standards	Implementing ISO 31000 requirements and adhering to institutional and program accreditation requirements related to risk management.	Number of training courses conducted annually
3	Promoting financial sustainability	Supporting the university in protecting its resources, maximizing efficiency, and minimizing waste through the management of financial and operational risks.	Results of risk management awareness surveys
4	Protecting academic reputation	Managing reputational risks that could affect the university's standing and image within the academic and professional community.	Number of reputational incidents recorded annually
5	Enhancing the quality of decision-making	Providing accurate data and risk-based analytics to support leadership in making effective and informed decisions.	Speed of response to critical incidents
6	Ensuring business continuity	Enhancing the university's resilience to disruptions through business continuity and crisis management plans.	Stakeholder satisfaction indicators
7	Strengthening the university's competitive advantage	Supporting institutional excellence through managing risks related to innovation, quality, and leadership in the educational environment.	Percentage of decisions based on risk reports
8	Protecting the interests of stakeholders	Ensuring the safety and security of students, staff, faculty, and partners, and mitigating risks affecting them.	Number of safety-related incidents
9	Transforming and innovating in risk management	Utilizing digital systems and intelligent analytics to enhance the effectiveness of risk assessment and response.	Stakeholder satisfaction indicators
10	Continuous improvement	Develop a risk management methodology and regularly review records and processes to ensure sustainable development.	Level of compliance with safety procedures
6.2	Promoting transparency and accountability	Provide an environment based on transparency, accuracy, and documentation of all stages of risk assessment and mitigation.	Percentage of automation in risk management
12	Integration with the strategy	Ensuring that risk management is an essential part of the university's strategic planning and programs.	Number of systems/technical tools used

2.5 Core Values of the Risk Management Department

Integrity and transparency:	Adherence to the highest standards of integrity and transparency in all risk management and information disclosure processes.
Responsibility and accountability:	Full responsibility for the outcomes of risk management and accountability for all involved.
Continuous improvement:	Continuous pursuit of developing and improving risk management methods and processes.
Teamwork:	Fostering teamwork and collaboration among all stakeholders involved in risk management.
Proactivity:	Adopting a proactive approach to identifying and managing risks before they occur.
Flexibility and adaptability:	Accessibility to adapt to changes and new challenges quickly and effectively
Accuracy and reliability:	. Ensuring the accuracy and reliability of all risk-related information and analysis.
Innovation and creativity:	Encouraging innovation and creativity in developing new risk management solutions.

Chapter III
Reference Framework for Risk Management

3.1 International Standards for Risk Management

3.1.1 ISO 31000:2018 Standard

Standard Overview

ISO 31000:2018 is the leading international standard for risk management, developed by the International Organization for Standardization (ISO). The standard provides principles, a framework, and a process for risk management that can be used by any organization, regardless of its size, type, or activity.

The Eight Principles of Risk Management

ISO 31000 identifies eight fundamental principles for effective risk management:

No.	Principle	Description	University Application
1	(Integrated)	Risk management is an integral part of all organizational activities.	Integrating risk management into strategic planning, academic processes, financial decision-making, and all levels of management.
2	(Structured and Comprehensive)	A structured and comprehensive approach contributes to consistent and comparable results.	Implementing a unified risk management methodology across all colleges and departments while respecting the specific needs of each.
3	(Customized)	A risk management framework and process is tailored and context-appropriate.	Adapting risk management to the unique nature of the university, its competitive environment, and its specific requirements.
4	(Inclusive)	Stakeholders are engaged appropriately and promptly.	Involving students, faculty, administration, investors, and the community in risk management processes.
5	(Dynamic)	Risks emerge, change, and disappear as the internal and external contexts change.	Continuously reviewing risks and adapting to changes in the market, regulations, and technology.
6	(Best Available Information)	Utilize the best available information while understanding its limitations.	Relying on historical data, analytics, experience, and comparative studies in risk assessment.
7	(Human and Cultural Factors)	Human behavior and culture significantly influence all aspects of risk management.	Building a positive risk culture, training staff, and promoting risk awareness at all levels.
8	(Continual Improvement)	Risk management is constantly improving through learning and experience.	Periodic review, learning from incidents, and continuous improvement of processes and tools

Framework

The ISO 31000 framework consists of five main components:

A. Leadership and Commitment

• Senior leadership commitment to risk management
• Allocating necessary resources
• Defining responsibilities and authorities
• Integrating risk management into university governance

B. Design

• Understanding the university and its context
• Clarifying the risk management commitment
• Defining roles and responsibilities
• Allocating resources
• Establishing communication and consultation mechanisms

C. Implementation

• Developing an implementation plan
• Applying the risk management process
• Ensuring the integration of risk management across all operations
• Developing training and awareness programs

D. Evaluation

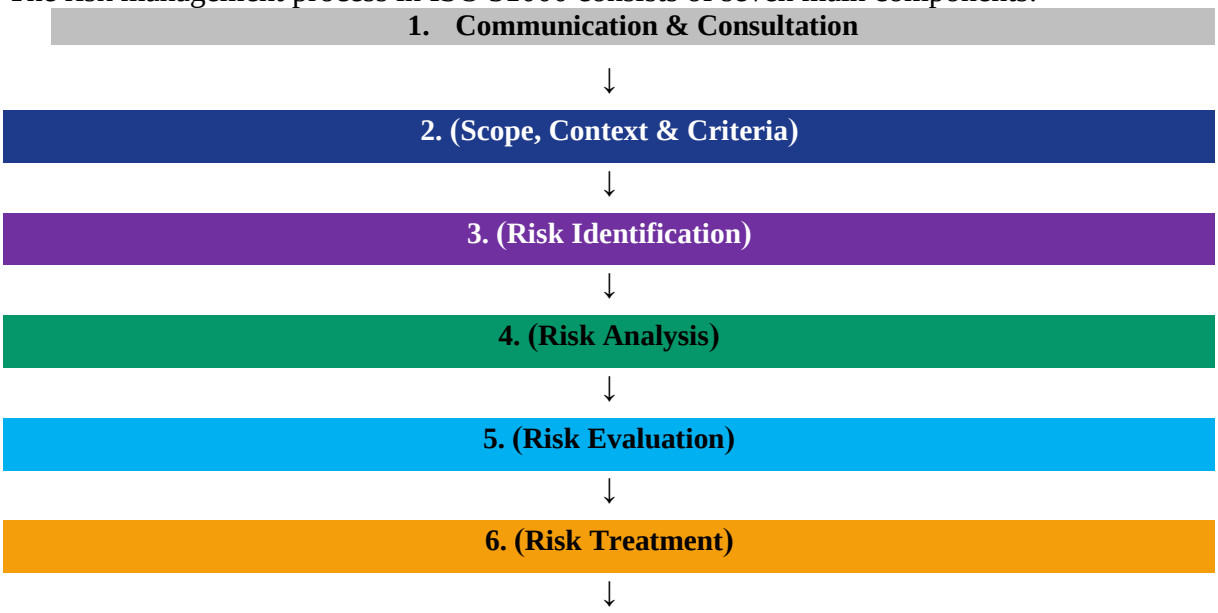
• Measuring the performance of risk management
• Evaluating the effectiveness of the framework
• Reporting on risks and results
• Reviewing the framework's suitability

E. Improvement

• Continuously adapting to improve performance
• Learning from experiences
• Developing processes and procedures
• Keeping abreast of best practices

Risk Management Process

The risk management process in ISO 31000 consists of seven main components:



7. (Monitoring, Review & Recording)

3.1.2 COSO ERM Framework

Overview on COSO ERM

The COSO Enterprise Risk Management Framework (COSO ERM - Integrating with Strategy and Performance) is a comprehensive framework developed by the Committee of Sponsoring Organizations of the Tread Way Commission in 2017. The COSO ERM framework clearly links risk management, strategy and performance, emphasizing the role of risk management in creating, protecting and achieving value.

The five components of the COSO ERM framework

No.	Component	Description and Application
1	(Governance & Culture)	**Description:** Governance defines the university's procedural policies, promotes the importance of risk management, and establishes accountability for it. Culture pertains to ethical values, desired behaviors, and a shared understanding of risk. **Application to the University:** • The role of the University Council in overseeing risk management • Defining risk appetite and tolerance limits • Building an organizational culture that values transparency and accountability • Promoting ethical values in all decisions
2	(Strategy & Objective-Setting)	**Description:** Risk management is integrated into the strategic planning process. Risks are considered when developing the strategy and selecting objectives. **Application at the University:** • Strategic risk analysis when developing the strategic plan • Aligning objectives with risk appetite • Evaluating strategic alternatives from a risk perspective • Identifying acceptable risks to achieve objectives
3	(Performance)	**Description:** Risks must be identified, assessed, prioritized, addressed, and reported across the university to support performance. **Application at the University:** • Comprehensive risk identification across all sectors

		• Risk severity and probability assessment • Prioritization based on risk assessment • Selection and implementation of appropriate risk responses • Development of a risk portfolio
4	(Review & Revision)	**Description:** By reviewing the university's performance, it can assess how well the components of its enterprise risk management system have functioned over time and identify any necessary adjustments. **Applications at the university include:** • Periodic review of risk management effectiveness • Assessing whether risk management capabilities are adequate • Reviewing and updating the risk portfolio • Learning from past events and incidents • Updating strategies based on reviews
5	(Information, Communication & Reporting)	**Description:** Enterprise risk management requires a continuous flow of information from internal and external sources that flows through, upstream, and downstream of the university. **Applications at the university include:** • Establishing effective risk communication channels • Providing accurate and timely information • Regular reports to management and the Board of Trustees • Mechanisms for reporting risks and incidents

3.1.3 Information security - ISO/IEC 27001

The ISO/IEC 27001 standard provides requirements for establishing, implementing, maintaining, and improving an Information Security Management System (ISMS). The standard includes Annex A, which contains 6.24 security officers distributed across 14 categories. The standard's importance to the university is highlighted by:

• Protecting sensitive student and staff data
• Ensuring the availability of academic and administrative systems
• Complying with personal data protection requirements
• Enhancing the confidence of students and stakeholders

3.1.4 Business Continuity - ISO 22301

The ISO 22301 standard specifies the requirements for a Business Continuity Management System (BCMS). This standard helps universities prepare for, respond to, and recover from disruptive incidents. Its importance to the university is highlighted by:

• Ensuring the continuity of educational services
• Minimizing the impact of crises on students
• Protecting reputation and financial sustainability
• Complying with the requirements of the accreditation body

3.2 General Policy for Risk Management

3.2.1 Policy Statement

Mustaqbal University is committed to implementing a comprehensive, integrated risk management system to protect the interests of its stakeholders and achieve the university's strategic and operational objectives.

We believe that effective risk management is a shared responsibility of all university members, and we are committed to integrating risk management into all decision-making and operational processes through a proactive and systematic approach that aligns with best practices and international standards.

The university will review and update this policy periodically to ensure its continued relevance and effectiveness in light of internal and external changes.

3.2.2 Core Principles

The general risk management policy at Mustaqbal University is based on the following principles:

No.	Principle	Description
1	Leadership Commitment	A full commitment from senior leadership (the College Council and the University President) to support and enhance risk management, allocate the necessary resources, and assume ultimate responsibility for the system's effectiveness.
2	Strategic Integration	Integrating risk management into all phases of strategic and operational planning and linking it to decision-making processes at all levels to ensure alignment with university objectives.
3	Proactive Approach	Adopting a proactive approach to identifying, assessing, and addressing risks before they materialize, rather than waiting until they become actual problems, with a focus on early warning and prevention.
4	Inclusive Engagement	Engaging all university personnel in risk management processes and fostering a culture of shared responsibility, where each individual is responsible for identifying and reporting risks within their area of expertise.
5	Informed Decision-Making	Ensuring that all administrative and academic decisions are based on a clear understanding of the associated risks, and providing accurate and reliable risk information to decision-makers.
6	Balance of Risks and Opportunities	Viewing risks not only as threats but also as potential opportunities for improvement and growth, while striving to achieve an appropriate balance between risk tolerance and expected returns.
7	Transparency and Accountability	A commitment to full transparency in all risk management processes and disclosure of significant risks, with clear definition of responsibilities and accountability for outcomes.

8	Continuous Improvement	Regular review of the effectiveness of the risk management system, learning from experiences and incidents, and continuous improvement of processes and methods to align with best practices.
9	Proportionality and flexibility	Implementing a level of risk management commensurate with the complexity and magnitude of the risks, while maintaining sufficient flexibility to adapt to changes and emerging circumstances.
10	Compliance and governance	Ensuring full compliance with relevant local regulations and international standards, and applying the principles of good governance in all aspects of risk management.
6.2	Protecting stakeholders	Placing the interests of students, staff, investors, and the community at the heart of risk management processes, while ensuring the protection of their rights and interests at all times.
12	Long-term sustainability	Focusing on achieving the long-term financial and operational sustainability of the university, not just short-term results, through prudent risk management.

3.2.3 Policy Scope

i- Covered Departments

This policy applies to all units of the university without exception, including:

- All academic colleges
- All central departments
- Research centers and special-purpose units
- University-affiliated companies and entities

ii- Concerned Individuals

The policy applies to all individuals associated with the university:

- Members of the University Council
- The University President and Vice-Presidents
- Deans and Vice-Deans
- Faculty members (full-time and part-time)
- All administrative and technical staff
- Contractors and consultants
- Students (in relevant aspects)

iii- Operations and Activities

The policy covers all operations and activities:

- Strategic and operational planning
- Academic and research operations
- Financial management and procurement
- Human resources management
- Information technology and systems

• Student services and academic support
• Facilities and support services
• External relations and partnerships

3.2.4 General Responsibilities

A. University Council Responsibilities

• Adopting the overall risk management policy and any amendments thereto
• Determining the university's overall risk appetite
• Overseeing the effectiveness of the risk management system
• Reviewing periodic risk reports
• Ensuring the availability of necessary resources for risk management

B. University President Responsibilities

• Leading the implementation of the risk management policy
• Chairing the Higher Committee for Risk Management
• Making strategic decisions related to major risks
• Ensuring the integration of risk management into the university culture
• Appointing the Director of Risk Management

C. Senior Management Responsibilities

• Implementing the policy within their areas of expertise
• Identifying and assessing major risks
• Developing and implementing risk mitigation plans
• Appointing risk owners
• Submitting periodic reports

D. All Staff Responsibilities

• Actively participating in risk identification
• Promptly reporting risks and incidents
• Implementing risk control procedures
• Participating in training programs
• Adhering to risk management policies and procedures

Chapter IV
Structural Organization and Responsibilities

4.1 The Organizational Structure of the Risk Management Department

The risk management department's organizational structure aligns with the university's overall structure, ensuring clear lines of communication and defined responsibilities at all levels.

4.1.1 Authorities and Responsibilities

A. Strategic Level

A.1 University Council

Strategic Oversight Role:

• Approving the overall risk management policy and proposed updates
• Determining the university's overall risk appetite and acceptable tolerance limits
• Reviewing and approving the comprehensive risk management strategy
• Overseeing the effectiveness of the risk management and governance system
• Ensuring the availability of necessary resources (financial, human, and technological) for risk management

Report Review:

• Reviewing the comprehensive annual risk management report
• Reviewing quarterly reports on critical risks

• Reviewing immediate reports on major crises
• Discussing internal and external audit reports of the risk management system

Strategic Decision Making:

• Approving major strategic risks (outside the risk appetite)
• Adopting plans to address critical risks with significant financial impact
• Approving insurance and risk transfer policies
• Making decisions regarding high-risk initiatives and projects

Activity	Frequency	Expected Outputs:
Risk Management Review Meeting	Quarterly/Semi-annual	Decisions and Meeting Minutes, Management Directives
Review and Approval of General Policy	Annual	Updated and Approved Policy
Review and Approval of Risk Appetite	Annual	Updated Risk Appetite Statement
Evaluation of the Effectiveness of the Risk Management Policy	Annual	Assessment Report with Recommendations

A.2 University President

Executive Leadership:

• Chair the Senior Risk Management and Business Continuity Committee
• Lead efforts to integrate risk management into the corporate culture
• Appoint the Director of Risk Management and members of the Senior Committee
• Allocate the necessary resources to implement risk treatment plans
• Approve the general directions and priorities in risk management

Decision-Making:

• Approve strategic risk mitigation plans
• Make immediate decisions in crisis situations
• Approve the organizational structure for risk management
• Approve the annual budget for the Risk Management Unit

Accountability and Oversight:

• Hold Vice Presidents accountable for risk management in their respective areas
• Review periodic performance reports of the risk management system
• Communicate with the Board of Trustees regarding critical risks
• Follow up on the implementation of internal and external audit recommendations

A.3 Senior Risk Management and Business Continuity Committee

Committee Composition:

Positions	Title	Role in the Committee
University President	Committee Chair	General Leadership, Strategic Decision-Making
Executive Director	Member	Human Resources Risks/Financial Risks/Security and Safety Risks
Vice President for Academic	Member	Academic and Research Risks

Affairs		
Vice President for Graduate Studies and Research	Member	Technical Risks/Cybersecurity Risks/Research Risks
Vice President for Development and Community Responsibility	Member	Marketing Risks/Community Partnership Risks/Reputational Risks
Director of Quality and Accreditation	Member	Quality and Accreditation Risks
Director of Legal Affairs	Member	Legal and Regulatory Risks
Director of Internal Audit	Member	Compliance and Adherence Risks
Director of Strategic Planning	Member	Strategic Risks
Director of Risk Management	Member and Secretary	Work Coordination, Reporting

Responsibilities of the Higher Committee:

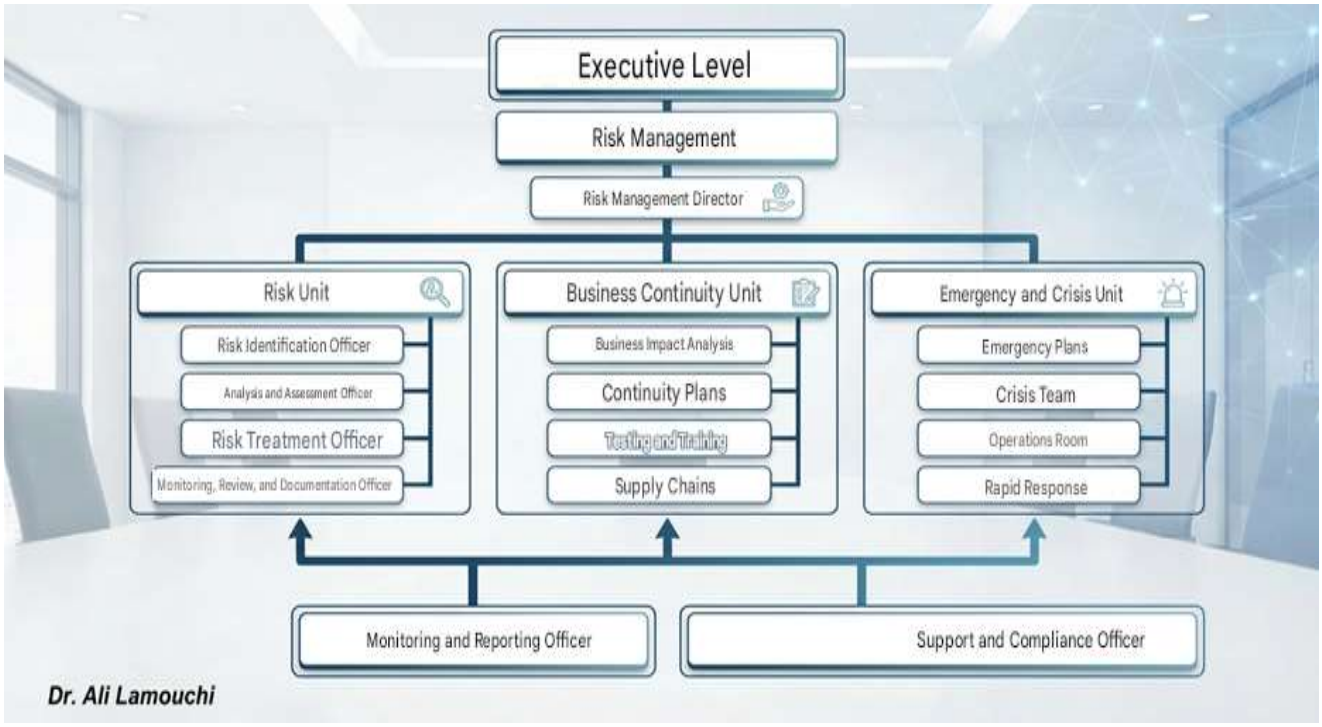
• Developing and annually reviewing the risk management strategy
• Reviewing and approving the university's key risk register
• Identifying and prioritizing critical risks
• Reviewing and approving key risk mitigation plans
• Monitoring the implementation of mitigation plans and progress
• Allocating resources to risk management initiatives
• Adopting detailed policies and procedures
• Overseeing business continuity and crisis management plans
• Recommending amendments to general policy
• Submitting periodic reports to the university president and the university council

Meeting Frequency:

• Regular meetings: Monthly (or as needed)
• Emergency meetings: In the event of a crisis or critical risk
• Annual review meeting: At the end of the fiscal year

B. Executive Level

B.1 Risk Management



B.1.1 Risk Management Director - Role and Responsibilities:

• Leadership: Leading the Risk Management Unit and overseeing all departments.
• Coordination: Coordinating with all administrative and academic units.
• Planning: Developing annual plans for risk management activities.
• Reporting: Preparing periodic reports for the Higher Committee and the University President.
• Consulting: Advising senior management on risks.
• Development: Developing risk management policies, procedures, and models.
• Training: Overseeing training and awareness programs.
• Reviewing: Reviewing the effectiveness of the risk management system.

B.1.2 Risk Coordinators in Colleges and Departments

A risk coordinator is appointed in each college and department, serving as the liaison between the central unit and operational sectors.

Roles and Responsibilities

• Coordinate risk management activities within the college/department
• Identify potential risks in the workplace
• Collect and document risk information
• Assist in risk assessment and the development of mitigation plans
• Monitor the implementation of risk control procedures
• Submit periodic reports to the central risk unit
• Promptly report new incidents and risks
• Raise awareness of risk management among colleagues
• Participate in training programs

Coordination with Central Administration

Activity	Frequency	Mechanism
Risk Report	Monthly	Monthly Report Template

Coordination Meeting	Quarterly	Meeting with all Coordinators
Incident Reporting	Immediately	Immediate Reporting Template
Risk Log Update	Monthly	Electronic System

4.2 Specialized Units

In addition to the Supreme Committee and the Central Risk Management Department, some specialized departments and units focus on specific categories of tasks and report to the Central Management:

4.2.1 Risk Unit – Tasks and Outputs

No.	Area	Tasks and Responsibilities:	Expected Outputs
1	Policies	Preparing and updating the Enterprise Risk Management Policy	Adopted and Updated Risk Management Policy
2	Risk Log	Creating and updating the comprehensive Enterprise Risk Register	Updated and Approved Risk Register
3	Assessment	Developing the Risk Matrix (5x5)	Approved Risk Thermal Matrix
4	Coordination	Coordinating with all departments	Completed Sectoral Risk Records
5	Reporting	Preparing and submitting periodic reports	Periodic Reports for Senior Management
6	Compliance	Supporting governance and compliance requirements	Audit-Ready Compliance Reports
7	Corporate Culture	Promoting a risk management culture	Awareness Programs and Training Reports
8	Improvement	Supporting continuous improvement	Approved Improvement Plans

4.2.2 Risk Assessment Officer

No.	Area	Tasks and Responsibilities	Expected Outcomes
1	Analysis	Risk Probability Analysis	Approved Probability Values
2	Impact	Financial, Operational, and Reputational Impact Analysis	Detailed Impact Reports
3	Evaluation	Risk Level Determination	Risk Level Classification
4	Maps	Preparation of Risk Heat Maps	5x5 Risk Maps
5	Priorities	Prioritization of Risks	Critical Risk List
6	Reports	Preparation of Risk Analysis and Assessment Reports	Approved Analysis Reports

4.2.3 Risk Analysis and Assessment Officer

No.	Area	Tasks and Responsibilities	Expected Outcomes
1	Analysis	Risk probability analysis	Approved probability values
2	Impact	Financial, operational, and reputational impact analysis	Detailed impact reports
3	Evaluation	Risk level assessment for each risk	Risk level classification
4	Mapping	Preparation of risk heat maps	5x5 risk maps
5	Priorities	Priority risk identification	Critical risk list
6	Reports	Preparation of risk analysis and assessment reports	Approved analysis reports

4.2.4 Risk Management Officer

No.	Area	Tasks and Responsibilities	Expected Outcomes
1	Strategies	Propose remediation strategies	Risk Response Plans
2	Plans	Prepare risk remediation plans	Remediation Plan Templates
3	Follow-up	Monitor implementation of remediation plans	Performance Reports
4	Controls	Evaluate control effectiveness	Control Efficiency Reports
5	Residual Risks	Update risk level after remediation	Updated Risk Levels
6	Reporting	Prepare remediation efficiency reports	Periodic Reports

4.2.5 Monitoring, Review and Documentation Officer

No.	Area	Tasks and Responsibilities	Expected Outcomes
1	Monitoring	Monitoring compliance with policies	Compliance reports
2	Reviewing	Conducting periodic reviews	Audit reports
3	Documenting	Verifying complete documentation	Documented files
4	Archiving	Electronic document storage	Electronic archives
5	Auditing	Supporting internal and external audits	Completed audit files
6	Reporting	Preparing audit reports	Official reports

4.2.6 Business Continuity Unit – Tasks and Outputs

No.	Area	Tasks and Responsibilities	Expected Outcomes
1	Policy	Developing a business continuity policy	Approved Policy
2	Impact Analysis	Conducting a Business Impact Analysis (BIA)	BIA Reports
3	Critical Operations	Identifying critical processes	Critical Operations List
4	Plans	Developing continuity plans	BCP Plans
5	Recovery	Developing disaster recovery plans	DRP Plans
6	Testing	Conducting simulation exercises	Test Reports

7	Readiness	Measuring readiness levels	Readiness Indicators
8	Reporting	Preparing continuity reports	Periodic Reports
9	Training	Training staff	Training Programs

4.2.7 Crisis and Emergency Management Unit – Tasks and Outputs

No.	Area	Tasks and Responsibilities	Expected Outcomes
1	Plan	Developing a crisis management plan	Approved Crisis Plan
2	Teams	Forming emergency teams	Formation Decisions
3	Coordination	Coordinating with government agencies	Coordination Minutes
4	Communication	Managing communications	Communication Plans
5	Response	Activating immediate response	Response Records
6	Follow-up	Monitoring emergency scenarios	Follow-up Reports
7	Documentation	Documenting lessons learned	Lessons Learned Reports
8	Evaluation	Evaluating the response	Evaluation Reports
9	Improvement	Developing improvement plans	Improvement Plans

4.3 Detailed Roles and Responsibilities - RACI Matrix

The RACI matrix is used to illustrate roles and responsibilities in risk management processes. RACI stands for:

- **R-Responsible** (the one responsible for implementation): The person or entity that actually carries out the work.
- **A - Accountable** (the one held accountable): The person who bears ultimate responsibility for the results.
- **C - Consulted** (the one consulted): People who are consulted before a decision is made.
- **I - Informed** (the one informed): People who are informed of the decisions and results.

4.3.1 RACI's comprehensive matrix for risk management activities

Activity	University Council	University President	Supreme Committee	Risk Manager	Risk Units	Vice Presidents	Deans	Risk Coordinators	All Staff
Governance and policies									
Adopting a general risk management policy	**A**	**C**	**C**	**R**	**I**	**I**	**I**	**I**	**I**
Defining risk appetite and tolerance limits	**A**	**C**	**C**	**R**	**R**	**C**	**I**	**I**	**I**
Developing a risk management strategy	**I**	**A**	**R**	**R**	**R**	**C**	**C**	**I**	**I**
Adopting a risk management organizational structure	**A**	**R**	**C**	**C**	**I**	**I**	**I**	**I**	**I**
Risk identification									

Identifying strategic risks	**I**	**A**	**R**	**R**	**R**	**C**	**C**	**R**	**I**
Identifying operational risks	**I**	**I**	**I**	**C**	**C**	**A**	**R**	**R**	**R**
Conducting risk identification workshops		**I**	**I**	**A**	**R**	**C**	**C**	**R**	**R**
Reporting new risks		**I**	**I**	**I**	**A**	**I**	**R**	**R**	**R**
Risk assessment and analysis									
Assess the likelihood and impact of risks		**I**	**I**	**A**	**R**	**C**	**R**	**R**	**C**
Prioritize risks		**I**	**A**	**R**	**R**	**C**	**C**	**I**	
Update the risk register		**I**	**I**	**A**	**R**	**I**	**C**	**R**	
Conduct a quantitative analysis of major risks		**I**	**I**	**A**	**R**	**C**	**C**	**R**	
Risk management									
Choosing a risk management strategy		**I**	**A**	**C**	**C**	**R**	**R**	**C**	
Preparing risk treatment plans		**I**	**I**	**C**	**C**	**A**	**R**	**R**	
Approving critical management plans		**A**	**C**	**C**	**C**	**R**	**I**	**I**	
Implementing management actions		**I**	**I**	**I**	**C**	**A**	**R**	**R**	**R**
Allocating resources for management plans		**A**	**C**	**C**	**I**	**R**	**R**	**I**	
Monitoring and follow-up									
Monitoring the implementation of treatment plans		**I**	**I**	**A**	**R**	**R**	**R**	**R**	
Measuring Key Performance Indicators (KPIs)		**I**	**I**	**A**	**R**	**C**	**C**	**R**	
Monitoring Key Risk Indicators (KRIs)		**I**	**I**	**A**	**R**	**R**	**R**	**R**	
Reports and Communications									
Preparing monthly reports		**I**	**I**	**A**	**R**	**C**	**C**	**R**	
Preparing quarterly reports	**I**	**I**	**A**	**R**	**R**	**C**	**C**	**R**	
Preparing the annual report	**I**	**A**	**C**	**R**	**R**	**C**	**C**	**R**	
Communicating with stakeholders		**A**	**C**	**R**	**R**	**R**	**R**	**R**	**I**
Review and Improvement									
Periodic review of system	**A**	**C**	**C**	**R**	**R**	**C**	**C**	**I**	

effectiveness									
Updating policies and procedures	**A**	**C**	**C**	**R**	**R**	**C**	**I**	**I**	**I**
Implementing proposed improvements	**I**	**A**	**C**	**R**	**R**	**R**	**R**	**R**	
Training and awareness									
Developing the annual training plan		**I**	**A**	**R**	**R**	**C**	**C**	**I**	
Implementing training programs		**I**	**I**	**A**	**R**	**R**	**R**	**R**	**R**
Disseminating awareness campaigns		**I**	**I**	**A**	**R**	**R**	**R**	**R**	**I**
Crisis and Emergency Management									
Activating the emergency plan	**I**	**A**	**R**	**R**	**R**	**R**	**R**	**R**	**R**
Crisis management	**I**	**A**	**R**	**R**	**R**	**R**	**R**	**R**	**R**
Crisis communication	**I**	**A**	**C**	**R**	**R**	**R**	**I**	**I**	**I**

Table Key:
• A = Accountable - Ultimate responsibility
• R = Responsible - Performing the actual work
• C = Consulted - Consulted before the decision
• I = Informed - Informed of the decision

4.3.2 Job description of a risk management manager

Job Title: Director of Risk Management
Reports to: University President
Functional Reporting to: Senior Risk Management Committee
Job Level: Senior Management
Primary Job Purpose: To lead and coordinate all risk management and business continuity activities at the university, ensure the effective implementation of risk management policies and procedures, and advise senior management on strategic and operational risks.
Key Tasks and Responsibilities:
1. Strategy and Policies:
• Lead the development of the risk management strategy in collaboration with the Higher Committee
• Prepare and update policies and procedures related to risk management
• Develop an integrated risk management framework that aligns with international standards
• Define and update risk appetite and tolerance limits in coordination with senior management
2. Leadership and Supervision:
• Lead and supervise the Risk Management Unit team (5-8 employees)
• Set performance objectives for team members and monitor their achievement
• Develop team capabilities through training and mentoring
• Coordinate work between the different departments within the Risk Unit
3. Risk Identification and Assessment:

• Oversee risk identification processes across all university sectors
• Lead the assessment of strategic and major risks
• Ensure the application of a standardized risk assessment methodology
• Review and approve risk assessments submitted by different sectors

4. Risk Register Management:

• Oversee the development and maintenance of the central risk register
• Ensure the risk register is updated regularly and systematically
• Review and approve changes to the risk register
• Prepare analytical reports from the risk register

5. Remediation Plans:

• Assist in developing critical risk remediation plans
• Review and approve Sector-Submitted Remediation Plans
• Monitoring the implementation of remediation plans and progress achieved
• Escalating issues and delays to the relevant department

6. Reporting and Communication:

• Preparing periodic reports (monthly, quarterly, annual) on the risk status
• Presenting reports to the Higher Committee and the Board of Trustees
• Effective communication with all stakeholders
• Preparing special reports upon request

7. Business Continuity and Crisis Management:

• Overseeing the development and testing of business continuity plans
• Leading the crisis management team when needed
• Ensuring the readiness of emergency and rapid response plans
• Coordinating post-incident recovery operations

8. Training and Awareness:

• Developing the annual training and awareness plan
• Designing and implementing risk management training programs
• Promoting a risk management culture within the university
• Measuring the effectiveness of training and awareness programs

9. Compliance and Auditing:

• Ensuring compliance with international and local standards
• Coordinating with internal and external audits
• Implementing audit recommendations
• Periodically reviewing the effectiveness of the risk management system

10. Continuous Improvement:

• Identifying opportunities for improvement in risk management processes
• Keeping abreast of best practices and developments in the field Develop new tools and models as needed
• Lead improvement initiatives

Required Qualifications and Experience:

A. Academic Qualifications:

• Minimum Master's degree in Finance and Risk Management, Business Administration, Accounting, Engineering, or a related field

B. Professional Certifications (Preferred):

• Certified Risk Manager (CRM)

• Financial Risk Manager (FRM)
• Certified in Risk and Information Systems Control (CRISC)
• Professional Risk Manager (PRM)
• Certified Business Continuity Professional (CBCP)
• ISO 31000 Risk Management Professional

C. Work Experience:

• At least 5 years of experience in risk management or internal audit
• At least 3 years of experience in a leadership position
• Experience in the education sector or service organizations
• Familiarity with ISO 31000 and COSO ERM standards

D. Required Skills:

• Strong leadership and management skills
• Analytical and problem-solving skills
• Communication and presentation skills (Arabic and English)
• Ability to work under pressure
• Proficiency in Microsoft Office applications and management tools Risk Management
• Strategic Thinking Skills
• Relationship Building and Influence Skills

Authorities:

• Approving sub-critical risk assessments
• Approving procedural modifications within the scope of the approved policy
• Allocating the unit's budget within the approved limits
• Accessing all relevant risk-related information and documents
• Direct communication with all levels of management
• Forming special task forces when needed

Chapter V
Comprehensive Risk Classification

5.1 Risk classification by category

Risks at Mustaqbal University are classified into 6.2 main categories covering all aspects of university operations. This classification helps in:

- Systematic and comprehensive risk identification
- Clear assignment of responsibilities
- Development of appropriate mitigation strategies
- Facilitating reporting and monitoring

5.1.1 Strategic Risks

Definition

Risks associated with achieving the university's long-term strategic goals and plans, which may affect its competitive position, reputation, and future growth.

Types of Strategic Risks

No.	Type of risk	Description:	Examples:	Official
1	Expansion risks	Failure of geographic or program expansion plans	The futility of opening a new branch	University President
2	Competitive strategy risks	Weak competitive position compared to other universities	The failure of a new academic program	Strategic Planning Department
3	Strategic partnership risks	Failure of partnerships with local and international universities or institutions	Loss of market share	Vice President for Development
4	Innovation risks	Inability to innovate and keep pace with developments Traditional programs	A decline in the university's appeal	Vice President for Development
5	Diversity risks	Over-reliance on a single revenue stream	Reliance on a single specialization	Financial Director
6	Governance risks	Weak corporate governance and decision-making	Single source of income	University Council
7	Leadership risks	Loss of key leaders or inadequate succession planning	Ill-considered decisions	University Board
8	Strategic planning risks	Unrealistic or unfeasible strategic plan	Weak oversight	University President
9	Brand risks	Erosion of the university's brand value	Sudden resignation of a president	Marketing Department
10	Strategic investment risks	Failure of major investment projects	Lack of succession plans	Project Management
6.2	Organizational change risks	Resistance to change or poor management of it	Unmeasurable goals	Vice President for Development
12	Government policy risks	Changes in educational policies that affect the university	Resource shortages	Legal Department

5.1.2 Financial Risks

Definition

Risks related to financial aspects that may affect the financial sustainability of the university. These risks are of paramount importance to private universities due to their reliance on self-generated revenue.

Types of financial risks

No.	Type of risk	Description:	Examples:	Official
1	Liquidity risks	Inability to meet short-term financial obligations	Cash flow shortage	Financial Director
2	Revenue risks	Decreased tuition revenue	Delayed salary payments	Financial Department
3	Collection risks	Late or unpaid tuition fees	Decreased student enrollment	Financial Department
4	Investment risks	Losses on university investments	Increased scholarships	Projects Committee
5	Operating cost risks	Excessive increase in operating costs	Students defaulting on payments	Human Resources Department
6	Financing risks	Difficulty in securing project funding	Bad debt	Financial Department
7	Budget risks	Budget overruns or poor financial planning	Decreased asset value	Budget Department
8	Pricing risks	Uncompetitive tuition pricing	Failed investments	Finance Committee
9	Financial fraud risks	Fraud, embezzlement, or financial corruption	Salary increases	Internal Audit
10	Financial control risks	Weak internal controls over financial operations	Higher service prices	Internal Audit
6.2	Financial reporting risks	Errors in financial reporting	Loan application rejections	Financial Director
12	Tax and duty risks	Non-compliance with tax requirements	Hard-term financing terms	Financial Department
13	Currency risks	Exchange rate fluctuations (for international transactions)	Unplanned expenses	Financial Department
14	Procurement risks	Poor procurement management	Budget deficit	Contracts and Procurement Department
15	Financial sustainability risks	Failure to achieve long-term financial sustainability	Excessively high fees	University President

5.1.3 Operational Risks

Definition

Risks arising from daily operations, systems, procedures, and physical resources.

Types of Operational Risks

No.	Type of risk	Description:	Examples:	Official
1	Operational risks	Errors or delays in administrative processes	Administrative Process Risks Errors or delays in administrative processes; delays in issuing documents; data errors;	Department Directors

			department managers.	
2	Facilities risks	Problems with buildings and facilities	Facilities Risks: Problems with buildings and facilities; elevator malfunctions; air conditioning problems; facilities and inventory management.	Facilities and Inventory Management
3	Maintenance risks	Poor or delayed maintenance	Maintenance Risks: Poor or delayed maintenance; frequent breakdowns; high repair costs; facilities and inventory management.	Facilities and Inventory Management
4	Supply chain risks	Disruptions in supply chains for materials and services	Supply Chain Risks: Disruptions in the supply chains of materials and services; shortages of laboratory materials; supply delays; contract and procurement management.	Contracts and Procurement Management
5	Security and safety risks	Security incidents or thefts	Security and Safety Risks: Security incidents or thefts; property theft; unauthorized entry; security and safety manager.	Security and Safety Manager
6	Emergency risks	Lack of emergency preparedness	Emergency Risks: Lack of emergency preparedness; ineffective evacuation plans; shortage of equipment; security and safety manager.	Security and Safety Manager
7	Procedure risks	Complex or ineffective procedures	Procedural Risks: Complex or ineffective procedures; excessive bureaucracy; administrative complexities; vice president for development.	Vice President for Development
8	Document and record risks	Loss or damage to important records	Documents and Records Risks: Loss or damage to important records; missing documents; outdated records; administrative communications management.	Administrative Communications Management
9	Logistics risks	Poor management of logistics	Logistics Risks: Poor logistics management; event delays; lack of coordination; facilities and inventory management.	Facilities and Inventory Management
10	Project management risks	Failure or delay of internal projects	Project Management Risks: Failure or delay of internal projects; budget overruns; delivery delays; project management.	Projects Management
6.2	Internal communications risks	Poor internal communication	Internal Communications Risks: Poor communication. Internal misunderstandings	Administrative Communications Management

5.1.4 Academic and research risks

Definition

Risks related to the quality of education, academic programs, scientific research and

academic accreditation.

Types of Academic and research tasks

No.	Type of risk	Description:	Examples:	Official
1	Risks to the Quality of Education	Low quality of education provided	Student complaints	Quality and Accreditation Management
2	Risks to Academic Accreditation	Lack of or failure to obtain accreditation	Poor assessments	Quality Director
3	Risks to Program Design	Academic programs that do not meet market needs	Accreditation applications rejected	Curriculum and Planning Department
4	Risks to Faculty Members	Lack of or inadequate faculty competence	Accreditation revoked	Deans of Colleges
5	Risks to Assessment and Examinations	Problems with assessment processes	Unrequired programs	College Examination Committees
6	Risks to Scientific Research	Weak scientific research and publication	Outdated content	Scientific Research Department
7	Risks to Research Ethics	Violations of research ethics	Resignations	Scientific Research Department
8	Risks to Curriculum	Outdated or inappropriate curricula	Poor performance	Curriculum Committees
9	Risks to Learning Outcomes	Failure to achieve targeted learning outcomes	Exam leaks	Deans of Colleges
10	Risks to Admissions and Registration	Problems with admissions processes	Grading errors	Admissions and Registration Department
6.2	Risks to Student Services	Inadequate student services	Lack of published research	Vice President for Academic Affairs
12	Risks to E-Learning	Problems with distance learning	Poor quality	E-Learning and Distance Education Department
13	Risks to Field Training	Difficulties in providing training opportunities	Plagiarism	Field Training Units
14	Risks to Library and Resources	Lack of educational and research resources	Data falsification	Learning Resources Department
15	Risks to Laboratories and Workshops	Problems with laboratories and workshops	Outdated content	Laboratory Supervisors

5.1.5 Reputational Risks

Definition

Risks resulting from damage that may affect the university's reputation and image among stakeholders.

Types of Reputational Risks

No.	Type of risk	Description	Examples	Official
1	Risks of negative media coverage	Negative news or media reports	Scandals	Media and Corporate Communications Department
2	Risks of social media	Negative content or attacks on social media platforms	Accidents	Media Department
3	Risks of student satisfaction	Student and parent dissatisfaction	Negative news	Vice President for Academic Affairs
4	Risks of graduate satisfaction	Graduate dissatisfaction with their experience	Negative posts	Student and Alumni Affairs Department
5	Risks of employer relations	Poor reputation among employers	Rumors	University Council
6	Risks of ratings	Decline in local and international rankings	Smear campaigns	Quality and Accreditation Department
7	Risks of complaints and disputes	Escalating complaints and public disputes	Frequent complaints	Legal Department
8	Risks of unethical conduct	Incidents of unethical conduct by university staff	Negative surveys	University President
9	Risks of crisis management	Poor crisis management and communication	Negative reviews	Crisis and Emergency Management Unit
10	Risks of social responsibility	Lack of social responsibility	Weak loyalty	Vice President for Development and Community Responsibility

5.1.6 Human Resources Risks

Definition

Risks related to human resource management, including attracting, retaining, and developing talent.

Types of Human Resources Risks

No.	Type of risk	Description	Examples	Official
1	Risks of Attracting Talent	Difficulty attracting top talent	Difficulty in recruiting professors, unattractive offers	Human Resources Manager
2	Risks of Retaining Employees	High employee turnover and resignation	Frequent resignations, employees moving to competitors	Human Resources Manager
3	Risks of Job Performance	Poor employee performance	Failure to meet targets, frequent complaints	Line Supervisors
4	Risks of Training and Development	Lack of training and skills development	Outdated skills, failure to keep up with developments	Training Department
5	Risks of Job Satisfaction	Low job satisfaction and motivation	Negative surveys, low productivity	Human Resources
6	Risks of Occupational Health and Safety	Workplace accidents or injuries	Occupational injuries and illnesses	Security and Safety Manager
7	Risks of Compensation and Benefits	Uncompetitive salaries and benefits	Below-market salaries, limited benefits	Human Resources
8	Risks of Diversity and Inclusion	Lack of diversity in the workplace	Un-representation of certain groups,	Human Resources

			discrimination	
9	Risks of Labor Relations	Labor disputes and conflicts	Collective complaints, labor disputes	Employee Relations
10	Risks of Succession Planning	Absence of succession planning for critical positions	Sudden leadership vacancies, lack of alternatives	Senior Management
6.2	Risks of Labor Compliance	Non-compliance with labor laws	Violations of labor regulations, fines	Human Resources
12	Risks of Inappropriate Conduct	Harassment or misconduct	Harassment, discrimination, violence	Investigation Committee

5.1.7 Technical and Cyber Risks

Definition

Risks related to information technology, information security, technical infrastructure, and cyberattacks.

Types of Technical and Cyber Risks

No.		Type of risk	Description	Examples	Official
1		Information security risks	Breach or leak of sensitive information	Database breaches - Data leaks	Information Security Officer
2		Cyberattack risks	Cyberattacks on university systems	Viruses - Ransomware - DDoS	Cybersecurity Team
3		Data protection risks	Non-compliance with data protection regulations	PDPL violations - Lack of data encryption	Data Protection Officer
4		Infrastructure risks	Defects or outdated technical infrastructure	Outdated servers - Weak networks	Infrastructure Officer
5		Academic systems risks	Faults in learning management and registration systems	LMS system failure - Log errors	Systems Officer
6		Financial systems risks	Faults in financial and accounting systems	ERP system failure - Financial errors	Financial Systems Officer
7		Network risks	Network outages or slowdowns	Internet outages - Slow network	Network Officer
8		Backup risks	Failure or inadequacy of backups	Data loss - Outdated backups	Systems Officer
9		Disaster recovery risks	Inability to recover from a technical disaster	No DR plan - Unready backup site	IT Manager
10		Technology vendor risks	Over-reliance on or failure of suppliers	Vendor bankruptcy - Poor support	Procurement
6.2		Digital transformation	Failure or delay of digital	Refusal to change - Technical	Digital Transformation

		risks	transformation projects	complexities	Team
12		Privacy risks	Violation of user privacy	Unauthorized access - Data sharing	Privacy Officer
13		Social engineering risks	Deceiving users to obtain information	Cyber fraud - Phishing	Cybersecurity Officer
14		Access and permissions risks	Inappropriate privileges or unauthorized access	Excessive privileges - Unmonitored accounts	Security Management
15		Technical compliance risks	Non-compliance with technical standards	Non-compliance with ISO 27001 PCI DSS standards	Technical Compliance Coordinator

5.1.8 Legal and Regulatory Risks

Definition

Risks arising from non-compliance with laws, regulations, or changes thereto.

Types of Legal and Regulatory Risks

No.	Type of risk	Description	Examples	Official
1	Risks of non-compliance	Non-compliance with rules and regulations	Regulatory Violations - Penalties	Compliance Officer
2	Risks of litigation	Legal cases against the university	Student Lawsuits - Labor Cases	Legal Department
3	Risks of contracts	Unfavorable contracts or contractual disputes	Unfair Conditions - Disputes	Legal Department
4	Risks of intellectual property	Infringement of intellectual property rights	Copyright Infringement - Patents	Vice President for Graduate Studies and Scientific Research
5	Risks of licensing and accreditation	Loss of licenses or legal accreditations	License Cancellation - Non-Renewal	Legal Department
6	Risks of regulatory changes	Unexpected changes in regulations	New Laws - Additional Requirements	Legal Department
7	Risks of legal liability	Assuming significant legal liabilities	Accidents / Damages / Negligence	Legal Department
8	Risks of corruption and bribery	Corruption or bribery cases	Bribery / Abuse of Power	University President
9	Risks of government investigations	Investigations by regulatory bodies	Ministry of Education / Oversight Authority Investigations	University President
10	Risks to student rights	Violation of student rights	Injustice / Discrimination / Deprivation	Vice President for Academic Affairs

5.1.9 Health and Environmental Risks

Definition

Health, safety, and environmental risks on campus.

Types of Health and Environmental Risks

No.	Type of risk	Description	Examples	Official
1	Public Health Risks	Disease outbreaks or epidemics	COVID-19 / Infectious Diseases	Occupational Physician
2	Fire Risks	Building fires	Laboratory Fire / Electrical Short Circuit	Safety Manager
3	Chemical Risks	Risks chemical accidents	Chemical Leak / Pollution	Laboratory and Laboratory Supervisor
4	Occupational Safety Risks	Workplace accidents or injuries	Falls / Injuries / Accidents	Occupational Safety Officer
5	Natural Disaster Risks	Earthquakes, floods, storms	Earthquake / Floods / Storms	Emergency Team
6	Evacuation Risks	Evacuation failures	Ineffective Plans / Poor Training	Safety Manager
7	Air Quality Risks	Indoor air pollution	Poor Ventilation / Mold / Dust	Facilities Management
8	Waste Risks	Poor waste management	Riskous Waste / Pollution	Environmental Management
9	Environmental Sustainability Risks	Failure to comply with environmental standards	Excessive Energy Consumption / Environmental Violations	Vice President for Development and Social Responsibility
10	Food and Beverage Risks	Food contamination or poisoning	Food Poisoning / Spoiled Food	Facilities Management

5.1.10 Competition Risks

Definition

Risks associated with competition in the higher education market. This category is particularly important for private universities due to their reliance on attracting students and competing with other universities.

Types of Competition Risks

No.	Type of risk	Description	Examples	Official
1	Risks of new entrants	The entry of new private universities or international branches	Opening of new universities / Branches of international universities	Planning Department
2	Risks of competitive pricing	Tuition price wars	Significant discounts from competitors / Attractive scholarships	Finance Committee
3	Risks of competitor quality	Significant improvements in quality by competitors	Competitors obtaining international accreditations / Improved rankings	Vice President for Academic Affairs
4	Risks of competitive	Strong marketing	Massive advertising	Marketing

	marketing	campaigns by competitors	campaigns / Innovative marketing strategies	Department
5	Risks of talent acquisition	Attraction of distinguished faculty members by competitors	Faculty transfers to competitors / Better offers	Human Resources
6	Risks of new programs	Launching of innovative and attractive programs by competitors	Distinguished programs / Rare specializations	Vice President for Academic Affairs
7	Risks of competitive alliances	Alliances between competitors or with external entities	Strategic partnerships / Mergers	University President
8	Risks of competitive innovation	Technological or academic innovations by competitors	Advanced educational platforms / New teaching methods	Vice President for Development and Community Responsibility

5.1.11 Sustainability Risks

Definition

Risks related to the university's ability to continue operating and growing in the long term.

Types of Sustainability Risks

No.	Type of risk	Description	Examples	Official
1	Financial sustainability risks	Inability to achieve financial sustainability	Ongoing losses / Depletion of reserves	Financial Director
2	Program demand risks	Decreased demand for university programs	Declining number of applicants / Undesirable programs	Admissions and Registration
3	Innovation and development risks	Inability to innovate and develop	Stagnation / Failure to keep pace with developments	Vice President for Development and Community Responsibility
4	Sustainable expansion risks	Unplanned expansion that impacts sustainability	Unprofitable branches / Failed investments	University President
5	Sustainable human resources risks	Inability to build a sustainable workforce	High turnover / Failure to attract talent	Human Resources
6	Infrastructure risks	Outdated or inadequate infrastructure	Outdated buildings / Dilapidated equipment	Facilities Management
7	Sustainable partnership risks	Failure to build sustainable strategic partnerships	Short-term partnerships / Failure to renew	Cooperation and Knowledge Exchange
8	Demographic changes risks	Changes in student demographics	Decreasing age group / Changing interests	Strategic Planning

5.2 Risk Classification Summary

Total Risks Identified: 136 types of risks distributed across 6.2 main categories

- **Strategic Risks:** 12 types
- **Financial Risks:** 15 types

- **Operational Risks:** 6.2 types
- **Academic and Research Risks**: 15 types
- **Reputational Risks:** 10 types
- **Human Resources Risks:** 12 types
- **Technical and Cyber Risks:** 15 types
- **Legal and Regulatory Risks**: 10 types
- **Health and Environmental Risks**: 10 types
- **Competitive Risks:** 8 types
- **Sustainability Risks:** 8 types

Note: This classification is comprehensive and covers all potential risks. Each department within the university should focus on the risks directly relevant to its work.

Chapter VI
Risk Management Processes

Overview: This section outlines the systematic and integrated processes for risk management in accordance with international standards, with detailed procedures and practical tools that can be immediately applied.

6.1 Risk Identification Process

6.1.1 Introduction

Risk identification is the ongoing and systematic process of identifying, recognizing, and describing risks that may affect the achievement of the university's objectives. This process must be comprehensive and continuous.

6.1.2 Risk Identification Objectives

- **Comprehensiveness:** Identifying all potential risks without exception
- **Documentation:** Documenting risks in a systematic and organized manner
- **Continuous Updating:** Periodic review to ensure the detection of emerging risks
- **Participation:** Engaging all management and operational levels

6.1.3 Sources of risk

Source type	Description	Examples
Internal sources	Risks arising from within the university	Weak systems / Lack of skills / Mismanagement
External sources	Risks from the surrounding environment	Organizational changes / Competition / Natural disasters
Strategic sources	Related to strategic decisions	Unplanned expansion / Faulty partnerships
Operational sources	Related to daily operations	Process errors / System failures
Technical sources	Related to technology and information	Cyberattacks / System failures
Human sources	Related to human behavior	Human error / Fraud / Misuse

6.1.4 Risk Assessment Methods and Techniques

A. Brainstorming Sessions

Description: Structured sessions that bring together experts and stakeholders to collectively identify risks.

Steps:

1. Identify participants (leaders, executives, experts)
2. Define the scope (specific sector or the entire university)

3. Determine the duration of the brainstorming session (number of hours)
4. Document all identified risks
5. Classify and prioritize risks
Recommended frequency: One session every 6 months per sector

B. Structured Interviews
Description: Individual interviews with stakeholders to understand risks from their perspective.

Key questions:
• What are the biggest threats to achieving your goals?
• What events could disrupt your work?
• What are the weaknesses in your processes?
• What opportunities might we miss?
Target audience: Deans, department heads, section chiefs, executive staff

C. Surveys and Checklists
Description: Standardized questionnaires widely distributed to gather information about risks.
Example: Operational Risk Checklist
• Are there documented procedures for all operations?
• Are procedures reviewed regularly?
• Are there data backups?
• Are there contingency plans for critical operations?
• Are staff trained on the procedures?

D. Scenario Analysis
Description: Developing potential scenarios for future events and identifying the associated risks.
Example: Scenario: "30% decrease in student enrollment"
• **Financial Risks:** Revenue shortfall, difficulty meeting obligations
• **Operational Risks**: Excess resources, excess capacity
• **Human Resources Risks:** Need for staff reductions
• **Reputational Risks**: Doubts about the university's quality

E. Historical Data Analysis
Reviewing past incidents and risks encountered by the university or similar universities.

F. Review of documents and records
• Internal and external audit reports
• Academic accreditation reports
• Student and parent complaints
• Accident and malfunction reports
• Meeting and committee minutes

6.1.5 Risk identification workshops

Workshop Type	Objective	Participants	Frequency

Strategic Workshop	Identify strategic risks	University Council, Senior Administration	Annually
Operational Workshop	Identify operational risks	Department Directors, Department Heads	Every 6 months
Technical Workshop	Identify technical and cyber risks	Information Technology Team, Information Security	Quarterly
Academic Workshop	Identify academic risks	Deans of Colleges, Department Heads	Every 6 months

6.1.6 Documenting Identified Risks

Each identified risk must be documented in the Risk Register, including:

- Risk Number: A unique identifier such as (ST-001, FN-012)
- Risk Name: A brief description
- Detailed Description: A clear explanation of the risk
- Category: Risk classification (strategic, financial, operational, etc.)
- Root Cause: What could cause this risk?
- Potential Impact: What are the consequences if it occurs?
- Risk Owner: Who is responsible for managing the risk?
- Date Identified: When was the risk identified?
- Status: Active / Under Observation / Closed

6.1.7 Identifying Emerging Risks

Emerging risks are new or evolving risks that are difficult to identify but may have a significant impact. The following must be monitored:

- Technological developments: artificial intelligence, distance learning
- Social changes: student expectations, the labor market, societal values
- Economic shifts: recession, inflation, exchange rates
- Regulatory changes: new laws, updated accreditation standards
- Political developments: government policies, international relations
- Environmental shifts: climate change, environmental awareness

Monitoring mechanism: A "Re-emerging Risks Monitoring" team will meet every three months to review developments and identify new risks.

6.1.8 Performance indicators for the identification process

Indicator	Objective	Frequency
Number of newly identified risks	10 new risks every quarter	Annual
Percentage of units involved in risk identification	100% of units	Semi-annual
Number of workshops conducted	≥ 4 workshops annually	Annual
Percentage of risks fully documented	100%	Monthly
Average time for risk documentation after identification	≤ 5 working days	Monthly

6.2 Risk Analysis & Assessment

6.2.1 Introduction

Risk analysis and assessment is the process of understanding the nature of risks and determining their level. This process includes estimating the probability of occurrence and the potential impact of each risk.

6.2.2 Types of Analysis

A. Qualitative Analysis

Using descriptive measures to determine the probability and impact of risks. Suitable for rapid assessment and when sufficient quantitative data are unavailable.

Likelihood Measure

Level	Rating	Description	Expected frequency:
1	Very rare	Extremely low probability	Once every 10 years or more
2	Rare	May occur in exceptional circumstances	Once every 5-10 years
3	Possible	May occur occasionally	Once every 2-5 years
4	High	Expected to occur in most circumstances	Once every 1-2 years
5	Almost certain	Expected to occur in most cases	Once or more per year

Impact

Level	Rating	Financial impact	Reputational impact	Operational impact
1	Slight	Less than 100,000 riyals	Limited local impact	Minor outage (less than 24 hours)
2	Low	100,000 riyals – 500,000 riyals	Local media coverage	Outage (1-3 days)
3	Moderate	500,000 riyals – 1 million riyals	National media coverage	Outage (3-7 days)
4	Large	1 – 5 million riyals	Significant reputational damage	Outage (1-4 weeks)
5	Catastrophic	More than 5 million riyals	Threat to the university's existence	Outage (more than a month)

B. Quantitative Analysis

Using data and mathematical models to numerically calculate the probability and impact of risks. Used for critical and strategic risks.

Main quantitative methods:
Expected Monetary Value (EMV): EMV = Probability × Financial Impact
Monte Carlo Simulation: Running thousands of scenarios to determine the range of possible outcomes
Sensitivity Analysis: Examining the effect of changing a single variable on the outcome

Decision Tree Analysis: Evaluating different options using multiple probabilities

6.2.3 Risk Assessment Matrix
5x5 Colored Matrix

Probability Impact	Slight (1)	Simple (2)	Average (3)	Large (4)	Catastrophic (5)
Almost certain (5)	Moderate 5	High 10	High 15	Critical 20	Critical 25
Probable (4)	Low 4	Medium 8	High 12	High 16	Critical 20
Possible (3)	Low 3	Low 6	Average 9	High 12	High 15
Rare (2)	Low 2	Low 4	Low 6	Medium 8	High 10
Very rare (1)	Low 1	Low 2	Low 3	Low 4	Moderate 5

Interpreting the matrix and response procedures

Risk level	Range	Color	Required Action
Low	1 - 5	Green	Periodic Monitoring. No immediate action required. Semi-annual Review.
Moderate	6 - 9	Yellow	Active Monitoring. Development of a remediation plan within 3 months. Quarterly Review.
High	10 - 16	Brown	Immediate action. A resolution plan within one month. Monthly review. Reporting to senior management.
Critical	20 - 25	Red	Immediate and urgent action. Senior management intervention. Immediate action plan. Weekly review.

6.2.4 Risk Priority Classification
After assessing all risks, they are prioritized as follows:
1. Critical: Requires immediate action and significant resources
2. High: Requires planning and treatment within a short timeframe
3. Medium: Requires scheduled treatment
4. Low: Monitored periodically

6.2.5 Risk Heat Map
A visual representation of all risks on a single matrix to identify concentrations and patterns.
Example: Future University Strategic Risk Map
ST-001: Decreased Student Enrollment (Probability: 4, Impact: 5) = 20 (Critical)
FN-003: Non-Collection of Fees (Probability: 3, Impact: 4) = 12 (High)
AC-002: Non-Renewal of Accreditation (Probability: 2, Impact: 5) = 10 (High)
OP-005: Power Outage (Probability: 3, Impact: 3) = 9 (Moderate)
HR-007: Staff Absence (Probability: 4, Impact: 1) = 4 (Low)

6.2.6 Aggregate Risk Assessment
Assess the total risks at the university level to understand the overall "risk appetite":
• Total Critical Risks: Number of red risks
• Total Financial Exposure: Sum of expected monetary values for all risks

• Sectoral Concentration: Which sectors face the highest concentration of risks?

6.2.7 Review and Update of Assessments

Risk assessments should be reviewed regularly:

Type of review	Purpose	Frequency
Periodic review	Updating assessments based on developments	Quarterly (for high risk) / Semi-annually (for medium risk)
Eventual review	Following significant changes or events	When needed
Comprehensive review	reassessment of all risks	Annually

6.3 Risk Management

6.3.1 Introduction

Risk management is the process of selecting and implementing measures to modify risks. The goal is to reduce risks to an acceptable level or to capitalize on potential opportunities.

6.3.2 The Four Strategies for Risk Management

No.	Strategy	Description	When to use:	Examples
1	Avoid	Eliminating the risk by canceling the activity that caused it	Critical risks that cannot be reduced	Not opening a branch in an unsafe area / Canceling an unprofitable program
2	Reduce/Mitigate	Taking measures to reduce the likelihood or impact	Most common - for medium and high risks	Staff training / Security systems / Preventive measures
3	Transfer	Transferring the risk or consequences to a third party	Risks that can be insured or outsourced	Insurance / Contracts / Outsourcing
4	Accept	Accepting the risk without taking further action	Low risk or cost-effective treatment that exceeds the benefit	Low impact risk / Acceptable risk within risk appetite

6.3.3 Choosing the appropriate strategy

A matrix for selecting a treatment strategy:

Risk level:	Recommended strategy:	Actions
Critical (20-25)	Avoid or drastically reduce	Suspension of activity / Implementation of strict controls / Significant investment in processing
High (10-16)	Reduce or relocate	Implementation of controls / Security / Improvement of procedures
Moderate (6-9)	Reduce or accept with monitoring	Moderate measures / Active monitoring / Contingency plans
Low (1-5)	Accept with monitoring	Documentation only / Periodic review / No additional actions

6.3.4 Developing a Risk Treatment Plan

A risk treatment plan should include the following elements:
1. Risk Number and Name: Risk reference in the risk register
2. Selected Strategy: Avoid/Minimize/Transfer/Accept
3. Specific Actions: Detailed steps
4. Responsible Person or Department: The person or department responsible
5. Required Resources: Budget, personnel, equipment
6. Timeline: Start and end dates
7. Success Indicators: How we measure the effectiveness of the management
8. Residual Risk: The level of risk after management

6.3.5 Practical Examples of Treatment Plans

Example 1: "Decline in Student Numbers" Treatment Plan (ST-001)

Risk:	**Decreased student admissions (ST-001)**
Initial Assessment:	Probability: 4 (likely) × Impact: 5 (catastrophic) = 20 (critical)
Strategy:	Risk reduction (Reduce)
Actions:	1. Intensive marketing campaign (500,000 riyals) 2. Development of new programs in demand in the job market 3. Improvement of scholarships 4. Partnerships with major companies 5. Improvement of university rankings
Responsible Party:	Decreased student admissions (ST-001)
Budget:	Probability: 4 (likely) × Impact: 5 (catastrophic) = 20 (critical)
Timeline:	Risk reduction (Reduce)
Success Indicators:	- Increase in applicants by 20% - Improved acceptance rate - Increased awareness of the university
Residual Risk:	Probability: 2 x Effect: 4 = 8 (Average)

6.3.6 Preventive, detection, and corrective controls

Control Type	**Description and Objective**	**Examples**
Preventive	Preventing danger from occurring.	-Policies and Procedures -Access Permissions -Segregation of Duties -Training -Routine Maintenance
Detective	Detecting events as they happen.	- Monitoring and inspection - Internal auditing - Alarm systems - Exceptional reports - Ongoing auditing
Corrective	Remediating the impact	- Business continuity plans

	after a danger has occurred.	- Recovery from backups - Insurance - Contingency plans - Recovery procedures

6.3.7 Monitoring Treatment Effectiveness

After treatment implementation, its effectiveness should be monitored through: - Key Performance Indicators (KRIs): Risk indicators
- Periodic Testing: of systems and controls
- Incident Reports: Analysis of actual incidents
- Periodic Reviews: Ongoing evaluation

6.4. Monitoring and Review

6.4.1 Introduction

Monitoring and review are ongoing processes to ensure that risk management is effective and keeps pace with changes. They must be systematic and regular.

6.4.2 Objectives of Monitoring and Review

• Verify the effectiveness of risk management plans
• Identify new and emerging risks
• Update risk assessments
• Ensure compliance with policies
• Continuously improve risk management processes

6.4.3 Monitoring Levels

Level	Responsible Party	Frequency	Tools
Strategic level	University Council Higher Risk Committee	Quarterly	Dashboard Reports Comprehensive review
Management level	Risk Management Senior Management	Monthly	Risk Log Performance Indicators Incident Reports
Executive level	Departmental Risk Officers Risk Owners	Weekly/Daily	Daily Inspections Field Observations Immediate Reports

6.4.4 Monitoring Mechanisms

A. Key Risk Indicators – KRIs

Measures that provide early warnings of increased risk levels. Examples:

Risks	Risk Index (KRI)	Critical Threshold

Decreasing student numbers	Number of Admissions and Registrations	Greater than 15% year-on-year decrease
Liquidity risks	Current Liquidity Ratio	Greater than 1.2
Cyberattacks	Number of Hacking Attempts	More than 100 attempts/day
Student satisfaction	Student Satisfaction Index	Less than 70%
Staff turnover	Employee Turnover Rate	More than 15% year-on-year decrease

B. Risk Dashboard

Monthly dashboard including:

• Risk distribution: Number of risks by level (critical, high, medium, low)
• Risk trends: Are risks increasing or decreasing?
•Top 10 risks: Highest rated risks
• Remediation plan status: Percentage of completion
• Risks exceeding thresholds: Risks that have crossed thresholds
• New risks: Newly identified risks

C. Incident and loss reports

Documentation and analysis of all incidents that occur to understand risk patterns and improve controls.

D. Internal and external audits

• Internal audit: Independent assessment of risk management effectiveness (semi-annual)
• External audit: Assessment by independent third parties (annual)

6.4.5 Comprehensive periodic review

A comprehensive annual review including:

1. Reassessment of all risks
2. Review of the effectiveness of remediation plans
3. Update of policies and procedures
4. Assessment of risk management culture
5. Review of the organizational structure for risk management
6. Assessment of compliance with international standards

6.4.6 Reporting and Escalation

Risk reporting protocol:

Risk level	Reports are to be submitted to:	Timeline	Method
High	University President + Higher Committee + University Council	Immediate (within 24 hours)	Urgent Report + Emergency Meeting
Moderate	Risk Management + Higher Committee	Within 3 days	Report

Low	Risk Management	Included in the monthly report	Monthly Report
Critical	Risk Unit Officer	Included in the periodic report	Documentation in the Log

6.4.7 Continuous Improvement

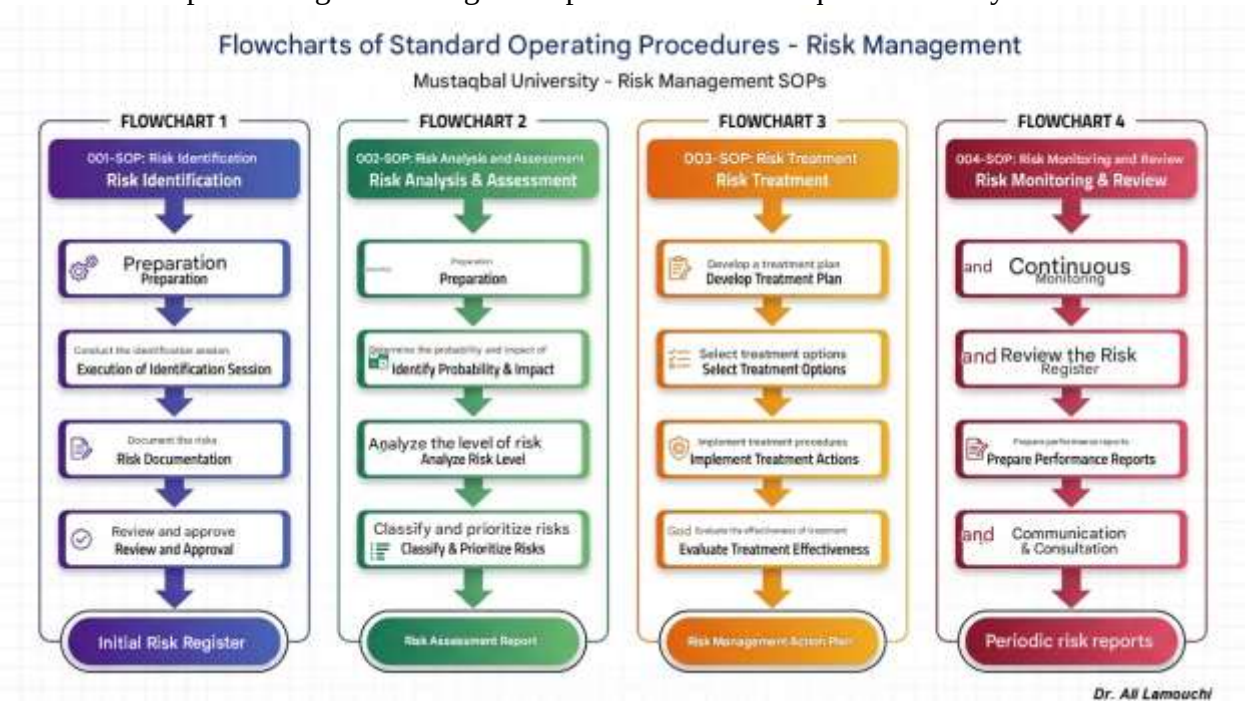
Using monitoring and review results to improve:

- Risk identification processes
- Accuracy of risk assessment
- Effectiveness of remediation plans
- Tools and models used
- Risk management culture at the university

6.5 Detailed Operating Procedures for Each Stage

6.5.1 Overview

This section contains detailed Standard Operating Procedures (SOPs) for each stage of risk management. These procedures are designed to be a practical, step-by-step guide for all those involved in implementing risk management processes at Mustaqbal University.

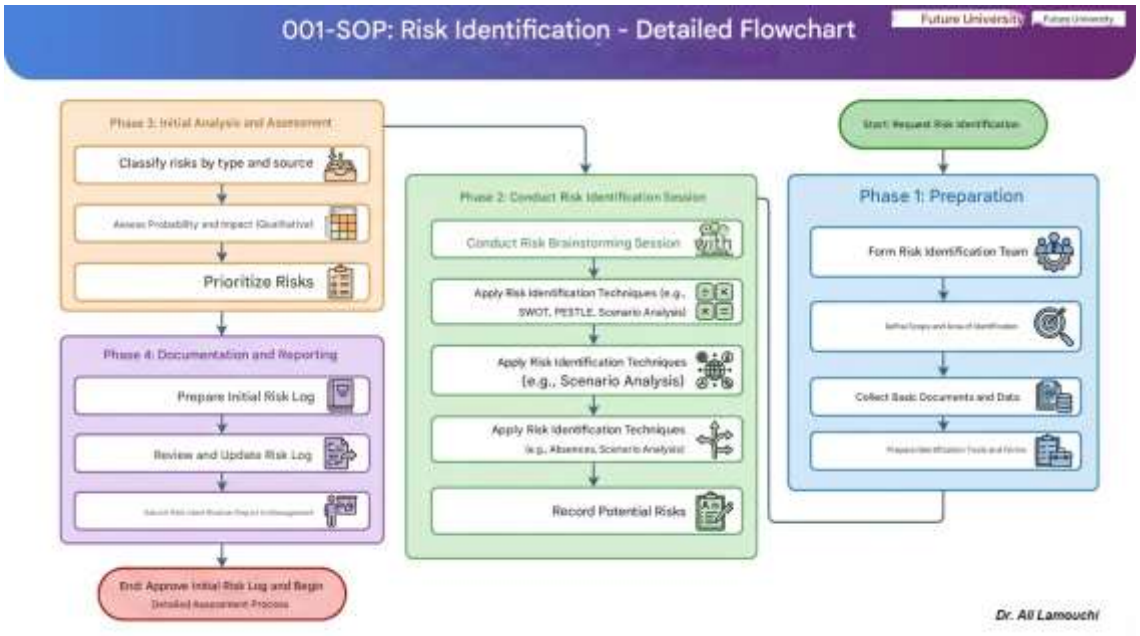


6.5.1 Standard Operating Procedure No. (1): Risk Identification

Action Number	SOP-RM-001
Action Title	Risk Identification Procedures
Purpose	Providing a standardized methodology for identifying and documenting all potential risks that may affect the achievement of Future University's objectives.

Scope	All academic and administrative units within the university.
Responsible Authority	Central Risk Management Unit in collaboration with the risk coordinators in the units.
Repetition	Quarterly (or as needed)
Version Number	1.0
Version Date	January 2025

Detailed procedures



Step 1: Preparation and setup

No.	Action	Official	Outcomes
1.1	Define the scope of the risk assessment process (unit, department, project, activity)	Unit Manager / Risk Coordinator	Scope Definition Document
1.2	Review the unit's strategic and operational objectives	Risk Coordinator	List of Targeted Objectives
1.3	Form the risk assessment team (including representatives from all relevant departments)	Unit Manager	Team Formation Decision
1.4	Gather relevant information and documentation (strategic plans, past reports, lessons learned)	Risk Coordinator	Basic Information Package
1.5	Set the date and location for the risk assessment session	Risk Coordinator	Meeting Invitation
1.6	Send invitations and preparatory materials to team members	Risk Coordinator	Confirmation of Materials Receipt

Step 2: Conducting a risk assessment session

No.	Action	Official	Outcomes
2.1	Opening the session and clarifying the objectives and methodology	Risk Manager	Attendance documentation
2.2	Reviewing the unit's strategic and operational objectives	Risk Unit Officer	Meeting minutes
2.3	Applying brainstorming techniques to identify potential risks	All Members	Preliminary risk list
2.4	Using a standardized checklist to ensure all risk categories are covered	Risk Coordinator	Completed checklist
2.5	Conducting a SWOT analysis to identify risks and opportunities	Risk Unit Team	SWOT matrix
2.6	Reviewing lessons learned from past incidents	Risk Coordinator	Historical risk list
2.7	Classifying risks by category (strategic, financial, operational, etc.)	Risk Unit Team	Classified risk list

Step 3: Documenting the identified risks

No.	Action	Official	Outcomes
3.1	For each identified risk, record: risk code, description, source, and potential causes.	Risk coordinator	Initial risk assessment
3.2	Determine the potential impact of each risk on the targets.	Team	Description of potential effects
3.3	. Document early warning indicators for each risk. Identify the unit or department affected by each risk.	Team	List of early indicators
3.4	Identify the unit or department affected by each risk.	Risk coordinator	Affected entities map
3.5	.Enter all data into the standardized risk identification form.	Risk coordinator	Completed risk assessment model

Step 4: Review and approval

No.	Action	Official	Outcomes
4.1	Review the risk list identified by the unit manager	Unit Manager	Review Risk List
4.2	Submit the risk list to the Central Risk Management Unit for review	Risk Coordinator	Risk Identification Report
4.3	Verify the completeness of the data and ensure there are no duplicates with risks from other units	Risk Unit	Audit Report
4.4	Approve the risk list by the Central Risk Unit manager	Risk Unit Manager	Approved List

4.5	Include the risks in the university's comprehensive risk register	Risk Unit	Updated Risk Register
4.6	Issue unique reference numbers (Risk IDs) for each risk	Risk Unit	Reference Numbers
4.7	Review the risk list identified by the unit manager	Unit Manager	Review Risk List

Tools and Forms Used

- Risk Identification Form (RM-F01)
- Comprehensive Risk Category Checklist (RM-CL01)
- Risk Identification Meeting Minutes (RM-F02)
- SWOT Matrix (RM-T01)
- Early Indicators List (RM-F03)

Responsibilities

Role	Responsibilities:
Risk Unit Officer	Leading the risk identification process Forming the risk identification unit team Reviewing and approving the risk list
Risk coordinator	Organize risk identification sessions Document identified risks Continue updating the risk register
Team members	Active participation in sessions Presenting information and data Identifying risks in their areas of expertise
Central Risk Unit	Review the submitted risk lists Verify consistency and comprehensiveness Integrate the risks into the overall register

Performance Criteria

Success Indicators:
- Comprehensiveness: Coverage of all major risk categories (minimum 10 categories)
- Timeliness: Completion of the identification process within 15 working days
- Quality: Clarity and completeness of each risk description (at least 80% of the required data)
- Participation: Participation of representatives from all relevant departments
- Documentation: 100% of identified risks documented in the register

Key Notes

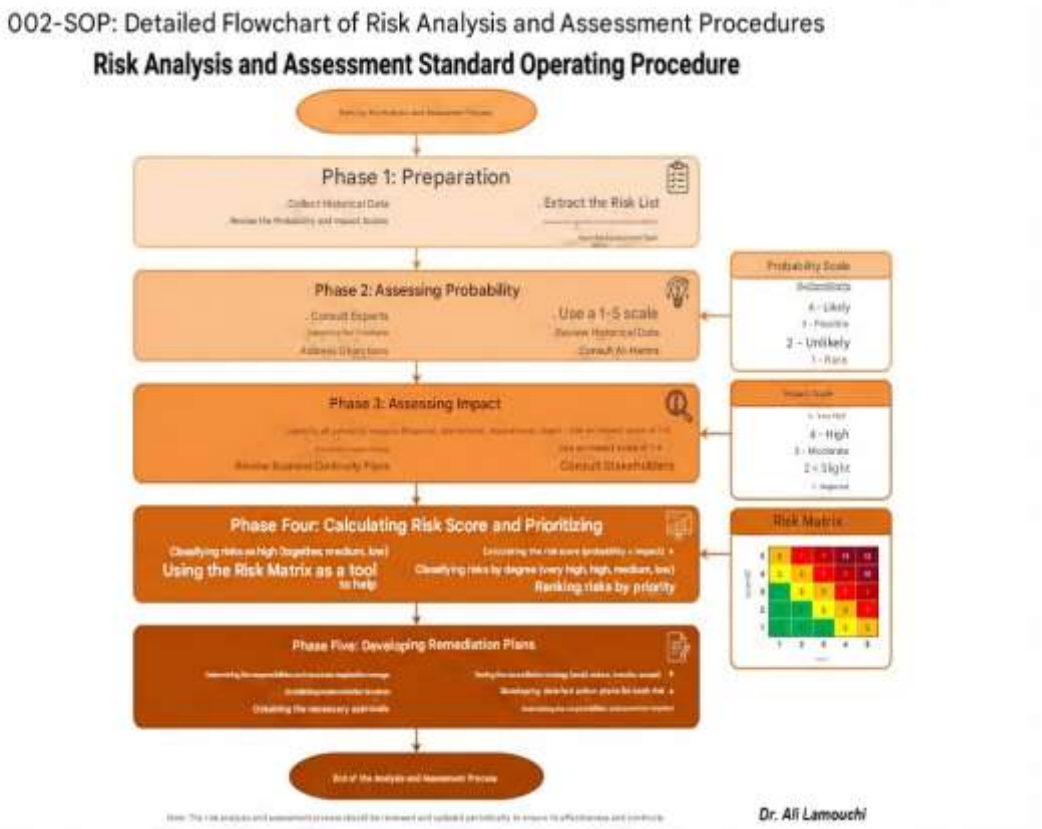
- The risk identification process should be ongoing, not a one-time event.
- New risks can be identified at any time as new information becomes available.

• All levels should be involved in the risk identification process.
• Focus on risks that impact goal achievement, not just routine risks.
• The risk register should be updated immediately upon the identification of new risks.

6.5.2 Standard Operating Procedure No. (2): Risk Analysis and Assessment

Action Number	SOP-RM-002
Action Title	Risk Analysis and Assessment Procedures
Purpose	Provide a standardized methodology for analyzing and assessing identified risks to prioritize them and allocate appropriate resources for their management.
Scope	All risks listed in the risk register.
Responsible Authority	Central Risk Management Unit and Risk Coordinators
Repetition	Quarterly (with immediate review of critical risks).
Version Number	1.0
Version Date	January 2025

Detailed Procedures



Step 1: Preparation

No.	Action	Official	Outcomes

1.1	Extracting the list of risks from the risk register that require assessment	Risk Unit	Targeted Risk List
1.2	Identifying risks requiring quantitative or qualitative assessment	Risk Unit Officer	List Classified by Assessment Type
1.3	Assembling an assessment team for each risk (field experts)	Risk Coordinator	List of Participating Experts
1.4	Collecting relevant historical and statistical data for each risk	Risk Analyst	Historical Data Pack
1.5	Reviewing the approved probability and impact measures	Risk Coordinator	Standardized Measurement Tables

Step 2: Probability assessment

No.	Action	Official	Outcomes
2.1	Determine the probability of risk occurrence using the established scale (1-5)	Assessment Team	Probability Grade
2.2	Review historical data for similar events	Risk Analyst	Analysis of historical events
2.3	Consult with experts in the field to verify estimates	Risk Coordinator	Documented expert opinions
2.4	Define the reference time period for the assessment (one year)	Assessment Team	Timeframe
2.5	Document the assumptions and bases used in the probability assessment	Risk Analyst	Assumptions document

The adopted probability scale:

Grade	Level	Description	Expected frequency
5	Almost certain	The danger is highly likely	More than once a year
4	High	The danger is probable	Once a year
3	Probable	The danger may occur	Once every 2-3 years
2	Rare	The danger is unlikely	Once every 3-5 years
1	Very rare	The danger rarely occurs	Less than once every 5 years

Step 3: Impact assessment

No.	Action	Official	Outcomes
3.1	Identify all potential impacts of the risk (financial, operational, reputational, legal, etc.)	Assessment Team	List of potential impacts
3.2	Assess the impact score for each dimension using the established scale (1-5)	Assessment Team	Impact score for each dimension
3.3	Determine the overall impact (the highest impact across all dimensions)	Risk Analyst	Overall impact score
3.4	Estimate the financial impact in monetary	Financial Analyst	Financial estimate

	terms (if applicable)		
3.5	Document potential scenarios for the risk to occur	Assessment team	Scenario document

The adopted probability scale:

Grade	Level of impact	Financial impact	operational impact	reputational impact	legal impact
5	Catastrophic	More than 5 million riyals	Complete work stoppage	Permanent reputational damage	Serious violations and penalties
4	Large	1-5 million riyals	Major work disruption	Severe reputational damage	Significant violations and fines
3	Medium	500-1 million riyals	Work delay	Limited reputational damage	Minor violations
2	Simple	100,000-500,000 riyals	Minor impact	Minor impact on reputation	Warnings
1	Minor	Less than 100,000 riyals	Very minimal impact	No impact on reputation	No legal consequences

Step 4: Calculating the risk level

No.	Action	Official	Outcomes
4.1	Calculate the initial risk level = Probability × Impact	Risk Analyst	Initial risk score
4.2	Classify the risk according to the matrix: Critical (20-25), High (12-19), Moderate (6-6.2), Low (1-5)	Risk Analyst	Risk classification
4.3	Assign a color to the risk in the log (red, orange, yellow, green)	Risk Coordinator	Color coding
4.4	Compare the risk level with the acceptable risk level (Risk Appetite)	Risk Unit Officer	Comparative report
4.5	Determine whether the risk is acceptable or requires intervention	Risk Unit Officer	Treatment decision

Step 5: Setting priorities

No.	Action	Official	Outcomes
5.1	Rank risks in descending order of risk level	Risk Analyst	: Prioritized Checklist
5.2	Prioritize treatment: Immediate (critical), Urgent (high), Planned (medium), Routine	Risk Unit Officer	Prioritized Schedule

	(low)		
5.3	Allocate resources according to priorities (budget, team, time)	High-Level Risk Committee	Resource Allocation Plan
5.4	Define the target timeframe for initiating treatment	Risk Coordinator	Timeline

• Priority criteria:

Risk level	Risk description	Priority	Treatment start time	Level of interest
(20-25)	Critical	Immediate	Within 24 hours	University President + Higher Committee
(10-16)	High	Urgent	Within a week	Higher Risk Committee
(6-9)	Moderate	Planned	Within a month	Risk Management
(1-5)	Low	Routine	As part of the annual plan	Risk Coordinator

Step 6: Documentation and Certification

No.	Action	Official	Outcomes
6.1	Enter all assessment results into the risk register	Risk Coordinator	Updated Risk Register
6.2	Prepare a comprehensive risk assessment report	Risk Unit	Assessment Report
6.3	Review of the assessment by the Higher Risk Committee	Supreme Committee	Audit Minutes
6.4	Approval of the assessment by the Head of the Higher Committee	Committee Chair	Accreditation Decision
6.5	Distribute the assessment report to relevant parties	Risk Coordinator	Distribution Lists
6.6	Update the heat risk map (Heat Map)	Risk Analyst	Updated Risk Map

6.5.3 Tools and Models Used

• Risk Assessment Model (RM-F04)
• Risk Assessment Matrix (RM-M01)
• Quantitative Risk Assessment Model (RM-F05)
• Heat Map of Risks (RM-V01)
• Risk Assessment Report (RM-R01)

Responsibilities

Role	Responsibilities:
Supreme Committee	Review and approve risk assessments Define acceptable risk levels Prioritize risk management
Risk Management	Supervising the evaluation process

Director	Verifying the validity of the evaluations.
Risk Analysis and Assessment Unit Team	Conducting quantitative and qualitative analyses Calculating risk levels Preparing reports and matrices
Risk Unit Manager	Providing professional assessments Participating in assessment sessions Reviewing assessment results

Performance Criteria

Success Indicators:

• Accuracy: Assessment accuracy (comparison of assessments with actual results) must be greater than 85%
• Timeliness: Assessment must be completed within 10 working days of risk identification
• Consistency: The same criteria and metrics must be used for all risks
• Comprehensiveness: All dimensions of impact (financial, operational, reputational, legal) must be assessed
• Documentation: 100% of assessments must be documented, including the basis and assumptions

Key Notes

• Risks must be reassessed periodically (at least quarterly)
• If a material change occurs in the internal or external environment, the assessment must be reassessed immediately
• Critical and high risks require monthly review
• Quantitative assessment of financial risks should be used whenever possible
• It is preferable to involve more than one expert in assessing key risks to ensure accuracy
• The assessment must take into account existing controls

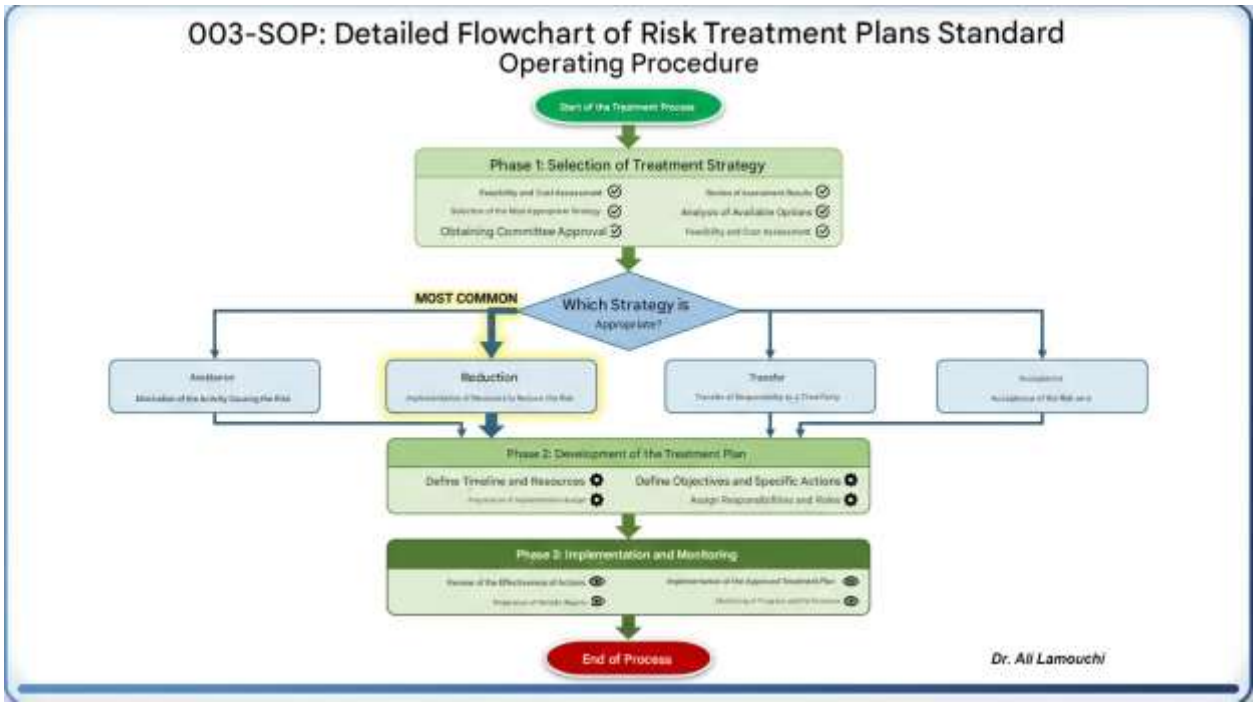
6.5.4 Standard Operating Procedure No. (3): Risk Treatment Plans

Action Number	SOP-RM-003
Action Title	Procedures for Preparing and Implementing Risk Management Plans
Purpose	Providing a standardized methodology for developing, implementing, and monitoring risk management plans to reduce the impact and likelihood of risks.
Scope	All risks requiring management (not acceptable within the acceptable risk level).
Responsible Authority	Risk owners in collaboration with the Central Risk Management Unit.
Repetition	When needed (based on assessment results).
Version Number	1.0
Version Date	January 2025

Risk Treatment Strategies

Strategy	Description	When to use	Example
Avoid	Cancel the activity or decision causing the risk.	When the risk is critical and cannot be reduced to an acceptable level	Cancel an ineffective academic program
Reduce	Implement measures to reduce the likelihood or impact of the risk.	most high and medium risks.	Train staff, improve procedures
Transfer	Transfer responsibility for the risk to a third party.	when another party can manage the risk more efficiently	Insurance, outsourcing
Accept	Accept the risk without taking further action.	when the risk is low or the cost of treatment exceeds the benefit.	Low risk within acceptable risk levels

Detailed procedures



Step 1: Choosing a treatment strategy

No.	Action	Official	Outcomes
1.1	Review the risk assessment results (probability, impact, risk level)	Risk Owner	Evaluation data
1.2	Analyze available options for addressing	Risk Management	List of options

	the risk (avoidance, reduction, transfer, acceptance)	Team	
1.3	Evaluate the feasibility, cost-benefit analysis of each option	Financial Analyst + Risk Owner	Feasibility analysis
1.4	Select the most appropriate strategy based on the analysis	Risk Owner + Risk Coordinator	Strategy decision
1.5	Obtain approval from the Higher Risk Committee (for critical and high risks)	Risk Owner	Committee approval

Step 2: Develop a detailed treatment plan

No.	Action	Official	Outcomes
2.1	Define the specific actions required to implement the strategy.	Risk Owner	Action List
2.2	Assign responsibility for each action.	Risk Owner	Responsibilities Matrix
2.3	Develop a detailed timeline for each action (start and end dates).	Risk Coordinator	Timeline
2.4	Estimate the required resources (budget, human resources, equipment).	Risk Owner	Required Resources List
2.5	Define key performance indicators (KPIs) to measure the plan's effectiveness.	Risk Coordinator	Performance Indicators List
2.6	Estimate the residual risk level after plan implementation.	Risk Analyst	Residual Risk Assessment
2.7	Document the plan in a standardized risk management plan template.	Risk Coordinator	Remediation Plan Document

Step 3: Adopt the treatment plan

No.	Action	Official	Outcomes
3.1	The plan is reviewed by the Central Risk Unit Manager.	Risk Management Unit Manager	Audit Report
3.2	The availability of required resources (budget, staff) is verified.	Finance + Human Resources	Confirmation of Resource Availability
3.3	The plan is then submitted to the Higher Risk Committee for approval.	Risk Coordinator	Plan Report
3.4	The plan is approved by the Higher Committee (for critical and high risks).	Higher Committee	Approval Decision
3.5	Distributing the approved plan to all relevant parties	Risk Coordinator	Distribution Lists

Step 4: Implementing the treatment plan

No.	Action	Official	Outcomes
4.1	Begin implementing the procedures according to the established schedule.	Those responsible for implementation	Implementation Start Reports
4.2	Document all implemented procedures and their actual dates.	Risk Coordinator	Implementation Log
4.3	Track implementation progress periodically (weekly or monthly, depending on priority).	Risk Owner	Progress Reports
4.4	Address any obstacles or challenges encountered during implementation. Continuously update the implementation status in the risk log.	Risk Owner + Risk Unit	Corrective Action Plans
4.5	Begin implementing the procedures according to the established schedule.	Risk Coordinator	Updated Risk Log

Step 5: Monitoring and Follow-up

No.	Action	Official	Outcomes
5.1	Monitoring the Key Performance Indicators (KPIs) defined in the plan	Risk Coordinator	KPI Reports
5.2	Measuring the effectiveness of implemented actions in reducing the risk level	Risk Analyst	Effectiveness Assessment
5.3	Reassessing the risk after completion of implementation	Assessment Team	Reassessment Report
5.4	Comparing the actual residual risk level with the target level	Risk Analyst	Comparison Report
5.5	If the target level is not achieved, developing an additional remediation plan	Risk Owner	Revised Action Plan
5.6	Submitting the final progress report to the Higher Committee	Risk Unit Officer	Achievement Report

Processing Priority Criteria

Risk level	Risk description	Priority	Treatment start time	Alocated resources
(20-25)	Critical	Immediate	Immediately - Within 2 weeks	Unlimited resources as needed
(10-16)	High	Urgent	Within 1-3 months	Large resources (80% of processing requests)
(6-9)	Moderate	Planned	Within 3-6 months	Limited resources (50% of requests)
(1-5)	Low	Routine	According to the annual	Basic resources only

			plan	

Tools and Forms Used

• Risk Treatment Plan Form (RM-F06)
• Cost-Benefit Analysis Form (RM-F07)
• Implementation Tracking Form (RM-F08)
• Residual Risk Assessment Form (RM-F09)
• Completion Report Form (RM-R02)

Responsibilities

Role	Responsibilities:
Risk Owner	Leading the development and implementation of the treatment plan Allocating necessary resources Monitoring implementation and resolving obstacles
Supreme Risk Committee	Approval of master treatment plans Allocation of budgets Review of progress reports
Risk Management	Supporting plan development Monitoring implementation Preparing reports
Implementation Officers	Implementing the specified procedures Documenting and reporting progress Coordinating with relevant parties

Performance Standards

Success Indicators:
• Plan Completion Rate: Over 90% of approved plans are fully implemented
• Schedule Adherence: Over 85% of actions are completed on time
• Remediation Effectiveness: Over 80% of plans achieve the target level of residual risk
• Resource Efficiency: Actual remediation cost < 6.20% of the estimated budget
• Risk Reduction: Average risk level reduction > 40%

Key Notes:

• Remediation plans must be realistic and feasible within available resources
• No single remediation plan is suitable for all risks – each plan must be tailored
• Focusing on preventative actions (reducing likelihood) is preferable to remedial actions (reducing impact)
• Remediation plans should be flexible and adaptable to changing circumstances
• Periodic review of the effectiveness of implemented actions is essential for continuous improvement
• Lessons learned from each remediation plan should be documented to improve future plans

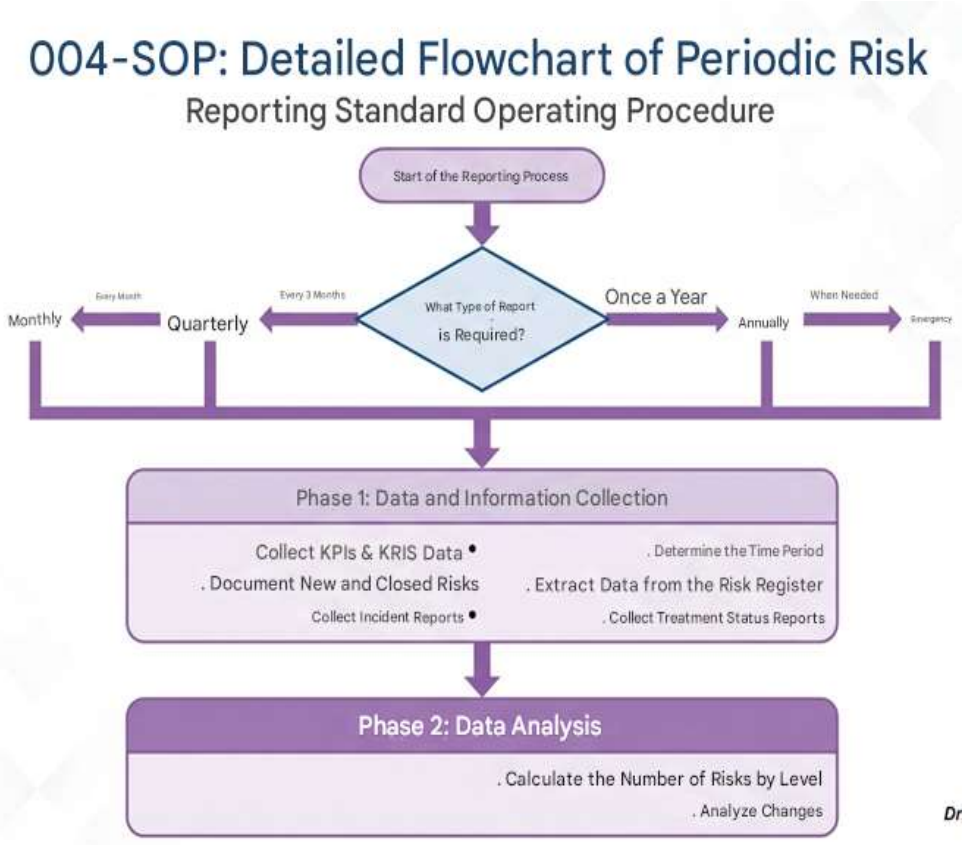
6.5.5 Standard Operating Procedure No. (4): Periodic Risk Management Reports

Action Number	SOP-RM-004
Action Title	Procedures for Preparing and Distributing Periodic Risk Management Reports
Purpose	Providing a standardized methodology for preparing and distributing periodic risk status reports to ensure transparency and accountability
Scope	All types of risk management reports (monthly, quarterly, annual, ad hoc)
Responsible Authority	Centralized risk management
Repetition	According to report type (monthly, quarterly, annual, or as required)
Version Number	1.0
Version Date	January 2025

Types of reports and their frequency

Report Type	Frequency	Recipients	Main Content Urgent
Monthly Report	Monthly (within 5 working days of the end of the month)	Higher Risk Committee	Critical and high risks Status of treatment plans Emerging risks
Quarterly Report	Quarterly	University President, Higher Committee	Comprehensive analysis of all risks, trends and insights Key performance indicators
Annual Report	Once a year	University Council, Higher Committee, Quality and Accreditation Department	Comprehensive annual review Risk management effectiveness assessment Strategic recommendations
Emergency Report	As needed (for critical emergencies)	University President, Higher Committee, Affected Parties	Emergency risk details Immediate actions Urgent recommendations
Processing Status Report	Weekly (for critical risks)	Risk Owner, Risk Management	Remediation Plan Obstacles and Challenges Next Steps

Detailed Procedures



Step 1: Data and information collection

No.	Action	Risk Coordinator	Outcomes
1.1	Defining the time period covered in the report	Risk Analyst	Specific time frame
1.2	Extracting data from the comprehensive risk register	Risk Coordinators	Risk log data
1.3	Collecting treatment status reports from risk owners	Risk Analyst	Processing status reports
1.4	Collecting Key Performance Indicator (KPI) and Key Risk Indicator (KRI) data	Risk Coordinator	KPIs & KRIs data
1.5	Documenting emerging and closed risks	Risk Coordinators	New and closed risk lists
1.6	Collecting incident and event reports related to risks	Risk Coordinator	Incident reports

Step 2: Data and Information Analysis

No.	Action	Official	Outcomes
2.1	Calculating the number of risks by	Risk Analyst	Risk statistics

	category and level		
2.2	Analyzing changes in risk levels compared to the previous period	Risk Analyst	Trend analysis
2.3	Evaluating the progress of implementing remediation plans	Risk Analyst	Treatment progress report
2.4	Analyzing the performance of Key Risk Indicators (KRIs)	Risk Analyst	KRI analysis
2.5	Identifying the most critical risks requiring urgent attention	Risk Unit Officer	Priority risk list
2.6	Analyzing the effectiveness of implemented remediation measures	Risk Analyst	Effectiveness report

Step 3: Report preparation

No.	Action	Official	Outcomes
3.1	Prepare an executive summary (1-2 pages) including key points	Risk Unit Officer	Executive Summary
3.2	Prepare a visual dashboard for key indicators	Risk Analyst	Dashboard
3.3	Document full details of critical and high-risk areas	Risk Coordinator	Detailed Tables
3.4	Prepare charts and matrices (heat map)	Risk Analyst	Charts and Matrices
3.5	Form recommendations and proposed actions	Risk Unit Officer	Recommendations List
3.6	Proofread the report for accuracy and completeness.	Risk Unit Officer	Auditor's Report
3.7	Prepare the final version using the standardized template.	Risk Coordinator	Final Report

Step 4: Review and approval

No.	Action	Official	Outcomes
4.1	Initial review by the Risk Management Director	Risk Management Director	Review Notes
4.2	Report revisions based on review feedback	Risk Coordinator	Revised Report
4.3	Presentation of the report to the Senior Risk Committee (for quarterly and annual reports)	Risk Management Director	Presentation
4.4	Approval of the report by the Chairman of the Senior Risk Committee	Committee Chair	Approved Report

Step 5: Distribution and Publishing

No.	Action	Official	Outcomes
5.1	Set the distribution list by report type	Risk Coordinator	Distribution list
5.2	Send the report to the target audience via	Risk Coordinator	Send notifications

	email		
5.3	Upload the report to the electronic document management system	Risk Coordinator	Web link
5.4	Prepare a presentation of the report (for quarterly and annual reports)	Risk Management Manager	Presentation
5.5	Keep a copy in the risk management unit archive	Risk Coordinator	Archive log

Step 6: Follow-up and feedback

No.	Action	Official	Outcomes
61	Follow up on the implementation of the report's recommendations	Risk Management	Recommendations Follow-up Table
6.2	Gather feedback from recipients on the report's quality and usefulness	Risk Coordinator	Feedback Form
6.3	Analyze the feedback and identify areas for improvement	Risk Management Manager	Improvement Report
6.4	Update report templates based on feedback	Risk Coordinator	Updated Templates

Standard Report Content

Comprehensive Report Elements:
• Executive Summary: Key Points and Recommendations (1 page)
• Dashboard: Key Indicators Visualized
• Risk Environment Overview: Number of Risks by Level and Category
• Critical Risks: Details of Critical Risks (Level 20-25)
• High Risks: Details of High Risks (Level 12-19)
• Status of Remediation Plans: Implementation and Completion Progress
• Emerging Risks: Newly Identified Risks
• Closed Risks: Risks Successfully Remediated
• Trends and Analysis: Timeframe Comparisons and Trends
• Performance Indicators: Key Performance Indicators (KPIs) & Key Risk Reductions (KRIs)
• Heat Map: Updated Heat Map
• Recorded Incidents: Incidents Related to Risks
• Recommendations: Proposed Actions
• Next Steps: Plan for the Next Period
• Appendices: Detailed Tables and Supporting Information

Tools and Templates Used

• Monthly Report Template (RM-T01)
• Quarterly Report Template (RM-T02)
• Annual Report Template (RM-T03)
• Emergency Report Template (RM-T04)
• Dashboard Template (RM-D01)
• Report Feedback Form (RM-F10)

Responsibilities

Role	Responsibilities:
Risk Management Director	General oversight of the reporting process Review and approval of reports Provision of strategic recommendations
Risk Analyst	Data collection and analysis Preparation of matrices and graphs Calculation of indicators and statistics
Risk Coordinator	Report drafting Coordination with stakeholders Distribution and publication of reports
Risk Owners	Providing processing status reports Commenting on risks within their respective areas Providing the required data on time

Performance Standards

Success Indicators:

• Timeliness: 100% of reports issued on schedule
• Accuracy: Over 98% accuracy of data and information
• Completeness: Coverage of all required elements in the template
• Clarity: Report easily understood by target audiences
• Usefulness: Greater than 4/5 average rating of report usefulness from recipients
• Distribution: Report delivered to all target audiences on time

Reporting Schedule

Month	Report Type	Presentation Dates
January	Monthly Report (December)	
February	Monthly Report	- University Council Meeting (March)
March	Monthly Report	- Supreme Committee Meeting
April	Monthly Report + Quarterly Report (Q1)	- Supreme Committee Meeting (July)
May - July	Monthly Reports + Quarterly Report (Q2)	- Supreme Committee Meeting (October)
August - October	Monthly Reports + Quarterly Report (Q3) + Annual Report	Presentation Dates
November - December	Monthly Reports + Quarterly Report (Q4)	

Key Notes

• Reports should focus on critical information useful for decision-making.
• Avoid excessive detail that may distract from key points.
• Use charts and graphs to facilitate understanding.

• Recommendations should be actionable and clear.
• Focus on trends and changes, not just static figures.
• Urgent reports should be issued immediately without waiting for the regular cycle.
• All reports should be archived in an organized manner for future reference.

Monthly Dashboard Template

Risk Dashboard - [Month/Year]

Indicator	Current Value	Previous Month	Result
Total Risks Recorded	XX	XX	↑ / ↓ / →
Critical Risks	XX	XX	↑ / ↓ / →
High Risks	XX	XX	↑ / ↓ / →
Medium Risks	XX	XX	↑ / ↓ / →
Low Risks	XX	XX	↑ / ↓ / →
Treatment Plans in Implementation	XX	XX	-
Treatment Plan Completion Rate	XX%	XX%	↑ / ↓ / →
New Risks Identified	XX	XX	-
Closed Risks	XX	XX	-

Chapter VII
Key Performance Indicators and Risks

Overview: This chapter contains the key performance indicators (KPIs) and key risk indicators (KRIs) needed to monitor the effectiveness of risk management and early warning.

7.1 Key Performance Indicators (KPIs)
7.1.1 Introduction

Key performance indicators (KPIs) measure how successfully risk management achieves its objectives. They should be measured periodically and compared to the set targets.

7.1.2 Risk management process performance indicators

No.	Performance Indicator	Measurement Method	Objective	Frequency	Responsible Party
A. Risk identification indicators					
1	Number of newly identified risks	Count new risks added to the record	More than 10 risks/quarter	Quarterly	Risk Unit
2	Percentage of units involved in risk identification	(Participation units / Total units) x 100	100%	Semi-annual	Risk Unit
3	Average risk documentation time	Average period between identification and documentation (days)	Less than 5 working days	Monthly	Risk Unit
4	Number of risk identification workshops conducted	Count workshops and meetings held	More than 4 workshops/year	Quarterly	Risk Unit
B. Risk Assessment Indicators					
5	Assessed risk percentage	(Assessed Risks / Total Risks) × 100	100%	Monthly	Risk Unit
6	Average assessment time	Average Time Between Identification and Assessment (Days)	Less than 10 business days	Monthly	Risk Unit
7	Critical and high risk percentage	(Critical + High Risks / Total) × 100	Less than 20%	Monthly	Risk Unit
8	Assessment accuracy	Percentage of Risks Realized Within Expected Assessment	More than 80%	Semi-annual	Risk Unit
C. Risk mitigation indicators					
9	Percentage of high-risk risks addressed	(High-risk processing/total high) x 100	Over 90%	Quarterly	Risk Owners
10	Percentage of treatment plans completed on time	(Plans completed by date/total plans) x 100	Over 85%	Quarterly	Risk Unit
6.2	Average risk closure time	Average time from selection to closure (months)	Under 6 months (High)	Quarterly	Risk Owners
12	Risk reduction rate	Average reduction (initial	Under 12 months	Quarterly	Risk Unit

		assessment - remaining assessment)	(Medium)		
D. Monitoring and Reporting Indicators					
13	Count new risks added to the record	(Risks reviewed/due to review) x 100	Greater than 95%	Monthly	Risk Unit
14	(Participation units / Total units) x 100	(Reports on time/Total reports) x 100	100%	Monthly	Risk Unit
15	Average period between identification and documentation (days)	Average time from detection to response (hours)	Less than 4 hours (critical)	Monthly	Risk Unit
E. Indicators of culture and awareness					
16	Percentage of employees trained in risk management	(Trained staff / Total staff) x 100	Greater than 80%	Annually	Human Resources
17	Number of awareness campaigns implemented	Count of awareness campaigns	Greater than 4 campaigns/year	Quarterly	Risk Unit
18	Risk culture index	Risk culture questionnaire (scale 1-10)	Greater than 7.5	Annually	Risk Unit
F. Compliance indicators					
19	Risk Management Policy Compliance Rate	Compliance audit results (%)	Greater than 90%	Semi-annual	Internal Audit
20	Number of Risk Policy Violations	Number of recorded violations	Less than 5 violations/year	Quarterly	Risk Unit

7.2 Key Risk Indicators (KRIs)

7.2.1 Introduction

Key Risk Indicators (KRIs) are early warning signs of rising risk levels before they materialize. They must be continuously monitored, and action taken when acceptable limits are exceeded.

7.2.2 Risk Indicators by Category

No.	Risk Indicator	Risk Category	Measurement Method	Green Threshold	Red Threshold
A. Strategic Risks					
1	Student growth rate	Strategy	Annual Change in Student Numbers	< 5%	
2	Market share	Strategy	Percentage of University Students in the Region	< 15%	
3	Admission rate	Strategy	(Admitted/Applicants) x 100	< 70%	
4	University ranking	Strategy	Rank in National/International Rankings	Top 100 Locally	
B. Financial risks					
5	Current liquidity ratio	Financial	Current Assets / Current Liabilities	< From 1.5	> From 1.0
6	Fee collection ratio	Financial	(Collected Fees / Due Fees) x 100	< From 95%	> From 80%

7	Overdue receivables ratio	Financial	(Debts > 90 Days / Total Debts) x 100	> From 5%	< From 15%
8	Operating profit margin	Financial	(Operating Income / Revenue) x 100	< From 15%	> From 5%
9	Expenses coverage ratio	Financial	Number of Months Covered by Reserves	< From 6 months	> From 3 months
C. Operational Risks					
10	Number of operational incidents	Operational	Number of incidents recorded monthly	> From 5 incidents	< From 15 incidents
6.2	Critical systems availability rate	Operational	(Operating time / Total time) × 100	< From 99%	> From 95%
12	Average repair time (MTTR)	Operational	Average troubleshooting time (hours)	> From 4 hours	> From 12 hours
D. Academic risks					
13	Student satisfaction rate	Academic	Student Satisfaction Index (1-10 Survey)	< I 4.7	> I 3.5
14	Student retention rate	Academic	(Continuing Students / Total Students) x 100	< I 90%	> I 75%
15	On-time graduation rate	Academic	(On-Time Graduates / Total Expected Graduates) x 100	< I 80%	> I 60%
16	Program accreditation success rate	Academic	(Accredited Programs / Total Programs) x 100	100%	> I 90%
E. Technical and cyber risks					
17	Number of hacking attempts	Technical	Number of hacking attempts detected daily	From > 50 attempts	From < 150 attempts
18	Number of critical vulnerabilities	Technical	Number of open vulnerabilities (CVSS > 7)	0	From< 5
19	Average vulnerability patching time	Technical	Average time from discovery to patch (days)	From >7 days	From< 30 days
20	Percentage of updated systems	Technical	(Updated systems / Total systems) x 100	From< 95%	From> 80%
F. Human resources risks					
21	Employee turnover rate	Human Resources	(Employees leaving / Total employees) x 100	From > 10%	From< 20%
22	Absenteeism rate	Human Resources	(Days absent / Total days worked) x 100	From> 3%	From <7%
23	Average time to fill vacant positions	Human Resources	Average days from announcement to hiring	From> 45 days	From <90 days
24	Employee satisfaction index	Human Resources	Employee satisfaction survey (1-10)	From < 7.5	From > 5.5
G. Reputational risks					
25	Social media sentiment index	Reputational	Percentage of positive feedback	< 80%	> 50%
26	Number of registered complaints	Reputational	Number of official complaints per month	> 10 complaints	< 30 complaints
27	Complaint resolution rate	Reputational	(Resolved complaints / Total complaints) x 100	< 95%	> 75%

H. Legal and regulatory risks					
28	Number of open legal cases	Legal	Number of active legal cases	0	< I 3
29	Regulatory compliance rate	Legal	Compliance audit results (%)	< out of 95%	> I 80%
30	Number of regulatory violations	Legal	Number of violations recorded annually	0	< I 2

7.2.3 Risk Indicators Dashboard

KRIs Dashboard Template - Current Month

Indicator	Current Value	Target	Condition	Action
Student Enrollment Growth Rate	+7.2%	> +5%	Normal	Immediate financial review
Current Liquidity Ratio	1.3	> 1.5	Warning	Regular monitoring
Student Satisfaction Rate	8.3	> 8.0	Normal	Activation of cybersecurity protocol
Number of Hacking Attempts	185/day	< 150	Critical	Review of human resources policies
Employee Turnover Rate	14%	< 10%	Warning	Regular monitoring
Tuition Collection Rate	96%	> 95%	Normal	Regular monitoring

7.2.4 Indicator Response Protocol

Indicator Condition	Required action	Responsible Officer	Timing
Green (Normal)	-Periodic monitoring only - no additional actions.	Index Manager	Monthly review
Yellow (Warning)	1. Analyze the causes 2. Develop a treatment plan 3. Report to the risk manager	Risk Owner	Within 5 days
Brown (High)	1.Immediate analysis of the causes 2.Implementation of a remediation plan 3.Reporting to the higher committee 4. Daily monitoring	Risk Owner + Risk Unit	Within 24 hours
Red (Critical)	1. Immediate emergency meeting 2. Activate the emergency plan 3. Inform the university president and the university council 4. Continuous monitoring	University President + Supreme Committee	Immediate (within hours)

Best practices for using risk indicators:

- **Automation:** Link indicators to data systems for automatic updates whenever possible.
- **Visualization:** Use interactive dashboards for easy understanding.

• **Alerts:** Set up automatic alerts when thresholds are exceeded.
• **Periodic review:** Review the suitability of indicators and thresholds quarterly.
• **Integration:** Integrate indicators with ERP systems and performance management systems.

Chapter VIII
Emergency and Business Continuity Plans

Overview: This section contains emergency and crisis preparedness plans, business continuity plans, and disaster recovery plans to ensure the university continues to operate even in exceptional circumstances.

8.1. Emergency and Crisis Management Plan
8.1.1 Definitions

Emergency	A sudden event requiring an immediate response but not threatening complete business continuity.
Crisis	A serious event threatening business continuity and requiring exceptional management and intervention from senior leadership.
Disaster	A catastrophic event causing a complete or near-complete disruption of operations.

8.1.2 Emergency levels

Level	Description	Examples	Response
Level 1 (Low)	A limited event that can be managed with local resources	Brief power outage / Single device malfunction	Department Management + Security Notification
Level 2 (Medium)	An event affecting multiple departments and requiring coordination	Minor fire / Moderate injury	Activation of Emergency Team + Management Notification
Level 3 (High)	A serious event that threatens a large part of the university	Large fire / Widespread cyberattack	Activation of Operations Room + University President Notification
Level 4 (Critical)	A disaster that threatens the continuity of the entire university	Earthquake / Massive flood / Terrorist attack	Activation of Business Continuity Plan + Notification of All

8.1.3 Crisis Management Team

Role	Official	Responsibilities:
Crisis Leader	University President	- Making strategic decisions -Communicating with higher authorities - Declaring a state of emergency
Crisis Coordinator	Director of Risk Management	-Coordinating all response teams -Managing the operations room -Monitoring the implementation of the plan
Communications Officer	Director of Media and Corporate Communications	- Media relations - Issuing official statements - Social media management
Safety Officer	Director of Security and Safety	-Site security -Safe evacuation -Coordination with Civil Defense
Logistics Officer	Director of Facilities and Services	-Providing resources -Arranging alternative locations -Managing supplies
IT Officer	Director of Information Technology	-System recovery - Data protection - Providing alternative connections

8.1.4 Emergency Response Procedures

Example: University Building Fire Response Plan

Phase 1: Detection and Alarm (0-5 minutes)		
1	Fire detection (automatic system or human)	Action: Activate the fire alarm immediately.
2	Contact the control room	Action: Immediately call 998 (Emergency) + (University Security).
3	Rapid assessment	Action: Determine location, size, and risks
Phase 2: Evacuation (5-15 minutes)		
4	Evacuate the affected building	Action: Use emergency exits + assemble at evacuation points
5	Verify that everyone has evacuated	Action: Count attendees + search for missing persons

6	Securing the area	Action: Prevent entry + secure a 100-meter perimeter
Phase 3: Combat and control (15-60 minutes)		
7	Initial firefighting attempt (if safe)	Action: Fire extinguishers to be used by trained personnel only.
8	Arrival of Civil Defense	Action:: Full coordination and information provision.
9	Declaration of control	Action: Confirmation that the fire has been extinguished by the Civil Defense.
Phase 4: Recovery and Return (1-24 hours)		
10	Damage assessment	Action: Building inspection + damage assessment
6.2	Site security	Action: Urgent repairs + security
12	Gradual return	Action: After approval from Civil Defense and the administration

8.2. Business Continuity Plan (BCP)

8.2.1 Objectives

• Ensure the continuity of critical operations during and after crises
• Minimize downtime and its impact on students and staff
• Protect the university's reputation and financial sustainability
• Comply with regulatory requirements

8.2.2 Business Impact Analysis – (BIA)

Process	Impact Level	RTO*	RPO**	Impact after 72 hours:
Student Information System (SIS)	Critical	4 hours	1 hour	Data loss + Disruption to admissions and registration
Learning Management System (LMS)	Critical	8 hours	2 hours	Class suspension + student anger
Financial System	High	24 hours	4 hours	Delayed payments + accounting problems
Email	High	12 hours	2 hours -	Loss of communication + delayed decisions
Classrooms	High	24 hours	-	Disruption of in-person classes
Website	Medium	48 hours	24 hours -	Reputational damage + loss of admission applications
Library	Medium	72 hours	-	Disruption for students and researchers

*RTO (Recovery Time Objective): Maximum acceptable downtime
**RPO (Recovery Point Objective): Maximum acceptable data loss

8.2.3 Continuity strategies

Field	Core Strategy	Detailed Actions
Education and Teaching	Transition to Remote Learning	Full activation of the LMS platform Modified schedules Extensive technical support Accommodations for affected students
Information Technology	Alternative Site + Cloud	- Ready-made backup data center - Daily cloud backup - Backup devices
Human Resources	Remote Work	- A ready-made remote work policy - Communication tools (Teams, Zoom) - Support for affected employees - On-site rotation
Facilities	Alternative Sites	-Agreements with other universities -Alternative halls -Temporary offices -Generators and emergency services
Communications	Multiple Channels	- Backup website Social media - Bulk SMS messaging - Emergency hotline

8.2.4 Disaster Recovery Plan (DRP)

Recovery Priorities (in order):
1. Safety: Ensure the safety of all personnel (0-24 hours)
2. Critical Systems: Restore the student information system (24-48 hours)
3. Core Operations: Email + Website + Financial System (48-72 hours)
4. Education: Resume classes (in-person or remote) (72 hours - 1 week)
5. Supporting Operations: Remaining services and systems (1-4 weeks)
6. Full Return: Return of all operations to normal (1-3 months)

8.2.5 Testing and Training

Test Type	Description:	Frequency	Participants
Desktop Test	Reviewing plans and procedures without actual implementation	Every 6 months	Crisis Team
Simulation	Reenacting a realistic scenario without actual disruption	Annually	All Staff
Evacuation Drill	Practical evacuation of university buildings	Twice a year	Everyone
System Recovery Test	Experimental recovery of critical systems		
Comprehensive Test	Full implementation of the continuity plan		

Essential emergency resources:

Key emergency numbers:	Civil Defense: 998 Ambulance: 997 Police: 999 University Security: (Internal)
Assembly locations:	-Primary location: University main square -Alternative location: Football stadium -Emergency location: Parking lot
Alternate operations center:	Company headquarters

Chapter IX
Training and Awareness

Overview: Building a risk management culture through comprehensive training and awareness programs at all levels within the university.

9.1. Risk Management Training Program

9.1.1Training Objectives

• To build a shared understanding of risk management concepts and principles
• To equip staff with the skills necessary to identify and assess risks
• To promote a culture of risk awareness at all levels of the university
• To ensure the effective implementation of risk management policies and procedures

9.1.2 Training Programs by Target Groups

Target Audience:	Training Program	Duration	Basic content	Repetition
University Council and Senior Administration	Governance and Risk Strategy	4 hours (day)	- The role of the university council - Risk appetite - Strategic oversight	Annually
Higher Risk Committee	Advanced Risk Management	8 hours (4 days)	- Enterprise risk management - Advanced analysis - Risk-informed decision-making	Annually
Central Risk Management Team	Professional Risk Management	20 hours (2 weeks)	- ISO 31000 and COSO-ERM standards - Advanced tools and techniques - Professional certifications (CRMP, FRM)	Upon appointment + Annual update
Risk Owners	Applied Risk Management	8 hours (2 days)	-Departmental risk identification - Development of remediation plans - Use of templates	Annually

Departmental Risk Coordinators	Risk Management Coordination	12 hours	- Risk management processes - Documentation and reporting - Coordination with the central unit	Annually
All Staff	Risk Management Awareness	2 hours	- Basic concepts - Employee role - Risk reporting	Upon appointment + Biennial update
Faculty Members	Academic Risks	3 hours	- Academic Quality Risks - Accreditation - Research Ethics	Upon appointment + Annually
Students	Safety and Awareness	1 hour	- Campus Safety - Emergency and Evacuation - Incident Reporting	Upon registration

9.1.3 Annual training programs

Training program dates are determined in coordination with the university's Training and Skills Development Department. Below are some examples of key courses expected to be offered during the year:

Program	Target Audience	Implementing Entity
Professional Risk Management	Risk Management Team	External Consultant
Public Awareness of the Importance of Risk Management	All Staff	Risk Unit + Human Resources
Applied Risk Management	Risk Owners	Risk Department
Evacuation Drill (Practical)	All Staff and Students	Security and Safety
Academic Risks	Faculty Members	Quality and Accreditation Management
Cybersecurity	All Staff + Faculty Members	Information Technology
Risk Management Coordination	Risk Coordinators	Risk Management
Governance and Risk Strategy	University Council + Senior Management	External Consultant

9.1.4 Awareness Campaigns

Awareness campaign dates are determined in coordination with the university's Intellectual Awareness Unit. Below is a list of the most prominent campaigns expected to be implemented annually:

Campaign	Activities	Tools
Annual Risk Awareness Month	- Awareness seminars - Competitions - Prizes - Exhibitions	- In-person events - LMS platform (Teams) - Email - Social media

Cybersecurity Campaign	Weekly tips - Phishing quizzes - Educational videos	- Email - Screens - Website
Safety Campaign	Evacuation drills Posters SMS messages	- Field campaign - Posters - Text messages
Early Reporting Campaign	Encouraging reporting Success stories Simplified procedures	- Leaflets - Meetings - Email + Text messages

9.1.5 Training Effectiveness Evaluation

Training Effectiveness Indicators:
• Attendance Indicator: Actual/Targeted Attendance Rate (Target 90%)
• Satisfaction Indicator: Participant Evaluation of the Program (Target 4.5/5 or 80%)
• Comprehension Indicator: Post-Test Results (Target 80% Achieve Full Marks)
• Application Indicator: Percentage of Knowledge Applied in the Workplace (Target 3.5/5 or 70%)
• Culture Indicator: Improvement in the Annual Risk Culture Indicator (Target 4/5 or 80%)

Chapter X
Review and Continuous Improvement

Overview: Risk management is a dynamic process that requires periodic review and continuous improvement to ensure its effectiveness and adaptability to internal and external changes.

10.1 The Review and Continuous Improvement Cycle

Objectives of Review and Improvement
• Ensuring the effectiveness and implementation of the risk management framework
• Identifying opportunities for improvement and development
• Keeping pace with changes in the internal and external environment
• Ensuring compliance with standards and policies
• Fostering a culture of continuous improvement

10.2 Levels of Review

Level	Frequency	Scope	Responsible Parties
Daily Review	Daily	- Monitoring critical indicators - Tracking events - Updating data	Risk Owners
Weekly Review	Weekly	- Review the progress of treatment plans - Update risk records - Follow up on procedures	Departmental Risk Coordinators
Monthly Review	Monthly	- Evaluate the effectiveness of controls - Review overall indicators - Departmental reports	Risk Management Unit
Quarterly Review	Every 3 months	- Comprehensive review of the risk register - Risk appetite assessment - Review of mitigation strategies	Higher Risk Committee
Semi-Annual Review	Every 6 months	-Review of policies and procedures - System performance evaluation - Updating priorities	Higher Committee + Senior Management
Comprehensive Annual Review	Annually	-Comprehensive review of the entire framework - Overall effectiveness assessment - Strategy update - Governance review	Board of Trustees + University President

10.3 Comprehensive Annual Review - Key Elements

Key elements of the annual review:

1. Strategy Review:

a. Alignment of risk management with strategic objectives
b. Appropriateness of the approved risk appetite
c. Effectiveness of integrating risk into strategic planning

2. Governance Review:

a. Effectiveness of the organizational structure for risk management
b. Clarity of roles and responsibilities
c. Performance of committees and units

3. Process Review:

a. Effectiveness of risk identification, assessment, and treatment processes
b. Adequate documentation and reporting
c. Appropriateness of tools and models

4. Performance Review:

a. Achievement of Key Performance Indicators (KPIs)
b. Effectiveness of Key Risk Indicators (KRIs)
c. Risk outcomes achieved

5. Culture Review:

a. Level of risk awareness
b. Effectiveness of training and awareness programs
c. Employee engagement

6. Compliance Review:

a. Adherence to policies and procedures
b. Compliance with international standards (ISO 31000, COSO)
c. Compliance with local regulatory requirements

10.4 Continuous Improvement Methodology (PDCA)

Phase	Activities	Tools	Responsible Officer
Plan	-Defining improvement objectives / Gap analysis / Developing an improvement plan /	SWOT analysis Interviews	Risk Management

	Allocating resources		
(Planning)	Implementing improvement initiatives - Developing tools and procedures - Training and awareness - Documentation	Project plans Change management tools Training programs	Risk Management + All Units and Departments
Do	- Monitoring progress - Measuring results - Evaluating effectiveness - Gathering feedback	- Key Performance Indicators (KPIs) - Surveys - Performance Reports - Periodic Reviews	Risk Management (Monitoring and Audit Unit)
(Execution)	- Analyzing results - Implementing effective improvements - Correcting deviations - Documentation and dissemination	- Lessons Learned Reports - Policy Updates - Corrective Actions	Risk Management

10.5 Sources of Improvement Inputs

Source	Description	Frequency
Internal Audit	Internal audit reports on the effectiveness of risk management	Annually
External Audit	External evaluation by consultants or accrediting bodies	Every 2-3 years
Employee Feedback	Questions and interviews on risk management experience	Annually
Actual Incidents and Risks	Lessons learned from realized risks	When it occurs
Best Practices	A review of other universities' experiences and new standards	Continuous
Organizational Changes	Updates in laws, regulations, and standards	When it occurs
Performance Indicator Results	Analysis of KPIs and KRIs to identify weaknesses	Semi-annually

10.6 Annual Improvement Plan - Template

Demonstrative Example: Risk Management Improvement Plan

No.	Improvement Initiative	Objective	Budget	Duration	Responsible Person
1	Implementation of an Integrated GRC System	Automate risk management processes	500,000 Riyals	6 months	Information Technology
2	CRMP Certification Program for the Risk Team	Increase team efficiency	80,000 Riyals	12 months	Risk Unit
3	Development of an Interactive Dashboard	Improve risk visibility	150,000 Riyals	3 months	Information Technology
4	Expansion of Risk Insurance Coverage	Enhance risk transformation	200,000 Riyals annually	Continuous	Finance
5	Creating a 24/7 SOC	Strengthen cybersecurity	800,000 Riyals	8 months	Information Technology

Total budget: SAR 1,730,000
Expected return: Reduce potential losses by 30%, improve operational efficiency by 25%.

10.7 Risk Management Maturity Model Indicators (RMM)

Level Description Characteristics Status at Mustaqbal University

No.	Level	Description	Features:	Status at Mustaqbal University
1	Beginner	No structured approach	- No frame - Feedback only - No documentation	Previous Stage
2	Limited	Basic awareness only	-Some procedures -Irregular -Limited to units and departments	Previous Stage
3	Defined	Documented framework	-Approved policy -Documented processes -Implementation start	Current Status (after applying this guide)
4	Managed	Comprehensive and systematic application	-Full implementation -Performance measurement -Periodic improvement	Goal within 2-3 years
5	Enhanced	Continuous improvement and leadership	-Established culture -Continuous improvement -Setting an example for others	Aspiration after 5 years

10.8 Roadmap to Level 5 (Enhanced Level)

• Years 1-2: Full implementation of the guide and reaching Level 3 (Defined)

• Years 3-4: Consolidating practices and measuring effectiveness – reaching Level 4 (Managed)

• Year 5+: Continuous improvement and innovation – reaching Level 5 (Enhanced)

Chapter XI
Quality Assurance System

11.1 Introduction

The Risk Management Department at Mustaqbal University adopts an integrated Quality Assurance System (QAS). The system aims to achieve efficiency and effectiveness in managing institutional risks, ensure compliance with national regulations and standards, enhance the reliability of management outputs, and support the sustainability of institutional performance. The quality system aims to achieve the following:

1. Enhance the quality of administrative processes in risk management.
2. Ensure consistency between operational plans and actual management outputs.
3. Enhance the efficiency of risk management in protecting the university's assets and reputation.
4. Measure performance periodically using approved performance indicators.
5. Support data-driven decision-making.
6. Achieve integration between risk management and the university's quality unit.
7. Establish a culture of quality and continuous improvement within the department.

This system utilizes a continuous improvement cycle (Fig. 11.1) based on:

- NCAAA institutional accreditation requirements.
- Best practices in risk governance and management (ISO 31000).
- The continuous improvement methodology (Plan-Do-Check-Act).

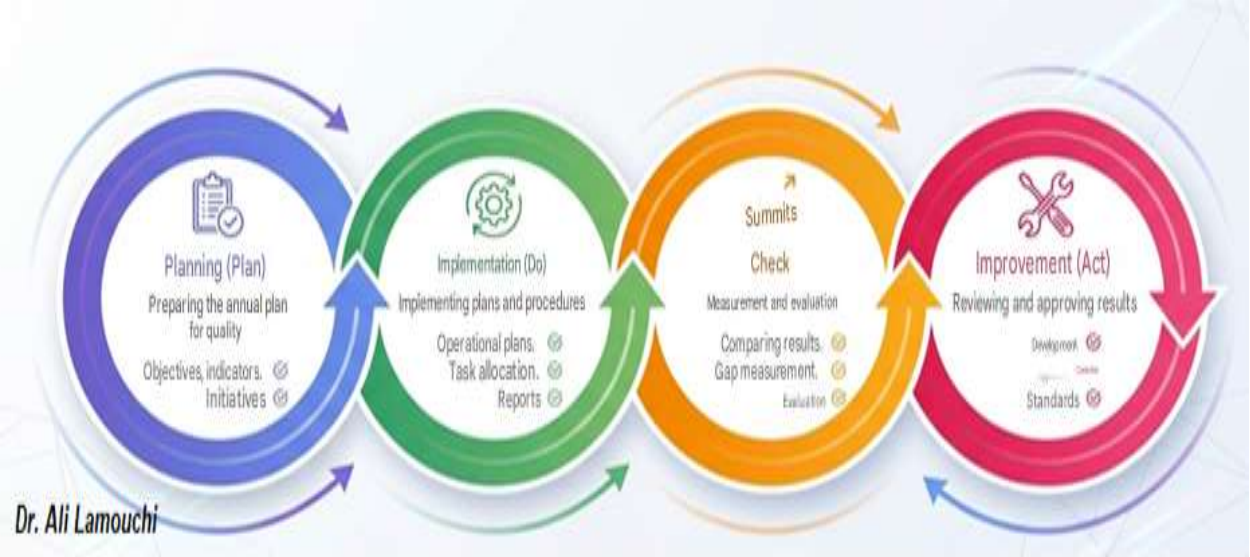


Fig. 11.1: Continuous improvement cycle

The system quality cycle includes the following main actions:

Phase	Description
Plan	Preparing the annual operational quality plan
(Planning)	Implementing plans through risk management units
Do	Measurement and evaluation using performance indicators
(Execution)	Preparing the annual operational quality plan

The plan is approved by:
• The Risk Management Manager.
• The Senior Risk Management Committee.

The Quality Assurance System encompasses all risk management activities, including:
• Identifying, assessing, and addressing risks.
• Preparing the corporate risk register.
• Monitoring critical risks.
• Periodic risk reporting.
• Business continuity.
• Crisis and emergency management.
• Auditing and documentation.
• Compliance and governance.

11.2 Implementing the Quality System within Risk Management

The quality system is implemented through:
• Departmental operational plans.
• Task allocation according to the organizational structure.
• Periodic progress reports.
• Periodic follow-up meetings.

11.3 Performance Analysis and Evaluation Mechanism

Quality data is collected through the following tools:
• Key Performance Indicator (KPI) results.
• Periodic progress reports.
• Customer satisfaction surveys.
• Administrative follow-up records.
• Meeting reports.
• Periodic risk reports.
• Quality and compliance audit results.
Thereafter, the performance is analyzed through to the following steps:
1. Comparing results with approved objectives.
2. Measuring performance gaps.
3. Classifying performance level (Excellent – Very Good – Good – Needs Improvement).
4. Analyzing the causes of any shortcomings.
5. Documenting evaluation results in official reports.

11.4 Identifying Strengths, Improvement Opportunities, and

Action Plan

Based on the evaluation results, the following is done:
• Identifying areas of excellence in risk management performance.
• Identifying improvement opportunities according to the methodology of:
 Organizational reasons
 Technical reasons
 Administrative reasons
 Technological reasons
As explained previously, an annual improvement plan is prepared according to the following elements:
• Improvement initiative.
• Objective of the initiative.
• Responsible party.
• Time period.
• Proposed budget

11.5 Quality Roles and Responsibilities in the Risk Management Department

Entity	Responsibilities
Risk Management Director	General supervision – Plan approval – Performance monitoring
Quality Coordinator	Data collection – Documentation – Report preparation
Heads of Departments	Plan implementation – Report submission
Quality and Accreditation Management + Internal Audit Management	Review – Audit – Final evaluation

11.6 Outputs of the Quality Assurance System

• Certified quality reports.
• Documented performance indicators.
• Annual improvement record.
• Ongoing development plans.
• Compliance and standards reports.
• Direct support for institutional accreditation

Chapter XII
Templates

Overview: This chapter contains all the practical tools and templates needed to effectively implement risk management at Future University. All templates are ready for immediate use.

12.1 Risk Register

The risk register is the central document containing all identified risks, their assessments, and their treatment status. It must be continuously updated and made available to all stakeholders.

Risk number	Name of the danger	Category	Description	Probability (1-5)	Impact (1-5)	Initial Assessment	Strategy	Treatment Procedures	Responsible Official	Residual Assessment	Status:	Review Date
ST-001	Decreased student numbers	Strategic	A significant decrease in the number of accepted students	4	5	20	Reduction	Marketing Campaign + New Programs + Grants	Academic Vice President	**8**	In progress	2025-01-15
FN-003	Failure to collect fees	Financial	Students are late in paying tuition fees or have not paid them at all	3	4	12	Reduction + Transfer	Strict Collection Policy + Insurance	Financial Director	**6**	Active	2025-01-10

Risk Register Usage Notes:

- **Update:** The register must be updated at least monthly for high risks and quarterly for medium and low risks.
- **Availability:** The register is available to the Higher Risk Committee and risk owners.
- **Archiving:** Maintain historical copies to track progress.
- **Export:** The register can be exported to Excel or specialized GRC systems.

12.2 Risk Assessment Template

Risk Assessment Model - Mustaqbal University	
Section 1: Basic Information	
Risk Code and Number:	----------
Risk Name:	----------
Date of Identification:	----------
Identified by:	----------
Department/Unit:	----------
Risk Category:	☐Strategic ☐ Financial ☐ Operational ☐ Academic ☐ Technical ☐ Human Resources ☐ Legal ☐ Reputation ☐ Environmental ☐

	Other: _____
Section 2: Risk Description	
Detailed Description	---------- ---------- ----------
Section 3: Risk assessment	
Probability (1-5):	☐1 (Very rare) ☐2 (Rare) ☐3 (Possible) ☐4 (High) ☐5 (Almost certain)
Impact (1-5):	Value: ____
Overall Assessment:	☐1 (Mild) ☐2 (Mild) ☐3 (Moderate) ☐4 (Large) ☐5 (Catastrophic)
Section 4: Treatment strategy	
Selected Strategy:	☐ Avoid ☐ Reduce ☐ Transfer ☐ Accept
Processing Actions:	1.---------- 2.---------- 3.----------
Responsible Person:	----------
Required Budget:	---------- Riyal
Timeline:	From: ---------- To:----------
Expected Remaining Assessment:	Probability: --------× Effect: ---------- = ----------
Section 5: Approvals	
Risk Owner:	Name: ----------Signature: ----------Date: ----------
Risk Management Director:	Name: ----------Signature: ----------Date: ----------
Supreme Committee:	Name: ----------Signature: ----------Date: ----------

12.3 Risk Management Plan Template

Risk Treatment Plan-Mustaqbal University						
Risk Information						
Risk Code and Number:	----------					
Risk Name:	----------					
Current risk level:	☐ Critical ☐ High ☐ Medium ☐ Low					
Digital assessment:	Probability:-------- × Effect: ------ = ------					
Strategies and actions						
Strategy	Avoid ☐ Reduce ☐ Transfer ☐ Accept					
Detailed actions						
No	Action	Responsible	Start date	End date	Budget	Status
1	----------	----------	----------	----------	----------	☐ In progress ☐ Completed
2	----------	----------	----------	----------	----------	

3	----------	----------	----------	----------	----------	
4	----------	----------	----------	----------	----------	

Resources and Budget	
Total Budget:	----------Riyals
Source of Funding:	☐ Risk Budget ☐ University Budget ☐ Reserve ☐ Other: _____
Human Resources:	Number of Personnel Required: ---- Working Hours: ----
Success Indicators and Monitoring	
Success indicators:	1.---------- 2.---------- 3.----------
Expected residual assessment:	Probability: ____ × Impact: ____ = ____ Expected Level: ☐ Critical ☐ High ☐ Medium ☐ Low
Monitoring frequency:	Weekly ☐ Monthly ☐ Quarterly ☐ Semi-annual
Reporting to:	----------
Approvals and Accreditations	
Plan developer:	Name: ----------Signature: ---------- Date: ----------
Risk owner:	Name: ----------Signature: ---------- Date: ----------
Risk management director:	Name: ----------Signature: ---------- Date: ----------
High-level risk committee:	Name: ----------Signature: ---------- Date: -----

12.4 Accident/Realized Risk Report Template

Accident Report - Mustaqbal University	
Section 1: Accident Information	
Report code and number:	----------
Date and time of incident:	Date----------Time----------
Location:	----------
Type of incident:	☐ Risks that materialized: ☐ Emergency incident ☐ Near miss ☐ Security breach ☐ Disaster ☐ Other: _____
Reporter	Name: ----------Signature: ----------Date: ----------
Section 2: Accident Description	
A detailed description of what happened: ---------- - ---------- - ----------	

---------- Affected Parties: ☐ Students ☐ Staff ☐ Faculty ☐ Visitors Number of Affected: ----------	
Section 3: Impact and losses	
Financial impact:	Estimated losses: _____ Riyals
Operational impact:	Duration of downtime/disruption: _____ hours/day Affected activities: _____
Reputational impact:	☐ Low ☐ Moderate ☐ High ☐ Critical
Human injuries/damage:	☐ None ☐ Minor injuries ☐ Serious injuries ☐ Fatalities
Section 4: Immediate response	
Immediate actions taken: 1.---------- 2.---------- 3.----------	
Reporting entities:	☐ Senior Management ☐ Civil Defense ☐ Police ☐ Insurance ☐ Other:----------
Section 5: Analysis and Recommendations	
The root cause:	----------
Was the risk predetermined?	Yes (Risk number: ----------) ☐ No (New risk)
Recommendations to prevent recurrence: ---------- ---------- ----------	
Lessons learned:	---------- ---------- ----------
Section6: Follow-up	
Responsible party for follow-up:	Name:----------Position:----------
Incident status:	☐ Open ☐ Processing ☐ Closed
Expected closing date:	----------
Signatures	
Report prepared by:	Name: ----------Signature: ----------Date: ----------
Director of Risk Management:	Name: ----------Signature: ----------Date: ----------

	--------
University President:	Name: ----------Signature: ----------Date: ---------- --------

Important Note: Incident reports must be submitted within 24 hours of the incident for critical and high-risk incidents, and within 72 hours for medium and low-risk incidents. All reports are confidential and used for improvement purposes only.

[**Note:** The following appears to be a separate, unrelated statement:] ...

12.5 References and Sources

International Standards and Frameworks:

• ISO 31000:2018 - Risk Management Guidelines
• COSO Enterprise Risk Management (ERM) Framework
• ISO 27001:2013 - Information Security Management
• ISO 22301:2019 - Business Continuity Management
• NIST Cybersecurity Framework

Local References:

• Ministry of Education Regulations
• Council of Private Colleges and Universities Regulations
• Institutional and Academic Accreditation Standards - National Center for Academic Accreditation and Evaluation (NCAAA)
• Information Security Governance Framework - National Cybersecurity Authority
• Frameworks and Guidelines of the General Secretariat of the National Risk Council
• Risk Management and Business Continuity Controls for Digital Government
• Operational Risk Management - Saudi Central Bank
• King Khalid University Risk Management Guide
• Risk Management Guide 2020 - Imam Abdulrahman Bin Faisal University
• Risk Management Guidance Manual - Ministry of Finance

Books:

• The Essentials of Risk Management (Michel Crouhy et al.) al.)
• Enterprise Risk Management: A Common Framework for the Entire Organization (COSO)
• Risk Management in Higher Education (Various Authors)
• Business Continuity Planning: A Step-by-Step Guide (Kenneth Doughty)

12.6 List of terms and abbreviations

Abbreviation	Term in English
ERM	**Enterprise Risk Management**
BCP	**Business Continuity Plan**
DRP	**Disaster Recovery Plan**
KPI	**Key Performance Indicator**
KRI	**Key Risk Indicator**

RTO	**Recovery Time Objective**
RPO	**Recovery Point Objective**
BIA	**Business Impact Analysis**
RACI	**Responsible, Accountable, Consulted, Informed**
ISO	**International Organization for Standardization**
COSO	**Committee of Sponsoring Organizations**
GRC	**Governance, Risk, and Compliance**
SOC	**Security Operations Center**
LMS	**Learning Management System**
SIS	**Student Information System**

12.7. Final Approval and Adoption Form

Adoption and Publication of the Guide

Based on the contents of this Risk Management Guide, which was prepared in accordance with international standards and best practices, and in light of its objectives to enhance governance, sustainability, and quality at Future University:

We approve the adoption of this guide and its implementation effective from: ____/____/_____Hijri

University President:	Name:----------	Signature:----------	Date:----------
Chairman of the Higher Risk Committee:	Name:----------	Signature:----------	Date:----------
Risk Management Director:	Name:----------	Signature:----------	Date:----------

University Seal: