


Category	University Governance and Management	Policy Number	UNI-GOV-601	 جامعة زايد ZAYED UNIVERSITY
Distribution	Internal	Version	3.0	
Responsible Office	President	Policy Owner	Internal Audit	
Date Approved	31 December 2020	Effective Date	31 December 2020	
Date Last Reviewed	17 December 2020	Due Date for Next Review	17 December 2023	

POLICY

Enterprise Risk Management

1. Purpose

This policy outlines the scope, governance, strategy, process and tools necessary to effectively implement an Enterprise Risk Management (“ERM”) capability.

2. Scope of Application

This policy applies to all staff, services, departments, and sections operating within ZU. However, it shall be of a particular importance to the University Council (“UC”), Audit, Risk and Compliance Committee (“ARCC”), President (who is a member of the UC), Executive Committee (“EC”) and finally the Internal Audit Department, which houses the ERM Function.

3. Definitions and Abbreviations

Term	Definition
Audit, Risk and Compliance Committee (“ARCC”)	The ARCC is a Board Committee delegated by the University Council to evaluate the effectiveness of actual risk management practices and the defined ERM Framework.
Executive Committee (“EC”)	The EC is a committee responsible for the discussion and validation of highly rated identified risks and treatment strategies, especially where cross-functional solutions are required. It comprises the Vice President, Chief Administration & Finance Officer, Provost and Chief Academic Officer, Assistant Provost for Student Affairs, Associate Provost for Academic Services and Assistant Provost for Research.

ERM Function	The ERM Function is the section within the Internal Audit Department responsible for coordinating, overseeing and ensuring completion of risk management activities.
ERM Framework	The ERM Framework is a set of components providing the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization. This comprises, amongst other things, the ERM Governance, Strategy, Risk Appetite, Policy and Process.
Internal Audit Department	The Internal Audit Department is responsible for the oversight of all risk management activities in the interim until the Function matures.
Key Risk Indicators (“KRIs”)	Key Risk Indicators provide a tool to facilitate an early warning mechanism to identify potential event(s) that may impact the ability or inability to achieve set objectives. These are not to be confused with Key Performance Indicators.
Risk	Risk is the effect of uncertainty on objectives, where an effect is a deviation from the expected — positive and /or negative. Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). Risk is often characterized by reference to potential events and consequences and how they obstruct the achievement of objectives.
Risk Appetite	Addresses the balance of risk and reward that the organization is willing to accept. It highlights the amount of risk that the organization is willing to accept.
Risk Assessment Criteria	Terms of reference against which the significance of a risk is evaluated. This is comprised of both likelihood and impact scales.
Risk Champion	Risk Champions are ZU Department Directors who are responsible for the supervision and coordination of risk management activities within their department, such as the development of Departmental Risk Registers.

Risk Manager	The Risk Manager is an employee within the ERM Function responsible for working with Risk Champions to gather, challenge and report on risk inputs within the business and ensure all risk management activities are performed in alignment with the ERM Framework.
Risk Owner	The Risk Owner is the individual that is accountable for the management of a specific risk and is responsible for executing ERM guidance in relation to their risk(s). This is oftentimes one who has identified or would experience the impact of an identified risk. The Risk Champion shall approve all assignments of Risk Owners.
Risk Register	Comprises the catalogue of risks and details their inherent and residual likelihood and impact scores. The register also details current and potential controls / mitigations.
Risk Treatment Owner	The Risk Treatment Owner is the individual of the concerned department/section responsible for treating the risk through the implementation of solutions.
Stakeholders	Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
University Council (“UC”)	The University Council is the equivalent of the Board of Directors. They are ultimately responsible for ensuring risks are managed and the risk management system is effective.

4. Overview and Background

4.1 Introduction

- 4.1.1** Zayed University (“ZU”) recognizes that risk management is a core, integral part of how it operates and is committed to establishing an organizational culture that embeds risk management in all of its activities, including decision-making and strategic planning.
- 4.1.2** The purpose of Enterprise Risk Management (“ERM”) is to support the ZU vision and management decision making. As such, the purpose of this policy is to provide all areas of ZU with a framework for identifying, understanding, assessing, managing and monitoring key risks. Risks will be identified and managed in accordance with this policy, taking into account regulatory requirements and the broader organizational objectives and priorities. It is the responsibility of all ZU employees to adhere to the framework, report risks as they become aware and to manage them in line with their defined span of control.

4.2 ERM Principles

- 4.2.1** Risk management activities are proportionate to the level of risk faced by the organization, ensuring risks are managed and opportunities leveraged in anticipation of changing social, environmental and legislative requirements.
- 4.2.2** ERM activities are aligned with the other activities in the organization, and deployed in a consistent and coordinated manner, ensuring risk management is effective, reliable and sustainable.
- 4.2.3** The risk management approach is comprehensive and tailored, and the ERM Framework is understood and implemented by staff with an operational responsibility to risk.
- 4.2.4** Risk management activities are embedded in and integral to the organization’s strategic planning, activity planning, performance management and resource allocation decisions.
- 4.2.5** Risk management activities are dynamic and sensitive to changes in the environment, designed to achieve the best possible outcome, reduce volatility or uncertainty of outcomes and facilitate continuous improvement.
- 4.2.6** Risk management activities incorporate timely involvement of relevant stakeholders, considering their views, perceptions and expertise for informed risk-based decision-making.

4.2.7 Inputs to risk management are based on the best available information, considering historical, current and future data, as well as associated limitations, and shall be timely and transparent for relevant stakeholders.

4.3 ERM Governance

4.3.1 The ERM Strategy is a key component of the governance framework and is composed of:

- a) **Vision, Mission and Philosophy:** These set the overall direction of ERM within ZU and are defined in alignment with the ZU organizational strategy; and
- b) **Risk Appetite:** This is a set of metrics, known as Key Risk Indicators (“KRIs”), and statements that set the levels and types of risk that ZU is willing to pursue in order to achieve its business goals and objectives. This should consider risk events (e.g. zero tolerance for breach of regulations) as well as target levels, which ascertain how well ZU should be operating its controls at the department and organizational level.

4.3.2 The risk appetite is defined by the EC, with guidance from the ERM Function, and approved and ratified by the ARCC and UC respectively. It is comprised of the following elements:

- a) **Existing risk profile:** The existing level and distribution of risks across risk categories and classes;
- b) **Risk capacity:** The maximum risk ZU may bear and remain resilient; and
- c) **Risk tolerance:** Acceptable levels of variation an entity is willing to accept around specific objectives.

4.3.3 The risk appetite should be cascaded to risk assessment criteria and governance shall be clearly defined such that, if operational tolerances or limits are breached, a flag is raised and the breach is communicated through an appropriate escalation procedure for proper remedial actions.

4.3.4 The ERM Governance Structure shall comprise of the following elements, with details of this found in the Operating Model Section of the policy:

- a) **Risk management operating model:** This describes the way ERM activities are conducted in the organization;
- b) **Functional structure:** This describes the reporting relationships based on specialty or department;
- c) **Positional structure:** This details the different positions and personnel assigned within established reporting lines of the functional structure; and
- d) **Charters and job descriptions:** These shall be in place for key ERM stakeholders and associated committees.

4.4 Reviews and Changes to the ERM Framework

The ERM Framework, and all other subsequent reviews and amendments to it, shall be reviewed and approved as per the following table:

Order	Documents	Periodical Review/Approval	Responsibility of Review	Approval of Modifications
1	Risk Appetite	Annually	Risk Manager, Director of Internal Audit and EC	ARCC as First Approver and UC as Ultimate Approver
2	Risk Strategy	Annually	Risk Manager and Director of Internal Audit	Vice President as First Approver and ARCC as Ultimate Approver
3	ERM Objectives	Annually	Risk Manager and Director of Internal Audit	Vice President as First Approver and ARCC as Ultimate Approver
4	ERM Policy	Annually	Risk Manager, Director of Internal Audit and EC	ARCC as First Approver and UC as Ultimate Approver
5	ERM Framework	Annually	Risk Manager and Director of Internal Audit	Vice President as First Approver and ARCC as Ultimate Approver
6	ERM Structure	Annually	Risk Manager and Director of Internal Audit	Vice President as First Approver and ARCC as Ultimate Approver
7	ERM Authority Matrix	Annually	Risk Manager and Director of Internal Audit	Vice President as First Approver and ARCC as Ultimate Approver
8	Departmental Risk Registers	Biannually	Risk Champions	Risk Manager and Director of Internal Audit as First Approver and relevant EC member as Ultimate Approver
9	Corporate Risk Register	Biannually	Risk Manager, Director of Internal Audit and EC	ARCC as First Approver and UC as Ultimate Approver

4.5 Risk Management Tools

In order to execute ERM activities, the following tools may be used:

- a) **Risk registers:** These shall be developed on both a department and corporate level.
- b) **Heat map:** This is a visualization of the risk landscape, facilitating the prioritization of action plans.
- c) **Risk reports:** Reports to management are key to ensuring key risks are highlighted and agreed upon for action.

4.6 Quality Assurance

4.6.1 The ERM Function shall be subject to validation and regular review through two types of separate evaluations in order to assess its ongoing operational effectiveness:

- a) **Independent evaluations:** These shall be conducted by Internal Auditors in the course of their regular duties or at the specific request of higher management at ZU.
- b) **Self-assessments:** The ERM Function shall determine the effectiveness of risk management activities based on the ERM Key Performance Indicators (“KPIs”), which shall be developed and reported on a regular basis by the ERM Function.

4.6.2 Results of the separate evaluations shall be documented, and extreme issues reported to the President along with the key issues, recommendations and benefits realized.

4.6.3 Cases of conflicts of interest noted within ZU risk management activities shall be monitored by the Internal Audit Department and the President shall have the casting right to resolve the issue as deemed appropriate. An example of such a situation would be where a treatment owner who is responsible for implementing a control is also assessing the effectiveness of the said control.

4.6.4 In the case of any ERM Policy violation, the ERM Function shall highlight the issue to ensure a timely resolution of the violation or breach. This shall be completed by identifying a set of disciplinary actions as per ZU’s approved disciplinary policies. Examples of such a policy violation include but are not limited to:

- a) Departments not undertaking the biannual review of their risk register and reporting in a timely manner;
- b) Failing to escalate high priority risks in line with the defined procedures; and
- c) Risk Champions failing to promote an open and honest risk-aware culture as well as failing to encourage new risks to be identified and discussed by members of the business.

4.7 Stakeholder Management and Communication

4.7.1 ZU shall establish internal communication, consultation and reporting mechanisms with regards to the ERM Framework and its outcomes. This is in order to support and encourage accountability and ownership of risk.

4.7.2 A communication strategy and plan for ZU's external stakeholders shall also be established in order to ensure the alignment of key strategic or business partner activities with the objectives of ERM. This shall involve:

- a) **Establishing communication channels:** Direct links with stakeholders should be in place to respond appropriately in the event of a crisis or contingency.
- b) **External reporting and obtaining feedback:** This is in order to comply with legal, regulatory, and governance requirements.

5. Strategy

5.1 ERM Function Vision

Opportunities are seized and risks are managed to enable the achievement of the highest possible quality of educational system, in which students, faculty and the community can reach their full potential.

5.2 ERM Function Mission

The ZU ERM Framework will facilitate the achievement of a leadership role in scientific research and development and the preparation of graduates in innovative ways, in addition to efficient, transparent and quality administrative services, through the systematic identification, assessment, treatment, monitoring and reporting on any risks that would threaten the university's values, ambitions and responsibilities to its students and community.

5.3 ERM Function Objectives

5.3.1 The overall benefit of adopting a solid ERM Framework is to identify, assess, treat, monitor and report on different types of risks in order to minimize the impact and occurrence of risk events and enable the achievement of the strategic objectives of ZU.

5.3.2 ZU shall be clear on its strategic objectives and ensure these are reviewed on a yearly basis, so that the correct risks are identified and prioritized.

5.3.2 The key objectives of the ERM Function that will help ZU deliver the ERM vision and mission are listed below:

- a) Encourage the integration of risk management with strategy formulation and business planning processes, helping ensure decisions are made in alignment with the risk appetite;
- b) Facilitate improvements to the management of internal resources through awareness of risk severity;
- c) Improve the financial sustainability of ZU by identifying waste and challenges to operating efficiencies;
- d) Ensure the continuous availability and quality of faculty, counselors and advisors provided to students.
- e) Facilitate the achievement and maintenance of university and program accreditation in alignment with local and international standards;
- f) Safeguard the reputation of ZU as a safe environment where students can learn, excel and launch their careers;
- g) Support ZU's contribution to the UAE knowledge-based economy;
- h) Build an appropriate culture of integrity, innovation and risk awareness;

- i) Support the identification of critical risks and development opportunities in partnerships, services and student experience, in order to enhance the quality of academics and educational services; and
- j) Establish effective and transparent communication and reporting lines, ensuring that information relating to key risks is provided to decision-makers in a timely manner, so that the interests of ZU can be protected through risk-based proactive decision-making.

5.4 ERM Function Philosophy

That the effectiveness of the ERM Function becomes the active responsibility of all ZU leadership and staff. Everyone will have a strong understanding, ownership and commitment to the management of foreseeable risks that may conflict with ZU’s values of a positive educational environment, leadership, excellence, professional ethics, innovation, collaboration, and civic responsibility. The ERM Function shall endeavor to support ZU in the achievement of its strategic objectives and its contribution to disseminate knowledge to local, regional and global communities.

5.5 Risk Categories

Risks within ZU can be grouped into common themes based on unique characteristics. These risk categories are documented below with explanations to guide the user in their use. All risk registers should have an associated risk category matched to each identified risk.

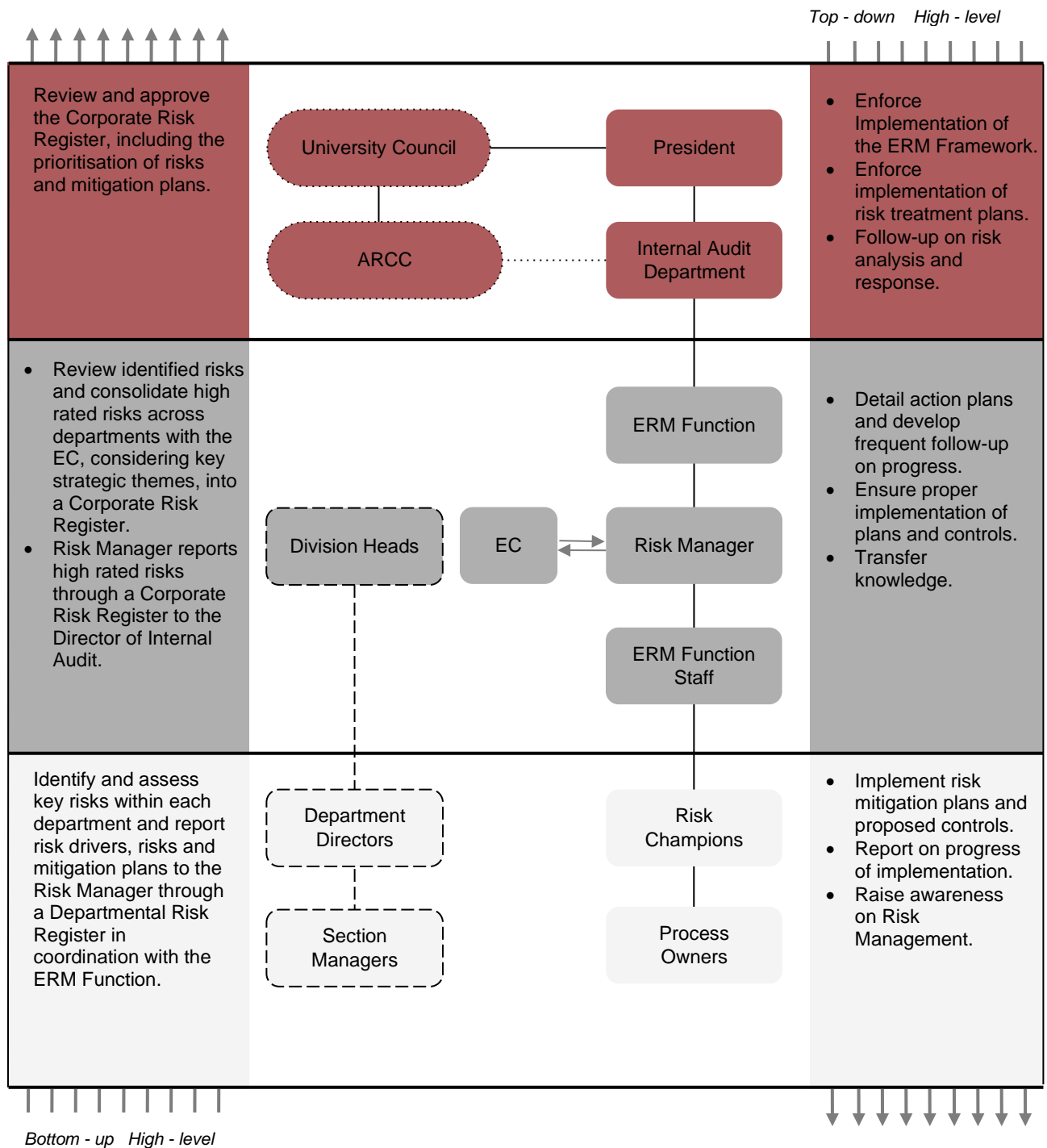
#	Risk Category	Description
1	Strategy & Governance	Risks related to developing and executing ZU's strategic objectives, the public perception of ZU and oversight of key ZU processes, decisions and governance structures.
2	Financial	Risks related to financial losses and the ability of ZU to secure and manage government and external sources of funding.
3	Accreditation, Program & Academic Quality	Risks related to maintaining the highest level of teaching, program and academic quality. This includes risks related to obtaining and maintaining accreditations, designing programs in line with job market requirements and building strong capabilities in the educational sector.
4	Students	Risks related to the attraction and retention of students and developing student capabilities so that they can launch successful careers in the private and public sectors. In addition, this will cover risks related to maintaining a safe, inclusive and supportive environment for all students at ZU, including underprivileged students, students of determination and other

		vulnerable students.
5	People	Risks related to attracting, retaining and developing faculty and staff of the right caliber in ZU, and ensuring their well-being, so that they can achieve the highest level of administrative, academic and research performance.
6	Research	Risks related to developing research capabilities, and generating relevant, valuable and timely research in line with ZU's strategic objectives and the UAE vision, in a safe and ethical manner.
7	Technology & Information	Risks related to the leakage of confidential information, data quality, system utilization and availability, and the implementation of new technologies.
8	Projects	Risks related to effective project management, including scoping, costing, quality and resource optimization.
9	Compliance & HSSE	Risks related to both internal and external compliance and HSSE incidents. This includes the adherence of ZU staff to internal mandates, policies and procedures as well as the adherence of ZU to relevant federal and local regulations.

6. Risk Management Operating Model

6.1 Reporting to the Internal Audit Department

- 6.1.1** The ERM Function shall be set under the Internal Audit Department, which in turn reports directly to the President. The ERM Function will include a Risk Manager who reports to the Director of Internal Audit, in addition to other staff members.
- 6.1.2** The ERM Function shall be responsible for not only the oversight of risk management activities but also for the consolidation and reporting of key organization-wide risks. Once the ERM Function is deemed to be sufficiently mature, the reporting structure shall be reevaluated.
- 6.1.3** The EC is represented by the Vice President, Chief Administration & Finance Officer, Provost and Chief Academic Officer, Assistant Provost for Student Affairs, Associate Provost for Academic Services and Assistant Provost for Research. They are responsible for the validation and mitigation of high-rated and strategic cross-functional risks.
- 6.1.4** The ARCC is responsible for evaluating the effectiveness of risk management practices at ZU and approving the ERM Framework (which is detailed in relevant policies and procedures) and Corporate Risk Register. The UC has ultimate responsibility for ensuring risks are managed and the risk management system at ZU is effective. The UC is responsible for setting the risk appetite and approving the ERM Policy and ZU Corporate Risk Register once reviewed and initially approved by the ARCC. The UC includes the President as a member.
- 6.1.5** The Risk Champions (i.e. Department Directors) are responsible for conducting the department risk management activities themselves. Risk Champions shall conduct risk identification and risk assessment workshops for the risks owned by their departments to facilitate the development of Departmental Risk Registers, inclusive of suggested treatment strategies.
- 6.1.6** In the incubation period, the ERM Function may facilitate risk identification and assessment workshops and assist in documenting and reviewing risk information until Risk Champions are sufficiently trained and inducted.
- 6.1.7** The completed Departmental Risk Registers shall be reported to the associated EC member for review and approval. Thereafter, the ERM Function shall facilitate the selection and consolidation of higher rated strategic risks from all Departmental Risk Registers in the form of a Corporate Risk Register. This will then be presented and discussed at the EC meeting together with the Director of Internal Audit (i.e. the Head of the ERM Function).
- 6.1.8** The Corporate Risk Register and decisions made in relation to these risks shall be endorsed and approved by the ARCC, before receiving ultimate approval from the UC.
- 6.1.9** The following illustration depicts the operating model of the ERM Function:



6.2 RACI Matrix

The following table depicts the RACI Authority Matrix for the ERM Framework. The RACI Authority Matrix details who takes on the roles in a given activity regarding Responsible, Accountable, Consult and Inform.

Particulars	UC	ARCC	VP	EC	ERM	RC
ERM Framework Policy Change Management	A2	A1	C	C	R	I
ERM Framework Procedural Change Management	I	A2	A1	C	R	I
Risk Training Policies	I	C	A	C	R	I
ERM Framework Self-Assessment	I	C	A	C	R	C
Risk Appetite Review and Update	A2	A1	C	C	R	I
Risk Assessment Criteria Review and Update	I	A2	A1	C	R	I
Corporate Risk Register	A2	A1	C	C	R	I
Departmental Risk Registers	I	I	I	A	C	R
Risk Responses Formalization	C	C	A*	R*	C	R*
Risk Management Plan	I	C	A	C	R	I
Stakeholder Communication Plan	I	I	A	C	R	I

*Risk responses shall be formalized considering the scope of responsibilities detailed in the Risk Treatment Ownership Matrix.

LEGEND	
UC	University Council

ARCC	Audit, Risk & Compliance Committee
VP	Vice President
EC	Executive Committee
ERM	Enterprise Risk Management Function
RC	Risk Champions
R	Responsible
A	Accountable/Ultimate Approver
A1	First Approver
A2	Second Approver
C	Consulted
I	Informed

6.3 Risk Treatment Ownership Matrix

- 6.3.1** The Risk Treatment Ownership Matrix assigns the risk treatment ownership based on the risk rating of risks. The Risk Treatment Owner (RTO) is tasked with the implementation and reporting of identified risk treatment strategies.
- 6.3.2** All RTOs should be identified with reference to their function and position within the organization i.e. job title. It is possible to have two types of RTOs; an Accountable RTO and a Responsible RTO. This means that the Accountable RTO may delegate some of the execution/planning to another individual, who would thereby be responsible for the execution of the risk treatment strategy. However, as the name suggests, the accountability for the success of the risk treatment strategy will lie with the Accountable RTO. For example, the Vice President may delegate aspects of the development of a Project Plan to a Risk Champion of the Strategy & Future Department.
- 6.3.3** The following table depicts the RTO matrix, which will serve as a guidance for assigning ownership for Accountable RTO. However, it is the responsibility of the Risk Champion and / or EC member to decide whether

this role is appropriate to delegate for specific risks. More details of their responsibilities can be found in the appendices.

Risk Treatment Ownership Particulars for Risks that have Scores of	UC	ECM	RC
Low (1-2)			RTO
Moderate (3-6)			RTO
High (8-12 & 5)		RTO	
Significant (15-16)*		RTO	
Extreme (20-25)*	RTO		

LEGEND	
UC	University Council (which includes the President)
ECM	EC Members
RC	Risk Champions
RTO	Risk Treatment Owner

6.4 Internal Audit Safeguards

6.4.1 Given that Internal Audit is not permitted to conduct any execution-related roles of the entities that they audit, it is important to maintain certain safeguards in order to protect the independence of the Internal Audit Department.

6.4.2 The Internal Audit Department shall not undertake any management functions when performing ERM activities. Such functions include:

- a) **Risk appetite:** Setting the risk appetite for risk management is purely a management role and shall not be established by the Internal Audit Department. However, the Internal Audit Department may provide guidance or suggest input to its development as a result of their strong understanding of the organization;

- b) **Risk management operations:** The Internal Audit Department may not impose any risk management processes. Risk management, while a corporate initiative, is mandated only by management;
- c) **Risk ownership:** The Internal Audit Department shall not be accountable for the management of individual risks; and
- d) **Risk treatment:** The Internal Audit Department shall not take decisions on which risks should be actioned nor how they shall be actioned. Similarly, it is not the Internal Audit Department's role to execute risk strategies on management's behalf.

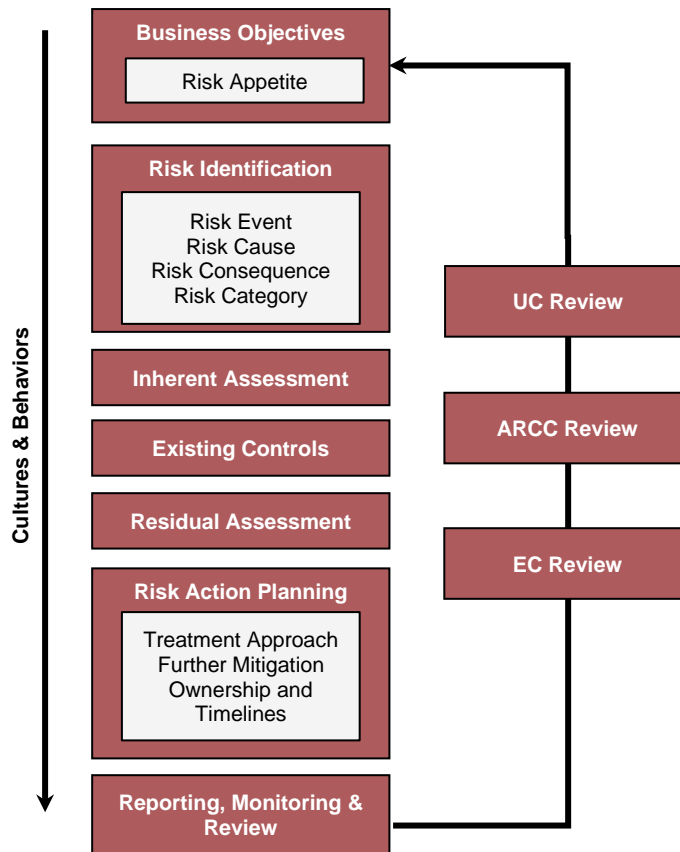
6.4.3 While the above activities are prohibited for the Internal Audit Department to undertake, the Internal Audit Department may provide guidance or suggestions on these given their strong knowledge of the organization.

6.4.4 Conversely, the following are legitimate roles undertaken by the Internal Audit Department:

- a) **Risk strategy:** The Internal Audit Department may assist in developing the risk strategy with the EC which is approved by the President and ARCC;
- b) **ERM framework:** The Internal Audit Department may develop or conduct maintenance for the framework and obtain the appropriate approvals;
- c) **Reporting:** The Internal Audit Department may provide consolidated reporting on the risk landscape to facilitate management decision-making;
- d) **Risk management operations:** The Internal Audit Department may coordinate ERM activities in order to activate the ERM Function;
- e) **Risk assessment:** While the Internal Audit Department is not the risk owner, they may facilitate the identification and evaluation of risks with risk owners, providing coaching to management on appropriate risk responses; and
- f) **Assurance:** The Internal Audit Department may review and evaluate the management and reporting of key risks, ensuring they are correctly evaluated. They may also evaluate and provide assurance on the risk management process. However, they shall not provide assurance on any part of the ERM Framework for which they are responsible.

6.5 Risk Management Process

There are a number of key activities required to establish a robust and sustainable risk management system at ZU, specifically the process that is adopted. The diagram below illustrates the key steps required to ensure the effective application of the risk assessment process:



1. Identifying and describing risks

- Consider the organizational context;
- Capture risk event, cause and consequence;
- Allocate a risk owner with the greatest awareness of the risk; and
- Assign a risk category.

2. Inherent/Gross Assessment

Assess likelihood and impact:

- Based on the severity of the risk without controls in place (Inherent/Gross); and
- Using the Risk Assessment Criteria.

3. Existing Controls

- List all of the existing controls which are currently in place to manage the risk.

4. Residual/Net Assessment

Assess likelihood and impact:

- Based on the severity of the risks considering existing controls (Residual/Net); and
- Using the Risk Assessment Criteria.

5. Action Planning

- Select the treatment approach:
 - Treat
 - Tolerate
 - Transfer
 - Terminate
- Identify further actions as required including owner and timescales; and
- Challenge based on the analysis of cost and effectiveness.

6. Risk monitoring and review

- Reporting following the cycle;
- Ongoing review and discussion around the risks and supporting information; and
- Monitoring of the risks, actions and trends.

7. Oversight

- Ongoing review and challenge from management with the support of the Risk Champions to facilitate the approach; and
- Further review and challenge will be provided from the EC, ARCC and UC (which includes the President).

6.6 Embedding Risk Management

6.6.1 To ensure that risk management activities are embedded within ZU such that they create and protect the organizational values, the following shall guide the approach to risk management:

- a) The UC shall have the ultimate responsibility for risk management, delegating core risk management activities to appropriate management layers to ensure:
 - The risk management framework is embedded;
 - The receipt of periodic risk reporting on the risk landscape; and
 - Determine the overall risk appetite.
- b) The ERM Framework shall be reviewed annually by the ERM Function, the Vice President and ARCC and aligned with the strategic objectives, strategic planning, project management and decision-making processes. Specific ERM Framework elements such as the risk appetite or ERM Policy shall be reviewed in line with the table for “Review and Changes to the ERM Framework” in Section 4.4;
- c) The Risk Champions shall conduct biannual risk identification workshops to identify risks and controls within their department’s risk landscape, together with the Risk Manager, who in turn facilitates the identification of risks and assists in the development of controls;
- d) The Risk Champions shall conduct biannual risk assessment workshops within their departments in order to assess risks, assign risk scores and identify action plans to remediate them, together with the Risk Manager;
- e) The Risk Champions shall develop the Departmental Risk Registers with the support of the ERM Function, which in turn facilitates in the development by challenging the Risk Champions to capture the risks reflective of the respective departments;
- f) The ERM Function shall assist in the development of the Corporate Risk Register based on the biannual risk workshops and Departmental Risk Registers, which will be reported to the EC for validation;
- g) The EC shall meet on a biannual basis to discuss key risks, their scores and evaluate risk treatment strategies, together with the ERM Function. Outcomes of this meeting shall be reviewed by the ARCC;
- h) The ARCC and UC shall ratify and approve decisions made in relation to the Corporate Risk Register by the EC; and
- i) Regular monitoring over the risk landscape, policy violations and progress on risk treatment strategies shall take place and be reported to the EC, ARCC and UC by the ERM Function. Risk reporting shall include the following:
 - Updates made to the Corporate Risk Register;
 - Changes in the heat maps;
 - Status of treatment plans; and
 - Latest relevant market data.

- 6.6.2** Risks shall be managed so that the level of exposure relating to a particular activity will be proportionate to the significance of that activity to ZU. When evaluating the appropriate response to a risk, the following shall be considered:
- a) **Tolerating the risk:** Accepting the risk or taking / increasing the risk in order to pursue an opportunity;
 - b) **Terminating the risk:** Removing the risk source or avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
 - c) **Treating the risk:** Changing the likelihood by introducing new controls or changing the consequences by introducing a mitigation strategy; and
 - d) **Transferring the risk:** Sharing the risk with another party or transferring the risk e.g. insurance.
- 6.6.3** It is not the intention of this framework to remove all risks or to manage risks to a low severity assessment. ZU shall take informed risks in order to be successful. Risk Champions shall give clear consideration to action priority on the basis of ease, cost and impact of implementation.
- 6.6.4** ZU shall have in place recovery plans to ensure the continuity of the business in the event of a risk materializing.
- 6.6.5** Executive management shall provide adequate support and endorsement for risk management training and activities.
- 6.6.6** The ERM Framework shall be applied consistently across all parts of ZU's activities and embedded in culture and operations.

7. Related Policies and Laws

N/A

8. Administration

This policy is administered by the Internal Audit Department.

9. Revision History

Date	Revision
17 February 2023	Administrative change: <ul style="list-style-type: none">• Updated information header.• Updated policy number from UNI-ADM-06 to UNI-GOV-601.
31 December 2020	President's Decree issued (PD#112 of 2020).
17 December 2020	Approved by the University Council (No.4 of 2020) Revisions: <ul style="list-style-type: none">• Entirely redrafted to be appropriate to current requirements;• "Enterprise" added to name of the policy.
18 December 2019	Updated the policy number (from UNI-ADM-05) and the numbering format.
15 May 2018	Approved by the University Council to be moved from the Financial Resources policy group to the University Administration policy group to be administered by the Office of the Vice-President, with no changes required (President's Decision # 20 of 2018).
16 June 2015	New policy required by CAA approved by the University Council.

Attachments:

- Appendix 1: Risk Heat Map
- Appendix 2: Role & Responsibilities
- Appendix 3: Risk Assessment Criteria

Appendices

Appendix 1: Risk Heat Map

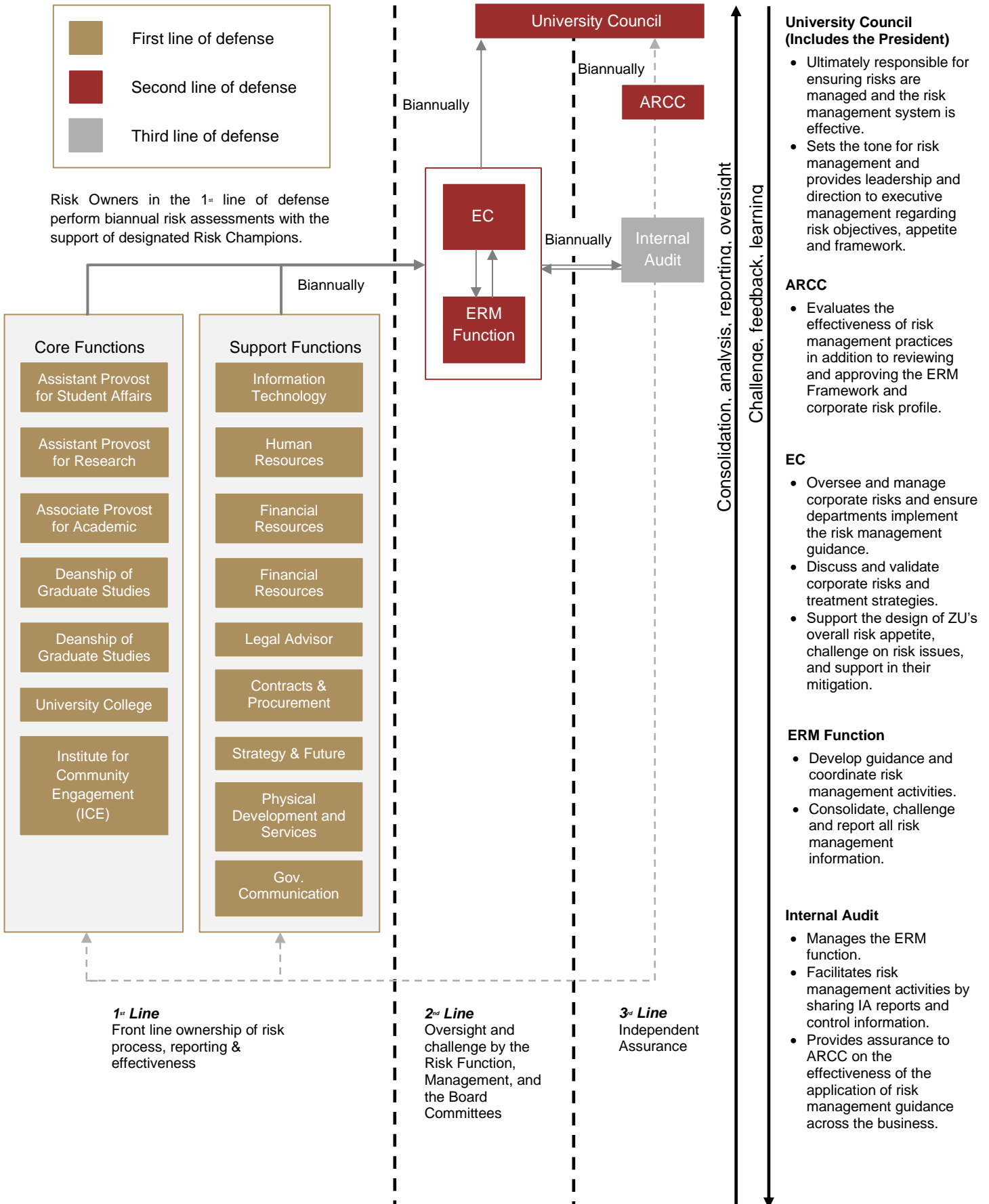
- 1.1 When rating the inherent and residual risk scores, the following risk heat map will be used to determine the severity, taking into account the impact and likelihood scores allocated.
- 1.2 Required actions shall depend on the risk severity and are summarised in the table below, although this shall also consider the established risk appetite and cost-benefit analysis of expected risk treatment strategies.

Impact	5	High	High	Significant	Extreme	Extreme
	4	Moderate	High	High	Significant	Extreme
	3	Moderate	Moderate	High	High	Significant
	2	Low	Moderate	Moderate	High	High
	1	Low	Low	Moderate	Moderate	High
		1	2	3	4	5
		Likelihood				

Risk Severity	Corresponding Guiding Action
Extreme	Immediate action required by EC members and the UC with detailed planning, allocation of resources and regular monitoring.
Significant	Potential to become an extreme risk, therefore requiring immediate action by relevant EC members with some planning, allocation of resources and monitoring.
High	Potential to become a significant risk, therefore requiring immediate action by the Risk Owners with some planning, allocation of resources and monitoring.
Moderate	Management responsibility must be specified, and the risk monitored.
Low	Monitor and manage by routine procedures.

Appendix 2 - Roles & Responsibilities

The roles and responsibilities of ZU's key risk management stakeholders are defined below. They are not intended to replace existing accountabilities and it is not an exhaustive list of tasks to be undertaken.



Who	What	When	Activities	Output
UC (Includes the President)	Approves and ratifies the Corporate Risk Register	Biannually	<p>Reviews and provides challenge to the Corporate Risk Register and summary reports that are presented by the ARCC, in consideration of contextual information such as the strategic objectives and external environment. Key decisions, particularly on treatment strategies are then fed back to the relevant stakeholders for action</p> <p>The UC will closely examine suggested treatment strategies to ensure:</p> <ul style="list-style-type: none"> - They are adequate to address associated risks; - Adequate seniority is assigned to oversee their implementation; and - That there is a reasonable effort made to implement and progress treatment strategies. 	<p>i) Approved and communicated ZU Corporate Risk Register; and</p> <p>ii) Feedback to stakeholders on key decisions made and actions required, captured in meeting minutes</p>
	Sets the Risk Appetite and approves the ERM Policy	Annually	<p>Reviews the Risk Appetite and changes to the ERM Policy presented by the ARCC. The UC ensures that the policy adequately considers the business operating environment and context, and that the suggested appetite statements, KRIs and thresholds adequately represent the risk that is tolerated and accepted, and best reflects ZU's interests.</p>	Approved and communicated Risk Appetite and ERM Policy
ARCC	Reviews and monitors ZU's strategic risks	Biannually	<p>Reviews summary risk reports that contain an overview of ZU's corporate risks, key updates or movements and items requiring action. Key recommendations, particularly on treatment strategies are then fed back to the relevant stakeholders for action.</p>	<p>i) Updated ZU Corporate Risk Register (<i>awaiting ultimate approval from the UC</i>); and</p> <p>ii) Feedback to stakeholders on key decisions made and actions required, captured in meeting minutes</p>
	Approves the Risk Appetite, ERM Policy and the ERM Framework	Annually	<p>Approves the Risk Appetite, ERM Policy and ERM Framework in consideration of the business operating environment and the education sector.</p>	<p>i) Approved ERM Policy (<i>awaiting ultimate approval from the UC</i>);</p> <p>ii) Approved ERM Procedures; and</p> <p>iii) Approved Risk Appetite (<i>awaiting ultimate approval from the UC</i>) and Assessment Criteria</p>
EC	Promotes a 'risk-aware' culture	Ongoing	<p>Consciously considers risk in all strategic decisions and processes, encouraging the communication of potential risks and concerns for action. Also ensures that relevant departments are implementing the risk management guidance.</p>	Regular updates regarding risk management to the business and discussions on potential risks
	Reviews and discusses ZU's Corporate Risk Profile	Biannually	<p>Reviews and discusses the risk report prepared by the ERM Function that provides an update on ZU's corporate risk profile. Discussions will include:</p> <ul style="list-style-type: none"> - Overview of the corporate risks; 	<p>i) Revised Corporate Risk Register, including action plans (<i>awaiting subsequent approval from the ARCC</i>); and</p> <p>ii) Feedback to stakeholders on key decisions made and</p>

			<ul style="list-style-type: none"> - Key risk updates / movements / areas for consideration, led by relevant risk champions; - Update on key actions due, approaching due date or are overdue; - Potential internal or external events that could impact a corporate risk; and - Periodic deep-dives into key topics that could impact ZU's strategic objectives as well as its risk profile, to determine appropriate actions to take. 	actions required, captured in meeting minutes.
	Reviews and approves the Departmental Risk Registers	Biannually	<p>Reviews and approves the Departmental Risk Registers developed by the Risk Champions advising on any modifications to reflect:</p> <ul style="list-style-type: none"> - New or emerging risks; - Accurate risk scores and owners; and - Adjustments to risk treatment strategies. 	Approved Departmental Risk Registers
Director of Internal Audit	Facilitates EC meetings	Biannually	Presents the risk report to the EC and facilitates an open discussion by all attendees, seeking input from attendees on key risks / treatment strategies to determine what updates are required to ZU's corporate risk profile.	<ul style="list-style-type: none"> i) Updated Corporate Risk Register, including action plans (<i>awaiting subsequent approval from the ARCC</i>); and ii) Updated EC risk report
	Reviews the EC risk report	Biannually	Reviews the risk report for the EC prepared by the Risk Manager, ensuring it provides an accurate view of the ZU risk profile and its progress in managing risks in accordance with the Risk Appetite. The Director of Internal Audit may find it pertinent to also supplement the report with relevant external and internal market contextual information.	Updated EC risk report
	Reviews the Corporate Risk Register	Biannually	Reviews the consolidated corporate risk profile prepared by the Risk Manager before it is shared with the EC, providing feedback for incorporation.	Updated Corporate Risk Register (<i>awaiting endorsement from the EC</i>)
	Reviews the Departmental Risk Registers	Biannually	Reviews the Departmental Risk Register prepared by the Risk Champions in conjunction with the Risk Manager before it is shared with the relevant EC member, providing feedback for incorporation.	Updated Departmental Risk Registers (<i>awaiting ultimate approval from the relevant EC member</i>)
	Reviews the ERM Framework	Annually	Reviews suggested updates to ERM documentation, including Policy, Procedures, Risk Appetite and Risk Assessment Criteria to reflect ZU's operating model, strategic objectives, new developments in the educational sector and Dubai's risk landscape.	<ul style="list-style-type: none"> i) Updated Risk Appetite and Risk Assessment Criteria (<i>awaiting subsequent approval from the ARCC</i>); and ii) Updated ERM Policy, Procedures and templates (<i>awaiting subsequent approval from the Vice President as relevant and the ARCC</i>)

Risk Manager	Reviews key risk updates	Quarterly	Obtains an update on the status of risk treatment strategies and risks by risk owners, providing an avenue of support in case of any obstacles encountered.	Escalation or support for risk treatment strategies
	Prepares an EC risk report	Biannually	Prepares a risk report for the EC that provides an overview on: <ul style="list-style-type: none"> - ZU's risk heat map and corporate risks; - Key changes to the risk profile; - Potential risks that ZU could face that should be considered; and - Key risks / topics for discussion. 	EC risk report
	Prepares the Corporate Risk Register	Biannually	Prepares an updated Corporate Risk Register through a review and assessment of the following: <ul style="list-style-type: none"> - Strategic priorities; - Performance against strategy; - Changes in the external business environment; and - Departmental risk profile. 	Corporate Risk Register
	Reviews the Departmental Risk Registers	Biannually	Reviews the Department Risk Registers prepared by the Risk Champion to ensure they adequately represent the outcomes of risk workshops and business context. In addition, the Risk Manager ensures that risk management guidelines are being adhered to e.g. appropriate usage of Risk Assessment Criteria.	Updated Departmental Risk Registers <i>(awaiting subsequent approval from the Director of Internal Audit)</i>
	Prepares updates to the ERM Framework	Annually	Ensures that ERM Policy and Procedures are kept up to date with the requirements of ZU and the changing risk landscape. Prepares suggested updates to the Risk Appetite and Risk Assessment Criteria to reflect ZU's strategic objectives. The ERM policy and procedures will be submitted to the Director of Internal Audit for review, before obtaining the approvals of the Vice President (as relevant), ARCC and UC.	i) Risk Appetite and Risk Assessment Criteria; and ii) ERM Policy, Procedures and templates
Risk Champion	Prepares the Departmental Risk Register	Biannually	Conducts biannual risk identification and assessment meetings to update the relevant department risks. These will be documented in Departmental Risk Registers and should consider: <ul style="list-style-type: none"> - Movements in the risk severity scores; - Control changes; - Updates on treatments due for implementation; - Other factors / events that could potentially have an impact on the risk; and 	Departmental Risk Register

			- New risks that should be taken into consideration.	
Risk Owner	Monitors and manages assigned risks	Ongoing	Ensures that the risks they are responsible for are closely monitored and controlled, with sufficient treatments (including timeframes and owners) in place to further address the risk if it has not been lowered to an acceptable level. The implementation of treatments will be overseen by the Risk Owner, even if the responsibility for actioning the treatment is another individual i.e. the Risk Treatment Owner (see below).	Adequately managed risks with additional treatments being implemented in the required timeframe
Risk Treatment Owner	Implements delegated risk treatment strategies	Ongoing	Implements the associated agreed risk treatment strategy documented within the risk register, ensuring that it is completed by the prescribed timeline. In addition, the Risk Treatment Owner evaluates the effectiveness of the treatment strategy in lowering the risk to an acceptable level and reports to the relevant authority as needed e.g. in case additional support is required.	Implemented risk treatment strategies
All Staff	Identifies, assesses and escalates risks	Ongoing	Continues to monitor ZU's risk landscape and if a new potential risk is identified, escalates it to their Line Manager and / or the ERM Function for consideration as to whether it should be closely monitored at a strategic level or whether it is the responsibility of Management to monitor.	New potential risk escalated to their Line Manager and / or the ERM Function for consideration

Appendix 3: Risk Assessment Criteria

Risk Impact Criteria (TBC)

Risk Category	1 - Low	2 - Moderate	3 - High	4 - Significant	5 - Extreme
Strategy & Governance					
Financial					
Accreditation, Program & Academic Quality					
Students					
People					
Research					
Technology & Information					
Projects					
Compliance & HSSE					

Risk Likelihood Criteria

Likelihood	1 - Rare	2 - Unlikely	3 - Possible	4 - Likely	5 - Almost certain
Probability	<10%	10-30%	30-50%	50-90%	>90%
	Has not happened over the last 5 years	Has happened at least once in the last 5 years	Has happened at least once in the last 24 months	Has happened at least once in the last 12 months	Has happened on a regular basis over the last 12 months
Description	Event may occur only in exceptional circumstances	Event may occur in exceptional circumstances	Event could occur at sometime	Event will occur fairly often	Event will probably occur in most circumstances