RISK MANAGEMENT POLICY

Policy Number	**Version 1.1**
Date of Approval	**October 2024**
Policy Sponsor	**Executive Director: Office of the Vice-Chancellor and Principal**
Next Review Date	**October 2027**
Approver	**Council**
Department/Unit	**Enterprise Risk Management [ERM]**

TABLE OF CONTENTS

1. PURPOSE

To provide a strategic and integrated approach to the management of institutional (enterprise) risks at the University.

2. SCOPE

2.1 This policy applies to all University strategies, projects, plans, processes, and initiatives, across all areas of the University.

2.2 Applicable to all staff and students, without exception.

2.3 The University works closely with third parties and all those with whom it enters into partnership with must ensure that they adhere to this policy.

3. OBJECTIVE(S)

3.1 The overarching purpose for the Risk Management Policy is to provide direction and, increase the confidence of the University in achieving its goals and objectives, whilst protecting students, staff and the reputation and sustainability of the University.

3.2 To integrate and embed a consistent and robust approach to managing risk by adopting an Enterprise Risk Management (ERM) framework, methodology and processes across the University.

3.3 To enable planning and strategic decision-making processes to be informed by accurate and congruent assessment of risk. The University recognizes that risk management is a systematic and formalised process to identify, assess, measure, monitor, and report risks and therefore adopts a comprehensive and integrated approach to the management of risk.

3.4 To engender risk management across the University that identifies operational risks and facilitates feedback into the institutional and strategic risk arena.

3.5 Promote a risk awareness culture that encourages environmental horizon scanning and the taking of managed risks in pursuit of opportunities and innovation that benefits the University.

3.6 To integrate risk management into strategic, financial, project, operational, and performance management processes of the University. The University embraces intelligent risk taking and recognizes that risk can have both positive and negative consequences. Risks will be managed in a way that effectively manage potential opportunities and adverse effects to the University.

3.7 To specify key risk management responsibilities across all areas of the University, and to augment the Combined Assurance Framework of the University.

3.8 To provide assurance to:

> 3.8.1 The Audit and Risk Oversight Committee (AROC), that managers across the University are focusing on key risks.

> 3.8.2 Council, that the University's robust ERM framework and methodology to manage risk provides confidence towards the achievement of its strategic, tactical and operational objectives.

3.9 Improve institutional performance.

3.10 To align with leading practices in ERM.

4. POLICY PRINCIPLE

4.1 Policy Overview

The realisation of the University's Vision 2030 One Smart CPUT (the 10-year Strategic Plan) depends on the University being able to take calculated risks in a way that does not jeopardise the direct interests of stakeholders. Sound management of risk will enable the University to anticipate and respond to changes in its service delivery environment, as well as make informed decisions under conditions of uncertainty.

The University subscribes to the fundamental principles that all resources will be applied economically and intelligently to ensure:
4.1.1 The highest standards of service delivery;

4.1.2 A management system containing the appropriate elements aimed at minimising risks and costs, taking advantage of opportunities in the interest of all stakeholders;

4.1.3 Education and training of all staff and students to ensure continuous improvement in knowledge, skills and capabilities which facilitate consistent conformance to the stakeholders' expectations; and

4.1.4 Maintaining an environment, which promotes the right attitude and sensitivity towards internal and external stakeholder satisfaction.

An institution-wide approach to risk management is adopted by the University, which means that every key risk in each part of the University will be included in a structured and systematic process of risk identification, analysis and evaluation. Risk management will be fully integrated with the University's strategic, financial

and annual planning processes. It is expected that the risk management processes will become embedded into the University's systems and processes, ensuring that our responses to risks remain current and dynamic. All risk management efforts will be focused on supporting the University strategic goals, objectives and focus areas of the Vision 2030 Strategic Plan. Equally, they will ensure compliance with relevant legislation, and fulfil the expectations of students, staff, and other stakeholders in terms of governance.

4.2 Enterprise Risk Management Framework and Methodology

4.2.1 The CPUT ERM framework (see CPUT ERM Framework and Methodology document on the institutional repository) involves the systematic and proactive application of the policy, and practices by understanding the context, assessing the risk, taking actions to manage and respond to that risk and reporting it to the appropriate structures.

4.2.2 This framework will be integrated into the University's ways of working at strategic, operational and project level.

4.2.3 Awareness and where appropriate training of individuals will be undertaken to improve capability, promote a culture of risk management and develop a skilled community of practice seeded within the University.

4.2.4 The University's risk appetite and tolerance approach sets out the overarching principles that define its appetite for risk and guides the University's approach to the acceptance of risk. Risk appetite is determined for the University as a whole, and for individual issues as appropriate by Council.

4.2.5 Specifically, the CPUT ERM process:

4.2.5.1 Internal and external context setting – the process of appreciating the internal and external environmental factors that present both downside and upside risks which influence the achievement of key university objectives.

4.2.5.2 Risk Identification – The process of discovering and describing the risk, within a risk register, that may help or hinder the University achieving its objectives.

4.2.5.3 Risk Analysis – Comprehending the nature of the risk and its characteristics stating the contributing factors (root causes), velocity and impacts of the risk.

4.2.5.4 Risk Evaluation – Utilising risk scoring criteria to assess the likelihood, impact, and the nature and magnitude of its consequences. This scoring also enables prioritisation of risks.

4.2.5.5 Risk Mitigation – specific, measurable, attainable, realistic and time framed (SMART) actions assigned to an owner that will reduce negative or raise positive impacts of the risk.

4.2.5.6 Risk Monitoring – Establishing a regular process to review the risk, its mitigating actions and revised scoring to demonstrate changes to the risk profile.

4.2.5.7 Risk Reporting – Communicates to the appropriate structures risks that the University identifies and demonstrates actions being taken to mitigate those risks.

4.3 Governance

Enterprise risk management, as both a process and discipline is approached from a governance perspective. The principal goal of ERM is to ensure that the University continues to create value for its stakeholders (including students, staff, donor community, management, and Council) through achieving its strategic objectives whilst exploiting opportunities and managing risks. Risk management and opportunity management go hand in hand. The King IV Report on Governance for South Africa (2016) for example defines risk as "…. uncertain future events that could influence, both in a negative and positive manner, the achievement of the institutional objectives." It states that risk arises as much from failing to capture opportunities when pursuing strategic objectives as it does from a threat that something bad will happen.

Opportunities that arise will be identified when necessary and managed within the enterprise risk management process.

4.4 Risk and Opportunity Management

Risk refers to an unwanted outcome, actual or potential, to the University's service delivery and other performance objectives, caused by the presence of risk factor(s). Some risk factor(s) also present upside potential, which Management must be aware of and be prepared to exploit. Such opportunities are encompassed in this definition of risk. In short, risk is the effect of uncertainty on objectives, including opportunities. Enterprise risk management is a systematic and formalised process instituted by the University to assess, manage and monitor risks.

Since opportunities arise from risks, this means that opportunities will be incorporated in the same process as followed with managing risk. The contributing factors and the impacts of opportunities will be identified as well as its associated controls and treatments. The value of rating the opportunity against the effort required does not warrant the rating exercise at this initial stage. Once a list of opportunities present itself then a rating exercise will become worthwhile against the competing opportunity list.

The risk-opportunity matrix (see ERM framework and methodology document) will inform the understanding, analysis and prioritisation of key opportunities to be pursued by the University. Once an assessment is completed of the opportunity, this will be presented to the Quality and Risk Management (QARM) Committee and after consultation included in the risk register.

4.5 The benefits of enterprise risk management

The University implements and maintains effective, efficient, and transparent systems of risk management and internal control. Risk management will assist the University to achieve, among other things, the following outcomes needed to underpin and enhance institutional performance:

4.5.1 Consideration of risk during strategy and objective setting;

4.5.2 Exploitation or capitalisation of opportunities;

4.5.3 Understanding and the proactive management of critical risks impacting goals throughout the University;

4.5.4 Alignment of internal audit focus with the risk profile of the University, to foster the combined assurance process;

4.5.5 Identification and implementation of cost effective, integrated responses to multiple risks;

4.5.6 Enabling Council and Management to have a portfolio view of risks across the entire University;

4.5.7 Rationalisation of resources (better value for money through more effective and efficient use of resources);

4.5.8 Reduction in operational surprises and losses;

4.5.9 Reporting with greater confidence;

4.5.10 Support governance responsibilities and satisfy legal and regulatory requirements;

4.5.11 More sustainable and reliable delivery of services;

4.5.12 Informed decisions underpinned by appropriate rigour and analysis;

4.5.13 Augments the creation and sharing of innovative solutions;

4.5.14 Prevention of fraud, theft and corruption; and;

4.5.1.5 Better outputs and outcomes through improved project management.

5. COMMON TERMS AND DEFINITIONS

5.1 Combined Assurance
Combined assurance is the process of internal and external assurance providers, working together and combining activities to reach the goal of communicating information to management and the governance bodies of the University. The objective is to integrate and align assurance processes so that executive management and governance bodies (Council and the Audit and Risk Oversight Committee) obtain a holistic view of the effectiveness of the University's governance processes, risks, and controls to enable them to set priorities and take the necessary action.

5.2 Enterprise risk management (ERM)
Enterprise (integrated) or institutional risk management is a continuous, proactive, and systematic process, effected by CPUT's Council, Management and other personnel, applied in strategic planning and across the University, designed to identify potential events that may affect the University, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of goals.

5.3 Risk
The threat or possibility that an action or event will adversely or beneficially affect the University's ability to achieve its objectives. Risk is also the effect of uncertainty on achievement of objectives.

5.4 Risk appetite
The broad-based level of risk that the University is willing to accept in pursuing its institutional goals and its strategic imperatives.

5.5 Risk assessment
The process that enables management to understand the likelihood, impact, and velocity of potential events and associated risks. It entails and provides a conducive platform for the identification, analysis, evaluation, measurement, response, and reporting of key risks.

5.6 Risk Owners
University officials responsible for ensuring that approved risk responses to identified risks are effectively and efficiently implemented.

5.7 Risk tolerance
The acceptable level of variation relative to the achievement of goals. It is also the desired level of residual risk rating.

6.   RESPONSIBILITY

6.0   Role players

An effective Enterprise Risk Management framework permeates through existing management processes and provides assurance over the management of key risks, and interdependence between strategic and operational objectives. Risk management must be embedded throughout the University to enable all staff to have a role in identifying and mitigating risk and sharing good practice. Every employee is responsible for executing risk management processes and adhering to risk management procedures adopted by the University management in their areas of responsibilities.

6.1 RISK MANAGEMENT OVERSIGHT

6.1.1 Council

The Council, as specified in its terms of reference, takes an interest in risk management to the extent necessary to obtain comfort that properly established and functioning systems of risk management and internal control are in place to protect the University against significant risks and take advantage of opportunities.
Specifically, Council:

> 6.1.1.1 Approves the risk appetite and tolerance approach, and major decisions affecting the University's risk profile and exposure.

> 6.1.1.2 Annually reviews the University's overall approach to risk management.

> 6.1.1.3 Sets the tone and influences the culture of risk management within the University.

6.1.2 Audit and Risk Oversight Committee (AROC)

The Audit and Risk Oversight Committee (AROC) is an independent committee of Council responsible for oversight of the University's governance, risk management and control processes. The University is served by AROC and the committee's responsibilities regarding risk management are formally defined in the AROC Charter, specifying the terms of reference.
Specifically, among other aspects,

> 6.1.2.1 The AROC provides an independent and objective view on institutional risk management effectiveness. The standard number of meetings is 4 (four) per annum, excluding extra ordinary sessions.

> 6.1.2.2 Advises Council on the effectiveness of internal controls systems, including the management of risk.

6.1.2.3 Monitors the management of significant risks identified across the University.

6.1.2.4 Ensures that the Enterprise Risk Management framework and methodology has been adopted throughout the University.

6.1.3 Information Technology Governance Committee (ITGC)

The ITGC is a committee of Council that focuses on information, communication, and technology (ICT) related risks. It reviews all University IT related structures, policies, procedures, strategies, plans, projects, and budget to obtain comfort that key IT institutional and operational risks are being identified, understood, assessed, and effectively and efficiently managed and reported on timeously. All ICT risks are managed as part of the overall CPUT ERM Framework and Methodology. The standard number of meetings is 4 (four) per annum, excluding extra ordinary sessions. The ITGC discharges its risk responsibilities as codified in its approved terms of reference.

6.1.4 Quality Assurance and Risk Management Committee (QARM)

The Quality Assurance and Risk Management Committee (QARM), joint committee of Senate and Council, is chaired by the Vice Chancellor and Principal to assist in discharging the responsibilities for risk management and quality management.

6.1.4.1 The responsibilities of the QARM as formally defined in its terms of reference, on a high-level entail the review of risk and quality management progress and maturity of the University, the effectiveness of risk management activities, the key risks facing the University, and the responses to address these key risks. The standard number of meetings is 4 (four) per annum, excluding extra ordinary sessions.

6.1.4.2 Additionally QARM challenges and reviews 'high level' risks identified within the institutional and operational risk registers on a periodic basis.

6.1.4.3 Enables a process to review and where appropriate promote operational risks on to the institutional (enterprise) risk register.

6.1.5 Governance and Ethics Committee (GEC)

The GEC is a committee of Council that provides oversight on the response to ethics and compliance related risks, including forensics services, and financial crime risks. It reviews and provides guidance on all University ethics, compliance, privacy and information related structures, policies, procedures, strategies, plans, projects, and budget to obtain comfort that key ethics and compliance risks are managed within Council approved risk appetite and tolerance limits. The standard number of meetings is 4 (four) per annum, excluding extra ordinary sessions.

6.1.6 Institutional Combined Assurance Forum (ICAF)

The university's executive management must establish an Institutional Combined Assurance Forum (ICAF), with Council approved terms of reference to implement the tenets of the Council approved Combined Assurance Framework. Management must designate a member of the executive to provide oversight on the activities of the forum.

Specifically, the ICAF,

6.1.6.1 Advises, coordinates, and monitors the implementation of combined assurance initiatives across the university.

6.1.6.2 Ensures integrated combined assurance reporting across all faculties and support service functions.

6.1.6.3 Ensures executive management, Council, and its risk-related committees receive adequate, accurate, and timely risk and internal control information to effectively discharge their combined assurance oversight responsibilities.

6.2 RISK MANAGEMENT IMPLEMENTERS
6.2.1 Management

6.2.1.1 The Vice Chancellor and Principal drives university business on behalf of Council) is ultimately accountable to Council for the University's overall approach and management of risk. By setting the right tone at the top, the Vice Chancellor promotes accountability, integrity and other factors that will create a positive internal control environment.

All risk owners are expected to exercise due diligence and care in the management of identified risks, to ensure economic, timely, effective, and efficient implementation of agreed upon mitigating strategies (action plans).

6.2.1.2 Providing leadership, commitment, and resources to implement the Risk Management policy and internal controls.

6.2.1.3 Identifying and evaluating institutional and operational risks and managing the actions to mitigate those risks.

6.2.1.4 Undertake an annual review on the effectiveness of risk management and internal control providing an assurance report for review by Audit and Risk Oversight Committee, on behalf of Council.

6.2.1.5 Report its view of the institutional risk register to the Audit and Risk Oversight Committee on a regular basis.

6.2.1.6 Report to Council regularly on progress made against the performance indicators outlined in the University's Strategic Plan.

6.2.1.7 Challenge and review 'high level' risks identified within the institutional and operational risk registers on a periodic basis.

6.2.1.8 Enable a process to review and where appropriate promote operational risks (and other risks) on to the institutional risk register.

6.2.2 Faculty Deans and Directors of Support (Professional) Services

6.2.2.1 Provide leadership and commitment to implement the Risk Management policy within their faculty, department, division, function or unit.

6.2.2.2 Provide a resource to lead risk within their faculty, department, division, function or unit and who will become part of the University Combined Assurance Champions Forum (community of practice).

6.2.2.3 Identify and manage the operational risk (and other risks) portfolio with their senior leadership team on a regular basis.

6.2.2.4 Maintain their risk register and report progress to their quarterly performance review meetings.

6.2.2.5 Management is responsible for executing their responsibilities outlined in the ERM Framework and Methodology, the ERM Strategy and Implementation Plan and for integrating risk management into the operational routines.

6.2.3 Operational staff and/or other Officials

6.2.3.1 Operational staff and/or other officials are responsible for integrating risk management into their day-to-day activities.

6.2.3.2 They must ensure that their delegated risk management responsibilities are executed and continuously report on progress to their line managers.

6.3 ENTERPRISE RISK MANAGEMENT SUPPORT

6.3.1 Manager: Enterprise Risk Management

The Manager: Enterprise Risk Management (Manager: ERM) is the custodian of the Enterprise Risk Management Strategy and Framework, and coordinator of institutional (integrated) risk management activities throughout the University. The primary responsibility of the Manager: ERM is to bring to bear specialist expertise to assist the University in embedding risk management and leverage its benefits to enhance institutional strategic, tactical, and operational performance. This responsibility is executed by the Enterprise Risk Management (ERM) function in the Office of the Vice Chancellor, administratively reporting to the Executive Director, Office of the Vice Chancellor, and functionally to the Chair of the Audit and Risk Oversight Committee (AROC) of Council.

Specifically, the Manager: Enterprise Risk Management:

6.3.1.1 Drives the implementation of the Risk Management Policy and the Enterprise Risk Management Framework and Methodology across the University.

6.3.1.2 Provides subject matter expertise and training to senior management, Faculty, Support (Professional) Services and Combined Assurance Champions (community of practice) to enable implementation of the Risk Management Policy.

6.3.1.3 Reviews and adopts good practice risk management tools and techniques on a periodic basis.

6.3.1.4 Identifies and develops (in consultation with management) key resources to join the Combined Assurance Champions community of practice to support the University in developing good quality risk registers.

6.3.2 Combined Assurance Champions

Combined Assurance Champions are responsible for:
6.3.2.1 Supporting and developing faculty and support services risk registers on a regular basis and identify common themes across the University.

6.3.2.2 Supporting training and awareness of risk management throughout the University.

6.2.2.3 Attending and contributing to the activities of the Institutional Combined Assurance Forum and share good risk management practices and optimise risk performance across the University. The Forum's terms of reference are approved by Council, as part of the ERM Framework and Methodology.

6.2.2.4 Intervening in instances where the risk management efforts are being hampered, for example, by the lack of co-operation by management and other officials and the lack of skills and expertise. The Combined Assurance Champion should provide guidance and support to manage "problematic" risks and risks of a cross-functional nature that require a multiple participant approach, across functional, project, faculty, or departmental lines.

6.2.2.5 Facilitating the implementation of the ERM Framework and Methodology within their respective areas.

6.4 RISK MANAGEMENT ASSURANCE PROVIDERS

6.4.1 Internal Audit

6.4.1.1 The role of Internal Audit in enterprise risk management is to provide an independent, objective assurance and consulting service on the effectiveness of the University's system of risk management and internal control.

6.4.1.2 Internal Audit must evaluate the effectiveness of the entire system of risk management controls and provide recommendations for improvement where necessary. This will be considered in line with the risk profile of the University at the time of planning the internal audit coverage for the University, and in preparation for the integrated annual report.

6.4.2 External Audit

6.4.2.1 The External Auditor reviews the risk management process to ensure it complies with the requirements of the guidelines of the King IV Report on Good Governance for South Africa (2016), and other binding rules, codes, standards, and legislative prescripts, including the CPUT Institutional Statute.

6.4.2.2 The External Auditors, furthermore, consider risks during the strategic and detailed planning processes of the statutory audit.

Accountability and Authority:	
Implementation:	Executive Management
Compliance:	All executives and respective line management; Compliance Management Function
Monitoring and Evaluation:	ERM Services Function; Executive Director: Office of the VC and Principal
Development/Review:	ERM Services Function; Executive Director: Office of the VC and Principal
Approval Authority:	Council
Interpretation and Advice:	ERM Services Function; Executive Director: Office of the Vice-Chancellor and Principal

Policy Development Framework					
Policy Type(s):	A: Institutional Governance Policy C: Administrative Policy				
Type: Tick document category	Policy	✓	Guideline		Manual
	Procedure		Regulation		Plan
CPUT Statute and/or Regulation Reference no. and date:	Cape Peninsula University of Technology Statute, Government Notice No 46382 of 20 May 2022				

Relevant Legislation and/or Policy, Codes of practice, Professional authorities:	Constitution of South Africa Act, No. 108 of 1996
	Higher Education Act, No. 101 of 1997, as amended
	Income Tax Act, No. 58 of 1962
	Tax Administration Act 28 of 2011
	Companies Act, No. 71 of 2008, as amended
	Protection of Personal Information Act, No. 4 of 2013
	Prevention and Combating of Corrupt Activities Act, No. 12 of 2004
	Promotion of Access to Information, No. Act 2 of 2000
	ISO 31 000: 2018 Risk Management Standards
	COSO ERM Integrated Framework (2004, 2017)
	COSO Integrated Internal Control Framework (2017)
	King IV Report and Code for Good Governance for South Africa (2016)
	Association of Certified Fraud Examiners (ACFE)'s Fraud Examiners Manual (2022)
	ACFE Fraud Risk Governance and Management Scorecard (ACFE FRGMS)
	The IIAGlobal's Global Internal Audit Standards: GIAS (2023)
	The IIAGlobal's International Professional Practices Framework (IPPF)
	Information Systems Audit and Control Association (ISACA)'s Information Technology Audit Framework (2020)
	Information Systems Audit and Control Association (ISACA)'s Information System Security Management Standards and Practices (2020)
	Control Objectives for Information and related Technology (COBIT)
	CPUT's Approved Forensic Services process
	Compliance Institute of Southern Africa (CISA)'s Generally Accepted Compliance Management Framework and Practices
	Compliance Institute of Southern Africa (CISA)'s Compliance Risk Management Plans (CRMPs)
	UK Bribery Act

	US Foreign Corrupt Practices Act (FCPA)
	Eurozone's General Data Protection Regulations (GDPR)
	International Financial Reporting Standards (IFRS)
	National Institute of Standards and Technology (NIST)
	BCI Business Continuity Management Standards
Relevant Institutional Policies/ documents/manuals/ handbooks:	Vision 2030 One Smart CPUT Strategy (2021-2030)
	CPUT Ethics Framework
	CPUT Combined Assurance Framework (CAF)
	V2030 ERM Strategy
	ERM Framework and Methodology
	ERM Annual Implementation Plans
	Internal Audit Charter
	V2030 Internal Audit Strategy
	Internal Audit Annual Plans
	V2030 Compliance Strategy
	Compliance Management Programme
	Quality Management Framework
	V2030 Quality Management Strategic Plan
	V2030 Business Continuity Management (BCM) Strategy
	Business Continuity Policy (draft, en route for approval)
	Anti- Corruption anti-Bribery Policy
	Conflict of Interest Policy
	Gifts and Hospitality Policy
	Whistle Blowing Policy

Policy Reference and Version no.:	Version 1.1
Consultation Process: To be verified and signed off before approval	Approved by Council on 28 August 2021, after following the university's policy development process.
Policy Owner/Sponsor:	Executive Director: Office of the VC and Principal
Compliance Officers:	All Executives
Certification of Due process: To be verified and signed once approved by the relevant authority	*[signature]* _____ Vice Chancellor and Principal 30.10.2024 _____ Date

Approval Date		Commencement Date		Review Date	

REVISION HISTORY: Only applicable to amended or reviewed policies. Record details of amendments/revision.

Version No.	Approved/ Rescinded	Date	Approving Authority	Resolution Number/ (Minute number)	Date for next review (start date for review process)